

Labris UTM Yönetim Kılavuzu

<http://labrisnetworks.com/support-training/>

Tel: +90 850 455 4555



Labris
NETWORKS

1. Telif Hakkı

Tüm hakları saklıdır. Bu yayının hiçbir bölümü yazarın/yayıncının yazılı izni olmadan hiçbir şekilde veya hiçbir suretle, elektronik olarak, mekanik olarak, fotokopiyle, kaydederek veya başka türlü, çoğaltılamaz, bir erişim sisteminde saklanamaz veya iletilemez.

2. Feragatname

Ne yazar ne de yayıncı kitapta yer alan bilgilere ilişkin hiçbir bir şekilde beyan veya garanti vermez. Doğrudan veya dolaylı olarak bu kitapta yer alan bilgilerin kullanımından kaynaklanan veya kaynaklandığı iddia edilen hiçbir eylem için sorumluluk kabul edilmez.

© Copyright 2024-2025. All rights reserved.

3. Belge Düzeltme Tarihçesi

#	Belgeyi Değiştiren	Açıklama	Onaylayan
1			
2			
3			
4			
5			

1. TELİF HAKKI	1
2. FERAGATNAME.....	1
3. BELGE DÜZELTME TARİHÇESİ.....	1
4. LABRIS NETWORKS HAKKINDA	7
5. LABRIS UTM HAKKINDA	7
6. LABRIS UTM NASIL SATIN ALINIR?	8
7. LABRIS UTM CİHAZ DAĞITIM MİMARİSİ	9
8. CİHAZA BAĞLANMA.....	9
9. WEB YÖNETİCİ KONSOLUNA ERIŞME.....	9
9.1 Açılış sayfası veya ana ekranı anlama	11
9.1.1 Sistem Bilgisi.....	11
9.1.2 İmza Veri tabanı	12
9.1.3 Sistem Durumu.....	13
9.1.4 Uygulama Kullanımı.....	13
9.1.5 Ağ Arayüzleri.....	14
9.1.6 İşlem İstatistikleri	16
10. SİSTEM.....	17
10.1 Genel Ayarlar	18
10.1.1 Genel Ayarlar	18
10.1.2 SMTP Ayarları	21
10.2 Yönetim.....	22
10.2.1 Kullanıcılar	23
10.2.2 Profiller.....	25
10.3 Sertifika Yönetimi.....	27
10.3.1 Sertifikalar	27
10.3.2 Sertifika Otoritesi.....	30
10.4 Yedeklilik.....	33
10.4.1 Yüksek Kullanabilirlik Ayarları	33
10.4.2 Kontrol Ayarları	34
10.4.3 Yük Transfer Ayarları.....	37
10.4.4 Durum.....	37
10.5 Yedeklilik.....	38
10.5.1 Ayarlar.....	39
10.5.2 Yedekle ve Yapılandırma Ayarlarını Geri Yükle.....	39
10.5.3 Fabrika Ayarlarına Geri Yükle	40
10.5.4 Yedekler	40
10.6 Yazılım Güncelleme	41
10.7 Konsol Erişim	41
10.8 Lisans	43
10.8.1 Gelen Bakış.....	43
10.8.2 Lisansı Yükle	43
10.8.3 Lisans Detayları.....	44
11. AĞ.....	45
11.1 Arabirim	45
11.1.1 Arabirim Düzenleme.....	46
11.1.2 Arabirim Ekleme	48
11.1.2.1 Takma İsim.....	48
11.1.2.2 Köprü Arabirimi	49
11.1.2.3 VLAN Arabirimi.....	50
11.1.2.4 Bağlı Arabirimi	52
11.1.2.5 PPPoE.....	56
11.1.2.6 3G/4G	57
11.2 Statik Yönlendirme.....	58
11.3 SD-WAN.....	61
11.3.1 Ağ Geçitleri	62

11.3.2 Ağ Geçidi Grupları.....	63
11.4 DHCP.....	64
11.4.1 Sunucu.....	65
11.4.2 Kira Listesi.....	70
11.4.3 Yönlendir.....	71
11.4.4 Genel Ayarlar.....	72
11.5 DNS.....	73
12. VPN.....	75
12.1 L2TP.....	76
12.2 PPTP.....	77
12.3 SSL VPN.....	79
12.3.1 Tünel.....	80
12.3.1.1 Ağ Ayarları.....	80
12.3.1.2 Güvenlik Ayarları.....	81
12.3.1.3 İstemci Ayarları.....	82
12.3.1.4 Diğer Ayarlar.....	83
12.3.2 Yer İmi.....	83
12.3.3 Portal.....	85
12.4 IPSec.....	89
12.4.1 Tünel.....	89
12.4.2 IKE Profili.....	92
12.4.3 IPsec Profil.....	94
13. POLİTİKALAR.....	99
13.1 Güvenlik Duvarı.....	99
13.1.1 Kurallar.....	100
13.1.2 Ayarlar.....	106
13.1.2.1 Dolaylı Politikalar.....	107
13.1.2.2 Koruma Portu Tarayıcı.....	109
13.1.2.3 Saldırı Kontrolü.....	110
13.2 NAT.....	111
13.3 SD-WAN Kuralları.....	117
13.4 Web Filtre.....	120
13.4.1 Politikalar.....	121
13.4.2 İstisnalar.....	128
13.5 Wauth.....	130
13.5.1 Kurallar.....	130
13.5.1.1 Yeni Kural Ekleme.....	131
13.5.1.2 Alt Ağ Kuralları.....	131
13.5.1.3 Genel Ayarlar.....	132
13.5.2 Referans Kayıtları.....	144
13.5.2.1 Bekleyen Referans Kayıtları.....	144
13.5.2.2 Geçmiş Referans Kayıtları.....	145
13.5.3 İstisna.....	146
13.5.4 Arabirim Ayarları.....	148
13.6 IP MAC Eşleme.....	150
14. E-POSTA GÜVENLİĞİ.....	153
14.1 Ayarlar.....	153
14.1.1 General.....	153
14.1.2 Alan Adı Kontrolü.....	154
14.1.3 Kimlik Doğrulama.....	156
14.1.4 Antispam.....	157
14.1.5 Antivirüs.....	160
14.1.6 Karantina Özet.....	161
14.1.7 Politika.....	163
14.1.8 Spam Öğrenme.....	166
14.1.9 RBL Sunucusu.....	167

14.1.10 RBL Ayrıcalıkları.....	168
14.1.11 İzin Ver/Reddet Listesi.....	169
14.2 Antispam.....	171
14.2.1 Web Site Filtresi.....	171
14.2.2 Web Site İstisnaları.....	173
14.2.3 İçerik Filtreleme.....	175
14.2.4 Hariç Bırak.....	184
14.2.5 Bayes.....	185
14.3 Antivirüs.....	187
14.3.1 Uzantı Engelle.....	187
14.3.2 Hariç Bırak.....	188
14.4 Karantina.....	190
14.4.1 İstenmeyen E-posta.....	190
14.4.2 Virüs.....	191
15.IDS&IPS.....	192
15.1 Sensör.....	192
15.1.1 Adres Ayarları.....	194
15.1.2 Port Ayarları.....	197
15.2 İmza Profili.....	198
15.3 DLP Profili.....	204
15.4 İstisna IP Adresleri.....	208
15.5 Ayarlar.....	210
16.NESNELER VE KİMLİKLER.....	212
16.1 Ağ Nesneleri.....	212
16.1.1 Adres.....	213
16.1.2 Adres Grubu.....	217
16.1.3 Ülke.....	218
16.1.4 Servis.....	219
16.1.5 Servis Grubu.....	222
16.2 Politika Nesnesi.....	223
16.2.1 Zaman.....	224
16.2.2 Bant Genişliği.....	226
16.2.3 DoS&DDoS.....	228
16.3 Kota Nesnesi.....	230
16.3.1 Kota Nesnesi.....	231
16.3.2 Kota İstisnası.....	233
16.4 Uygulama.....	235
16.4.2 Liste.....	235
16.4.2 Grup.....	236
16.5 Kimlik.....	238
16.5.1 Kullanıcı.....	238
16.5.2 Gruplar.....	242
16.5.3 Alan Adı.....	244
16.4.4 Kullanıcı Şablonu.....	245
16.5.5 L2TP/PPTP Kullanıcıları.....	248
16.5.6 Kimlik Doğrulama.....	250
16.5.7 MFA Sağlayıcılar.....	252
16.5.8 Ayarlar.....	255
16.6 Alıcı Profilleri.....	256
16.6.1 Syslog.....	256
16.6.2 SNMP Tuzağı.....	259
16.6.3 HTTP.....	261
16.6.4 E-Posta.....	262
16.6.5 FTP.....	264
17. İZLEME.....	268
17.1 Kural Kullanımı.....	268

17.2 Saldırılar.....	269
17.3 Arayüzler.....	270
17.4 Hat/Hedef.....	270
17.5 E-Posta Güvenliği.....	271
17.6 Bağlı Kullanıcılar.....	272
17.7 Kota Kullanımı.....	273
17.8 IPSec.....	274
17.9 SSL VPN Client.....	276
17.10 L2TP.....	277
17.11 PPTP.....	277
17.12 Yönlendirme Tablosu.....	278
17.13 Bağlantılar.....	279
17.14 Arp Cache.....	280
17.15 Servisler.....	281
18. TRAFİK ANALIZI.....	282
18.1 Arabirim Seçimi.....	283
18.2 Kontrol Paneli.....	284
18.2.1 Trafik Kontrol Panel.....	284
18.2.1.1 Talkers.....	285
18.2.1.2 Cihazlar.....	285
18.2.1.3 Portlar.....	285
18.2.1.4 Uygulama.....	286
18.2.2 Ağ Keşfi.....	286
18.3 Uyarılar.....	286
18.3.1 Engaged Uyarılar.....	286
18.3.2 Geçmiş Uyarılar.....	287
18.3.3 Uyarı Akışları.....	288
18.4 Akış.....	289
18.5 Cihazlar.....	291
18.5.1 Cihazlar.....	291
18.5.2 Mac Adres.....	293
18.5.3 Ağlar.....	294
18.5.4 Cihaz Havuzları.....	296
18.5.5 İşletim Sistemi.....	297
18.5.6 HTTP Sunucu.....	298
18.5.7 Top cihazlar.....	299
18.6 Arabirim.....	300
18.6.1 Ağ.....	301
18.6.2 Paketler.....	301
18.6.3 DSCP.....	302
18.6.4 Uygulamalar.....	302
18.6.5 ICMP.....	303
18.6.6 ARP.....	303
18.6.7 Grafik.....	303
19. KAYITLAR VE RAPORLAR.....	304
19.1 Kayıtlar.....	304
19.1.1 Anlık İzleme.....	305
19.1.1.1 Güvenlik Duvarı.....	305
19.1.1.2 Web Filtre.....	307
19.1.1.3 Servis.....	309
19.1.1.4 Yönetimsel.....	311
19.1.1.5 Wauth.....	313
19.1.1.6 Mail.....	314
19.1.1.7 IPMAC.....	316
19.1.1.8 DHCP.....	316
19.1.1.9 SSL VPN.....	318

19.1.1.10IPSec.....	320
19.1.1.11Bağlantı.....	322
19.1.2 Arşiv.....	323
19.2 Raporlar.....	325
19.2.1 Alınan Raporlar.....	325
19.2.2 Şablonlar.....	326
19.2.3 Objeler.....	329
19.3.4 Veri Setleri.....	331
19.3 Zaman Damgalı Kayıtlar.....	333

4. Labris Networks Hakkında

2002 yılından bu yana Labris Networks evrensel olarak kanıtlanmış ürünleriyle Ar-Ge odaklı ve hızla büyüyen bir ağ güvenlik çözümleri sağlayıcısı olmuştur. Labris, LABRIS UTM, LBRLOG ve DDoS Mitigator cihazlarında Güvenlik Duvarı/VPN, Web Güvenliği, E-posta Güvenliği, Yasal Dinleme ve Erişilebilirlik Koruma çözümlerini içeren geniş ürün yelpazesi aracılığıyla en üst düzey ağ güvenliğini garanti eder. Gelecek nesil çözümler, sızmalar, virüs, spam, zararlı yazılım ve erişilebilirlik saldırılarına karşı bir akıllı kalkan sağlayarak her türlü gerçek zamanlı tehditleri, uygulamaları tespit etmek, tanımlamak üzere geliştirilmiştir.

Labris ürünleri çeşitli topolojiler ve dağıtım senaryolarına sahip tüm boyutlardaki ağları korur. Labris FLEX donanım yazılımı seçenekleri sayesinde kullanıcılar ihtiyaç duydukları güvenlik yazılımının yanı sıra Kablosuz Misafir Kimlik Doğrulaması, Ayrıntılı İnternet Raporlama, Yasal Dinleme ve Log kaydetme gibi ekstra modülleri alma ayrıcalıklarına sahiptir. Müşteri odaklı, geleceğe yönelik ve esnek bir yaklaşıma sahip olan Labris, teknoloji harikası yazılımını bir Bulut Hizmeti olarak sunmaktadır.

20'den fazla ülkede hızla büyüyen küresel ağlarda işlemleri olan Labris ürünleri işletmeleri, markaları, devlet kurumlarını, hizmet sağlayıcıları ve kritik altyapıları korumaktadır.

Dünya çapındaki ortakları ile Labris, çok dilli Küresel Destek Merkezi ile en iyi satış sonrası desteği sağlayarak en yüksek düzeyde müşteri memnuniyeti ve sadakatine kendisini adanmıştır. Dünyada Ortak Kriterler EAL4+ sertifikalı güvenlik ağ geçidi markalarından biri ve hızla büyüyen küresel bir oyuncu olan Labris, müşterilerine en uygun maliyetle en üst düzeyde güvenlik sağlamaktadır. Ankara merkezli Labris, Avrupa, Orta Doğu, Kuzey Afrika, Kafkaslar ve Güneydoğu Asya'ya hizmet veren ofislere sahiptir.

5. Labris UTM Hakkında

Labris UTM, Kimlik tabanlı bir UTM Cihazıdır. Labris UTM'in çözümü şirketlerin, devlet kuruluşlarının ve eğitim kurumlarının güvenlik ihtiyaçlarını karşılamak üzere amaca göre üretilmiştir. Labris UTM'in türünün en iyi çözümlerinin mükemmel karışımı Kimlik Tabanlı Güvenlik Duvarı, İçerik Filtreleme, AntiVirüs, AntiSpam, Saldırı Tespit ve Önleme (IDS/IPS) ve VPN içerir.

Labris UTM, DMZ içinde tutulan, dış dünyaya açık ve yine de güvenlik duvarı koruması olan Web Sunucu, Posta Sunucu, FTP Sunucu gibi halka açık sunuculara bağlanmak için ayrı port sağlayarak artırılmış LAN güvenliği sağlar. Ayrıca, bant genişliği yönetimini iyileştirmede yardım sağlayarak çalışanların verimini arttırır ve istenmeyen internet içeriğine erişimle ilgili yasal yükümlülüğü azaltır.

Labris UTM Küçük İşletmeler, Orta Ölçekli İşletmeler ile birlikte Büyük İşletmeler tarafından da kullanılabilir.

Labris UTM, Web Güvenliği uygunsuz ve yasadışı web sitelerinin yanı sıra anlık mesajlaşma ve eşler arası uygulamaları engellemek üzere daha fazla kontrol sağlar. Labris UTM, Uygulama analizi ve kontrol sosyal medya platformları (Facebook, twitter, vb.), çevrimiçi ticaret, anlık mesajlaşma/sohbet, eşler arası paylaşım ve akan video siteleri gibi verimsiz web uygulamaları üzerindeki kontrolü genişletir. Labris, elektronik posta güvenliği, spam ve oltalama saldırılarına karşı etkili koruma ile çalışanlar sadece meşru e-postaları okurlar ve sahte e-postalara maruz kalmazlar. Labris UTM'in akıllı çözümleri değerli bilgilerinizi ve iletişim kaynaklarınızı düşük toplam sahip olma maliyeti (TCO) ile korurken yerel ve uzak ağ hizmetlerinin merkezi yönetimini basitleştirir.

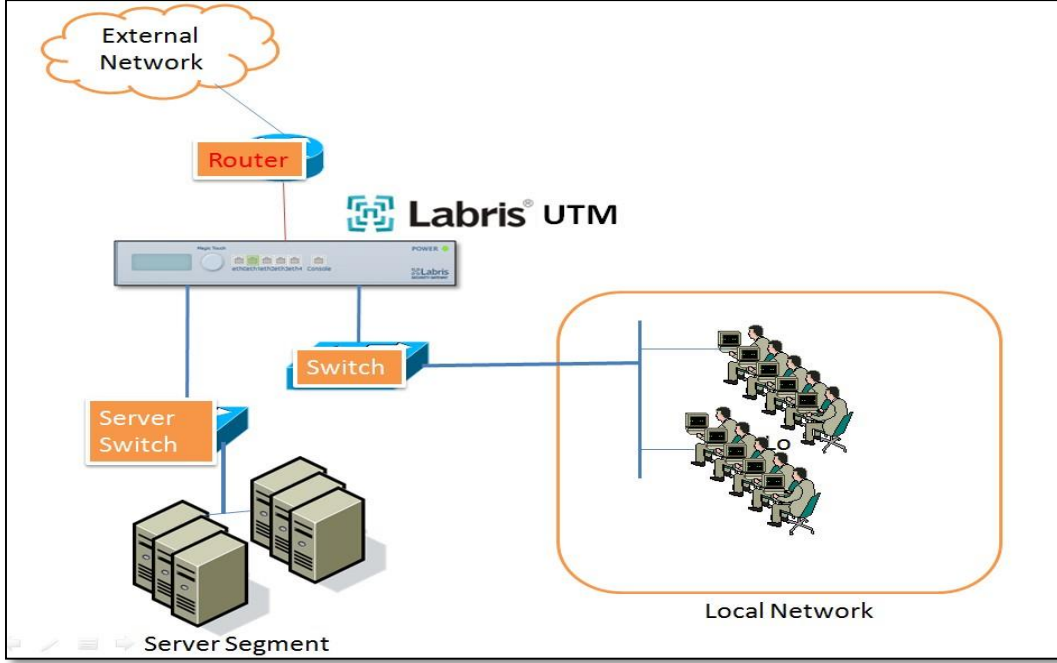
6. Labris UTM Nasıl Satın Alınır?

Labris UTM satın almak için, <http://labrisnetworks.com/products/product/lbrutm-series-appliances/> sayfasını ziyaret edebilirsiniz.

Yetkili dağıtıcılar aracılığıyla satın alabilirsiniz; <http://labrisnetworks.com/authorized-distributors/>

7. Labris UTM Cihaz Dağıtım Mimarisi

Bu bölüm, belirlenmiş dağıtım mimarisi için, mantıksal ve fiziksel tasarım hakkında bilgiler sağlar. Labris UTM cihaz dağıtım mimarisi; sunucular olarak adlandırılan yazılım süreçleri, düğümler olarak belirtilen topolojik birimler ve Labris UTM olarak bilinen güvenlik cihazından oluşur. Aşağıdaki dağıtım mimarisinde tüm sunucular ve LAN kullanıcıları Labris UTM'e L2 anahtarlar aracılığıyla bağlanır. Labris UTM cihazı, yönlendirici aracılığıyla dış ağa bağlıdır.



8. Cihaza Bağlanma

Cihazı bir yönetim bilgisayarının Ethernet arayüzüne bağlayın. Doğrudan bağlanmak için çapraz Ethernet kablosu veya hub ya da switch aracılığıyla bağlanmak için düz Ethernet kablosu kullanabilirsiniz. Her iki kablo da cihaz ile birlikte verilmektedir. Ethernet kablosunun bir ucunu eth0'dan Labris UTM cihazına ve diğer ucunu bilgisayara bağlayın.

9. Web Yönetici Konsoluna Erişme

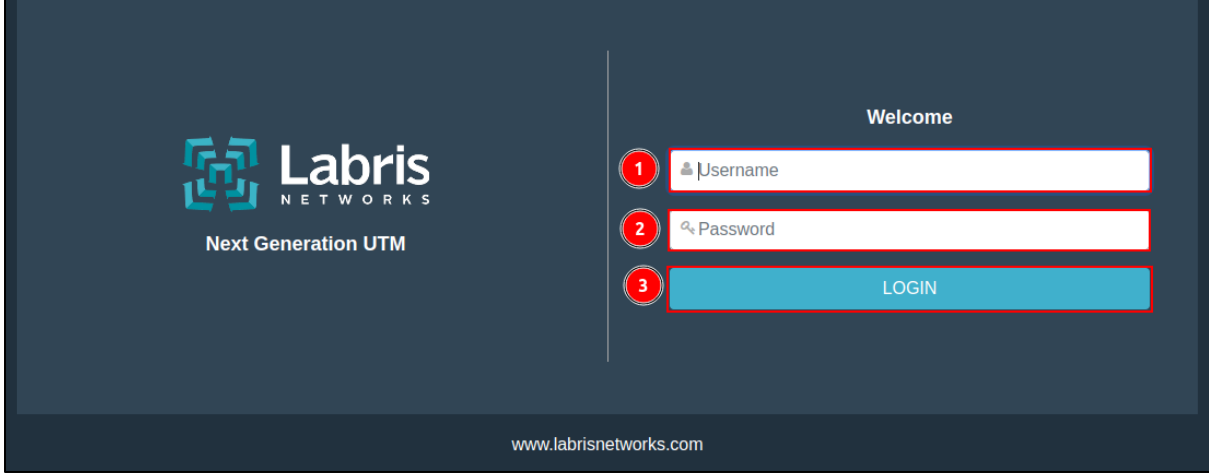
Labris Varsayılan Yönetim Portu= eth0/Port1/Net0/Mgt(cihazın ilk portu)

Labris üzerinde eth0/Port 1/Net 0/Mgt(cihazın ilk portu) portalarının varsayılan IP adresi 169.254.1.1/16(255.255.0.0)'tır.

Labris Varsayılan Kullanıcı Adı: admin

Labris Varsayılan Şifre: labris

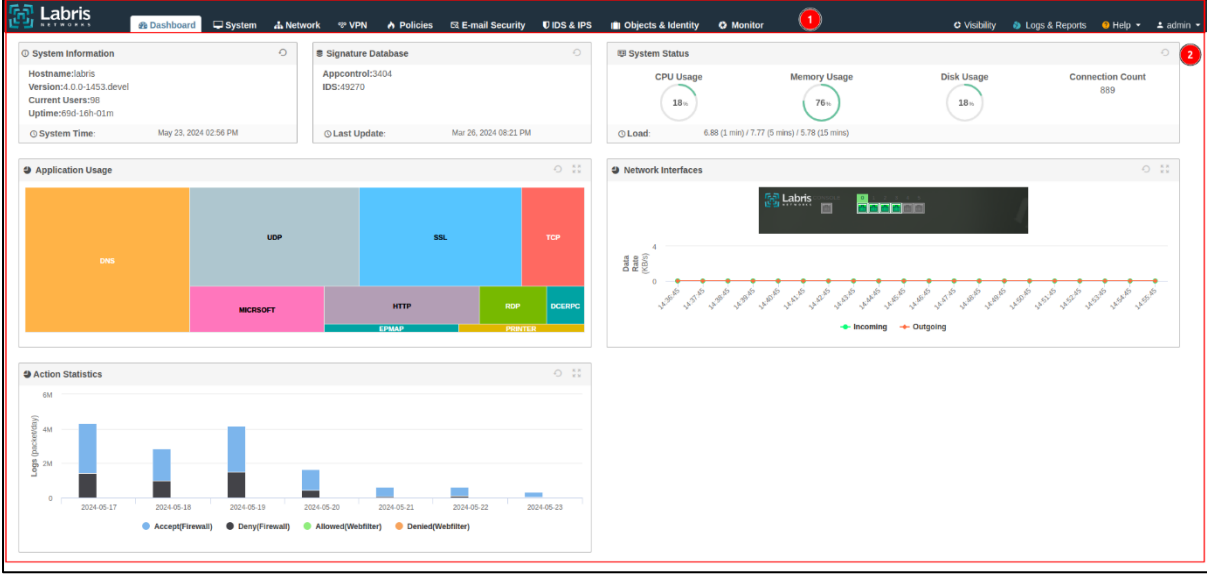
Bilgisayarınızı Labris üzerindeki ilk porta bağlayın ve ardından bilgisayarın ağ ayarları bölümünü açın ve bilgisayarınıza 169.254.1.10 IP adresini ve 255.255.0.0 alt ağını atayın. Tarayıcınızı açın ve **LABRIS UTM** Web Konsoluna erişmek için <https://169.254.1.1:81> (Burada IP adresi cihazınızın IP adresidir) adresine göz atın. Giriş sayfası görüntülenir ve giriş kimlik bilgilerini girmeniz istenir. Giriş yapmak için varsayılan olarak tanımlanan kullanıcı adını ve şifresini kullanın.



1	Kullanıcı Adı	Geçerli Varsayılan kullanıcı adınızı yazın. Bu kullanıcı adı kurulum sırasında verilir.
2	Şifre	Geçerli Varsayılan şifrenizi yazın. Bu şifre kurulum sırasında sizin verdiğinizdir. İyi bir şifre en az 8 karakter uzunlukta birlikte harfler, sayılar ve özel karakterlerin bir karışımıdır.
3	Giriş	Cihazına giriş yapmak için " Giriş " düğmesine tıklayın

9.1 Açılış sayfası veya ana ekranı anlama

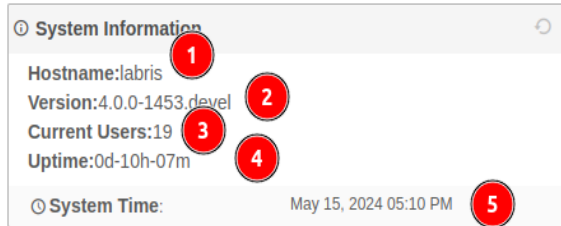
Kullanıcı adı ve şifresi ile giriş yaptıktan sonra **Labris UTM** cihazının ana ekranının çeşitli bölümlerini anlayacaksınız.



1	Sekme Bölümü	Kontrol Paneli, Sistem, Ağ, VPN, Politika, E-mail Security, Nesne ve Kimlikler, İzleme, Trafik Analizi, Kayıtlar ve Raporlar, Ayarlar ve Giriş Yapan kullanıcı gibi çeşitli bölümlerde gezebilirsiniz.
2	Kontrol Paneli	İlk giriş yaptıktan sonra Labris Güvenlik Kontrol paneli getirileceksiniz. Kontrol Paneli sistem, imza veritabanı, sistem durumu, uygulama kullanımı, arabirimleri ve işlem istatistiklerini görebilirsiniz.

9.1.1 Sistem Bilgisi

Kontrol panelindeki Sistem Bilgileri alanında cihazın adını, sürümünü, kullanıcı sayısını, çalışma zamanı ve sistem zamanı bilgilerini görüntüleyebilirsiniz.



1	Sunucu İsmi	Cihazın ismini gösterir.
2	Sürüm	Sürüm bilgisini gösterir.
3	Şu Anki Kullanıcılar	Cihaza bağlı kullanıcıların anlık sayısını gösterir.
4	Çalışma Zamanı	Cihazın çalışma zamanını gün, saat ve dakika olarak gösterir.
5	Sistem Zamanı	Cihazın saatini ve tarihini gösterir.

9.1.2 İmza Veri tabanı

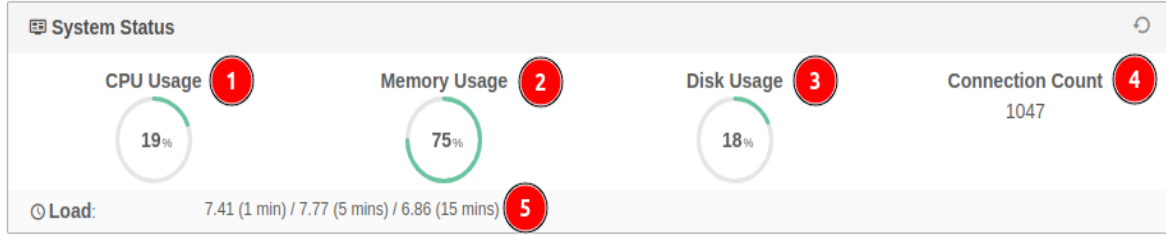
İmza veri tabanları UTM cihazına ilişkin bilgileri gösterir.



1	Uygulama Kontrolü	Uygulama kontrolü imzalarının sayısını gösterir.
2	Saldırı Tespit Sistemi	Saldırı tespit sistemi imzalarının sayısını gösterir.
3	Son Güncelleme	Uygulama kontrolü ve saldırı tespit sisteminin güncellendiği tarih ve saati gösterir.

9.1.3 Sistem Durumu

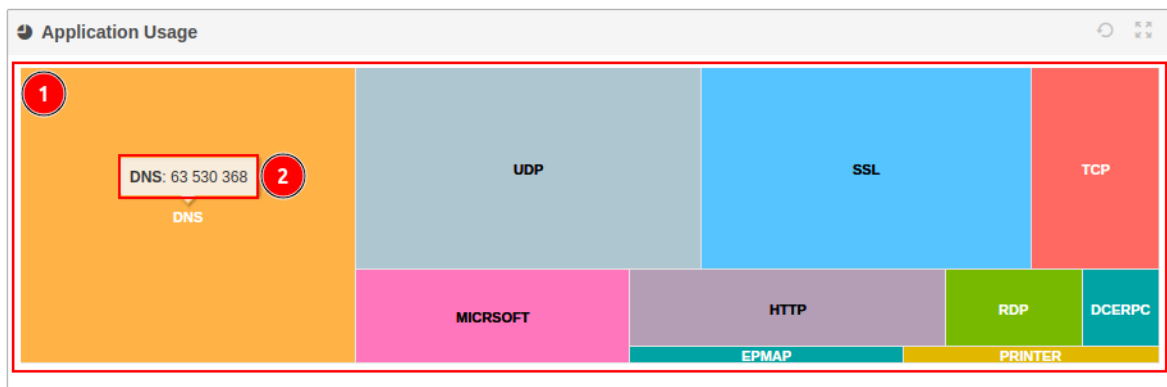
Sistem durumunda cihazın işlemci kullanımı, bellek kullanımı, disk kullanımı, bağlantı sayısı ve yük durumları görüntülenir ve işlemci, bellek, disk ve bağlantı sayısını kullanım durumlarını kolayca anlamamızı sağlayan diyagramlarla bilgileri gösterir.



1	İşlemci Kullanımı	Cihazın işlemci kullanımını sayısal olarak gösterir.
2	Bellek Kullanımı	Cihazın bellek kullanımını sayısal olarak gösterir.
3	Disk Kullanımı	Cihazın disk kullanımını sayısal olarak gösterir.
4	Bağlantı Sayısı	Cihaza bağlı olan cihazların sayısını gösterir.
5	Yük	Cihazın çalışan servislerinin yük durumlarını gösterir. Buradaki değerler 1, 5 ve 15 dakikalık ortalama yük değerlerini gösterir.

9.1.4 Uygulama Kullanımı

Uygulama katmanında bulunan protokollerin isimlerini ve kullanım sayısını görebiliriz.



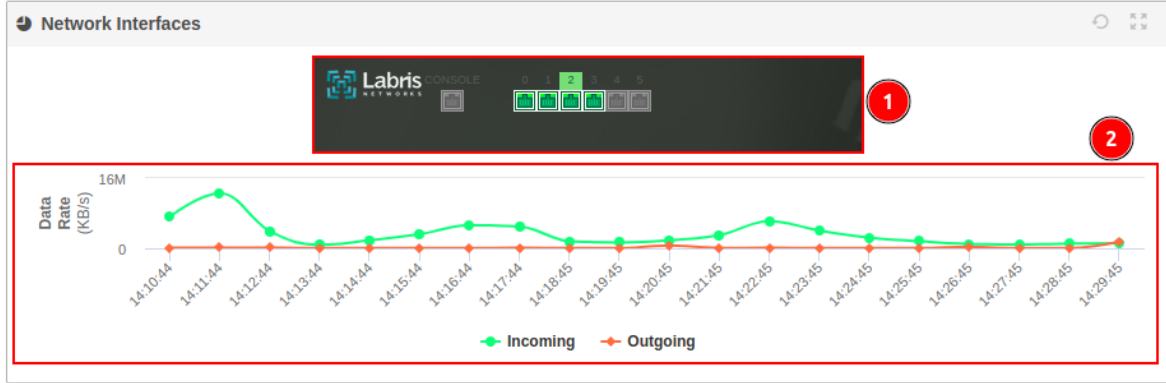
1	Uygulama İsimleri	Uygulama katmanındaki en çok kullanılan protokollerin isimlerini gösterir.
2	Uygulama Sayısı	Uygulama katmanındaki en çok kullanılan protokollerin kullanım sayısını gösterir.

Not

Uygulama sayısını görmek için ilk olarak imleci sayısını görmek istediğiniz uygulama isminin üzerine getirmeniz gerekmektedir.

9.1.5 Ağ Arayüzleri

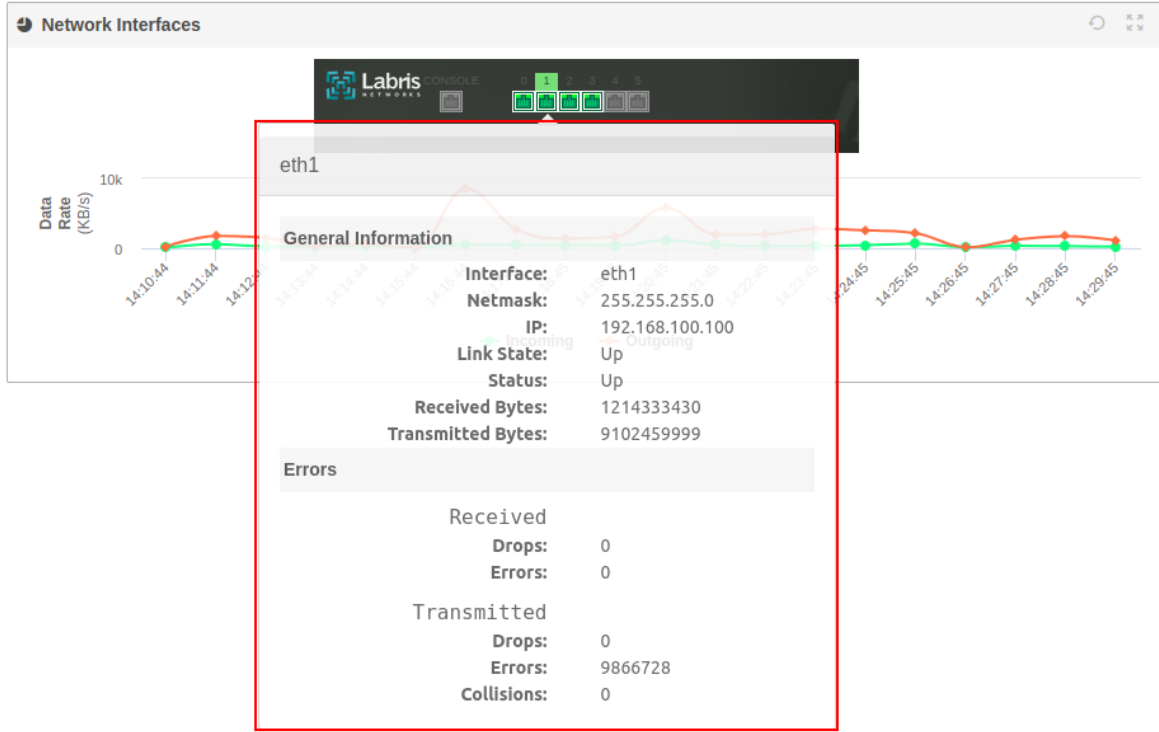
Cihaz üzerinde tanımlı olan arabirimlerin görüntülediği ve tanımlı olan arabirimler hakkında detaylı bilgileri gösterir. Labris cihazının portları üzerinde kablo takılı ise yeşil renktir. Eğer kablo takılı veya port kullanımda değilse gri renk gözükür. Bu sayede cihaza bağla olan kablolar hakkında bilgi sahibi olunur.



1	Arayüzler	Arayüzlerin port bilgilerini ve kablonun bağlı olduğu port görüntülenir. Porta bağlı bir kablo var ise yeşil renk, kablo bağlı değil ise gri renk şeklinde görünür.
2	Gelen/Giden Paketler	Gelen/giden paketlerin saat aralığını KB/s cinsinden görüntülenir. Yeşil renkli grafik gelen paketleri gösterirken turuncu renk grafik giden paketleri gösterir.

Not

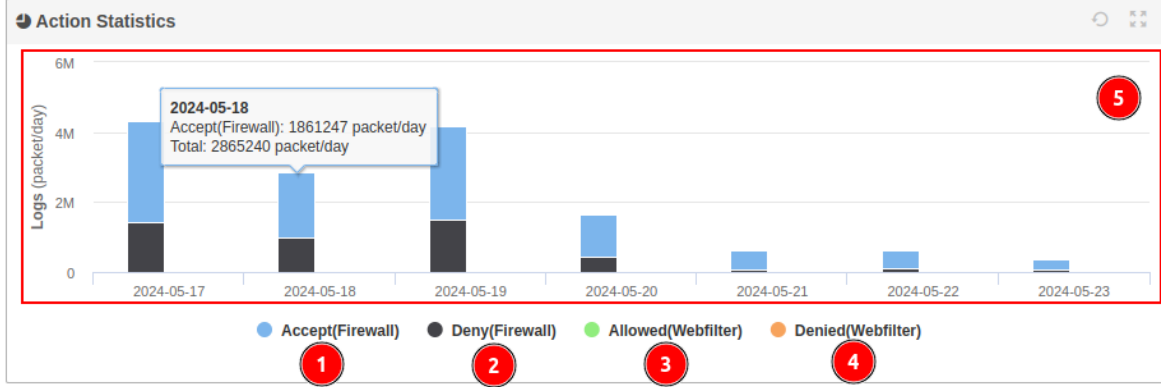
İzin verilen veya engellenen trafiğin grafikte sayısını görmek için ilk imleci sayısını kontrol etmek istenilen sütunun üzerinde olması gerekmektedir.



Yukarıda imleci Port1'e getirdiğimizde Port1 ile ilgili detaylı bilgileri gösterir. Arabirim bilgilerini, IP ve ağ maskesini, hat durumunu, alınan ve gönderilen verileri gelen bilgileri göstermektedir. Hatalar bölümünde ise alınan ve gönderilen paketlerin hatalarını göstermektedir.

9.1.6 İşlem İstatistikleri

İşlem istatistikleri politikalar modülünde bulunan güvenlik duvarı ve webfiltre kurallarından izinli ya da engelli geçen trafiğin sayısını grafik halinde gösterir. İşlem istatistiklerinde tutulan veriler 7 günlük verilerdir.



1	İzin Verilen(Güvenlik Duvarı)	Politika modülünde bulunan güvenlik duvarı kurallarından izinli olarak geçen trafiğin grafiğini gösterir. Açık mavi renklidir.
2	Engellenen(Güvenlik Duvarı)	Politika modülünde bulunan güvenlik duvarı kurallarından engelli olarak geçen trafiğin grafiğini gösterir. Siyah renklidir.
3	İzin Verilen(Webfiltre)	Politikalar modülünde bulunan webfiltre kullarından izinli olarak geçen trafiğin grafiğini gösterir. Yeşil renklidir.
4	Engellenen(Webfiltre)	Politikalar modülünde bulunan webfiltre kullarından engelli olarak geçen trafiğin grafiğini gösterir. Turuncu renklidir.
5	Grafik	Güvenlik duvarı ve webfiltre kurallarından geçen trafiği grafik halinde gösterir. 7 günlük veriyi grafik olarak göstermektedir.

10. Sistem

Sistem modülünde, cihazın adı belirlenir ve web ile SSH port bilgileri atanır. Ayrıca, cihaza erişim yetkisi verilecek kullanıcılar ve bunların yetki ayarları düzenlenir. Bu modülde sertifika oluşturulur ve yedeklilik yapısı (aktif/aktif veya aktif/pasif şeklinde) için cihazların yapılandırma ayarları yapılır. Cihaz üzerindeki ayarların yedekleri alınır ve yazılım güncellemeleri gerçekleştirilir. Cihaza erişim yetkisi verilecek IP adresi eklenir ve son olarak lisans bilgileri görüntülenir.

Yukarıda bahsi geçen işlemlerin tümü Sistem Modülünde yapılmaktadır. Sistem Modülüne tıkladığında karşılama ekranı olarak Genel Ayarlar modülü gelmektedir.

The screenshot shows the Labris UTM System Settings page. The left sidebar contains a navigation menu with the following items: General Settings, Administration, Certificate Manager, High Availability, Backup & Restore, Firmware, Console Access, and License. The main content area is divided into three sections:

- General Settings:** Hostname (labris), Web Port (81), SSH Port (22), and Certificate Based Authentication (disabled).
- Date/Time Settings:** Time Zone (EuropeIstanbul), Date & Time (manual selected), and Date (2024-05-15 17:43:26).
- SMTP Settings:** Enable (disabled), SMTP Server (192.168.2.20), Mode (Normal), Server Port (465), Mail From (labris@labrisnetworks.com), Username (labris@labrisnetworks.com), and Password (masked). A 'Send Test Mail' button is also present.

10.1 Genel Ayarlar

Cihazın ismini, web ve ssh portunu, tarih ve zaman ayarları ve SMTP ayarlarını görüntülenir ve burada varsayılan olarak tutulan ayarlar değiştirilir. Genel Ayarlar sekmesi 3 bölüme ayrılmaktadır. Bunlar Genel Ayarlar, Tarih ve Zaman Ayarları ve SMTP Ayarlarıdır.

The screenshot shows the Labris UTM General Settings page. The page is divided into three sections: General Settings, Date/Time Settings, and SMTP Settings. The General Settings section includes fields for Hostname (labris), Web Port (81), SSH Port (22), and a Certificate Based Authentication toggle. The Date/Time Settings section includes a Time Zone dropdown (Europe/Istanbul), Date & Time radio buttons (ntp and manual), and a Date field (2024-09-02 17:24:07). The SMTP Settings section includes an Enable toggle, SMTP Server (smtp.labrisnetworks.com), Mode (Normal), Server Port (456), Mail From (report@labrisnetworks.com), Username (mehmet@labrisnetworks.com), and Password (masked). A Save button is located at the top left of the settings area.

10.1.1 Genel Ayarlar

Cihaz üzerinde tanımlı olarak gelen cihazın ismini, ssh ve web portunu gösterir. Genel Ayarlar modülünü kullanarak cihaz ismi değiştirilir ve Sertifika Yönetimi modülünde eklenen sertifikayı ekleme işlemi yapılır.

The screenshot shows the Labris UTM General Settings page with numbered callouts. 1: Save button. 2: Hostname field. 3: Web Port field. 4: SSH Port field. 5: Certificate Based Authentication toggle. 6: Enforce toggle. 7: Certificate Authority dropdown.

1	Kaydet	Genel Ayarlar modülünde yapılan değişiklikleri kaydeder.
---	---------------	--

2	Sunucu İsmi	Cihazın ismini gösterir. Cihazın ismini değiştirmek için istediğiniz sunucu ismini yazıp kaydet butonuna basılarak cihaz ismi değiştirilmiş olur.
3	Web Portu	Web arayüze bağlanmayı sağlayan portu gösterir.(Örn. 192.168.1.1: 81)
4	SSH Portu	Ssh'a bağlanmayı sağlayan portu gösterir.
5	Sertifika Tabanlı Doğrulama	Web arayüze bağlanmayı sertifika ile yapmayı sağlayan butondur. Bu sayede Sertifika Yönetimi modülünde eklenen sertifikaya sahip olan cihaza bağlanabilir.
6	Zorunlu	Web arayüze bağlanmada sertifika ile bağlanmayı zorunlu hale getirir.
7	Sertifika Otoritesi	Sertifika Yönetimi modülünde eklenen sertifika otoritesi seçilir.

Not

Web ve ssh portlarını değiştirdiğinizde bağlantınız düşebilir. Bu sebepten dolayı güvenlik nedeniyle devredışı durumundadır.

10.1.2 Tarih ve Zaman Ayarları

Cihazın tarihi ve saati, Genel Ayarlar sekmesinde bulunan Tarih/Zaman Ayarları bölümünde manuel olarak veya bir NTP sunucusu aracılığıyla ayarlanır.

● Date/Time Settings

1 Time Zone Europe/Istanbul

2 Date & Time ntp manual

3 Date 2024-05-15 18:09:10

1	Zaman Dilimi	Cihazın tarih ve saatini zaman dilimine göre ayarlamak için kullanılır.
---	---------------------	---

2	Tarih & Zaman	Cihazın tarih ve saatini ntp sunucusundan veya manuel olarak eklemek için kullanılır.
3	Tarih	Manuel seçildiğinde tarih ve zamanı ayarlanabilir. Ntp seçildiğinde ise eklenen ntp sunucusuna göre tarih ve zaman ayarları yapılır.

-Tarih&Zaman Ayarları bölümünde manual seçilmesi durumunda aşağıdaki adımlar takip edilir.

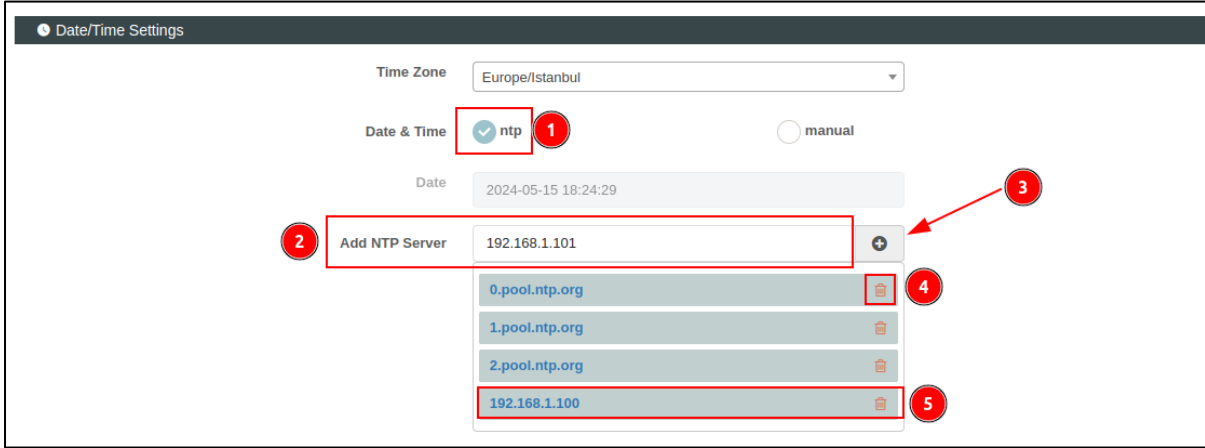
- 1- Tarih&Zaman kısmından manual'in işaretli olması gerekmektedir.
- 2- Tarih manual olarak takvimden ayarlanır.

Not

Tarih/Zaman Ayarları bölümünde yapılan herhangi bir değişiklik sonrası Genel Ayarlar sekmesinde bulunan Kaydet butonuna tıklayarak yapılan işlemleri kaydetmelisiniz.

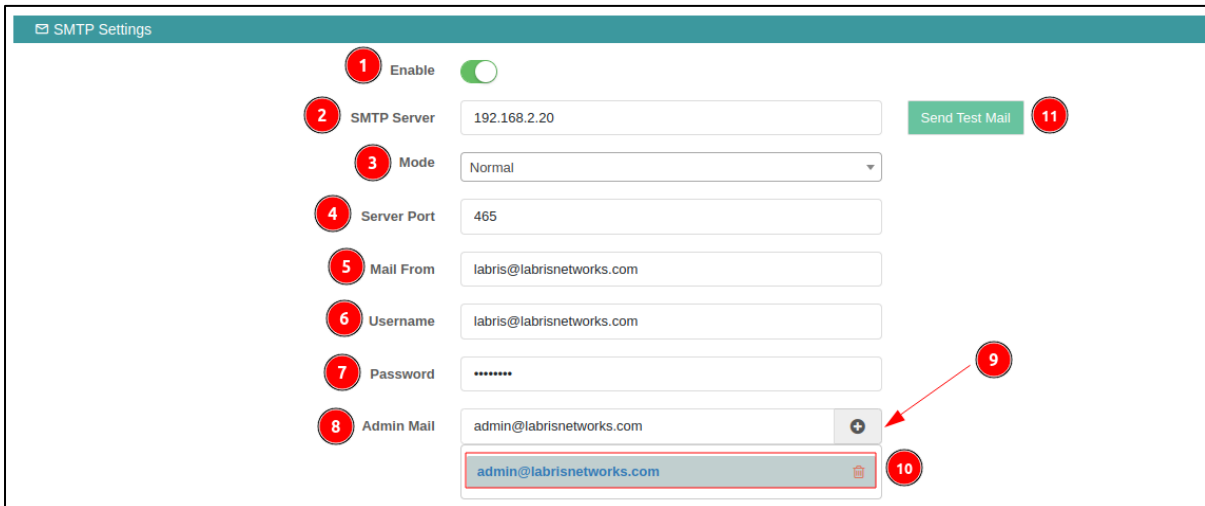
-Tarih&Zaman Ayarları bölümünde ntp seçilmesi durumunda aşağıdaki adımlar takip edilir.

- 1- Tarih&Zaman kısmından ntp'nin işaretli olması gerekmektedir.
- 2- Varsayılan olarak gelen 0.pool.ntp.org, 1.pool.ntp.org ve 2.pool.ntp.org dışında başka bir IP veya domain adresi girilir.
- 3- NTP sunucusuna ait olan IP veya domain adresi girildikten sonra ekle butonuna basarak ekleme işlemi yapılır.
- 4- Eklediğiniz NTP sunucusunu silmek ise eklenmiş olan sil butonuna basarak silme işlemi yapılır.
- 5- Eklenen NTP sunucusu listenin en sonuna eklenir.



10.1.2 SMTP Ayarları

Labris UTM cihazı üzerinde SMTP sunucu ayarlarının yapıldığı bölümdür. Bu bölüm yapılandırıldığında cihazın çalışma durumu ile ilgili bilgi maili alınır. Gelen mail'in kapsamında cihaz üzerinde çalışmayan servisler, disk durumu vb. durumlarda bilgi maili gönderir. Bunlarla birlikte SMTP etkinleştirince Ayar Yedekleme sekmesinde yedek alındığı durumlarda ekli olan yönetici e-posta adresinde mail gönderir.



1	Etkinleştir	SMTP ayarlarının etkinleştirildiği butondur.
2	SMTP Sunucusu	SMTP sunucusunun domain adresinin girildiği yerdir.
3	Mod	SMTP sunucusunun şifreleme modu seçildiği yerdir.
4	Sunucu Portu	SMTP sunucusunun portunun girildiği yerdir. Örn. 465
5	Posta Göndericisi Adresi	Gelen postanın gönderici adresinin girildiği bölümdür, buraya yazılan e-posta adresine posta

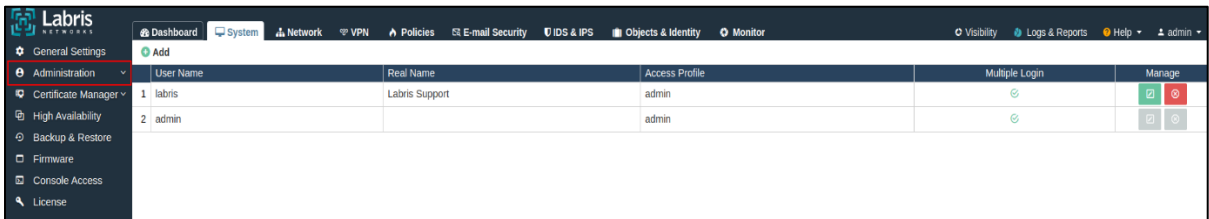
		gönderilecektir.. Örn. labris@labrisnetworks.com
6	Kullanıcı Adı	SMTP sunucu üzerinde açılan posta adresinin kullanıcı adının yazıldığı yerdir. Örn. labris@labrisnetworks.com
7	Şifre	SMTP sunucu üzerinde açılan posta adresinin şifresinin yazıldığı yerdir.
8	Yönetici E-posta Adresi	Postanın gönderileceği yönetici adresinin girildiği yerdir.Örn. yonetim@labrisnetworks.com
9	Yönetici E-posta Adresi Ekle	Ekleme istediğiniz yönetici posta adresinin yazıldığı yerdir. Örn. destek@labrisnetworks.com
10	Yönetici E-posta Adresi Listesi	Eklene yönetici posta adreslerinin listesini gösterir. Burada eklenmiş kullanıcıları listeden çıkarılır.
11	Test Maili Gönder	SMTP ayarları yapıldıktan sonra test amacıyla bir test e-postası gönderilerek SMTP ayarları denener.

Not

SMTP Ayarlarında yapılan herhangi bir değişiklik sonrası Genel Ayarlar sekmesinde bulunan Kaydet butonuna tıklayarak yapılan işlemleri kaydetmelisiniz.

10.2 Yönetim

Labris UTM cihazının web arayüzüne erişim yetkisi verilecek olan kullanıcıların eklendiği ve eklenen kullanıcılara özgü profillerin(yetkilerinin) ayarlandığı sekmedir. Kullanıcılar ve profiller olarak 2 tane alt sekmesi bulunur.

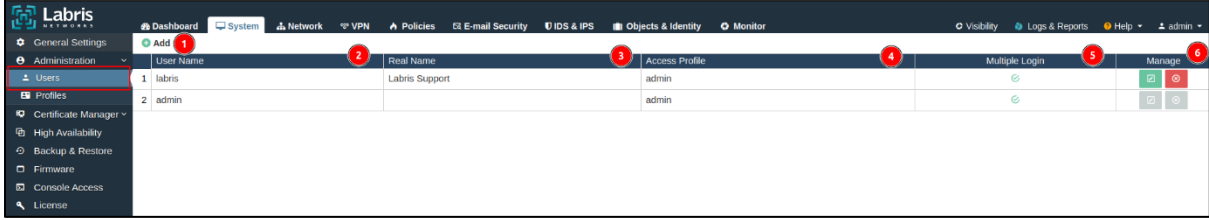


	User Name	Real Name	Access Profile	Multiple Login	Manage
1	labris	Labris Support	admin	⊕	⊕ ⊖
2	admin		admin	⊕	⊕ ⊖

Varsayılan olarak admin kullanıcısı gelmektedir. Admin kullanıcısının şifresi ilk kurulum sonrası labris olarak gelmektedir.

10.2.1 Kullanıcılar

Web arayüzüne erişecek kullanıcıların eklendiği sekmedir. Kullanıcı eklemek için ilk olarak Nesneler ve Kimlikler modülünde bulunan Kimlik sekmesinden kullanıcı eklemesi yapılması gerekmektedir.



1	Ekle	Cihaza erişecek olan kullanıcının eklendiği butondur.
2	Kullanıcı Adı	Labris UTM cihazına giriş yetkisi verilen kullanıcının adının görüntülediği bölümdür.
3	Gerçek İsmi	SMTP sunucusunun şifreleme modu seçildiği yerdir.
4	Erişim Profili	SMTP sunucusunun portunun girildiği yerdir. Örn. 465
5	Çoklu Giriş İzni	Gelen postanın gönderici adresinin girildiği bölümdür, buraya yazılan e-posta adresine posta gönderilecektir.. Örn. labris@labrisnetworks.com
6	Yönet	SMTP sunucu üzerinde açılan posta adresinin kullanıcı adının yazıldığı yerdir. Örn. labris@labrisnetworks.com

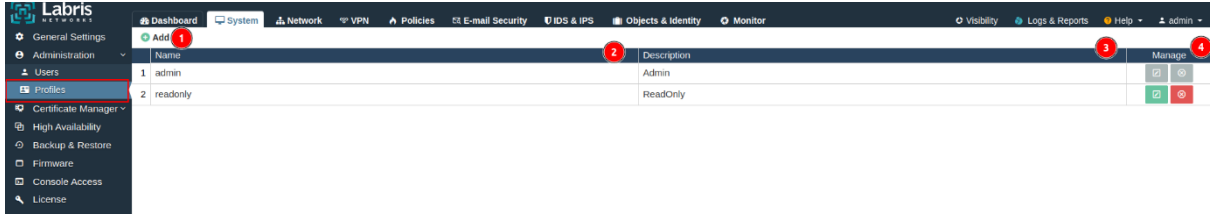
-Kullanıcı eklemesi yapmak için ekle butonuna basmak gerekir. Basıldıktan sonra eklenen Nesnelar ve Kimlikler modülünde eklenen kullanıcıyı seçmemiz gerekir. Ekle butonunda basıldıktan sonra aşağıdaki ekran gelmektedir.

1	Kullanıcı Seç	Nesneler ve Kimlikler modülünde oluşturulmuş kullanıcılardan erişim yetkisi verilecek olan seçilir.
2	Profile Eriş	Web arayüzüne erişim yetkisi verilen kullanıcıların profil erişim yetkileri verilir. Örn. VPN modülü özelinde profil oluşturulup kullanıcıya profil atandığında kullanıcı sadece VPN modülünü gösterir.
3	Çoklu Giriş	Erişim yetkisi verilen kullanıcının birden fazla giriş yetkisinin etkinleştirildiği yerdir.
4	API Key Service	Erişim yetkisi verilecek olan kullanıcıya kimlik doğrulaması için oluşturulan anahtardır. API anahtarı yeniden oluşturulur veya silinir.
5	IP Whitelist	Eklenen IP adreslerinden API Key isteği ile arayüze bağlanması gereken durumlarda kullanılır.
6	Kaydet	Web arayüze erişim yetkisi verilecek olan kullanıcının ayarlarının kaydedildiği butondur.

7	Kapat	Ekle butonuna basıldıktan sonra açılan pencerenin kapatıldığı butondur.
---	--------------	---

10.2.2 Profiller

Web arayüzüne erişim yetkisi verilecek olan kullanıcıların profil ayarlarının yapıldığı sekmedir. Profiller sekmesinde kullanıcının erişebilecekleri modüllere erişim yetkisi verilir. Varsayılan olarak 2 adet profil gelmektedir.



1	Ekle	Labris UTM cihazına bağlanacak olan kullanıcının profilinin eklendiği butondur.
2	İsim	Eklene profilin isminin görüntülediği bölümdür.
3	Açıklama	Eklene profil ile ilgili açıklamanın görüntülediği bölümdür.
4	Yönet	Eklene profilin yetkilerinin düzenlendiği veya silindiği bölümdür.

-Profil eklemek için ekle butonuna tıklanır. Ekle butonuna tıkladıktan sonra aşağıdaki ekran gelmektedir.

The screenshot shows the 'System Profiles' configuration window. It includes the following elements:

- Profile Name:** VPN
- Description:** VPN access profile
- Permissions Table:**

	Read	Write	Delete
- Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- System	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- VPN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- - L2TP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- - PPTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- - SSL VPN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- - IPsec	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- E-mail Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- IDS & IPS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Buttons:** Save (4), Close (5)

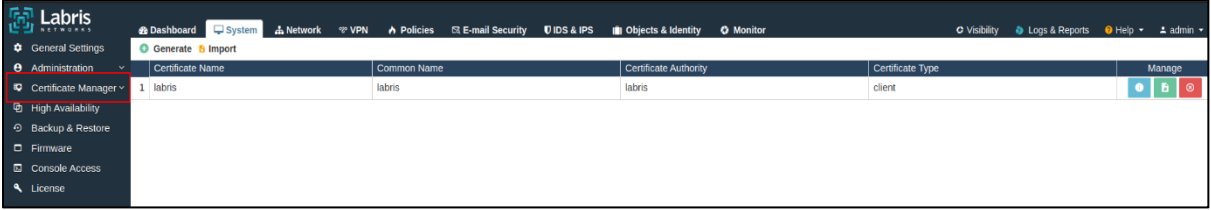
1	Profil İsmi	Oluşturulacak olan profile isim girilen yerdir. Örn. VPN
2	Açıklama	Oluşturalacak olan profile ilgili açıklamanın yazıldığı yerdir.
3	Yetki Verilecek Modüller	Yönetim yetkisi verilecek olacak kullanıcıya yönetim yetkisi verilecek modül seçilir. Modül için okuma, yazma ve silme yetkileri verilir.
4	Kaydet	Profil ayarlandıktan sonra ayarların kaydedildiği butondur.
5	Kapat	Ekle butonun tıklayarak açılan pencerenin kapatıldığı butondur.

Not

Yönetim yetkisi modül eğer diğer modüllerin içinde varsa oluşturulan profil kaydedilmez. Örn. **Nesneler ve kimlikler modülüne izin verilen kullanıcıya VPN yetkisi vermeniz gerekmektedir.**

10.3 Sertifika Yönetimi

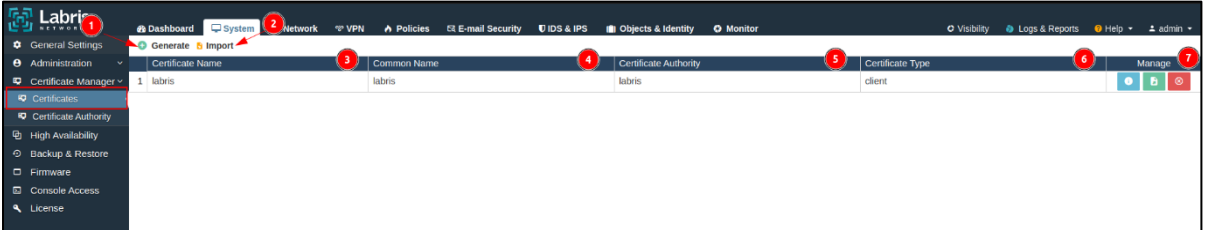
Sertifika Yönetimi sekmesinde cihaz içerisinde sertifika oluşturulması sağlar. Oluşturulan sertifika kullanıcı bazlıda olabilir. Oluşturulan sertifika SSLVPN ve web arayüze erişimde kullanır. Web arayüze sertifika ile erişim için Genel Ayarlar modülünde sertifikayı etkinleştirmek gerekmektedir.



Sertifika Yönetimi sekmesinde 2 adet alt sekme vardır. Bunlar Sertifikalar ve Sertifika Otoritesi'dir.

10.3.1 Sertifikalar

Cihaz üzerinde sertifika oluşturulan veya oluşturulmuş olan sertifikayı cihaza eklendiği sekmedir. Sertifikalar sekmesine oluşturulan sertifika client ve istemci bazlı sertifika oluşturulur. Ek olarak oluşturulan sertifika normal veya kullanıcı bazlı olabilir.



1	Oluştur	Sertifika oluşturmak için kullanılır.
2	İndir	Oluşturulmuş olan başka bir sertifikayı cihaza eklemek için kullanılır.
3	Sertifika İsmi	Oluşturulan sertifikanın adı görülür.
4	Yaygın Ad	Oluşturulan sertifikanın yaygın adı görülür.

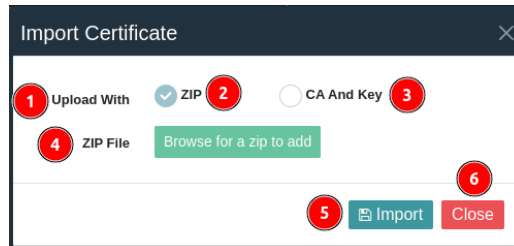
5	Sertifika Otoritesi	Oluşturulan sertifikanın otoritesini gösterir.
6	Sertifika Tipi	Oluşturulmuş sertifikanın tipinin gösterir. Client ve İstemci olmak üzere iki adet tip vardır.
7	Yönet	Oluşturulan sertifikanın içeriğini görüntülediği, sertifikanın indirildiği ve silindiği bölümdür.

-Sertifika oluşturmak için oluştur butonuna tıklanır. Oluştur butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.

1	Sertifika Adı	Oluşturulacak olan sertifikanın adının girildiği bölümdür.
2	Anahtar Uzunluğu	Oluşturulacak olan sertifikanın anahtar uzunluğunun seçildiği bölümdür. Şifrelemenin yapılacağı bit uzunluğunun seçilir. Bit uzunluğu 1024, 2048 ve 4096 uzunluğundan biri seçilir.
3	Geçerlilik Süresi(Gün)	Oluşturulacak olan sertifikanın geçerlilik süresi girilir. Girilen geçerlilik süresi gün belirlenir. Örn. 1825 gün sonra sertifikanın geçerlilik süresi biter.
4	Sertifika Otoritesi	Sertifika Otoritesi sekmesinde oluşturulan otoritenin seçildiği yerdir.
5	Anahtar Tipi	Sertifikanın anahtar tipinin seçildiği yerdir. Client ve

		İstemci olmak üzere 2 adet anahtar tipi vardır
6	Ülke Kodu	Sertifikanın Ülke kodunun seçildiği yerdir. Örn. TR.
7	Eyalet	Oluşturulacak olan sertifikanın eyaletinin girildiği yerdir. Örn. Türkiye.
8	Şehir	Oluşturulacak olan sertifikanın şehir isminin girildiği yerdir. Örn. Ankara.
9	Organizasyon	Organizasyon isminin girildiği yerdir. Örn. Labris Networks.
10	E-posta	E-posta adresinin girildiği yerdir. Örn. support@labrisnetworks.com
11	Ortak İsim Türü	Oluşturulacak olan sertifikanın normal veya kullanıcı bazlı olacağına seçildiği yerdir.
12	Ortak Anahtar/Kullanıcı	Normal seçilmesinde ise ortak anahtar girilmesi gerekir. Kullanıcı seçildiği durumda Nesnelere ve Kimlikler modülünde oluşturulan kullanıcı seçilir. Kullanıcı seçilmesi durumunda sertifikanın SSLVPN ve web arayüzünde kullanım durumu belirtilir.
13	Kaydet	Oluşturulacak sertifikanın konfigürasyonu yapıldıktan sonra kaydedilmesi gereken durumlarda kullanılır.
14	Kapat	Oluştur butonuna tıkladıktan sonra ekranın kapatılması gereken durumlarda kullanılır.

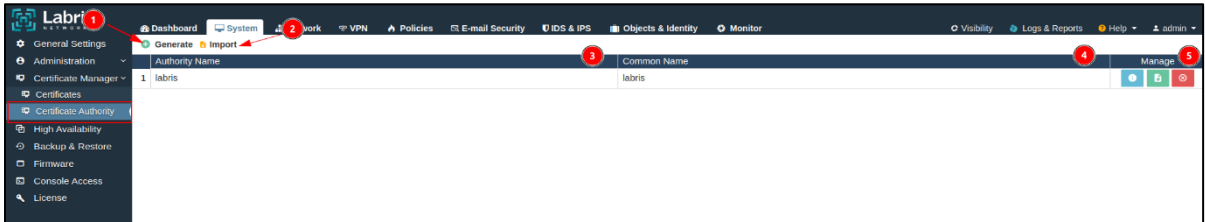
-Oluşturulmuş Sertifika Otoritesi eklemek için indir butonuna tıklanır. İndir butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.



1	Bununla Yükle	İndirilecek Sertifika Otoritesinin yükleme tipi seçilir.
2	ZIP	İndirilecek olan Sertifika Otoritesinin indirme işlemini ZIP ile yapar.
3	CA ve Anahtar	İndirilecek olan Sertifika Otoritesinin indirme işlemini CA ve Anahtarıyla yapar.
4	ZIP Dosyası	Bilgisayarınızdan eklenecek olan Sertifika Otoritesinin seçildiği yerdir.
5	İndir	Seçilen Sertifika Otoritesinin indirildiği butondur.
6	Kapat	İndir butonuna tıklandığında açılan pencereyi kapatır.

10.3.2 Sertifika Otoritesi

Sertifikalar sekmesine oluşturulan sertifika için otorite oluşturulur. Cihaz üzerinde olmayan sertifika otoritesi cihazlara eklenebilir.



1	Oluştur	Sertifika otoritesini oluşturmak için kullanılır.
2	İndir	Cihazın dışında başka bir sertifika otoritesini eklemek için kullanılır.
3	Yetki İsmi	Sertifika otoritesinin ismi görüntülenir.
4	Yaygın Ad	Sertifika otoritesinin yaygın adı görüntülenir.
5	Yönet	Oluşturulan sertifika otoritesinin içeriğini görüntülendiği, sertifika otoritesinin indirildiği ve silindiği bölümdür.

-Sertifika otoritesi oluşturmak için oluştur butonuna tıklanır. Oluştur butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.

Generate Certificate Authority

1 Certificate Name labrisauthority

2 Key Length 2048

3 Valid For 1825 day

4 Country Code TR

5 Country of Province Turkey

6 City Ankara

7 Organization Labris Networks

8 E-mail support@labrisnetworks.com

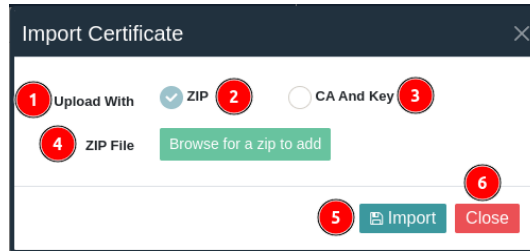
9 Common Name labris

10 Save Close

1	Sertifika Adı	Oluşturulacak olan sertifikanın adının girildiği bölümdür.
2	Anahtar Uzunluğu	Oluşturulacak olan sertifikanın anahtar uzunluğunun seçildiği bölümdür. Şifrelemenin yapılacağı bit uzunluğunun seçilir. Bit uzunluğu 1024, 2048 ve 4096 uzunluğundan biri seçilir.
3	Geçerlilik Süresi(Gün)	Oluşturulacak olan sertifikanın geçerlilik süresi girilir. Girilen geçerlilik süresi gün belirlenir. Örn. 1825 gün sonra sertifikanın geçerlilik süresi biter.
4	Ülke Kodu	Sertifikanın Ülke kodunun seçildiği yerdir. Örn. TR .
5	Eyalet	Oluşturulacak olan sertifikanın eyaletinin girildiği yerdir. Örn. Turkiye .
6	Şehir	Oluşturulacak olan sertifikanın şehir isminin girildiği yerdir. Örn. Ankara .

7	Organizasyon	Organizasyon isminin girildiği yerdir. Örn. Labris Networks.
8	E-posta	E-posta adresinin girildiği yerdir. Örn. support@labrisnetworks.com
9	Ortak İsim Türü	Oluşturulacak olan sertifikanın normal veya kullanıcı bazlı olacağını seçildiği yerdir.
10	Kaydet	Oluşturulacak sertifikanın konfigürasyonu yapıldıktan sonra kaydedilmesi gereken durumlarda kullanılır.
11	Kapat	Oluştur butonuna tıkladıktan sonra ekranın kapatılması gereken durumlarda kullanılır.

-Oluşturulmuş Sertifika Otoritesi eklemek için indir butonuna tıklanır. İndir butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.



1	Bununla Yükle	İndirilecek Sertifika Otoritesinin yükleme tipi seçilir.
2	ZIP	İndirilecek olan Sertifika Otoritesinin indirme işlemini ZIP ile yapar.
3	CA ve Anahtar	İndirilecek olan Sertifika Otoritesinin indirme işlemini CA ve Anahtarıyla yapar.
4	ZIP Dosyası	Bilgisayarınızdan eklenecek olan Sertifika Otoritesinin seçildiği yerdir.
5	İndir	Seçilen Sertifika Otoritesinin indirildiği butondur.
6	Kapat	İndir butonuna tıklandığında açılan pencereyi kapatır.

10.4 Yedeklilik

Labris cihazlarının yedeklilik ayarlarının yapıldığı modüldür. İki adet cihazın birbirini yedeklemesiyle oluşur, cihazlardan birinin bozulması, arızalanması gibi durumlarda pasif olan cihaza geçmesi ile yedeklilik yapısı oluşur. Çalışan cihazlar aktif-aktif ya da aktif-pasif çalışacaktır.

	Bu Düğüm	Esgörevli Düğüm
Düğüm Adı	Active (labris)	Standby (labristw2)
Durumları Eşle	OK	OK
Firmware Sürümü	4.0.0-1449	4.0.0-1449
Servis	Running	Running

10.4.1 Yüksek Kullanılabilirlik Ayarları

Yüksek Kullanılabilirlik Ayarları bölümünde cihazların yedeklilik ayarlarının yapıldığı ve protokol bilgilerini, yedeklilik yapılacak arabirim, cihazın eşleme döneminin seçildiği bölümdür.

- Save
- Enable
- Mode
- Protocol
- Role
- HA Interface
- Peer IP
- Sync Period
- Shared Key

1	Kaydet	Yedeklilik yapılandırma kaydedilir.
2	Etkinleştir	Yedeklilik ayarlarının etkinleştirilir.
3	Mod	Yedekli olarak çalışan cihazların aktif-aktif veya aktif-pasif olarak ayarlandığı bölümdür.
4	Protokol	Yedekli olarak çalışacak cihazların protokolleri seçilir. VRRP veya cluster olarak protokolü seçmek gerekir. VRRP seçildiği durumda seçilen arabirimdeki durumuna bakar. Cluster seçildiğinde ise güvenilir bir ping sunucu girilmesi gerekir ve ping sunucusundaki duruma bakar.
5	Görev	Yedekli olarak yapılandırılacak cihazın görevi seçilir. Görev Aktif seçilirse yapılandırdığınız cihazın görevi pasif cihaza devredene kadar görevine devam eder.
6	HA Arabirim	Yedeklilik yapılacak olan arabirimin seçildiği bölümdür.
7	Eş Görevli IP	Yedekli yapılandırılacak olan diğer cihazın IP adresinin girildiği bölümdür.
8	Eşleme Dönemi	Cihazın konfigürasyonunun eşleme dönemi seçilir. Eşleme aktif-pasif olarak kurulu cihazlarda aktif cihazdaki konfigürasyon pasif cihaza geçerek yapılır.
9	Paylaşılan Anahtar	Cihazların paylaşılan anahtarının girildiği bölümdür.

10.4.2 Kontrol Ayarları

Kontrol Ayarları, Yüksek Kullanılabilirlik Ayarları bölümünde seçilen protokole göre değişiklik göstermektedir.

-Yüksek Kullanılabilirlik Ayarlarında protokol cluster seçilmesi durumunda aşağıdaki ekran düzenlenir.

Callout	Setting Name	Value
1	Control Settings	
2	Keepalive	1
3	Dead Time	4
4	Warning Time	2
5	Initial Dead Time	6
6	Reliable Ping Host	192.0.0.52

1	Kontrol Ayarları	Yedekli çalışan cihazların kontrol ayarlarının yapıldığı bölümdür.
2	Canlı Tut	Güvenilir ping sunucusuna erişiminin test edileceği sürenin girildiği yerdir.
3	Ölüm Zamanı	Ping sunucusuna erişiminin kesildiği süresinin girildiği bölümdür. Örn. 4 saniye içerisinde erişemediği durumda 4 saniyenin sonunda görevi pasif olan cihaza devreder.
4	Uyarı Zamanı	Ping sunucusuna erişmede 2 saniye uyarı paketi alırsa görevi pasif cihaza devreder. Uyarı zamanı bu bölümde ayarlanır.
5	İlk Ölüm Zamanı	Ölüm zamanından itibaren 6 saniye ping sunucusuna erişimi test eder. Ping sunucusuna erişim geldiğinde görevi aktif cihaz devralır. Ping sunucusuna erişim sağlanamadığında ise göre pasif cihazda kalır.
6	Güvenilir Ping Sunucusu	Cihazın ping atacağı sunucunun IP adresini girildiği bölümdür. Buraya yazılan ping sunucusu iç ve dış ağda çalışan bir sunucu olabilir.

-Yüksek Kullanılabilirlik Ayarlarında protokol VRRP seçilmesi durumunda aşağıdaki ekran düzenlenir.

The screenshot shows the 'Control Settings' window for VRRP. It contains the following fields:

- 1** Interval: 30 Sec.
- 2** Fall: 2 Count
- 3** Rise: 2 Count
- 4** Track Interfaces: eth1 (192.168.2.1)
- 5** Interface State Check:
- 6** Collision: 2 Count
- 7** Error: 2 Count
- 8** Rx Packets: 2 Count
- 9** Tx Packets: 2 Count

1	Aralık	Belirlenen arayüzü kontrol eden saniyenin belirtildiği yerdir.
2	Azalış	Aralık kısmında belirtilen saniyede yani 30 sn'de 2 kere erişemezse görevi pasif cihaza devreder.
3	Artış	Artış kısmında belirtilen saniyede yani 30 sn'de 2 kere erişirse göreve devam eder.
4	Arayüzleri Takip Et	Kontrol edilecek arayüzün seçildiği bölümdür.
5	Arayüz Durumu Kontrolü	Arayüz durumunun kontrol edilmesinin istenildiği durumlarda etkinleştirildiği bölümdür.
6	Çarpışma	Arayüzün çarpışma değerlerinin girildiği bölümdür.
7	Hata	Arayüze gelen paketlerdeki Hata değerleri girilir.
8	Rx Paketleri	Rx(Alıcı) paket sayısını belirtilir.
9	Tx Paketleri	Tx(İletilen) paket sayısını belirtilir.

10.4.3 Yük Transfer Ayarları

Yüksek Kullanılabilirlik Ayarları'nda seçilen protokol VRRP olması durumunda açılır. VRRP seçildiğinde aşağıdaki bölüm gelmektedir.

Load Transfer Settings

1	Shutdown-Reboot Interval	<input type="text" value="1"/>	Sec.
2	Shutdown-Reboot Fall	<input type="text" value="5"/>	Count
3	Shutdown-Reboot Rise	<input type="text" value="1"/>	Count

1	Kapatma-Yeniden Açma Aralığı	Aktif olarak çalışan cihazın takip ettiği arabirimde bir sorun olması durumunda görevi Pasif cihaza devretme süresidir.
2	Kapatma-Yeniden Açma Düşür	Aktif olarak çalışan cihazın kapanması veya yeniden başlatılması sonucunda devreye giriş sürecini ifade eder.
3	Kapatma-Yeniden Açma Yükselt	Aktif olarak çalışan cihazın kapanıp yeniden başlatılması sürecindeki açılma durumunda görevi devralma süresini ifade eder.

10.4.4 Durum

Yedek olarak ayalarlanan cihazların durumları kontrol edildiği bölümdür.

Status

	1 This Node	2 Peer Node	
3	Node Name	Active	Standby
4	Sync Status	OK	OK
5	Firmware Version	4.0.0-1447	4.0.0-1447
6	Service	Running	Running

1	Bu Düğüm	Web arayüzüne bağlı olunan cihazın durum bilgilerini gösterir.
2	Eş Görevli Düğüm	Eş görevli çalışan cihazın durumu görüntülenir.
3	Düğüm Adı	Yedekli olarak çalışan cihazların isimleri görüntülenir.
4	Durumları Eşle	Yedekli olarak çalışan cihazların eşleme durumları görüntülenir.

5	Firmware Sürümü	Cihazların sürüm bilgilerini gösterir.
6	Servis	Cihazların çalışma durumlarını gösterir.

-Pasif olarak çalışan cihazdaki durum bilgileri aşağıdaki gibi olmalıdır.

Durum		
	Bu Düğüm	Eşgörevli Düğüm
Düğüm Adı	Standby (labrisfw2)	Active (labris)
Durumları Eşle	OK	OK
Firmware Sürümü	4.0.0-1449	4.0.0-1449
Servis	Running	Running

Not

Düğüm adında Active yazdığında cihazın aktif olduğunu gösterir. Standby yazması durumunda ise cihazın Aktif cihazdan görevi dervalmak için beklediğini göstermektedir.

Not

Yedeklilik modülünde ayar yapıldığında Kaydet butonuna tıklayarak ayarları kaydetmeyi unutulmamalıdır.

10.5 Yedeklilik

Cihazın ayarlarının yedeklendiği, alınan yedeklerin FTP sunucusuna gönderme işlemlerin yapıldığı, alınan yedeklere geri dönüş yapıldığı modüldür.

The screenshot displays the 'Backup & Restore' configuration page in the Labris UTM interface. The page is divided into several sections: 'Settings', 'Backup And Restore Configuration', 'Factory Default', and 'Backups'. The 'Settings' section includes fields for 'Max Backup' (set to 10), 'Schedule' (set to Weekly), and three toggle switches for 'Notify Admin', 'Notify Only Fail', and 'Send Backup To Server' (set to LabrisFTP). The 'Backup And Restore Configuration' section has buttons for 'Get Backup', 'Browse', and 'Restore'. The 'Factory Default' section has a 'Restore' button. The 'Backups' section shows a table with the following data:

Date	Description	Version	Manage
2024-05-15 13:03:57	22.05.2024	4.0.0-1453.devel	[Icons]

10.5.1 Ayarlar

Cihazdan alınacak yedeklerin bir sunucuya yedeklenmesinin yapıldığı bölümdür. Burada günlük, haftalık ve aylık olarak yedekler seçilen FTP sunucuya ya da cihaza alınır.

1	Kaydedilecek Yedek Sayısı	Kaydedilecek olan sayının seçildiği bölümdür. Örn. 10 seçildiği durumda ilk aldığı yedeği siler.
2	Zaman	Yedek alınacak zaman seçilir.
3	Yöneticiye Bildir	Yedek alındığında Genel Ayarlar modülünde SMTP sunucu ile yöneticiye mail gönderir.
4	Sadece Hata Bildir	Yedekleme sırasında alınan hatayı bildirir.
5	Yedeği Sunucuya Gönder	FTP sunucuna alınan yedekleri göndermesi gereken durumlarda kullanılır.
6	Sunucu	Nesneler ve Kimliklerde ayarlanan FTP sunucusu seçilir.

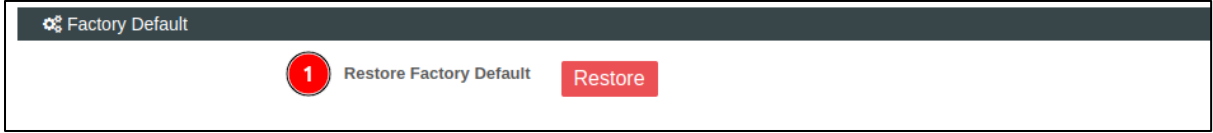
10.5.2 Yedekle ve Yapılandırma Ayarlarını Geri Yükle

Manuel olarak cihazdan yedek alınması gereken durumlarda kullanılır. Bu bölümdeki asıl amaç cihazdan yapılandırma yedeklerinin alınması veya alınan yapılandırma yedeklerinin cihaza geri yüklenmesidir.

1	Yapılandırmaları Şimdi Yedekle	Yapılandırma ayarlarının yedeklendiği butondur.
2	Yedeklenmiş Yapılandırmaları Geri Yükle	Önceden alınan yapılandırma yedeğinin seçildiği ve seçilen yapılandırma yedeğinin geri yüklendiği butonlardır.

10.5.3 Fabrika Ayarlarına Geri Yükle

Fabrika ayarlarına dönmesi gerektiği durumlarda kullanılan bölümdür.



1	Fabrika Ayarlarına Geri Yükle	Fabrika Ayarlarına geri yükleme butonudur.
---	--------------------------------------	--

10.5.4 Yedekler

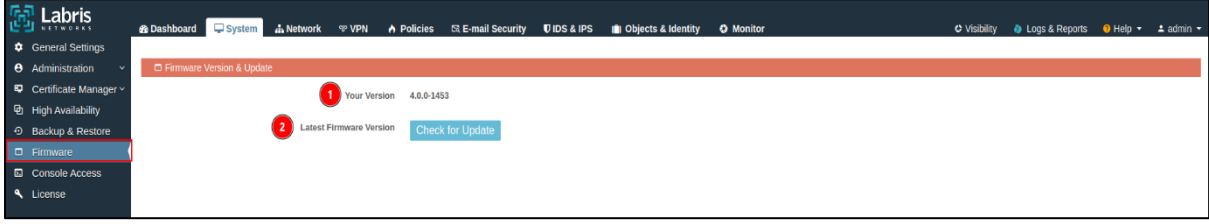
Cihazdan alınan yedeklerin görüntülediği bölümdür.

	Date	Description	Version	Manage
1	2024-05-15 13:03:57	22.05.2024	4.0.0-1453.devel	

1	Tarih	Yedeklerin alındığı tarihi gösterir.
2	Açıklama	Yedek ile ilgili açıklama görüntülenir.
3	Sürüm	Yedeğin alındığı sürümünü gösterir.
4	Yönet	Alınan yedeğin geri yüklendiği, indirildiği ve silindiği bölümdür.

10.6 Yazılım Güncelleme

Cihazın yazılım güncellemelerinin yapıldığı yapıldığı ve cihazın sürüm bilgilerinin görüntülediği modüldür.



1	Sizin Sürümünüz	Cihazınızın sürümü görüntülenir.
2	Son Firmware Sürümü	Cihazın sürüm güncellemesinin yapıldığı butondur.

10.7 Konsol Erişim

Cihaza erişim yetkisi verilecek olan genel ve özel IP adreslerinin eklendiği ve eklenen IP adreslerine erişim yetkisi verildiği modüldür. Erişim yetkisini ssh,web ve ping olarak ayarlanabilir.



1	Ekle	Konsol Erişim yetkisi verilecek olan IP adresini, ağ adresinin eklendiği butondur.
2	Adres	Konsol Erişim yetkisi verilen IP adresi görülür.
3	Ağ Maskesi	Eklenen IP adresinin Ağ Maskesi görülür.
4	Servisler	Konsol Erişim yetkisi verilecek olan IP adresinin erişebileceği servisler görüntülenir.
5	Durum	Erişim yetkisi verilen adresin durumu görüntülenir. Durum yeşil ise aktiftir. Durum kırmızı ise pasiftir.
6	Açıklama	Konsol Erişim yetkisi verilecek IP adresine ait açıklamanın girildiği bölümdür.

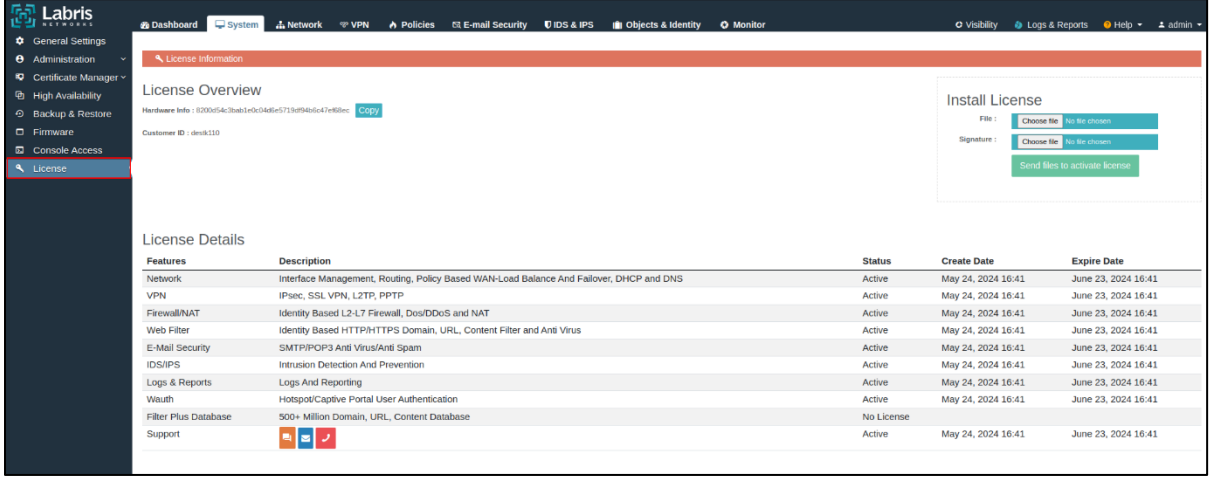
7	Yönet	Konsol Erişim yetkisi verilen IP adresinin değiştirildiği veya silindiği bölümdür.
---	--------------	--

-Konsol Erişim yetkisi verilecek IP veya ağ adresini ekleme için ekle butonuna tıklanır. Ekle butonuna tıkladıktan sonra aşağıdaki ekran gelmektedir.

1	Etkinleştir	Konsol Erişim yetkisi verilecek IP veya Ağ adresinin etkinleştirildiği yerdir.
2	IP	Konsol Erişim yetkisi verilecek olan IP adresi girilir.
3	Ağ Maskesi	IP adresinin Ağ Maskesi girilir.
4	Açıklama	Konsol Erişim yetkisi verilecek olan IP adresinin açıklaması girilir.
5	Servisler	Erişim yetkisi verilecek olan servislerin seçildiği yerdir.
6	Kaydet	Yapılan ayarlarının kaydedildiği butondur.
7	Kapat	Ekle butonuna tıklandığında açılan pencerenin kapatıldığı butondur.

10.8 Lisans

Lisans modülünde donanım kodunu, lisans yükleme ve lisans detaylarını görüntülenir.



10.8.1 Gelen Bakış

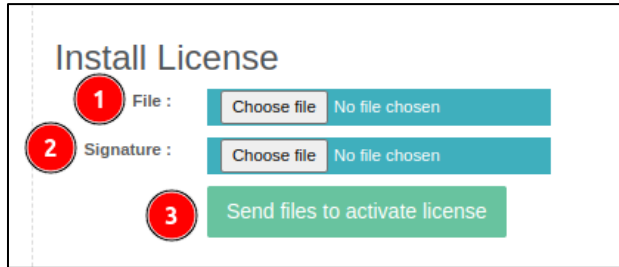
Genel bakış bölümünde donanım bilgisi ve müşteri kimlik numarası bilgileri bulunur.



1	Donanım Bilgisi	Cihazın donanım kodu görüntülenir. Donanım kodu lisans üretiminde kullanılır.
2	Müşteri Kimlik Numarası	Müşteri Kimlik Numarası görüntülenir.

10.8.2 Lisansı Yükle

Genel Bakış bölümünde bulunan Donanım Bilgisine göre oluşturulan lisansın yükleme işleminin yapıldığı bölümdür.




1	Dosya	Cihazın donanım bilgisine göre üretilen tar.gz uzantılı
---	--------------	---

		dosya eklenir.
2	İmza	Cihazın donanım bilgisine göre üretilen sig uzantılı dosya eklenir.
3	Lisansı etkinleştirmek için dosyaları gönder	Eklenen dosya ve imza seçildikten sonra lisansı etkinleştirmek için kullanılan butondur.

10.8.3 Lisans Detayları

Lisans Yükle bölümünde lisans yüklendikten sonra Lisans Detayları görüntülenir.

Features ¹	Description ²	Status ³	Create Date ⁴	Expire Date ⁵
Network	Interface Management, Routing, Policy Based WAN-Load Balance And Failover, DHCP and DNS	Active	May 24, 2024 16:41	June 23, 2024 16:41
VPN	IPsec, SSL VPN, L2TP, PPTP	Active	May 24, 2024 16:41	June 23, 2024 16:41
Firewall/NAT	Identity Based L2-L7 Firewall, Dos/DDoS and NAT	Active	May 24, 2024 16:41	June 23, 2024 16:41
Web Filter	Identity Based HTTP/HTTPS Domain, URL, Content Filter and Anti Virus	Active	May 24, 2024 16:41	June 23, 2024 16:41
E-Mail Security	SMTP/POP3 Anti Virus/Anti Spam	Active	May 24, 2024 16:41	June 23, 2024 16:41
IDS/IPS	Intrusion Detection And Prevention	Active	May 24, 2024 16:41	June 23, 2024 16:41
Logs & Reports	Logs And Reporting	Active	May 24, 2024 16:41	June 23, 2024 16:41
Wauth	Hotspot/Captive Portal User Authentication	Active	May 24, 2024 16:41	June 23, 2024 16:41
Filter Plus Database	500+ Million Domain, URL, Content Database	No License		
Support		Active	May 24, 2024 16:41	June 23, 2024 16:41

1	Özellikler	Yüklenen lisansın modülleri görüntülenir.
2	Açıklama	Lisansı olan modüller ile ilgili açıklama görüntülenir.
3	Durum	Özelliklere göre lisans durumu görüntülenir. Özellikte lisansınız varsa Durum satırında aktif yazar, eğer özellikte lisans yoksa No Lisence yazar.
4	Oluşturma Tarihi	Lisansınızın oluşturma tarihi görüntülenir.
5	Son Kullanma Tarihi	Lisansın son kullanım tarihi görüntülenir.

11.Ağ

Ağ menüsünde, Labris UTM cihazı için IP yapılandırması, statik yönlendirmeler, SD-WAN, DHCP ve DNS ayarları yapılır. Bu bölümde arabirim eklenebilir, eklediğimiz IP adreslerine yönlendirme yazılır, dış hatlarınızı SD-WAN'a tanımlayabiliriz, local arabirimlerinize DHCP sunucusu tanımlanabilir.

Interface #	Interface Name	Name	Interface Type	Status	IPv4 Address	Role	MAC	MTU	Speed	Manage
1	eth0	eth0	ethernet	🟢	169.254.1.2/255.255.0.0	external	08:00:27:3f:8d:81	1500	autoneg on	🔧 🟢 🗑️
2	eth1	eth1	ethernet	🟢	192.168.2.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
3	eth2	wan	ethernet	🟢	10.14.15.1/255.255.255.0	external	08:00:27:15:f7:ae	1500	autoneg on	🔧 🟢 🗑️
4	eth3	eth3	ethernet	🟢	192.0.0.1/255.255.255.0	external	08:00:27:e8:6c:9a	1500	autoneg on	🔧 🟢 🗑️
5	eth1.23	vlan23	vlan	🔴	192.168.23.1/255.255.255.0	internal	none	1500	autoneg on	🔧 🟢 🗑️
6	eth1.0	lan	alias	🟢	192.168.1.254/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
7	eth1.1	lan2	alias	🟢	10.0.0.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
8	ppp0	Modem1	pppoe	🔴	0.0.0.0/0.0.0.0	external			autoneg on	🔧 🟢 🗑️
9	ppp1	ppp0	pppoe	🔴	0.0.0.0/0.0.0.0	external			autoneg on	🔧 🟢 🗑️

11.1 Arabirim

Labris UTM cihazı üzerindeki arayüzlerin yapılandırıldığı veya takma isim olarak bir arabirim altına IP ekleyebilirsiniz. Bunların dışında köprü arabirimi, VLAN, Bağlı arabirim, PPPoE ve 3G/4G arabirimleri ekleyebilirsiniz.

Interface #	Interface Name	Name	Interface Type	Status	IPv4 Address	Role	MAC	MTU	Speed	Manage
1	eth0	eth0	ethernet	🟢	169.254.1.2/255.255.0.0	external	08:00:27:3f:8d:81	1500	autoneg on	🔧 🟢 🗑️
2	eth1	eth1	ethernet	🟢	192.168.2.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
3	eth2	wan	ethernet	🟢	10.14.15.1/255.255.255.0	external	08:00:27:15:f7:ae	1500	autoneg on	🔧 🟢 🗑️
4	eth3	eth3	ethernet	🟢	192.0.0.1/255.255.255.0	external	08:00:27:e8:6c:9a	1500	autoneg on	🔧 🟢 🗑️
5	eth1.23	Vlan23	vlan	🔴	192.168.23.1/255.255.255.0	internal	none	1500	autoneg on	🔧 🟢 🗑️
6	eth1.0	lan	alias	🟢	192.168.1.254/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
7	eth1.1	lan2	alias	🟢	10.0.0.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 🟢 🗑️
8	ppp0	Modem1	pppoe	🔴	0.0.0.0/0.0.0.0	external			autoneg on	🔧 🟢 🗑️
9	ppp1	ppp0	pppoe	🔴	0.0.0.0/0.0.0.0	external			autoneg on	🔧 🟢 🗑️

1	Ekle	Takma isim, köprü arabirimi, VLAN, Bağlı arabirimler, PPPoE ve 3G/4G arabirimlerinin eklendiği butondur.
2	Arabirim	Düzenleme yapılacak veya eklenen arabirime sistem verilen ismin görüntülediği satırdır.
3	İsim	Düzenlenen veya eklenen arabirime ait isim görüntülenir.
4	Arabirim Tipi	Düzenlenen veya eklenen arabirime ait arabirim tipi görüntülenir. Örn. Ethernet yazıyorsa
5	Durum	Arabirim durumunun görüntülediği bölümdür.

6	IPv4 Adresi	Arabirimlerin Ipv4 adreslerinin görüntülenir.
7	Rol	Arabirimin rolü görüntülenir.
8	MAC	Arabirime ait MAC adresleri görüntülenir.
9	MTU	Arabirimin MTU değeri görüntülenir.
10	Hız	Arabirime ait Hız görüntülenir.
11	Yönet	Arabirime ait istatistiklerin görüntülediği, arabirimin düzenliği veya eklenen arabirimin silindiği bölümdür.

Not

Labris UTM cihazı üzerinde bulunan arabirimler silinemez, düzenlenebilir. Sadece eklenen arabirimler silinebilir.

11.1.1 Arabirim Düzenleme

Labris cihazı üzerindeki arabirimi düzenlemek için Yönet bölümünde bulunan Düzenleme butonuna (yeşil renkli buton) tıklıyoruz. Karşımıza gelen ekrandan topolojinize göre düzenleme yapabilirsiniz. Düzenle butonuna tıkladıktan sonra karşımıza gelen aşağıdaki gibidir.

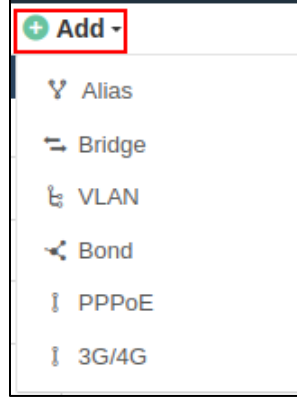
Interface *	Name	Interface Type	Status	IPv4 Address	Role	MAC	MTU	Speed	Manage
1	eth0	eth0	ethernet	169.254.1.2/255.255.0.0	external	08:00:27:3f:8d:81	1500	autoneg on	
2	eth1	eth1	ethernet	192.168.2.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	
3	eth2	wan	ethernet	10.14.15.1/255.255.255.0	external	08:00:27:15:f7:ae	1500	autoneg on	

1	İsim	Düzenlenen arabirimin ismi girilir.
2	IP/Ağ Maskesi	Düzenlenen arabirim IP ve Ağ Maskesinin girilir.
3	DHCP	Arabirimin önünde bulunan bir cihazdan IP alması gereken durumlarda işaretlenmesi gerekmektedir.
4	Görev	Arabirimin dahili(iç ağ) veya harici(dış ağ) olarak ayarlandığı yerdir.
5	Hız	Arabirimin hızının seçildiği bölümdür.
6	Dinamik Adres Dönüşümü	Tek dış ağınız olduğu durumlarda açılması gerekir.
7	MTU	Arabirime ait MTU değerinin girildiği bölümdür.
8	Cihaz Durumu	Arabirimin açıldığı yerdir. Arabirimi etkinleştirmek için kullanılan butondur.
9	Trafik Analizi	Arabirimin trafik analizini menüsünde görüntülenmesi istenildiği durumlarda açılır.
10	Kaydet	Düzenlenen arabirimin kaydedildiği butondur.

11	Kapat	Düzenle butonuna tıklanıldığında açılan pencerenin kapatıldığı butondur.
----	--------------	--

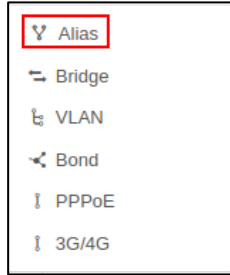
11.1.2 Arabirim Ekleme

Labris cihazı üzerinde varsayılan olarak arabirimlerin dışında arabirim eklemek için kullanılır. Arabirim eklemek için ekle butonuna tıklayarak arabirim eklemesi yapılır. Ekle butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.



11.1.2.1 Takma İsim

Takma İsim arabirimi ile birlikte Labris cihazı üzerinde sanal IP eklemesi gereken durumlarda kullanılır. Eklenen Takma İsim arabirimleri iç veya dış ağ olabilir.



1	İsim	Eklenecek olan Takma İsim arabirimine verilecek olan isim girilir.
2	IP/Ağ Maskesi	Eklenecek olan Takma İsim arabirimin IP ve Alt Ağ maskesinin girildiği kısımdır.
3	Arabirim	Takma İsim arabirimin hangi arabirimin altına eklenecekse o arabirimin seçildiği kısımdır.

4	Cihaz Durumu	Takma İsim arabiriminin etkinleştirildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz Durumu kapalı ise arabirim pasiftir.
5	Kaydet	Yapılan ayarların kaydedildiği butondur.
6	Kapat	Takma İsim'e tıklandığında açılan pencerenin kapatıldığı butondur.

-Eklenen Takma İsim arabirimi aşağıdaki gibi gözükür.

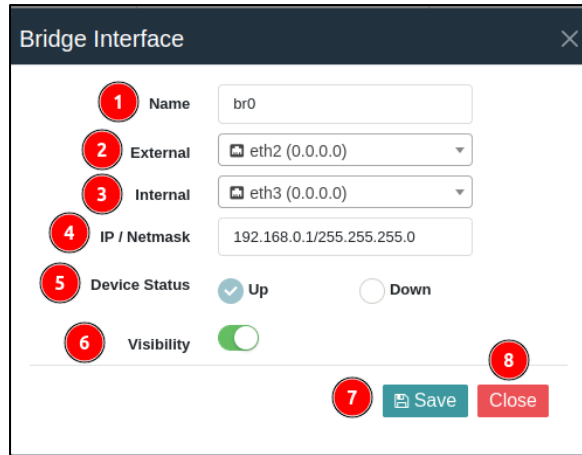
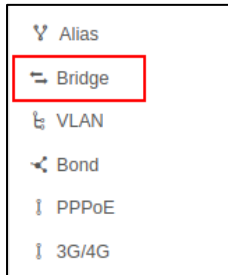
eth1:2	LAN-Employee	alias		10.0.0.1/255.255.252.0	internal	08:00:27:6e:a1:e3	1500	autoneg on		
--------	--------------	-------	--	------------------------	----------	-------------------	------	------------	--	--

Not

Eklenen Takma İsim arabirime altına eklenen arabirimin görevini alır. Örn. Eklenen arabirimin görevi Dahili ise eklenen Takma İsmın görevide Dahili olur.

11.1.2.2 Köprü Arabirimi

Köprü arabirimi ile birlikte Labris cihazı üzerindeki arabirimlerin Köprülendiği yerdir. Labris cihazının önündeki cihazdaki yapılandırmanın değiştirilmek istenmediği durumlarda kullanılır.



1	İsim	Eklenecek olan Köprü arabirimine verilecek olan isim girilir.
2	Harici	Harici(Dış ağ) olacak arabirimin seçildiği yerdir.

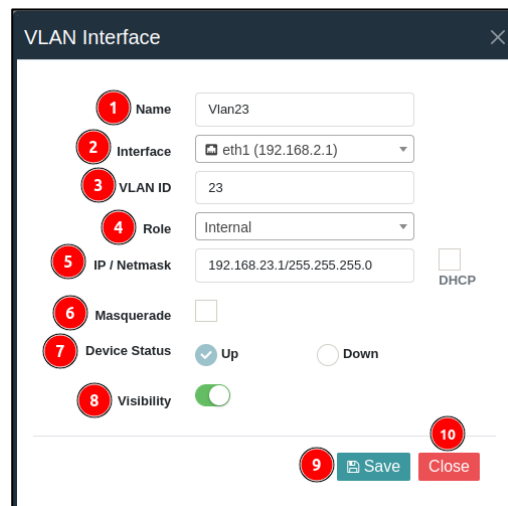
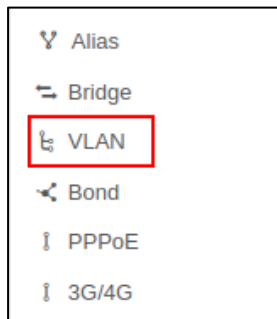
3	Dahili	Dahili(İç ağ) olacak arabirimin seçildiği yerdir.
4	IP / Ağ Maskesi	Köprü Arabirim' in IP ve Ağ maskesinin bilgilerinin girildiği yerdir.
5	Cihaz Durumu	Köprü Arabirim' in cihaz durumunun belirtildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz Durumu kapalı ise arabirim pasiftir.
6	Trafik Analizi	Köprü Arabirim' in Trafik Analizi modülünde arabirimin trafiğini detaylı olarak incelemek istenildiği durumda açılır.
7	Kaydet	Köprü Arabirim'de yapılan yapılandırmanın kaydedildiği butondur.
8	Kapat	Köprü Arabirim'e tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

-Eklenen Köprü Arabirim aşağıdaki gibi görünmektedir.

1	br0	br0	bridge	○	192.168.0.1/255.255.255.0	harici	08:00:27:15:f7:ae	1500	autoneg on	🔍	📄	🔴
---	-----	-----	--------	---	---------------------------	--------	-------------------	------	------------	---	---	---

11.1.2.3 VLAN Arabirimi

Labris cihazına VLAN arabirimi tanımlamak için kullanılır. Switch üzerinde yapılan VLAN yapılandırmasını Labris Cihazına tanımlanabilir.



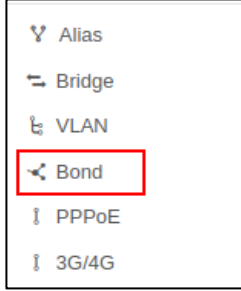
1	İsim	Eklenecek olan Vlan arabirimine verilecek olan isim girilir.
2	Arabirim	Vlan yapılandırması yapılacak olan arabirimin seçildiği bölümdür.
3	VLAN Kimlik Numarası	Switch üzerinde belirlenen Vlan Kimlik Numarasının girildiği yerdir.
4	Görev	Vlan arabirimin görevinin seçildiği bölümdür.
5	IP/Ağ Maskesi	Vlan arabirimin IP ve Ağ maskesi bilgilerinin girildiği yerdir.
6	Dinamik Adres Dönüşümü	Vlan arabirimi üzerinde dinamik adres dönüşümünün açıldığı yerdir.
7	Cihaz Durumu	Vlan arabiriminin cihaz durumunun belirtildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz Durumu kapalı ise arabirim pasiftir.
8	Trafik Analizi	VLAN arabiriminin Trafik Analizi modülünde arabirimin trafiğini detaylı olarak incelemek istenildiği durumda açılır.
9	Kaydet	Vlan arabirimi üzerinde yapılan yapılandırmanın kaydedildiği butondur.
10	Kapat	Vlan arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

-Eklenen Vlan Arabirim aşağıdaki gibi gözükmetedir.

eth1.23	Vlan23	vlan		192.168.23.1/255.255.255.0	dahili	08:00:27:6e:a1:e3	1500	autoneg on			
---------	--------	------	--	----------------------------	--------	-------------------	------	------------	--	--	--

11.1.2.4 Bağlı Arabirimi

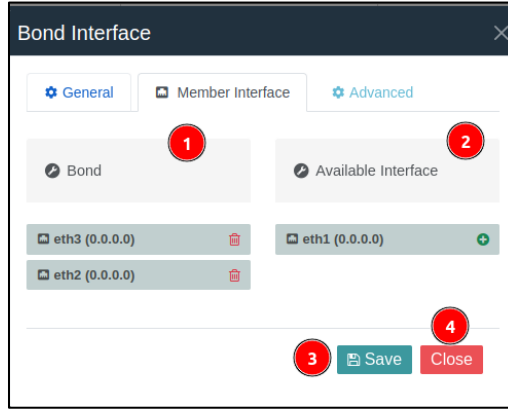
Labris cihazına Bağlı Arabirim tanımlamak için kullanılır. Arabirimleri birbirine bağlayarak yedeklilik yapısı oluşturulur.



1	Genel	Bağlı Arabirimın Genel Ayarlarının yapıldığı sekmedir.
2	Üye Arabirim	Bağlı Arabirime, arabirim ekleme işleminin yapıldığı sekmedir.
3	Gelişmiş	Bağlı Arabirimın gelişmiş ayarlarının yapıldığı sekmedir.
4	İsim	Bağlı Arabirime verilecek olan ismin girildiği bölümdür.
5	Mod	Bağlı Arabirimın çalışma modu seçilir.
6	Görev	Bağlı Arabirimın dahili(iç ağ) veya harici(dış ağ) olarak ayarlandığı yerdir.
7	IP/Ağ Maskesi	Bağlı Arabirimın IP ve Ağ Maskesi bilgilerinin girildiği bölümdür.
8	Dinamik Adres Dönüşümü	Bağlı Arabirim'de dinamik adres dönüşümünün açıldığı butondur.
9	Cihaz Durumu	Bağlı Arabiriminin cihaz durumunun belirtildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz Durumu kapalı ise arabirim pasiftir.

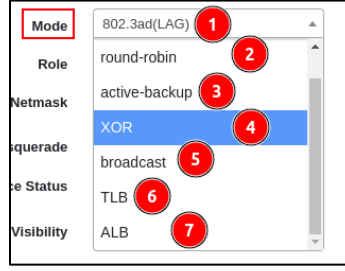
10	Trafik Analizi	Bağlı Arabirimin Trafik Analizi modülünde arabirimin trafiğini detaylı olarak incelemek istenildiği durumda açılır.
11	Kaydet	Bağlı Arabirimi üzerinde yapılan yapılandırmanın kaydedildiği butondur.
12	Kapat	Bağlı Arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

-Bağlı Arabirimin üye arabirimleri yazılır. Üye Arabirim yapmak için Üye Arabirim sekmesine tıklanır tıklandıktan sonra gelen ekranda arabirim seçilir.



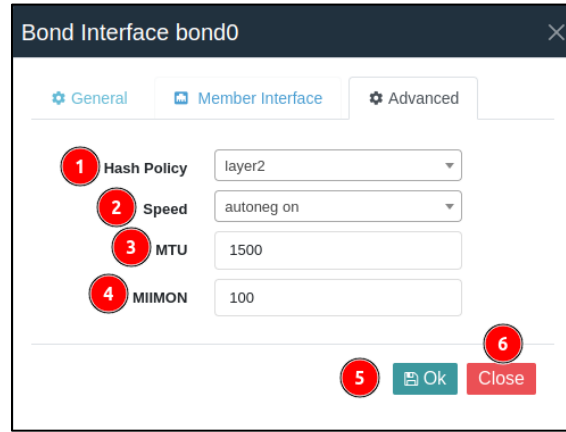
1	Bağlı	Bağlı Arabirimine eklenen arabirimlerin görüntülediği bölümdür.
2	Uygun Arabirim	Bağlı Arabirim olarak eklenecek arabirimlerin görüntülediği bölümdür.
3	Kaydet	Bağlı Arabirimin üye arabirim olarak kaydetildiği butondur.
4	Kapat	Bağlı Arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

-Bağlı Arabirimin modlarına değilenim. Mod bölümüne tıkladığında karşımıza gelen ekran aşağıdaki gibidir.



1	802.3ad(LAG)	Çoklu bağlantıları tek bir bağlantı haline getirmeyi sağlayan protokoldür.
2	Round-robin	Sunucuları sıralı olarak seçildiği ve trafiğin bu sıralama paylaştırıldığı algoritmadır.
3	Active-backup	Aktif yedek mantığıyla çalışır. Sadece bir arabirim aktiftir. Pasif olan sadece ve sadece aktif olarak çalışan arabirimde bir sorun olması durumunda görevi pasif cihaza devreder.
4	XOR	Kaynak MAC adresi, hedef MAC adresi algoritmasına göre paketleri gönderir. Her Hedef için aynı arabirimi seçer.
5	Broadcast	Tüm paketleri tüm arabirimlere gönderir.
6	TLB	Toplam yük her arabirimin kendi yüküne göre paylaşır. Her arabirimin yükü hızına oranlar ölçülür.
7	ALB	Hem gidiş hem de geliş trafiği yük paylaşımı yapılır ve özel bir anahtarlama cihazı desteği gerektirmez.

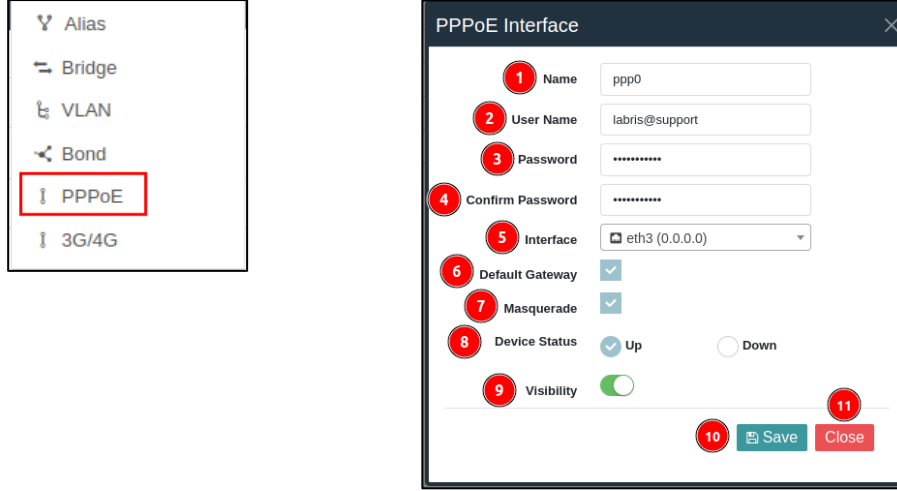
-Bağlı Arabirimin modlarına değilenim. Gelişmiş sekmesine tıklandığında karşımıza gelen ekran aşağıdaki gibidir.



1	Hash Kuralı	XOR modu seçildiği durumlarda kullanılır.
2	Hız	Birbirine bağlı olan arabirimlerin hızının ayarlandığı yerdir.
3	MTU	MTU değerinin girildiği kısımdır.
4	MIIMON	Seçilen arabirimlerin kontrolü sıklığı girilir.
5	Kaydet	Bağlı arabirim olarak ayarlanan arabirimlerin kaydedildiği butondur.
6	Kapat	Bağlı Arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

11.1.2.5 PPPoE

ADSL modem köprü moduna alındığı durumlarda Labris cihazı üzerinde PPPoE arabirimi kullanılır. İnternet Servis Sağlayıcı(İSS) tarafından verilen kullanıcı adı ve şifre doğru girilerek tanımlanır. Girilen bilgiler doğru ise arabirimin IP bölümünde dış IP adresiniz görünür.



1	İsim	PPPoE olarak eklenecek olan arabirime
2	Kullanıcı Adı	İnternet Servis Sağlayıcı tarafından verilen kullanıcı adının girildiği bölümdür.
3	Şifre	İnternet Servis Sağlayıcı tarafından verilen şifrenin girildiği bölümdür.
4	Şifre Doğrulama	İnternet Servis Sağlayıcı tarafından verilen tekrar girildiği bölümdür.
5	Arabirim	PPPoE arabiriminin tanımlanacağı arabirimin seçildiği yerdir.
6	Öntanımlı Ağ Geçidi	PPPoE arabirimin öntanımlı ağ geçidi olarak ayarlanmasının yapıldığı butondur.
7	Dinamik Adres Dönüşümü	PPPoE arabirimin dinamik adres dönüşümünün açıldığı butondur.
8	Cihaz Durumunu	PPPoE arabirimin cihaz durumunun belirtildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz

		Durumu kapalı ise arabirim pasiftir.
9	Trafik Analizi	PPPoE Arabiriminin Trafik Analizi modülünde arabiriminin trafiğini detaylı olarak incelemek istenildiği durumda açılır.
10	Kaydet	PPPoE Arabirimi üzerinde yapılan yapılandırmanın kaydedildiği butondur.
11	Kapat	PPPoE Arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

-Eklenen PPPoE Arabirimi Labris UTM cihazı üzerinde aşağıdaki gözükür.

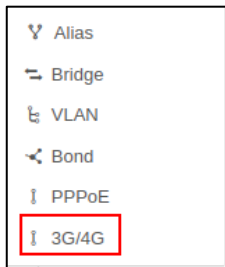
ppp1	ppp0	pppoe	0.0.0.0/0.0.0.0	hancı	autoneg on
------	------	-------	-----------------	-------	------------

Not

PPPoE arabirim eklendiği durumda dikkat edilmesi gereken durum İnternet Servis Sağlayıcı tarafından verilen kullanıcı adı ve şifrenin doğru girilmesi gerekir.

11.1.2.6 3G/4G

3G/4G modemlerin(VINN vb.) Labris UTM cihazı üzerine tanımlanması gerektiği durumlarda kullanılır.



1	İsim	3G/4G Arabirimine verilecek ismin girildiği yerdir.
---	-------------	---

2	Sağlayıcı	3G/4G Arabiriminin sağlayıcının seçildiği yerdir.
3	Modem	3G/4G Arabiriminin modem bilgilerinin seçildiği yerdir.
4	Pin	3G/4G Arabirimine ait olan pin bilgisinin yazıldığı bölümdür.
5	Öntanımlı Ağ Geçidi	3G/4G Arabiriminin ön tanımlı ağ geçidi olarak ayarlanması gereken durumlarda kullanılır.
6	Dinamik Adres Dönüşümü	Eklenecek 3G/4G Arabiriminin dinamik adres dönüşümünün açıldığı butondur.
7	Cihaz Durumu	3G/4G arabirimin cihaz durumunun belirtildiği bölümdür. Cihaz Durumu açık ise arabirim aktif, Cihaz Durumu kapalı ise arabirim pasiftir..
8	Trafik Analizi	3G/4G Arabirimin Trafik Analizi modülünde arabirimin trafiğini detaylı olarak incelemek istenildiği durumda açılır.
9	Kaydet	3G/4G Arabirimi üzerinde yapılan yapılandırmanın kaydedildiği butondur.
10	Kapat	3G/4G Arabirimine tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

11.2 Statik Yönlendirme

Statik yönlendirme, bir IP adresinin bir sonraki hedef adresine manuel olarak yapılandırılmış gönderimidir.

Statik yönlendirme, paketlerin varsayılan yapılandırılmış ağ geçidinden başka bir hedefe yönlendirilmelerine neden olur. Paketin hangi arabirimden/ağ geçidinden ayrılacağını ve paketin hangi cihaza yönlendirileceğini belirleyerek statik yollar, Labris UTM'den çıkan trafiği kontrol eder.

Statik yönlendirme bölümünde bir ağ veya bir bilgisayar için ayrılan trafiği varsayılan bir yol yerine farklı bir sonraki durak aracılığıyla yönlendirmek istediğinizde yollar eklenir.

Name	Destination	Netmask	Gateway	Metric	Interface	Manage
1 Lan15	192.168.15.0	255.255.255.0	192.168.2.1	1	eth1	[Add] [Edit] [Delete]
2 WAN1	10.20.30.48	255.255.255.255	10.14.15.2	1	eth2	[Add] [Edit] [Delete]
3 default	0.0.0.0	0.0.0.0	0.0.0.0	1	eth2	[Add]

1	Ekle	Statik Yönlendirme ekleme işlemi yapılan butondur.
2	İsim	Statik Yönlendirmeye verilen isim görüntülenir.
3	Hedef	Hedef adresi görüntülenir.
4	Ağ Maskesi	Hedef adresin ağ maskesi görüntülenir.
5	Ağ Geçidi	Hedef adresin ağ geçidi görüntülenir.
6	Ölçü	Yönlendirmenin ölçü(metrik) değeri görüntülenir.
7	Arabirim	Yönlendirmenin yazıldığı arabirim görüntülenir.
8	Statik Yönlendirmeler	İzleme modülündeki Statik Yönlendirme tablosu görüntülenir.
9	Yönet	Yazılan Statik Yönlendirmenin silindiği veya düzenlendiği bölümdür. Yönlendirmeyi silmek için Kırmızı buton seçilir. Yazılan yönlendirmeyi düzenlemek için Yeşil buton seçilir.

-Statik Yönlendirme eklemek için ekle butonuna tıklayarak ekleme işlemi yapılır. Ekle butonuna tıkladıktan sonra karşımıza gelen pencerede gerekli bilgilerini doldurarak Statik Yönlendirme eklenir.

Static Routes

1 Name: Lan15

2 Destination Address: 192.168.15.0

3 Netmask: 255.255.255.0

4 Gateway: 192.168.2.1

5 Interface: eth1 (192.168.2.1)

6 Metric: 1
(0-4,294,967,295)

7 Ok Close

1	İsim	Statik Yönlendirmeye verilen ismin girildiği bölümdür.
2	Hedef	Yönlendirme yazılacak hedef adresin girildiği bölümdür.
3	Ağ Maskesi	Hedef adresin ağ maskesinin girildiği bölümdür.
4	Ağ Geçidi	Hedef adresin yönlendirileceği ağ geçidinin girildiği bölümdür.
5	Arabirim	Yazılacak Statik Yönlendirmenin arabirimin seçildiği bölümdür.
6	Ölçü	Yazılacak Statik Yönlendirmenin metrik(ölçü) biriminin yazıldığı bölümdür.
7	Tamam	Statik yönlendirmenin yapılandırmasının kaydedildiği butondur.
8	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

11.3 SD-WAN

Geleneksel geniş alan ağlarını(WAN) modern bir yaklaşımla ele alan teknolojidir. SD-WAN, ağ yöneticilerine geniş ağlarının performansını arttırmak, esneklik sağlamak için kullanılır.

SD-WAN yazılım tabanlı geniş alan ağlarıdır. Kurumların internet hatlarında herhangi bir kesinti olması durumunda yazılım bazlı yedekleme yapısı sunar.

İki veya daha fazla bir internet hattı olduğu durumlarda Labris UTM cihazı üzerindeki SD-WAN modülünü kullanılarak internet hatlarını yedekli olarak yapılandırabilirken, internet hatlarının bant genişliğini grup haline getirilir.

Name	Gateway	Interface	Reachable	Router	Manage
1 DLS2	192.168.12.1	eth2	○	○	○
2 DLS1	192.168.11.1	eth3	○	○	○

1	Ekle	Dış ağ olarak eklenen arabirimlerin SD-WAN'a eklemek için kullanılan butondur.
2	İsim	Eklenen ağ geçidinin ismi görüntülenir
3	Ağ Geçidi	Eklenen ağ geçidinin arabirim adresi görüntülenir.
4	Arabirim	Eklenen ağ geçidinin arabirimin görüntülenir.
5	Ulaşılabilir	Ağ geçidine ulaşıldığı durumlarda yeşil, ulaşılamadığı durumda ise kırmızı renk görünür.
6	Yönlendirici	Ağ geçidinin trafiği yönlendirdiği durumlarda yeşil renk yönlendiremediği durumlarda kırmızı renk görünür.
7	Yönet	Eklenen ağ geçidinin düzenlendiği veya silindiği butonlar bulunur. Yeşil renk buton ile eklenen ağ geçidi düzenlenir, kırmızı renkli buton ile eklenen ağ geçidi silinir.

11.3.1 Ağ Geçitleri

Dış ağ olarak ayarlanan arabirimlerin ağ geçitlerinin tanımlandığı modüldür. Ağ geçidi eklemek için ekle butonuna tıklayarak SD-WAN ağ geçidi eklenir.

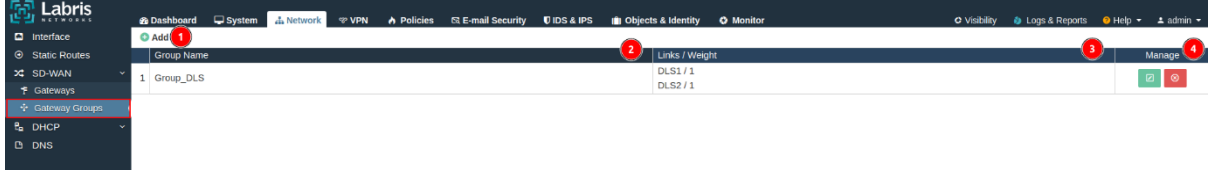
1	İsim	Eklenecek ağ geçidinin isminin girildiği bölümdür.
2	Arabirim	Eklenecek ağ geçidinin arabirimin seçildiği bölümdür.
3	Ağ Geçidi	Ağ geçidi adresinin yazıldığı yerdir.
4	Ping Adresleri	Ağ geçidinin erişebileceği ping sunucusunun girildiği bölümdür.
5	Ping Adresleri Ekle	Ağ geçidinin erişebileceği ping sunucusunun eklendiği bölümdür.
6	Ping Adresleri Listesi	Ağ geçidinin ping adreslerinin listesi görüntülenir.
7	Kaydet	Ağ geçidini yapılandırmasının kaydedildiği butondur.
8	Kapat	Ağ geçidi yapılandırma ayarlarının kapatıldığı butondur.

-Eklenen Ağ Geçitleri aşağıdaki gibi görünür.

DSL2	192.168.11.2	eth1	○	○	○	○
------	--------------	------	---	---	---	---

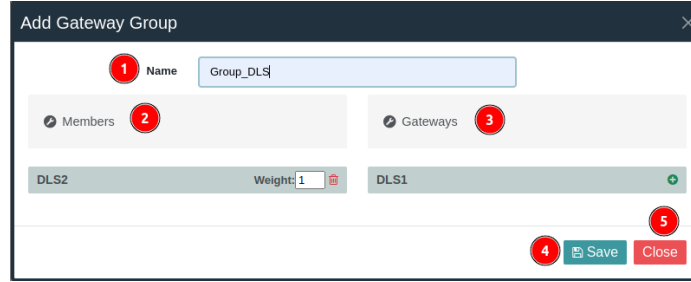
11.3.2 Ağ Geçidi Grupları

SD-WAN modülünde ağ geçitlerinin gruplandırıldığı ve daha önce gruplanmış olan ağ geçitlerinin görüntülediği modüldür. Ağ geçidi grubu oluşturmak için ekle butonuna tıklayarak ağ geçitleri gruplanır.



1	Ekle	Eklenecek Ağ Geçitlerinin gruplandırıldığı butondur.
2	Grup İsmi	Eklenecek ağ geçidi gruplarının ismi görüntülenir.
3	Bağlantılar/Ağırlık	Gruplanan ağ geçitlerini ve ağ geçitlerinin öncelik değerleri görüntülenir.
4	Yönet	Gruplanan ağ geçitlerini düzenleyebilir veya silebilir.


-Ağ Geçidi modülünde eklenecek ağ geçitlerini gruplamak için ekle butonuna tıklayarak ağ geçitleri gruplanır.



1	İsim	Ağ geçidi grubuna verilecek isim girilir.
2	Üyeler	Ağ geçidi grubuna üye olan Ağ Geçitlerini gösterir. Eklenecek Ağ Geçitlerinin üyeler listesinden silindiği bölümdür.
3	Ağ Geçitleri	Ağ Geçitlerinin listesinin görüntülediği ve görüntülenen Ağ Geçitlerini üye olarak eklendiği bölümdür.
4	Kaydet	Ağ Geçitlerinin gruplarının ayarlarının kaydedildiği butondur.

5	Kapat	Ekle butonuna tıklanılarak açılan pencerenin kapatıldığı butondur.
---	--------------	--

-Eklenen Ağ Geçidi Grupları aşağıdaki gibi görünür.

DSL_LB	DSL2 / 1 DSL / 1	
--------	---------------------	---

11.4 DHCP

DHCP, Dinamik Host Konfigürasyonu Protokolü anlamına gelir.

DHCP Sunucusu, LAN içerisindeki host sistemleri için alt ağ maskesi ve standard ağ geçiş noktası gibi ilgili konfigürasyon bilgilerini ve IP adresini sağlar. Her bilgisayar için, sisteme tanımlanacak benzersiz bir IP adresi belirler.

DHCP, insanlar tarafından yapılan hataları azaltmak için IP yönetimini merkezileştirmek istenilen büyük ağlar üzerinde kullanışlı bir birimdir.

DHCP, bir takım IP üzerinden talep edilen istemciler için otomatik olarak IP atayan bir sunucudur.

-DHCP servisinin çalışma adımları;

1.DHCP Keşif(Discover): Bir cihaz ağa ilk bağlandığında veya ayarlandırması gerektiğinde DHCP keşfetmeye başlar. Cihaz, ağdaki DHCP sunucusunu bulmak için broadcast bir mesaj gönderir. Mesajın içeriğinde ağ ismi, MAC adresi gibi bilgiler bulunur.

2.DHCP Teklifi(Offer): DHCP sunucusu, DHCP keşif mesajını alır ve ağdaki kullanılabilir IP adreslerinden birini ve diğer ağ yapılandırma bilgilerini içeren bir teklif hazırlar. Bu teklif, DHCP sunucusu tarafından cihaza gönderilir.

3.DHCP İsteği(Request): Cihaz, aldığı DHCP teklifini kabul eder ve isteğe bağlı olarak IP adresini kullanmak istediğini belirten bir DHCP isteği gönderir.

4.DHCP Kabulü(Acknowledge): DHCP sunucusu, isteği aldığını doğrulayan bir kabul mesajı(ACK) gönderir. Bu mesaj, cihazın belirli bir IP adresini kullanmasına izin verir ve diğer ağ yapılandırma bilgilerini içerir.

Not

Yukarıdaki DHCP adımları genellikle bir cihazın ağa ilk kez bağlandığında veya mevcut IP adresi kiralama süresinde dolduğunda gerçekleşir.

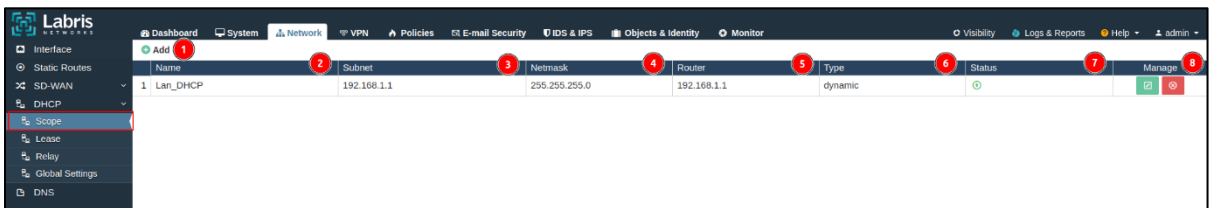
-Labris UTM cihazı üzerinde DHCP sunucu, DHCP'nin kira listesini, başka bir DHCP sunucusudan IP dağıtılabılır ve DHCP genel ayarları yapılır.



1	Ekle	DHCP Sunucusu ekleme işlemini yapıldığı butondur.
2	İsim	Eklenecek DHCP sunucusuna verilen isim görüntülenir.
3	Alt Ağ	DHCP sunucusunun tanımlandığı ağ adresi görüntülenir.
4	Ağ Maskesi	DHCP sunucusunun Ağ Maskesi görüntülenir.
5	Yönlendirici	Eklenecek DHCP sunucusunun yönlendirici adresi görüntülenir.
6	Tip	Sunucunun Tipi görüntülenir.
7	Durum	DHCP sunucusunun durumunu gösterir. Durum bölümünde yeşil ifade var ise DHCP sunucusu aktif, kırmızı ifade var ise DHCP sunucusu pasiftir.
8	Yönet	Eklenecek DHCP sunucusunu silmek ve bilgilerini tekrar düzenlemek için kullanılır.

11.4.1 Sunucu

Labris UTM cihazı üzerinde DHCP Sunucusu tanımlandığı modüldür. Bu modülde Labris UTM cihazı DHCP Sunucu görevi görür.



Labris UTM cihazı üzerinde DHCP Sunucu ekleme için ekle butonuna tıklanır. Ekle butonuna tıkladıktan sonra karşımıza gelen ekrandaki bilgileri doldurarak Labris UTM cihazına DHCP Sunucu tanımlanabilir.

-Ekle butonuna tıkladıktan sonra karşımıza gelen ekran aşağıdaki gibidir.

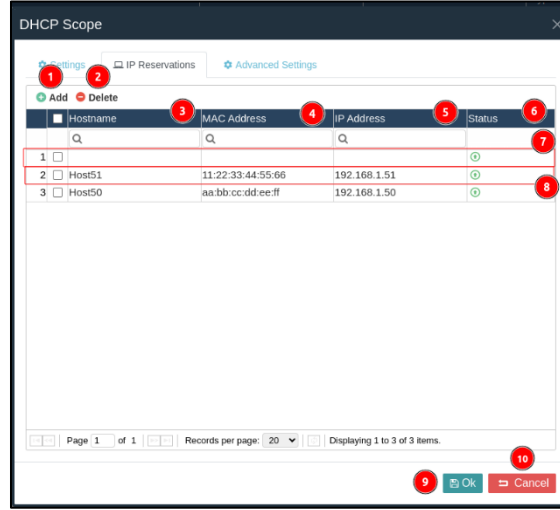
1	Ayarlar	DHCP Sunucusu ayarlarının düzenlendiği ekrandır.
2	IP Rezervasyonları	DHCP sunucusu üzerindeki IP rezervasyonların yapıldığı bölümdür.
3	Gelişmiş Ayarlar	Eklenecek DHCP sunucusunun gelişmiş ayarları yapılır.
4	Etkinleştir	DHCP sunucusunun etkinleştirildiği butondur.
5	Tip	Eklenecek DHCP tipi ayarlanır. Sunucu tipi olarak Dinamik ya da Statik seçilir. Dinamik seçilmesi durumunda DHCP sunucusu IP adreslerini otomatik dağıtır. Statik seçilmesi durumunda DHCP sunucusunda IP Rezervasyon bölümünde ekli olması gerekir. Sunucu IP adreslerini otomatik olarak dağıtmaz.
6	Kapsam Adı	DHCP sunucusunun ismi girilir.

7	Arabirim	DHCP sunucusu oluşturulacak arabirim seçilir.
8	Ağ Adresi	DHCP sunucusunun ağ adresini özel olarak girmek için kullanılan butondur. İşaretlenmediği durumda ise arabirime ait ağ adresi kullanılır.
9	Yönlendirici	DHCP sunucusun yönlendirici adresini özel olarak girmek için kullanılan butondur. İşaretlenmediği durumda ise arabirime ait yönlendirici adresi kullanılır.
10	Kira Süresi	DHCP sunucusunun istemciye vermiş olduğu IP adresinin kullanılabileceği sürenin girildiği bölümdür.
11	Azami Kira Süresi	DHCP sunucusunun istemciye vermiş olduğu IP adresinin kullanılabileceği azami sürenin girildiği bölümdür.
12	Alan Adı	DCHP sunucusunun alan adının girildiği bölümdür.
13	DNS	DNS adreslerini özel olarak ayarlamak istenilen durumlarda etkinleştirir.
14	Birincil DNS	DNS bölümünü işaretlendiğinde Birincil DNS adresleri girilir.
15	İkincil DNS	DNS bölümünü işaretlendiğinde İkincil DNS adresleri girilir.
16	IP Aralığı	DHCP sunucusunun IP Aralığının seçildiği bölümdür. Burada başlangıç ve bitiş IP adresleri girilmesi gerekmektedir.
17	İp Aralığı Ekle	Başlangıç ve bitiş IP adresleri girildikten sonra + butonuna tıklamak gerekmektedir.
18	IP Aralığı Listesi	Eklenecek IP aralıklarının liste halinde görüntülenir.
19	Kaydet	DHCP sunucusunda yapılan konfigürasyon ayarlarının kaydedildiği butondur.

20	İptal	Ekle butonuna tıklandığında açılan pencerenin kapatıldığı butondur.
----	--------------	---

Labris cihazı üzerinde yapılandırılan DHCP sunucusunda IP/MAC eşleştirmesi yapmak için aşağıdaki adımlar uygulanır.

- 1- Ağ/Dhcp/Sunucu modülüne girilir.
- 2- IP/MAC eşleştirilecek sunucunun yönet sütunundan düzenle butonuna tıklanır.
- 3- Düzenle butonuna tıklandıktan sonra gelen ekrandan IP Rezervasyonları bölümü seçilir.
- 4- IP Rezervasyonları bölümünden ekle butonuna tıklayarak sunucu adı, MAC Adresi ve IP Adresi bilgileri girilerek IP/MAC eşleşmesi yapılır.
- 5- Son olarak IP/MAC Eşleşmesi yapılan sunucularını silmek için sil butonuna tıklayarak işaretlediğiniz istemcileri silebilirsiniz.

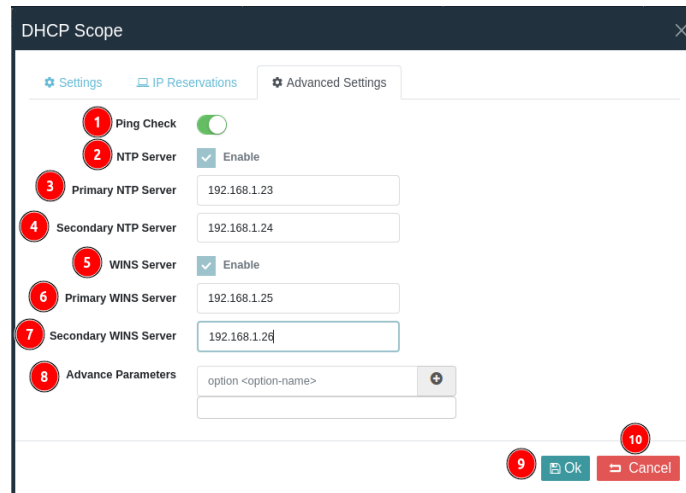


1	Ekle	IP/MAC eşleme yapabilmek için kullanılır.
2	Sil	IP/MAC eşleme yapılan istemcileri silmek için kullanılır.
3	Sunucu Adı	IP/MAC eşleme yapılan sunucunun adının görüntülediği bölümdür.
4	MAC Adresi	IP/MAC eşleşmesi yapılan cihazın MAC adresinin düzenlendiği bölümdür.

5	IP Adresi	IP/MAC eşlemesi yapılan cihazın IP adresinin düzenlendiği bölümdür.
6	Durum	IP/MAC eşlemesi yapılan cihazın durumu görüntülenir. Durum yeşil renk ise IP/MAC eşleşmesi yapılmıştır. Kırmızı renk ise IP/MAC eşleşmesi yapılmamıştır.
7	Adres Ekleme	IP/MAC eşleşmesi eklemek için ekle butonuna tıkladıktan sonra sunucu adı, MAC adresi, IP adresi ve durum bilgileri ayarlanır.
8	Eklenmiş Adres	IP/MAC eşleşme yapılmış olan istemciler bu şekilde görünür.
9	Kaydet	IP/MAC eşleşme yapılmış olan istemcilerin kaydedildiği butondur.
10	İptal	DHCP sunucusun ekranın iptal edildiği butondur.

-Labris cihazı üzerinde yapılandırılan DHCP sunucusuna gelişmiş ayarlar aşağıdaki adımlar uygulanır. Gelişmiş Ayarlar'la birlikte DHCP sunucu üzerinde DNS, varsayılan ağ geçidi, zaman sunucusu, WINS sunucuları vb. İşlemler yapılır.

- 1- Ağ/Dhcp/Sunucu modülüne girilir.
- 2- Gelişmiş Ayarları yapılacak olan sunucunun yönet sütunundan düzenle butonuna tıklanır.
- 3- Düzenle butonuna tıklandıktan sonra gelen ekrandan Gelişmiş Ayarlar bölümü seçilir.
- 4- Buradan eklemek istediğiniz NTP, WINS serverları ekleyebilir, DHCP gelişmiş parameter ekleyebilirsiniz.



1	Ping Kontrolü	DHCP üzerinde ping kontrolünün açıldığı butondur.
2	NTP Sunucusu	DHCP sunucunuzu üzerine NTP sunucu eklemek için işaretlenmesi gereken butondur. NTP sunucusunun IP adresini eklemek için etkinleştirin işaretli olması gerekir.
3	Birincil NTP Sunucusu	Birincil NTP sunucusun adresi girilir.
4	İkincil NTP Sunucusu	İkincil NTP sunucusu adresi girilir.
5	WINS Sunucusu	DHCP sunucu üzerinde WINS sunucusu eklemek için kullanılan butondur. WINS sunucusu eklemek için etkinleştir butonun işaretli olması gerekir.
6	Birincil WINS Sunucusu	Birincil olarak eklenecek WINS sunucusu eklenir.
7	İkincil WINS Sunucusu	İkincil olarak eklenecek WINS sunucusu eklenir.
8	Gelişmiş Parametreler	DHCP sunucusu üzerinde gelişmiş parametre eklenmesi için kullanılır.
9	Kaydet	DHCP ayarlarının kaydedildiği butondur.
10	İptal	DHCP ayarlarının iptal edildiği butondur.

11.4.2 Kira Listesi

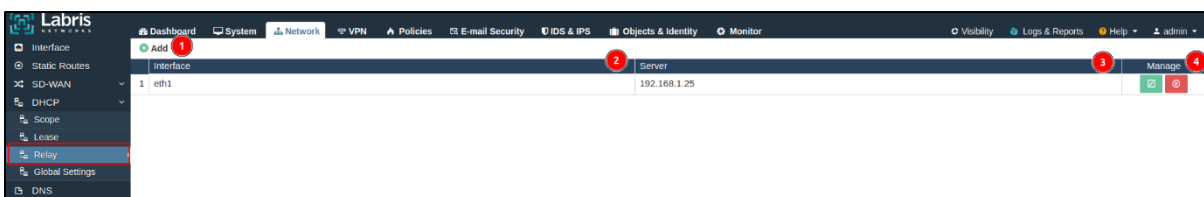
Kira Listesi modülünde DHCP sunucunun istemciye vermiş olduğu IP adreslerinin listesini görülür.

	1	2	3	4	5	6	7	8	9	10
	Reserve	Delete	IP Address	Physical Address	Start Date	End Date	Scope	Name	Lease	Status
1	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.51	11:22:33:44:55:66	2024/03/14 10:22:40	2025/03/14 10:22:40	Lan_DHCP	Host51	reserved	⊕
2	<input type="checkbox"/>	<input type="checkbox"/>	192.168.1.50	aa:bb:cc:dd:ee:ff	2024/03/14 10:22:40	2025/03/14 10:22:40	Lan_DHCP	Host50	reserved	⊕

1	Rezerve Et	DHCP sunucusundan IP alan istemcilerin IP ve MAC adreslerinin eşleşmesinin yapıldığı butondur. Eşleşme yapılacak istemcinin işaretlenmesi gerekmektedir.
2	Sil	DHCP sunucusundan IP alan istemcilerin kira listesinden silindiği butondur. Silme işlemi yapılacak olan istemcinin işaretlenmesi gerekmektedir.
3	IP Adresi	İstemcinin DHCP sunucusundan aldığı IP adresinin görüntülediği bölümdür.
4	Fiziksel Adres	İstemcinin MAC adresi görüntülenir.
5	Başlangıç Tarihi	İstemcinin DHCP sunucusundan IP aldığı ilk tarih görüntülenir.
6	Bitiş Tarihi	İstemcinin DHCP sunucusundan IP adresini bırakacağı tarih görüntülenir.
7	Kapsam	IP adresini hangi DHCP sunucusundan aldığı görüntülenir.
8	İsim	İstemcinin ismi görüntülenir.
9	Kira	DHCP sunucusundan IP adresi alan istemcinin kira durumu görüntülenir.
10	Durum	DHCP sunucusundan IP alan istemcinin durumu görüntülenir

11.4.3 Yönlendir

Labris UTM cihazı üzerinde olmayan DHCP sunucusunu tanımlamak için kullanılan modüldür.



1	Ekle	Labris UTM cihazı üzerinde olmayan DHCP sunucu eklemek için kullanılan butondur.
2	Arabirim	DHCP sunucunun bulunduğu arabirimin görüntülenir.
3	Sunucu	DHCP sunucunun IP adresi görüntülenir.
4	Yönet	DHCP sunucunun silindiği veya yapılandırmanın düzenlendiği bölümdür.

-Labris UTM cihazına DHCP server eklemek için ekle butonuna tıklanır. Ekle butonuna tıkladıktan sonra karşımıza gelen ekrandaki gerekli bilgiler girilerek ekleme işlemi yapılır.

1	Sunucu	DHCP sunucusunun IP adresi girilir.
2	Arabirim	DHCP sunucusunun bulunduğu arabirim seçilir.
3	Kaydet	DHCP sunucusunun ayarlarının kaydedildiği butondur.
4	Kapat	DHCP sunucusunun ayarlarının kapatıldığı butondur.

11.4.4 Genel Ayarlar

DHCP modülünde eklenen sunucuların Genel Ayarlarının yapıldığı bölümdür.

1	Kaydet	Yazılan gelişmiş parametrelerin kaydedildiği butondur.
---	---------------	--

2	Gelişmiş Parametreler	DHCP sunucusuyla Gelişmiş Parametrelerin girildiği yerdir.
3	Gelişmiş Parametre Ekle	Girilen parametrenin eklendiği butondur.
4	Gelişmiş Parametre Lisesi	Girilen parametrelerinin listesinin görüntülendiği yerdir.

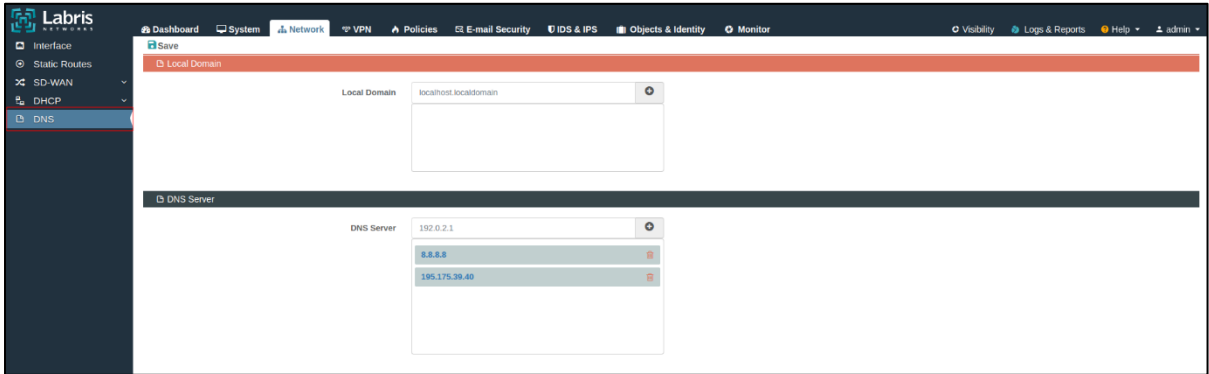
11.5 DNS

Alan Adı Sistemi(Domain Name System), internet üzerindeki cihazların adreslerini, anlamlı ve hatırlanabilir alan adlarıyla eşleştiren bir sistemdir.

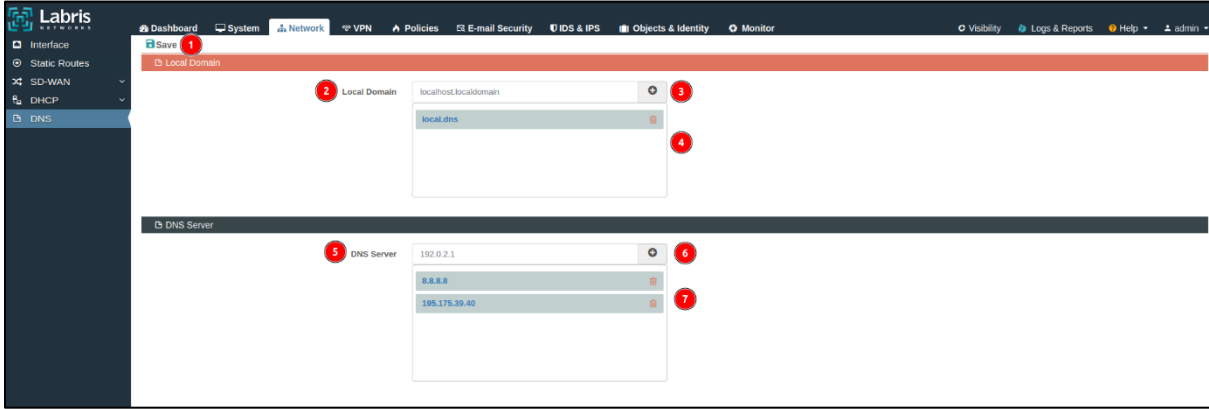
İnternet üzerinde gezinirken, bir web sitesine erişmek istediğinizde, tarayıcınıza yazdığınız alan adı DNS tarafından ilgili IP adresine çevrilir.

DNS'in temel amacı insanların kolayca anlayabilecekleri alan adlarını internetin anlayabileceği sayısal IP adreslerine dönüştürür. Bu sayede internetin daha kullanıcı dostu ve erişebilir olmasını sağlar.

Labris UTM cihazındaki kullanım amacı ise cihazın DNS çözümlemesi yapmasıdır.



Labris cihazı üzerinde Yerel Alan Adı olarak veya Alan Adı Server Sunucusunun IP adresi girilerek yapılır.



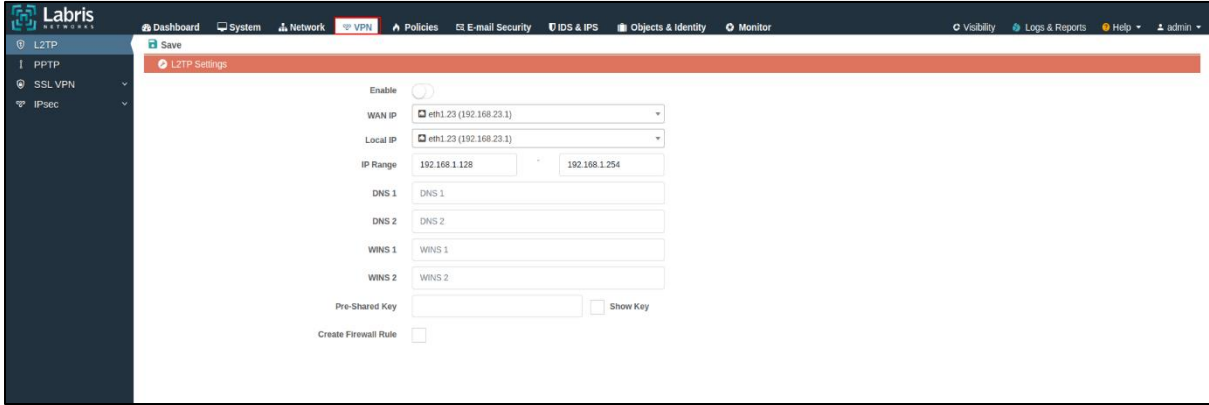
1	Kaydet	DNS modülünde yapılan değişikliklerin kaydedildiği butondur.
2	Yerel Alan Adı	Yerel Alan Adı sunucusunun domain adresini girilir. DNS sunucunuzun domain adresidir.
3	Yerel Alan Adı Ekle	Yazılan domain adresinin eklendiği yerdir.
4	Eklenen Yerel Alan Adı Listele	Eklenmiş olan domain adresinin listesinin görüntülediği yerdir.
5	Alan Adı Sistemi Sunucusu	Alan adı sunucusunun IP adresinin eklendiği bölümdür. Eklenecek olan DNS sunucusunun IP adresi girilir.
6	Alan Adı Sistemi Sunucusu Ekle	Alan adı sunucusunun IP adresinin eklendiği yerdir.
7	Eklenen Alan Adı Sistemi Sunucusu Listesi	Eklenmiş olan DNS sunucusunun IP adresinin listesinin görüntülediği yerdir.

12. VPN

VPN, Sanal Özel Ağ anlamına gelir. Güvenli bir yol ile uzaktan kamuya açık ağa bağlanmamızı sağlayan Özel bir ağıdır.

Kişisel VPN'ler verilerinizin bilgisayarınızdan bir VPN sunucusuna gönderilmemesi için şifrelenmiştir. Bu durumda sanal korsanların(hacker) kamuya açık bir Wi-Fi üzerinden internete bağlandığınız sırada bilgilerinizi çalmayı engeller. VPN'ler yalnızca engellenmiş sitelere erişim dışında bir takım işlemler için de kullanılabilir, ayrıca Kamuya açık bir Wi-Fi noktasını güvenli konuma getirmek için VPN kullanırken, torrent istemcisi, tarayıcı, yükleme yönetici vs. Birimler gibi seçili uygulamalar için VPN olmayan trafik akışlarını engellemek adına Windows Güvenlik Duvarını kullanır.

Labris UTM cihazı üzerinde VPN, kurumların Özel Ağ kullanarak kurum içi veya kurumlar arası ağlara erişmek için kullanılır. Cihaz üzerinde kurum içi ve kurumlar arası ağlara erişmek için L2TP, PPTP, SSLVPN ve IPSec kullanılır.

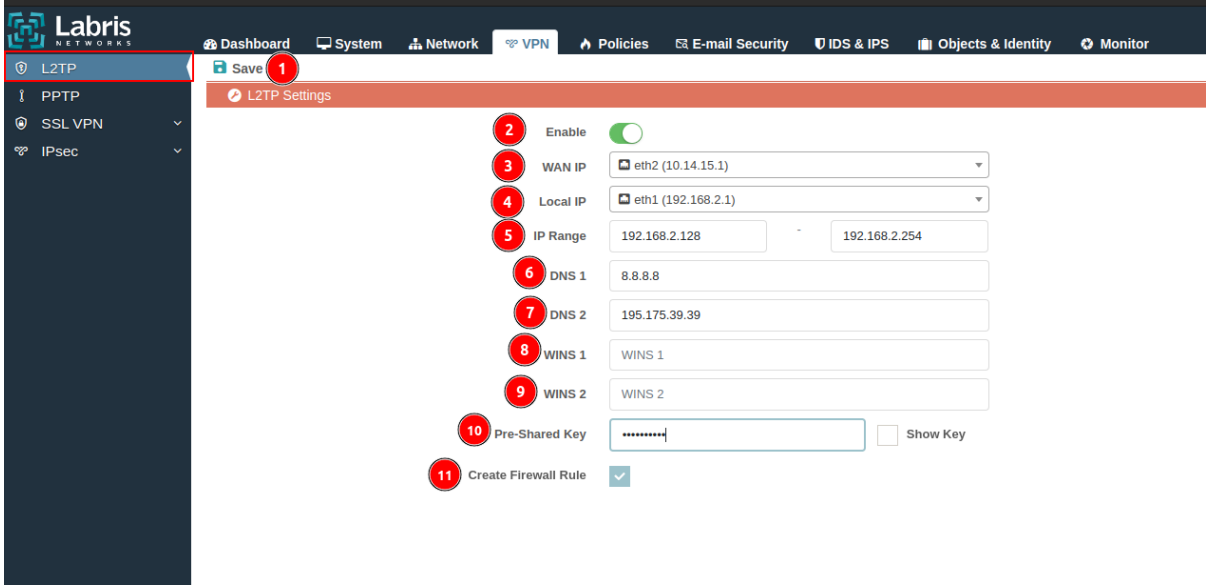


12.1 L2TP

L2TP (Katman 2 Tünelleme Protokolü), sanal özel ağlar (VPN'ler) veya internet servis sağlayıcıları (ISS) tarafından hizmetlerin sunulmasında kullanılan bir tünel protokolüdür.

OSI modelinin veri bağlantı katmanında (Katman2) çalışır.

L2TP, PPP (Point to Point Protocol) çerçevelerini IP paketleri içine kapsüller ve bunları internet veya diğer IP tabanlı ağlar üzerinden veri iletimini sağlar.



1	Kaydet	L2TP yapılandırma ayarlarının kaydedildiği butondur.
2	Etkinleştir	L2TP VPN'in etkinleştirildiği butondur.
3	WAN IP	L2TP VPN'in WAN IP adresinin seçildiği yerdir.
4	Yerel IP	L2TP VPN ile erişilecek yerel ağın seçildiği yerdir.
5	IP Aralığı	L2TP VPN'e bağlanacak olan kullanıcıların alacağı IP'nin girildiği yerdir.
6	DNS 1	VPN kullanıcıları için DNS çözmeleri için girilecek ilk DNS sunucunun IP adresi girilir.
7	DNS 2	VPN kullanıcıları için DNS çözmeleri için girilecek ikinci DNS sunucunun IP adresi girilir.

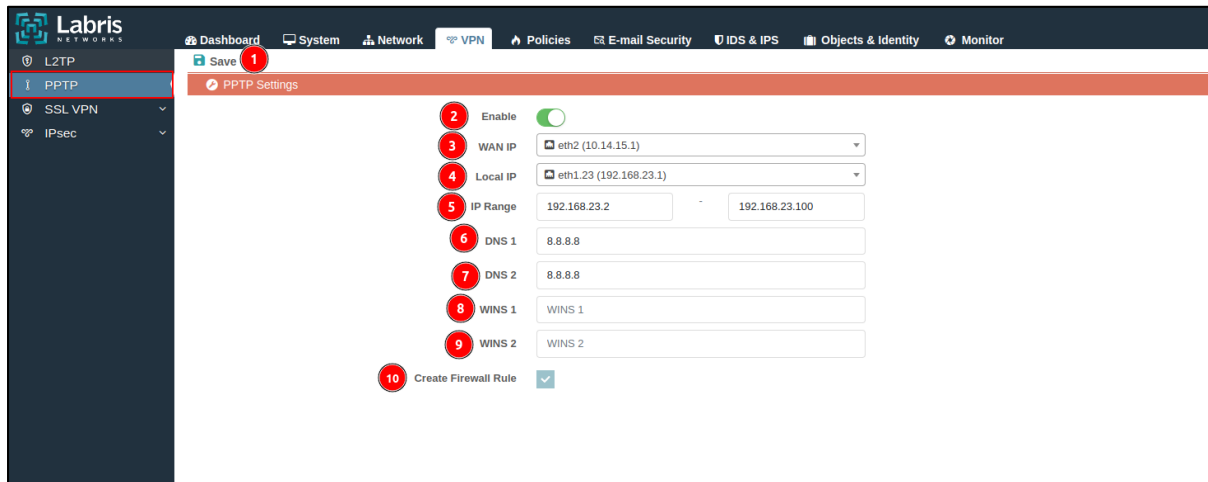
8	WINS 1	Windows ağlarında NetBIOS adlarının çözümlenmesinde kullanılan servistir. WINS varsa buraya sunucusunuzun IP adresi girilir.
9	WINS 2	Windows ağlarında NetBIOS adlarının çözümlenmesinde kullanılan servistir. İkinci bir WINS varsa buraya sunucusunuzun IP adresi girilir.
10	Önceden Paylaşılan Anahtar	L2TP bağlantısı için önceden paylaşılan anahtar oluşturulması gerekir. Bu bölümden paylaşılan anahtar oluşturulur.
11	Güvenlik Duvarı Kuralı Oluştur	L2TP VPN için güvenlik duvarı kuralı oluşturur.

12.2 PPTP

PPTP(Noktadan Noktaya Tünel Protokolü), sanal özel ağları uygulamanın bir yoludur.

PPTP, uzak erişim VPN'leri için kullanılan bir iletişim protokolüdür.

PPTP, bir bilgisayarın uzak bir ağa güvenli bir şekilde bağlanmasını sağlar. Bu genellikle bir çalışanın evden veya dış ofisten şirket ağına erişmek için kullanılır. İnternet üzerinden şifrelenmiş bir tünel oluşturarak, veri iletimini güvenli hale getirir.



1	Kaydet	PPTP yapılandırma ayarlarının kaydedildiği butondur.
2	Etkinleştir	PPTP VPN'in etkinleştirildiği butondur.
3	WAN IP	PPTP VPN'in WAN IP adresinin seçildiği yerdir.

4	Yerel IP	PPTP VPN ile erişebilecek yerel ağın seçildiği yerdir.
5	IP Aralığı	PPTP VPN'e bağlanacak olan kullanıcıların alacağı IP'nin girildiği yerdir.
6	DNS 1	VPN kullanıcıları için DNS çözmeleri için girilecek ilk DNS sunucunun IP adresi girilir.
7	DNS 2	VPN kullanıcıları için DNS çözmeleri için girilecek ikinci DNS sunucunun IP adresi girilir.
8	WINS(Windows Internet Naming Service) 1	Windows ağlarında NetBIOS adlarının çözümlenmesinde kullanılan servistir. WINS varsa buraya sunucusunuzun IP adresi girilir.
9	WINS(Windows Internet Naming Service) 2	Windows ağlarında NetBIOS adlarının çözümlenmesinde kullanılan servistir. İkinci bir WINS varsa buraya sunucusunuzun IP adresi girilir.
10	Güvenlik Duvarı Kuralı Oluştur	PPTP VPN için güvenlik duvarı kuralı oluşturulduğu butondur.

Not

WINS, NetBIOS adlarını IP adreslerine çevirir ve bu sayede bilgisayarlar birbirlerini bulabilir.

12.3 SSL VPN

SSL VPN(Secure Socket Layer Virtual Private Network), uzaktan erişim sağlamak için sağlamak için kullanılan bir VPN türüdür ve genellikle web tarayıcıları üzerinden erişilebilir.

SSL VPN'le birlikte yerel ağınıza erişimi uzaktan sağlamak için kullanılır.

SSL VPN kullanıcıların uzak ağ kaynaklarına güvenli bir şekilde erişmelerine olanak tanır ve erişim Labris UTM cihazı üzerinden kontrol edilir ve gerektiği durumlarda kullanıcılara erişim yetkisi verilebilir.

SSL VPN, Labris UTM cihazı tarafından desteklenir ve yapılandırılması kurumların ağlarına göre özel olarak yapılandırılabilir.

The screenshot displays the Labris UTM VPN configuration interface. The left sidebar shows the navigation menu with 'SSL VPN' selected. The main content area is divided into three sections:

- Network Settings:** Includes an 'Enable' toggle (checked), 'Protocol' set to 'TCP', 'Port' set to '4443', 'Tunnel Network / Mask' set to '10.8.3.0' and '255.255.255.0', and 'WAN IP' set to '10.20.30.40'.
- Security Settings:** Includes 'Server Certificate' set to 'Default', 'Authentication Method' set to 'User', 'Diffie-Hellman Group' set to '2048', 'Encryption Algorithm' set to 'AES-256-CBC', and 'Authentication Algorithm' set to 'SHA1'.
- Client Settings:** Includes 'Redirect Internet traffic into VPN' toggle (checked), 'Local Networks' list with '0.0.0.0/0.0.0.0', '192.168.1.0/255.255.255.0', and '192.168.23.5/255.255.255.255', 'Domain' set to 'vpn.dns', 'DNS 1' set to '8.8.8.8', and 'DNS 2' set to '8.8.4.4'.

12.3.1 Tünel

Labris UTM cihazı üzerinde SSL VPN yapılandırması için tünel ayarlarının yapılır. SSL VPN'e public IP adresini, kullanılacak protokol bilgileri, port numarası, SSL VPN kullanılarak erişilecekleri ağların konfigürasyonları yapılır.

12.3.1.1 Ağ Ayarları

SSL VPN' in etkinleştirildiği, protokol, port, tünel ağı ve WAN IP adresinin girildiği bölümdür.

1	Kaydet	SSL VPN yapılandırılmasının kaydedildiği butondur.
2	Etkinleştir	SSL VPN' in etkinleştirildiği butondur.
3	Protokol	SSL VPN'e bağlanırken kullanılacak protokol seçilir. TCP protokolü kullanılacak ise TCP, UDP protokolü

		kullanılacak ise UDP protokolünün seçilmesi gerekmektedir.
4	Port	SSL VPN'e bağlanırken kullanılacak port numarasının girildiği bölümdür.
5	Tünel Ağı / Maske	SSL VPN'e bağlandıktan sonra kullanıcıların alacağı IP adresinin belirtildiği yerdir. İlk Tünelin kullanacağı ağ ve ağ maskesi girilir.
6	WAN IP	SSL VPN'e bağlanırken kullanılacak WAN IP adresinin girildiği bölümdür. Eğer tek hat var ise any olarak bırakılması gerekir.

12.3.1.2 Güvenlik Ayarları

SSL VPN'in şifreleme ayarlarının yapıldığı, bağlanan kullanıcıların sertifika ayarlarının bölümdür.

Security Settings

1

Server Certificate

Default

2

Authentication Method

User

3

Diffie-Hellman Group

2048

4

Encryption Algorithm

AES-256-CBC

5

Authentication Algorithm

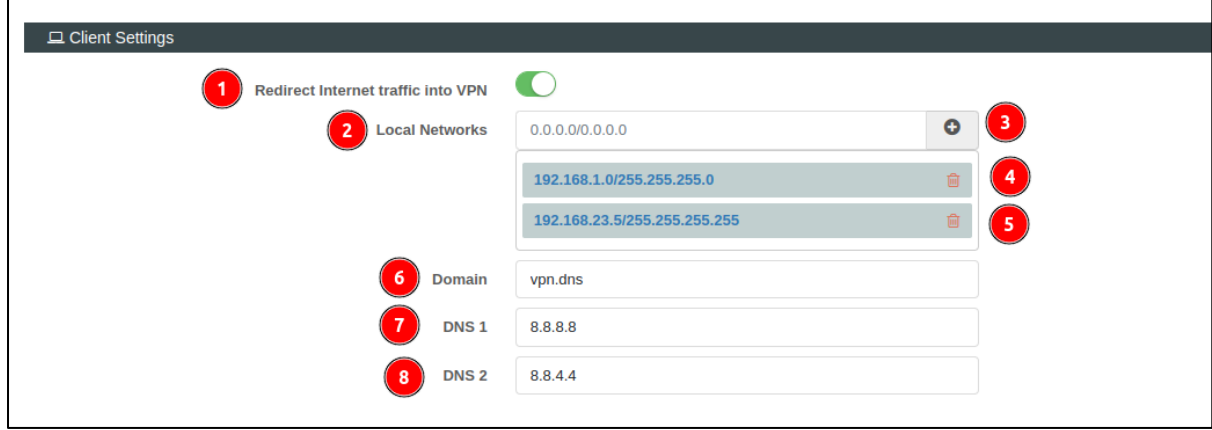
SHA1

1	Sunucu Sertifikası	SSL VPN'de bağlantı sağlayacak kullanıcının sertifikasının seçildiği bölümdür.
2	Kimlik Doğrulama Metodu	SSL VPN' e bağlanacak olan kullanıcıların kimlik doğrulama metodu seçilir. Sunucu Sertifikasında, Sertifika Yönetiminde eklenen sertifikanın seçilmesiyle açılır.
3	Diffie-Hellman Grubu	SSL VPN'in anahtar paylaşımının güvenli bir şekilde yapılmasını sağlayan protokoldür.
4	Şifreleme Algoritması	SSL VPN'e bağlanan kullanıcıların şifreleme algoritmasının seçildiği yerdir.
5	Kimlik Doğrulama	SSL VPN'e bağlanan kullanıcıların kimlik doğrulama

	Algoritması	algoritmasının seçildiği yerdir.
--	--------------------	----------------------------------

12.3.1.3 İstemci Ayarları

İstemci Ayarlarında SSL VPN'e bağlanan kullanıcıların internete VPN üzerinden çıkılması gereken durumlarda, erişebilecekleri yerel ağları, DNS adresleri belirtilir.



1	İnternet Trafiğini VPN'e Yönlendir	Bağlanan kullanıcıların VPN üzerinden internete çıkması gereken durumlarda kullanılır.
2	Yerel Ağlar	SSL VPN'e bağlanan kullanıcıların erişebilecekleri yerel ağların eklendiği bölümdür.
3	Yerel Ağ Ekle	Yazılan yerel ağın eklendiği butondur. 192.168.23.22/255.255.255.255 şeklinde yazılır.
4	Yerel Ağ Listesi	Eklene yerel ağların listesinin görüntülediği veya eklenen yerel ağların listeden çıkarıldığı bölümdür.
5	Alan Adı	Alan adı sunucusunun domain adresinin girildiği bölümdür.
6	DNS 1	SSL VPN'e bağlanan kullanıcıların DNS çözmeleri için gerekli olan birincil DNS sunucusunun IP adresi girilir.
7	DNS 2	SSL VPN'e bağlanan kullanıcıların DNS çözmeleri için gerekli olan ikincil DNS sunucusunun IP adresi girilir.

12.3.1.4 Diğer Ayarlar

SSL VPN'e bağlanan kullanıcıların sayısının belirtildiği, dinamik IP değişikliğindeki oturum durumu gibi ayarlarının yapıldığı bölümdür.

1	Maksimum Eş Zamanlı Bağlantı	SSL VPN bağlantısı yapan maksimum bağlantı sayısıdır.
2	Dinamik değişimleri için oturumu yükler	SSL VPN'e bağlanan kullanıcıların dinamik IP adresinin değiştirildiği durumlarda açılan oturumu geri yükler.
3	İstemciler arası bağlantılara izin ver	SSL VPN'e bağlanan kullanıcıların kendi arasındaki iletişime izin verir.
4	Sıkıştırma	SSL VPN'de VPN trafiğini optimize etmek ve bant genişliğini azaltmak için sıkıştırma işlemi yapan protokollerin seçildiği yerdir.

12.3.2 Yer İmi

SSL VPN Yer imi, kullanıcıların SSL VPN istemcisinde erişirken kullanabilecekleri bir bağlantı noktasıdır. Yer imiyle birlikte kullanıcıların belirli bir SSL VPN hedefine(yer imine) erişmek için kullanabilecekleri bir kısayol veya adrestir.

SSL VPN Yer imi, kullanıcıların herhangi bir cihazda SSL VPN'e hızlı erişimlerini sağlar. Kullanıcılar yer imini tarayıcılarına kaydedebilirler.

1	Ekle	SSL VPN yer imini eklendiği butondur.
---	-------------	---------------------------------------

2	İsim	SSLVPN yer imine verilen ismin görüntülediği bölümdür.
3	Alan Adı	Yer imi olarak eklenen yer iminin alan adı görüntülenir.
4	URL	Yer imi olarak eklenen URL'in görüntülediği bölümdür.
5	Alt Alan Adlarına İzin Ver	Yer imi olarak eklenen alan adının alt alan adlarına izin verildiğinin görüntülediği sütundur.
6	Yönet	Eklenen yer iminin silindiği veya düzenlendiği sütundur.

-SSL VPN yer imi eklemek için ekle butonuna tıklayarak yer imi ekleme işlemi yapılır.

1	İsim	SSL VPN yer imine verilen ismin girildiği bölümdür.
2	Alan Adı	SSLVPN yer iminin Alan Adının girildiği bölümdür.
3	URL	SSL VPN yer imine verilen URL adresinin girildiği bölümdür.
4	Alt Alanlara İzin Ver	SSL VPN yer iminin alt alanlarına izin verildiği bölümdür.
5	Kaydet	SSL VPN yer imi yapılandırılmasının kaydedildiği butondur.

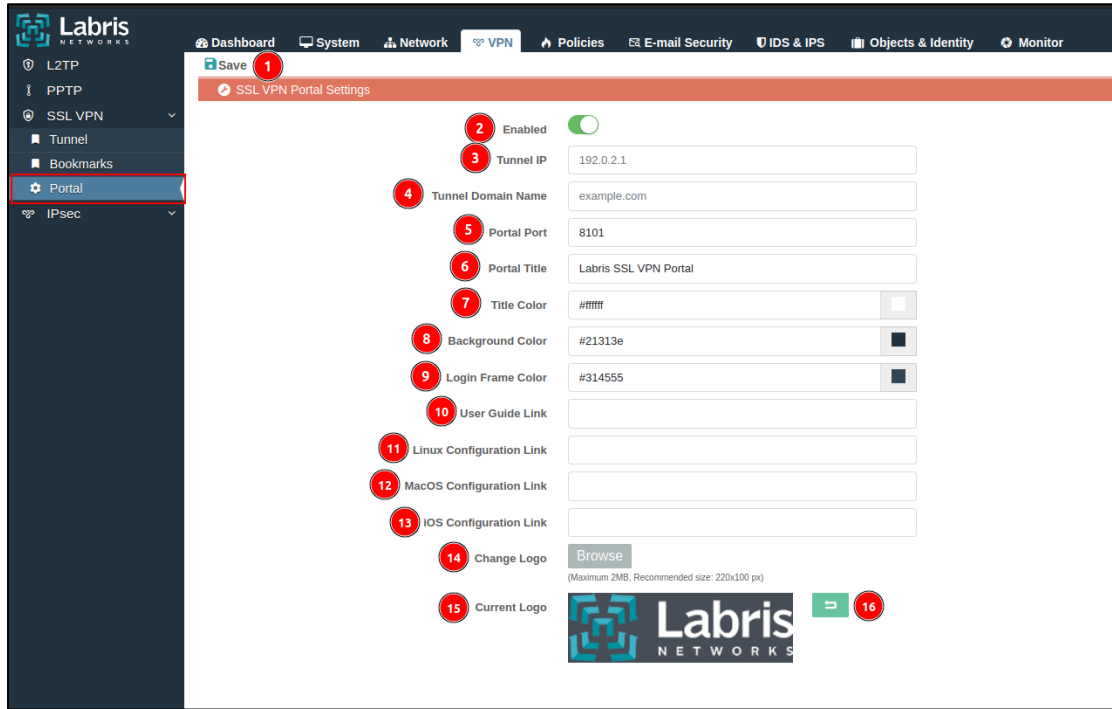
6	Kapat	SSL VPN yer imi penceresinin kapatıldığı butondur.
---	--------------	--

12.3.3 Portal

Kullanıcıların uzaktan erişmek istedikleri ağ kaynaklarına erişim sağladıkları bir web tabanlı portal olarak tasarlanmıştır.

SSL VPN portalı, kullanıcıların tarayıcılarını kullanarak güvenli bir şekilde uzaktan ağ kaynaklarına bağlanmalarını sağlar.

SSL VPN portal, kullanıcıların farklı cihazlardan ve farklı yerlerden güvenli bir şekilde ağ kaynaklarına erişimlerini sağlar.



1	Kaydet	SSL VPN portal'ın ayalarının kaydedildiği butondur.
2	Etkin	SSL VPN portal'ın etkinleştirildiği butondur.
3	Tünel IP'si	SSL VPN portal'ın IP adresinin girildiği yerdir.
4	Tünel Alan Adı İsmi	SSL VPN portal'ın alan adının girildiği yerdir.
5	Portal Portu	SSL VPN portal'ının portunun girildiği bölümdür.
6	Portal Başlığı	SSL VPN portalın başlık bilgisi girilir.


7	Başlık Rengi	SSL VPN portalın başlık renginin seçildiği bölümdür.
8	Arkaplan Rengi	SSL VPN portalın arkaplan renginin seçildiği bölümdür.
9	Giriş Çerçeve Rengi	SSL VPN portalın giriş çerçeve renginin seçildiği bölümdür.
10	Kullanıcı Rehber Linki	SSL VPN'e bağlanacak kullanıcılar için kullanıcı rehber linkinin eklendiği yerdir.
11	Linux Ayarları Linki	SSL VPN'e bağlanacak kullanıcılar için kullanıcı Linux ayarları linkinin eklendiği yerdir
12	MacOS Ayarları Linki	SSL VPN'e bağlanacak kullanıcılar için kullanıcı MacOS ayarları linkinin eklendiği yerdir
13	iOS Ayarları Linki	SSL VPN'e bağlanacak kullanıcılar için kullanıcı iOS ayarları linkinin eklendiği yerdir
14	Logoyu Değiştir.	SSL VPN portalın logosunun değiştirildiği bölümdür.
15	Şimdiki Logo	Eklenecek logonun görüntülendiği yerdir.
16	Ayarları Sıfırla	SSL VPN Portal'da yapılan yapılandırma ayarlarının sıfırlandığı bölümdür.





Not

SSL VPN yapılandırılması yapıldıktan sonra Politikalar modülünde kuralların yazılması gerekmektedir.

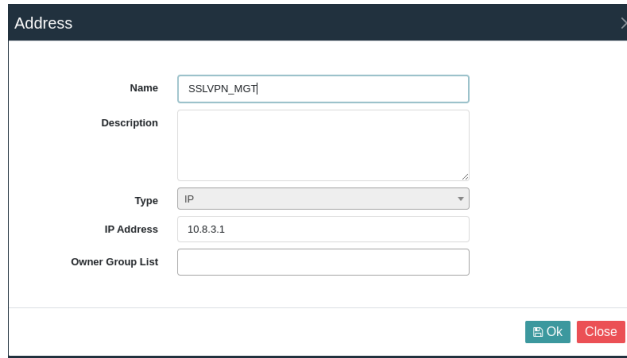
-SSL VPN'in Politikalar modülünde kuralının yazılmasının adımları;

1. SSL VPN konfigürasyonu yapılır.
2. Nesnelar ve Kimlikler modülü açılır.



Type	Name	Address	Manage
1 IP Address	Eğitim-1	192.168.1.80	  
2 IP Address	Eğitim-2	192.168.1.81	  
3 IP Address	Eğitim-3	192.168.1.82	  
4 IP Address	IPsec-WAN	10.20.30.40	  
5 IP Address	lan	192.168.1.1	  
6 IP Address	PublicIP-wan	10.14.15.1	  
7 IP Address	S-Web_6	192.168.1.6	  

3. Nesnelar ve Kimlikle modülü açıldıktan sonra SSL VPN için nesnelar oluşturulur. Ekle butonuna tıklanarak nesne eklemesi yapılır.



Name: SSLVPN_MGİT

Description:

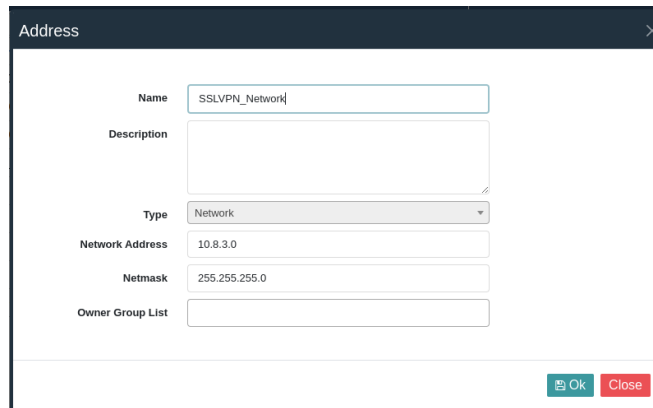
Type: IP

IP Address: 10.8.3.1

Owner Group List:

Ok Close

SSL VPN Arabirim IP Adresi Ekleme



Name: SSLVPN_Network

Description:

Type: Network

Network Address: 10.8.3.0

Netmask: 255.255.255.0

Owner Group List:

Ok Close

SSLVPN Ağ Adresini Ekleme

- Arabirim ve ağ adresleri tanımlandıktan sonra SSLVPN'in yapılacağı portunda Labris UTM cihazı üzerinde tanımlanması gerekir.

Service configuration window showing the following details:

- Name: TCP_4443
- Description: (Empty)
- Type: TCP
- TCP Options: Source Port Range: 0, Destination Port Range: 4443
- Flags: URG: Any, ACK: Any, PSH: Any, RST: Any, SYN: Any, FIN: Any
- TCP Flag Info: Any: DONT check flag (Predefined), 7: Use: Flag should be set

SSLVPN port ekleme

- Nesneler ve Kimlikler modülünde SSLVPN için nesnelere eklenir. Nesnelere eklendikten sonra Politikalar modülü açılır.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDOS	Logging	Manage
default (5)	SSLVPN_MGT WAN vlan23	*	*	*	Accept	*	*	*	On	[Edit] [Delete]
2	test	WAN	TCP_4443	*	Accept	*	*	*	On	[Edit] [Delete]
3	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	*	*	Accept	*	*	*	On	[Edit] [Delete]
4	*	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

- Politika modülü açıldıktan sonra 0. Kurala SSLVPN arabirim adresi eklenir.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDOS	Logging	Manage
0	SSLVPN_MGT WAN vLan23	*	*	*	Accept	*	*	*	On	[Edit] [Delete]
1	test	*	*	*	Accept	*	*	*	On	[Edit] [Delete]
2	*	WAN	TCP_4443	*	Accept	*	*	*	On	[Edit] [Delete]
3	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	*	*	Accept	*	*	*	On	[Edit] [Delete]
4	*	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

7. 0. Kurala SSLVPN arabirim eklendikten sonra 0. ile 1. kural arasına aşağıdaki kuralı yazmak gerekir.

Policy Name	Source	Destination	Service	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
0	SSLVPN_MGT WAN vLan23	*	*	Accept	*	*	*	On	[Manage]
1	test	*	*	Accept	*	*	*	On	[Manage]
2	*	WAN	TCP_4443	Accept	*	*	*	On	[Manage]
3	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	*	Accept	*	*	*	On	[Manage]
4	*	*	*	Drop	*	*	*	On	[Manage]

8. Yukarıdaki erişim kuralı yazıldıktan sonra SSLVPN ile SSLVPN yapılandırma ayarlarında bulunan İstemci Ayarlarında yazılı olan ağlara izin vermek gerekir.

Policy Name	Source	Destination	Service	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
0	SSLVPN_MGT WAN vLan23	*	*	Accept	*	*	*	On	[Manage]
1	test	*	*	Accept	*	*	*	On	[Manage]
2	*	WAN	TCP_4443	Accept	*	*	*	On	[Manage]
3	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	vLan23	Accept	*	*	*	On	[Manage]
4	*	*	*	Drop	*	*	*	On	[Manage]

9. Yukarıdaki tanımlamalar yapıldıktan SSLVPN erişimini test edebilirsiniz.

12.4 IPSec

IPSec(Internet Protocol Security), internet üzerinde veri iletişimde kullanılan bir güvenlik protokolüdür.

IPSec, internet üzerinden iletilen verilerin gizliliğini, bütünlüğünü ve güvenilirliğini sağlamak için kullanılır.

IPSec, bir ağ üzerinden güvenli bağlantılar kurmak için bir dizi iletişim kuralı veya protokolüdür.

Name	Description	Manage
1 IPSec	Q	[Manage]

12.4.1 Tünel

IPSec VPN için aşama 1 ve aşama 2 yapılandırılması yapılır.

Name	Description	Manage
1 IPSec	Q	[Manage]

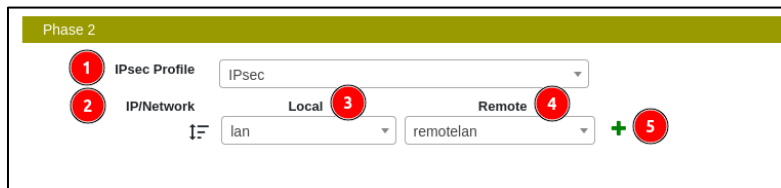
1	Ekle	IPSec tüneli ekleme işleminin yapıldığı butondur.
2	İsim	IPSec tüneline verilen ismin görüldüğü sütundur.
3	Açıklama	IPSec tüneline verilen açıklamanın girildiği bölümdür.
4	Yönet	Eklenen IPSec tünellerinin silindiği veya düzenlendiği bölümdür.

-IPSec tüneli eklemek için 'ekle' butonuna basıldıktan karşına gelen ekrandaki aşama-1 ve aşama-2 yapılandırmalarını IPSec yapılacak diğer cihazla aynı şekilde ayarlamak gerekir.

1	Etkinleştir	IPSec tüneli yapılandırılmasının etkinleştirildiği butondur.
2	İsim	IPSec tüneline isim verildiği bölümdür.
3	Açıklama	IPSec tüneliyle ilgili açıklamanın girildiği bölümdür.

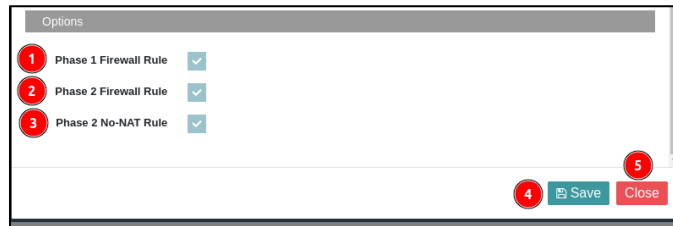
1	NAT Gezinmesi	IPSec paketlerinin NAT cihazları üzerinden geçmesine izin vermek için açılır ya da kapatılır.
2	IKE Profili	IKE profili modülünde hazırlanan IKE profilinin

		seçildiği yerdir.
3	Otomatik	Aşama-1'deki IKE protokolünü otomatik olarak başlatmak için kullanılır.
4	Yerel IP	IPSec yapılacak yerel IP adresinin seçildiği kısımdır.
5	Yerel Kimlik	Yerel kimlik bilgisinin yazıldığı bölümdür.
6	Uzak IP	IPSec yapılacak lokasyonun genel(public) IP adresinin girildiği bölümdür.
7	Uzak Kimlik	IPSec yapılacak lokasyonun genel(public) IP adresinin kimlik bilgisinin girildiği bölümdür.
8	Önceden Paylaşılan Anahtar	IPSec tünel için oluşturulan paylaşılan anahtarın girildiği bölümdür.
9	Şifreyi Göster	Oluşturulan paylaşılan anahtarın şifresinin gösterildiği butondur.



1	IPSec Profili	IPSec Profili modülünde yapılandırması yapılan IPSec Profilinin seçildiği kısımdır.
2	IP/Ağ	IPSec yapılacak yerel ve uzak IP adreslerinin seçilmesi gerekir. (Burada eklenecek IP adresleri yerel IP adresleridir ve Uzak yerel adresin Nesnelere ve Kimlikler menüsünden eklenmesi gerekmektedir.)
3	Yerel	Labris UTM cihazındaki yerel IP/Ağ adresi seçilir.
4	Uzak	IPSec yapılacak diğer cihazın yerel IP/Ağ adresi seçilir

5	IP/Ağ Ekle	IPSec yapılacak yerel ve uzak IP/Ağ adreslerinin eklendiği butondur.
---	-------------------	--



1	Aşama 1 Güvenlik Duvarı Kuralı	Aşama-1 için güvenlik duvarı kuralının yazıldığı butondur.
2	Aşama 2 Güvenlik Duvarı Kuralı	Aşama-2 için güvenlik duvarı kuralının yazıldığı butondur.
3	Aşama 2 No-NAT Kuralı	Aşama-2 için No-NAT kuralının yazıldığı butondur.
4	Kaydet	IPSec Tünel yapılandırılmasının kaydedildiği butondur.
5	Kapat	Ekle butonuna tıklanarak açılan IPSec Tünel penceresinin kapatıldığı butondur.

12.4.2 IKE Profili

IPSec IKE profili, IPSec VPN bağlantılarını yapılandırmak için kullanılır.

IKE, iki nokta arasındaki güvenli iletişim kanallarının kurulmasını sağlamak için kullanılan bir protokoldür.

IKE profili ise IKE iletişimlerinin nasıl gerçekleştirileceğini belirleyen çeşitli parametreler içerir.



1	Ekle	IKE Profilleri ekleme işleminin yapıldığı butondur.
2	İsim	IKE Profillerinin isminin görüntülediği sütundur.

3	Açıklama	IKE Profillerinin açıklamanın görüntülediği sütundur.
4	Anahtar Değişimi	Anahtar değişim protokolünün görüntülediği sütundur. Seçilecek anahtar değişim protokoller IKEv1 ve IKEv2'dir. İki protokolde VPN üzerinden güvenli bağlantı kurmak için kullanılır.
5	Agresif	IKE Profilleri üzerinde agresif modun durumunu gösteren sütundur.
6	Yönet	Eklenmiş olan IKE Profillerinin silindiği veya düzenlendiği sütundur.

-IKE Profili eklemek için 'ekle' butonuna tıklayarak IKE Profili eklenebilir.

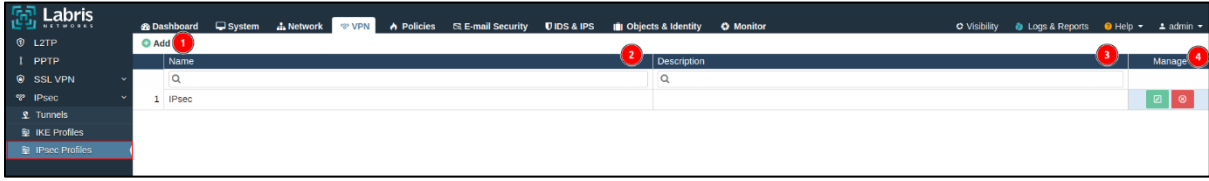
1	İsim	IKE Profilinın isminin girildiği bölümdür.
2	Açıklama	Eklenecek IKE Profilinın açıklaması girilir.
3	Anahtar Değişimi	Eklenecek IKE Profilinın anahtar değişimi protokolü seçilir.
4	Saldırgan Mod	Saldırgan modu açıldığı durumlarda cihazların kimlik doğrulaması ve anahtar değişimini hızlı bir şekilde yaparlar. Saldırgan modun açılması gerektiği durumlarda açılır.

1	Ömür	IKE Profilinin etkin olacağı süre belirlenir.
2	Sistem Varsayılanlarını Kullan	Labris UTM cihazı üzerinden varsayılan olarak gelen ayarları kullanıldığı butondur.
3	Şifreleme/Kimlik Doğrulama	IKE profili için şifreleme ve kimlik doğrulama metodlarının belirttiği bölümdür.
4	Diffie-Hellman Grupları	IKE profili için anahtar değişim protokolünün seçildiği bölümdür.
5	Ölen Eşgörevli Saptaması(DPD)	IKE profili bağlantısında karşı taraftaki cihazın çalışıp çalışmadığını belirlemek için kullanılır.
6	İşlem	DPD ile karşı taraftaki cihaza erişemediği durumlarda yapılması gereken işlem seçilir.
7	Gecikme	IKE haberleşmesindeki gecikme süresi belirtilir.
8	Zaman Aşımı	IKE haberleşmesindeki zaman aşımı süresi belirtilir.
9	Kaydet	IKE Profili ayarlarının kaydedildiği butondur.
10	Kapat	Açılan IKE Profili penceresinin kapatıldığı butondur.

12.4.3 IPsec Profil

IPSec Profili, belirli bir güvenlik ayarlarının anahtar değişim algoritmalarının ve diğer parametrelerini içerir.

IPSec Profili, güvenlik algoritmalarının hangilerinin kullanılacağını, anahtar uzunluklarını, kimlik doğrulama yöntemlerini ve diğer güvenlik parametreleri belirlenir.



1	Ekle	IPSec Profili eklemek için kullanılan butondur.
2	İsim	IPSec Profiline verilen ismin görüntülediği sütündür.
3	Açıklama	IPSec Profiline verilen açıklamanın görüntülediği sütündür.
4	Yönet	IPSec Profilin silindiği veya düzenlendiği bölümdür.

-IPSec Profili eklemek için 'ekle' butonuna tıklayarak IPSec Profili eklenebilir.

1	İsim	IPSec Profiline verilecek ismin girildiği bölümdür.
2	Açıklama	IPSec Profiline verilecek açıklamanın girildiği bölümdür.

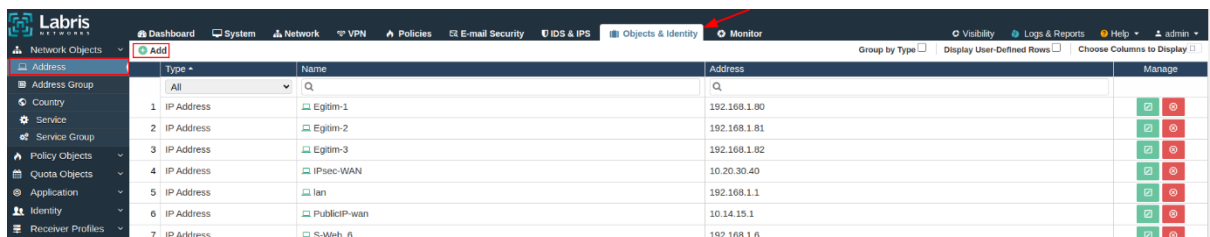
3	Ömür	IPSec Profili teklifinin ömrünün belirtildiği bölümdür.
4	Sistem Varsayılanını Kullan	Sistem varsayılanı olarak Şifreleme / Kimlik Doğrulamalarını kullanılır.
5	Şifreleme / Kimlik Doğrulama	IPSec profili için şifreleme ve kimlik doğrulama metodlarının belirtildiği bölümdür.
6	PFS Grubu(DH)	Diffie-Hellman şifreleme grubunu seçmek için kullanılır.
7	Diffie-Hellman Grupları	IPSec profili için anahtar değişim protokolünün seçildiği bölümdür.
8	Yeniden Anahtarlama	IPSec Profili için yeniden anahtarlamanın açıldığı butondur.
9	Giriş Denemeleri	IPSec Profili teklifi için giriş deneme sayısının belirtildiği bölümdür.
10	Kaydet	IPSec Profili yapılandırılmasının kaydedildiği butondur.
11	Kapat	Açılan IPSec Profili penceresinin kapatıldığı butondur.

Not

IPSec VPN yapılandırılması yapıldıktan sonra Politikalar modülünde kuralların yazılması gerekmektedir.

-IPSec VPN'in Politikalar modülünde kuralının yazılmasının adımları;

1. IPSec VPN konfigürasyonu yapılır.
2. Nesneler ve Kimlikler modülü açılır.



ID	Type	Name	Address
1	IP Address	Eğitim-1	192.168.1.80
2	IP Address	Eğitim-2	192.168.1.81
3	IP Address	Eğitim-3	192.168.1.82
4	IP Address	IPsec-WAN	10.20.30.40
5	IP Address	lan	192.168.1.1
6	IP Address	PublicIP-wan	10.14.15.1
7	IP Address	S-Web_0	192.168.1.6

3. Nesneler ve Kimlikle modülü açıldıktan sonra IPSec VPN için nesnelere oluşturulur. Ekle butonuna tıklanarak nesne eklenir.

Address

Name: Remote_WAN

Description:

Type: IP

IP Address: 10.20.30.40

Owner Group List:

Save Close

IPSec Yapılacak Olan Cihazın Public IP'sini Ekleme

Address

Name: remotelan

Description:

Type: Network

Network Address: 192.168.25.0

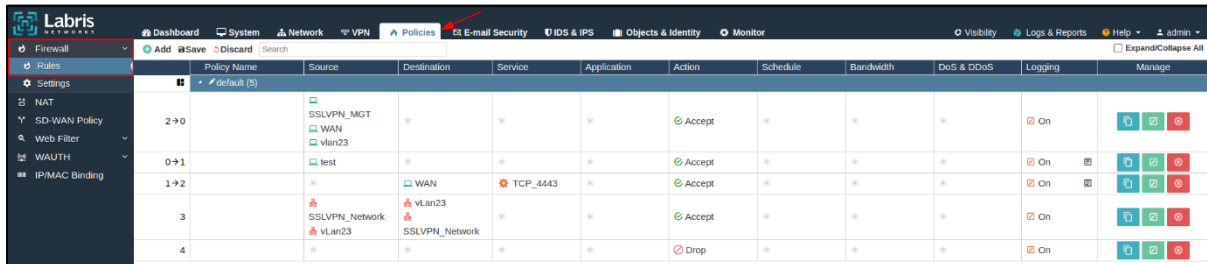
Netmask: 255.255.255.0

Owner Group List:

Ok Close

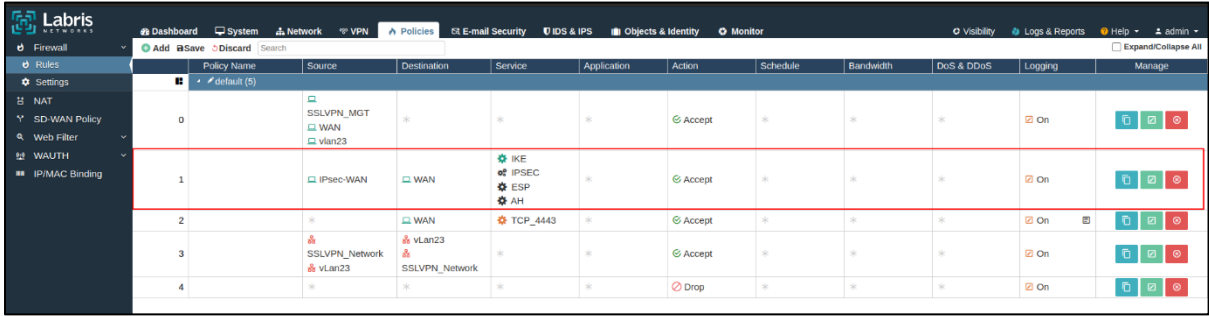
IPSec Yapılacak Olan Cihazın Yerel IP'sini Ekleme

4. Nesneler ve Kimlikler modülünde IPSec VPN için nesnelere eklenir. Nesnelere eklendikten sonra Politikalar modülü açılır.



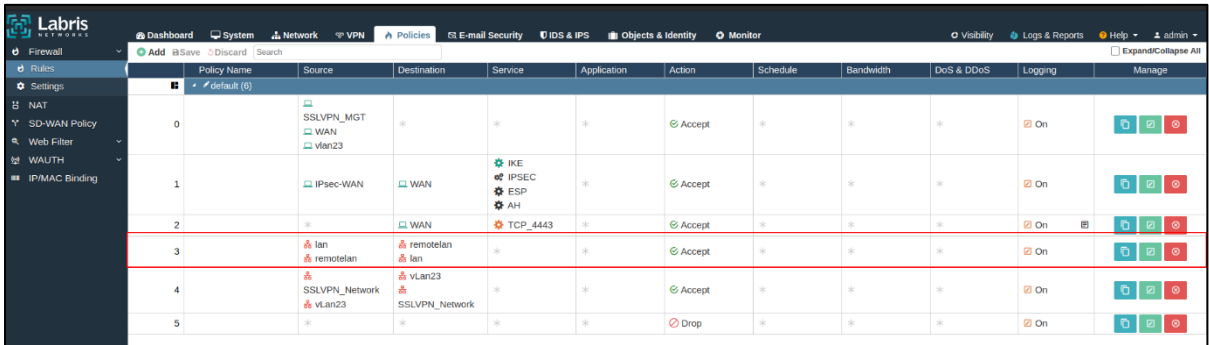
Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
2-0	SSLVPN_MGT WAN vlan23	*	*	*	Accept	*	*	*	On	
0-1	test	*	*	*	Accept	*	*	*	On	
1-2	*	WAN	TCP_4443	*	Accept	*	*	*	On	
3	SSLVPN_Network vlan23	vlan23	*	*	Accept	*	*	*	On	
4	*	SSLVPN_Network	*	*	Drop	*	*	*	On	

5. 0. Kurala SSLVPN arabirim eklendikten sonra 0. ile 1. kural arasına aşağıdaki kuralı yazmak gerekir.



Policy Name	Source	Destination	Service	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
0	SSLVPN_MGT WAN vlan23	*	*	Accept	*	*	*	On	[Edit] [Delete]
1	IPsec-WAN	WAN	IKE IPSEC ESP AH	Accept	*	*	*	On	[Edit] [Delete]
2	*	WAN	TCP_4443	Accept	*	*	*	On	[Edit] [Delete]
3	SSLVPN_Network vLan23	SSLVPN_Network	*	Accept	*	*	*	On	[Edit] [Delete]
4	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

6. Yukarıdaki erişim kuralı yazıldıktan sonra IPsec VPN yapılacak olan karşı taraftaki yerel ağ ile Labris UTM cihazı üzerinde bulan yerel ağın haberleşme kuralını yazmak gerek



Policy Name	Source	Destination	Service	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
0	SSLVPN_MGT WAN vlan23	*	*	Accept	*	*	*	On	[Edit] [Delete]
1	IPsec-WAN	WAN	IKE IPSEC ESP AH	Accept	*	*	*	On	[Edit] [Delete]
2	*	WAN	TCP_4443	Accept	*	*	*	On	[Edit] [Delete]
3	lan remotelan	remotelan lan	*	Accept	*	*	*	On	[Edit] [Delete]
4	SSLVPN_Network vLan23	SSLVPN_Network	*	Accept	*	*	*	On	[Edit] [Delete]
5	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

7. Yukarıdaki tanımlamalar yapıldıktan IPsec VPN erişimini test edebilirsiniz.

13. Politikalar

Politikalar modülünde güvenlik duvarının hangi trafiği engelleyeceğini veya izin verileceğini gibi güvenlik politikalarını tanımlamak için kullanılan bir bileşendir.

Labris UTM cihazı üzerindeki güvenlik duvarı izinlerini veya yönlendirme izinlerinin yazıldığı modüldür.

Labris UTM cihazında politikalar, izin verilebilen veya bir ağda olmayan veri paketlerini analiz ederek geliş ve gidiş trafiğini kontrol eder.

Politikalar menüsünde güvenlik duvarı kuralı, NAT, SD-WAN Kuralları, Web Filtre, WAUTH ve IP/MAC Eşleme modüllerinde kurallar yazılır.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (0)	SSLVPN_MGT WAN vLan23	*	*	*	Accept	*	*	*	On	[Edit] [Delete]
1	IPsec-WAN	WAN	IKE IPSEC ESP AH	*	Accept	*	*	*	On	[Edit] [Delete]
2	*	WAN	TCP_4443	*	Accept	*	*	*	On	[Edit] [Delete]
3	lan remotelan	remotelan lan	*	*	Accept	*	*	*	On	[Edit] [Delete]
4	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	*	*	Accept	*	*	*	On	[Edit] [Delete]
5	*	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

13.1 Güvenlik Duvarı

Güvenlik duvarı modülünde, bir bilgisayar ağı veya bilgisayar sistemini dış tehditlere karşı korumak için kullanılır.

Güvenlik Duvarı, gelen ve giden trafiği Güvenlik Duvarı modülünde yazılan kurallara göre engellenebilir.

Güvenlik Duvarı modülünde, genellikle portlar üzerinden gelen trafiği engelleme veya izin verme, belirli IP adreslerinden gelen trafiği kısıtlama veya engelleme gibi politikalara dayanır.

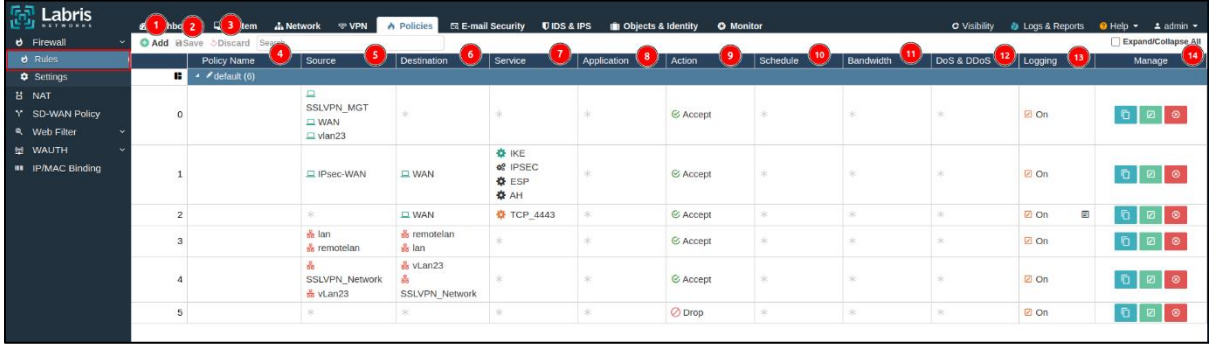
Güvenlik Duvarı, istenmeyen trafiği engelleyen, ağın her iki tarafından da trafiği istenilen şekilde akmasını sağlar.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (0)	SSLVPN_MGT WAN vLan23	*	*	*	Accept	*	*	*	On	[Edit] [Delete]
1	IPsec-WAN	WAN	IKE IPSEC ESP AH	*	Accept	*	*	*	On	[Edit] [Delete]
2	*	WAN	TCP_4443	*	Accept	*	*	*	On	[Edit] [Delete]
3	lan remotelan	remotelan lan	*	*	Accept	*	*	*	On	[Edit] [Delete]
4	SSLVPN_Network vLan23	vLan23 SSLVPN_Network	*	*	Accept	*	*	*	On	[Edit] [Delete]
5	*	*	*	*	Drop	*	*	*	On	[Edit] [Delete]

13.1.1 Kurallar

Labris UTM cihazı üzerine kurallar yazıldığı modüldür. Kaynaktan hedefe doğru gelen trafik kontrol edilir.

Yazılacak kurallar içerisinde kaynak adres, hedef adres, servis, uygulama, işlem, zaman, bant genişliği, DoS&DDoS nesneleri eklenir. Yazılacak kurallar buna göre düzenlenebilir.



1	Ekle	Kural ekleme işleminin yapıldığı butondur.
2	Kaydet	Eklene kuralların kaydedildiği butondur.
3	Vazgeç	Eklenmiş olan kuraldan vazgeçilme işleminin yapıldığı butondur.
4	Politika İsmi	Eklene politikanın isminin görüntülediği sütundur.
5	Kaynak	Kaynak adresin/adreslerinin görüntülediği sütundur.
6	Hedef	Hedef adresin/adreslerinin görüntülediği sütundur.
7	Servis	Kurala eklene servisin görüntülediği sütundur.
8	Uygulama	Kurala eklene uygulamaların görüntülediği sütundur.
9	İşlem	Kurala verilen işlemin görüntülediği yerdir. Bu sütunda izin ver, engelle, reddet veya kayıt tut görüntülenir.
10	Zaman	Kurala zaman tanımlanması yapıldığı ve görüntülediği sütundur.

11	Bant Geniřliđi	Kurala eklenen bant geniřliđi nesneleri görüntülenir.
12	DoS&DDoS	Kurala eklenen DoS&DDoS nesnesinin görüntülendiđi sütundur.
13	Kayıt Tut	Eklenen kuralın kayıt tutulduđu sutündür.
14	Yönet	Eklenen kuralın yönetildiđi, silindiđi veya kopyalandıđı sutündür.

-Güvenlik duvarına kural eklemek için 'ekle' butonuna tıklayarak kural ekleme işlemi yapılır. Ekle butonuna basıldıktan sonra karřımıza gelen ekrandaki bilgileri doldurarak kural ekleme işlemi yapılır.

1	Etkinleřtir	Yazılan kuralın etkinleřtirildiđi butondur.
2	İsim	Eklenecek olan kuralın isminin verildiđi yerdir.
3	Grup	Kuralın ekleneceđi grubun seçildiđi bölümdür.
4	İřlem	Kuralın işleminin belirtildiđi bölümdür.
5	Kaynak	Kaynak adresinin/adreslerinin seçildiđi bölümdür. Seçilecek olan Kaynak adresler Nesnelere ve Kimlikler menüsünde ekli olması gerekir.
6	Hedef	Hedef adresinin/adreslerinin seçildiđi bölümdür.

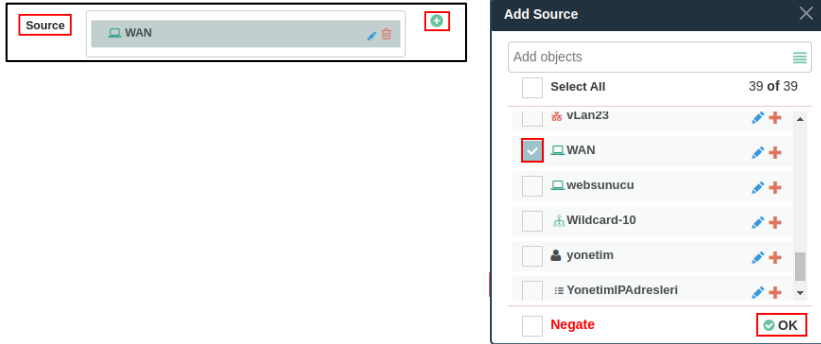
		Seçilecek olan Hedef adresler Nesnelere ve Kimlikler menüsünde ekli olması gerekir.
7	Servis	Kurala eklenecek olan Servislerin(TCP, UDP, IP ve ICMP) seçildiği bölümdür. Eklenecek olan Servislerin Nesnelere ve Kimlikler menüsünde ekli olması gerekir.
8	Uygulama	Kurala eklenecek olan uygulamalar seçilir. Uygulama seçmek için Nesnelere ve Kimlikler menüsünde listeli olması gerekir.
9	Zaman	Kurala eklenecek olan ve kuralın çalışma zamanı seçilir. Zaman nesnesini kurala eklemek için Nesnelere ve Kimlikler menüsünde ekli olması gerekir.
10	Bant Genişliği	Kurala eklenecek Bant Genişliği nesnesi seçilir. Bant Genişliği nesnesini seçmek için Nesnelere ve Kimlikler menüsünde ekli olması gerekir.
11	DoS&DDoS	Kurala eklenecek DoS&DDoS nesnesi seçilir. DoS&DDoS nesnesini kurala eklemek için Nesnelere ve Kimlikler menüsünde ekli olması gerekir.

- Güvenlik duvarında kurallara uygulanacak 4 adet işlem bulunmaktadır. Bunlar; İzin ver, engelle, reddet ve kayıttır.

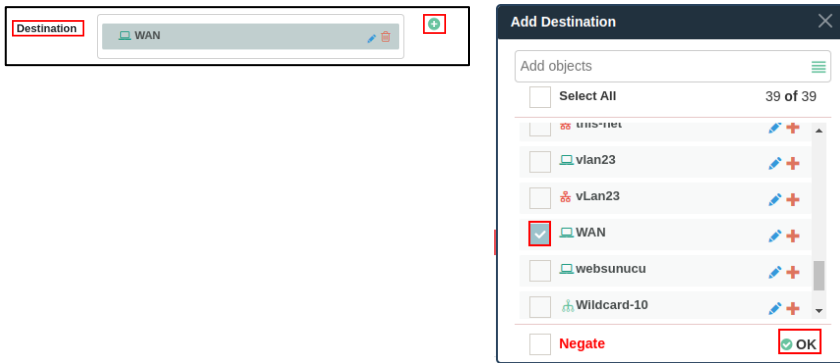


- İzin ver:** Yazılan kurala izin verir. Eğer kurala uyan bir durum olması durumunda kural izinli olarak geçer.
- Engelle:** Yazılan kuralı engelleme işleminin yapıldığı işlemidir. Kurala uyan bir durum olması durumunda engelleme işlemi yapar.
- Reddet:** Yazılan kuralı engeller fakat geri dönüş paketi yollamaz.
- Kayıt:** Bant genişliği kuralında kullanılır.

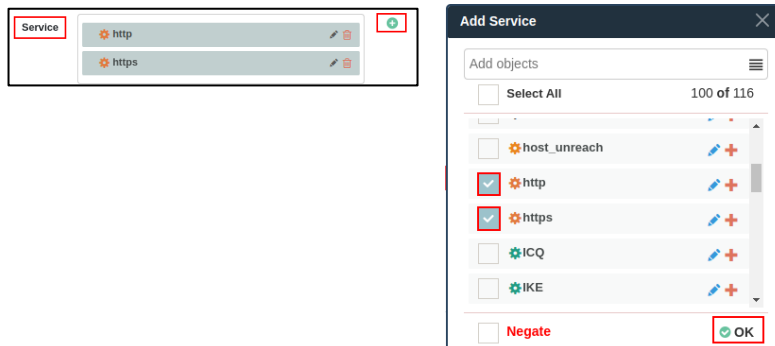
-Kurala Kaynak Adresi eklemek için Kaynak yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimliklere menüsünde eklenen nesne veya kimlik eklenir.



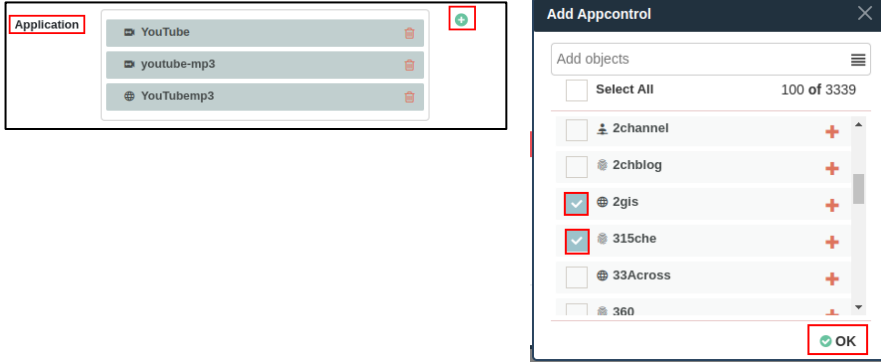
-Kurala Hedef Adresi eklemek için Hedef yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimliklere menüsünde eklenen nesne veya kimlik eklenir.



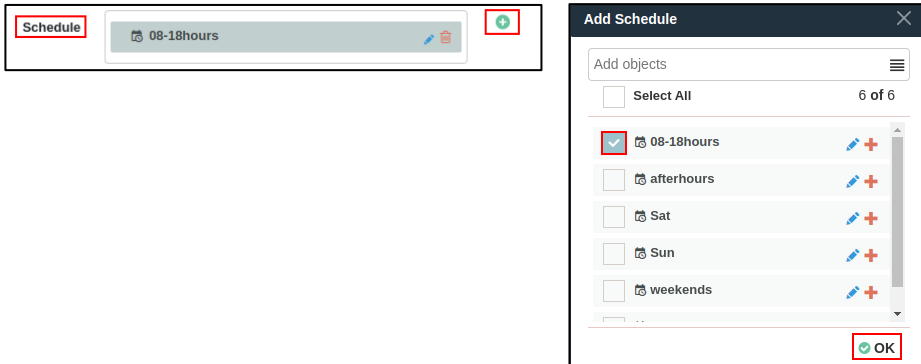
-Yazılacak olan kurala servis eklemek için Servis yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimliklere menüsünde eklenen servis objeleri eklenir.



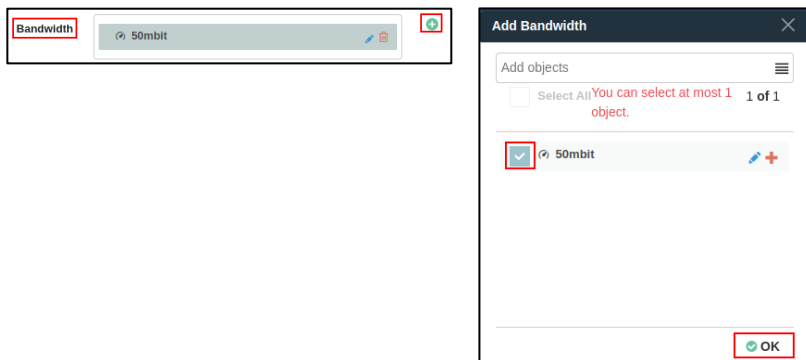
-Yazılacak olan kurala uygulama eklemek için Uygulama yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan uygulamaların seçilmesinin yanından uygulama gruplarını da kurala eklenebilir.



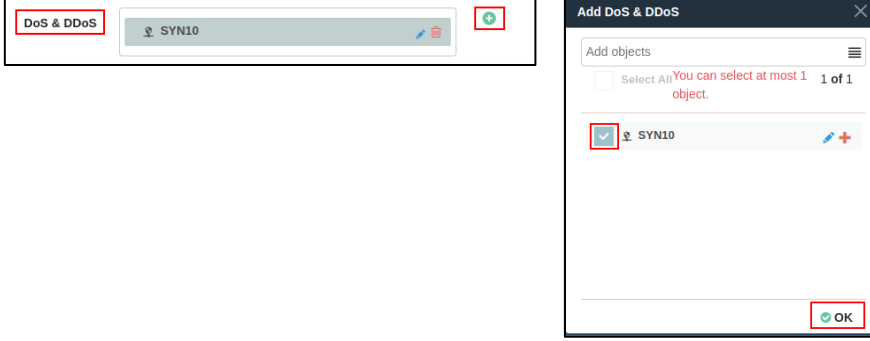
-Yazılacak olan kurala zaman eklemek için Zaman yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan veya Nesnelere ve Kimlikler modülünde eklenen zaman nesneleri seçilerek kurala eklenir.



-Yazılacak olan kurala zaman nesnesi eklemek için Zaman yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan veya Nesnelere ve Kimlikler modülünde eklenen zaman nesneleri seçilerek kurala eklenir.



-Yazılacak olan kurala DDoS nesnesi eklemek için DDoS yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan veya Nesneler ve Kimlikler modülünde eklenen DDoS nesneleri seçilerek kurala eklenir.



Not

Güvenlik Duvarı kuralı eklendikten sonra kuralın etkin olabilmesi için Kaydet butonuna basılmalıdır.

Advanced

- 1 Severity: INFO
- 2 Reject With: ICMP port unreachable
- 3 Stateful Inspection:
- 4 Log Forwarding:
- 5 IDS Policy: None

1	Kayıt Düzeyi	Kuralın kayıt düzeyinin belirtildiği bölümdür.
2	Bununla Reddet	Kuralın reddetme tipinin belirtildiği bölümdür.
3	Durum Denetimi	Kuralın durum denetiminin açıldığı bölümdür.
4	Kayıt Yönlendirme	Kuralın kaydının gönderileceği Syslog sunucusunun seçilir.

5	Saldırı Tespit Sistemi Politikası	IDS politikasının seçilir.
---	--	----------------------------

13.1.2 Ayarlar

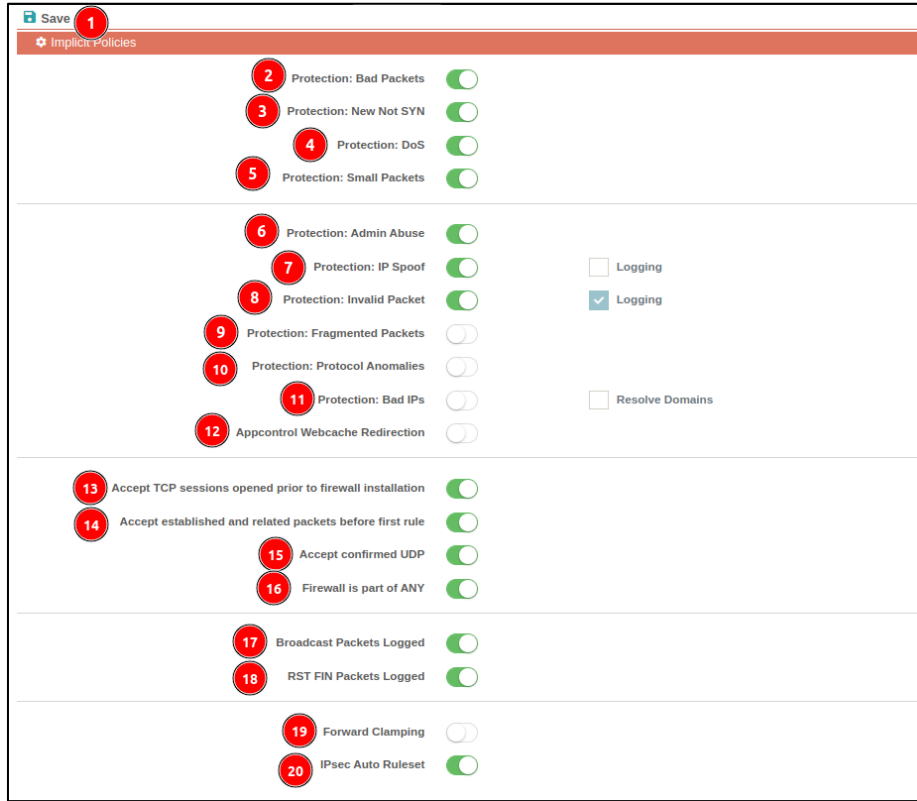
Güvenlik duvarı ayarlarının yapıldığı modüldür. Bu modülde dolaylı politikalar, koruma portu tarayıcı, saldırı kontrolü ve ssh incelemesi yapılır.

The screenshot shows the Labris Networks UTM Settings page for Implicit Policies. The interface includes a top navigation bar with tabs for Dashboard, System, Network, VPN, Policies (selected), E-mail Security, IDS & IPS, Objects & Identity, and Monitor. A left sidebar contains a menu with options: Firewall, Rules, Settings (selected), NAT, SD-WAN Policy, Web Filter, WAUTH, and IP/MAC Binding. The main content area is titled 'Implicit Policies' and features a 'Save' button. The settings are organized into several sections, each with a list of policies and their corresponding toggle switches. The 'Logging' checkbox is checked for 'Protection: Invalid Packet'. The 'Resolve Domains' checkbox is unchecked for 'Protection: Bad IPs'. The 'Appcontrol Webcache Redirection' toggle is also unchecked.

Policy Name	Toggle State	Logging	Resolve Domains
Protection: Bad Packets	On		
Protection: New Not SYN	On		
Protection: DoS	On		
Protection: Small Packets	On		
Protection: Admin Abuse	On		
Protection: IP Spoof	On	<input type="checkbox"/>	
Protection: Invalid Packet	On	<input checked="" type="checkbox"/>	
Protection: Fragmented Packets	Off		
Protection: Protocol Anomalies	Off		
Protection: Bad IPs	Off		<input type="checkbox"/>
Appcontrol Webcache Redirection	Off		
Accept TCP sessions opened prior to firewall installation	On		
Accept established and related packets before first rule	On		
Accept confirmed UDP	On		
Firewall is part of ANY	On		
Broadcast Packets Logged	On		
RST FIN Packets Logged	On		

13.1.2.1 Dolaylı Politikalar

Dolaylı Politikalar, güvenlik duvarında belirlenen kurallar gibi doğrudan müdahale etmek yerine, genellikle daha uzun vadeli ve kapsamlı politikaların belirlendiği bölümdür.



1	Kaydet	Ayarlar modülünde yapılan değişikliklerin kaydedildiği butondur.
2	Kötü Paket Koruması	Kötü paketlerin tespit edilip engellemek için kullanılan bir özelliktir.
3	Koruma: Yeni Oturumda SYN Olmayan Paketler	3' lü el sıkışmanın yapılmadı durumlarda engelleme yapan bir özelliktir.
4	Koruma: DoS	DoS olarak tanımladığı isteklerin yasaklama işlemini yapan özelliktir.
5	Koruma: Küçük Paketler	Küçük boyutlu paketlerin yasaklama işleminin yapıldığı özelliktir.

6	Koruma: Yönetim Erişimi Kötüye Kullanma	Yönetim erişimi verilen kullanıcının ağ üzerindeki trafiğini kontrol ederek erişim yetkisini kötüye kullanmayı engelleyen bir özelliktir.
7	Koruma: Sahte IP	Sahte IP adreslerine karşı koruma sağlayan bir özelliktir.
8	Koruma: Geçersiz Paket	Geçersiz olarak algılanan paketlerinden koruma sağlayan bir özelliktir.
9	Koruma: Parçalanmış Paketler	Parçalanmış IP paketlerinden koruma sağlayan bir özelliktir.
10	Koruma: Protokol Bozuklukları	Ağ trafiğindeki protokollerin standard olmayan bir trafik olması durumunda koruma sağlayan özelliktir.
11	Koruma: Kötü IP Adresleri	Ağ trafiğindeki IP adreslerini denetleyen özelliktir.
12	Uygulama Kontrolü Web Önbellek Yönlendirmesi	Uygulama kontrolü kuralına takılan istemciler için önbelleğe yönlendirme yapmasını sağlayan özelliktir.
13	Güvenlik duvarı kurulmadan önce açılmış olan TCP oturumlarını kabul et	Güvenlik duvarında yapılan değişikliklerin kaydedildiği sırada önceden açılan TCP oturumlarını kabul etmesini sağlayan özelliktir.
14	Kurulmuş bağlantılar ve ilgili paketlerini ilk kuraldan önce kabul et	Kurulmuş bağlantılar ve ilgili paketlerini ilk kuraldan önce kabul etmesini sağlayan özelliktir.
15	Doğrulanmış UDP erişimini kabul et	Doğrulan UDP bağlantılarını kabul eden özelliktir.

16	Güvenlik duvarını ANY'nin bir parçası olarak kabul et	Güvenlik duvarının ANY'nin bir parçası olarak kabul edildiği özelliktir.
17	Broadcast Paketlerini Kayıt Tut	Broadcast paketlerinin kayıt tutan özelliktir.
18	RST FIN Paketlerini Kayıt Tut	RST ve FIN paketlerinin kaydını tutan özelliktir.
19	İleri Kenetlenme	İleri kenetlenmenin açıldığı bölümdür.
20	IPsec Otomatik Kural Belirleme	IPsec için otomatik Kural belirleyen özelliktir.

13.1.2.2 Koruma Portu Tarayıcı

Labris UTM, ağ trafiğini izleyerek bir IP adresinden farklı portlarına gelen istekleri engelleyen bölümdür.

The screenshot shows the 'Protection Port Scanner' configuration page. It includes the following elements:

- 1 Enable:** A green toggle switch is turned on.
- 2 Rate:** A text input field containing the number '10'.
- 3 Timeout:** A text input field containing '30' with a 'seconds' label and a dropdown arrow.
- 4 Excluded Interfaces:** An empty text input field.
- 5 Whitelist IPs:** An empty text input field with a green plus icon to its right.

1	Etkinleştir	Koruma portu tarayıcısının etkinleştirildiği butondur.
2	Hız(Oran)	IP adresinden gelen toplam istek sayısı belirtilir.
3	Zaman Aşımı	Orana takılan IP adresinin yasaklandığı süre(sn) belirtilir.
4	Dahil Edilmemiş Arayüzler	Korumaya dahil olmayacak arayüzün seçilir.
5	Beyaz Liste IP'leri	Korumaya dahil olmayacak IP adresleri seçilir.

13.1.2.3 Saldırı Kontrolü

Ağ trafiğiniz izleyerek saldırı kontrolünün yapıldığı bölümdür.

1	Etkinleştir	Saldırı kontrolünün etkinleştirildiği butondur.
2	Vekil Sunucu(Proxy) Trafiği Büyüklüğü	IP adresinden gelen toplam istek sayısı belirtilir.
3	HTTP Trafiği	HTTP trafiğinin saniyedeki bağlantı değerinin girildiği bölümdür.
4	Hedef Trafiği Büyüklüğü	Hedef trafiğin büyüklük değeri girilir.
5	İstemci Trafiği Büyüklüğü	İstemcinin yarattığı trafiğin büyüklük değeri girilir.
6	TCP Bağlantı Sınırı	TCP bağlantı sınırının değeri girilir.
7	Vekil Sunucu(Proxy) TCP Bağlantı Sınırı	Vekil sunucunun TCP bağlantı sınırının değeri girilir.
8	Dahil Edilmemiş Adres	Saldırı korumasına dahil edilmeyecek adres veya adresler girilir.
9	Vekil Sunucu(Proxy) Atılımı	Vekil Sunucu atılım değeri girilir.

10	HTTP Atılımı	HTTP atılım değeri girilir.
11	Hedef Atılımı	Hedef atılım değeri girilir.
12	İstemci Atılımı	İstemci atılım değeri girilir.

13.2 NAT

NAT, bir ağ üzerindeki cihazların özel IP adreslerinin(192.168.x.x veya 10.x.x.x gibi) genel, yani internete erişebilir IP adresleriyle değiştirir.

NAT, aynı ağ içerisinde bulunan birden fazla cihazın aynı genel IP'yi kullanarak internete erişebilmesini sağlar.

Policy Name	Source	Destination	Service	Translated	Service	Manage
default (2)			http	lan	Labris Webfilter	
HTTP_Filter	lan	*	http	lan	Labris Webfilter	
HTTPS_Filter	lan	*	https	lan	Labris SSL Proxy	

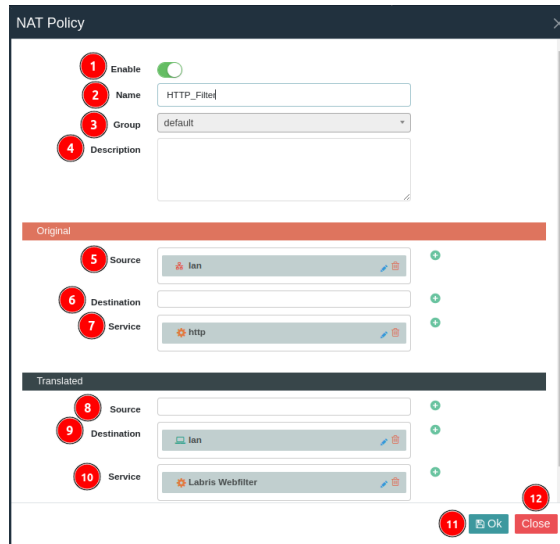
-NAT modülünde bulunan tablonun açıklaması ve NAT kuralının yazılımı;

Policy Name	Source	Destination	Service	Translated	Service	Manage
default (2)			http	lan	Labris Webfilter	
HTTP_Filter	lan	*	http	lan	Labris Webfilter	
HTTPS_Filter	lan	*	https	lan	Labris SSL Proxy	

1	Ekle	NAT kural ekleme işleminin yapıldığı butondur.
2	Kaydet	Eklene NAT kuralların kaydedildiği butondur.
3	Vazgeç	Eklenmiş olan NAT kuralından vazgeçilme işleminin yapıldığı butondur.
4	Ara	Eklene kuralda arama yapılan bölümdür.
5	Politika İsmi	Eklene NAT kuralının isminin görüntülediği sütundur.
6	Orjinal Kaynak	Kurala eklene Orjinal kaynak adresin/adreslerinin görüntülediği sütundur.
7	Orjinal Hedef	Kurala eklene Orjinal hedef adresin/adreslerinin

		görüntülediği sütundur.
8	Orjinal Servis	Kurala eklenen orjinal servisin görüntülediği sütundur.
9	Değişen Kaynak	Kurala eklenen Değişen kaynak adresin/adreslerinin görüntülediği sütundur.
10	Değişen Hedef	Kurala eklenen Değişen hedef adresin/adreslerinin görüntülediği sütundur.
11	Değişen Servis	Kurala eklenen Değişen servis adresin/adreslerinin görüntülediği sütundur.
12	Yönet	Yazılan kuralın düzenlendiği, kopyalandığı veya silindiği bölümdür.

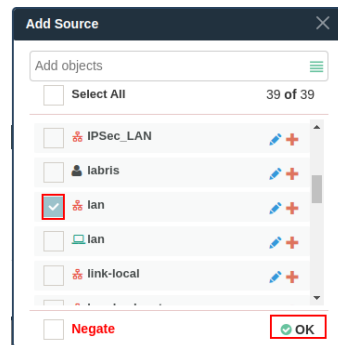
-NAT kuralı ekleme için 'ekle' butonuna tıklanarak karşımıza gelen ekrandaki bilgileri doldurarak Kural ekleme işlemi yapılır.



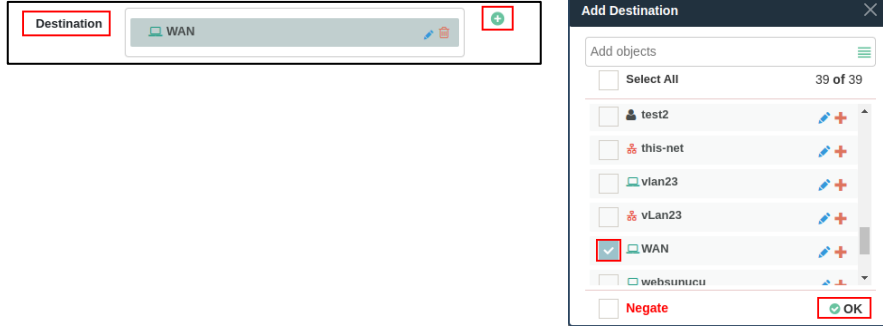
1	Etkinleştir	Yazılacak NAT kuralının etkinleştirildiği butondur.
2	İsim	Eklenecek NAT kuralına verilecek isim girilir.
3	Grup	Eklenecek olan NAT kuralının grubu seçilir.
4	Açıklama	Eklenecek olan NAT kuralının açıklaması girilir.

5	Orjinal Kaynak	Orjinal kaynak adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan Kaynak adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
6	Orjinal Hedef	Orjinal hedef adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan hedef adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
7	Orjinal Servis	Orjinal servis adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan servis adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
8	Değişen Kaynak	Değişen kaynak adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan Kaynak adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
9	Değişen Hedef	Değişen hedef adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan hedef adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
10	Değişen Servis	Orjinal servis adresinin/adreslerinin seçildiği bölümdür. Seçilecek olan servis adresler Nesneler ve Kimlikler menüsünde ekli olması gerekir.
11	Ekle	Yazılan NAT kuralının kaydedildiği butondur.
12	Kapat	Ekle butonuna tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

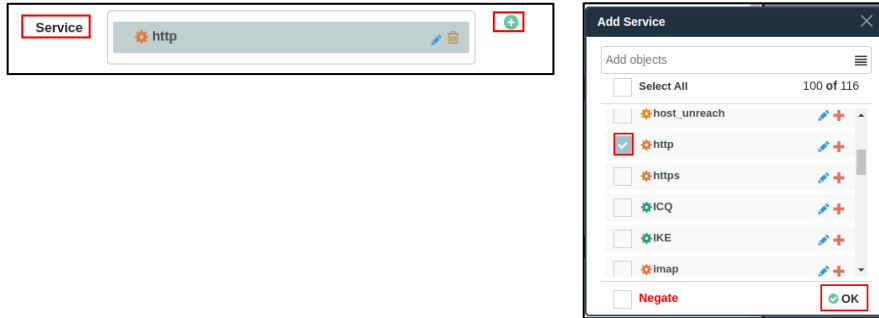
-NAT kuralına Orjinal kaynak Adresi eklemek için Kaynak yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesneler ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



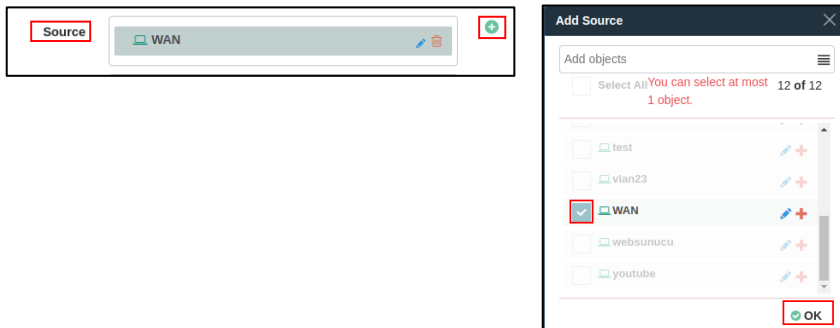
-NAT kuralına Orjinal hedef Adresi eklemek için Hedef yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



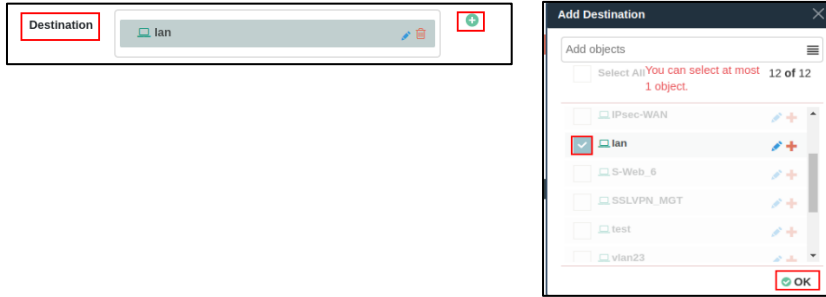
-NAT kuralına Orjinal servis Adresi eklemek için Servis yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



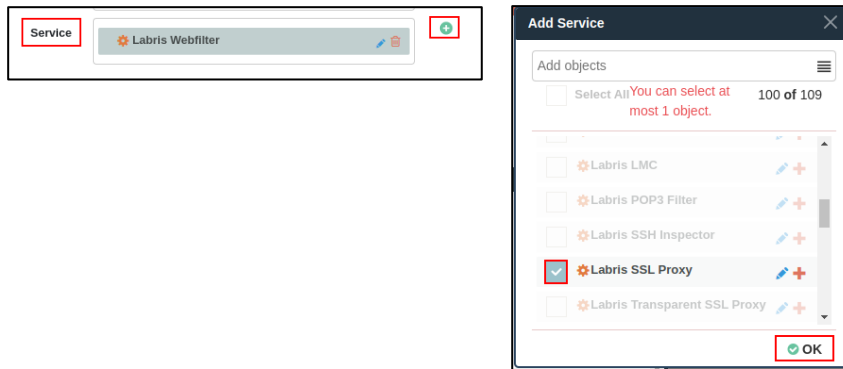
-NAT kuralına Değişen kaynak Adresi eklemek için Kaynak yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesnelere ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



-NAT kuralına Değişen hedef Adresi eklemek için Hedef yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesneler ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



-NAT kuralına Değişen servis eklemek için Servis yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda Nesneler ve Kimlikler menüsünde eklenen nesne veya kimlik eklenir.



Not

NAT kuralı eklendikten sonra kuralın etkin olabilmesi için Kaydet butonuna basılmalıdır.

-Labris UTM cihazı üzerinde HTTP ve HTTPS filtreleme kuralları aşağıdaki gibi yazılır. Bu kuralların yazılmasının amacı ise Web Filtre modülünde engellenecek olan sitelerin engellenmesini sağlamaktır. Eğer HTTP filtreleme kuralı var ise HTTP sitelerini denetlenebilir. HTTPS bir filtreleme var ise Labris UTM cihazı içerisinde bulunan sertifikanın istemcilere yüklenmesi gerekir. Bu sayede HTTPS siteleri üzerinde Web Filtre modülünde Kural yazılır.

	Policy Name	Original			Translated			Manage
		Source	Destination	Service	Source	Destination	Service	
0	default (2)	lan	*	http	lan	lan	Labris Webfilter	  
1		lan	*	https	lan	lan	Labris SSL Proxy	  

-Örnek1: İçerideki Web Sunucusuna erişimi için NAT ve Güvenlik Duvarı kurallarının yazımı;

NAT Kuralı;

Policy Name	Original			Translated			Manage
	Source	Destination	Service	Source	Destination	Service	
0	*	WAN	https http	*	Server_16	*	

Genel Politika;

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
0	*	Server_16	https http	*	Accept	*	*	*	On	

-Örnek-1 için yukarı NAT ve Genel Politikada kuralların yazılması gerekir.

Not

Nat ve Genel Politikada yazılan kurallarda * olarak görülen yerler herhangi anlamına gelmektedir. Örnek-1'i incelediğimizde kaynak kısmının * olarak görmekteyiz. Bu NAT kuralı herhangi bir kaynaktan dış hattına gelen http(80) ve https(443) isteklerini web sunucusuna yönlendir şeklinde okuyabiliriz.

Not

Yazılacak NAT ve Genel Politika kurallarındaki sırala önemlidir.Yazılan kurallar yukarıdan aşağıya doğru sırayla okunur.

13.3 SD-WAN Kuralları

Ağ menüsünde eklenen Ağ Geçitlerine kuralların yazıldığı modüldür.

Ekle	Kaydet	Vazgeç	Ara	VPN	Politikalar	E-posta Güvenliği	IDS & IPS	Nesneler ve Kimlik	İzleme	Trafik Analizi	Kayıtlar & Raporlar	Yardım	admin
		Politika İsmi	Kaynak	Hedef	Ağ Geçidi	Yedek Ağ Geçidi	Yönet						
0	websunucu	websunucu	0.0.0.0	adsl-2									
1	lan	lan	0.0.0.0	adsl-1	adsl-2								
2	default	0.0.0.0	0.0.0.0	default									

İki ve üzeri dış hattının olması durumunda kullanılır. Bu modülde ise kaynak adresinden hedef adresine giderken hangi hattı kullanacağını kuralı yazılır. Yazılan kurala yedek hat eklemesi de yapılır.

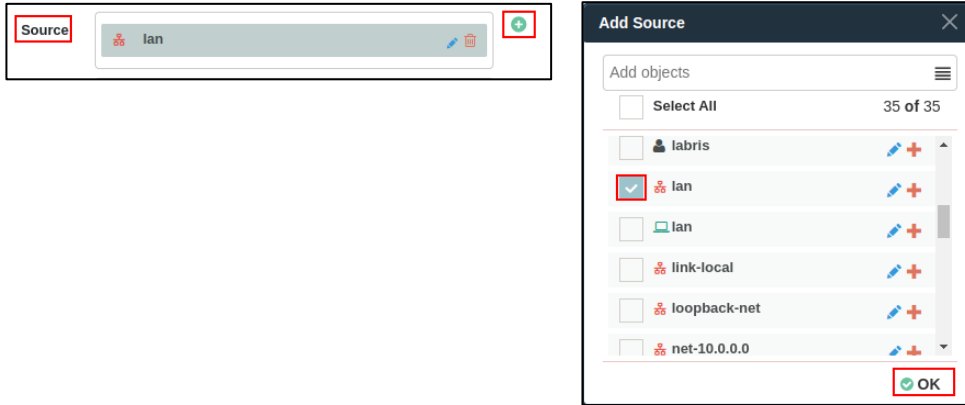
1	2	3	4	5	6	7	8	9	10
		Politika İsmi	Kaynak	Hedef	Ağ Geçidi	Yedek Ağ Geçidi	Yönet		
0	websunucu	websunucu	0.0.0.0	adsl-2					
1	lan	lan	0.0.0.0	adsl-1	adsl-2				
2	default	0.0.0.0	0.0.0.0	default					

1	Ekle	SD-WAN politikası eklenen butondur.
2	Kaydet	SD-WAN Politikasındaki yapılan değişikliklerin kaydedildiği butondur.
3	Vazgeç	SD-WAN Politikasındaki yapılan değişikliklerden vazgeçildiği butondur.
4	Ara	SD-WAN Politikasında arama yapılan yerdir.
5	Politika İsmi	SD-WAN Politikasına verilen isim görüntülenir.
6	Kaynak	Kaynak adreslerin görüntülediği bölümdür.
7	Hedef	Hedef adreslerin görüntülediği bölümdür.
8	Ağ Geçidi	Seçilen ağ geçidinin görüntülediği bölümdür.
9	Yedek Ağ Geçidi	Yedek olarak seçilen ağ geçidinin görüntülediği bölümdür.
10	Yönet	Eklenen SD-WAN Politikalarının düzenlendiği, silindiği veya koptandığı bölümdür.

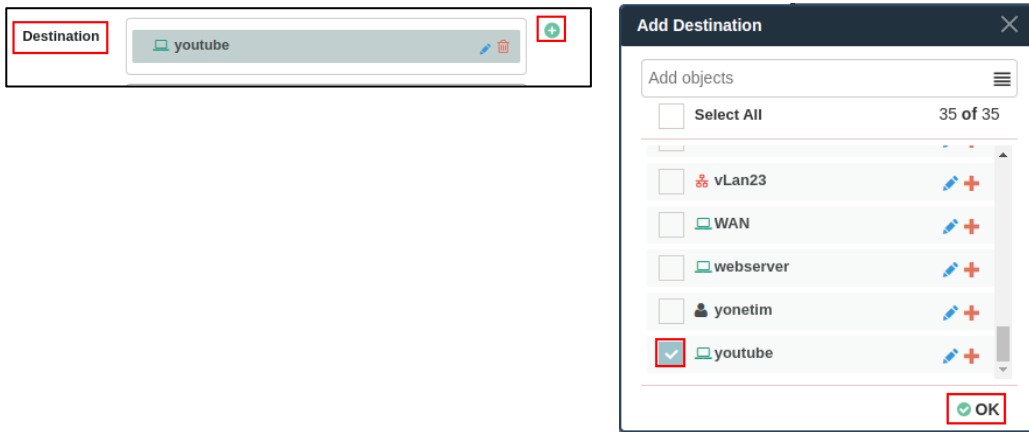
-SD-WAN Politikası ekleme için 'ekle' butonuna tıklayarak SD-WAN politikası eklenir. 'ekle' butonuna basıldıktan sonra karşımıza gelen ekrandaki bilgiler doldurarak SD-WAN Politikası yazılır.

1	Ekle	SD-WAN politikası eklenen butondur.
2	Kaydet	SD-WAN Politikasındaki yapılan değişikliklerin kaydedildiği butondur.
3	Vazgeç	SD-WAN Politikasındaki yapılan değişikliklerden vazgeçildiği butondur.
4	Ara	SD-WAN Politikasında arama yapılan yerdir.
5	Politika İsmi	SD-WAN Politikasına verilen isim görüntülenir.
6	Kaynak	Kaynak adreslerin görüntülendiği bölümdür.
7	Hedef	Hedef adreslerin görüntülendiği bölümdür.
8	Ağ Geçidi	Seçilen ağ geçidinin görüntülendiği bölümdür.
9	Yedek Ağ Geçidi	Yedek olarak seçilen ağ geçidinin görüntülendiği bölümdür.
10	Yönet	Eklenen SD-WAN Politikalarının düzenlendiği, silindiği veya koptandığı bölümdür.

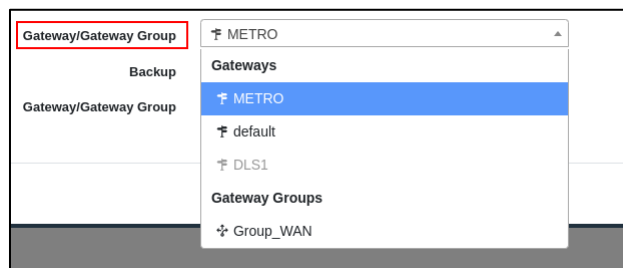
-Yazılacak olan kurala SD-WAN politikasına kaynak adres eklemek için Kaynak yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan veya Nesnelere ve Kimliklere modülünde eklenen adres veya adresler seçilerek kurala eklenir.



-Yazılacak olan kurala SD-WAN politikasına hedef adres eklemek için Hedef yazılı olan yerdeki '+' ifadesine tıklanır. Tıkladıktan sonra gelen ekranda veritabanında bulunan veya Nesnelere ve Kimliklere modülünde eklenen adres veya adresler seçilerek kurala eklenir.



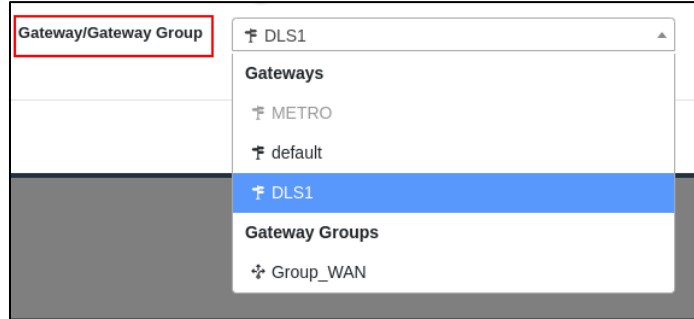
-Yazılacak olan kurala SD-WAN politikasına ağ geçidi veya ağ geçidi grubu eklemek için '+' ifadesine tıklanır. Tıkladıktan sonra Ağ>SDWAN>Ağ Geçitlerinde eklenen ağ geçitleri veya ağ geçidi grupları seçilir.



-Yazılacak olan kural için eklenen ağ geçidinin yanında yedek olarak başka bir hat eklemek için Yedek butonunun aktifleştirilmesi gerekir.



-Yedek hat butonu aktif edildikten sonra yedek olacak hattı seçmek gerekir.

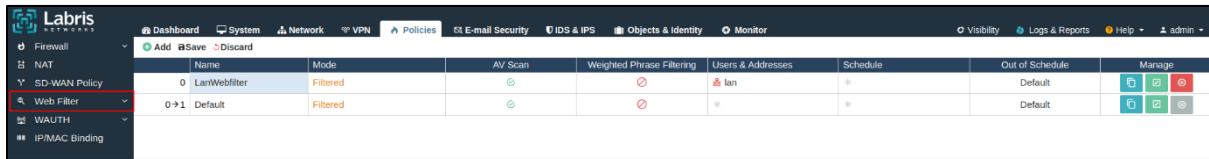


13.4 Web Filtre

Web Filtre, ağdaki web trafiğini denetlemek ve filtrelemek için kullanılır.

Kullanıcıların belirli web sitelerine erişimini kontrol etmeye ve belirli içerik kategorilerini engellemeye olanak sağlar. Bu sayede, ağa zararlı içeriklerin girmesi engellenir ve belirli web sitelerine erişimi kısıtlayarak güvenlik sağlar.

Labris UTM cihazında NAT modülüne HTTP ve HTTPS kuralları eklendikten sonra Web Filtre modülü düzenlenir.



Name	Mode	AV Scan	Weighted Phrase Filtering	Users & Addresses	Schedule	Out of Schedule	Manage
LanWebfilter	Filtered			lan	*	Default	
Web Filter	0+1 Default			*	*	Default	

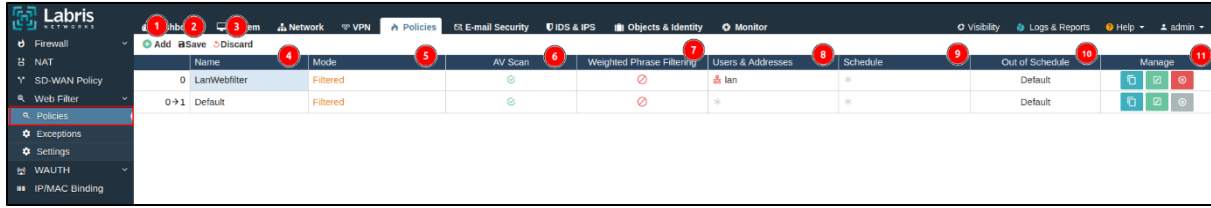
Not

HTTP kuralı yazılması durumunda Web Filtre modülünde sadece HTTP siteler üzerinde kurallar yazılır.

HTTPS kuralının yazılması durumunda ise SSL sertifikaların cihazlara yüklendikten sonra HTTPS siteler üzerinde de kuralları yazılabilir.

13.4.1 Politikalar

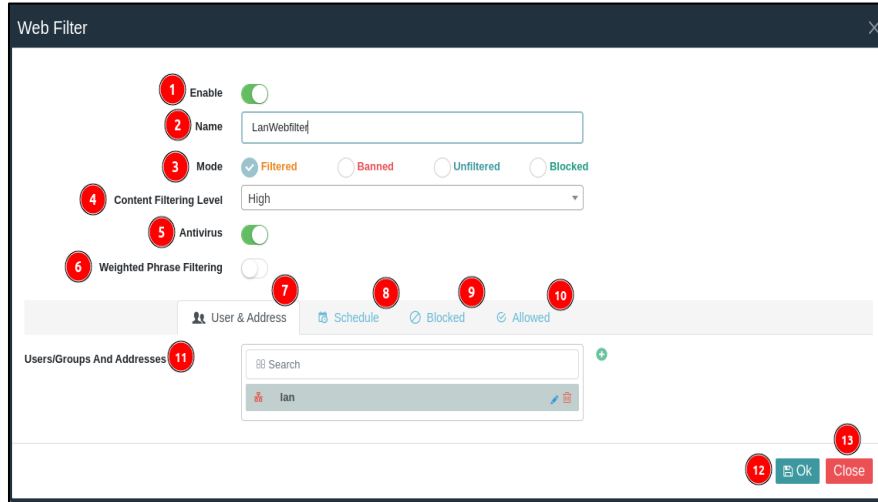
HTTP ve HTTPS filtreleme kuralları yazıldıktan sonra Web Filtre kuralları düzenlenir. Kullanıcı, cihaz, ağ adresi bazlı kurallar yazılabilir ve topolojinize göre düzenlenebilir.



1	Ekle	Web Filtre politikası eklenen butondur.
2	Kaydet	Web Filtre politikasında yapılan değişikliklerin kaydedildiği butondur.
3	Vazgeç	Web Filtre politikasında yapılan değişikliklerden vazgeçildiği butondur.
4	İsim	Eklenen Web Filtre politikalarının ismi görüntülenir.
5	Mod	Eklenen Web Filtre politikalarının Modu görüntülenir.
6	Antivirüs Taraması	Eklenmiş olan Web Filtre politikalarının Antivirüs Taramasının açık veya kapalı olma durumları görüntülenir.
7	Ağırlıklı İfade Filtreleme	Eklenmiş olan Web Filtre politikalarının Ağırlıklı İfade Filtrelemenin açık veya kapalı olma durumları görüntülenir.
8	Kullanıcılar ve Adresler	Web Filtre politikalarına eklenen kullanıcıların ve adresleri görüntülenir.
9	Zaman	Web Filtrede yazılan kuralın çalışma zamanı görüntülenir.
10	Zamanlama Dışı	Çalışma zamanının dışında hangi kuralın devrede olduğu görüntülenir.
11	Yönet	Web Filtre kuralının kopyalandığı, düzenlendiği veya

		kuralın silindiği bölümdür.
--	--	-----------------------------

-Politika eklemek için 'ekle' butonuna tıklayarak Web Filtre politikası eklenbilir. Ekle butonuna basıldıktan sonra karşımıza gelen ekrandaki bilgileri doldurarak Web Filtre kuralı eklenebilir.



1	Etkinleştir	Web Filtre politikası etkinleştirildiği butondur
2	İsim	Web Filtre politikasının ismi girilir.
3	Mod	Web Filtre politikasının modu seçilir.
4	İçerik Filtreleme Seviyesi	Web Filtre politikasının içerik filtreleme seviyesi belirtilir.
5	Antivirüs	Web Filtre politikasında antivirüs modunun açıldığı butondur.
6	Ağırlıklı İfade Filtreleme	Web Filtre politikasında ağırlıklı ifade filtreleme modunun açıldığı butondur.
7	Kullanıcı&Adres	Web Filtre politikasının uygulanacağı kullanıcı ve adreslerin seçilir.
8	Zaman	Web Filtre politikasının etkin olacağı zaman belirtilir.
9	Engelli	Web Filtre politikasında engellenecek alan adlarını,

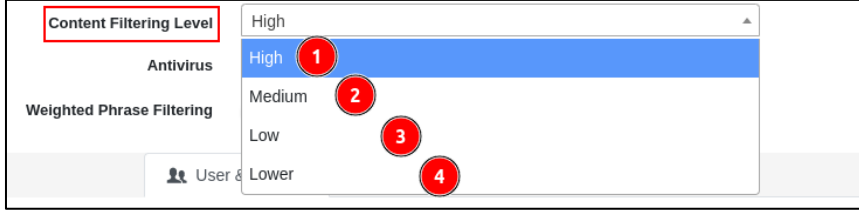
		URL, uzantıları, uygulama tiplerini, düzenli ifadeleri, içerikleri engellenebilir.
10	İzinli	Web Filtre politikasında izinli alan adlarını, URL ve içeriklere izin verilir.
11	Kullanıcılar/Grupları ve Adresler	Web Filtre politikasına kullanıcı ve adres ekleme işlemi yapılır.
12	Kaydet	Web Filtre politikasının kaydedildiği butondur.
13	Kapat	'ekle' butonuna tıkladıktan sonra açılan Web Filtre politikası ekranının kapatıldığı butondur.

-Web Filtre politikası yazmak için filtre Mod seçilmesi gerekir. Seçilen her modun görevi farklıdır.



1	Filtreli	Web Filtre politikasını engelli ve izinli bölümleri kullanılır. Bu mod aktif ise Engelli ve İzinli bölümleri aktiftir.
2	Yasaklı	Engelli ve izinli bölümleri kullanılamaz. Bütün siteler yasaklıdır. Bu mod aktif ise Engelli ve İzinli bölümleri pasiftir.
3	Filtresiz	Engelle ve izinli bölümleri kullanılamaz. Kullanıcılar web filtre politikasına takılmadan filtresiz olarak internet kullanır. Bu mod aktif ise Engelli ve İzinli bölümleri pasiftir.
4	Engelli	Engelli bölümündeki kategorilerden tamamını seçilidir. İzinli bölümüne eklenen siteler dışında bütün siteler veya kategoriler engellidir.

-İçerik filtreleme seviyesi, kullanıcıların erişimine izin veren veya engellenen içerik türlerini belirlemek için kullanılır. Labris UTM cihazında 'daha düşük, düşük, orta ve yüksek' olmak üzere 4 adet içerik filtreleme seviyesi bulunur.



1	Yüksek	En kısıtlayıcı filtreleme seviyesidir. İçerik filtreleme seviyesinin yüksek seçilmesi durumunda yetişkin içeriklerine, şiddet içeren içeriklere, kumar siteleri vb. kötü amaçlı içerikleri engellenir.
2	Orta	İçerik filtreleme seviyesinin orta seviyesi seçilmesi durumunda yetişkin içeriklerini ve şiddet içeren içerikleri engellerken, bazı kategorilerdeki içeriklere daha geniş bir erişim sağlar.
3	Düşük	Düşük seviye seçildiğinde genellikle çocuklar veya hassas kullanıcılar için düzenlenmiştir. Yetişkin içerikleri, şiddet içeren içerikleri ve kumar gibi belirli kategorileri engeller.
4	Daha Düşük	En az kısıtlayıcı filtreleme seviyesidir. Filtreleme seviyesi daha az kısıtlayıcı ve kullanıcıların daha çeşitli içeriklerine erişmesine izin verir.

-Anti Virüs etkinleştirildiği takdirde Virüslü olarak sayılan sitelere erişimi denetleyerek engeller.



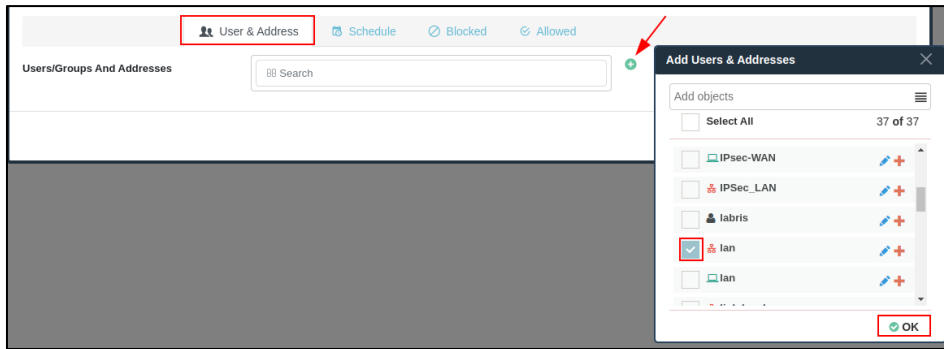
-Ağırlıklı İfade Filtreleme, belirli anahtar kelimelerin veya ifadelerin önemini belirlemek için ağırlıklandırma yöntemlerini kullanılır. Belirli bir anahtar kelimenin veya ifadenin bir tehdit oluşturup oluşturmadığına veya izin verilmesi gereken bir içerik olup olmadığına karar vererek engelleme yapar.



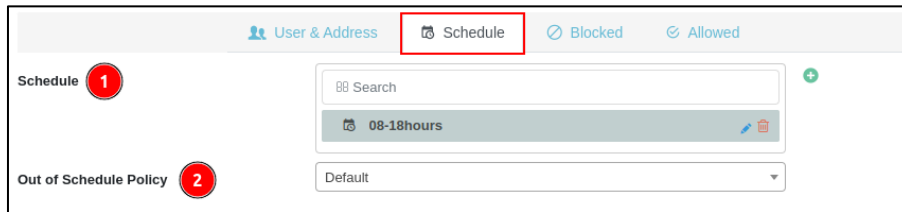
-Web Filtre politikasına Kullanıcı&Adres ekleme için Nesnelere ve Kimlikler modülünde eklenmek istenilen kullanıcıların veya adreslerin ekli olması gerekmektedir. Nesnelere ve Kimlikler modülünde eklenen kullanıcı veya adresler eklenerek web filtre kuralına eklenir.



-Web Filtre kuralına kullanıcı veya adres eklemek için 'ekle' butonuna tıklayarak Web Filtre kuralına kullanıcı ve adres eklenebilir.

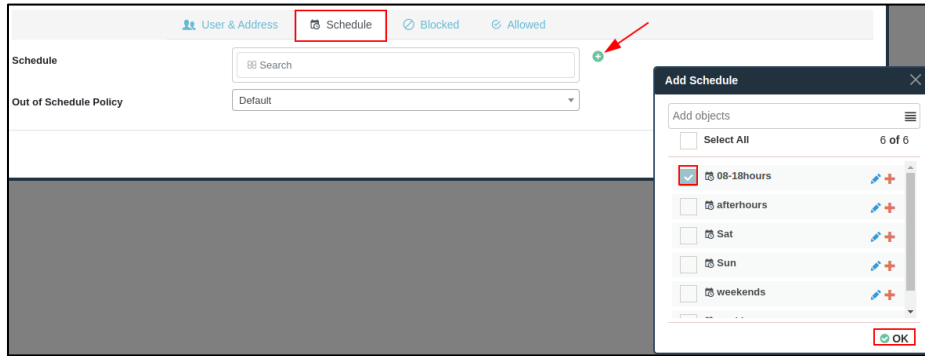


-Web Filtre politikasının çalışma zamanı eklemek için Nesnelere ve Kimlikler menüsünde Zaman nesnesi eklenmesi gerekir. Zaman nesnesini ekledikten sonra Web Filtre politikasına Zaman eklenebilir.

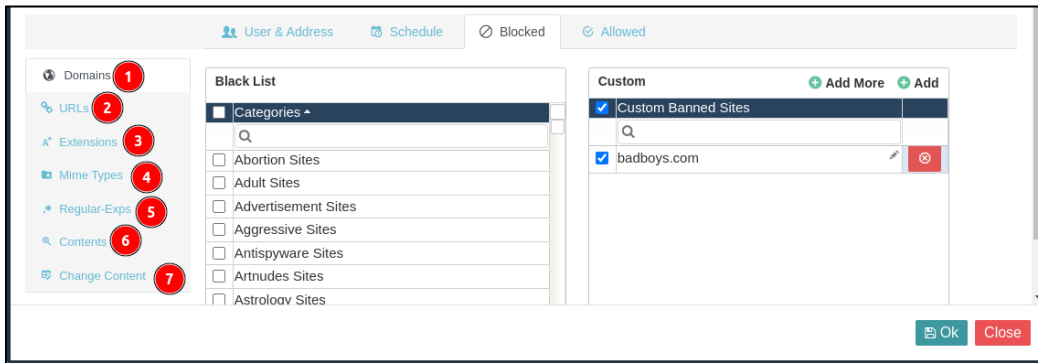


1	Zaman	Web filtre kuralının çalışacağı zamanın belirlenir.
2	Zamanlama Dışındaki Politika	Belirtilen zamandan farklı bir zaman aralığında hangi Web Filtre politikasının uygulanması gerektiği belirlenir.

-Politikaya zaman ekleme için 'ekle' butonuna tıklanarak Web Filtre politikasının çalışma zamanı seçilir.



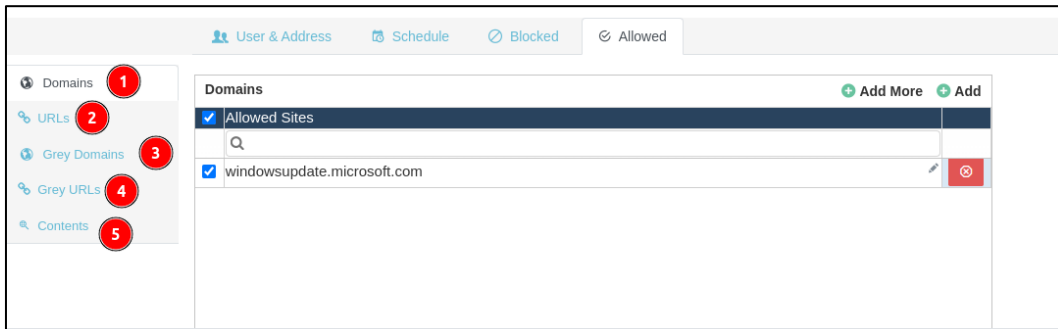
-Web Filtre politikasında Alan Adı, URL, Uzantılar, Uygulama Tipi, Düzenli İfadeler, İçerikler ve İçerik Değiştirme engellemelerini yapmak için Engelli sekmesi kullanılır.



1	Alan Adı	Belirli kategorilerdeki Alan Adlarının engellenmesi için seçilen kategoriler veya özel olarak eklenmek istenen Alan Adları engellenebilir. Örneğin, "youtube.com" gibi belirli bir Alan Adı özel olarak engellenebilir veya kategorilere göre engelleme yapılabilir.
2	URL	Belirli kategorilerdeki URL engellenmesi için seçilen kategoriler veya özel olarak eklenmek istenen URL engellenebilir. Örneğin, "profile.youtube.com" gibi belirli bir URL özel olarak engellenebilir veya kategorilere göre engelleme yapılabilir.
3	Uzantılar	Engellenecek olan uzantıların seçildiği sekmedir. Özel olarak uzantı eklenebilir. (Örn. .pdf)
4	Uygulama Tipi	Bir dosyanın içeriğinin türünü tanımlayarak engelleme işlemi yapar. Labris UTM cihazı üzerinde varsayılan olan Uygulama tipleri seçilebilir veya Özel Uygulama

		Tipi Web Filtre kurallarına eklenebilir.(Örn. application/mp4, image/jpeg)
5	Düzenli İfadeler	Varsayılan olarak cihaz üzerinde bulunan Düzenli İfadeler seçilebilir veya Düzenli İfade eklenebilir. (Örn. (yimg.com\imageV))
6	İçerikler	Sitenin içeriğinde bulunan içerikleri yasaklandığı yerdir. Varsayılan cihaz üzerinde bulunan İçerikler seçilebilir veya özel olarak içerik eklemesi yapılır. (Örn. kumar)
7	İçeriği Değiştir	Sitenin içeriğindeki metnin içeriğini değiştirdiği bölümdür.Burada değiştirilecek metin ve yeni metin girilir. (Örn. kumar içerenen bir metni yasak olarak değiştirir.)

-Web Filtre politikasında Alan Adı, URL, Uzantılar, Gri Siteler, Gri URL, İçeriklere izin vermek için İzinli sekmesi kullanılır.



1	Alan Adı	Eklene Alan Adlarına izin verildiği bölümdür. (Örn. youtube.com)
2	URL	Eklene URL adresine izin verildiği bölümdür. (Örn youtube.com/spor)
3	Gri Site	Bir sitenin tamamını filtrelemek için kullanılır.(Örn. labristeknoloji.com)
4	Gri URL	Bir sitenin belirli bir kısmını filtrelemek kalanını filtrelememek istenildiği durumlarda kullanılır.(Örn labristeknoloji.com/support)

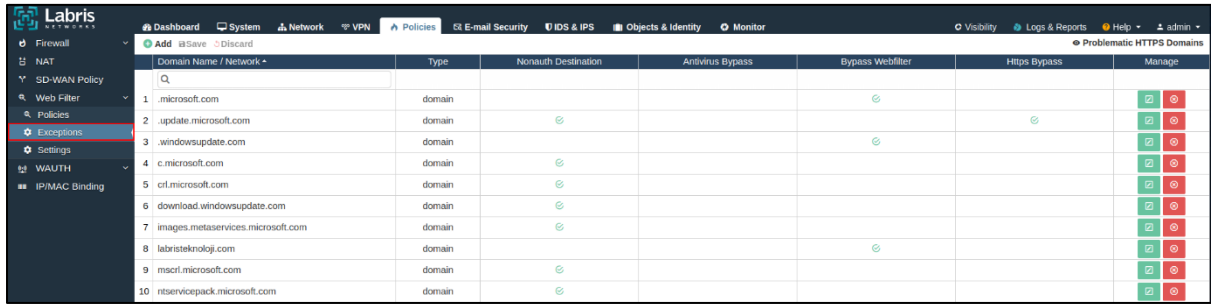
5	İçerikler	Sitenin içeriğinde bulunan içerikleri izin verildiği böümdür. Varsayılan cihaz üzerinde bulunan İçerikler seçilebilir veya özel olarak içerik eklemesi yapılır. (Örn. kumar)
---	------------------	--

Not

İzinli olarak eklenen siteler öncelikli olarak çalışmaktadır.

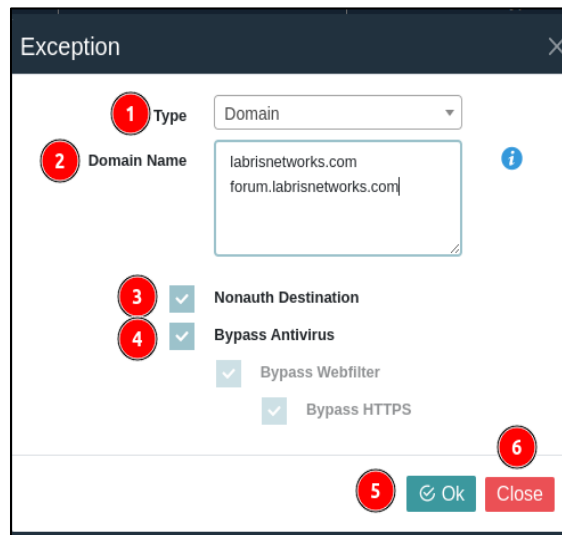
13.4.2 İstisnalar

Web filtre politikasına dahil olmayacak sitelerin girildiği modüldür. Labris UTM cihazı üzerinde varsayılan olarak gelen istisna olarak eklenmiş sitelerin yanında istisna olarak yeni bir site eklendiği modüldür.



Domain Name / Network	Type	Nonauth Destination	Antivirus Bypass	Bypass Webfilter	Https Bypass	Manage
1 .microsoft.com	domain					
2 .update.microsoft.com	domain					
3 .windowsupdate.com	domain					
4 c.microsoft.com	domain					
5 ctf.microsoft.com	domain					
6 download.windowsupdate.com	domain					
7 images.metaservices.microsoft.com	domain					
8 labristeknoloji.com	domain					
9 msctf.microsoft.com	domain					
10 ntservicepack.microsoft.com	domain					

İstisna olarak Web sitesi eklemek için 'ekle' butonuna tıklayarak istisna sitesi eklenir.



Exception

1 Type: Domain

2 Domain Name: labrisnetworks.com, forum.labrisnetworks.com

3 Nonauth Destination:

4 Bypass Antivirus:

Bypass Webfilter:

Bypass HTTPS:

5 Ok, 6 Close

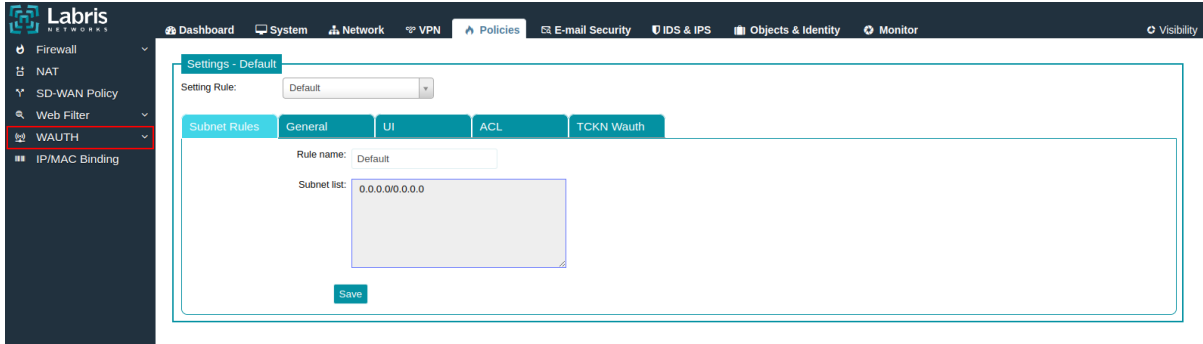
1	Tip	İstisna olarak eklenecek tip seçilir. Alan Adı veya Ağ
---	------------	--

		Adresi tipleri seçilerek ekleme yapılır.
2	Alan Adı(Tip: Alan Adı)	İstisna olarak eklenecek Alan Adlarının girildiği bölümdür.
3	Yetkilendirmesiz Hedefler(Tip: Alan Adı)	Site içerisindeki yetkilendirmesiz hedeflere giriş izni verildiği butondurç
4	Antivirüsü Es Geç(Tip: Alan Adı)	İstisna olarak eklenecek site üzerinde antivirus taramasını es geçer.
5	Web Filtrelemeyi Es Geç(Tip: Alan Adı)	İstisna olarak eklenecek site üzerinde Web filtre politikasını es geçer.
6	HTTPS Filtrelemeyi Es Geç(Tip: Alan Adı)	İstisna olarak eklenecek sitenin HTTPS filtrelemeyi es geçer.
7	HTTPS Filtreleme Es Geçilecek Ağlar(Tip: Ağ Adresi)	Tipin Ağ adresi seçildiği durumda açılır. HTTPS Filtreye dahil olmayacak Ağ Adreslerini eklendiği bölümdür.
7	Tamam	Yapılan değişikliklerin kaydedildiği butondur.
8	Kapat	Açılan pencerenin kapatıldığı butondur.

13.5 Wauth

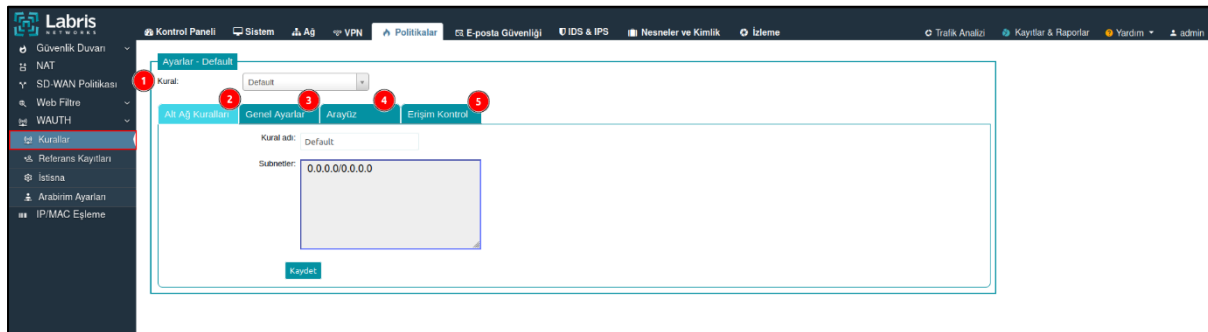
Wauth kullanıcı ve misafirler için kimlik doğrulama için kullanılan modüldür. Kurumsal ağlarda veya misafirler için kullanılan ağlarda Kullanıcı yetkilendirmesi ile giriş işlemlerinin yapılır. Kullanıcılar giriş bilgileri ile İnternet üzerindeki gezintisini kayıt altına alınmasını sağlar.

Labris UTM cihazında Yerel Yetkilendirme, SMS, Aktif Dizin, Otel Entegrasyonu, TC NO NVI Doğrulama ve Pasaport yetkilendirilmeleri bulunur.



13.5.1 Kurallar

Kullanıcı ve misafirlerin yetkilendirme biçimlerinin ayarlandığı, giriş ekrandaki bilgilerin düzenlendiği gibi ayarların yapıldığı modüldür. Yerel IP adresleri için **Wauth** kuralının düzenlendiği modüldür.

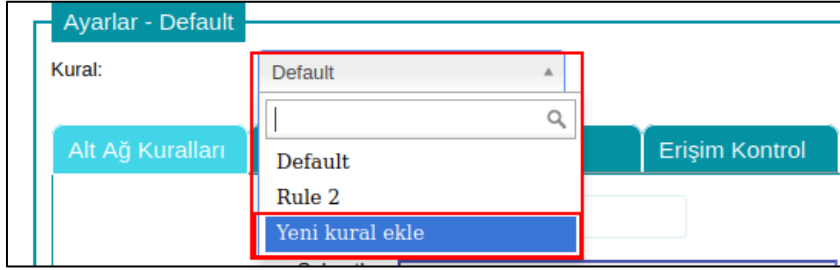


1	Kural	Wauth politikasının yazılacağı kural seçilir.
2	Alt Ağ Kuralları	Seçilen kuralın ağ adresinin girildiği bölümdür.
3	Genel Ayarlar	Wauth'a girişi yapacak kullanıcıların yetkilendirilmesinin ayarlandığı bölümdür.
4	Arayüz	Wauth'a giriş yapacak kullanıcılar için arayüz düzenlemesinin yapıldığı bölümdür.

5	Erişim Kontrol	Wauth'a giriş yapacak kullanıcıların erişimlerini kontrol edilmesine yönelik kurallarının yazıldığı bölümdür.
---	-----------------------	---

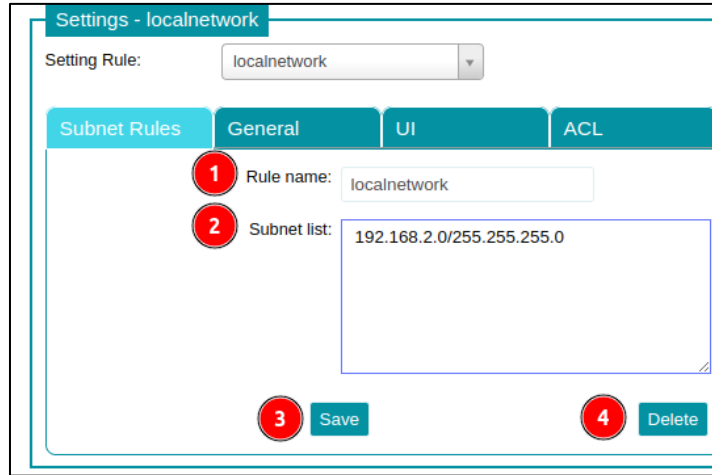
13.5.1.1 Yeni Kural Ekleme

Labris UTM cihazı üzerinde varsayılan olarak gelen Wauth kuralının dışında yeni bir kural eklemek için kullanılır. Yeni bir kural eklenmesinin amacı iki adet yerel ağınızda da farklı yetkilendirme kullanabilmek veya iki yerel ağda farklı kurallarda yönetmek olabilir.



13.5.1.2 Alt Ağ Kuralları

Wauth kuralının uygulanacağı ağ adresinin girildiği bölümdür. Labris UTM cihazı üzerinde varsayılan olarak '0.0.0.0/0.0.0.0' olarak gelmektedir. Yeni bir IP adresi eklemek için yeni kural eklenmesi gerekmektedir.



1	Kural Adı	Alt Ağ Kuralının adının girildiği yerdir.
2	Subnetler	Politika uygulanacak olan yerel ağ adresinin girildiği yerdir. Birden fazla yerel ağ adresi girilir. (Örn. 192.168.2.0/255.255.255.0, 10.10.1.0/255.255.0.0)
3	Kaydet	Alt Ağ Kurallarının kaydedildiği butondur.

4	Sil	Alt Ağ Kuralının silindiği butondur.
---	------------	--------------------------------------

13.5.1.3 Genel Ayarlar

Genel Ayarlar bölümünde, kullanıcılara gelen karşılama ekranını, kullanıcıların yetkilendirme biçimlerinin ayarlandığı bölümdür.

1	Karşılama Mesajı	Kullanıcıların Wautha giriş yaptıktan sonra gelen karşılama mesajıdır.
2	Karşılama Mesajı(EN)	Kullanıcıların Wautha giriş yaptıktan sonra gelen İngilizce karşılama mesajıdır.
3	Yerel Yetkilendirme Biçimi	Alt Ağ Kurallarının kaydedildiği butondur. Labris UTM cihazı üzerinde Nesnelere ve Kimlikler modülünde ekli olan kullanıcılar Wauth'a giriş yapar.
4	SMS Wauth	Kullanıcıların ağa dahil olması için SMS ile kimlik

		doğrulaması yapar.
5	Aktif Dizin Yetkilendirmesi	Labris UTM cihazı üzerinde Aktif Dizin entegrasyonu yapıldıktan sonra Aktif Dizindeki kullanıcıların, kullanıcı adları ve şifreleriyle birlikte Wauth'a giriş yapması gerektiği durumlarda kullanılır.
6	TC NO NVI Doğrulama	Kullanıcıların TC Kimlik numaralarını kullanarak Wauth'a Giriş yapması için kullanılır.
7	Pasaport Wauth	Kullanıcıların Pasaport bilgilerini kullanarak Wauth'a Giriş yapması için kullanılır.
8	Sözleşme Etkin/Devre Dışı	Wauth'a giriş yaparken sözleşmenin etkinleştirildiği ya da devre dışı bırakıldığı butondur.
9	Sözleşme	Sözleşmenin Türkçe'sinin görüntülediği butondur.
10	Sözleşme(EN)	Sözleşmenin İngilizce'sinin görüntülediği butondur.

-Yerel Yetkilendirme Biçiminin etkinleştirildiği durumda kullanıcıların TC Kimlik numarası veya pasaport ile yetkilendirme yapılır

The screenshot shows a configuration window for Wauth. The 'Local Auth. Format:' dropdown menu is open, displaying two options: 'Passaport or Free Username' (selected) and 'TC Identification'. Below this, there is a search bar for 'SMS Wauth:' and another dropdown menu for 'Active Directory Authent.' with 'Passaport or Free Username' selected.

-SMS Wauth etkinleştirildiğinde kullanıcılara SMS ile Wauth'a giriş yapma imkanı verir. SMS Wauth etkinleştirilen sonra SMSWauth bölümü açılmaktadır.

The screenshot shows the 'SMS Wauth:' dropdown menu open, with 'Enable' selected. Below it, there is a search bar and another dropdown menu for 'Confirmation:' with 'Disable' selected.

Settings - localnetwork

Setting Rule: localnetwork

Subnet Rules General **SMSWauth** UI ACL

1 Default Group: Default

2 Multiple Login Limit: 1

3 Apply multiple login limit to all SMS users:

4 Account Expiration Date: 24 (hours)

5 Timeout: 1440 (mins)

6 Cust. Serv. Tel: 5555555555

7 Comp. Mobile***: 5555555555

8 Cust. Serv. Email: support@labrisnetworks.com

9 Enable Common Key:

10 SMS sending will be afforded by the company*:

11 Require mail for SMS signup:

12 Require Whitelist Check:

13 Use Custom SMS Api:

14 Remained Token**: 0

15 Custom SMS Service Configuration

16 Buy tokens

17 Show Common Key

18 Save

1	Varsayılan Grup	SmsWauth'un etkinleştirilideceği grubun seçilir.
2	Çoklu Bağlantı Limiti	SMSWauth ile açılan giriş yapan kullanıcının kaç hesapla bağlanacağını seçilir.
3	Çoklu Bağlantı Limitini Tüm SMS Kullanıcılarına Uygula	SMS ile giriş yapan kullanıcılara çoklu bağlantı limitinin etkinleştirildiği bölümd
4	Hesap Silinme Tarihi	SMS Wauth ile açılan hesabın silinme zamanı belirtildiği bölümdür.
5	Zaman Aşımı	Giriş yapan kullanıcının zaman aşımı süresinin belirtildiği bölümdür.

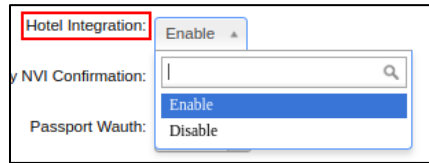
6	Teknik Destek Tel	Teknik destek Telefon numarasının girildiği bölümdür.
7	Kurum Cep Tel	Kurum Cep telefon numarasının girildiği bölümdür.
8	Ortak Anahtarı Etkinleştir	Ortak anahtarın etkinleştirildiği bölümdür.
9	Bütün SMS gönderimleri firma/kurum tarafından karşılanacak	SMS gönderimini firma ve kurum tarafından karşılanacak ise açılır. Açıldığı durumda firmadan jeton almak gerekmektedir.
10	SMS girişi için posta adresi gereklidir:	SMS girişi yapmak için posta adresinin gerekli olması gerektiği durumlarda etkinleştirilir.
11	GSM Numarası 'İzin Verilenler' listesinde olmalı	İzin verilmiş olan GSM numaralarına SMSWauth ile giriş izni verilir.
12	Üçüncü-parti SMS Servisi Kullan:	SMS sağlayıcı kullanılacağı durumda kullanılır.
13	Kalan Jeton	Jeton alınması durumunda kalan jeton görülür. Her bir jeton bir SMS hakkını belirtir.
14	SMS Servis Ayarlarını Yap	SMS Sağlayıcı olarak kullanılacak olan sağlayıcı ayarlarının yapıldığı butondur.
15	Jeton Al	SMS sağlayıcı olarak Labris UTM cihazı kullanıldığı durumlarda kalan SMS hakkının görüntülediği yerdir.
16	Ortak Anahtarı Göster	SMS Wauth için belirtilen ortak anahtarın görüntülediği butondur.
17	Kaydet	SMSWauth ayarlarının kaydedildiği butondur.

-Wauth'a giriş yapacak kullanıcıların Aktif Dizin'den çekilmesi gerektiği durumlarda kullanılır. Aktif Dizin etkinleştirildiğinde Aktif Dizindeki kullanıcıların wauth'a giriş yapması için kullanılır.

1	Çoklu Giriş Limiti	Aktif Dizindeki kullanıcıların WAUTH'a çoklu giriş limiti belirtilir.
2	Çoklu Giriş Limitini Tüm AD Kullanıcılarına Uygula	Aktif Dizindeki kullanıcılara çoklu limit girişi uygulanın etkinleştirildiği bölümdür.
3	Grup Yetkilendirmelerini Kapat	Aktif Dizindeki grup adlarını devre dışı bıraktığı bölümdür.
4	Sınırsız Zaman Aşımı	Aktif Dizindeki kullanıcıların zaman aşımını süresinin devredışı bırakıldığı bölümdür.

5	AD Zaman Aşımı	AD zaman aşımı süresi belirtilir.
6	Sınırsız Hesap Silinme Süresi	Kullanıcıların hesaplarının sonsuz silinme zamanının etkinleştirildiği bölümdür.
7	AD Hesap Silinme Süresi	AD üzerinde sona erme zamanının belirtildiği bölümdür.
8	AD Kontrol	Aktif Dizindeki kullanıcıların test edildiği butondur.
9	Kaydet	Aktif Dizin Yetkilendir ayarlarının kaydedildiği butondur.

-Otel Entegrasyonu etkinleştirildiği durumda veritabanında tutulan verileri kullanarak Wauth'a giriş yapma olanağı sağlar.



Settings - Default

Setting Rule: Default

Subnet Rules | General | **Hotel** | UI | ACL | TCKN Wauth

1 Default Group: Default

2 Hotel Name:

3 Product Type: Fidelio (OracleDB)

4 Machine Address: ip or domain name

5 Machine Port: 3306

6 Database Name (or file path):

7 Table Name:

8 Username:

9 Password:

10 Username Field Name: Room No

11 Password Field Name: VERILENODANO

12 Name Field Name: auto

13 Surname Field Name: auto

14 Departure Date: auto

15 Timeout: 0 (mins)

16 Extra Time: 15 (hours)

17 Synchronization Interval: 15 (mins)

18 Infinite timeout:

19 Multiple Login Limit: 1

20 Apply multiple login limit to all hotel users:

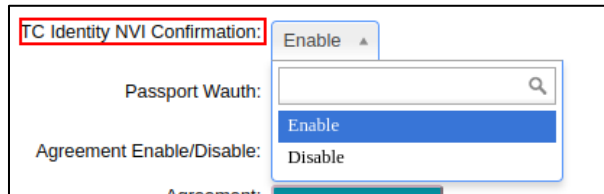
21 Test

22 Save

1	Varsayılan Grup	Otel entegrasyonunun etkinleştirildiği grup seçilir.
2	Otel İsmi	Otel isminin girildiği bölümdür.
3	Ürün	Veritabanı türünün seçilir. Labris UTM cihazında desteklenen veritabanı türleri Fidelio(OracleDB), Sentez(MsSQL), Amonra(XML), Rmos(XML),Akinsoft_Wolvox(Firebird),Asyasoft'tür. Desteklenen veri tabanı türleri dışında Custom olarakta veri tabanından veri alınır.
4	Sunucu Adresi	Veritabanı sunucusunun adresinin girildiği bölümdür
5	Sunucu Portu	Veritabanı sunucusunun portunun girildiği bölümdür.
6	Veritabanı İsmi	Veritabanı sunucusunun isminin girildiği bölümdür.
7	Tablo İsmi	Veritabanının tablo isminin girildiği bölümdür.
8	Kullanıcı Adı	Veritabanına giriş yapılırken kullanılan Kullanıcı adı girildiği bölümdür.
9	Parola	Veritabanına giriş yapılırken kullanılan parolanın girildiği bölümdür.
10	Kullanıcı Alanı İsmi	Wauth'a giriş yapan kullanıcının alan adının seçildiği bölümdür.
11	Şifre Alan İsmi	Veritabanından otomatik olarak çekilir.
12	İsim Alan Adı	Veritabanından otomatik olarak çekilir.
13	Soyisim Alan Adı	Veritabanından otomatik olarak çekilir.
14	Ayrılış Tarihi	Veritabanından otomatik olarak çekilir.

15	Zaman Aşımı	Kullanıcının giriş yaptıktan sonra zaman aşımının belirtildiği bölümdür.
16	Ekstra İzin Süresi	Giriş yapıldıktan kullanıcılara verilen ekstra izin süresinin belirtildiği bölümdür.
17	Sekronizasyon Aralığı	Veritabanına eklenen yeni verilerin Labris UTM cihazına aktarıldığı zamanın belirtildiği bölümdür.
18	Sınırsız Zaman Aşımı	Zaman aşımının sınırsız olması gerektiği durumlarda kullanılır.
19	Çoklu Bağlantı Limiti	Kullanıcıların aynı hesaptan kaç kere bağlanacağını belirtildiği bölümdür.
20	Çoklu Bağlantı Limitini Tüm Özel Kullanıcılarına Uygula	Tüm kullanıcılar için çoklu bağlantı limitinin açılır.
21	Test	Veritabanı entegrasyonunun test edildiği butondur.
22	Kaydet	Otel entegrasyonu ayarlarının kaydedildiği butondur.

-TC Kimlik Numarası ile giriş yapılması gerektiği durumlarda açılır. TC NO NVI Doğrulama ile WAUTH'a giriş yapılması gerekir. Kullanıcılar TC kimlikleri ile kayıt olduklarında NVI ile kullanıcının TC kimlik numarasını doğum tarihiyle eşleştirir. Eşleşme sağlanması durumunda kullanıcı TC Kimlik Numarası ve doğum yılı ile WAUTH'a giriş yapar.



The screenshot shows the 'Settings - Default' page with the 'TCKN Wauth' tab selected. The 'Setting Rule' is set to 'Default'. The configuration options are as follows:

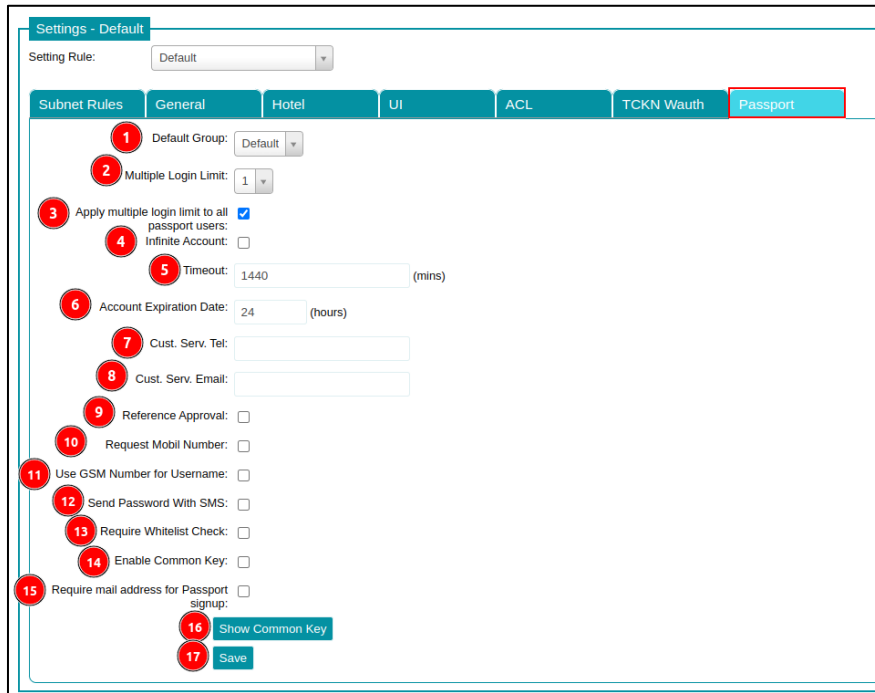
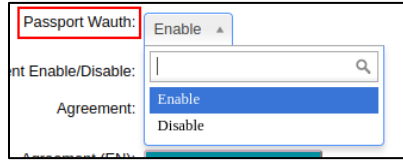
- 1. Default Group: Default
- 2. Multiple Login Limit: 1
- 3. Apply multiple login limit to all TCKN users:
- 4. Infinite Account:
- 5. Timeout: 1440 (mins)
- 6. Account Expiration Date: 24 (hours)
- 7. Cust. Serv. Tel: 5555555555
- 8. Cust. Serv. Email: test@labrisnetworks.com
- 9. Reference Approval:
- 10. Request Mobil Number:
- 11. Use GSM Number for Username:
- 12. Send Password With SMS:
- 13. Require Whitelist Check:
- 14. Enable Common Key:
- 15. Require mail address for TCKN signup:
- 16. Send TCKN with Reference Mail:
- 17. Login auto when sign up:
- 18. Show Common Key button
- 19. Save button

1	Varsayılan Grup	TCKN Wauth varsayılan grup seçilir.
2	Çoklu Bağlantı Limiti	Wauth'a giriş yapacak olan kullanıcıların çoklu bağlantı limiti belirtilir.
3	Çoklu Bağlantı Limitini Tüm TCKN Kullanıcılarına Uygula	Çoklu bağlantı limitini tüm TCKN kullanıcılarına uygulamak için kullanılan yerdir.
4	Sınırsız Zaman Aşımı	Zaman aşımı süresinin sınırsız olması gerektiği durumlarda işaretlenir.
5	Zaman Aşımı	Zaman aşım süresinin dakika cinsinden belirttiği bölümdür.
6	Hesap Silinme Tarihi	Kullanıcıların açtıkları hesaplarının silinme zamanının saat cinsinden belirtildiği bölümdür.
7	Teknik Destek	Teknik Destek Telefonunun girildiği bölümdür.

	Telefonu	
8	Teknik Destek Email	Teknik Destek mail adresinin girildiği bölümdür.
9	Referans Onayı	TCKN ile kaydolan kullanıcıların referans onayından sonra oturumunun açılması gerektiği durumlarda açılır.
10	Kullanıcıdan GSM No İste	Kullanıcılar kayıt olurken GSM numarası istenmesi gereken durumlarda etkinleştirilir.
11	Kullanıcı Adı GSM No Olsun	Kullanıcıların giriş yaptıktan sonraki kullanıcı adlarının telefon numarası olarak ayarlanmak istenilen durumlarda etkinleştirilir.
12	Giriş Bilgilerini SMS ile Gönder	Etkinleştirildiğinde kullanıcıların giriş bilgilerinin SMS ile gönderilir.
13	GSM Numarası 'izin Verilenler' Listesinde olmalı	GSM numarasının izin verilen listesinde olan kullanıcıların WAUTH' a giriş izni verilir.
14	Ortak Anahtarı Etkinleştir	WAUTH' a giriş için yönetim tarafından belirtilen ortak anahtarın belirtildiği bölümdür.
15	TCKN Girişi için Posta adresi gereklidir.	TCKN ile giriş yaparak posta adresinin girilmesi gereken durumlarda etkinleştirilir.
16	TCKN'yi Referans Postası ile Gönderin	TCKN'yi referans postası ile gönderir.
17	Kayıt olurken otomatik giriş yapın:	Kayıt olduktan sonra WAUTH'a otomatik olarak giriş yapar
18	Ortak Anahtarı Göster	Belirlenen ortak anahtarı gösterir.

19	Kaydet	TCKN WAUTH'da yapılan ayarların kaydedildiği butondur.
----	---------------	--

-Kullanıcıların Wauth' a kayıt olurken Pasaport kullanılması gerektiği durumlarda Pasaport Wauth etkinleştirilir. Etkinleştirildikten sonra kullanıcılar Wauth'a kayıt olurken pasaport numaralarını kullanır.



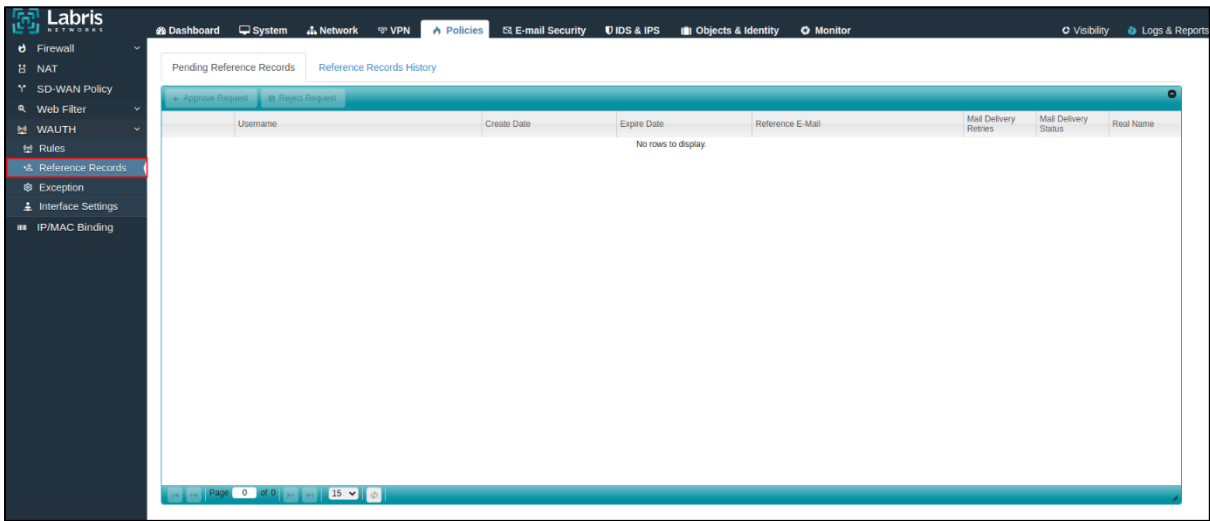
1	Varsayılan Grup	Pasaport Wauth için varsayılan grup seçilir.
2	Çoklu Bağlantı Limiti	Wauth'a giriş yapacak olan kullanıcıların çoklu bağlantı limiti belirtilir.
3	Çoklu Bağlantı Limitini Tüm Pasaport Wauth Kullanıcılarına Uygula	Çoklu bağlantı limitini tüm Pasaport ile bağlanan kullanıcılara uygulamak için kullanılan yerdir.
4	Sınırsız Zaman	Zaman aşımı süresinin sınırsız olması gerektiği

	Aşımı	durumlarda işaretlenir.
5	Zaman Aşımı	Zaman aşım süresinin dakika cinsinden belirttiği bölümdür.
6	Hesap Silinme Tarihi	Kullanıcıların açtıkları hesaplarının silinme zamanın saat cinsinden belirtildiği bölümdür.
7	Teknik Destek Telefonu	Teknik Destek Telefonunun girildiği bölümdür.
8	Teknik Destek Email	Teknik Destek mail adresinin girildiği bölümdür.
9	Referans Onayı	Pasaport ile kaydolmuş kullanıcıların referans onayından sonra oturumunun açılması gerektiği durumlarda açılır.
10	Kullanıcıdan GSM No İste	Kullanıcılar kayıt olurken GSM numarası istenmesi gereken durumlarda etkinleştirilir.
11	Kullanıcı Adı GSM No Olsun	Kullanıcıların giriş yaptıktan sonraki kullanıcı adlarının telefon numarası olarak ayarlanmak istenilen durumlarda etkinleştirilir.
12	Giriş Bilgilerini SMS ile Gönder	Etkinleştirildiğinde kullanıcıların giriş bilgilerinin SMS ile gönderilir.
13	GSM Numarası 'İzin Verilenler' Listesinde olmalı	GSM numarasının izin verilen listesinde olan kullanıcıların WAUTH' a giriş izni verilir.
14	Ortak Anahtarı Etkinleştir	WAUTH' a giriş için yönetim tarafından belirtilen ortak anahtarın belirtildiği bölümdür.
15	Pasaport Giriş İçin Posta Adresi Gereklidir	Kayıt olduktan sonra WAUTH'a otomatik olarak giriş yapar

16	Ortak Anahtarı Göster	Belirlenen ortak anahtarı gösterir.
17	Kaydet	Pasaport WAUTH'da yapılan ayarların kaydedildiği butondur.

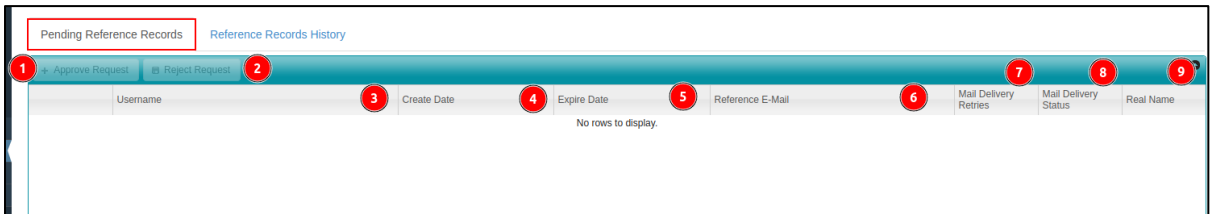
13.5.2 Referans Kayıtları

Wauth kurallarında Referans Onayının etkinleştirildiğinde kullanılır. Referans Onayı verilen kullanıcıların Wauth'da açtıkları hesabı onaylanır ve kullanıcılar kayıt oldukları hesap ile WAUTH'a giriş yapar.



13.5.2.1 Bekleyen Referans Kayıtları

Kullanıcıların WAUTH'a giriş yaparkenki referans onayı bekleyen referans kayıtlarının listesini gösterir. Referans onayından sonra kullanıcıların WAUTH'a giriş yapar.



1	İsteği Onayla	WAUTH'a kayıt olan kullanıcıların WAUTH isteğinin onaylandığı butondur.
2	İsteği Reddet	WAUTH'a kayıt olan kullanıcıların WAUTH isteğinin reddedildiği butondur.
3	Kullanıcı Adı	WAUTH'a giriş yapan kullanıcının Kullanıcı Adının görüntülediği bölümdür.

4	Oluşturma Tarihi	WAUTH hesabının oluşturulma tarihinin görüntülediği bölümdür.
5	Geçerlilik Süresi	Referans isteğinin geçerlilik süresi görüntülenir.
6	Referans Email	Referans mail adresinin görüntülediği bölümdür.
7	E-Posta İletim Deneme Sayısı	E-posta gönderiminin deneme sayısını gösteren bölümdür
8	E-Posta İletim Durumu	Teknik Destek mail adresinin girildiği bölümdür.
9	Ad Soyad	Pasaport ile kaydolun kullanıcıların referans onayından sonra oturumunun açılması gerektiği durumlarda açılır.

13.5.2.2 Geçmiş Referans Kayıtları

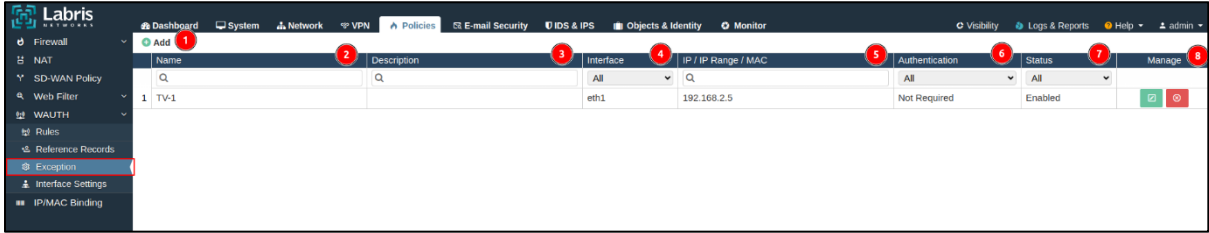
Geçmişte yapılan referans kayıtlarının listesi görüntülenir.

Pending Reference Records		Reference Records History				
Username	Decision Time	Real Name	Reference E-Mail	Decided By	Action	
@labris	19/04/2024 08:44:07	Mehmet KAYA	@gmail.com	Timeout System	Rejected	
@labris	28/03/2024 17:25:57	Mehmet KAYA	@gmail.com	Admin Interface	Approved	

Page 1 of 1 | 15 | Displaying 1 to 2 of 2 items

13.5.3 İstisna

İstisna olarak eklenen IP adreslerine WAUTH sormadan internete girebilmesini sağlar. İstisna olarak eklenecekler genellikle WAUTH'da oturum açamayan cihazlar için kullanılmaktadır.



1	Ekle	İstisna olarak eklenecek IP, IP Aralığı ve MAC Adreslerinin eklendiği butondur.
2	İsim	İstisna olarak eklenen cihazın isminin görüntülediği bölümdür.
3	Açıklama	İstisna olarak eklenen cihazla ilgili açıklamanın görüntülediği bölümdür.
4	Arabirim	İstisna olarak eklenen cihazın arabiriminin görüntülediği bölümdür.
5	IP/IP Aralığı/ MAC	Eklenecek cihazın IP, IP Aralığı veya MAC adresinin görüntülediği bölümdür.
6	Kimlik Doğrulama	Eklenecek cihaz için WAUTH ile kimlik doğrulama yöntemi görüntülenir.
7	Durum	Yazılan istisnanın çalışıp çalışmadığı görüntülenir. Aktif ise eklenen istisna çalışır durumdadır. Pasif ise eklenen istisna çalışmayacaktır.
8	Yönet	Eklenecek istisnanın düzenlendiği veya silindiği bölümdür.

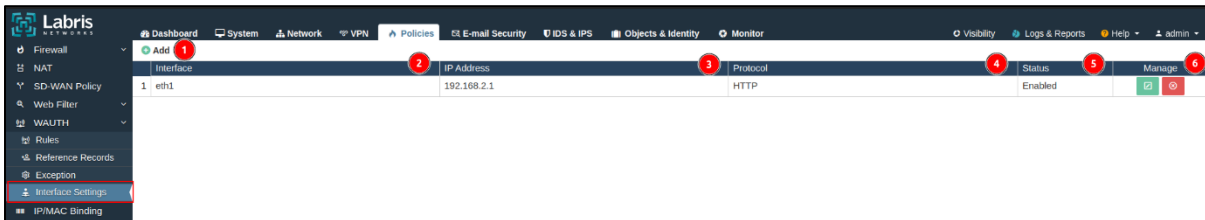
-İstisna eklemek için 'ekle' butonuna tıklayarak istisna IP, IP Aralığı, MAC Adresi istisna kuralına eklenir.

1	Etkinleştir	Eklenecek istisna kuralının etkinleştirildiği butondur.
2	İsim	İstisna olarak eklenecek cihazın isminin girildiği bölümdür.
3	Açıklama	İstisna olarak eklenecek cihaz ile ilgili açıklamanın girildiği bölümdür.
4	Arabirim	Eklenecek olan cihazın bağlı olduğu arabirim seçildiği bölümdür.(Seçilen arabirim üzerinde WAUTH açık olması gerekmektedir.)
5	Kimlik Doğrulama	Eklenecek cihazın kimlik doğrulama metodunun seçildiği bölümdür. Gerekli seçili ise WAUTH'a giriş yapması gerekmektedir. Gerekli Değil seçili ise eklenen cihazın WAUTH'a giriş yapmasına gerek yoktur.
6	Tip	İstisna kuralının Tipi belirtilir. IP seçilmesi durumunda sadece 1 adet IP adresine izin verilir(192.168.1.25). IP Aralığı seçilmesi durumunda belirli bir IP aralığı girilir(192.168.30-192.168.40). MAC seçilmesi durumunda cihazın MAC adresine göre istisna kuralı yazılır. SUBNET seçilirse belirtilen subnete göre

		istisna eklenir(192.168.1.0/24). Kaynak seçili ise kaynağa göre IP, IP Aralığı ve Subnet değerleri girilir. Hedef Seçilmesi durumunda hedef adrese göre IP, IP Aralığı ve Subnet değerleri girilir
7	Ağ Adresi	Seçilen Tip'e göre girilecek ağ adresleri değişkenlik göstermektedir.
8	Kaydet	Yazılan istisna kuralının kaydedildiği butondur.
9	Kapat	Ekle butonuna tıkladıktan sonra açılan ekranın kapatıldığı butondur. Yapılan işlemlerin kaydedilmeden kapatır.

13.5.4 Arabirim Ayarları

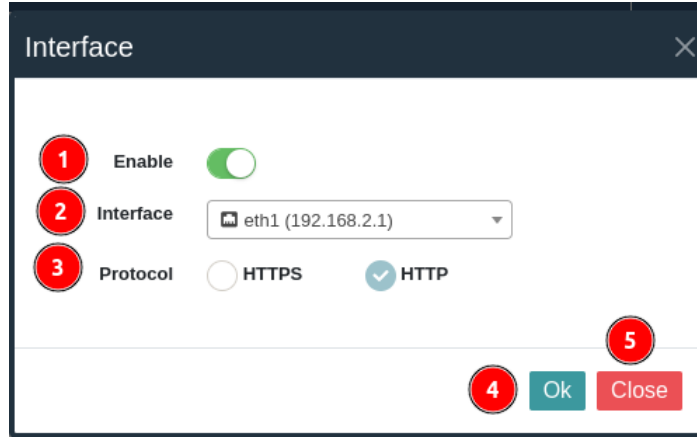
Wauth doğrulaması açılacak olan arabirimin seçildiği veya WAUTH için seçilen arabirimlerin görüntülediği modüldür.



1	Ekle	Wauth doğrulaması açılacak olan arabirimin eklendiği butondur.
2	Arabirim	Wauth doğrulamasının açık olduğu arabirim görüntülediği bölümdür.
3	IP Adresi	WAUTH arayüzüne erişilecek olan IP adresinin görüntülediği bölümdür.
4	Protokol	WAUTH çalıştığı protokol görüntülenir.(HTTP veya HTTPS)
5	Durum	WAUTH olarak seçilen arabirimin durumunun görüntülenir. Aktif ise WAUTH seçilen arabirimde açıktır. Pasifi se WAUTH seçilen arabirimde kapalıdır.

6	Yönet	WAUTH doğrulaması yapmak için eklenen arabirimlerin düzenlendiği veya silindiği butonlardır.
---	--------------	--

-Wauth'un çalışacağı arabirimin seçmek için 'ekle' butonuna tıklayarak karşımıza gelen ekranda arabirim seçimi yapılır. Seçim yapılacak arabirim iç ağ olması gerekir.



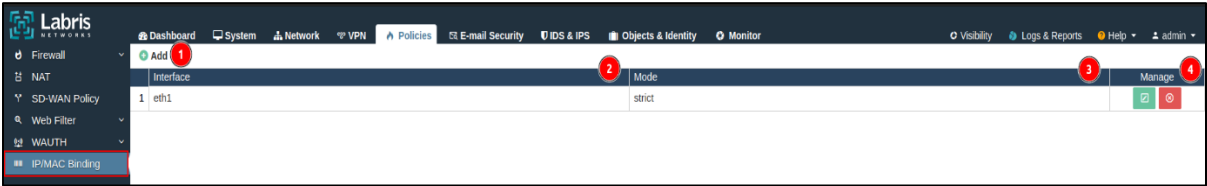
1	Etkinleştir	WAUTH'un etkinleştirildiği butondur.
2	Arabirim	WAUTH çalıştığı arabirim seçilir.
3	Protokol	WAUTH çalıştığı protokol seçilir.(HTTP veya HTTPS).
4	Kaydet	WAUTH arabirimin kaydedildiği butondur.
5	Kapat	'ekle' butonuna tıklayarak açılan ekran kapatılır.

13.6 IP MAC Eşleme

IP MAC Eşleme, bir ağdaki cihazın IP adresi ile MAC adresinin eşleştirme işlemidir. Ağdaki cihazlara cihazın donanımına özgü olan MAC adresi atanır.

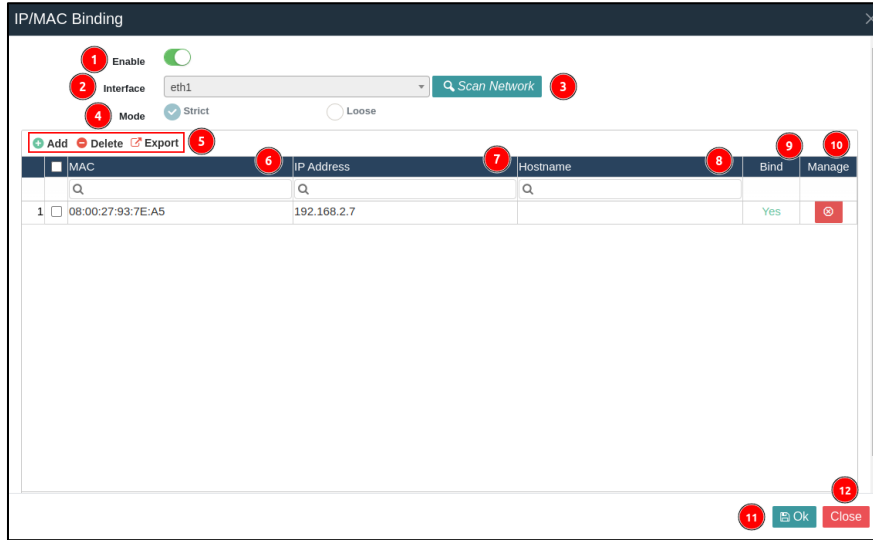
Sıkı Mod, ağ cihazlarının IP-MAC eşlemelerinin yapılması gerekir. Bir IP adresi belirli bir MAC adresiyle ilişkilendirilmiştir ve farklı bir Mac adresine sahip olan paketler reddedilir. IP-MAC eşlemesinin yapıldığı ağ cihazlarının dışında yeni bir ağ cihazı ağa dahil olduğunda gelen paketleri reddeder. Paketlerin kabul edilmesi için yeni cihazında IP-MAC eşlemesinin yapılması gerekir. Sıkı Mod, ağ güvenliği açısından daha sıkı bir kontrol sağlar.

Gevşek Mod, ağ cihazlarının IP-MAC eşleşmesi daha esnektir. IP-MAC eşlemesi yapılan cihazların dışında ağa yeni katılan farklı bir MAC adresinden gelen paketlere izin verir.



1	Ekle	IP-MAC eşleme politikasının eklendiği butondur
2	Arabirim	IP-MAC eşlemenin açıldığı arabirimin görüntülediği bölümdür.
3	Mod	IP-MAC eşlemenin modunun görüntülediği bölümdür.(Sıkı veya Gevşek)
4	Yönet	Eklene IP-MAC eşlemelerinin düzenlendiği veya silindiği bölümdür.

-IP-MAC Eşleme eklemek için 'ekle' butonuna tıklayarak IP-MAC eşleme işlemi yapılır.



1	Etkinleştir	IP-MAC eşleme politikasının etkinleştirildiği butondur.
2	Arabirim	IP-MAC eşlemenin açılacağı arabirimin görüntülediği butondur.
3	Ağı Tara	Seçilen arabirime bağlı olan ağ cihazlarının MAC ve IP adreslerinin görüntülediği butondur.
4	Mod	IP-MAC eşleminin modu seçilir.
5	Ekle-Sil-Dışarı Aktar	Ekle butonuna basıldığında seçilen arabirime ait cihazın MAC ve IP adresleri eklenir. Sil butonu ise seçilen IP-MAC eşleminin silinir. Dışarı Aktar butonu eklenen IP-MAC eşleme tablosunu dışarı aktarır.
6	MAC	Ağı Tara butonuna basıldıktan sonra ya da IP-MAC eşleşmesi yapılmış olan cihazların MAC adresleri görüntülenir.
7	IP Adresi	Ağı Tara butonuna basıldıktan sonra ya da IP-MAC eşleşmesi yapılmış olan cihazların IP adresleri görüntülenir.
8	Sunucu Adı	Ağ'da bulunan cihazların sunucu adları görüntülenir.

9	Eşle	Cihazların IP-MAC eşlemelerinin eşleme durumu görüntülenir. Eşleme yapmak için eşle durumunun evet olması gerekir.
10	Yönet	Yapılan IP-MAC eşleminin silindiği bölümdür.
11	Kaydet	IP-MAC eşleme politikasının kaydedildiği butondur.
12	Kapat	Açılan IP-MAC eşleme ekranının kapatıldığı butondur.

-Cihazların IP-MAC eşlemesi yapmak için 'ekle' butonuna tıklanır.

	MAC	IP Address	Hostname	Bind	Manage
1	<input type="checkbox"/> 08:00:27:93:7E:A5	192.168.2.7		Yes	

-Ekle butonuna basıldıktan sonra yeni bir satır eklenir. Eklenen satıra denk gelen kutucuklar doldurularak yeni eklenen cihazın IP adresi MAC adresiyle eklenmiş olur.

	MAC	IP Address	Hostname	Bind	Manage
1	<input checked="" type="checkbox"/> aa:bb:cc:dd:ee:ff	192.168.2.5	Labris2	Yes	
2	<input type="checkbox"/> 08:00:27:93:7E:A5	192.168.2.7		Yes	

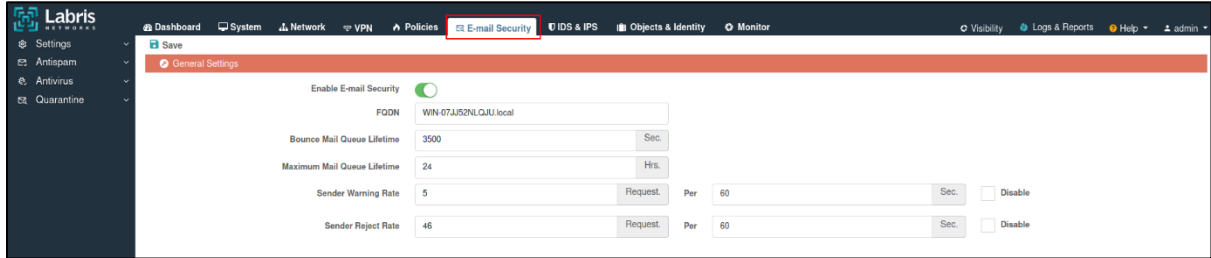
Not

Sıkı mod seçilmesi durumunda IP-MAC eşleşmesi yapılmayan cihazların paketleri drop olur.

14. E-Posta Güvenliği

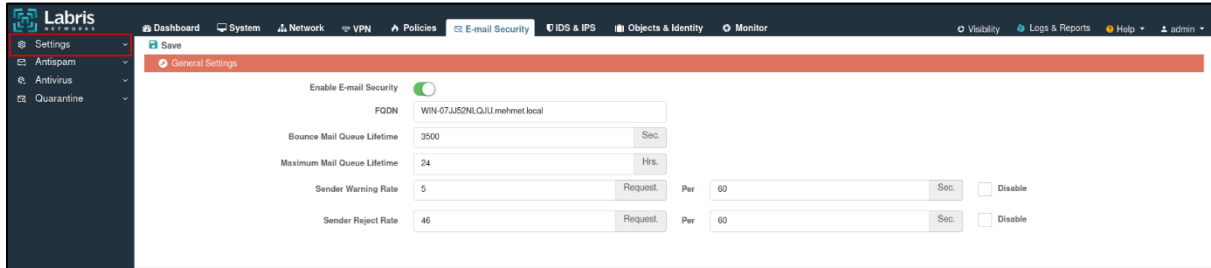
Labris UTM cihazının tarafından e-posta trafiğini korumak için kullanılır. E-posta trafiğini izler, filtreler ve kontrol eder, böylece zararlı yazılımların, spam'in ve diğer tehditlerin ağa ulaşmasını engeller.

Gelen ve giden e-posta mesajlarını filtreleyerek spam, kimlik avı, kötü amaçlı yazılım ve veri sızıntısı gibi çeşitli tehditleri önlemeye yardımcı olmaktadır.



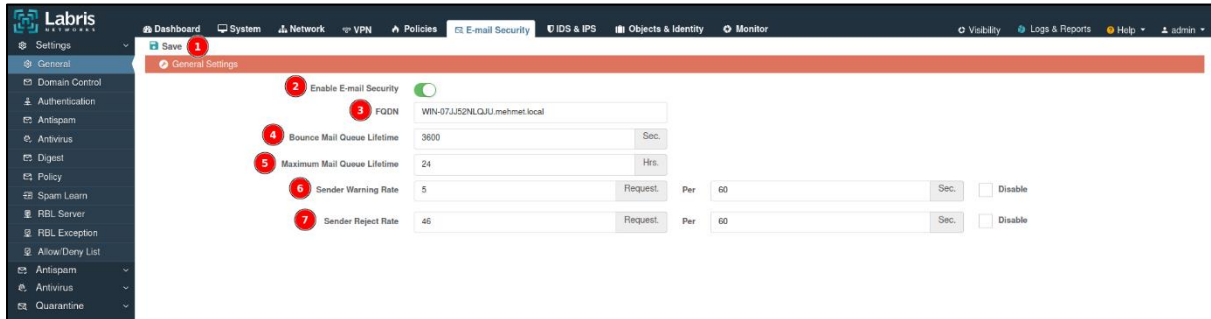
14.1 Ayarlar

İç ağda çalışan E-posta sunucusunun bilgilerinin düzenlendiği, spam, domain kontrolü, kimlik doğrulama, antispam, antivirüs, E-posta engellemesi, RBL sunucu ayarlarının yapıldığı bölümdür.



14.1.1 General

Labris UTM cihazındaki E-posta güvenliğinin genel ayarlarının yapıldığı modüldür.



1	Kaydet	E-Posta güvenliğinin ayarlarının kaydedildiği butondur.
---	---------------	---

2	E-Posta Güvenliğini Etkinleştir	E-Posta güvenliğinin etkinleştirildiği butondur.
3	Tam Nitelikli Alan Adı	Mail sunucusunun tam nitelikli alan adının girildiği bölümdür. ÖRN; 'mail.google.com'
4	Karşılıksız Posta Kuyruğu Bekleme Süresi	Geri dönen e-postaların(bounce messages) kuyrukta ne kadar süreyle bekletileceğini belirler. Bir geri dönen mesajın belirtilen süre içinde teslim edilememesi durumunda, mesaj teslim edilemiyor olarak kabul edilir ve kuyruktan silinir. Geri dönen mesajların belirtilen süre boyunca kuyrukta bekletilmesini sağlar.
5	Maksimum Posta Kuyruğu Bekleme Süresi	Bir mesajın kuyruğa alındıktan sonra ne kadar süreyle bekletilebileceğini belirlenir. Belirlenen süre sonunda teslim edilmeyen mesajlar geri gönderilir.
6	Gönderici Uyarı Oranı	Göndericilerin belirlenen süre içerisinde 5 adet eposta göndermesine izin verir ve limit aşıldığında ise göndericiye uyarı mesajı gönderirir.
7	Gönderici Red Oranı	Göndericilerin belirlenen süre içerisinde 5 adet e-posta göndermesine izin verir ve limiti aşan e postalar reddedilir.

14.1.2 Alan Adı Kontrolü

Mail sunucusunua gelen postaların alan adlarının kontrolünün yapıldığı modüldür.



1	Ekle	Alan adı kontrolünün ekleme işleminin yapıldığı butondur.
2	Kaydet	Eklene alan adı kontrol sunucusunun kaydedildiği

		bölümdür.
3	Vazgeç	Yapılan işlemlerden vazgeçildiği butondur.
4	Alan Adı	Eklenen alan adı kontrolü sunucusunun alan adının görüntülediği bölümdür.
5	SMTP Sunucusu	SMTP sunucusu bilgisinin görüntülediği bölümdür.
6	Port	SMTP sunucusunun port bilgisinin görüntülediği bölümdür.
7	Oturum Açma Gerekli	Yetkisiz girişlerin e-posta hesaplarına erişimini engellemek için kullanılır.
8	Yönet	Eklenen sunucunun düzenlendiği ve silindiği butonlar bulunur.

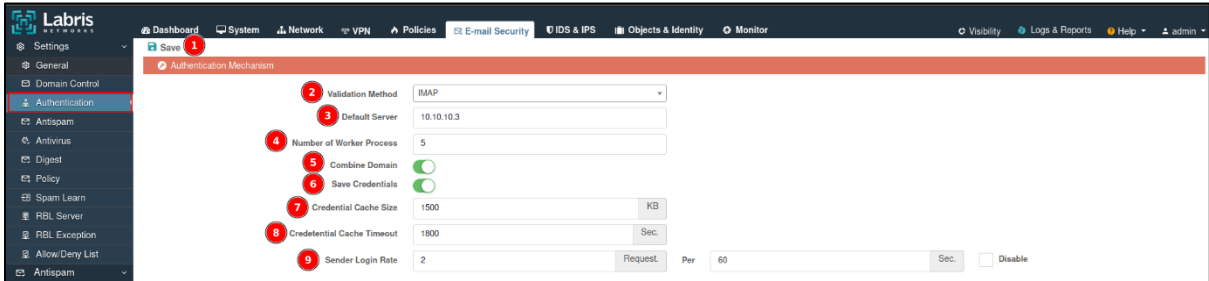
-Alan adı kontrol sunucusu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra çıkan penceredeki bilgiler doldurularak alan adı kontrol sunucu ekleme işlemi yapılır.

1	Alan Adı	Sunucunun alan adının girildiği bölümdür.
2	SMTP Server	SMTP sunucusunun alan adının girildiği bölümdür.
3	Server Port	Sunucunun port bilgisinin girildiği bölümdür.

4	Varsayılan Alan	Eklene sunucunun varsayılan alan olması gerektiği durumda açılır.
5	Oturum Açma Gerekli	Alan Adı kontrolü için oturum açmanın gerektiği durumlarda açılır.
6	Kaydet	Alan adı kontrolünün kaydedildiği butondur.
7	Kapat	'ekle' butonuna tıklanarak açılan pencerenin kapatıldığı butondur.

14.1.3 Kimlik Doğrulama

Mail sunucusuna gelen postaların kimlik doğrulama işleminin yapıldığı bölümdür. Yapılan kimlik doğrulama işlemi postayı gönderen kullanıcıların kimlik bilgileri doğrulanır.



1	Kaydet	Kimlik doğrulama ayarlarının kaydedildiği butondur.
2	Doğrulama Yöntemi	Doğrulama yönteminin yapılacağı protokol bilgisinin seçildiği bölümdür. Doğrulama yöntemi olarak POP3 ve IMAP protokolleri kullanılır.
3	Varsayılan Sunucu	İstemcilerin kimlik doğrulama isteklerinde bulunacağı sunucunun IP adresinin belirtildiği bölümdür.
4	İşçi İşlem Sayısı	Kimlik doğrulama işlemi sırasında aynı anda kaç işlemin gerçekleştirebileceğinin belirtildiği bölümdür.
5	Alanı Birleştir	Kimlik doğrulama mekanizmasına girmeden önce alanı giriş ile birleştirir.

6	Kimlik Kaydet	Bilgilerini	Kimlik doğrulama işlemi gerçekleştirilen istemcilerin kimlik bilgilerinin kaydedildiği bölümdür.
7	Kimlik Önbelleği Büyüklüğü	Bilgisi	Herbir işlem için maksimum bellek miktarının belirtildiği bölümdür.
8	Kimlik Önbelleği Aşımı	Bilgisi Zaman	Herbir kimlik doğrulama işlemi için geçici dosyaların ne kadar süreyle geçerli olacağını belirtildiği bölümdür.
9	Gönderici Oranı	Uyarı	Göndericilerin belirlenen süre(60 sn) içerisinde 2 adet istek göndermesine izin verir ve limit aşıldığında ise göndericiye uyarı mesajı gönderir.

14.1.4 Antispam

Mail sunucusuna gelen maillerin antispam olarak algılanması için gerek ayarların yapıldığı bölümdür.

The screenshot displays the 'Antispam Settings' page in the Labris Networks management interface. The page is divided into several sections: 'Antispam Settings' (containing 14 numbered items) and 'Report Options' (containing 4 numbered items). The 'Antispam Settings' section includes: 1. Save button, 2. Spam Tag Level Score (5.1), 3. Body Size Limit (204800 KB), 4. Mail Size Limit (40240000 MB), 5. Realtime Blackhole List (RBL) (checked), 6. Bayes (checked), 7. Bayes Auto Learn (unchecked), 8. Auto Whitelist (unchecked), 9. Reject Unknown Sender Domain (checked), 10. Reject Unknown Client Hostname (unchecked), 11. Reject Invalid Hello Hostname (unchecked), 12. Reject Non-FQDN Sender (checked), 13. Spam Mail Policy (Discard), 14. Bad Header Policy (Pass). The 'Report Options' section includes: 15. Warn Spam Sender (checked), 16. Modify Spam Mail Subject (unchecked), 17. Spam Subject Tag (***SPAM**), and 18. Spam Admin E-mail Address (spamalert@\$mydomain).

1	Kaydet	Antispam ayarlarının kaydedildiği butondur.
2	İstenmeyen E-Posta Etiketleme	Bir E-postanın spam olarak sınıflandırılması için gereken varsayılan puan eşliğini belirler. Bir e-postanın spam puanı bu eşliği geçerse, e-posta spam olarak

	Seviyesi Puanı	kabul edilir. '5.1' ayarlandığında, e-postalar 5.1 veya daha yüksek puan aldığından spam olarak değerlendirilir.
3	Gövde Büyüklüğü Sınırı	Spam analizi için işlenecek e-posta gövdesinin maksimum boyutunu belirtir. Bir e-postanın gövdesi bu boyut sınırını aşarsa içeriğin tamamını analiz etmez ve bazı kısımlarını atlar.
4	Posta Büyüklüğü Sınırı	Gelen E-postanın büyüklüğü limiti geçer ise gelen e-postayı spam olarak algılar ve engeller.
5	Gerçek Zamanlı Karadelik Listesi	Spam e-posta kontrolü için karadelik listesine bakarak engelleme yapılması istenildiği durumlarda etkinleştirildiği bölümdür.
6	Bayes	İstenmeyen e-postaları(spam) tespit etmek ve filtrelemek için etkinleştirilmesi gerekir. Etkinleştirildiği durumda ise e-posta mesaj içeriğini analiz ederek, spam ve istenilen e-postalar arasında ayırım yapar.
7	Bayes Otomatik Öğrenme	Bayes otomatik öğrenmenin açılması durumunda, kullanıcının işaretlediği e-postalara göre öğrenerek spam filtrelemesini sürekli olarak geliştirir
8	Otomatik Beyaz Liste	Güvenilir e-posta adreslerinden gelen iletilerin spam filtresi tarafından yanlışlıkla engellenmesini önleyerek kullanıcıların önemli mesajları spam olarak algılanmasını sağlar.
9	Bilinmeyen Gönderici Alanını Reddet	Gelen postasının alan adının çözülmediği veya bilinmediği durumda göndericinin postasını engeller.
10	Bilinmeyen İstemci Sunucu İsmi Reddet	Gelen postasının sunucu isminin çözülmediği veya bilinmediği durumda gönderici tarafından gelen postayı engeller.
11	Geçerli Olmayan Helo Sunucu	E-posta sunucusu Helo komutu ile kendini tanıtırken geçersiz bir sunucu adı kullanılmadığı durumda

	İsimini Reddet	gelen e-postayı engeller.
12	Tam Nitelikli Alan Adı Olmayan(Non-FQDN) Göndericiyi Reddet	E-posta sunucusunun gönderici alan adının tam nitelikli bir alan adı olmadığına gelen e-postayı engeller.
13	İstenmeyen Posta Politikası	Antispam olarak algılanan e-postaların engelleme sırasında yapılan işlem belirtilir. Belirlenen işlemler Engelle(Göndereni uyarma), R, Engelle(Gönderene Raport Et) veya Engelleme şeklindedir.
14	Kötü Başlık Politikası	Gelen e-postanın başlığını kontrol ederek spam olarak algıladığı e-postayı engeller, reddeter veya engellemez.
15	İstenmeyen Posta Göndericisini Uyar	Spam olarak algılanan posta göndericisini uyarma işleminin yapılır.
16	İstenmeyen Posta Konusu Değiştir	Spam olarak algılanan postanın konusunun değiştirilir.
17	İstenmeyen Posta Konusu Etiket	Spam olarak algılanan postanın konusunun etiketinin değiştirildiği bölümdür.
18	İstenmeyen Posta Yöneticisi E-Posta Adresi	Spam olarak algılanan e-postaların gönderileceği adresinin girildiği bölümdür.

14.1.5 Antivirüs

Mail sunucusuna gelen maillerin virüs olarak algılanması için gerek ayarların yapıldığı bölümdür. Gelen maillerin virus olarak algılandığı durumlarda gönderen ve alıcıyı uyarır.

1	Kaydet	Yapılan antivirus ayarlarının kaydedildiği bölümdür.
2	Maksimum İşlem Sayısı	Antivirüs taramasının işlem sayısının belirtildiği bölümdür.
3	Kayıt Seviyesi	Virüs olarak tespit edilen maillerin kayıt seviyesi seçilir.
4	Maksimum Derinlik Seviyesi	Dosya veya arşiv taranması durumunda ne kadar derine inileceğın belirtildiği bölümdür. 1-20 arasında derinlik seviyesi girilmektedir.
5	Maksimum Çıkarılan Dosya Sayısı	Gelen e-postada sıkıştırılmış dosyalar veya arşivler taranırken ya açılırken kaç dosyanın taranacağıın belirtildiği bölümdür.
6	Virüslü Posta Politikası	Virüs olarak algılandığı durumda uygulanacak politika seçilir.
7	Yasaklanmış Politika	Yasaklanmış politikaya takılan e-postalar için uygulanacak politikanın seçildiği bölümdür.

8	Göndericiye Haber Ver	Virüs olarak algılanan e-postaları için göndericiye mail gönderildiği bölümdür.
9	Alıcıya Haber Ver	Virüs olarak algılanan e-postaları için alıcıya mail gönderildiği bölümdür.
10	İstenmeyen Posta Yöneticisi E-Posta Adres	İstenmeyen postanın gönderileceği adresin girildiği bölümdür.
11	Başlık Satırı	Gönderilecek postanın başlık bilgisinin girildiği bölümdür.
12	Başlık Etiketleri	Gönderilecek postanın başlık etiketi bilgisinin girildiği bölümdür.

14.1.6 Karantina Özet

Labris UTM cihazında karantinaya alınan maillerin özetinin gönderildiği bölümdür.

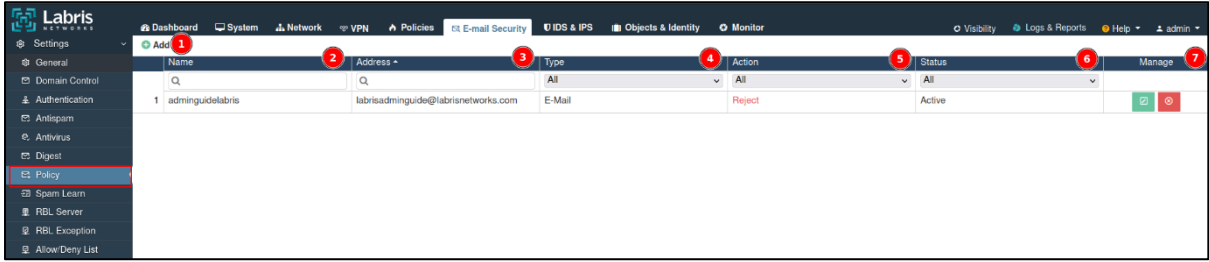
1	Kaydet	Karantina Özet ayarlarının kaydedildiği bölümdür.
2	Şirket Adı	Karantina özet maili gönderilecek olan şirketin adının girildiği bölümdür.

3	Özet Ağ Adresi	Karantina özel sunucusunun ağ adresinin girildiği bölümdür.
4	Posta Göndericisi Adı	Karantina özet olarak gönderilen postanın gönderici adresinin girildiği bölümdür.
5	Posta Göndericisi Adresi	Karantina özet olarak gönderilen posta adresinin girildiği bölümdür.
6	Posta Konusu	Karantina özet olarak gönderilecek postanın konusunun girildiği bölümdür.
7	Kontrol Frekansı	Karantinaya alınan e-postalar hakkında kullanıcıya ne sıklıkla özet rapor gönderileceğinin belirtildiği bölümdür.
8	Varsayılan Hesap Abonelik Frekansı	Bir kullanıcının belirli bir hizmete veya sisteme kaydolduğunda e-posta bildirimlerini veya raporlarını ne sıklıkta alacağını belirleyen başlangıç ayarıdır
9	Varsayılan Oturum Ömrü	Karantina Özet raporunun görüntülenmesi, alınması veya yönetilmesi sırasında kullanılan oturumun ne kadar süre boyunca aktif kalacağını belirtildiği bölümdür.
10	Ağ İsteği Oturum Ömrü	Karantina Özet raporunun oluşturulması veya alınması sırasında kullanılan oturumun ne kadar süre boyunca aktif kalacağı sürenin belirtildiği bölümdür.
11	Son Karantina Zamanı	Karantina Özet raporunda karantinaya alınan son e-postanın veya mesajın zamanını ifade eder.
12	Varsayılan Düzen	Karantina Özet raporunun oluşturulduğunda veya kullanıcıya gönderildiğinde sahip olduğu standard formatının belirtildiği bölümdür.
13	Posta İmzası	Karantina Özet olarak gönderilecek raporun posta imzasının girildiği bölümdür.

14	Şifre Değişimi İçin Posta Konusu	Şifre değişimi için gerekli bilgilerin girildiği bölümdür.
15	Yönlendirilen E-posta için Posta Konusu	Yönlendirilen E-posta için posta konusunun girildiği bölümdür.

14.1.7 Politika

Labris UTM cihazında tanımlanan kurallar görüntülenir alan adı veya e-posta adresine kural yazarak engellene veya izin verme işleminin yapıldığı bölümdür.



1	Ekle	Politika ekleme işleminin yapıldığı butondur.
2	İsim	Yazılan politika isimlerinin görüntülediği bölümdür.
3	Adres	Yazılan politika adreslerinin görüntülediği bölümdür.
4	Tip	Yazılan politikaların tipinin görüntülediği bölümdür. Tip olarak Alan Adı ve E-posta bulunur.
5	Eylem	Yazılan politikanın eylem bilgisinin görüntülediği bölümdür. Eylem olarak izin verir veya engeller.
6	Durum	Yazılan politikanın durumun bilgisi görüntülenir.
7	Yönet	Yazılan kuralın silindiği veya düzenlendiği bölümdür.

-Politika eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıkladıktan sonra yazılacak politikanın tipi 'e-mail' seçilemesi durumunda e-mail adresine göre engelleme veya izin verilecek kural yazılır.

1	Etkinleştir	Yazılacak politikanın etkinleştirildiği butondur.
2	İsim	Yazılacak politikanın isminin girildiği bölümdür.
3	Tip	Politikanın tipi seçilir ve seçilen tipe göre politika yazılır.
4	E-Mail	Tipin 'e-mail' seçilmesi durumunda engellenecek veya izin verilecek e-mail adresi yazılır.
5	Mesaj	Yazılan kural ile ilgili mesaj bilgisinin girildiği bölümdür.
6	Eylem	Yazılacak politikanın eylemi seçilir. Girilen e-mail adresinden posta gelicekse izin ver seçilir. Eğer girilen e-mail adresinden posta gelmeyecek ise engelle seçilir.
7	Kaydet	Yazılan kuralın kaydedildiği bölümdür.
8	Kapat	Ekle butonuna tıklayarak açılan ekranın kapatıldığı butondur.

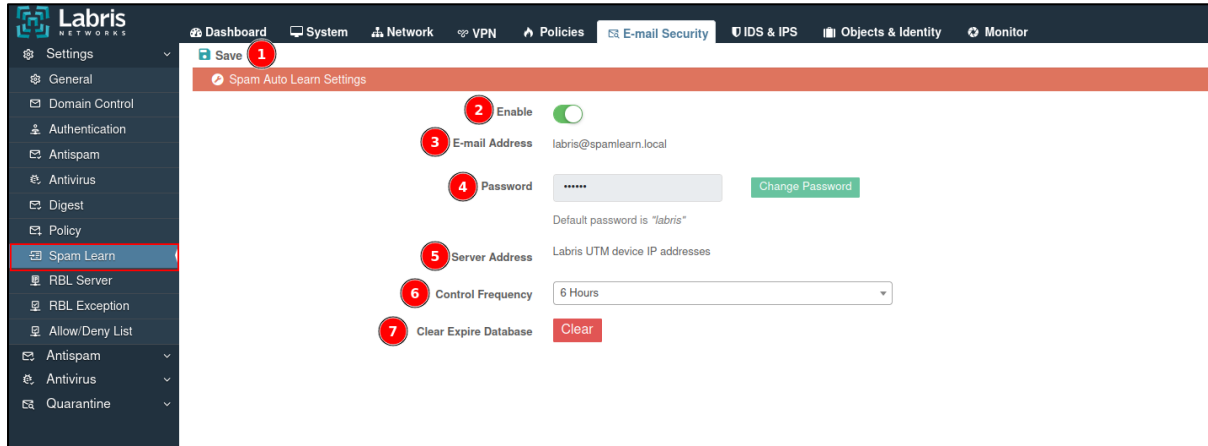
-Politika eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıkladıktan sonra yazılacak politikanın tipi 'alan adı' seçilmesi durumunda e-mail adresine göre engelleme veya izin verilecek kural yazılır.

1	Etkinleştir	Yazılacak politikanın etkinleştirildiği butondur.
2	İsim	Yazılacak politikanın isminin girildiği bölümdür.
3	Tip	Politikanın tipi seçilir ve seçilen tipe göre politika yazılır.
4	Alan Adı	Tipin 'Alan Adı' seçilmesi durumunda engellenecek veya izin verilecek alan adı adresi yazılır.
5	Mesaj	Yazılan kural ile ilgili mesaj bilgisinin girildiği bölümdür.
6	Eylem	Yazılacak politikanın eylemi seçilir. Girilen alan adı adresinden posta gelicekse izin ver seçilir. Eğer girilen alan adı adresinden posta gelmeyecek ise engelle seçilir.
7	İstisnalar	Alan adına ait olan mail adreslerinden posta gelmesi durumunda istisana olarak tanımlamak gerekmektedir.
7	Kaydet	Yazılan politikanın kaydedildiği bölümdür.

8	Kapat	Ekle butonuna tıklayarak açılan ekranın kapatıldığı butondur.
---	--------------	---

14.1.8 Spam Öğrenme

E-posta güvenliğindeki spam öğrenmesi için gerekli ayarların yapıldığı bölümdür.



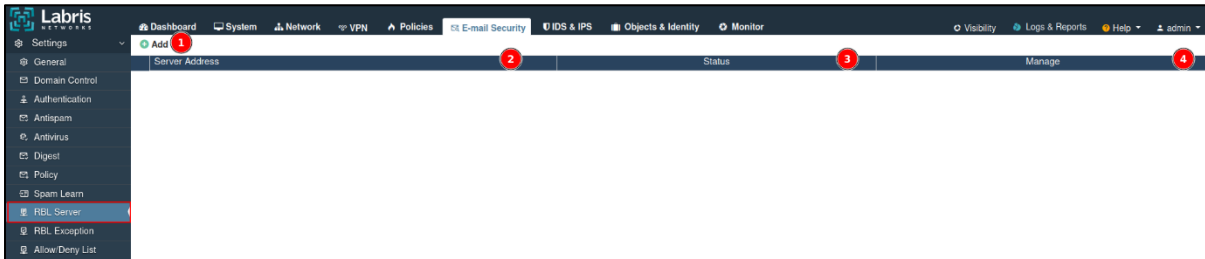
1	Kaydet	Spam öğrenmenin kaydedildiği butondur.
2	Etkinleştir	Spam öğrenmenin etkinleştirildiği butondur.
3	E-Posta Adresi	Spam öğrenmesi için girilen e-posta adresinin görüntülediği bölümdür.
4	Şifre	Spam öğrenmesi için tanımlanan şifrenin değiştirildiği bölümdür.
5	Sunucu Adresi	Spam öğrenme için sunucu adresinin görüntülediği bölümdür.
6	Kontrol Frekansı	Spam öğrenmesi için sunucunun kontrol frekansının seçildiği bölümdür.
7	Süresi Dolmuş Veritabanını Temizle	Süresi dolan ve spam olarak algılanan mail adreslerinin veri tabanından temizlendiği butondur.

14.1.9 RBL Sunucusu

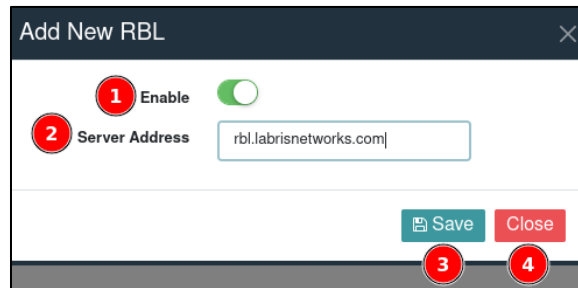
RBL Sunucu, e-posta sunucularının spam ve diğer istenmeyen e-postaları engellemek için kullandıkları kara liste sunucusudur. Genellikle spam gönderen IP adreslerini ve alan adlarını barındırır ve e-posta sunucuları bu listeyi kullanarak gelen e-postaların kaynağını doğrular.

E-posta sunucularının spam göndericileri tespit etmek ve engellemek için anlık olarak başvurduğu veri tabanıdır.

Labris UTM cihazında RBL sunucu tanımlamasının yapıldığı bölümdür.



1	Ekle	RBL Sunucu ekleme işleminin yapıldığı butondur.
2	Etkinleştir	RBL Sunucunun sunucu adreslerinin görüntülendiği bölümdür.
3	Durum	Eklene RBL sunucunun durumunun görüntülendiği bölümdür.
4	Yönet	Eklene RBL sunucunun düzenleme veya silme işlemlerinin yapıldığı bölümdür.



1	Etkinleştir	RBL Sunucunun etkinleştirildiği butondur.
2	Sunucu Adresi	RBL Sunucunun sunucu adresinin girildiği bölümdür.

3	Kayde	Eklenecek RBL sunucu adreslerinin kaydedildiği bölümdür.
4	Kapat	Ekle butonuna tıklayarak açılan pencerenen kaydedilmeden kapatıldığı butondur.

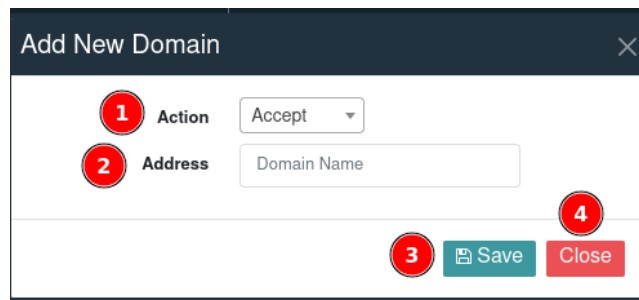
14.1.10 RBL Ayrıcalıkları

RBL sunucunun listesinde bulunan alan adı adreslerinden posta alınması için kullanılır.



1	Ekle	RBL Ayrıcalıkları ekleme işleminin yapıldığı butondur.
2	Sunucu Adresi	RBL Ayrıcalık olarak eklenen sunucuların alan adlarının görüntülediği bölümdür.
3	Durum	RBL Ayrıcalık olarak eklenen sunucunun durumunun görüntülediği bölümdür.
4	Yönet	Eklenen sunucunun silindiği veya düzenlendiği bölümdür.

-RBL ayrıcalık olarak alan adı eklemek için 'ekle' butonuna tıklanarak ekleme işlemi yapılır.

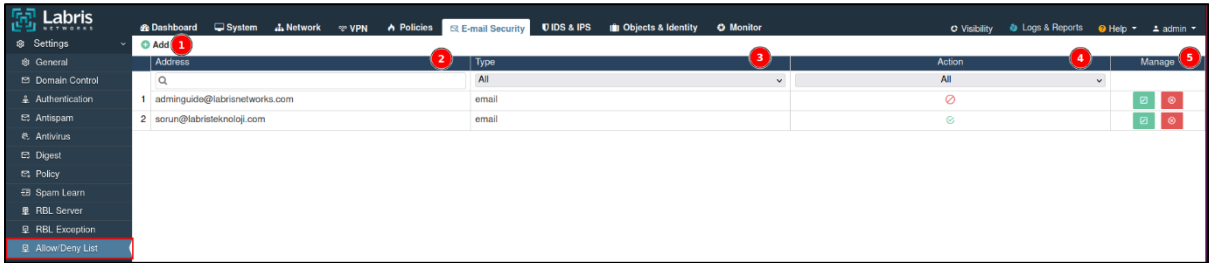


1	Eylem	RBL sunucu listesinde bulunan ve ayrıcalık olarak
---	--------------	---

		eklenen sunucu adresinden gelen postalar için uygulanacak eylemin belirtildiği bölümdür.
2	Adres	RBL Ayrıcalık olarak eklenen alan adının girildiği bölümdür.
3	Kaydet	RBL Ayrıcalıklarının kaydedildiği butondur.
4	Kapat	Ekle butonuna tıklayarak açılan pencerenin kaydedilmeden kapatıldığı butondur.

14.1.11 İzin Ver/Reddet Listesi

Alan adı ve e-posta adreslerinden gelen postalara izin verildiği veya reddedildiği modüldür.



1	Ekle	İzin verilen/reddedilen alan adının veya e-posta adreslerinin ekleme işleminin yapıldığı butondur.
2	Adres	Eklene alan adlarının veya e-posta adreslerinin görüntülediği bölümdür.
3	Tip	İzin verilen/reddedilen mail adreslerinin tipinin görüntülediği bölümdür.
4	Eylem	Eklene posta adreslerinin eylemlerinin görüntülediği bölümdür.
5	Yönet	Eklene posta adreslerinin düzenlendiği veya silindiği bölümdür.

-İzin verilecek/engellenecek mail adresleri eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıkladıktan sonra yazılacak politikanın tipi 'e-posta adresi' seçilmesi durumunda e-posta adresine göre engelleme veya izin verilecek kural yazılır.

The screenshot shows the 'Edit Allow/Deny' dialog box with the following settings:

- 1 Type:** Domain, E-mail Address
- 2 Address:** adminguide@labrisnetworks.com
- 3 Action:** Allow, Deny
- Sub Domain Control
- 4 Save** button
- 5 Close** button

1	Tip	Yazılacak olan kuralın tip seçilir.
2	Adres	Tipin 'e-posta adresi' seçilmesi durumunda engellenecek veya izin verilecek e-posta adresi yazılır.
3	Eylem	Yazılacak politikanın eylemi seçilir. Girilen e-mail adresinden posta gelecekse izin ver seçilir. Eğer girilen e-mail adresinden posta gelmeyecek ise engelle seçilir.
4	Kaydet	Eklenen kuralın kaydedildiği butondur.
5	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

-İzin verilecek/engellenecek mail adresleri eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıkladıktan sonra yazılacak politikanın tipi 'alan adı' seçilmesi durumunda alan adı adresine göre engelleme veya izin verilecek kural yazılır.

The screenshot shows the 'Edit Allow/Deny' dialog box with the following settings:

- 1 Type:** Domain, E-mail Address
- 2 Address:** sorun@labristeknoloji.com
- 3 Action:** Allow, Deny
- Sub Domain Control
- 4** (checkbox)
- 5 Save** button
- 6 Close** button

1	Tip	Yazılacak olan kuralın tip seçilir.
2	Adres	Tipin 'Alan Adı' seçilmesi durumunda engellenecek veya izin verilecek alan adı adresi yazılır.
3	Eylem	Yazılacak politikanın eylemi seçilir. Girilen alan adına ait bir posta adresinden posta gelicekse izin ver seçilir. Eğer girilen alan adı adresinden posta gelmeyecek ise engelle seçilir.
4	Alt Alan Adı Kontrolü	Etkinleştirildiğinde alan adına ait alt alan adlarının kontrolünün yapıldığı butondur.
5	Kaydet	Eklenecek kuralın kaydedildiği butondur.
6	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

14.2 Antispam

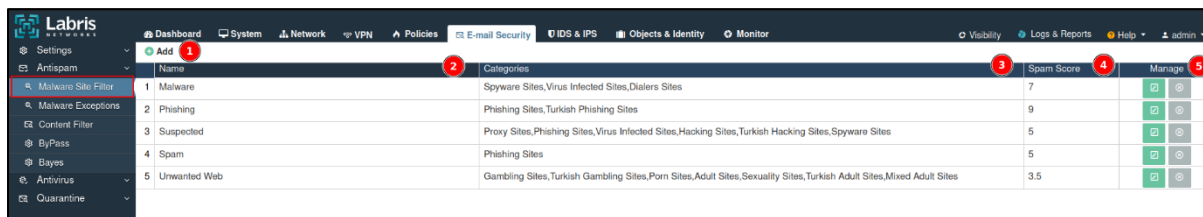
Mail sunucunuza gelen istenmeyen e-postaları tanımlamak, filtrelemek ve engellemek amacıyla kullanılan modüldür.



Name	Categories	Spam Score	Manage
1 Malware	Spyware Sites,Virus Infected Sites,Dialers Sites	7	<input type="checkbox"/> <input type="checkbox"/>
2 Phishing	Phishing Sites,Turkish Phishing Sites	9	<input type="checkbox"/> <input type="checkbox"/>
3 Suspected	Proxy Sites,Phishing Sites,Virus Infected Sites,Hacking Sites,Turkish Hacking Sites,Spyware Sites	5	<input type="checkbox"/> <input type="checkbox"/>
4 Spam	Phishing Sites	5	<input type="checkbox"/> <input type="checkbox"/>
5 Unwanted Web	Gambling Sites,Turkish Gambling Sites,Porn Sites,Adult Sites,Sexuality Sites,Turkish Adult Sites,Mixed Adult Sites	3.5	<input type="checkbox"/> <input type="checkbox"/>

14.2.1 Web Site Filtresi

Web site filtresi, kullanıcıların ziyaret ettiği web sitelerinin içeriklerini ve alan adlarını tarayarak, spam, phishing, kötü amaçlı yazılım veya diğer tehditleri içeren siteleri tespit ederek bu alan adlarından gelen mailleri engeller.



Name	Categories	Spam Score	Manage
1 Malware	Spyware Sites,Virus Infected Sites,Dialers Sites	7	<input type="checkbox"/> <input type="checkbox"/>
2 Phishing	Phishing Sites,Turkish Phishing Sites	9	<input type="checkbox"/> <input type="checkbox"/>
3 Suspected	Proxy Sites,Phishing Sites,Virus Infected Sites,Hacking Sites,Turkish Hacking Sites,Spyware Sites	5	<input type="checkbox"/> <input type="checkbox"/>
4 Spam	Phishing Sites	5	<input type="checkbox"/> <input type="checkbox"/>
5 Unwanted Web	Gambling Sites,Turkish Gambling Sites,Porn Sites,Adult Sites,Sexuality Sites,Turkish Adult Sites,Mixed Adult Sites	3.5	<input type="checkbox"/> <input type="checkbox"/>

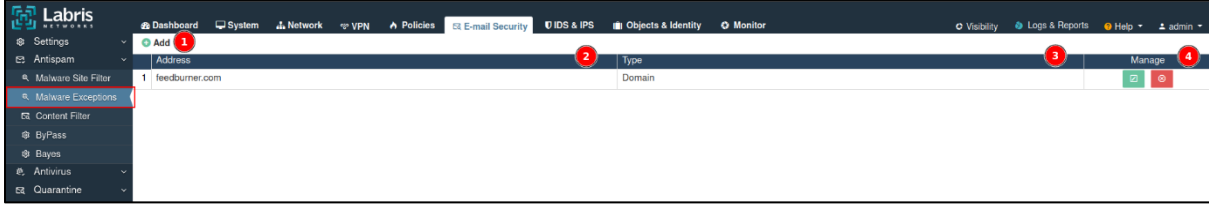
1	Ekle	Web site filtresi eklemek için kullanılan butondur.
2	İsim	Eklenen web site filtresinin isminin görüntülediği bölümdür.
3	Kategoriler	Eklenen web site filtresinin bulunduğu kategorilerin görüntülediği bölümdür.
4	İstenmeyen Posta Puanı	İstenmeyen posta olarak sayılacak postanın puanının görüntülediği bölümdür.
5	Yönet	Web site filtresinin silindiği veya düzenlendiği bölümdür.

-Web site filtresi eklemek için 'ekle' butonuna tıklayarak web site filtresi eklenir.

1	İsim	Web site filtresi isminin girildiği bölümdür.
2	Kategoriler	Web site filtresi kuralı için eklenecek kategorilerin seçildiği bölümdür. Birden fazla kategori eklenebilir.
3	İstenmeyen Posta Puanı	İstenmeyen posta puanının girildiği bölümdür.
4	Kaydet	Eklenen Web site filtresinin kaydedildiği butondur.
5	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı bölümdür.

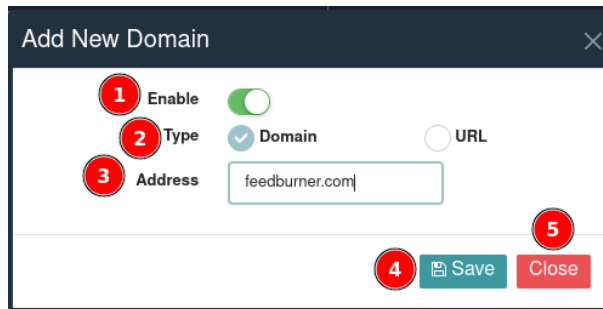
14.2.2 Web Site İstisnaları

Eklenecek web site filtresindeki kategorilerde bulunan bir alan adından mail gelmesi gerektiği durumlarda istisna olarak eklendiği modüldür.



1	Ekle	İstisna olarak alan adı veya url eklemesi için kullanılan butondur.
2	Adres	Eklenecek istisna adreslerinin görüntülediği bölümdür.
3	Tip	Eklenecek istisna adreslerinin tipinin görüntülediği bölümdür.
4	Yönet	Eklenecek istisna adreslerinin düzenlendiği veya silindiği bölümdür.

-İstisna olarak alan adı veya url eklemek için 'ekle' butonuna tıklayarak istisna olarak alan adı veya url eklenir. Tipin alan seçilmesi durumunda alan adı girilerek istisna tanımlanır.



1	Etkinleştir	İstisna olarak eklenecek adresin etkinleştirildiği butondur.
2	Tip	İstisna olarak eklenecek adresin tipinin seçildiği bölümdür.
3	Adres	Tipin 'alan adı' seçilmesi durumunda alan adının girildiği bölümdür.

4	Kaydet	İstisna olarak eklenen adreslerin kaydedildiği butondur.
5	Kapat	Ekle butonuna tıklanarak açılan pencerenin kapatıldığı butondur. Kapat butonuna tıklaması ile yapılan işlem kaydedilmez.

-İstisna tipinin 'URL' seçilmesi durumunda URL adresi girilerek istisna tanımlanır.

1	Etkinleştir	İstisna olarak eklenecek adresin etkinleştirildiği butondur.
2	Tip	İstisna olarak eklenecek adresin tipinin seçildiği bölümdür.
3	Adres	Tipin 'URL' seçilmesi durumunda alan adının girildiği bölümdür.
4	Kaydet	İstisna olarak eklenen adreslerin kaydedildiği butondur.
5	Kapat	Ekle butonuna tıklanarak açılan pencerenin kapatıldığı butondur. Kapat butonuna tıklaması ile yapılan işlem kaydedilmez.

14.2.3 İçerik Filtreleme

E-posta iletişimindeki içeriği analiz ederek, spam, zararlı yazılım, phishing ve diğer istenmeyen veya zararlı içeriklerin tespit edilmesi veya engellenme işleminin yapıldığı modüldür.

Name	Description	Rule Type	Test Type	Score	Manage
1 ALL 1	deny from all alias	header	normal	20	[Edit] [Delete]
2 HABERINIZCOM	haberinizcom	header	normal	20	[Edit] [Delete]
3 IPORIGTR1	iporigtr	header	normal	10	[Edit] [Delete]
4 KOMPLO_TEORI_01	ekomploteorilerigooglegroups	header	normal	20	[Edit] [Delete]
5 LMC_NOT_A_SPAM	not a spam	header	normal	-2000	[Edit] [Delete]
6 NO_SMTPT_AUTH		header	metamatch		[Edit] [Delete]
7 SMTPT_AUTH	Message sent using SMTP Authentication	meta	normal	-12	[Edit] [Delete]
8 VIRUS_UYARI	Virusuyari	header	normal	20	[Edit] [Delete]
9 VIRUS_WARNING1	UNHELPPFUL	header	normal	20	[Edit] [Delete]
10 VIRUS_WARNING15	Unhelpful MailScanner 'virus warning' (15)	header	normal	20	[Edit] [Delete]
11 VIRUS_WARNING158	Unhelpful Declude 'virus warning' (158)	header	normal	20	[Edit] [Delete]
12 VIRUS_WARNING19	Unhelpful Norton AntiVirus 'virus warning' (19)	header	normal	20	[Edit] [Delete]
13 VIRUS_WARNING45	Unhelpful 'virus warning' (45)	header	normal	20	[Edit] [Delete]
14 VIRUS_WARNING50	Unhelpful 'virus warning' (50)	header	normal	20	[Edit] [Delete]
15 VIRUS_WARNING57	Unhelpful 'virus warning' (57)	header	normal	20	[Edit] [Delete]
16 VIRUS_WARNING60	Unhelpful 'virus warning' (60)	header	normal	20	[Edit] [Delete]
17 VIRUS_WARNING61	Unhelpful 'virus warning' (61)	header	normal	20	[Edit] [Delete]
18 VIRUS_WARNING7	Unhelpful 'virus warning' (7)	header	normal	20	[Edit] [Delete]

1	Ekle	İçerik Filtreleme kuralının eklendiği butondur.
2	İsim	İçerik filtreleme kuralına verilen isminin görüntülediği bölümdür.
3	Açıklama	Eklenecek içerik filtreleme kuralının açıklamasının görüntülediği bölümdür.
4	Kural Tipi	Eklenecek içerik filtreleme kuralının kural tipinin görüntülediği bölümdür.
5	Test Tipi	Eklenecek içerik filtreleme kuralının test tipinin görüntülediği bölümdür.
6	Puan	Eklenecek içerik filtreleme kuralının puanının görüntülediği bölümdür.
7	Yönet	Eklenecek içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.

-İçerik Filtreleme kuralı ekleme için 'ekle' butona tıklanır. Kural tipi seçilerek kural tipine göre içerik filtreleme kuralı yazılır.

- Kural tipi Başlık seçilmesi durumunda Başlık tipi seçilerek içerik filtreleme kuralı yazılır.

Content Filter Rule

1 Name: ALL1

2 Description: Description

3 Score: 20

4 Rule Type: Header

5 Header Type: From

6 Test Type: Normal For Test Meta Match

7 Entry Type: Word Regex

8 Words: *.all@labristeknoloji.com.*

9 Match: Only This Word Any Word Repeat Count

10 Not Include Rule:

11 Case Insensitive:

12 Save 13 Close

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	İçerik filtreleme kuralının kural tipinin seçildiği bölümdür.
5	Başlık Tipi	İçerik filtreleme kuralının başlık tipinin seçildiği bölümdür.
6	Test Tipi	Spam e-postları veya istenmeyen içerikleri tespit etmek için kullanılan test tipinin seçildiği bölümdür.
7	Giriş Tipi	Eklenecek içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.

8	Sözcükler	İçerik bilgisinin girildiği bölümdür. Burada içerik olarak filtrelenecek sözcük veya regex url girilir.
9	Eşleştir	Yazılan içerik kelimesiyle eşleştiği durumda filtreleme işlemi yapar. Bütün kelimeleri içerik eşletirir veya yazılan sözcüğe göre eşleşmeleri sayar.
10	Kuralı Dahil Etme	Kuralı dahil edilmemesi durumlar işaretlendiği bölümdür.
11	Büyük/Küçük Harf Duyarsız	Büyük/küçük harf duyarsız olması istenilen durumlarda kullanılır.
12	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
13	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

- Kural tipi Gövde seçilmesi durumunda e-postanın gövdesi kontrol eden içerik filtreleme kuralı yazılır.

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
---	-------------	---

2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	İçerik filtreleme kuralının kural tipinin seçildiği bölümdür.
5	Test Tipi	Spam e-postları veya istenmeyen içerikleri tespit etmek için kullanılan test tipinin seçildiği bölümdür.
6	Giriş Tipi	Eklenen içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.
7	Sözcükler	İçerik bilgisinin girildiği bölümdür. Burada içerik olarak filtrelenecek sözcük veya regex url girilir.
8	Eşleştir	Yazılan içerik kelimesiyle eşleştiği durumda filtreleme işlemi yapar. Bütün kelimeleri içerik eşletirir veya yazılan sözcüğe göre eşleşmeleri sayar.
9	Büyük/Küçük Harf Duyarsız	Büyük/küçük harf duyarsız olması istenilen durumlarda kullanılır.
10	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
11	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

- Kural tipi Ham Gövde seçilmesi durumunda e-postanın gövdesi kontrol eden içerik filtreleme kuralı yazılır.

Content Filter Rule

1 Name: LABRIS_WARNING

2 Description: Description

3 Score: 20

4 Rule Type: Raw Body

5 Test Type: Normal For Test Meta Match

6 Entry Type: Word Regex

7 Words:

8 Match: Only This Word Any Word Repeat Count

9 Case Insensitive:

10 Save 11 Close

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	İçerik filtreleme kuralının kural tipinin seçildiği bölümdür.
5	Test Tipi	Spam e-postları veya istenmeyen içerikleri tespit etmek için kullanılan test tipinin seçildiği bölümdür.
6	Giriş Tipi	Eklenecek içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.
7	Sözcükler	İçerik bilgisinin girildiği bölümdür. Burada içerik olarak filtrelenecek sözcük veya regex url girilir.
8	Eşleştir	Yazılan içerik kelimesiyle eşleştiği durumda filtreleme işlemi yapar. Bütün kelimeleri içerik eşletirir veya

		yazılan sözcüğe göre eşleşmeleri sayar.
9	Büyük/Küçük Harf Duyarsız	Büyük/küçük harf duyarsız olması istenilen durumlarda kullanılır.
10	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
11	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

- Kural tipi URI seçilmesi durumunda URI bilgilerini kontrol eden içerik filtreleme kuralı yazılır.

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	İçerik filtreleme kuralının kural tipinin seçildiği bölümdür.

5	Test Tipi	Spam e-postları veya istenmeyen içerikleri tespit etmek için kullanılan test tipinin seçildiği bölümdür.
6	Giriş Tipi	Eklenecek içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.
7	Sözcükler	İçerik bilgisinin girildiği bölümdür. Burada içerik olarak filtrelenecek sözcük veya regex url girilir.
8	Eşleştir	Yazılan içerik kelimesiyle eşleştiği durumda filtreleme işlemi yapar. Bütün kelimeleri içerik eşletirir veya yazılan sözcüğe göre eşleşmeleri sayar.
9	Büyük/Küçük Harf Duyarsız	Büyük/küçük harf duyarlı olması istenilen durumlarda kullanılır.
10	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
11	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

- Kural tipinin Tamamı seçilmesi durumunda e-postanın tamamını kontrol eden içerik filtreleme kuralı yazılır.

Content Filter Rule

1 Name: LABRIS_WARNING

2 Description: Description

3 Score: 20

4 Rule Type: Full

5 Test Type: Normal For Test Meta Match

6 Entry Type: Word Regex

7 Words:

8 Match: Only This Word Any Word Repeat Count

9 Case Insensitive:

10 Save 11 Close

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	İçerik filtreleme kuralının kural tipinin seçildiği bölümdür.
5	Test Tipi	Spam e-postları veya istenmeyen içerikleri tespit etmek için kullanılan test tipinin seçildiği bölümdür.
6	Giriş Tipi	Eklenecek içerik filtreleme kuralının düzenlendiği veya silindiği bölümdür.
7	Sözcükler	İçerik bilgisinin girildiği bölümdür. Burada içerik olarak filtrelenecek sözcük veya regex url girilir.
8	Eşleştir	Yazılan içerik kelimesiyle eşleştiği durumda filtreleme işlemi yapar. Bütün kelimeleri içerik eşletirir veya yazılan sözcüğe göre eşleşmeleri sayar.
9	Büyük/Küçük Harf Duyarsız	Büyük/küçük harf duyarsız olması istenilen durumlarda kullanılır.
10	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
11	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

- Kural tipi Meta seçilmesi durumunda Meta bilgisini kontrol eden içerik filtreleme kuralı yazılır.

Content Filter Rule

1 Name LABRIS_WARNING

2 Description Description

3 Score 20

4 Rule Type Meta

5 Exceptions

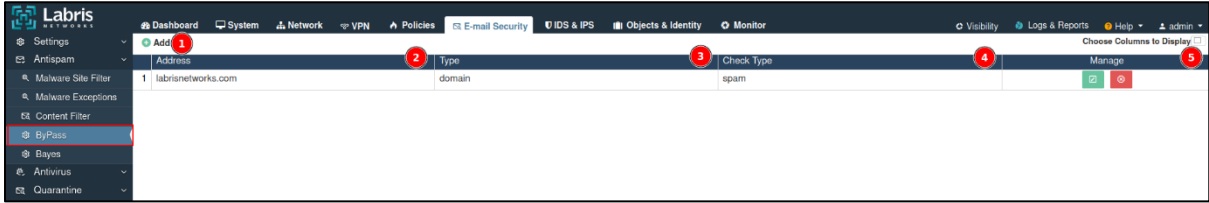
IPORGTR1 and +

6 Save Close 7

1	İsim	İçerik filtreleme kuralının isminin girildiği bölümdür.
2	Açıklama	İçerik filtreleme kuralının açıklamasının girildiği bölümdür.
3	Puan	İçerik filtreleme kuralının istenmeyen posta puanının girildiği bölümdür.
4	Kural Tipi	Eklenecek içerik filtreleme kuralının kural tipinin görüntülediği bölümdür.
5	İstisna	Yazılan kurallara istisna tanımlanmasının yapıldığı bölümdür.
6	Kaydet	İçerik filtreleme kuralının kaydedildiği butondur.
7	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur. Pencere kapatıldığında yapılan değişiklikler kaydedilmez.

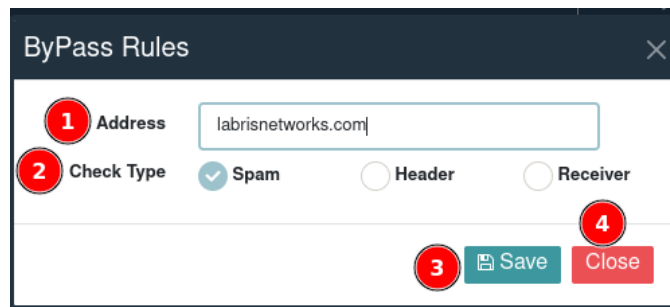
14.2.4 Hariç Bırak

Spam olarak algılanmaması gereken E-posta adreslerinin görüntülediği veya istenmeyen posta olarak algılanmaması gereken IP adreslerinin ekleme işleminin yapıldığı modüldür.



1	Ekle	Spam olarak algılanmaması gereken mail adreslerinin eklendiği bölümdür.
2	Adres	Eklenecek mail adreslerinin adres bilgisinin görüntülediği bölümdür.
3	Tip	Eklenecek mail adreslerinin adres tipi görüntülenir.
4	Tipi Kontrol Et	Eklenecek mail adreslerinin kontrol tipinin görüntülediği bölümdür.
5	Yönet	Ekleme mail adreslerinin düzenlendiği veya silindiği bölümdür.

-Spam olarak algılanmaması gereken domain adresi eklemek için 'ekle' butonuna tıklayarak ekleme işlemi yapılır.



1	Adres	Spam olarak algılanmayacak adreslerin girildiği bölümdür.
2	Kontrol Tipi	E-posta adreslerinin kontrol tipinin seçildiği bölümdür.

3	Kaydet	Yapılan değişikliklerin kaydedildiği butondur.
4	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında yapılan işlemler kaydedilmez.

14.2.5 Bayes

Labris UTM cihazının veritabanında tutulan Bayes puanlarının görüntülediği veya puanlarının değiştirildiği bölümdür.

Name	Score 1	Score 2	Score 3	Score 4	Active	Manage
1 BAYES_00			-5.901	-5.9	⊙	⊙
2 BAYES_01			-0.6	-1.524	⊙	⊙
3 BAYES_10			-0.734	-0.908	⊙	⊙
4 BAYES_20			-0.127	-1.428	⊙	⊙
5 BAYES_30			-0.349	-0.904	⊙	⊙
6 BAYES_40			-0.001	-0.001	⊙	⊙
7 BAYES_44			-0.001	-0.001	⊙	⊙
8 BAYES_50			2.701	2.701	⊙	⊙
9 BAYES_56			2.801	2.801	⊙	⊙
10 BAYES_60			4.889	3.992	⊙	⊙

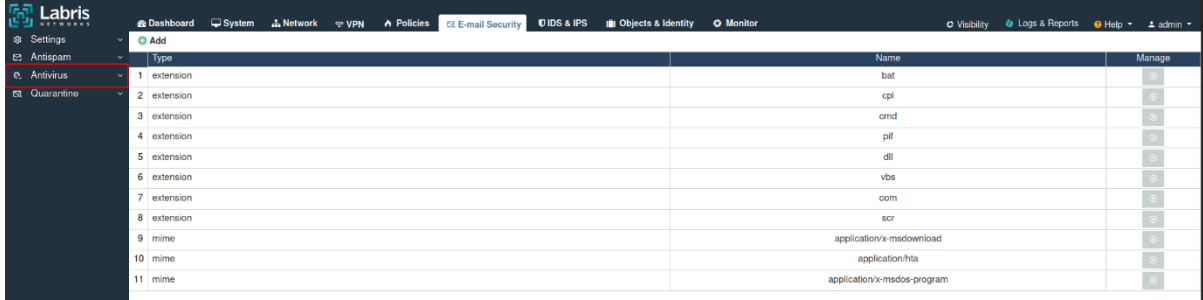
1	İsim	Bayes isminin görüntülediği bölümdür.
2	Puan 1	Veritabanında bulunan Bayesin puan 1'inin görüntülediği bölümdür.
3	Puan 2	Veritabanında bulunan Bayesin puan 2'inin görüntülediği bölümdür.
4	Puan 3	Veritabanında bulunan Bayesin puan 3'ün görüntülediği bölümdür.
5	Puan 4	Veritabanında bulunan Bayesin puan 4'ün görüntülediği bölümdür.
6	Aktif	Bayes'in aktiflik durumunun görüntülediği bölümdür.
7	Yönet	Veritabanında tutulan Bayeslerin puanlarının güncellendiği bölümdür.

-Eklenmiş olan Bayes puanlarını düzenlemek için düzenle butonuna tıklayarak düzenleme yapılır.

1	İsim	Bayes isminin görüntülediği bölümdür.
2	Puan 1	Bayes puan 1'in düzenlendiği bölümdür.
3	Puan 2	Bayes puan 2'nin düzenlendiği bölümdür.
4	Puan 3	Bayes puan 3'ün düzenlendiği bölümdür.
5	Puan 4	Bayes puan 4'ün düzenlendiği bölümdür.
6	Aktif	Bayes'in aktifleştirildiği bölümdür.
7	Kaydet	Veritabanında tutulan Bayeslerin puanlarında yapılan değişikliğinin kaydedildiği bölümdür.
8	Kapat	Düzenle butonuna basılarak açılan pencerenin kapatıldığı butondur.

14.3 Antivirüs

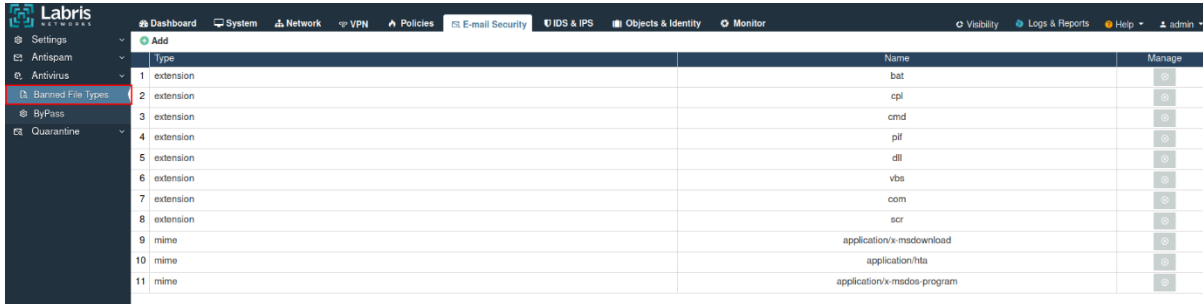
Mail sunucunuza gelen maillerin içeriğini inceleyerek posta içeriğinde virüs denetiminin yapıldığı bölümdür.



Type	Name	Manage
1 extension	bat	
2 extension	cpl	
3 extension	cmd	
4 extension	pif	
5 extension	dll	
6 extension	vbs	
7 extension	com	
8 extension	scr	
9 mime	application/x-msdownload	
10 mime	application/hta	
11 mime	application/x-msdos-program	

14.3.1 Uzantı Engelle

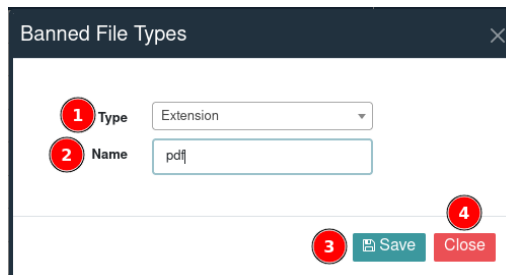
Virüs olarak tespit algılanacak uzantıların eklendiği veya eklenen uzantıların görüntülediği modüldür.



Type	Name	Manage
1 extension	bat	
2 extension	cpl	
3 extension	cmd	
4 extension	pif	
5 extension	dll	
6 extension	vbs	
7 extension	com	
8 extension	scr	
9 mime	application/x-msdownload	
10 mime	application/hta	
11 mime	application/x-msdos-program	

1	Ekle	Virüs olarak algılanacak uzantıların eklendiği butondur.
2	Tip	Eklenen uzantı tipinin görüntülediği bölümdür.
3	İsim	Uzantı isminin görüntülediği bölümdür.
4	Yönet	Eklenen uzantıların silindiği bölümdür.

-Virüs olarak algılanacak olan uzantı eklemek için 'ekle' butonuna tıklayarak yasaklanmış uzantı eklenebilir.



Banned File Types

1 Type: Extension

2 Name: pdf

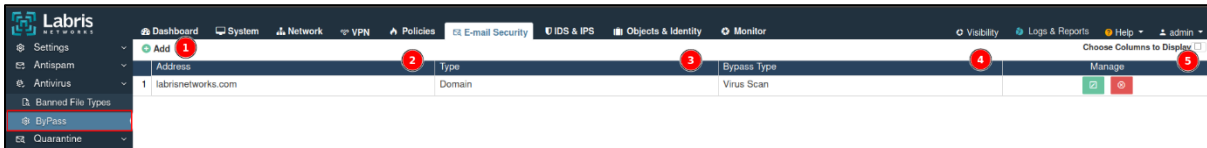
3 Save

4 Close

1	Tip	Engellenecek uzantının tipinin seçildiği bölümdür.
2	İsim	Engellenecek uzantının isminin girildiği bölümdür.
3	Kaydet	Engellenecek uzantının kaydedildiği butondur.
4	Kapat	Ekle butonuna basılarak açılan pencerenin kapatıldığı butondur.

14.3.2 Hariç Bırak

Mail sunucusuna gelen maillerin virüs taramasından hariç bırakıldığı modüldür.



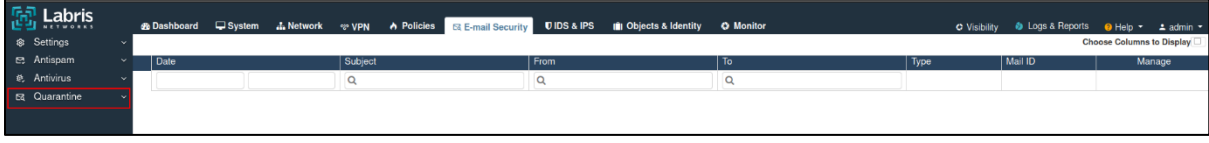
1	Ekle	Virüs taramasından geçmeyecek olan adreslerin eklendiği butondur.
2	Adres	Virüs taramasından hariç bırakılacak posta adreslerinin görüntülediği bölümdür.
3	Tip	Virüs taramasından hariç bırakılacak posta adreslerinin tipinin görüntülediği bölümdür.
4	Es Geçme Tipi	Es geçme tipinin görüntülediği bölümdür.
5	Yönet	Virüs taramasından hariç bırakılan alan adlarının veya e-posta adreslerinin kaldırıldığı veya düzenlendiği bölümdür.

-Virüs taramasından geçmeyecek alan adlarını veya e-posta adreslerinin eklemek için 'ekle' butonuna tıklayarak ekleme işlemi yapılır.

1	Tip	Virüs taramasından geçmeyecek olan adreslerin tipinin seçildiği bölümdür. Tip olarak alan adı veya e-posta adresi eklenir.
2	Adres	Tipi bağlı olarak alan adı adresi veya e-posta adresinin eklendiği bölümdür.
3	Es Geçme Tipi	Yazılan alan adı adresinin veya e-posta adresinin es geçme tipinin seçildiği bölümdür.
4	Dahil Etme	Virüs taramasına dahil edilmemesi istenildiği durumlarda açılır.
5	Alt Alan Adı Kontrolü	Eklenen adresin alt alan adı kontrolünün yapılması gereken durumlarda açılır.
6	Kaydet	Virüs taramasından geçmeyecek olan adreslerin kaydedildiği butondur.
7	Kapat	Ekle butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

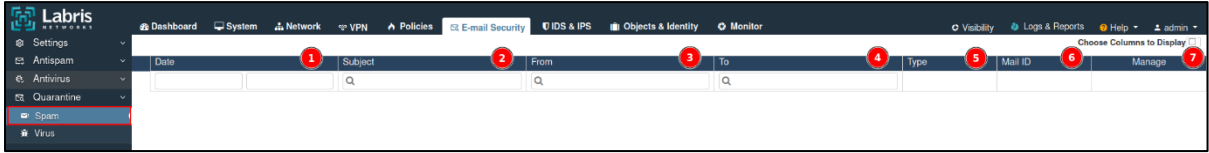
14.4 Karantina

Labris UTM cihazı tarafından karantinaya alınan maillerin görüntülediği bölümdür.



14.4.1 İstenmeyen E-posta

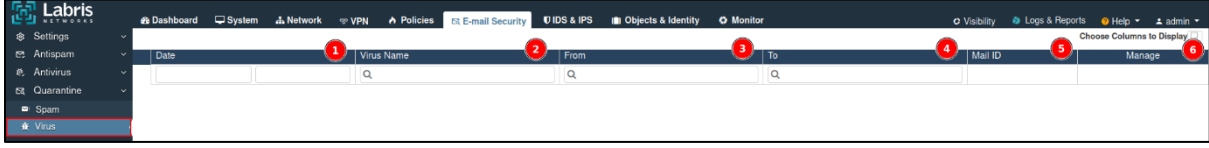
Labris UTM cihazı tarafından istenmeyen posta olarak algılanan postaların görüntülediği bölümdür.



1	Tarih	İstenmeyen postanın karantinaya alındığı tarihin görüntülediği bölümdür.
2	Konu	Karantinaya alınan postanın konusunun görüntülediği bölümdür.
3	Gönderici	Karantinaya alınan postanın gönderici adresinin görüntülediği bölümdür.
4	Alıcı	Karantinaya alınan postanın alıcı adresinin görüntülediği bölümdür.
5	Tip	Karantinaya alınan postanın tip bilgisinin görüntülediği bölümdür.
6	E-Posta Kimliği	Karantinaya alınan postanın E-posta kimliğinin görüntülediği bölümdür
7	Yönet	Karantinaya alınan postanın düzenlendiği bölümdür.

14.4.2 Virüs

Labris UTM cihazı tarafından virüslü olarak algılanan e-postaların görüntülediği bölümdür.



Tarih	Virüs tespiti yapılan e-postanın karantinaya alındığı tarihin görüntülediği bölümdür.
Konu	Karantinaya alınan virüslü postanın virüs isminin görüntülediği bölümdür.
Gönderici	Karantinaya alınan virüslü postanın gönderici adresinin görüntülediği bölümdür.
Alıcı	Karantinaya alınan virüslü postanın alıcı adresinin görüntülediği bölümdür.
Tip	Karantinaya alınan virüslü postanın tip bilgisinin görüntülediği bölümdür.
E-Posta Kimliği	Karantinaya alınan virüslü postanın E-posta kimliğinin görüntülediği bölümdür
Yönet	Karantinaya alınan virüslü postanın düzenlendiği bölümdür.

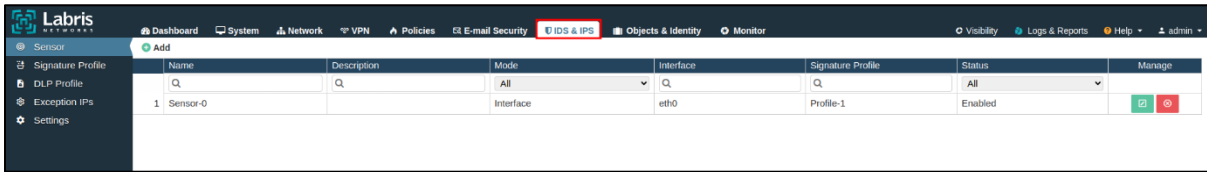
15 IDS&IPS

IDS(Saldırı Tespit Sistemi), ağ veya bilgisayar sistemlerindeki potansiyel kötü niyetli etkinlikleri izleyen ve tespit eden sistemdir. Ağ trafiğini analiz ederek anormal aktiviteleri tespit eder.

IPS(Saldırı Önleme Sistemi), belirli bir tehdidin algılanmasının ardından otomatik olarak müdahale edebilir ve saldırı girişimini durdurabilir. IPS, ağ trafiğini inceleyerek veya sistem düzeyinde davranış analizi yaparak saldırıları tespit eder ve müdahale eder.

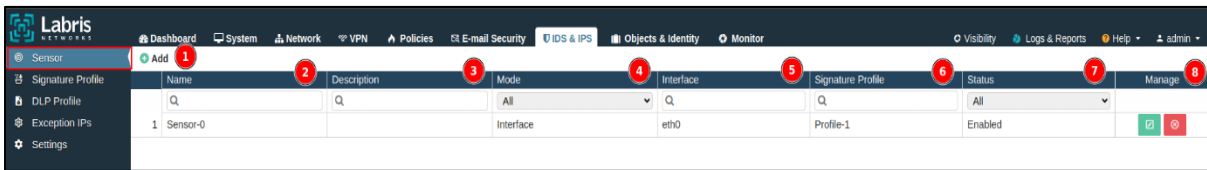
IPS, ağ trafiğiniz içerisindeki zararlı hareketleri veya zararları bağlantıların önlenmesi için kullanılır.

Labris UTM cihazında IDS ve IPS ile ilgili olarak sensör ayarları, veritabanında bulunan imza profilleri, DLP profili, istisna IP adresleri ve IDS, IPS'in genel ayarları yapılır.



15.1 Sensör

Labris UTM cihazında trafiğin dinleneceği portun seçildiği modüldür. Burada seçilen arabirimde IDS&IPS sensörü açılmaktadır. Belirlenen arabirimden geçen trafiği inceleyerek ağ trafiğindeki saldırıların tespiti ve engellenmesi yapılır.



1	Ekle	IDS&IPS sensörünün eklendiği butondur.
2	İsim	Eklenecek IDS&IPS sensörünün isminin görüntülediği bölümdür.
3	Açıklama	Eklenecek IDS&IPS sensör ile ilgili açıklamanın görüntülediği bölümdür.
4	Mod	IDS&IPS'in çalışması için modu görüntülenir. Mod arabirim seçilmesi durumunda IDS&IPS arabirimdeki trafiği dinleyerek tespit ve engelleme yapar. Politikanın mod seçildiği durumda ise belirlenen Kural setine göre

		tespit ve engelleme işlemi yapar.
5	Arabirim	IDS&IPS'in açıldığı arabirimin görüntülediği bölümdür.
6	İmza Profili	IDS&IPS' in imza profilinin görüntülediği bölümdür.
7	Durum	IDS&IPS' in durumu görüntülenir. Durum aktif ise IDS&IPS seçilen arabirimde çalışır. Durum pasif ise IDS&IPS kapalıdır.
8	Yönet	Eklenecek IDS&IPS sensörlerinin düzenlendiği veya silindiği bölümdür.

-Sensör eklemek için 'ekle' butonuna tıklayarak IDS&IPS sensör eklemesi yapılır. Ekle butonuna tıkladıktan sonra gelen ekrandaki bilgiler doldurarak IDS&IPS sensör eklemesi yapılır.

1	Etkinleştir	IDS&IPS sensörünün etkinleştirildiği butondur.
2	İsim	IDS&IPS sensörüne ait ismin girildiği bölümdür.
3	Açıklama	IDS&IPS sensörüne ait açıklamanın girildiği bölümdür.
4	Mod	IDS&IPS'in çalışması için modu seçilir. Mod arabirim seçilmesi durumunda IDS&IPS arabirimdeki trafiği

		dinleyerek tespit ve engelleme yapar. Politikanın mod seçildiği durumda ise belirlenen Kural setine göre tespit ve engelleme işlemi yapar.
5	Arabirim	IDS&IPS'in açılacağı arabirimin seçildiği bölümdür.
6	İmza Profili	Eklenen imza profilinin seçildiği bölümdür.
7	DLP Profili	DLP Profilinde eklenen DLP'nin seçildiği bölümdür.
8	Adresler	IDS&IPS sensörünün denetleyeceği adres bilgilerinin bulunduğu ve adres bilgilerinin düzenlendiği bölümdür.
9	Portlar	IDS&IPS sensörünün denetleyeceği port bilgilerinin bulunduğu ve port bilgilerinin düzenlendiği bölümdür.
10	Kaydet	IDS&IPS sensörünün kaydedildiği butondur.
11	Kapat	IDS&IPS sensör ekranının kapatıldığı butondur.


15.1.1 Adres Ayarları

IDS&IPS sensörün adres ayarlarının yapıldığı bölümdür.

Addresses		Port Settings
Name	Addresses	
<input type="text"/>	<input type="text"/>	
HOME_NET		
EXTERNAL_NET		
DNS_SERVERS	HOME_NET	
SMTP_SERVERS	HOME_NET	
HTTP_SERVERS	HOME_NET	
SQL_SERVERS	HOME_NET	
TELNET_SERVERS	HOME_NET	
SSH_SERVERS	HOME_NET	
FTP_SERVERS	HOME_NET	
SIP_SERVERS	HOME_NET	
AIM_SERVERS	64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.18	

1	İç_AĞ	IDS&IPS iç ağ adresinin yazıldığı bölümdür.
2	Dış_AĞ	IDS&IPS dış ağ adreslerinin yazıldığı bölümdür. Genellikle 'any' olarak bırakılır. IDS&IPS sensörünün dış IP adresinden gelen trafiği izleyeceği anlamına gelir.
3	DNS_SUNUCU	İç ağdaki DNS sunucu bilgileri girilir. DNS sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
4	SMTP_SUNUCU	İç ağdaki SMTP sunucu bilgileri girilir. SMTP sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
5	HTTP_SUNUCU	İç ağdaki HTTP sunucu bilgileri girilir. HTTP sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
6	SQL_SUNUCU	İç ağdaki SQL sunucu bilgileri girilir. SQL sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
7	TELNET_SUNUCU	İç ağdaki Telnet sunucu bilgileri girilir. Telnet sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
8	SSH_SUNUCU	İç ağdaki SSH sunucu bilgileri girilir. SSH sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
9	FTP_SUNUCU	İç ağdaki FTP sunucu bilgileri girilir. FTP sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
10	SIP_SUNUCU	İç ağdaki SIP sunucu bilgileri girilir. SIP sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır.
11	AIM_SUNUCU	İç ağdaki AIM sunucu bilgileri girilir. AIM sunucusu yok ise \$İç_AĞ(\$Home_NET) olarak bırakılır. AIM sunucu olarak tespit edilen IP adresleri varsayılan olarak gelmektedir.

-Adreslerin düzenlenmesi için 'düzenle' butonuna tıklanır.

Addresses		Port Settings
Name	Addresses	
<input type="text"/>	<input type="text"/>	
HOME_NET	192.168.1.0/24	

Addresses

1 Included Address

2 Excluded Address

3 OK

1	Dahili Adresler	IDS&IPS sensörü için dahili IP adreslerinin seçildiği bölümdür.
2	Harici Adresler	IDS&IPS sensörü için hariç adreslerinin seçildiği bölümdür.
3	Kaydet	Eklenen IDS&IPS sensörü IP adreslerin kaydedildiği butondur.

15.1.2 Port Ayarları

IDS&IPS sensörün port ayarlarının yapıldığı bölümdür.

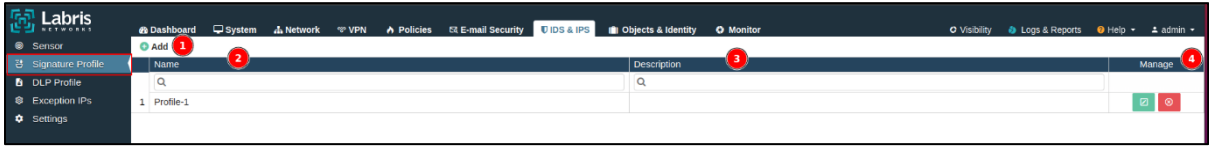
Addresses		Port Settings	
Name	Port Numbers		
Q	Q		
HTTP_PORTS	80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000,8008,8014,8028,8080,8085,8088,8090,8118,8123,8180,8181,8243,8280,8300,8800,8888,8899,9000,9060,9080,9090,9091,9443,9999,11371,34443,34444,41080,50002,55555		
SHELLCODE_PORTS	!80		
ORACLE_PORTS	1024:		
SSH_PORTS	22		
FTP_PORTS	21,2100,3535		
SIP_PORTS	5060,5061,5600		
FILE_DATA_PORTS	HTTP_PORTS,110,143		
GTP_PORTS	2123,2152,3386		

1	HTTP_PORTLARI	HTTP trafiğinin denetlendiği portların görüntülenir ve port eklemesi yapılır.
2	SHELLCODE_PORTLARI	Shellcode tespiti için kullanılacak portların görüntülediği veya shellcode tespiti yapılacak port bilgilerinin girildiği bölümdür. '!80' ifadesi ise, 80 numaralı portu tespit dışında bırakmak için yazılmıştır.
3	ORACLE_PORTLARI	Oracle veritabanı trafiğini izlemek için kullanılan portlar görüntülenir ve oracle veritabanı trafiğini incelemek için istenilen port numaraları girilir. '1024:' ifadesi, 1024 üzerindeki tüm portları izlemek için yazılmıştır.
4	SSH_PORTLARI	SSH trafiğinin denetlendiği port bilgisi görüntülenir ve SSH için kullanılan port numarası var ise port numarası girilir.
5	FTP_PORTLARI	FTP trafiğinin denetlendiği port bilgisi görüntülenir ve FTP için kullanılan port numarası var ise port numarası girilir.

6	SIP_PORTLARI	SIP trafiğinin denetlendiği port bilgisi görüntülenir. SIP portlarının dışında başka bir port numarası kullanılıyorsa bu bölümde ekleme işlemi yapılır.
7	FILE_DATA_POR TLARI	Seçilen arabirim ait ağ trafiğindeki dosya veri akışlarını izlemek için kullanılan portlar görüntülenir. Varsayılan olarak belirtilen portlar dışındaki başka bir port numarası ekleme işlemi bu bölümde yapılır.
8	GTP_PORTLARI	Seçilen arabirime ait olan ağ trafiğindeki GTP akışlarını izlemek için kullanılan portlar görüntülenir. Varsayılan olarak belirtilen portlar dışındaki başka bir port numarası ekleme işlemi bu bölümde yapılır.

15.2 İmza Profili

Ağ trafiğini dinleyerek anormal trafiği veya engelleme işlemleri, IDS&IPS imza profiline göre yapılır. Ağ trafiğini analiz ederek belirli imza kurallarına uyan davranışları tespit eder ve davranışa uygun işlem yapar. Bu modülde ise eklenen imza profilleri görüntülenir.



1	Ekle	İmza profili ekleme işleminin yapıldığı butondur.
2	İsim	Eklenen imza profilinin ismi görüntülenir.
3	Açıklama	Eklenen imza profili ile ilgili açıklama görüntülenir.
4	Yönet	İmza profillerinin düzenlendiği veya silindiği bölümdür.

-İmza profilini düzenlemek için düzenle butonuna basılır. Düzenle butonuna basıldıktan sonra imza profilleri düzenlenir.

The screenshot shows the 'Signature Profile' configuration window in the Labris UTM management interface. The window is titled 'Signature Profile' and contains several sections:

- 1 Name:** A text input field containing 'Profile-1'.
- 2 Description:** A text area for entering a description.
- 3 Categories:** Three sections for selecting categories:
 - Severity:** Radio buttons for 1 (High), 2 (Medium), and 3 (Low).
 - Flow:** Radio buttons for To Server, From Server, To Client, and From Client.
 - Classification:** A text area for classification.
- 4 Search:** A search bar with the placeholder text 'CVE-ID, SID, Signature, Category'.
- 5 Filter and Clear Filter:** Two buttons for filtering and clearing filters.
- 6 Table:** A table with columns: Category, Signatures, Enabled, and Manage. The table lists categories and their corresponding signature counts and enabled status.

Category	Signatures	Enabled	Manage
1 ACTIVEEX	537	No	Manage
2 ATTACK RESPONSE	740	No	Manage
3 BOTCC	50	No	Manage
4 CHAT	87	No	Manage
5 CIARMY	200	No	Manage
- 7 Save and Close:** Two buttons at the bottom right for saving and closing the window.

1	İsim	İmza profilinin isminin girildiği bölümdür.
2	Açıklama	İmza profili ile ilgili açıklamanın girildiği bölümdür.
3	Kategoriler	İmza profillerini kategorilere göre filtreleme işleminin yapıldığı bölümdür. Kritiklik Düzeyi (Severity), bir kuralın tespit ettiği olayın önem derecesine göre sınıflandırılır. Kritiklik düzeyi ise genellikle çok ciddi güvenlik tehditlerini veya saldırı girişimlerini temsil eder. Kritiklik düzeyi ortada ise potansiyel olarak önemli ancak doğrudan büyük bir tehdit oluşturmayan güvenlik olayıdır. Düşük seçilmesi durumunda ise genellikle daha az kritik olan veya bilgi amaçlı olan olaydır. Akış, kuralın hangi trafik yönünü ve bağlantı durumunu izleyeceği belirtir. Trafiğin sunucuya doğru, trafiğin sunucudan geldiği, trafiğin istemciye doğru ve

		trafiğin istemciden geldiğini belirtir. Sınıflandırma ise akış ve kritiklik düzeyine göre belirlenir.
4	İmza Arama	İmza veritabanında bulunan imzaların CVE-ID, SID, İmza ve Kategoriye göre filtrelemelerin yapıldığı bölümdür.
5	Kategori	İmzanın kategori isminin görüntülediği bölümdür.
6	İmzalar	İmza kategorisinin içindeki imza sayısının görüntülediği bölümdür.
7	Etkin	İmzanın aktiflik durumu görüntülenir.
8	Yönet	İmzaların düzenlendiği bölümdür.
9	Kaydet	Düzenlenen İmza profilinin kaydedildiği butondur.
10	Kapat	İmza profili ekranının kapatıldığı butondur.

-İmza profili düzenlemek için 'düzenle' butonuna basılır.

Signature Profile
✕

Name:

Description:

Severity

1 (High)

2 (Medium)

3 (Low)

Flow

To Server

From Server

To Client

From Client

Classification

CVE-ID, SID, Signature, Category Filter Clear Filter

Category	Signatures	Enabled	Manage
1 ACTIVEX	537	No	<input checked="" type="checkbox"/>
2 ATTACK RESPONSE	740	No	<input checked="" type="checkbox"/>
3 BOTCC	50	No	<input checked="" type="checkbox"/>
4 CHAT	87	No	<input checked="" type="checkbox"/>
5 CHARMV	200	No	<input checked="" type="checkbox"/>

Save Close

-Düzenle butonuna tıkladıktan sonra düzenlenen imza profili düzenlenir.

Category - ACTIVEX
✕

Severity: 1 (High), 2 (Medium), 3 (Low), 4 (Very Low)

Flow: To Server, From Server, To Client, From Client

Classification:

CVE-ID, SID, Signature Filter Clear Filter

SID	Severity	Signature	Classification	Flow	CVE	References	Enabled	E-Mail	Action
2009161	1	ET ACTIVEX GeoVision LiveX_v7000 ActiveX Control Arbitrary File Overwrite	Web application attack	To Client		1 2	No	No	Alert
2001624	1	ET ACTIVEX winhlp32 ActiveX control attack - phase 3	Web application attack	To Client			Yes	No	Alert
2010374	1	ET ACTIVEX Halhaisoft Universal Player ActiveX Control URL Property Buffer Overflow Function Call Attempt	Attempted user privilege gain	To Client		1 2	No	No	Alert
2011722	1	ET ACTIVEX Axis Media Controller ActiveX SetImage Method Remote Code Execution Attempt	Attempted user privilege gain	To Client			Yes	No	Alert
2010300	1	ET ACTIVEX COM Object MS06-042 CLSID 9 Access Attempt	Attempted user privilege gain	To Client	2006-3638	1	No	No	Alert
2009161	1	ET ACTIVEX Autodesk Design Review DWF Viewer	Web application attack	To Client			No	No	Alert

Edit Cancel

1	SID	İmza kimlik numarasının görüntülediği bölümdür.
2	Kritiklik Düzeyi	IDS&IPS imzaları ile ilgili kritiklik düzeyi görüntülenir. 1- Yüksek, 2- Orta, 3- Düşük ve 4- Çok Düşük

3	İmza	IDS&IPS imzalarını ve imza isimlerinin görüntülediği bölümdür.
3	Sınıflandırma	İmzaların sınıflandırma ismi görüntülenir.
4	Akış	IDS&IPS imzasının akışı bilgisi görüntülenir.
5	CVE	CVE, yazılım ve donanım güvenlik açıklarının tanımlanması ve sınıflandırılması için kullanılır. Bu bölümde ise imzaların CVE numaraları görüntülenir.
6	Referanslar	İmzaların referans bilgileri görüntülenir. Referans ile ilgili detaylarda bulunur.
7	Etkin	İmzanın aktiflik durumu görüntülenir. Eğer etkin ise 'evet' etkin değil ise 'hayır' yazar.
8	Email	İmzaya takılan uyarıların mail olarak gönderilme durumu görüntülenir. Eğer mail gidecek ise 'evet' mail gönderilmeyecek ise 'hayır' yazar.
9	Eylem	Ağ trafiğindeki anormallerin tespit ederek imzaya takılanlar için uyarı ya da engellemesinin yapılır.
10	Düzenle	İmzalar ile ilgili düzenlemenin kaydedildiği butondur.
11	Kapat	İmza profili ekranının kapatıldığı butondur.

-İmza profilindeki kurallar ile ilgili yapılacak eylemi düzenlemek için eylem bölümünde bulunan düzenleme butonuna basılır.

Category - ACTIVEX

Severity: 1 (High), 2 (Medium), 3 (Low), 4 (Very Low)

Flow: To Server, From Server, To Client, From Client

Classification:

CVE-ID, SID, Signature

Filter: [Filter] [Clear Filter]

SID	Severity	Signature	Classification	Flow	CVE	References	Enabled	EMail	Action
2009161	1	ET ACTIVEX GeoVision LiveX_v7000 ActiveX Control Arbitrary File Overwrite	Web application attack	To Client			No	No	Alert
2001624	1	ET ACTIVEX winhlp32 ActiveX control attack - phase 3	Web application attack	To Client			Yes	No	Alert
2010374	1	ET ACTIVEX Haihaisoft Universal Player ActiveX Control URL Property Buffer Overflow Function Call Attempt	Attempted user privilege gain	To Client			No	No	Alert
2011722	1	ET ACTIVEX Axis Media Controller ActiveX SetImage Method Remote Code Execution Attempt	Attempted user privilege gain	To Client			Yes	No	Alert
2010300	1	ET ACTIVEX COM Object MS06-042 CLSID 9 Access Attempt	Attempted user privilege gain	To Client	2006-3638		No	No	Alert
2009162	1	ET ACTIVEX Autodesk Design Review DWF Viewer	Web application attack	To Client			No	No	Alert

Edit Cancel

Action

1 Enable

2 E-Mail Alert

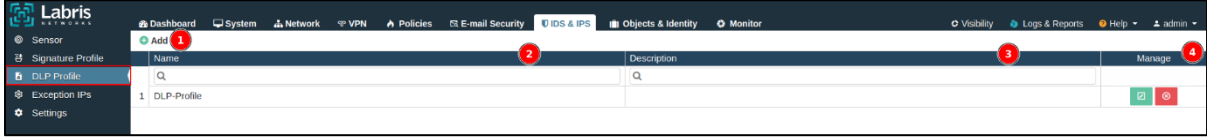
3 Action: Alert

4 Ok 5 Close

1	Etkinleştir	IDS&IPS kuralının etkinleştirildiği butondur.
2	E-Mail Uyarısı	IDS&IPS kuralı tarafından tespit edilen anormal trafikler için oluşturulan uyarıların mail olarak iletilmesi için etkinleştirilir.
3	Eylem	IDS&IPS kuralı için eylemin seçildiği bölümdür. Bu bölümde düzenlenen kural ile ilgili uyarı oluşturulur veya kuraldan geçen trafik engellenir.
4	Kaydet	Eylem ile ilgili yapılan değişikliklerin kaydedildiği butondur.
5	Kapat	Eylemi düzenlemek için açılan pencerenin kapatıldığı butondur.

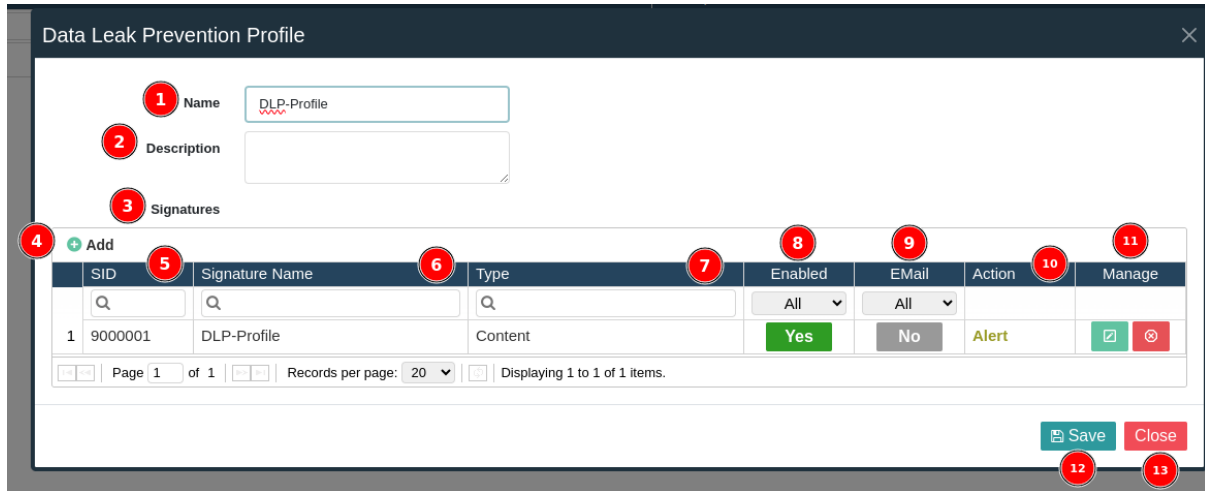
15.3 DLP Profili

DLP Profili, kuruluşun hassas bilgilerini yetkisiz erişimden, kullanım, aktarım ve sızdırmadan korumak için oluşturulmuş kurallardır. Hassas verilerin korunmasını sağlamak için oluşturulur. Oluşturulan profiller, veri sızıntılarını ve ihlallerini önlemeye yöneliktir. DLP Profilleri, ağ trafiği üzerindeki veri güvenliğini artırır.



1	Ekle	DLP Profili eklemek için kullanılan butondur.
2	İsim	Eklenecek DLP Profilinın ismi görüntülenir.
3	Açıklama	Eklenecek DLP Profili ile ilgili açıklamanın görüntülediği bölümdür.
4	Yönet	DLP Profilinın silindiği veya düzenlendiği bölümdür.

-DLP Profili eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıklandıktan sonra DLP kuralı eklenir.



1	İsim	DLP Profilinın isminin girildiği bölümdür.
2	Açıklama	DLP Profilinın açıklamasının girildiği bölümdür.
3	İmzalar	Eklenecek DLP kurallarının görüntülediği veya DLP

		kuralı ekleme işleminin yapıldığı bölümdür.
4	DLP Kuralı Ekle	DLP kuralı eklemek için kullanılan butondur.
5	SID	Eklenen DLP kuralının SID numarasının görüntülediği bölümdür.
6	İmza İsmi	Eklenen DLP imzasının isminin görüntülediği bölümdür.
7	Tip	DLP imzasının tipi görüntülenir.
8	Etkin	DLP imzasının etkinliği görüntülenir. Eğer 'evet' yazıyorsa DLP imzası etkindir. 'Hayır' ise DLP imzası kapalıdır.
9	Email	DLP İmzasına takılan trafik ile ilgili email durumu görüntülenir. Eğer 'evet' ise email gönderimi yapar. 'Hayır' ise email gönderimi yapmaz.
10	Eylem	DLP kuralı için eylemin seçildiği bölümdür. Bu bölümde düzenlenen kural ile ilgili uyarı oluşturulur veya kuraldan geçen trafik engellenir.
11	Yönet	DLP kurallarının düzenlendiği bölümdür.
12	Kaydet	DLP profilinin kaydedildiği butondur.
13	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

-DLP kuralı eklemek için 'ekle' butonuna tıklanır.

Data Leak Prevention Profile

Name: DLP-Profile

Description:

Signatures

Add

SID	Signature Name	Type	Enabled	Email	Action	Manage	
1	9000001	DLP-Profile	Content	Yes	No	Alert	

Page 1 of 1 Records per page: 20 Displaying 1 to 1 of 1 items.

Save **Close**

- Ekle butonuna tıkladıktan DLP kuralı düzenlenir.

Data Leak Prevention - Signature

1 Enable

2 Signature Name: DLP-Profile

3 Protocol: TCP

4 Source: HOME_NET

5 Source Port:

6 Destination: EXTERNAL_NET

7 Destination Port:

8 Type: Content

9 Content: 12345678901

10 Action: Alert

11 E-Mail Alert:

1	Etkinleştir	DLP imzasının etkinleştirildiği bölümdür.
2	İmza İsmi	DLP imzasının isminin girildiği bölümdür.
3	Protokol	DLP imzası için protokol seçildiği bölümdür
4	Kaynak	DLP imzasına kaynak adresin seçildiği bölümdür. Seçilen kaynak adresteki trafiği inceler ve trafiğe göre karar verir.
5	Kaynak Port	DLP imzasına kaynak portun seçildiği bölümdür. Kaynak port belirtilmesi durumunda kaynak porta bakarak anormalilere karar verir.
6	Hedef	DLP imzasına hedef adresin seçildiği bölümdür. Seçilen hedef adrese doğru trafiği inceler ve trafiğe göre karar verir.
7	Hedef Port	DLP imzasına hedef portun seçildiği bölümdür. Hedef port belirtilmesi durumunda hedef porta bakarak anormalilere karar verir.
8	Tip	DLP imzasının tipi seçilir. Seçilen tipe göre DLP kuralı oluşturulur. 3 adet DLP tipi bulunur. Bunlar; içerik, regex, dosya uzantısıdır.

9	İçerik/Regex/Dosya Uzantısı	Tip olarak içerik seçilmesi durumunda belirtilen içeriğe göre engelleme yapar. Tip regex seçilirse belirlenen regexe göre trafiği analiz ederek engeller veya kullanıcıyı uyarır. Tip dosya uzantısı seçilirse seçilen dosya uzantısına göre engeller veya uyarı oluşturur.
10	Eylem	DLP imzasına takılan trafiğin eylemi belirtilir.
11	E-mail Uyarısı	DLP imzasına takılan trafiği Email uyarısı oluşturmak için kullanılır.
12	Dahil Edilmemiş Kaynak	DLP korumasına dahil edilmeyen kaynak adreslerinin seçildiği bölümdür.
13	Dahil Edilmemiş Kaynak Port	DLP korumasına dahil edilmeyen kaynak portların seçildiği bölümdür.
14	Dahil Edilmemiş Hedef	DLP korumasına dahil edilmeyen hedef adres bilgisinin seçildiği bölümdür.
15	Dahil Edilmemiş Hedef Port	DLP korumasına dahil edilmeyen hedef portların seçildiği bölümdür.
16	Kaydet	DLP imzasının kaydedildiği butondur.
17	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur.

15.4 İstisna IP Adresleri

IDS&IPS kurallarına uymayacak IP adreslerinin eklendiği bölümdür.

Name	Description	IP / Network	Status	Manage
Exception-1		127.0.0.1	Enabled	

1	Ekle	IDS&IPS kurallarına uymayacak IP adreslerinin ekleme işleminin yapıldığı butondur.
2	İsim	İstisna olarak eklenen IP adreslerine verilen ismin

		görüntülendiği bölümdür.
3	Açıklama	İstisna olarak eklenen IP adreslerine verilen açıklama bilgisinin görüntülendiği bölümdür.
4	IP/Ağ	İstisna olarak eklenen IP Adresi veya Ağ adresinin görüntülendiği bölümdür.
5	Durum	İstisna olarak eklenen IP veya Ağ adreslerinin durumu görüntülenir. Eğer durum etkin ise görünen IP adresi IDS&IPS korumasına dahil değildir. Etkin değil görünen IP veya Ağ adresi IDS&IPS korumasına dahildir.
6	Yönet	Eklenen istisana IP/Ağ adreslerinin silindiği veya düzenlendiği bölümdür.

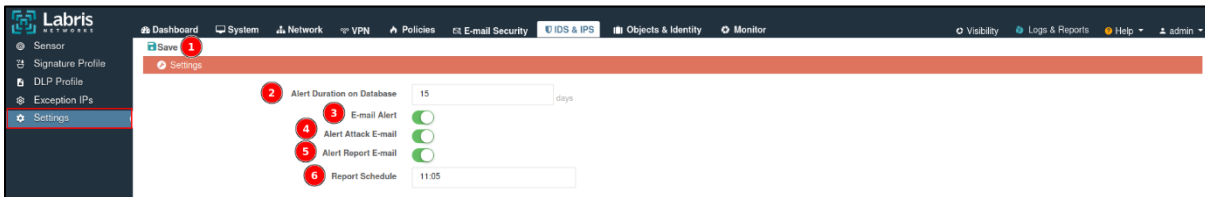
-IDS&IPS korumasına dahil edilmeyecek IP veya Ağ adreslerini eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra girilen IP veya Ağ adresleri IDS&IPS korumasına dahil edilmez.

1	Etkinleştir	İstisna olarak eklenen IP adresinin etkinleştirildiği bölümdür.
2	İsim	İstisna olarak eklenen IP adreslerine verilen ismin

		görüntülendiği bölümdür.
3	Açıklama	İstisna olarak eklenen IP adreslerine verilen açıklama bilgisinin görüntülendiği bölümdür.
4	IP/Ağ	İstisna olarak eklenen IP Adresi veya Ağ adresinin görüntülendiği bölümdür.
5	Kaydet	İstisna olarak eklenen IP veya Ağ adreslerinin durumu görüntülenir. Eğer durum etkin ise görünen IP adresi IDS&IPS korumasına dahil değildir. Etkin değil görünen IP veya Ağ adresi IDS&IPS korumasına dahildir.
6	Kapat	Eklenen istisana IP/Ağ adreslerinin silindiği veya düzenlendiği bölümdür.

15.5 Ayarlar

IDS&IPS'in uyarılarının gönderileceği ayarların yapıldığı bölümdür. Bu modülde IDS&IPS saldırıları ve uyarıları, sistem modülünde tanımlanan e-posta adresine gönderilir.



1	Kaydet	IDS&IPS mail ayarlarının kaydedildiği bölümdür.
2	Veritabanda Uyarıların Durma Süresi	Veritabanında uyarıların tutulma zamanının düzenlendiği bölümdür. Gün olarak düzenlenir.
3	Uyarı Maili	IDS&IPS politikasına takılan uyarıların mail gelmesi için etkinleştirildiği butondur.
4	Uyarı Saldırı E-Postası	IDS&IPS saldırılarında uyarı e-postası gönderilmesi durumunda etkinleştirilir.

5	Uyarı Raporu E-Postası	Uyarı raporlarının e-posta gönderilmesi gereken durumda etkinleştirilir.
6	Rapor Planı	Oluşturulan raporun planlı bir şekilde gönderir.

16. Nesneler ve Kimlikler

Güvenlik duvarı kurallarında kullanılacak olan nesnelerin ve kimliklerin eklendiği modüldür. Eklenen nesnelere güvenlik duvarı ve NAT politikalarında kullanılır. Bunlara ek olarak Kimlik nesnelere de Politikalar modülünde kullanılır. Labris UTM cihazı üzerinde Kullanıcı eklemek Aktif Dizin entegrasyonu yapılır. Bu sayede Aktif Dizin'de eklenmiş kullanıcıları Labris UTM cihazına aktarılır. Aktif Dizin'den çekilen kullanıcılar üzerinde Politika modülünde kural yazılır. Nesne ve Kimlikler modülünde Ağ Nesnesi, Politika Nesnesi, Kota Objeleri, Uygulama, Kimlik ve Alıcı Profilleri eklenir.

ID	Type	Name	Address	Manage
1	IP Address	IPsec-WAN	10.20.30.40	[Edit] [Delete] [Refresh]
2	IP Address	lan	192.168.1.1	[Edit] [Delete] [Refresh]
3	IP Address	PublicIP_55	10.10.10.55	[Edit] [Delete] [Refresh]
4	IP Address	S-Web_6	192.168.1.6	[Edit] [Delete] [Refresh]
5	IP Address	Server_16	192.168.2.16	[Edit] [Delete] [Refresh]
6	IP Address	SSLVPN_MGT	10.8.3.1	[Edit] [Delete] [Refresh]
7	IP Address	vlan23	192.168.23.1	[Edit] [Delete] [Refresh]
8	IP Address	WAN	10.14.15.1	[Edit] [Delete] [Refresh]
9	IP Address	webservers	192.168.1.5	[Edit] [Delete] [Refresh]
10	IP Address	youtube	172.217.17.110	[Edit] [Delete] [Refresh]
11	IP List	YonetimIPAdresleri	192.168.1.54,192.168.1.53,192.168.1.52,192.168.1.51,192.168.1.50	[Edit] [Delete] [Refresh]
12	IP Range	IPSO-150	192.168.1.50 - 192.168.1.150	[Edit] [Delete] [Refresh]
13	MAC Address	M-PC_1	AA:BB:CC:DD:EE:FF	[Edit] [Delete] [Refresh]
14	Network	all multicast	224.0.0.0 / 240.0.0.0	[Edit] [Delete] [Refresh]
15	Network	internal_network_3	224.0.0.0 / 240.0.0.0	[Edit] [Delete] [Refresh]
16	Network	IPsec_LAN	192.168.11.0 / 255.255.255.0	[Edit] [Delete] [Refresh]
17	Network	lan	192.168.1.0 / 255.255.255.0	[Edit] [Delete] [Refresh]
18	Network	link-local	169.254.0.0 / 255.255.0.0	[Edit] [Delete] [Refresh]
19	Network	loopback-net	127.0.0.0 / 255.0.0.0	[Edit] [Delete] [Refresh]
20	Network	net-10.0.0.0	10.0.0.0 / 255.0.0.0	[Edit] [Delete] [Refresh]

16.1 Ağ Nesneleri

Politikalar modülünde kullanılacak ağ nesnelere oluşturulduğu modüldür. Oluşturulan Ağ Nesnelere güvenlik duvarı ve NAT politikasında kural yazılır. Ağ Nesnelere menüsünde Adresler, Adres Grubu, Ülke, Servis ve Servis Grubu ekleme işlemleri yapılır.

ID	Type	Name	Address	Manage
1	IP Address	IPsec-WAN	10.20.30.40	[Edit] [Delete] [Refresh]
2	IP Address	lan	192.168.1.1	[Edit] [Delete] [Refresh]
3	IP Address	PublicIP_55	10.10.10.55	[Edit] [Delete] [Refresh]
4	IP Address	S-Web_6	192.168.1.6	[Edit] [Delete] [Refresh]
5	IP Address	Server_16	192.168.2.16	[Edit] [Delete] [Refresh]
6	IP Address	SSLVPN_MGT	10.8.3.1	[Edit] [Delete] [Refresh]
7	IP Address	vlan23	192.168.23.1	[Edit] [Delete] [Refresh]
8	IP Address	WAN	10.14.15.1	[Edit] [Delete] [Refresh]

16.1.1 Adres

Politikalar modülünde kullanılacak IP Adresi, IP-Aralığı, MAC Adresi, Ağ Adresi, Wildcard Network ve IP/Ağ Listesi eklenir.

	Type	Name	Address	Manage
1	All	Q	Q	
2	IP Address	IPsec-WAN	10.20.30.40	
3	IP Address	lan	192.168.1.1	
4	IP Address	PublicIP_55	10.10.10.55	
5	IP Address	S-Web_6	192.168.1.6	
6	IP Address	Server_16	192.168.2.16	
7	IP Address	SSLVPN_MGT	10.8.3.1	
8	IP Address	vlan23	192.168.23.1	

1	Ekle	IP Adresi, IP-Aralığı, MAC Adresi, Ağ Adresi, Wildcard Network ve IP/Ağ Listesi ekleme işlemi yapılır.
2	Tip	Eklenecek Adresin eklendiği tipin görüntülediği bölümdür.
3	İsim	Eklenecek Adrese verilen ismin görüntülediği bölümdür.
4	Adres	Eklenecek Adrese ait bilgilerin görüntülediği bölümdür.
5	Yönet	Eklenecek Adresin bilgilerinin değiştirildiği veya silindiği bölümdür. Sistem tarafından eklenen adresler silinmez veya değiştirilemez.

-Adres eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra gelen ekrandaki eklemek istediğiniz adres tipi seçilir. Adres tipi IP, IP-Aralığı, MAC, Ağ, Wildcard Network ve IP/Ağ Listesi seçeneklerinden biri seçilerek adres ekleme işlemi yapılır.

- Adres tipi IP seçilmesi durumunda eklenecek olan adres tek bir IP adresidir. Örn: 192.168.1.6 IP adresini eklemek için adres tipi olarak IP seçilir.

The screenshot shows a dialog box titled 'Address' with a close button (X) in the top right corner. The form contains the following fields:

- Name: Server_16
- Description: (empty text area)
- Type: IP (selected in a dropdown menu)
- IP Address: 192.168.2.16
- Owner Group List: (empty text area)

At the bottom right, there are two buttons: 'Save' (green) and 'Close' (red).

IP Address	S-Web_6	192.168.1.6
------------	---------	-------------

- Adres tipi IP-Aralığı seçildiği durumda belirli IP aralığı için adres eklenir. Örn: 192.168.1.50-192.168.1.150 IP aralığında adres eklemek için adres tipi olarak IP-Aralığı seçilir.

The screenshot shows a dialog box titled 'Address' with a close button (X) in the top right corner. The form contains the following fields:

- Name: IP50-150
- Description: (empty text area)
- Type: IP-Range (selected in a dropdown menu)
- IP Range: 192.168.1.50 - 192.168.1.150
- Owner Group List: (empty text area)

At the bottom right, there are two buttons: 'Ok' (green) and 'Close' (red).

IP Range	↔ IP50-150	192.168.1.50 - 192.168.1.150
----------	------------	------------------------------

- Adres tipi MAC Adresi seçildiği durumda cihazların MAC Adresleri eklenir. Örn: AA:BB:CC:DD:EE:FF MAC Adresini eklemek için adres tipi olarak MAC Adres seçilir.

Adres

İsim: M-PC_1

Açıklama: Bilgisayar 1'in MAC Adresi

Tip: MAC

MAC Adresi: AA:BB:CC:DD:EE:FF

Üye Olduğu Gruplar

Kaydet Kapat

MAC Address	M-PC_1	AA:BB:CC:DD:EE:FF
-------------	--------	-------------------

- Adres tipi Ağ seçildiği durumda cihazların Ağ Adresleri eklenir. Örn: 10.8.3.0/255.255.255.0 ağının tamamını eklemek için adres tipi olarak Ağ seçilir.

Address

Name: IPSec_LAN

Description



Type: Network

Network Address: 192.168.11.0

Netmask: 255.255.255.0

Owner Group List: xALL_Network

Ok Close

Network	IPSec_LAN	192.168.11.0 / 255.255.255.0		
---------	-----------	------------------------------	---	---

- Adres tipi Ağ seçildiği durumda cihazların Ağ Adresleri eklenir. Örn: 10.10.10.0/0.0.0.255 ağının tamamını eklemek için adres tipi olarak Wildcard Network seçilir.

Address

Name: Wildcard-10

Description: Wildcard-10 Ağı

Type: Wildcard network

Network Address: 10.10.10.0

Netmask: 0.0.0.255

IP Type: IPv4

Owner Group List:

Ok Close

Wildcard Network	Wildcard-10	10.10.10.0 / 0.0.0.255
------------------	-------------	------------------------

- Adres tipi IP Listesi seçildiği durumda birden fazla IP adresi eklenir. Örn: 192.168.1.50, 192.168.1.51, 192.168.1.52, 192.168.1.53 ve 192.168.1.54 IP adreslerini eklemek için adres tipi olarak IP Listesi seçilir.

Address

Name: AdminIPs

Description:

Type: IP/Network List

IP Network List: 192.168.1.54,192.168.1.53,192.168.1.52,192.168.1.51,192.168.1.50

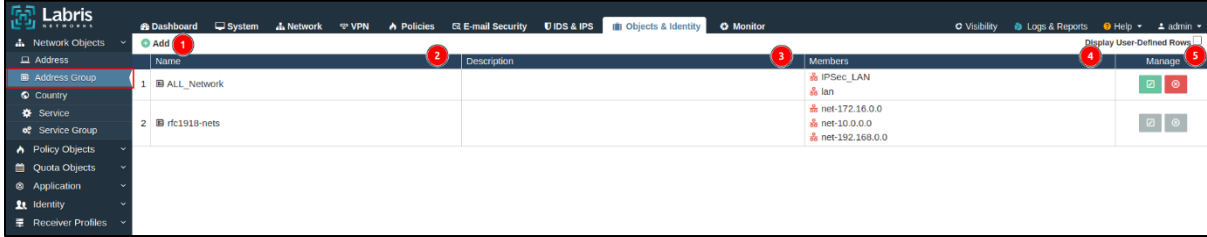
Owner Group List:

Ok Close

IP List	AdminIPs	192.168.1.54,192.168.1.53,192.168.1.52,192.168.1.51,192.168.1.50
---------	----------	--

16.1.2 Adres Grubu

Adres olarak eklenen nesnelerin gruplandığı modüldür. Politikalar modülünde yazılan kurallara birbirleriyle ilişkili olan IP adresleri gruplanır.



1	Ekle	Adres modülünde eklenen adreslerin gruplanması için kullanılan butondur.
2	İsim	Eklenen Adres Grubunun isminin görüntülediği bölümdür.
3	Açıklama	Eklenen Adres Grubunun açıklamasının görüntülediği bölümdür.
4	Üyeler	Adres Grubuna eklenen üyelerin görüntülediği bölümdür.
5	Yönet	Eklenen Adres Gruplarının bilgilerinin değiştirildiği veya silindiği bölümdür. Sistem tarafından eklenen Adres Grubları silinmez veya değiştirilemez.

-Adres Grubu eklemek için 'ekle' butonuna tıklanır. Ekle butonuna tıkladıktan sonra açılan ekranda Adres modülünde eklenen adresler gruplandırılır.

Address Group ✕

1 Name

2 Description

3 Address List × IPSec_LAN × lan

4 5

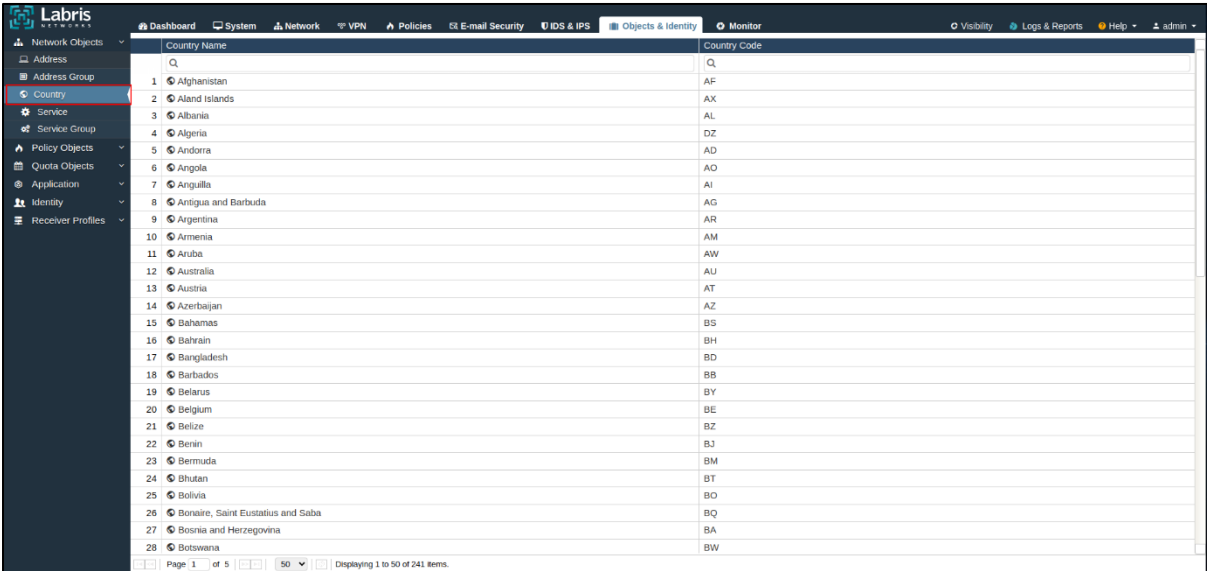
1	İsim	Eklenen Adres Grubuna verilen ismin girildiği bölümdür.
---	-------------	---

2	Açıklama	Eklenen Adres Grubuna verilen açıklamanın girildiği bölümdür.
3	Adres Listesi	Eklenen Adres Grubuna Adres eklendiği bölümdür.
4	Kaydet	Adres Grubunun kaydedildiği butondur.
5	Kapat	'ekle' butonuna basıldıktan sonra açılan ekranın kapatıldığı butondur.

Name	Description	Members	Manage
ALL_Network		IPSec_LAN lan	 

16.1.3 Ülke

Veritabanındaki **Ülke**'lerin görüntülediği bölümdür.



Country Name	Country code
1 Afghanistan	AF
2 Aland Islands	AX
3 Albania	AL
4 Algeria	DZ
5 Andorra	AD
6 Angola	AO
7 Anguilla	AI
8 Antigua and Barbuda	AG
9 Argentina	AR
10 Armenia	AM
11 Aruba	AW
12 Australia	AU
13 Austria	AT
14 Azerbaijan	AZ
15 Bahamas	BS
16 Bahrain	BH
17 Bangladesh	BD
18 Barbados	BB
19 Belarus	BY
20 Belgium	BE
21 Belize	BZ
22 Benin	BJ
23 Bermuda	BM
24 Bhutan	BT
25 Bolivia	BO
26 Bonaire, Saint Eustatius and Saba	BQ
27 Bosnia and Herzegovina	BA
28 Botswana	BW

16.1.4 Servis

Cihaz üzerindeki ekli olan Servislerin görüntülediği ve yeni Servis eklemesinin yapıldığı bölümdür.

Type	Name	Source Port	Destination Port	IP Protocol	Manage
1 Custom	ESTABLISHED	-	-	-	
2 ICMP	all ICMP unreachable	-	-	-	
3 ICMP	any ICMP	-	-	-	
4 ICMP	host_unreach	-	-	-	
5 ICMP	ping reply	-	-	-	
6 ICMP	ping request	-	-	-	
7 ICMP	port unreach	-	-	-	
8 ICMP	time exceeded	-	-	-	
9 ICMP	time exceeded in transit	-	-	-	
10 IP	AH	-	-	51	
11 IP	ESP	-	-	50	
12 IP	GRE	-	-	47	
13 IP	ip_fragments	-	-	-	
14 IP	SKIP	-	-	57	
15 IP	vrrp	-	-	112	
16 TCP	All TCP	0	0	-	
17 TCP	AOL	0	5190	-	
18 TCP	auth	0	113	-	
19 TCP	daytime	0	13	-	
20 TCP	domain	0	53	-	
21 TCP	finger	0	79	-	

1	Ekle	TCP, UDP, IP ve ICMP servis eklemesinin yapıldığı butondur.
2	Tip	Eklene Servisin tipinin görüntülediği bölümdür.
3	İsim	Eklene Servisin verilen ismin görüntülediği bölümdür.
4	Kaynak Port	Eklene Servisin kaynak port numarasının görüntülediği bölümdür.
5	Hedef Port	Eklene servisin hedef port numarasının görüntülediği bölümdür.
6	IP Protocol	Eklene ICMP servisinin port numarasının görüntülediği bölümdür.
5	Yönet	Eklene Servis bilgilerinin değiştirildiği veya silindiği bölümdür. Sistem tarafından eklene Servis silinmez veya değiştirilemez.

-Servis eklemek için 'ekle' butonuna tıklayarak Servis eklemesi yapılır. Ekle butonuna tıkladıkta gelen ekrandaki bilgileri doldurarak servis eklemesi yapılır.

The screenshot shows a 'Service' configuration window with the following fields and controls:

- 1 Name:** A text input field containing 'UDP-443'.
- 2 Description:** A large text area for entering a description.
- 3 Type:** A dropdown menu currently set to 'UDP'.
- 4 UDP Options:** Two port range fields. 'Source Port Range' is set to '0' to '0'. 'Destination Port Range' is set to '443' to '443'.
- 5 Service Group List:** A text area for selecting a service group.
- 6 Save:** A green button to save the configuration.
- 7 Close:** A red button to close the window.

1	İsim	Eklenecek Servisin isminin girildiği bölümdür.
2	Açıklama	Eklenecek Servisin tipinin görüntülediği bölümdür.
3	Tip	Eklenecek Servisin Tipi seçilir. TCP, UDP, ICMP ve IP tipleri bulunur.
4	Tip'e Ait Seçenekler	Seçilen Tip'e göre değişiklik göstermektedir.
5	Servis Grubu Listesi	Eklenecek Servisin dahil olacağı grubun seçildiği bölümdür.
6	Kaydet	Servis bilgilerinin kaydedildiği butondur.
7	Kapat	Açılan ekrandan çıkarıldığı butondur.

- Servis tipi TCP seçildiği durumda TCP Servisi eklenir. Kaynak Port, Hedef Port ve TCP bayrakları bilgilerine göre düzenlenir.

Service configuration window for TCP. The Name field is 'TCP_2222', Description is 'TCP 2222', and Type is 'TCP'. TCP Options show Source Port Range from 0 to 0 and Destination Port Range from 2222 to 2222. There are sections for Flags (URG, ACK, PSH, RST, SYN, FIN) and TCP Flag info.

TCP	TCP_2222	0	2222	-
-----	----------	---	------	---

- Servis tipi UDP seçildiği durumda UDP Servisi eklenir. Kaynak Port ve Hedef Port bilgilerine göre düzenlenir.

Service configuration window for UDP. The Name field is 'UDP-443', Description is empty, and Type is 'UDP'. UDP Options show Source Port Range from 0 to 0 and Destination Port Range from 443 to 443. There is a Service Group List field.

UDP	UDP-443	0	443	-
-----	---------	---	-----	---

- Servis tipi IP seçildiği durumda IP Protokol sayısına göre IP Servisi ekleme işlemi yapılır.
- Servis tipi ICMP seçildiği durumda ICMP seçeneklerine(Echo Reply, Destination Unreachable vb.) göre ekleme işlemi yapılır.

16.1.5 Servis Grubu

Eklenen Servislerin gruplandırılmasının yapıldığı modüldür.

Name	Description	Members	Manage
1 DHCP		bootpc bootps	[Edit] [Delete]
2 DNS		domain domain	[Edit] [Delete]
3 IPSEC		ESP AH	[Edit] [Delete]
4 NETBIOS		netbios-ns netbios-ssn netbios-dgm	[Edit] [Delete]
5 Real Player		Real-Audio rtsp	[Edit] [Delete]
6 Useful_ICMP		ping reply all ICMP unreachable time exceeded in transit time exceeded in transit	[Edit] [Delete]
7 nfs		nfs nfs	[Edit] [Delete]

1	Ekle	Eklenen servislerin gruplandırıldığı butondur.
2	İsim	Eklenen servis grubunun isminin görüntülediği bölümdür.
3	Açıklama	Servis Grubunun açıklamasının görüntülediği bölümdür.
4	Üyeler	Servis grubuna eklenen servislerin listesinin görüntülediği bölümdür.
5	Yönet	Eklenen servis grubunun silindiği veya düzenlendiği bölümdür. Cihaz üzerinde varsayılan olarak gelen servis grupları üzerinde düzenleme yapılmaz.

-Servis Grubu eklemek için 'ekle' butonuna tıkladıktan sonra Labris UTM cihazı üzerinde bulunan Servislerin gruplandırılması yapılır.

Service Group [X]

1 Name:

2 Description:

3 Service List:
 http
 https

4

5

1	İsim	Gruplanacak olan servislere verilecek ismin belirtildiği yerdir.
2	Açıklama	Eklenecek servis grubuna açıklama girildiği bölümdür.
3	Servis Listesi	Cihaz üzerinde bulunan servislerin veya eklenen servislerin seçildiği bölümdür.
4	Kaydet	Gruplandırılan servislerin kaydedildiği butondur.
5	Kapat	'ekle' butona basıldıktan sonra açılan ekranın kapatıldığı butondur. Kapat butonuna basıldıktan

Not

Servis Grubuna eklenen servisler aşağıdaki ekran görüntüsündeki olmaktadır.

16.2 Politika Nesnesi

Politikalar modülünde kullanılacak Politika Nesnelerinin oluşturulduğu modüldür. Politika Nesneleri menüsünde Zaman, Bant Genişliği ve DoS&DDoS nesneleri ekleme işlemleri yapılır.

Name	Start Date and Time	End Date and Time	Days	Manage
1 08-18hours	2024-05-27 08:00	2024-05-30 18:00	Monday, Tuesday, Wednesday, Thursday, Friday	[Edit] [Delete]
2 afterhours	18:00	00:00	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	[Edit] [Delete]
3 Sat			Saturday	[Edit] [Delete]
4 Sun			Sunday	[Edit] [Delete]
5 weekends			Saturday, Sunday	[Edit] [Delete]
6 workhours	09:00	17:00	Monday, Tuesday, Wednesday, Thursday, Friday	[Edit] [Delete]

Not

Politika Nesneleri sadece Güvenlik Duvarı modülünde kullanılır.

16.2.1 Zaman

Politikalar modülündeki Genel Politika modülünde kullanılmak üzere zaman nesnesi eklendiği veya Labris UTM cihazı üzerinde varsayılan olarak gelen zaman nesnelerinin görüntülediği modüldür. Gelen Politika modülünde kurala eklenen Zaman nesnelere kuralın çalışma zamanını belirtir.

Name	Start Date and Time	End Date and Time	Days	Manage
08-18hours	2024-05-27 08:00	2024-05-30 18:00	Monday, Tuesday, Wednesday, Thursday, Friday	[Edit] [Delete]
afterhours	18:00	00:00	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	[Edit] [Delete]
Sat			Saturday	[Edit] [Delete]
Sun			Sunday	[Edit] [Delete]
weekends			Saturday, Sunday	[Edit] [Delete]
workhours	09:00	17:00	Monday, Tuesday, Wednesday, Thursday, Friday	[Edit] [Delete]

1	Ekle	Zaman nesnesinin eklendiği butondur.
2	İsim	Eklene Zaman nesnelerinin ismi görüntülenir.
3	Başlangıç Tarihi ve Zaman	Eklene Zaman nesnelerinin başlangıç tarihinin ve zamanının görüntülediği bölümdür.
4	Bitiş Tarihi ve Zaman	Eklene Zaman nesnelerinin bitiş tarihinin ve zamanının görüntülediği bölümdür.
5	Günler	Eklene Zaman nesnelerinde seçilen günlerin görüntülediği bölümdür.
6	Yönet	Eklene Zaman nesnesinin düzenlendiği veya silindiği bölümdür. Varsayılan olarak cihaz üzerinde bulunan Zaman nesnelere silinemez veya düzenlenemez.

-Zaman nesnesi eklemek için 'ekle' butonuna tıklayarak Zaman nesnesi eklenir. 'ekle' butonuna tıkladıktan eklenecek Zaman nesnesinin başlangıç ve bitiş zamanı, başlangıç ve bitiş saati veya çalışacağı günlerin seçilir.

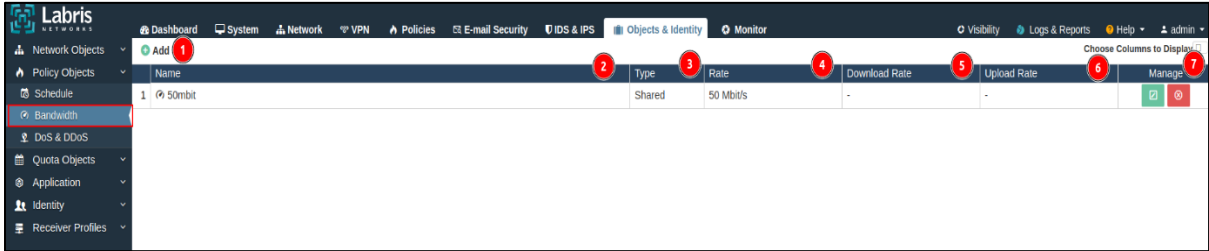
1	İsim	Eklenecek Zaman nesnesinin isminin girildiği bölümdür.
2	Açıklama	Eklenecek Zaman nesnesinin açıklamasının girildiği bölümdür.
3	Seçenekler	Kuralın çalışacağı, başlangıç ve bitiş tarihleri, başlangıç ve bitiş saatleri ve haftanın günleri seçilir.
4	Kaydet	Zaman nesnesinin kaydedildiği butondur.
5	Kapat	'ekle' butonuna tıklanarak açılan ekranın kapatıldığı butondur.

-Zaman nesnesi olarak eklenen nesnenin Genel Politika'da kullanımı aşağıdaki gibidir.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (7)	AdminIPs	remotelan	*	*	Drop	08-18hours	*	*	On	

16.2.2 Bant Genişliği

Politikalar modülünde kullanılmak üzere Bant Genişliği nesnesi tanımlanır. Tanımlanan nesneyi Genel Politika modülünde kullanılır. Bant Genişliği nesnesi eklemesi iç networklerinin Bant Genişliğini kontrol etmektir.



1	Ekle	Bant Genişliği nesnesinin eklendiği butondur.
2	İsim	Eklene Bant Genişliği nesnesinin isminin bölümdür.
3	Tip	Bant Genişliği nesnesinin tipinin görüntülediği bölümdür. Tip olarak paylaşımlı ve ortak olmak üzere iki adet vardır.
4	Oran	Bant Genişliği nesnesinin oranının görüntülediği bölümdür.
5	İndirme Oranı	Bant Genişliği nesnesinin indirme oranının görüntülediği bölümdür.
6	Yükleme Oranı	Bant Genişliği nesnesinin yükleme oranının görüntülediği bölümdür.
7	Yönet	Eklene Bant Genişliği nesnesinin silindiği veya düzenlendiği bölümdür.

-Bant Genişliği nesnesi eklemek için 'ekle' butonuna tıklayarak Bant Genişliği nesnesi eklenir. 'ekle' butonuna tıkladıktan eklenecek Bant Genişliği tipi belirtilerek ayarlamalar yapılır.

1	İsim	Bant Genişliği nesnesinin isminin girildiği bölümdür.
2	Açıklama	Bant Genişliği nesnesinin açıklamasının girildiği bölümdür.
3	Tip	Bant Genişliği nesnesinin tipinin seçildiği bölümdür. Tip olarak paylaşılan seçilmesi durumunda ağa dahil olan herkesin belirtilen değeri bölüşür. Örn (50Mbit seçilmesi durumunda ve ağda 50 kullanıcı varsa ağa bağlı olan cihazlar Bant Genişliği 1 Mbit'tir(50/50=1Mbit.) IP Başına Seçilmesi durumunda bant genişliği sabittir.
4	Hız	Tipin paylaşılan seçildiği durumda girilen değerdir. İnternet hızı belirtilir.
5	Tavan	Tipin paylaşılan seçildiği durumda girilen değerdir. Bant Genişliğinin tavan değeri girilir.
6	Atılım	Tipin paylaşılan seçildiği durumda girilen değerdir. Bant Genişliğinin atılım değeri girilir.

7	Öncelik	Tipin paylaşılan seçildiği durumda girilen değerdir. Bant Genişliğinin öncelik değeri girilir.
8	Arayüzler	Tipin paylaşılan seçildiği durumda girilen değerdir. Bant Genişliğinin uygulanacağı arabirim seçilir.
9	Kaydet	Bant Genişliği ayarlarının kaydedildiği butondur.
10	Kapat	'ekle' butonuna tıklanarak açılan pencerenin kapatıldığı butondur.

-Bant Genişliği nesnesinin Genel Politika'da kullanımı aşağıdaki gibidir.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (6)	lan	*	*	*	Log	*	50mbit	*	On	

16.2.3 DoS&DDoS

Politikalar modülünde kullanılmak üzere DoS&DDoS nesnesi tanımlanır. DoS&DDoS nesnesine tanımlanan değerlere göre iç ağda çalışan servislerin üzerinde koruma sağlar.

1	Ekle	Bant Genişliği nesnesinin isminin girildiği bölümdür.
2	İsim	Bant Genişliği nesnesinin açıklamasının girildiği bölümdür.
3	DNAT Öncesi	Paketlerin NAT işlemi yapılmadan önceki durumunu ifade eder. Nesnesinin DNAT işleminden önce çalışıp çalışmadığı bilgisinin verildiği bölümdür.
4	Log	DoS&DDoS nesnesinin engelleme yapıldığı durumda logunun tutulacağını gösterildiği bölümdür.

5	Drop	DoS&DDoS nesnesinin engelleme işleminin gösterildiği bölümdür.
6	Yönet	DoS&DDoS nesnesinin silindiği veya yönetildiği bölümdür.

-DoS&DDoS nesnesi eklemek için 'ekle' butonuna tıklayarak DoS&DDoS nesnesi eklenir. 'ekle' butonuna tıkladıktan eklenecek DoS&DDoS nesnesinin engelleyeceği saldırılar seçilir. Bunlar SYN, UDP, Bağlantı ve ICMP saldırılarıdır.

1	İsim	DoS&DDoS nesnesinin isminin girildiği bölümdür.
2	Açıklama	DoS&DDoS nesnesinin açıklamasının girildiği bölümdür.
3	İşlem	DoS&DDoS nesnesinin işlemi seçilir.
4	Syn Saldırısı	DoS&DDoS nesnesinin Syn Saldırısı olarak algılayacağı değerler girilir.
5	UDP Saldırısı	DoS&DDoS nesnesinin UDP Saldırısı olarak algılayacağı değerler girilir.
6	Bağlantı Saldırısı	DoS&DDoS nesnesinin Bağlantı(CONN) Saldırısı olarak algılayacağı değerler girilir.

7	ICMP Saldırısı	DoS&DDoS nesnesinin ICMP Saldırısı olarak algılayacağı değerler girilir.
8	Kaydet	DoS&DDoS nesnesinin kaydedildiği butondur.
9	Kapat	'ekle' butonuna tıkladıktan sonra açılan ekranın kapatıldığı butondur.

-SYN, UDP, Bağlantı ve ICMP Saldırı açılması durumunda kaynak başına, hedef başına ve toplam gelen isteklere göre DoS&DDoS nesnesi ayarlanır.

1	Per Source	10	11
2	Per Destination	10	11
3	Total	10	11

1	Kaynak Başına	Kaynak başına kaç adet istek geleceğinin belirtildiği bölümdür.
2	Hedef Başına	Hedef başına kaç adet istek geleceğinin belirtildiği bölümdür.
3	Toplam	Toplam kaç adet istek geleceğinin belirtildiği bölümdür.

-DoS&DDoS nesnesinin Genel Politika'da kullanımı aşağıdaki gibidir.

Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (9)	*	*	*	*	Drop	*	*	SYN10	On	

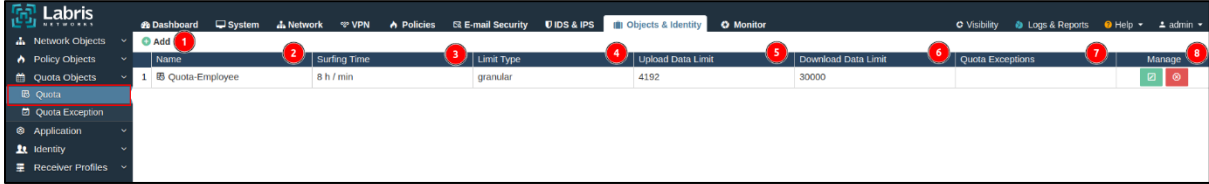
16.3 Kota Nesnesi

Politikalar modülünde kullanılacak Kota Nesnelerinin oluşturulduğu modüldür. Kota Nesneleri menüsünde Kota ve Kota İstisna nesneleri ekleme işlemleri yapılır.

Name	Surfing Time	Limit Type	Upload Data Limit	Download Data Limit	Quota Exceptions	Manage
1 Quota-Employee	8 h / min	granular	4192	30000		

16.3.1 Kota Nesnesi

Nesneler ve Kimlikler modülünde eklenen kullanıcılara kota nesnesi eklenmek istenildiği durumda Kota nesnesi oluşturmak gerekir. Nesneler ve Kimlikler modülünde eklenen kullanıcı Wauth'da oturum açtığı durumda belirlenen kota politikasına göre internette gezinebilir.



1	Ekle	Kota nesnesi eklendiği butondur.
2	İsim	Kota nesnesinin isminin görüntülediği bölümdür.
3	Gezirme Süresi	Kota nesnesinin sahip olan kullanıcının internette gezinme süresinin görüntülediği bölümdür.
4	Limit Tipi	Kota nesnesinin limit tipinin görüntülediği bölümdür.
5	Yüklenecek Veri Limiti	Kota nesnesinin yükleme limitinin görüntülediği bölümdür.
6	İndirilecek Veri Limiti	Kota nesnesinin indirme limitinin görüntülediği bölümdür.
7	Kota İstisnası	Kota istisnasının seçildiği bölümdür. Bu bölümü kullanmak için kota istisnası eklemek gerekir.
8	Yönet	Eklenen kota istisnasının silindiği veya düzenlendiği bölümdür.

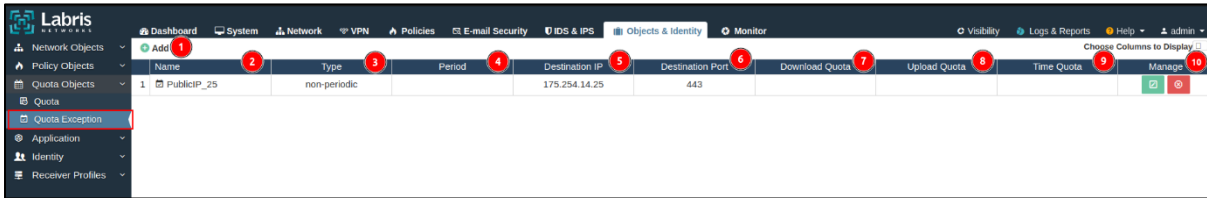
-Kota nesnesi eklemek için 'ekle' butonuna tıklayarak Kota nesnesi eklenir. 'ekle' butonuna tıkladıktan eklenecek Kota nesnesinin internette gezinme, yükleme ve indirme değerleri belirtilir.

1	İsim	Kota nesnesinin isminin girildiği bölümdür.
2	Tip	Kota nesnesinin tipinin seçildiği bölümdür. Tekrar Eden seçilmesi durumunda belirtilen dönem boyunca kota nesnesi sıfırlanır. Tekrar etmeyen seçildiği durumda ise kota nesnesi sadece belirtilen zamanda çalışır.
3	Dönem	Tipinin tekrar eden seçilmesi durumunda ayarlanır. Gün, hafta, ay ve yıl olarak seçilir.
4	İnternet Gezinme Süresi	İnternette gezinme süresi belirtilir. Sınırsız işaretlenmesi durumunda internette gezinme süresi sınırsızdır.
5	İndir	Kota nesnesinin indirme limiti belirtilir. Sınırsız işaretlenmesi durumunda indirme limiti sınırsızdır.
6	Yükle	Kota nesnesinin yükleme limiti belirtilir. Sınırsız işaretlenmesi durumunda yükleme limiti sınırsızdır.
7	Kota İstisnası	Kota istisnasının seçildiği bölümdür. Bu bölümü kullanmak için kota istisnası eklemek gerekir.

8	Kaydet	Kota nesnesinin kaydedildiği butondur.
9	Kapat	'ekle' butonuna basıldıktan sonra açılan ekranın kapatıldığı butondur.

16.3.2 Kota İstisnası

Kota istisnası modülünde İnternet gezinmesi boyunca kota politikasına takılmayacak istisna tanımlanır. İstisna tanımlaması yapılırken hedef IP adresi ve Port bilgilerinin bilinmesi gerekmektedir.



1	Ekle	Kota istisnası eklemek için kullanılan butondur.
2	İsim	Kota istisnasının isminin görüntülediği bölümdür.
3	Tip	Kota istisnasının tipinin görüntülediği bölümdür.
4	Süre	Hedef Ip adresinde geçirilecek süresinin görüntülediği bölümdür. Boş olarak görünüyorsa sınırsızdır.
5	Hedef IP	Kota istisnası yazılan Hedef IP adresinin görüntülediği bölümdür.
6	Hedef Port	Kota istisnası yazılan Hedef Portunun görüntülediği bölümdür.
7	İndirme Kotası	Hedef IP adresi özelinde indirme kotasının belirtildiği bölümdür.
8	Yükleme Kotası	Hedef IP adresi özelinde yükleme kotasının görüntülediği bölümdür.
9	Zaman Kotası	Hedef IP adresi özelinde zaman kotasının

		görüntülendiği bölümdür.
10	Yönet	Kota istisnasının düzenlendiği veya silindiği bölümdür.

-Kota istisnası ekleme için 'ekle' butonuna tıklayarak Kota İstisnası ekleme işlemi yapılır.

1	İsim	Kota istisnasının isminin görüntülendiği bölümdür.
2	Tip	Kota istisnasının tipinin seçildiği bölümdür.
3	Hedef IP/Port	Kota istisnası yazılacak IP adresi veya port bilgisinin girildiği bölümdür.
4	İnternet Gezinme Süresi	Belirtilen hedef IP adresindeki gezinme süresinin belirtildiği bölümdür.
5	İndir	Belirtilen Hedef IP adresindeki indirme limitinin belirtildiği bölümdür.
6	Yükleme	Belirtilen Hedef IP adresindeki yükleme limitinin belirtildiği bölümdür.
7	Kota İstisnası Döngüsü	Kota istisnasının tekrarlama sıklığının belirtildiği bölümdür.

8	Kaydet	Kota istinasının kaydedildiği butondur.
9	Kapat	'ekle' butonuna basıldıktan sonra açılan ekranın kapatıldığı butondur.

16.4 Uygulama

Labris UTM cihazı üzerinde tutulan Uygulamaların görüntülediği modüldür. Bu modülünde bulunan uygulamalar listelene halinde Politikalar modülünde kullanılır.

Name	Category	Risk Q	Productivity Q
Q	Q	Q	Q
1 050Plus	Messaging	2	2
2 104	Job Search, News	3	3
3 114la	Portal Sites	3	3
4 11st	Online Shopping	3	3
5 12306	Travel	3	3
6 12306.cn	Web Services	1	4
7 123cha	Technology (General)	3	3
8 123movies	Streaming Media	5	1
9 123rf	Online Shopping, Photo Sharing	3	3
10 126	Web-based E-mail	3	3
11 126.com	Mail	2	4
12 1337x	Torrent Repository	3	3
13 15bets10	Web Services	3	3
14 163	Online Ads, Portal Sites	3	3
15 1688	Fashion & Beauty	3	3
16 16lao	Content Servers	3	3
17 17173.com	Social Networking	2	2
18 17ok	Finance (General)	3	3
19 17rack	Shipping & Logistics	3	3
20 189	Online Shopping, Web Hosting, ISP & Telco	3	3
21 1905	Entertainment News & Celebrity Sites	3	3
22 1and1	Web Hosting, ISP & Telco	3	3
23 1fichier	File Transfer	5	1
24 2345	Malware Distribution Point, Compromised, Portal Sites	3	3
25 2345.com	Web Services	1	3
26 247 Media	Web Services	1	3
27 2ch	Sex & Erotic, Community Forums	3	3
28 2ch-c	Personal Pages & Blogs	3	3

16.4.2 Liste

Labris UTM cihazı üzerinde tutulan Uygulamaların liste halinde görüntülediği modüldür.

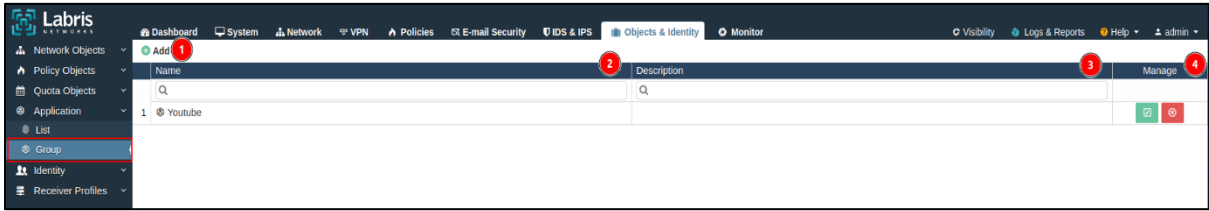
Name	Category	Risk Q	Productivity Q
1 050Plus	Messaging	2	2
2 104	Job Search, News	3	3
3 114la	Portal Sites	3	3
4 11st	Online Shopping	3	3
5 12306	Travel	3	3
6 12306.cn	Web Services	1	4
7 123cha	Technology (General)	3	3
8 123movies	Streaming Media	5	1
9 123rf	Online Shopping, Photo Sharing	3	3
10 126	Web-based E-mail	3	3
11 126.com	Mail	2	4

1	İsim	Uygulamaların adlarının görüntülediği bölümdür.
2	Kategori	Uygulamaların bulunduğu kategorilerin görüntülediği bölümdür.

3	Risk	Uygulamaların risk değerlerinin görüntülediği bölümdür. Risk seviyesi uygulama kullanırken istenmeyen durumların oluşabileceğini ifade eder.
4	Verimlilik	Uygulamaların verimlilik değerlerinin görüntülediği bölümdür. Verimlilik uygulamanın eğlence veya iş için kullanıldığı ile ilgili oran sunar.

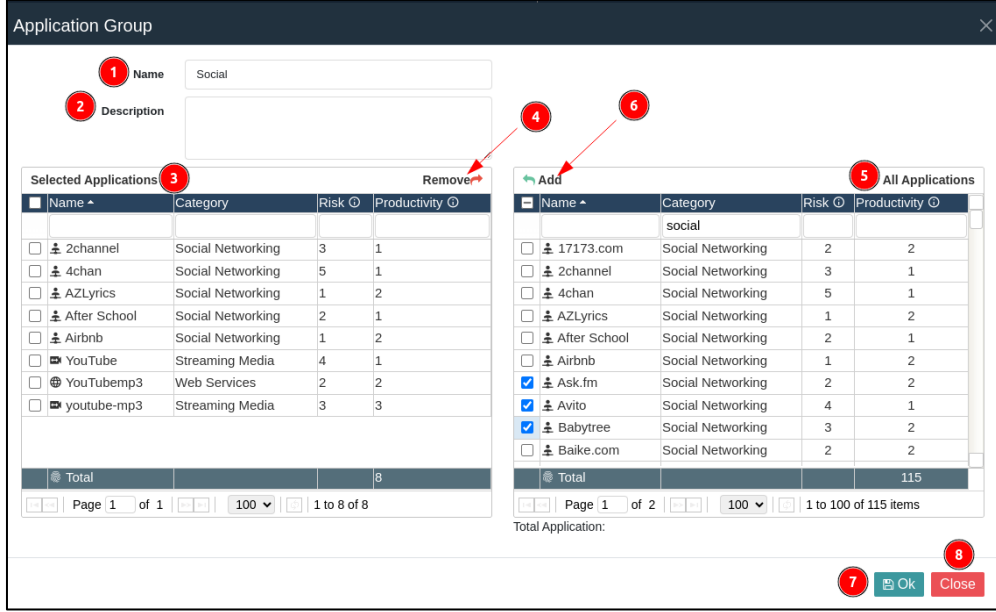
16.4.2 Grup

Uygulama listesinde bulunan uygulamaların gruplandırıldığı modüldür.



1	Ekle	Uygulama grubu ekleme işleminin yapıldığı butondur.
2	İsim	Uygulama grubunun isminin görüntülediği bölümdür.
3	Açıklama	Uygulama grubunun açıklamasının görüntülediği bölümdür.
4	Yönet	Uygulama grubunun düzenlendiği veya silindiği bölümdür.

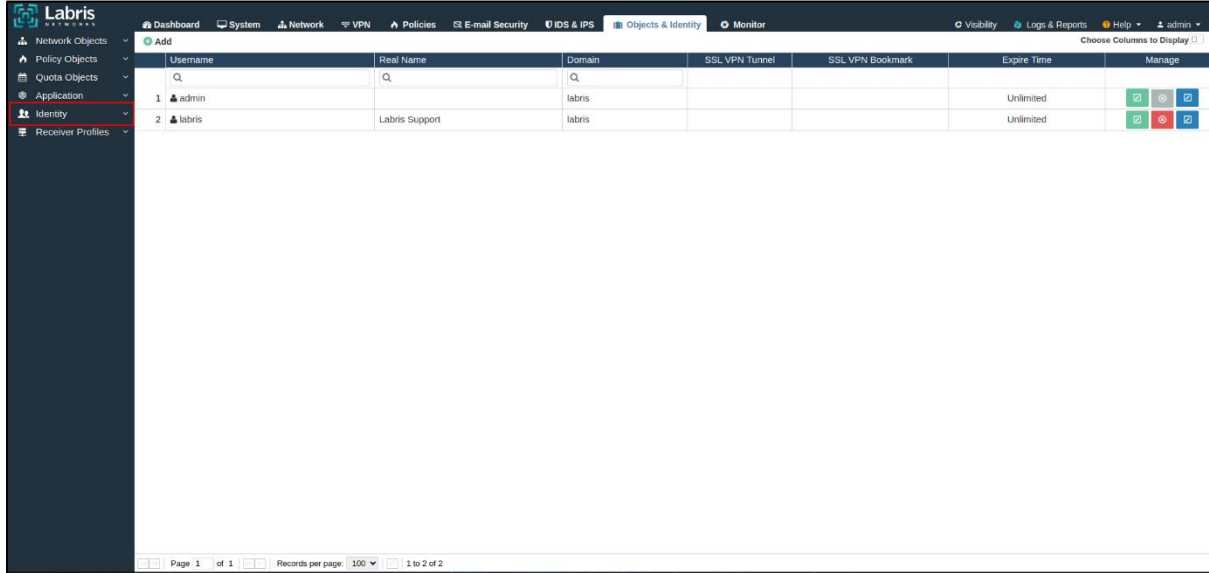
-Uygulama grubu eklemek için 'ekle' butonuna tıklamak gerekmektedir. 'ekle' butonuna tıkladıktan sonra Labris UTM cihazı üzerinde bulunan uygulamalar gruplandırılır.



1	İsim	Uygulama grubunun isminin girildiği bölümdür.
2	Açıklama	Uygulama grubuna ait açıklamanın girildiği bölümdür.
3	Seçilen Uygulamalar	Tüm Uygulamalar listesinden eklenen uygulamaların görüntülediği bölümdür.
4	Kaldır	Seçilen uygulamalar listesinden seçilen uygulamanın kaldırıldığı butondur.
5	Tüm Uygulamalar	Labris UTM cihazı üzerinde bulunan uygulamaların listesinin görüntülediği butondur.
6	Ekle	Tüm uygulamalar listesinden seçilen uygulamaların Seçilen Uygulamaların listesine eklendiği butondur.
7	Kaydet	Uygulama gruplarının kaydedildiği butondur.
8	Kapat	'ekle' butonuna tıkladıktan sonra açılan ekranın kapatıldığı butondur.

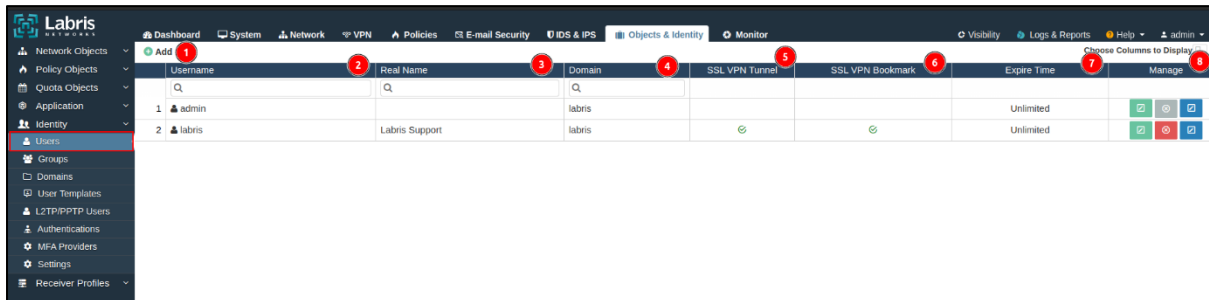
16.5 Kimlik

Labris UTM cihazı üzerinde kullanıcılar gruplanabilir, kullanıcıların alan adları değiştirilebilir, kullanıcı şablonları oluşturulabilir. Ayrıca, L2TP/PPTP VPN için kullanıcılar oluşturulabilir, Aktif Dizin sunucusundaki kullanıcılar çekilebilir ve SSLVPN'de kullanılacak MFA sağlayıcı eklenir ve Kimlik Ayarlarının yapıldığı modüldür.



16.5.1 Kullanıcı

Labris UTM cihazına kullanıcı ekleme işleminin yapıldığı bölümdür. Bu modüle eklenen kullanıcılar Labris UTM cihazına giriş yapmak için admin yetkisi verilir. SSL VPN'e bağlanması için gerekli yetkilendirme yapılır. Bunlara ek olarak oluşturulan kullanıcılar WAUTH'a giriş yapabilir.



1	Ekle	Labris UTM cihazı üzerinde kullanıcı ekleme işleminin yapıldığı butondur.
2	Kullanıcı Adı	Eklenen kullanıcının Kullanıcı Adının görüntülediği bölümdür. Kullanıcılar Kullanıcı Adlarını kullanarak SSL VPN ve Labris Web Arayüze giriş yapabilirler.

3	Gerçek İsim	Eklenecek kullanıcının gerçek isminin görüntülediği bölümdür.
4	Alan Adı	Eklenecek kullanıcının alan adı görüntülenir.
5	SSL VPN Tüneli	Eklenecek kullanıcının SSL VPN yetkisinin olup olmadığının görüntülediği bölümdür.
6	SSL VPN Yerimi	Eklenecek kullanıcının SSL VPN Yerimi yetkisinin olup olmadığının görüntülediği bölümdür.
7	Son Kullanma Zamanı	Eklenecek kullanıcının hesabının son kullanma zamanının görüntülediği bölümdür.
8	Yönet	Eklenecek kullanıcının düzenlediği, silindiği ve kotalarının sıfırlandığı bölümdür.






-Kullanıcı eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra açılan penceredeki kullanıcıya dair bilgileri doldurularak kullanıcı ekleme işlemi sonlanır.

1	Etkinleştir	Eklenecek olan kullanıcının etkinleştirildiği butondur.
2	Kullanıcı Şablonu	Kullanıcı Şablonu modülünde eklenecek Kullanıcı Şablonunun seçildiği bölümdür.

3	Kullanıcı Adı	Eklenecek kullanıcının Kullanıcı Adının girildiği bölümdür.
4	Gerçek İsim	Eklenecek kullanıcının Gerçek İsmine girildiği bölümdür.
5	Telefon	Kullanıcının telefon numarasının girildiği bölümdür.
6	E-posta	Kullanıcının e-posta adresinin girildiği bölümdür.
7	Şifre	Kullanıcının şifresinin girildiği bölümdür. Şifreyi rastgele vermek için 'çark' butonuna tıklamak gerekir.
8	Geçersiz Olacağı Zaman	Kullanıcı için açılan hesabın geçersiz olacağı zamanın belirtildiği bölümdür.
9	Dolaşım	Kullanıcıya dolaşım yetkisi verildiği butondur.
10	SSL VPN Tüneli	Eklenecek Kullanıcı hesabına SSL VPN'e giriş yapma yetkisi verildiği bölümdür.
11	SSL VPN Yerimi	Eklenecek Kullanıcı hesabına SSL VPN Yerimi yetkisinin verildiği bölümdür.
12	Ağ Adresi	Kullanıcı SSL VPN'de bağlandığında aldığı IP adresinin belirtildiği bölümdür. IP adresi yazmak istenildiği durumda otomatikteki işaretin kaldırılması gerekir.
13	Alan Adı	Kullanıcının alan adının seçildiği butondur.
14	Grup	Eklenecek kullanıcının ekleneceği grubun seçildiği bölümdür.
15	Kota	Kullanıcıya kota politikası uygulanacağı durumlarda eklenen Kota Objesi seçilir.

16	Wauth Kuralı	Kullanıcı için yazılmış WAUTH kuralı var ise WAUTH kuralı seçilir.
17	MAC Adresi	Kullanıcının MAC adresi bilgisinin girildiği bölümdür.
18	Eş Zamanlı Oturum	Kullanıcının eş zamanlı oturum sayısının düzenlendiği bölümdür.
19	2FKD	Kullanıcı SSL VPN'e giriş yaparken kimlik bilgisini doğrulamak için çift faktör doğrulamaya girmesini sağlayan butondur.
20	2FKD Metodu	2FKD metodunun seçildiği bölümdür.
21	Sağlayıcı Profili	2FKD sağlayıcı bilgisinin seçildiği bölümdür.
22	Kaydet	Eklenecek Kullanıcının bilgilerinin kaydedildiği butondur.
23	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında kullanıcı için yapılan değişiklikleri kaydetmeden kapatır.

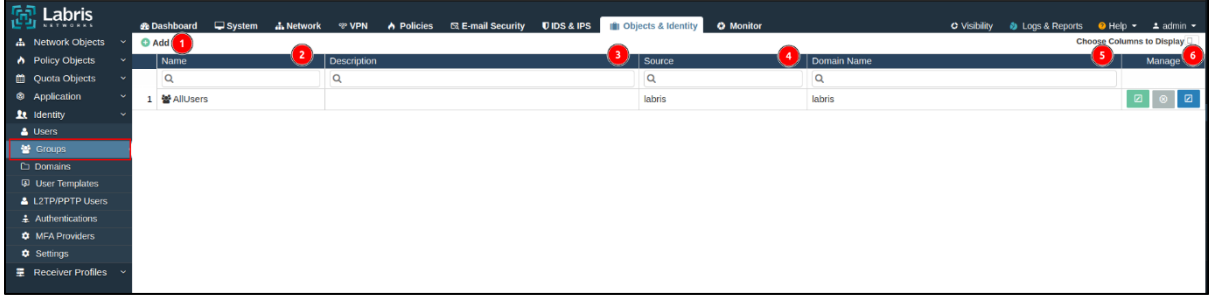
-Eklenecek kullanıcının bilgilerini değiştirmek için Yönet bölümünde bulunan düzenle butonuna tıklanır.

	Username	Real Name	Domain	SSL VPN Tunnel	SSL VPN Bookmark	Expire Time	Manage
	Q	Q	Q				
1	admin		labris			Unlimited	
2	2Labris	Labris Support2	labris			Unlimited	
3	labris	Labris Support	labris			Unlimited	

-Kullanıcının bulunduğu satırdaki düzenle butonuna tıkladıktan sonra kullanıcının hesap bilgileri düzenlenir.

16.5.2 Gruplar

Eklenen kullanıcıların gruplandırıldığı bölümdür. Gruba bağlı dahil olan kullanıcıların hepsine SSL VPN, Kota veya Wauth yetkilerinin verilir.



1	Ekle	Kullanıcı Grubu ekleme işleminin yapıldığı butondur.
2	İsim	Kullanıcı grubunun isminin görüntülediği bölümdür.
3	Açıklama	Kullanıcı grubunun açıklamasının görüntülediği bölümdür.
4	Kaynak	Kullanıcı grubunun kaynak bilgisinin görüntülediği bölümdür.
5	Alan Adı	Kullanıcı grubunun alan adının görüntülediği bölümdür.
6	Yönet	Kullanıcı grubunun düzenlendiği, silindiği veya kotalarının sıfırlandığı bölümdür.

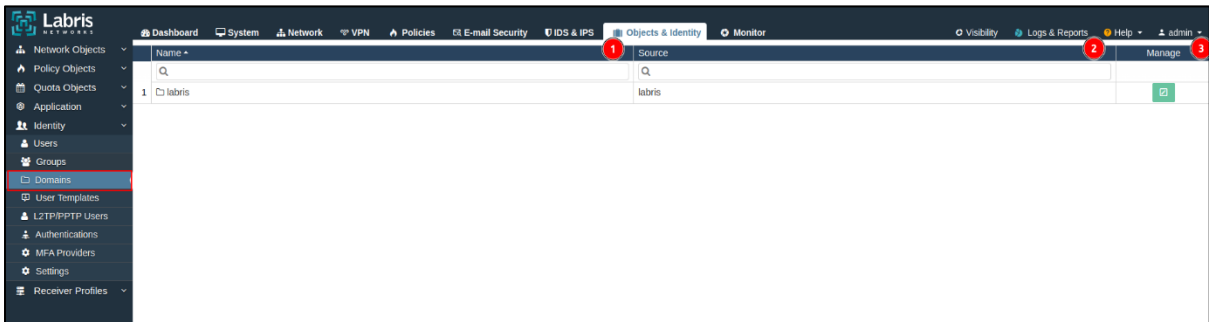
-Kullanıcı grubu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra eklenecek grup bilgileri veya eklenen kullanıcıların gruplandırılır.

1	Grup İsmi	Eklecek Grubun Grup isminin girildiği bölümdür.
2	Açıklama	Eklenecek Grup ile ilgili açıklamanın girildiği bölümdür.
3	SSL VPN Tünel	Gruba eklenen kullanıcıların SSL VPN yetkisi verildiği butondur.
4	SSL VPN Yerimi	Gruba eklenen kullanıcıların SSL VPN Yerimi yetkisi verildiği butondur.
5	Alan Adı	Eklenecek Grubun alan adının seçildiği bölümdür.
6	Wauth Kuralı	Eklenecek Grubun WAUTH Kuralı seçildiği bölümdür.
7	Kota	Gruba dahil olan kullanıcılar için Kota objesi seçildiği bölümdür.
8	2FKD	Gruba dahil olan kullanıcılar için çift faktör

		doğrulamasının açıldığı bölümdür.
9	Seçilen Kullanıcı ve Gruplar	Gruba dahil olan kullanıcıların görüntülediği bölümdür.
10	Kaldır	Gruba dahil olan kullanıcıların ve grupların kaldırıldığı butondur.
11	Tüm Kullanıcı ve Gruplar	Eklenen tüm kullanıcı ve grupların görüntülediği bölümdür.
12	Ekle	Tüm Kullanıcı ve Gruplarından seçilerin gruba dahil etmek için kullanıldığı butondur.
13	Kaydet	Kullanıcı grubunun kaydedildiği butondur.
14	Kapat	'ekle' butonun tıkladıktan sonra açılan pencerenin kapatıldığı butondur.

16.5.3 Alan Adı

Labris UTM cihazında Varsayılan olarak gelen alan adının görüntülediği veya düzenlendiği bölümdür.



1	İsim	Alan adının isminin görüntülediği bölümdür.
2	Kaynak	Alan adının görüntülediği bölümdür.
3	Yönet	Alan adının değiştirildiği bölümdür.

-Alan Adının düzenlenmesi için 'düzenle' butonuna tıklayarak Alan adı düzenlenir.



1	İsim	Alan adının isminin değiştirildiği bölümdür.
2	Kaydet	Alan adının kaydedildiği butondur.
3	Kapat	Alan adında değişiklik yapılmadan açılan pencerenin kapatıldığı butondur.

16.4.4 Kullanıcı Şablonu

Kullanıcı Şablonuna göre Kullanıcıların oluşturulması için kullanılan modüldür.



1	Ekle	Kullanıcı şablonu ekleme işleminin yapıldığı butondur.
2	Şablon Adı	Şablon adının görüntülediği bölümdür.
3	Kullanıcı Öneki adı	Eklenecek Kullanıcı Şablonunun Kullanıcı Adı Öneki'nin görüntülediği bölümdür.
4	Alan Adı	Kullanıcı şablonunun alan adının görüntülediği bölümdür.
5	SSL VPN Tüneli	Kullanıcı şablonunun SSL VPN Tünel yetkisinin görüntülediği bölümdür.
6	SSL VPN Yeri	Kullanıcı şablonunun SSL VPN Yeri yetkisinin görüntülediği bölümdür.

		görüntülediği bölümdür.
7	Geçersiz Olma Süresi	Kullanıcı Şablonuna göre eklenen kullanıcının hesabının geçersiz olma süresinin görüntülediği bölümdür.
8	Yönet	Eklenen Kullanıcı Şablonun düzenlendiği veya silindiği bölümdür.

-Kullanıcı Şablonu eklemek için 'ekle' butonuna tıklanır.

1	Etkinleştir	Eklenecek olan Kullanıcı Şablonun etkinleştirildiği butondur.
2	Şablon Adı	Şablon adının girildiği bölümdür.
3	Kullanıcı Adı Öneki	Kullanıcı Adı Önekinin girildiği bölümdür.
4	Gerçek İsim	Şablonun gerçek isminin girildiği bölümdür.
5	Telefon	Şablonun telefon numarasının girildiği bölümdür.
6	E-posta	Şablona ait olan e-posta adresinin girildiği bölümdür.

7	Şifre	Şablona ait şifrenin girildiği bölümdür.
8	Geçersiz Olacağı Zaman	Şablonun geçersiz olacağı sürenin seçildiği bölümdür.
9	Dolaşım	Şablonun dolaşım izni verildiği butondur.
10	SSL VPN Tüneli	Şablona SSL VPN'e giriş yapma yetkisi verildiği bölümdür.
11	SSL VPN Yerimi	Şablona SSL VPN Yerimi yetkisinin verildiği bölümdür.
12	Alan Adı	Şablonun alan adının seçildiği bölümdür.
14	Grup	Şablonun dahil olacağı grubun seçildiği bölümdür.
15	Kota	Şablonun dahil olacağı Kota Objесinin seçildiği bölümdür.
16	Wauth Kuralı	Şablonun dahil olacağı WAUTH Kuralının seçildiği bölümdür.
17	Eş Zamanlı Oturum	Şablonun eş zamanlı oturum sayısının düzenlendiği bölümdür.
19	2FKD	Şablonuna göre eklenen Kullanıcıların SSL VPN'e giriş yaparken kimlik bilgisini doğrulamak için çift faktör doğrulamaya girmesini sağlayan butondur.
20	Kaydet	Eklenecek Şablon bilgilerinin kaydedildiği butondur.
21	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında Şablon için yapılan değişiklikleri kaydetmeden kapatır.

-Kullanıcı şablonuna göre kullanıcı oluşturmak için Kullanıcı modülünde 'ekle' butonuna tıklayarak kullanıcı ekleme penceresini açıp Kullanıcı Şablonunu seçmek gerekmektedir.

The screenshot shows the 'User' configuration page. The 'User Template' dropdown is highlighted with a red box. The 'Enable' toggle is turned on. The 'Domain' is set to 'labris'. The 'Group' is set to 'Select Group'. The 'Quota' is set to 'Select Quota'. The 'WAUTH Rules' is set to 'Select Wauth Profile'. The 'MAC Address' is set to '00:00:00:00:00'. The 'Simultaneous Login' is set to '1-100' with an 'Unlimited' checkbox checked. The '2FA' toggle is turned off. The 'Send Account Information via SMS Provider' and 'E-mail' checkboxes are unchecked. The 'Create Another' checkbox is unchecked. The 'Save' button is highlighted in red.

16.5.5 L2TP/PPTP Kullanıcıları

L2TP ve PPTP VPN'e bağlanacak Kullanıcıların eklendiği modüldür. Bağlantı yapacak kullanıcıların kullanıcı adları, şifre ve IP bilgileri girilerek eklenir. Eklenen kullanıcı Kullanıcı adını ve şifresini kullanarak L2TP ve PPTP VPN'e giriş yaparlar.

The screenshot shows the 'L2TP/PPTP Users' table. The table has the following columns: Username, IP Address, Status, and Manage. The 'Add' button is highlighted with a red circle (1). The 'Username' column is highlighted with a red circle (2). The 'IP Address' column is highlighted with a red circle (3). The 'Status' column is highlighted with a red circle (4). The 'Manage' column is highlighted with a red circle (5). The table contains one row with the following data: Username: labrisupport, IP Address: 192.168.2.250, Status: (red circle), Manage: (green and red icons).

1	Ekle	L2TP/PPTP Kullanıcılarının eklendiği butondur.
2	Kullanıcı Adı	Eklenen L2TP/PPTP Kullanıcıların kullanıcı adlarının görüntülediği bölümdür.
3	IP Adresi	Eklenen L2TP ve PPTP kullanıcılarının IP adreslerinin girildiği bölümdür.

4	Durum	Eklenecek L2TP ve PPTP kullanıcılarının VPN yapabildiği durumunun görüntülediği bölümdür.
5	Yönet	Eklenecek L2TP ve PPTP VPN kullanıcısının bilgilerinin düzenlendiği veya kullanıcının silindiği bölümdür.

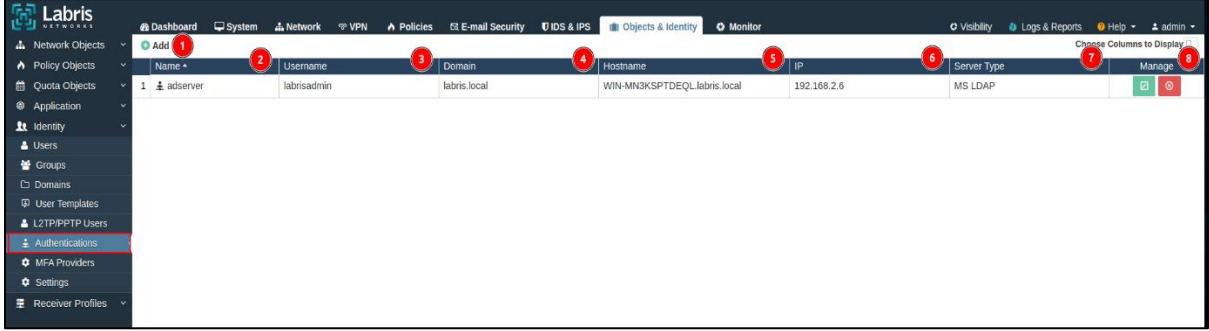
-L2TP/PPTP kullanıcı eklemek için 'ekle' butonuna tıklamak gerekir. 'ekle' butonuna tıkladıktan sonra açılan penceredeki L2TP/PPTP VPN' bağlanacak kullanıcının kullanıcı adının, şifresinin ve IP adresi bilgisi girilerek kaydedilir.

1	Etkinleştir	L2TP/PPTP Kullanıcılarının etkinleştirildiği butondur.
2	Kullanıcı Adı	Eklenecek L2TP/PPTP kullanıcısının kullanıcı adının girildiği bölümdür.
3	Şifre	Eklenecek L2TP/PPTP kullanıcısının şifresinin girildiği bölümdür.
4	IP Adresi	Eklenecek L2TP/PPTP kullanıcısının IP Adresinin girildiği bölümdür.
5	Açıklama	L2TP/PPTP kullanıcısına ait açıklamanın girildiği bölümdür.
6	Kaydet	L2TP/PPTP kullanıcısının bilgilerinin kaydedildiği butondur.
7	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında L2TP/PPTP Kullanıcısı için yapılan değişiklikleri kaydetmeden

		kapatır.
--	--	----------

16.5.6 Kimlik Doğrulama

Labris UTM cihazında Aktif Dizinde bulunan kullanıcı çekme işlemini yapmak için kullanılan modüldür. Aktif Dizinde bulunan kullanıcıları çekerek kullanıcılara WAUTH, SSL VPN ve Labris Web Arayüze erişim yetkisi verilir.



1	Ekle	Kimlik Doğrulama sunucusu ekleme işleminin yapıldığı butondur.
2	İsim	Kimlik doğrulama sunucusuna verilen ismin görüntülediği bölümdür.
3	Kullanıcı Adı	Kimlik Doğrulama sunucusu içerisinde açılmış admin yetkili kullanıcının kullanıcı adının görüntülediği bölümdür.
4	Alan Adı	Kimlik Doğrulama sunucusunun alan adı görüntülenir.
5	Sunucu İsmi	Kimlik Doğrulama sunucusunun ismi görüntülenir.
6	IP Adresi	Kimlik Doğrulama sunucusunun IP adresi görüntülenir.
7	Sunucu Tipi	Kimlik Doğrulama sunucusunun Sunucu Tipi görüntülenir. Sunucu tipleri MS LDAP, MS LDAP + NTML ve Open LDAP'tır.
8	Yönet	Eklene Kimlik Doğrulama sunucusunun düzenlendiği veya silindiği bölümdür.

-Kimlik Doğrulama sunucusu eklemek için “ekle” butonuna tıklanır. “ekle” butonuna tıkladıktan sonra sunucu tipi, alan adı, sunucu ismi, sunucunun IP adresi, çalışma grubu, Kimlik Doğrulama sunucusu içerisinde açılmış admin yetkili kullanıcı adı ve şifre bilgilerinin girilmesi gerekir.

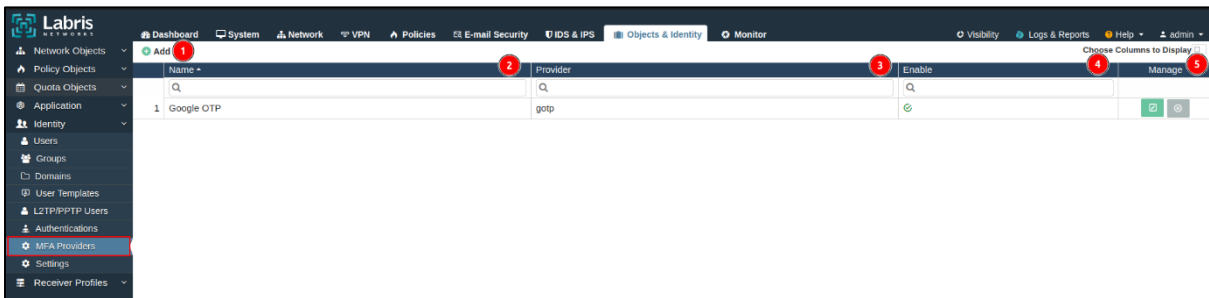
The screenshot shows the 'Authentication' configuration window. It has a dark header with the title 'Authentication' and a close button. The main area is white and contains several input fields and buttons. The fields are numbered 1 through 14. 1: Name (LBRAD), 2: Type (MS LDAP), 3: Domain Name (labris.local), 4: Hostname (WIN-MN3KSPTDEQL), 5: IP (192.168.1.100), 6: Workgroup (labris), 7: Username (adminlabris), 8: Password (masked), 9: Search Base, 10: Filter, 11: Port, 12: Test button, 13: Save button, 14: Close button. There is also a 'Show Password' checkbox.

1	İsim	Kimlik Doğrulama sunucusun Labris UTM cihazı üzerinde tutulacak isminin girildiği bölümdür.
2	Tip	Kimlik doğrulama sunucusunun Doğrulama tipinin seçildiği bölümdür.
3	Alan Adı	Kimlik Doğrulama sunucusunun alan adının girilir.
4	Sunucu İsmi	Kimlik Doğrulama sunucusunun isminin girildiği bölümdür.
5	IP	Kimlik Doğrulama sunucusunun IP adresinin girildiği bölümdür.
6	Çalışma Grubu	Kimlik Doğrulama sunucusunun Çalışma Grubunun girildiği bölümdür.
7	Kullanıcı Adı	Kimlik Doğrulama sunucusunda açılan admin yetkili

		kullanıcının kullanıcı adının girilir.
8	Şifre	Kimlik Doğrulama sunucusunda açılan admin yetkili kullanıcının şifresi girilir.
9	Arama Tabanı	Kimlik Doğrulama sunucusunun arama tabanı bilgileri girilir.
10	Filtre	Kimlik Doğrulama sunucusundan filtre dahilide kullanıcı çekmek için kullanılır.
11	Port	Kimlik Doğrulama sunucusundan kullanıcıları çekmek için kullanılacak portun girildiği bölümdür.
12	Test	Kimlik Doğrulama sunucusundan alınan verilerin doğruluğunun test edildiği butondur.
13	Kaydet	Kimlik Doğrulama sunucusundaki girilen değerlerin kaydedildiği butondur.
14	Kapat	' ekle ' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında Kimlik Doğrulama Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

16.5.7 MFA Sağlayıcılar

SSL VPN'de kullanılacak olan MFA sağlayıcıların görüntülediği veya MFA Sağlayıcı ekleme işleminin yapıldığı modüldür. SecurityID ve Google AUTH. Kullanarak MFA Sağlayıcı eklenir. Labris UTM cihazı içerisinde varsayılan olarak Google OTP gelmektedir.



1	Ekle	MFA Sağlayıcı eklendiği butondur.
---	-------------	-----------------------------------

2	İsim	Eklenen MFA Sağlayıcı isminin görüntülediği bölümdür.
3	Sağlayıcı	Sağlayıcı bilgisi görüntülenir.
4	Etkin	MFA Sağlayıcının etkinliğinin görüntülediği bölümdür.
5	Yönet	MFA Sağlayıcının düzenlendiği veya silindiği bölümdür.

-MFA Sağlayıcı eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra eklenecek MFA Sağlayıcının tipini SecurifyID veya Google Authenticator seçilir. Seçilen MFA Sağlayıcı tipine göre penceredeki veriler doldurulur.

-MFA Sağlayıcısının SecurifyID seçilmesi durumunda API URL, API Anahtarı, Kimlik Numarası, Faktör Türü(PUSH, Email, SMS ve Totp), bilgileri girilir.

1	Etkinleştir	Eklenecek MFA Sağlayıcının etkinleştirildiği butondur.
2	İsim	MFA Sağlayıcının isminin girildiği bölümdür.
3	Sağlayıcı	MFA Sağlayıcının seçildiği bölümdür.
4	API URL	SecurifyID seçilmesi durumunda girilecek sağlayıcının API URL.

5	API Anahtarı	SecurifyID seçilmesi durumunda girilecek sağlayıcının API Anahtarı.
6	Kiracı Kimlik Numarası	SecurifyID seçilmesi durumunda girilecek sağlayıcının kimlik numarasının girilir.
7	Varsayılan Faktör Tipi	Varsayılan faktör tipi seçilir.
8	Aynı IP Kimlik Doğrulama	Aynı IP adresinden OTP'siz isteklere izin verilmesi durumunda etkinleştirilir.
9	SSL Sertifikası	İsteklerde SSL Sertifikasını kullanılması gerektiği durumlarda etkinleştirilir.
10	Kaydet	MFA Sağlayıcı ayalarının kaydedildiği butondur.
11	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında MFA Sağlayıcı için yapılan değişiklikleri kaydetmeden kapatır.

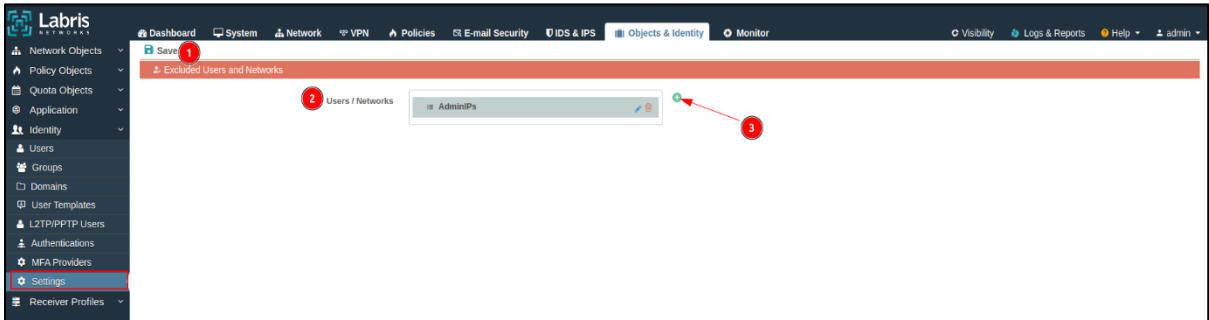
-MFA Sağlacısının Google Authenticator seçilmesi durumunda Sağlayıcı adı ve Geçerli Pencere Boyutu bilgileri girilir.

1	Etkinleştir	Eklenecek MFA Sağlayıcının etkinleştirildiği butondur.
2	İsim	MFA Sağlayıcının isminin girildiği bölümdür.

3	Sağlayıcı	MFA Sağlayıcının seçildiği bölümdür.
4	Sağlayıcı Adı	Google Auth. seçilmesi durumunda girilecek sağlayıcının Sağlayıcı Adı girilir
5	Geçerli Pencere Boyutu	Google Auth. seçilmesi durumunda girilecek sağlayıcının Geçerli Pencere Boyutu girilir.
6	Kaydet	MFA Sağlayıcı ayalarının kaydedildiği butondur.
7	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında MFA Sağlayıcı için yapılan değişiklikleri kaydetmeden kapatır.

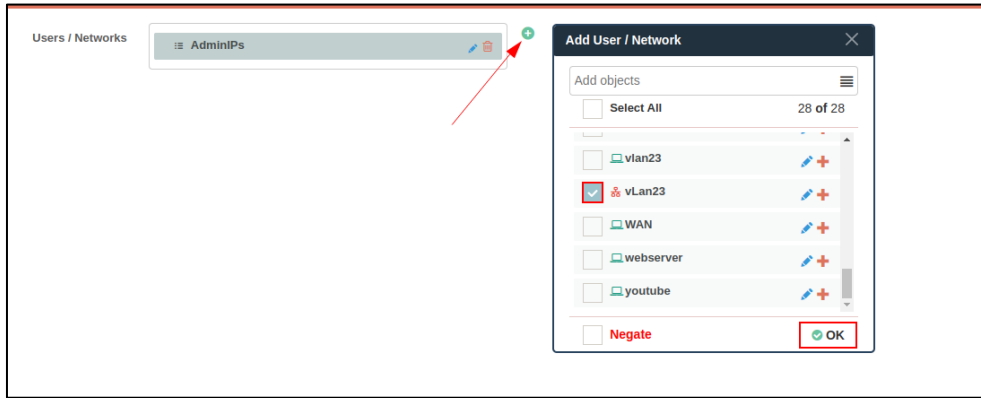
16.5.8 Ayarlar

Belirli kullanıcıların veya ağların güvenlik duvarının uyguladığı kısıtlamalardan muaf tutulmasını sağlar.



1	Kaydet	Dahil edilmemiş kullanıcı ve ağların kaydedildiği butondur.
2	Kullanıcı/Ağlar	Eklenecek kullanıcı ve ağların görüntülediği bölümdür.
3	Ekle	Dahil edilmemiş kullanıcı ve ağların eklendiği butondur.

-Dahil edilmemiş kullanıcı ve ağlar listesine eklemek için '+' butonuna tıklayarak kullanıcı ve ağlar eklenir.



16.6 Alıcı Profilleri

Labris UTM cihazı üzerinde Syslog, SNMP, HTTP, E-posta ve FTP profilleri eklenir.



16.6.1 Syslog

Labris UTM cihazına Syslog sunucusu eklemek için kullanılır. Eklenen Syslog sunucusu Güvenlik Duvarı modülünde kullanılır.



1	Ekle	Syslog sunucusu ekleme işleminin yapıldığı butondur.
2	İsim	Syslog sunucusunun isminin görüntülediği bölümdür.
3	Sunucu IP	Syslog sunucusunun IP adresinin görüntülediği bölümdür.
4	Port	Syslog sunucusunun port bilgisi görünütlenir.
5	Protokol	Eklenen syslog sunucusunun protokolü görüntülenir.

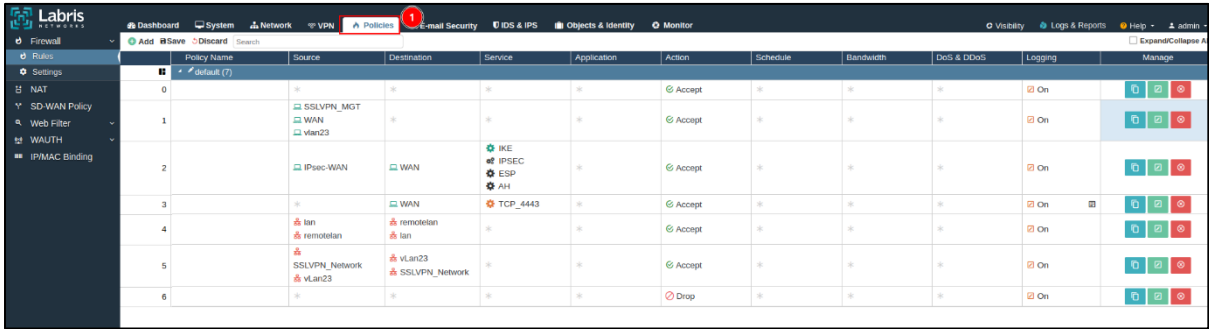
		Protokol UDP veya TCP'dir.
6	Yönet	Eklene Syslog sunucusunun düzenlendiği veya silindiği bölümdür.

-Syslog Sunucusu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra Syslog sunucusunun IP, port ve protokol bilgileri girilir.

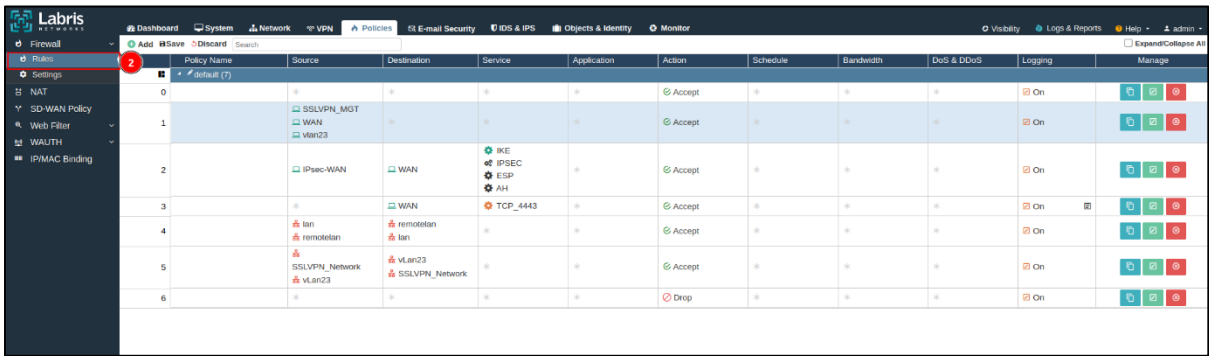
1	İsim	Syslog sunucusunun isminin girildiği bölümdür.
2	Sunucu IP	Syslog sunucusunun IP adresinin girildiği bölümdür.
3	Protokol	Syslog sunucusunun protokolünün seçildiği bölümdür. TCP ve UDP seçilir.
4	Port	Syslog sunucusunun port numarasının girildiği bölümdür.
5	Kaydet	Eklene syslog sunucusunun protokolü görüntülenir. Protokol UDP veya TCP'dir.
6	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında Syslog Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

-Eklenen Syslog sunucusunu kullanmak için ;

1. Politikalar menüsü açılır.



2. Güvenlik Duvarı modülü açılır.



3. Syslog sunucu eklemek istenilen kural için 'düzenle' butonuna tıklanır.



4. Log Yönlendir bölümünde eklenen Syslog sunucu seçilir.

Advanced

Severity: INFO

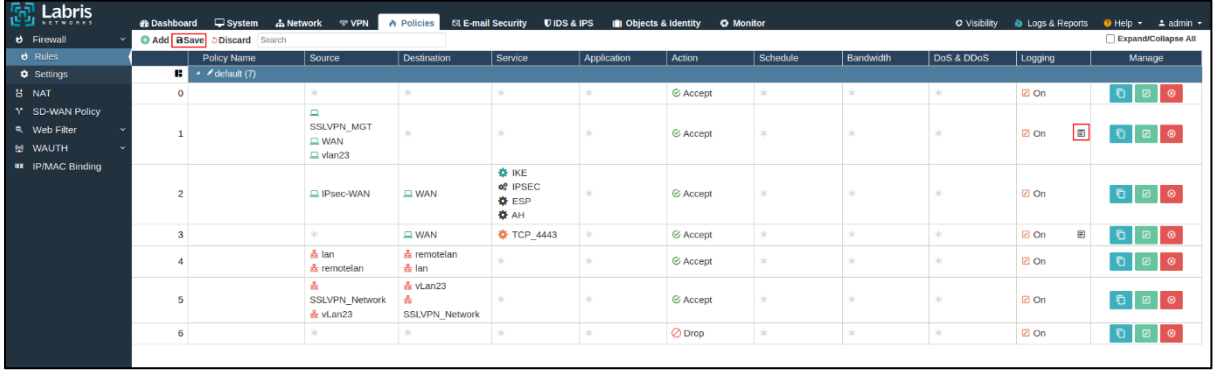
Reject With: ICMP port unreachable

Stateful Inspection:

Log Forwarding: (4)

IDS Policy: None

5. Syslog sunucusu eklendikten kurala syslog sunucusu eklenir. Daha sonra kural kaydedilir.

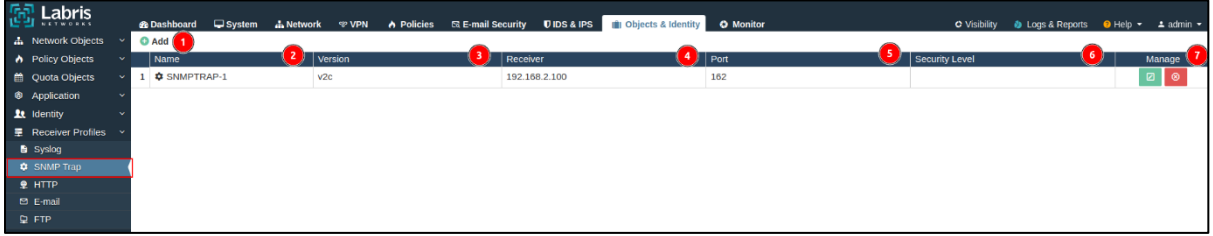


Policy Name	Source	Destination	Service	Application	Action	Schedule	Bandwidth	DoS & DDoS	Logging	Manage
default (7)	*	*	*	*	Accept	*	*	*	On	
1	SSLVPN_MGT WAN vlan23	*	*	*	Accept	*	*	*	On	
2	IPsec-WAN	WAN	IKE IPSEC ESP AH	*	Accept	*	*	*	On	
3	*	WAN	TCP_4443	*	Accept	*	*	*	On	
4	lan remotelan	remotelan lan	*	*	Accept	*	*	*	On	
5	SSLVPN_Network vlan23	vLan23 SSLVPN_Network	*	*	Accept	*	*	*	On	
6	*	*	*	*	Drop	*	*	*	On	

6. Yapılan işlemle birlikte kuraldan geçen istekler aynı zamanda Syslog sunucusuna gönderilir.

16.6.2 SNMP Tuzağı

Ağa bağlı olan cihazda belirli bir olay meydana geldiğinde otomatik olarak uyarılırlar. Labris UTM cihazı üzerinde de SNMP Tuzağı sunucuları eklenir.



Name	Version	Receiver	Port	Security Level	Manage
SNMPTRAP-1	v2c	192.168.2.100	162		

1	Ekle	SNMP Tuzağı ekleme işleminin yapıldığı butondur.
2	İsim	Eklenen SNMP Tuzağının isminin görüntülediği bölümdür.
3	Versiyon	Eklenen SNMP Tuzağı sunucusunun versiyonu görüntülenir.
4	Alıcı	SNMP Tuzağı sunucusunun IP adresi görüntülenir..
5	Port	SNMP Tuzağı sunucusunun port bilgisi görüntülenir.
6	Güvenlik Seviyesi	SNMP Tuzağı sunucusunun güvenlik seviyesi görüntülenir.

7	Yönet	Ekleneen SNMP Tuzağı sunucusunun düzenlendiği ve silindiği bölümdür.
---	--------------	--

-SNMP Tuzağı eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra SNMP Tuzağı eklemek için IP, port bilgileri girilir.

1	İsim	SNMP Tuzağı sunucusunun isminin girildiği bölümdür.
2	Alıcı IP/KAYNAK	SNMP Tuzağı sunucusunun IP adresinin girildiği bölümdür.
3	Port	SNMP Tuzağı sunucusunun çalıştığı port bilgisi görüntülenir.
4	Topluluk Adı	SNMP Tuzağı sunucusunun topluluk isminin girildiği bölümdür.
5	Versiyon	SNMP version bilgisinin seçildiği bölümdür.
6	Kaydet	SNMP Tuzağı sunucusunun bilgilerinin kaydedildiği bölümdür.
7	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında SNMP Tuzağı Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

16.6.3 HTTP

HTTP Alıcı profili genellikle bir web hizmetinin belirli bir URL'ine POST ve Get istekleri gönderilir. HTTP web sitesi üzerinde izleme, loglama ve uyarı gönderir.



1	Ekle	HTTP sunucu ekleme işleminin yapıldığı butondur.
2	İsim	HTTP sunucusunun isminin görüntülenir.
3	Adres	HTTP sunucusunun adresi görüntülenir.
4	Metod	HTTP sunucusunun metodunun görüntülediği bölümdür.
5	Agent	HTTP sunucunun Ajanının görüntülediği bölümdür.
6	Yönet	Eklenecek HTTP sunucusunun düzenlendiği veya silindiği bölümdür.

-HTTP Sunucusu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra HTTP sunucusu eklemek için IP, port bilgileri girilir.

HTTP Server

1 Name: HTTPServer

2 Address/URL: labrisnetworks.com

3 Method: POST

4 User Agent: Labris-Agent

5 Username: labris

6 Password:

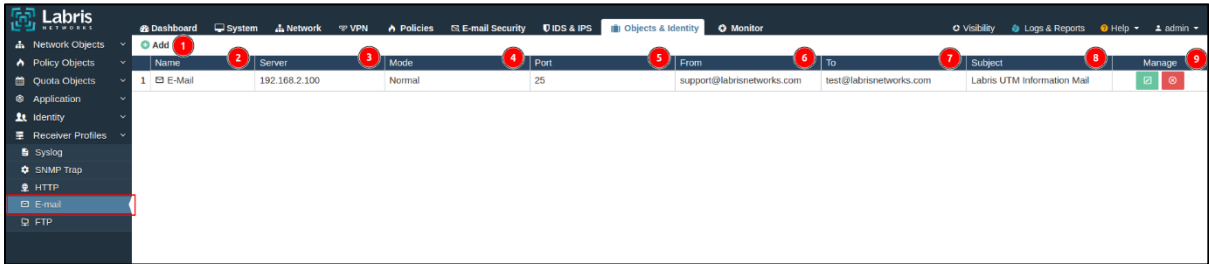
7 Save 8 Close

1	İsim	HTTP sunucusunun isminin girildiği bölümdür.
---	-------------	--

2	Adres/URL	HTTP sunucusunun URL'inin girildiği bölümdür.
3	Metod	HTTP sunucusunun metodunun seçildiği bölümdür.
4	Kullanıcı Uygulaması	HTTP sunucuna eklenecek kullanıcı uygulamasının seçildiği bölümdür.
5	Kullanıcı Adı	Kullanıcı Uygulaması üzerindeki kullanıcı adının girildiği bölümdür.
6	Şifre	Kullanıcı Uygulaması üzerindeki şifresinin girildiği bölümdür.
7	Kaydet	HTTP Sunucu bilgilerinin kaydedildiği butondur.
8	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında HTTP Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

16.6.4 E-Posta

Labris UTM cihazına e-posta sunucusunun eklendiği modüldür.



1	Ekle	E-Mail sunucusu ekleme işleminin yapıldığı bölümdür.
2	Server	Mail sunucusunun adresinin görüntülediği bölümdür.
3	İsim	E-mail sunucusunun isminin görüntülediği bölümdür.
4	Mod	Mail sunucusunun modunun görüntülediği bölümdür.

5	Port	Mail sunucusunun portunun bilgisi görüntülenir.
6	Gönderici	Gönderici posta adresinin görüntülediği bölümdür.
7	Alıcı	Alıcı posta adresinin görüntülediği bölümdür.
8	Konu	Mail göndereceği konunun görüntülediği bölümdür.
9	Yönet	Eklenen Mail sunucusunun düzenlendiği veya silindiği bölümdür.

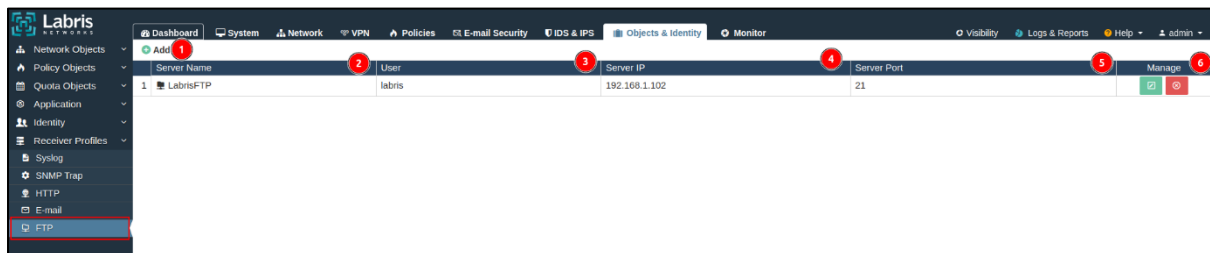
-HTTP Sunucusu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra E-Mail Sunucusu eklemek için server IP, mod, port, gönderici, alıcı bilgileri girilir.

1	İsim	Mail sunucusunun isminin girildiği bölümdür.
2	Sunucu IP/Sunucu Adı	Mail sunucusunun Sunucu IP adresinin girildiği bölümdür.

3	Mod	Mail sunucunun çalıştığı modun seçildiği bölümdür.
4	Port	Main sunucunun çalıştığı portun girildiği bölümdür.
5	Zaman Aşımı	Mail sunucusunun zaman aşımı değerinin girildiği bölümdür.
6	Gönderici	Gönderici mail adresinin girildiği bölümdür.
7	Alıcı	Mailin alıcı adresini girildiği bölümdür.
8	Konu	Mailin konusunun girildiği bölümdür.
9	Kullanıcı Adı	Mail sunucuda yetkili kullanıcının kullanıcı adının girildiği bölümdür.
10	Şifre	Mail sunucuda yetkili kullanıcının şifresinin girildiği bölümdür.
11	Kaydet	HTTP Sunucu bilgilerinin kaydedildiği butondur
12	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında E-Mail Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

16.6.5 FTP

Labris UTM cihazına FTP sunucusunun eklendiği modüldür. Eklenen FTP sunucusunu **Sistem** modülünde bulunan Yedekleme menüsünde kullanılır.



1	Ekle	FTP sunucusu ekleme işleminin yapıldığı bölümdür.
---	-------------	---

2	Sunucu İsmi	FTP sunucusunun isminin görüntülediği bölümdür.
3	Kullanıcı	FTP sunucusunda yetkili kullanıcının kullanıcı adının girildiği bölümdür.
4	Sunucu IP	FTP sunucusunun IP adresinin görüntülediği bölümdür.
5	Sunucu Portu	Eklenen FTP sunucusunun portunun görüntülediği bölümdür.
6	Yönet	Eklenen FTP sunucusunun düzenlendiği veya silindiği bölümdür.

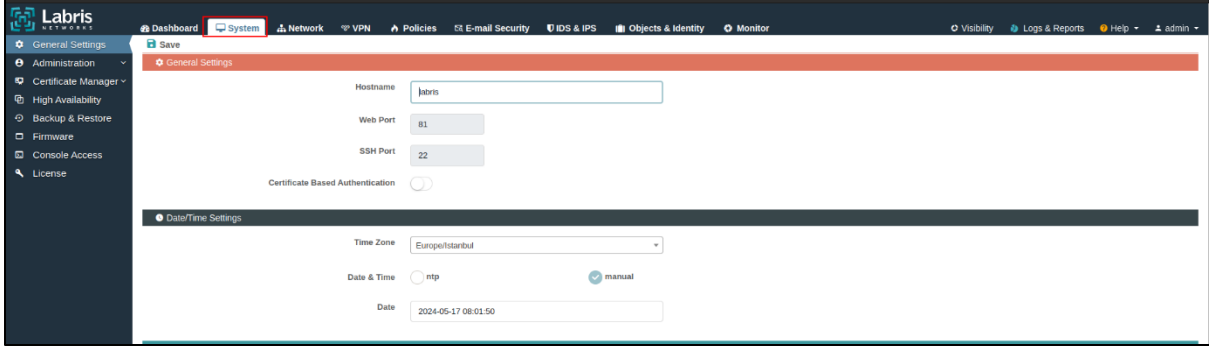
-FTP Sunucusu eklemek için 'ekle' butonuna tıklanır. 'ekle' butonuna tıkladıktan sonra FTP Sunucusu eklemek için server IP, port, FTP sunucusunda yetkili olan kullanıcı adı ve şifre bilgileri girilir.

1	Sunucu İsmi	FTP sunucusunun isminin girildiği bölümdür.
2	Kullanıcı Adı	FTP sunucusunda yetkili kullanıcının kullanıcı adının girildiği bölümdür.
3	Şifre	FTP sunucusunda yetkili kullanıcının şifresinin girildiği bölümdür.

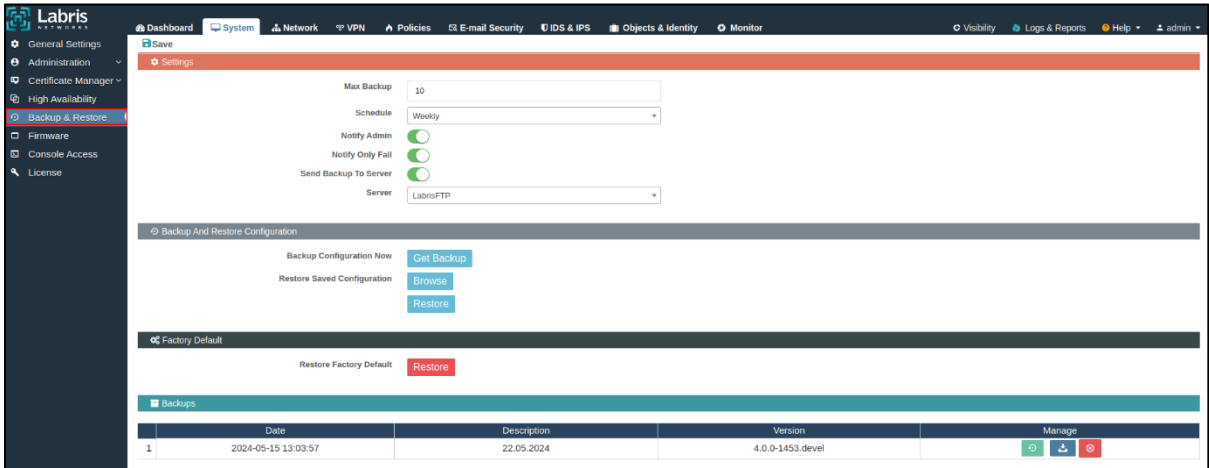
4	Sunucu IP	FTP sunucusunun IP adresinin girildiği bölümdür.
5	Sunucu Portu	FTP sunucusunun portunun girildiği bölümdür.
6	Uzak Dizin	FTP sunucusunun dizinin girildiği bölümdür.
7	Kaydet	HTTP Sunucu bilgilerinin kaydedildiği butondur.
8	Kapat	'ekle' butonuna tıklayarak açılan pencerenin kapatıldığı butondur. Kapat butonuna basıldığında E-Mail Sunucusu için yapılan değişiklikleri kaydetmeden kapatır.

-Eklenen FTP sunucusu kullanmak için;

1. Sistem modülüne girilir.



2. Ayar Yedekleme açılır.



3. Yedeği sunucuya gönder aktif edilir, FTP sunucu seçilir ve kaydet butonuna basılır.



17. İzleme

Labris UTM cihazı üzerindeki aktivitelerin görüntülediği modüldür. Bu modülde güvenlik duvarı istatistikleri, ataklar, arabirim istatistikleri, bağlantı/hedef istatistikleri, aktif kullanıcılar, kota kullanımı, IPSec Bağlantı durumu, SSLVPN'e bağlı olan kullanıcılar, L2TP Kullanıcıları, PPTP Kullanıcıları, yönlendirme tablosu, Arp Tablosu ve cihazda çalışan servisler görüntülenir.

Rule Number	Rule ID	Total Hit	Current Sessions	Total Bytes	Total Packets	First Hit	Last Hit	Rule Created	Rule Updated
1	0	9734	-1	205.8 MB	128883	16-05-2024, 22:10	13-06-2024, 06:01	16-05-2024, 22:07	17-05-2024, 18:18
2	1	4033		38624	8	12-02-2024, 06:51	16-05-2024, 08:00	09-02-2024, 13:47	17-05-2024, 18:18
3	2	4	-2		8	03-05-2024, 15:20	03-05-2024, 15:44	03-05-2024, 15:17	17-05-2024, 18:18
4	3	33148	-27	121.2 MB	174593	25-02-2024, 03:12	16-05-2024, 04:23	25-02-2024, 03:12	17-05-2024, 18:18
5	4							16-05-2024, 04:49	17-05-2024, 18:18
6	5							24-02-2024, 13:22	17-05-2024, 18:18
7	6	3217				23-02-2024, 17:59	16-05-2024, 22:06	23-02-2024, 17:59	17-05-2024, 18:18

17.1 Kural Kullanımı

Politikalar modülünde bulunan güvenlik duvarında yazılan kuralların kullanımına dair istatistikler görüntülenir. Kuralın numarasını, kural kimliğini, kuralın eşleşme zamanını, kuralın eklenme ve değiştirme zamanları görüntülenir.

Rule Number	Rule ID	Total Hit	Current Sessions	Total Bytes	Total Packets	First Hit	Last Hit	Rule Created	Rule Updated
1	0	9734	1000	205.8 MB	128883	16-05-2024, 22:10	13-06-2024, 06:01	16-05-2024, 22:07	17-05-2024, 18:18
2	1	4033		38624	8	12-02-2024, 06:51	16-05-2024, 08:00	09-02-2024, 13:47	17-05-2024, 18:18
3	2	4	20000		8	03-05-2024, 15:20	03-05-2024, 15:44	03-05-2024, 15:17	17-05-2024, 18:18
4	3	33148	27	121.2 MB	174593	25-02-2024, 03:12	16-05-2024, 04:23	25-02-2024, 03:12	17-05-2024, 18:18
5	4							16-05-2024, 04:49	17-05-2024, 18:18
6	5							24-02-2024, 13:22	17-05-2024, 18:18
7	6	3217				23-02-2024, 17:59	16-05-2024, 22:06	23-02-2024, 17:59	17-05-2024, 18:18

1	Kural Numarası	Kural numarasının görüntülediği bölümdür.
2	Kural Kimliği	Kural kimliğinin görüntülediği bölümdür.
3	Toplam Eşleme	Güvenlik duvarı kuralındaki toplam eşleme zamanı görüntülenir.
4	Aktif Oturum	Kuralın aktif kullanım sayısı görüntülenir.
5	Toplam Bayt	Kuraldan geçen trafiğin toplam bayt boyutu görüntülenir.

6	Toplam Paket	Kuraldan geçen trafiğin toplam paket boyutu görüntülenir.
7	İlk Eşleme	Kuraldan ilk geçen trafiğin zaman bilgisi görüntülenir.
8	Son Eşleme	Kuraldan son geçen trafiğin zaman bilgisi görüntülenir.
9	Eklenme Zamanı	Kuralın eklenme zamanı görüntülenir.
10	Değiştirilme Zamanı	Eklenme zamanından sonra kuralda yapılan değişikliklerin zamanı görüntülenir.

17.2 Saldırılar

Labris UTM cihazına gelen saldırıların detayları görüntülenir. Saldırı detaylarını görebilmek için IDS&IPS'in açılması gerekir.

The screenshot shows the Labris UTM management interface. The 'Monitor' tab is active, displaying the following information:

- Today's alerts:** 1
- Unique Alerts:** 0
- Categories:** 0
- Total Number of Alerts:** 0
- Sensors/Total:** 0 / 1
- Alerts:**
 - Src IP address: 0
 - Dest. IP address: 0
 - Unique IP links: 0
 - Source Ports: 0
 - TCP (0), UDP (0)
 - Dest Ports: 0
 - TCP (0), UDP (0)

The 'Traffic Profile by Protocol' section shows the following data:

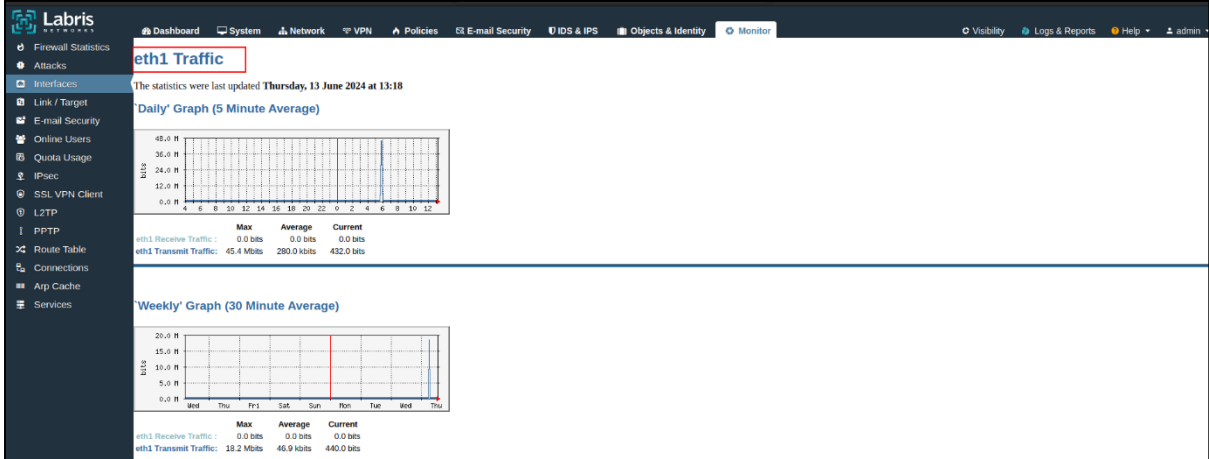
Protocol	Percentage
TCP	0%
UDP	0%
ICMP	0%
Portscan	0%

17.3 Arayüzler

Labris UTM cihazı üzerindeki arabirimlere ait gelen ve giden paketlerinin grafik halinde görüntülenir.



-Arabirimlere gelen ve giden trafiğin detaylarına bakmak için detay olarak görüntülenmek istenilen arabirime tıklanır. Seçilen arabirime ait verileri 5dk, 30dk, 2 saat ve 1 günlük veriler bulunur.



17.4 Hat/Hedef

Labris UTM cihazının ağ erişimini ve varsayılan ağ geçidine erişimin grafik olarak görüntülediği bölümdür.



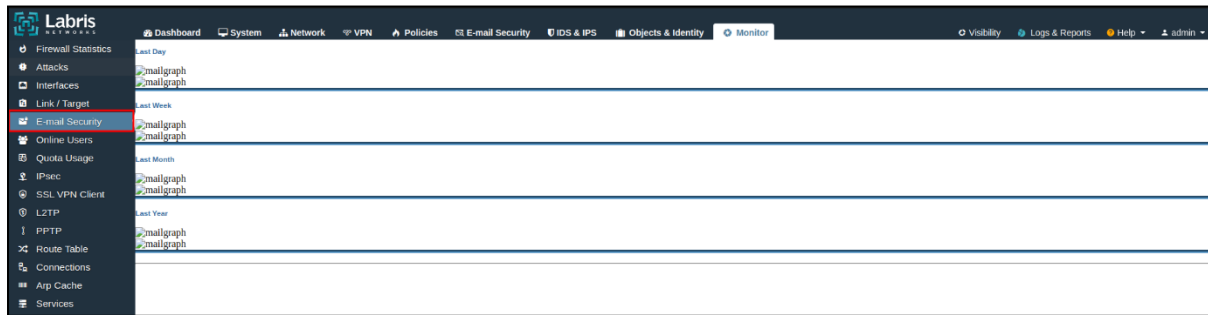
1	UTM Ağ Kullanılabilirliği	Labris UTM cihazının ağ kullanılabilirliğinin görüntülenir.
2	Ağ Geçidi Erişebilirliği	Labris UTM cihazının ağ geçidine erişilebilirliği görüntülenir.

-Ağ kullanılabilirliği veya ağ geçidi erişilebilirliğini detaylı olarak görüntülenmesi için görüntülenmek istenilen UTM Ağ Kullanılabilirliği veya Ağ Geçidi erişilebilirliğine tıklar. 3 saat, 30 saat ve 10 günlük grafik halinde görüntülenir.



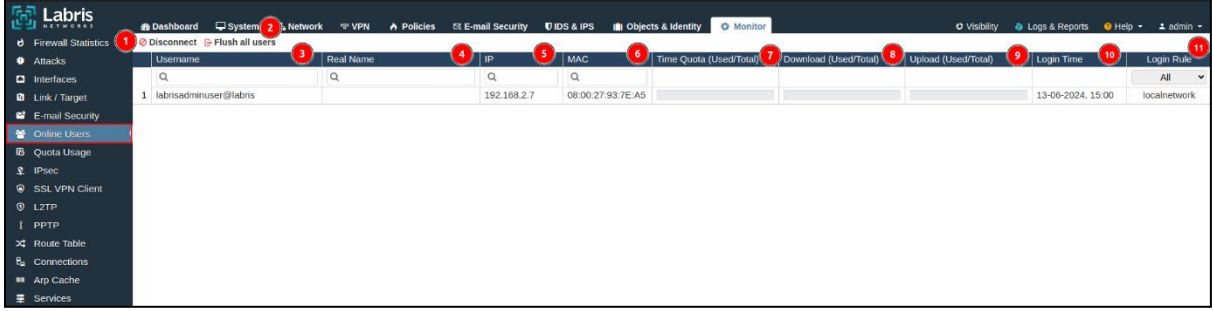
17.5 E-Posta Güvenliği

Labris UTM cihazındaki E-posta güvenliğinde dair kayıtlar görüntülenir.



17.6 Bağlı Kullanıcılar

Wauth'a bağlı olan kullanıcıların görüntülediği bölümdür.



1	Bağlantıyı Kes	Wauth'a bağlı olan kullanıcıların bağlantısının kesildiği butondur.
2	Bütün Kullanıcıları Temizle	Wauth'a bağlı olan kullanıcıların tamamının temizlendiği butondur.
3	Kullanıcı Adı	Wauth'a bağlı olan kullanıcıların kullanıcı adının görüntülediği bölümdür.
4	Gerçek İsim	Wauth'a bağlı olan kullanıcıların gerçek isminin görüntülediği bölümdür.
5	IP	Wauth'a bağlı olan kullanıcıların IP adreslerinin görüntülediği bölümdür.
6	MAC	Wauth'a bağlı olan kullanıcıların MAC adreslerinin görüntülediği bölümdür.
7	Zaman Kotası(Kullanılan/Toplam)	Wauth kullanıcılarının zaman kotası görüntülenir.
8	İndirme(Kullanılan/Toplam)	Wauth kullanıcılarının indirme kotası görüntülenir.
9	Yükleme(Kullanılan/Toplam)	Wauth kullanıcılarının yükleme kotası görüntülenir.

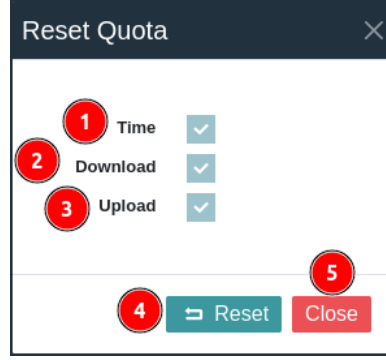
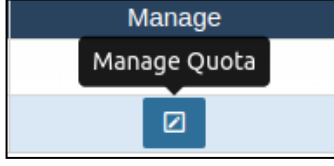
10	Oturum Zamanı Açma	Wauth kullanıcısının oturum açma zamanı görüntülenir.
11	Oturum Kuralı Açma	WAuth'a bağlı olan kullanıcının wauth kuralı görüntülenir.

17.7 Kota Kullanımı

Wauth'a bağlı olan kullanıcıların kota kullanımı görüntülenir.

1	Kullanıcı Adı	Kota politikası uygulanan kullanıcının kullanıcı adı görüntülenir.
2	Kural Adı	Kota politikasının adı görüntülendiği bölümdür.
3	Süre	Kota süresi görüntülendiği bölümdür.
4	Zaman Kotası(Kullanılan/Toplam)	Kota politikası uygulanan kullanıcının zaman kotası görüntülenir.
5	İndirme(Kullanılan/Toplam)	Kota politikası uygulanan kullanıcının zaman kotası görüntülenir.
6	Yükleme(Kullanılan/Toplam)	Kota politikası uygulanan kullanıcının yükleme kotası görüntülenir.
7	Yönet	Kullanıcıların kota politikasının yönetildiği bölümdür. Kota politikası yönet bölümünde sıfırlanır.

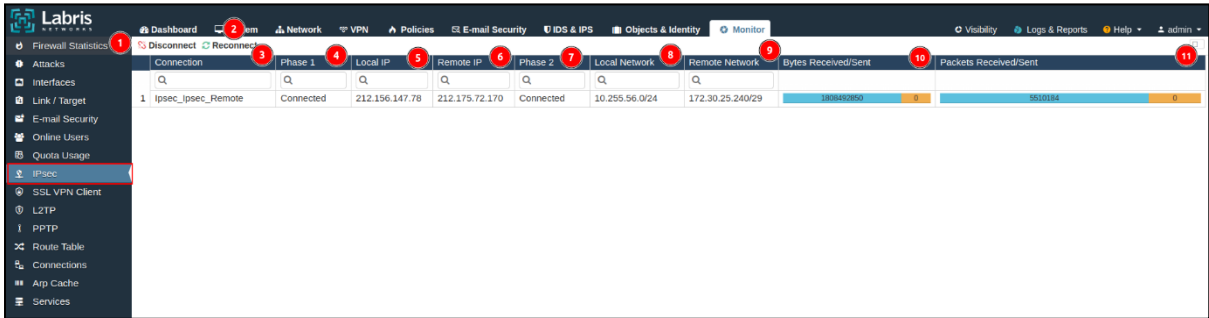
-Kota politikası uygulanan kullanıcının kotalarının sıfırlanmak için düzenle butonuna basılır. Düzenle butonuna basıldıktan sonra kullanıcının kotaları sıfırlanır.



1	Zaman	Kota politikası uygulanan kullanıcının zaman kotası sıfırlanır.
2	İndirme	Kota politikası uygulanan kullanıcının indirme kotası sıfırlanır.
3	Yükleme	Kota politikası uygulanan kullanıcının yükleme kotası sıfırlanır.
4	Sıfırla	Kotaların sıfırlama işleminin yapıldığı butondur.
5	Kapat	Yönet butonuna tıklanarak açılan pencerenin kapatıldığı butondur.

17.8 IPsec

Labris UTM cihazındaki IPsec bağlantılarının bilgilerinin görüntülediği bölümdür.



1	Bağlantıyı Kes	IPsec bağlantısının bağlantısının kesildiği butondur.
---	-----------------------	---

2	Yeniden Bağlan	IPSec bağlantısının yeniden bağlantısının yapıldığı butondur.
3	Bağlantı	IPSec bağlantısının adının görüntülediği bölümdür.
4	Aşama1	Aşama-1 bağlantısının görüntülediği bölümdür. Aşama-1 bağlantısı sağlanmışsa 'connected' şeklinde görüntülenir.
5	Yerel IP	IPSec yapılan Labris UTM cihazının genel IP adresinin görüntülediği bölümdür.
6	Uzak IP	IPSec yapılan diğer cihazın genel IP adresinin görüntülediği bölümdür.
7	Aşama2	Aşama-2 bağlantısının görüntülediği bölümdür. Aşama-2 bağlantısı sağlanmışsa 'connected' şeklinde görüntülenir.
8	Yerel Ağ	IPSec yapılan Labris UTM cihazının yerel IP adresinin görüntülediği bölümdür.
9	Uzak Ağ	IPsec yapılan diğer cihazın yerel IP adresinin görüntülediği bölümdür.
10	Alınan/Gönderilen Veri	IPSec bağlantısındaki alınan ve gönderilen veri miktarı görüntülenir.
11	Alınan/Gönderilen Paketler	IPSec bağlantısındaki alınan ve gönderilen paket miktarı görüntülenir.

17.9 SSL VPN Client

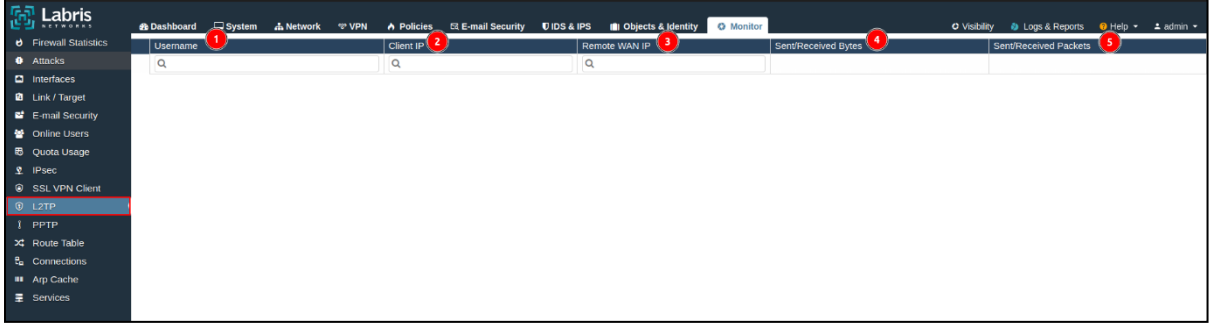
SSLVPN'e bağlı olan kullanıcıların görüntülediği modüldür. SSL VPN ile bağlı olan kullanıcıların bağlantıları bu modülde kesilebilir.

1	2	3	4	5	6	7
Username	Client IP	Remote WAN IP	Connected Since	Duration	Sent/Received	
1	10.8.3.2		14/06/2024 05:29:21	0d-0:37:34	2.7MB / 914.4KB	
2	10.8.3.26		13/06/2024 08:00:42	0d-22:6:13	88.5KB / 392.3KB	
3	10.8.3.4		14/06/2024 04:58:39	0d-1:8:16	21.5MB / 24.0KB	
4	10.8.3.19		14/06/2024 05:05:36	0d-1:1:19	2.3MB / 1.3MB	
5	-		14/06/2024 05:06:11	0d-0:0:44	22KB / 112B	
6	10.8.3.13		14/06/2024 05:35:01	0d-0:31:54	631.3KB / 232.9KB	
7	10.8.3.11		13/06/2024 15:10:33	0d-14:56:22	270.8KB / 242.5KB	
8	10.8.3.14		14/06/2024 04:51:02	0d-1:15:53	1.0MB / 679.6KB	
9	10.8.3.23		14/06/2024 05:06:11	0d-1:0:44	361.7KB / 278.0KB	
10	10.8.3.18		14/06/2024 04:51:29	0d-1:15:26	1.3MB / 493.0KB	
11	10.8.3.24		14/06/2024 05:06:23	0d-1:0:32	98.1KB / 318.9KB	

1	Bağlantıyı Kes	SSL VPN'e bağlı olan kullanıcının bağlantısının kesildiği butondur.
2	Kullanıcı Adı	SSL VPN'e bağlı olan kullanıcıların kullanıcı adlarının görüntülediği bölümdür.
3	İstemci IP'si	SSLVPN'e bağlı olan kullanıcıların aldığı IP adresleri görüntülenir.
4	Uzak WAN IP'si	SSL VPN'e bağlı olan kullanıcıların genel IP adreslerinin görüntülediği bölümdür.
5	Bağlandığı Zaman	Kullanıcıların SSL VPN'e bağlandığı zamanın görüntülediği bölümdür.
6	Süre(gün-saat-dakika-saniye)	SSL VPN'e bağlı kalınan süre bilgisi gün, saat, dakika ve saniye cinsinden görüntülenir.
7	Gönderilen/Alınan	Kullanıcıların SSL VPN'e bağlandıktan sonra gönderilen ve alınan veri miktarı görüntülenir.

17.10 L2TP

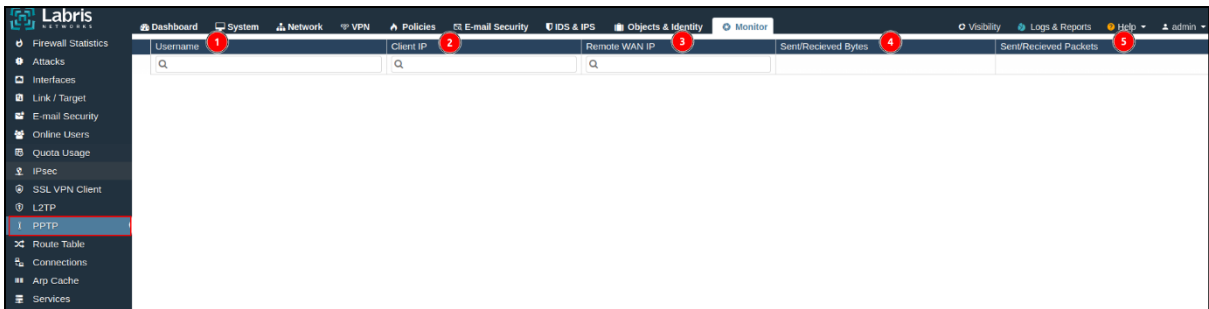
L2TP VPN'e bağlı olan kullanıcıların görüntülediği modüldür.



1	Kullanıcı Adı	L2TP VPN'e bağlı olan kullanıcıların kullanıcı adlarının görüntülediği bölümdür.
2	İstemci IP'si	L2TP VPN'e bağlandıktan sonra aldıkları IP adresleri görüntülenir.
3	Uzak WAN IP'si	L2TP VPN'e bağlanan kullanıcıların genel IP adresleri görüntülenir.
4	Gönderilen ve Alınan Veri	Kullanıcıların L2TP VPN'e bağlandıktan sonra gönderilen ve alınan veri miktarının görüntülediği bölümdür.
5	Gönderilen ve Alınan Paket	Kullanıcıların L2TP VPN'e bağlandıktan sonra gönderilen ve alınan paket miktarının görüntülediği bölümdür.

17.11 PPTP

PPTP VPN'e bağlı olan kullanıcıların görüntülediği modüldür.



1	Kullanıcı Adı	PPTP VPN'e bağlı olan kullanıcıların kullanıcı adlarının görüntülediği bölümdür.
---	----------------------	--

2	İstemci IP'si	PPTP VPN'e bağlandıktan sonra aldıkları IP adresleri görüntülenir.
3	Uzak WAN IP'si	PPTP VPN'e bağlanan kullanıcıların genel IP adresleri görüntülenir.
4	Gönderilen ve Alınan Veri	Kullanıcıların PPTP VPN'e bağlandıktan sonra gönderilen ve alınan veri miktarının görüntülediği bölümdür.
5	Gönderilen ve Alınan Paket	Kullanıcıların PPTP VPN'e bağlandıktan sonra gönderilen ve alınan paket miktarının görüntülediği bölümdür.

17.12 Yönlendirme Tablosu

Labris UTM cihazındaki yönlendirme tablosunun görüntülediği bölümdür.

Table	Proto	Dev	Target	Gateway	Source	Scope	Metric
1 main		eth2	default		10.0.4.2		
2 main	kernel	eth1	10.0.0.0/24		10.0.0.1	link	
3 main	kernel	eth2	10.0.4.0/24		10.0.4.15	link	
4 main	kernel	eth0	169.254.0.0/16		169.254.1.2	link	
5 main	kernel	eth3	192.168.0.0/24		192.168.0.2	link	
6 main	kernel	eth1	192.168.1.0/24		192.168.1.254	link	
7 main	kernel	eth1	192.168.2.0/24		192.168.2.1	link	
8 main	kernel	eth1.23	192.168.23.0/24		192.168.23.1	link	

1	Tablo	Yazılan yönlendirmenin tablo isminin görüntülediği bölümdür
2	Protokol	Yönlendirmenin protokol bilgisinin görüntülediği bölümdür.
3	Arabirim	Yönlendirmenin yazıldığı arabirimin görüntülediği bölümdür.
4	Hedef	Yönlendirmenin yazıldığı hedef IP adresinin görüntülediği bölümdür.
5	Ağ Geçidi	Yönlendirmenin yazıldığı ağ geçidinin görüntülediği bölümdür.

6	Kaynak	Yönlendirmenin yazıldığı kaynak IP adresinin görüntülediği bölümdür.
7	Kapsam	Yazılan yönlendirmenin kapsam bilgisi görüntülenir.
8	Ölçü	Yazılan yönlendirmenin ölçü değeri görüntülenir.

17.13 Bağlantılar

Labris UTM cihazındaki bağlantı bilgileri görüntülenir.

	1	2	3	4	5	6	7	8	9	10	11	12
	Protocol	State	Source	Destination	Source Port	Destination Port	Transmitted Packets	Received Packets	Transmitted Bytes	Received Bytes	Lifetime (s)	
1	tcp	TIME_WAIT	192.0.2.254	172.217.17.99	35755	80	8	5	824	714	3	
2	tcp	TIME_WAIT	192.168.0.61	91.228.166.14	49165	80	6	5	1342	1118	0	
3	tcp	TIME_WAIT	192.168.0.218	195.175.178.106	62600	80	11	10	918	1365	9	
4	tcp	TIME_WAIT	192.0.2.254	2.17.225.65	39410	80	6	4	547	479	2	
5	tcp	TIME_WAIT	192.0.2.254	172.217.20.67	43639	80	6	4	527	439	3	
6	tcp	TIME_WAIT	192.168.0.145	23.55.53.65	52943	80	7	6	519	1241	4	
7	tcp	TIME_WAIT	192.168.0.218	195.175.178.106	62601	80	11	10	918	1365	9	
8	tcp	TIME_WAIT	192.168.0.239	52.34.224.60	54892	443	24	18	19671	8061	1	
9	tcp	TIME_WAIT	192.168.0.218	34.107.221.82	62596	80	11	10	781	877	9	
10	tcp	TIME_WAIT	192.168.0.218	192.229.221.95	62610	80	13	13	1461	2186	9	
11	tcp	TIME_WAIT	192.168.0.158	162.247.243.29	51490	443	44	48	28494	8993	1	
12	tcp	TIME_WAIT	192.168.0.203	91.228.167.43	64508	80	5	5	419	903	9	
13	tcp	TIME_WAIT	192.168.0.218	34.107.221.82	62602	80	11	10	798	716	9	
14	tcp	TIME_WAIT	192.168.0.145	2.17.225.65	52944	80	7	6	519	1241	4	
15	tcp	TIME_WAIT	192.168.0.145	172.217.17.99	52942	80	8	6	732	878	4	
16	tcp	TIME_WAIT	192.0.2.254	199.232.214.172	43410	80	123	142	11614	173199	9	
17	tcp	TIME_WAIT	192.168.0.164	51.132.193.105	58769	443	15	13	3595	5468	0	
18	tcp	TIME_WAIT	192.168.0.145	172.217.20.67	52945	80	6	5	459	638	4	
19	tcp	TIME_WAIT	192.168.0.218	35.244.181.201	62604	443	24	31	2765	7790	9	
20	tcp	SYN_SENT	192.168.0.6	142.251.9.26	44950	25	1	0	60	0	6	
21	tcp	SYN_SENT	192.168.0.6	74.125.206.26	33052	25	1	0	60	0	6	
22	tcp	SYN_SENT	192.168.0.196	85.25.103.30	49776	443	2	0	104	0	24	
23	tcp	SYN_SENT	192.168.0.196	195.181.174.167	49774	443	3	0	152	0	26	
24	tcp	SYN_SENT	192.0.2.254	104.208.16.93	41870	80	4	0	240	0	24	
25	tcp	SYN_SENT	192.168.0.6	142.250.153.26	48896	25	1	0	60	0	6	
26	tcp	SYN_SENT	192.0.2.254	104.208.16.93	41841	80	6	0	360	0	16	
27	tcp	SYN_SENT	192.168.0.196	78.46.49.23	49771	443	3	0	152	0	14	

1	Bağlantıyı Kes	Seçilen bağlantının bağlantısının kesildiği butondur.
2	Protokol	Bağlantıdaki protokol bilgisinin görüntülediği bölümdür.
3	Durum	Bağlantı durumunun görüntülediği bölümdür.
4	Kaynak	Bağlantıdaki kaynak IP adresinin görüntülediği bölümdür.
5	Hedef	Bağlantıdaki hedef IP adresinin görüntülediği bölümdür.
6	Kaynak Portu	Bağlantıdaki kaynak portunun görüntülediği bölümdür.

7	Hedef Portu	Bağlantıdaki hedef portun görüntülediği bölümdür.
8	Gönderilen Paket	Bağlantı üzerindeki gönderilen paket miktarının görüntülediği bölümdür.
9	Alınan Paket	Bağlantı üzerindeki alınan paket miktarı görüntülediği bölümdür.
10	Gönderilen Veri	Bağlantı üzerindeki gönderilen veri miktarının görüntülediği bölümdür.
11	Alınan Veri	Bağlantı üzerindeki alınan veri miktarı görüntülediği bölümdür.
12	Bekleme Süresi	Bağlantının bekleme süresinin görüntülediği bölümdür.

17.14 Arp Cache

Labris UTM cihazındaki arp tablosunun görüntülediği bölümdür.

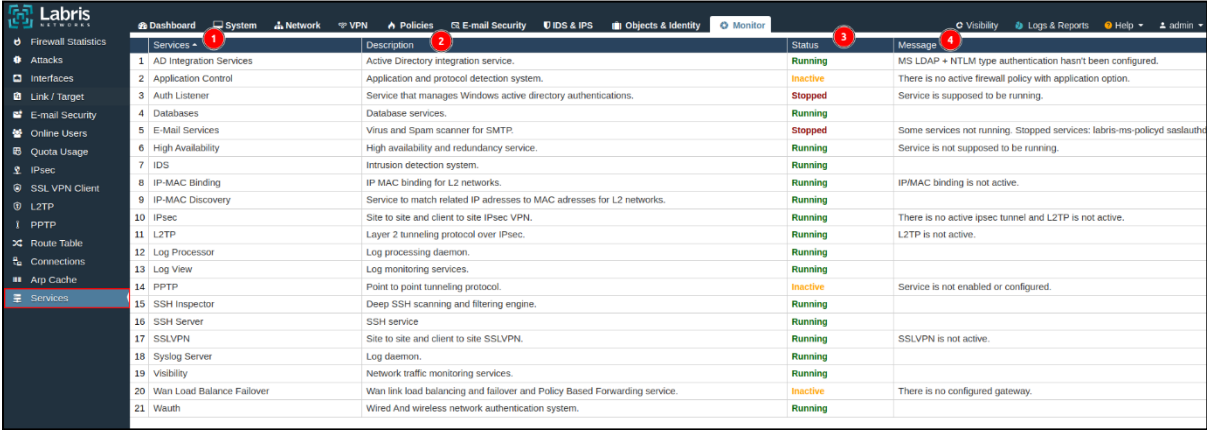
Dev	IP	MAC	Reference	Used	Probes	State
All	Q	Q	Q	Q	Q	Q
1 eth1	192.168.1.100					FAILED
2 eth0	169.254.1.10	0a:00:27:00:00:00	1	5669/0/4247	1	REACHABLE
3 eth2	10.0.4.2	52:54:00:12:35:02	1	21/16/16	1	REACHABLE
4 eth1	192.168.2.6					INCOMPLETE
5 eth1	192.168.2.7	08:00:27:93:7e:a5	1	4380/0/1103	1	REACHABLE

1	Arabirim	Arp girdisinin alındığı arabirim görüntülediği bölümdür.
2	IP	Arp tablosundaki IP adresinin görüntülediği bölümdür.
3	MAC	Arp tablosundaki MAC adresinin görüntülediği bölümdür.
4	Referans	Arp tablosundaki referans değerinin görüntülediği bölümdür.

5	Kullanılan	Arp girdisinin kaç kez kullanıldığının görüntülediği bölümdür.
6	Sondalar	Arp girdisi için kaç kez ARP sorgusu gönderildiğini gösterir.
7	Durum	Arp girdisinin durum bilgisinin görüntülediği bölümdür.

17.15 Servisler

Labris UTM cihazındaki çalışan servislerin durumlarının görüntülediği bölümdür.



Services	Description	Status	Message
1 AD Integration Services	Active Directory integration service.	Running	MS LDAP + NTLM type authentication hasn't been configured.
2 Application Control	Application and protocol detection system.	Inactive	There is no active firewall policy with application option.
3 Auth Listener	Service that manages Windows active directory authentications.	Stopped	Service is supposed to be running.
4 Databases	Database services.	Running	
5 E-Mail Services	Virus and Spam scanner for SMTP.	Stopped	Some services not running. Stopped services: labris-ms-policyd saslaauth
6 High Availability	High availability and redundancy service.	Running	Service is not supposed to be running.
7 IDS	Intrusion detection system.	Running	
8 IP-MAC Binding	IP MAC binding for L2 networks.	Running	IPMAC binding is not active.
9 IP-MAC Discovery	Service to match related IP addresses to MAC addresses for L2 networks.	Running	
10 IPsec	Site to site and client to site IPsec VPN.	Running	There is no active ipsec tunnel and L2TP is not active.
11 L2TP	Layer 2 tunneling protocol over IPsec.	Running	L2TP is not active.
12 Log Processor	Log processing daemon.	Running	
13 Log View	Log monitoring services.	Running	
14 PPTP	Point to point tunneling protocol.	Inactive	Service is not enabled or configured.
15 SSH Inspector	Deep SSH scanning and filtering engine.	Running	
16 SSH Server	SSH service	Running	
17 SSLVPN	Site to site and client to site SSLVPN.	Running	SSLVPN is not active.
18 Syslog Server	Log daemon.	Running	
19 Visibility	Network traffic monitoring services.	Running	
20 Wan Load Balance Failover	Wan link load balancing and failover and Policy Based Forwarding service.	Inactive	There is no configured gateway.
21 Wauth	Wired And wireless network authentication system.	Running	

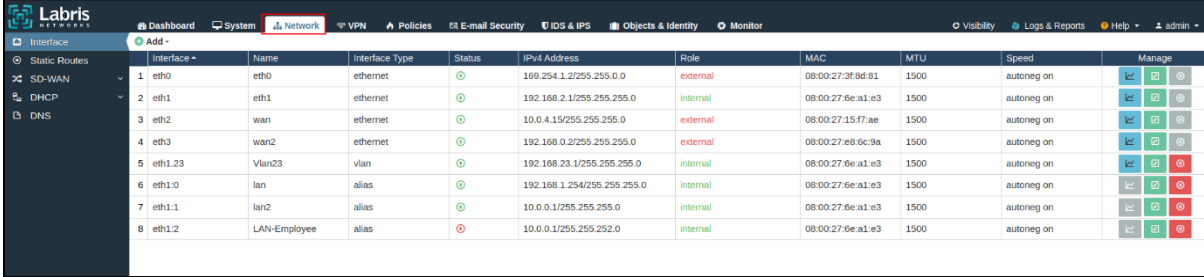
1	Servisler	Labris UTM cihazındaki çalışan servislerin isimlerinin görüntülediği bölümdür.
2	Açıklama	Labris UTM cihazındaki çalışan servisler ile ilgili açıklamaların görüntülediği bölümdür.
3	Durum	Labris UTM cihazındaki çalışan servislerin çalışma durumlarının görüntülediği bölümdür. Servis çalışıyor ise durum olarak 'çalışıyor' olarak görüntülenir.
4	Mesaj	Labris UTM cihazındaki çalışan servisleri isimlerinin görüntülediği bölümdür.

18. Trafik Analizi

Labris UTM cihazındaki trafik analizinin yapıldığı, arabirimlerden geçen trafiğin detaylarının görüntülediği modüldür. Trafik analizi yapılmak istenilen arabirim seçilerek seçilen arabirime ait trafik analizi yapılabilir. Trafik analizi yapılmak istenilen arabirimde Ağ modülünde arabirime ait trafik analizinin açılması gerekir.

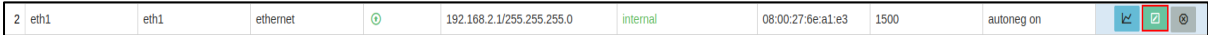
-Arabirimde trafik analizini açma adımları;

1. Ağ modülüne tıklanır.



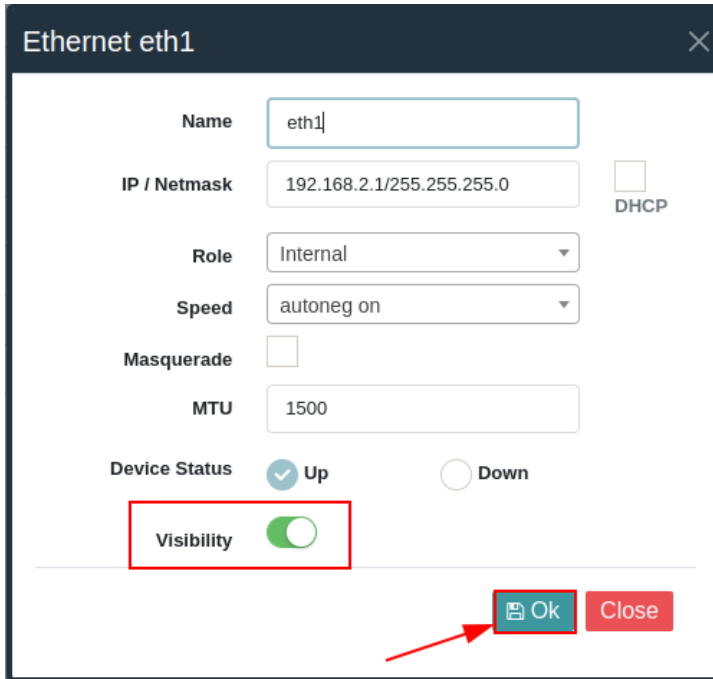
Interface	Name	Interface Type	Status	IPv4 Address	Role	MAC	MTU	Speed	Manage
1	eth0	ethernet	🟢	169.254.1.2/255.255.0.0	external	08:00:27:3f:8d:81	1500	autoneg on	🔧 📄 🗑️
2	eth1	ethernet	🟢	192.168.2.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️
3	eth2	wan	🟢	10.0.4.15/255.255.255.0	external	08:00:27:15:f7:ae	1500	autoneg on	🔧 📄 🗑️
4	eth3	wan2	🟢	192.168.0.2/255.255.255.0	external	08:00:27:e8:6c:9a	1500	autoneg on	🔧 📄 🗑️
5	eth1.23	vlan23	🟢	192.168.23.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️
6	eth1.0	lan	🟢	192.168.1.254/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️
7	eth1.1	lan2	🟢	10.0.0.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️
8	eth1.2	LAN-Employee	🔴	10.0.0.1/255.255.252.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️

2. Trafik analizinin açılacağı arabirime ait 'düzenle' butonunda tıklanır.



2	eth1	eth1	ethernet	🟢	192.168.2.1/255.255.255.0	internal	08:00:27:6e:a1:e3	1500	autoneg on	🔧 📄 🗑️
---	------	------	----------	---	---------------------------	----------	-------------------	------	------------	--------

3. Seçilen arabirimde düzenle butonuna tıkladıktan sonra gelen penceredeki trafik analizi işaretlenerek arabirim kaydedilir.



Ethernet eth1

Name: eth1

IP / Netmask: 192.168.2.1/255.255.255.0 DHCP

Role: Internal

Speed: autoneg on

Masquerade:

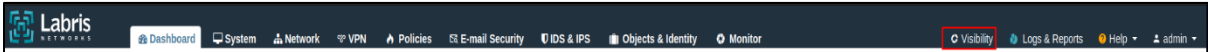
MTU: 1500

Device Status: Up Down

Visibility:

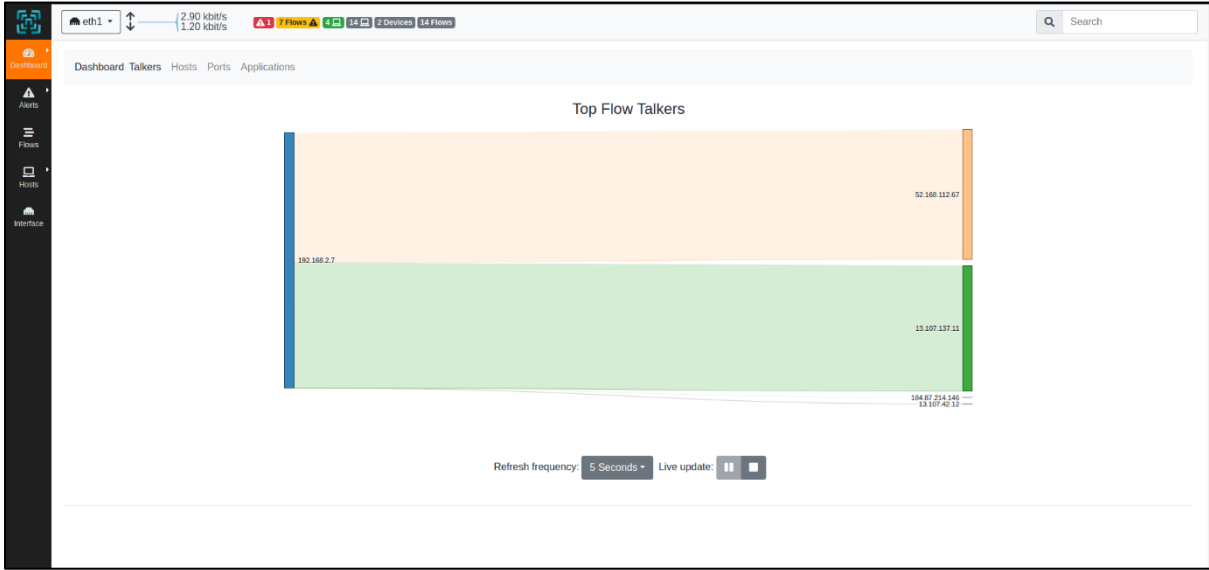
Ok Close

4. Trafik analiz açıldıktan sonra Trafik Analizi modülü açılır.



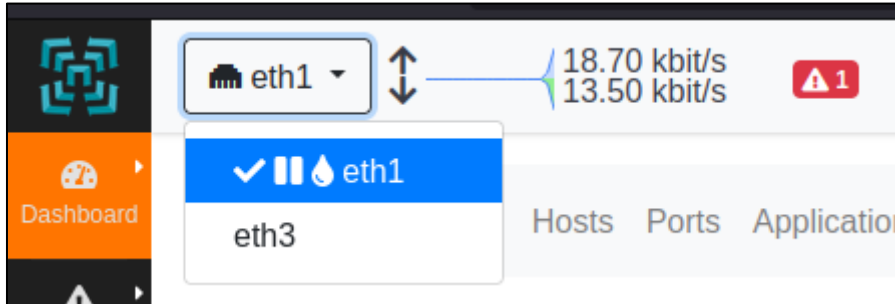
Dashboard	System	Network	VPN	Policies	E-mail Security	IDS & IPS	Objects & Identity	Monitor	Visibility	Logs & Reports	Help	admin
									🔍			

5. Trafik analizine tıklandıktan sonra yeni pencere açılır ve trafik detayları incelenir.



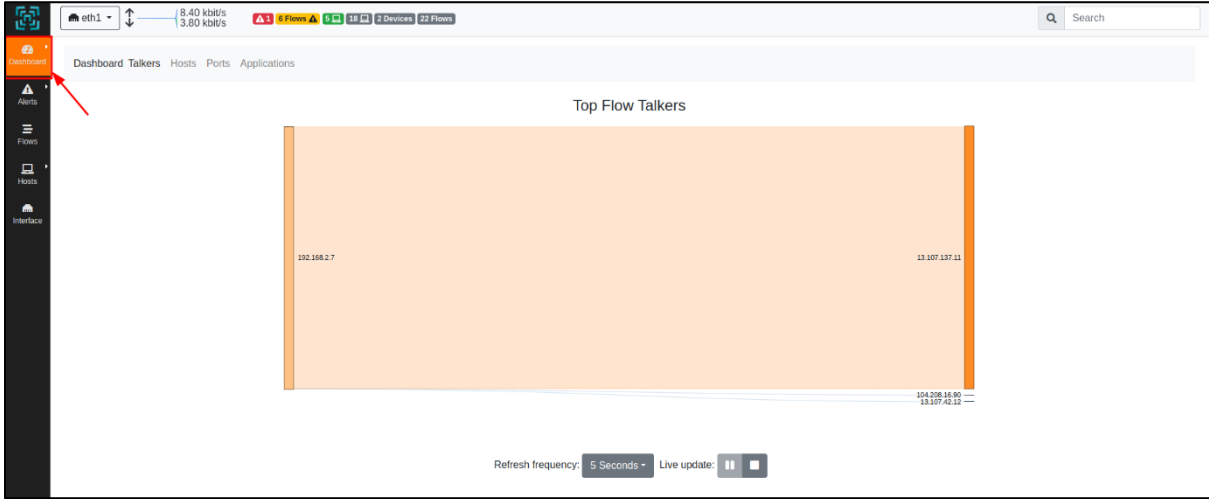
18.1 Arabirim Seçimi

Trafik analizi yapılacak olan arabirim seçilir. Seçilen arabirimin hız bilgileriyle birlikte görüntülenir.



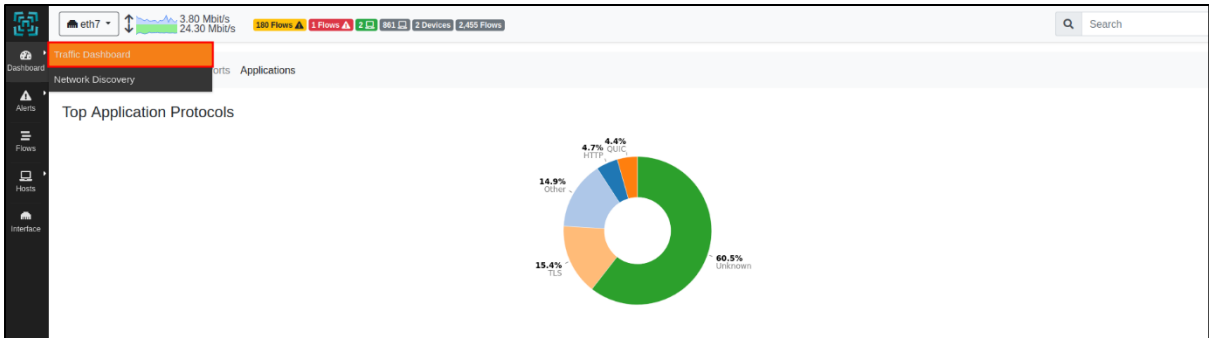
18.2 Kontrol Paneli

Seçilen arabirime ait olan trafiğin detaylı olarak incelendiği modüldür. Kontrol panelinde en çok trafik oluşturan kaynak ve hedef IP adresleri, en çok trafik oluşturan istemcilerin IP adresi, port bilgileri ve uygulama bilgilerinin detaylarının görüntülediği bölümdür.



18.2.1 Trafik Kontrol Panel

En çok haberleşen IP adresleri, trafik yaratan hostlar, en çok istek gelen portlar ve uygulamaların görüntülediği bölümdür.



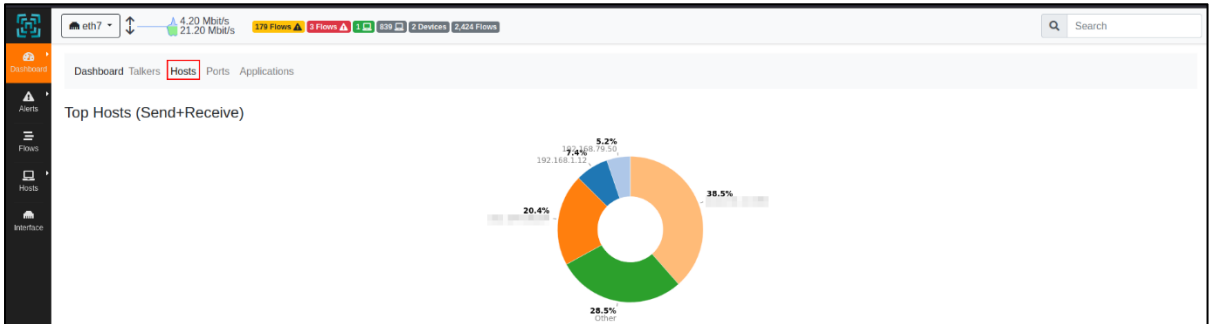
18.2.1.1 Talkers

Bu bölümümdede en çok trafik yaratan IP adresleri görüntülenir. Yapılan istekler kaynaktan hedefe doğrudur.



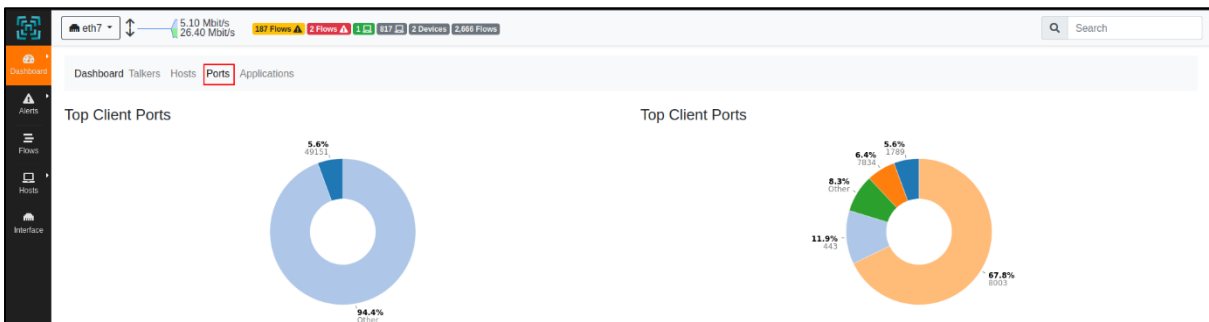
18.2.1.2 Cihazlar

Kullanıcıların yarattığı trafiğin grafik halinde görüntülenir. İstek gönderilen veya alınan hostların IP adresleri görüntülenir.



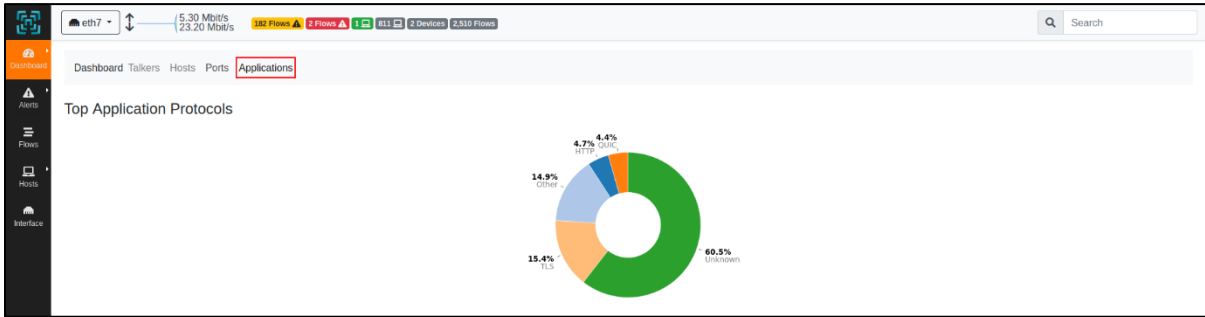
18.2.1.3 Portlar

En çok istek atılan port bilgileri görüntülenir.



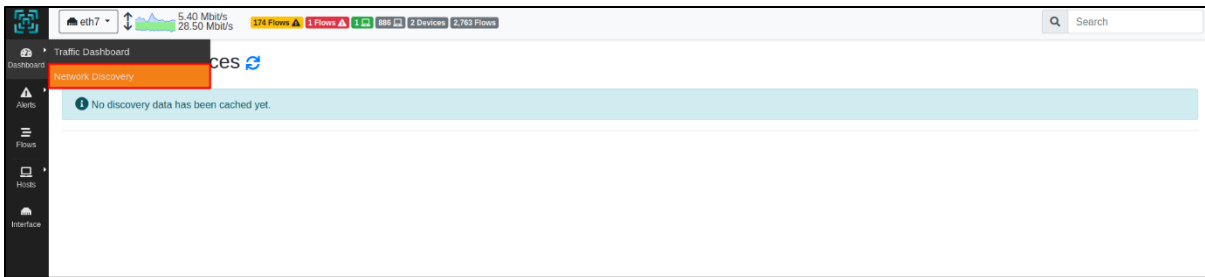
18.2.1.4 Uygulama

Kullanıcıların yarattığı trafikteki en çok kullanılan uygulama bilgisi görüntülenir.



18.2.2 Ağ Keşfi

Bilgisayar ağları üzerindeki cihazların ve kaynakların tespit edildiği bölümdür. Ağ trafiğindeki cihazların görüntülediği bölümdür.



18.3 Uyarılar

Ağ trafiğindeki anormal ve potansiyel uyarıların görüntülediği bölümdür.

Date/Time	Duration	Severity	Alert Type	Drilldown	Description	Actions
20:38:06	01:27:57	Error	Packet Drops	interface eth1	interface eth1 has too many dropped packets [> 0%]	[lock icon]

18.3.1 Engaged Uyarılar

Ağ trafiğindeki anormal trafiğin görüntülediği bölümdür.

1 Date/Time	2 Duration	3 Severity	4 Alert Type	5 Drilldown	6 Description	7 Actions
20:38:06	01:27:57	Error	Packet Drops	interface eth1	interface eth1 has too many dropped packets [> 0%]	[lock icon]

1	Tarih/Saat	Uyarının geldiği tarih ve satın görüntülediği bölümdür.
2	Süre	Uyarıların süresinin görüntülediği bölümdür.
3	Sertlik	Uyarının sertlik tipinin görüntülediği bölümdür.
4	Uyarı Tipi	Uyarı tipinin görüntülediği bölümdür.
5	Derinlik	Uyarının derinlik bilgisinin görüntülediği bölümdür.
6	Açıklama	Uyarı ile ilgili açıklamaların görüntülediği bölümdür.
7	Etki	Uyarı ile ilgili yapılacak eylemin seçildiği bölümdür. Uyarının yayımlandığı butondur.

18.3.2 Geçmiş Uyarılar

Geçmiş uyarıların görüntülediği bölümdür.

Date/Time	Duration	Count	Severity	Alert Type	Drilldown	Description	Actions
12/03/2024 13:09:00	02:01	1	Warning	Ghost Network Detected		Subnet 192.168.100.0/25 does not belong to the eth1 networks.	[Action]
13/03/2024 00:19:01	03:04	1	Warning	Ghost Network Detected		Subnet 192.168.100.0/25 does not belong to the eth1 networks.	[Action]
13/03/2024 00:32:06	00:55	1	Warning	Slow Periodic Activity		Periodic activity 'periodic_user_scripts.lua' running for too long [more than 01:00] or executed too late (blocked in queue).	[Action]
28/03/2024 16:52:06	20:00	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/28 does not belong to the eth1 networks.	[Action]
28/03/2024 17:17:05	04:00	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/28 does not belong to the eth1 networks.	[Action]
28/03/2024 17:24:06	02:00	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/28 does not belong to the eth1 networks.	[Action]
28/03/2024 17:26:06	00:59	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/27 does not belong to the eth1 networks.	[Action]
28/03/2024 17:28:05	03:01	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/27 does not belong to the eth1 networks.	[Action]
28/03/2024 17:35:05	02:00	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/27 does not belong to the eth1 networks.	[Action]
28/03/2024 18:04:06	06:47:00	1	Warning	Ghost Network Detected		Subnet 192.168.2.0/27 does not belong to the eth1 networks.	[Action]

1	Tarih/Saat	Geçmiş uyarının geldiği tarih ve satın görüntülediği bölümdür.
2	Süre	Gelen uyarıların süresinin görüntülediği bölümdür.
3	Toplam Uyarı	Gelen uyarının toplam uyarı sayısının görüntülediği bölümdür.

	Sayısı	bölümdür.
4	Sertlik	Gelen uyarının sertlik tipinin görüntülediği bölümdür.
5	Uyarı Tipi	Gelen uyarıların tipinin görüntülediği bölümdür.
6	Derinlik	Gelen uyarının derinlik bilgisinin görüntülediği bölümdür.
7	Açıklama	Gelen uyarılar ile ilgili açıklamaların görüntülediği bölümdür.
8	Etki	Gelen uyarı ile ilgili yapılacak eylemin seçildiği bölümdür. Uyarının silindiği butondur.

18.3.3 Uyarı Akışları

Gelen uyarıların detaylarının akış halinde görüntülediği bölümdür

1	2	3	4	5	6	7	8	9
Date/Time	Duration	Count	Severity	Alert Type	Score	Drilldown	Description	Actions
19/05/2024 03:55:27	04:42	2	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.1.254:137 ⇄ 192.168.1.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:05:23		1	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.23.1:137 ⇄ 192.168.23.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:05:23		1	Notice	Remote to Remote	15		Remote client and remote server [Flow: 10.0.0.1:137 ⇄ 10.0.0.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:05:23		1	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.1.254:137 ⇄ 192.168.1.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:10:28	04:38	2	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.23.1:137 ⇄ 192.168.23.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:10:28	04:38	2	Notice	Remote to Remote	15		Remote client and remote server [Flow: 10.0.0.1:137 ⇄ 10.0.0.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:10:28	04:38	2	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.1.254:137 ⇄ 192.168.1.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:20:20		1	Notice	Remote to Remote	15		Remote client and remote server [Flow: 192.168.23.1:137 ⇄ 192.168.23.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]
19/05/2024 04:20:20		1	Notice	Remote to Remote	15		Remote client and remote server [Flow: 10.0.0.1:137 ⇄ 10.0.0.255:137] [UDP] [Application: NetBIOS] [Info: labris]	[X]

1	Tarih/Saat	Uyarıların geldiği tarih ve saatin görüntülediği bölümdür.
2	Süre	Uyarıların süresinin görüntülediği bölümdür.
3	Toplam Uyarı	Gelen uyarının toplam uyarı sayısının görüntülediği bölümdür.

	Sayısı	bölümdür.
4	Sertlik	Gelen uyarının sertlik tipinin görüntülediği bölümdür.
5	Uyarı Tipi	Gelen uyarıların tipinin görüntülediği bölümdür.
6	Puan	Gelen uyarının puanının görüntülediği bölümdür.
7	Derinlik	Gelen uyarının derinlik bilgisinin görüntülediği bölümdür.
8	Açıklama	Gelen uyarılar ile ilgili açıklamaların görüntülediği bölümdür.
9	Etki	Gelen uyarı ile ilgili yapılacak eylemin seçildiği bölümdür. Uyarının silindiği butondur.

18.4 Akış

Trafik analizi özelliğinin açıldığı arabirime ait olan trafik akışının görüntülediği bölümdür.

1	2	3	4	5	6	7	8	9	10
Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info	Info
Unknown	UDP	192.168.10.25:50768	46.154.196.92:35577	36.27	Server	450.00 kbit/s ↑	115.16 MB ↑		
G+ Google	UDP	192.168.10.192:50491	173.194.15.168:443	23.32	Server	1.20 Mbit/s ↑	108.87 MB ↑		
Facebook	UDP	192.168.10.139:63352	157.240.234.63:443	08.15	Server	0 bps —	92.69 MB —		
G+ Google	UDP	173.194.182.70:443	192.168.10.138:60778	36.21	Client	760.80 kbit/s ↓	87.4 MB ↑		
G+ Google	UDP	192.168.11.21:50693	173.194.15.201:443	02.26	Server	0 bps —	112.77 MB ↑		
Facebook	UDP	192.168.10.139:55040	157.240.234.63:443	08.17	Server	0 bps —	54.45 MB —		
Facebook	UDP	192.168.10.54:53418	157.240.234.63:443	31.23	Server	0 bps ↓	51 MB ↑		
G+ Google	UDP	192.168.11.26:50357	173.194.15.105:443	27.37	Server	0 bps —	47 MB ↑		
Facebook	UDP	192.168.10.30:39175	157.240.9.52:443	06.30	Server	0 bps —	41.58 MB —		
Facebook	UDP	192.168.10.30:35170	157.240.234.63:443	06.42	Server	3.40 Mbit/s ↑	44.79 MB ↑		

1	Detay	Trafik akışının detayları görüntülenir.
2	Uygulama	Trafikteki uygulama bilgisi görüntülenir.

3	Protokol	İstemcinin yaratmış olduğu trafikteki protokol bilgisi görüntülenir.
4	İstemci	İstemcinin IP adresi ve kaynak port bilgisi görüntülenir.
5	Sunucu	Sunucu IP adresi ve hedef port bilgisi görüntülenir.
6	Süre	İstemcinin belirli bir hedefe doğru yarattığı süre görüntülenir.
7	Breakdown	İstemciden sunucuya doğru ya da sunucudan istemciye doğru trafiği gösterir. İstemciden sunucuya doğru trafik akışı var ise turuncu ile sunucudan istemciye doğru trafik akışı var ise mavi olarak görüntülenir.
8	Bantgeniřliđi	İstemcinin bantgeniřliđi kullanımı görüntülenir
9	Toplam Byte	Akıřtaki toplam byte boyutunun görüntülendiđi bölümdür. İstemci sunucu veya sunucu istemci arasındaki toplam byte boyutu görüntülenir.
10	Açıklama	Trafik akıřına ait açıklama görüntülenir.

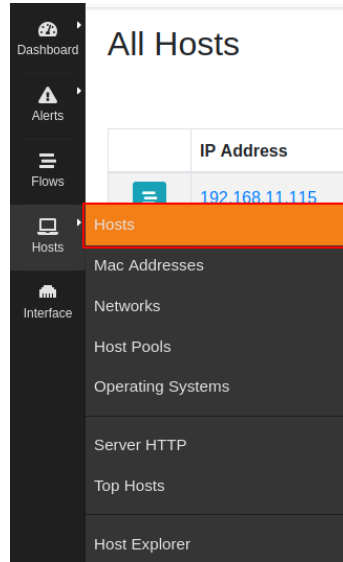
-Trafik akıřının detayı görebilmek için büyüteç butonuna basılır.

Application	Protocol	Client	Server	Duration	Breakdown	Actual Thp	Total Bytes	Info
G+ Google	UDP	192.168.10.197:55908	173.194.15.70:443	00:27	Server	0 bps ↓	11.44 MB ↑	

Flow: 192.168.10.197:55908 ⇄ 173.194.15.70:443 Overview	
Flow Peers [Client / Server]	192.168.10.197:55908 [] ⇄ 173.194.15.70:443 []
Protocol / Application	UDP / G+ Google (Web)
First / Last Seen	05/07/2024 08:54:23 [01:33 ago] 05/07/2024 08:55:53 [00:03 ago]
Total Traffic	Total: 27.3 MB ↑ Goodput: 26.3 MB (96.4 %) ↑
	Client → Server: 2,393 Pkts / 254.7 KB ↑ Client ← Server: 22,038 Pkts / 27 MB ↑
DSCP / ECN [Client / Server]	Best Effort (CS0) / Disabled (0) Best Effort (CS0) / Disabled (0)
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / 37.93 ms / 7492 ms Client ← Server: < 1 ms / 4.08 ms / 7499 ms
Entropy	Client → Server: 7.699 Client ← Server: 7.685
Actual / Peak Throughput	0 bit/s → / 16.6 Mbit/s

18.5 Cihazlar

Cihazların ağ trafiğinin analiz edildiği modüldür.



18.5.1 Cihazlar

Trafik analizinin açıldığı arabirimdeki tüm cihazların görüntülediği bölümdür.

1	2	3	4	5	6	7	8	9	10
IP Address	Location	Flows	Total Bytes Sent	Name	Seen Since	Breakdown	Throughput	Total Bytes	
192.168.10.46	Local	11	33.34 MB		03:02:40	Recv	0 bit/s	1.65 GB	
74.125.13.39	Remote	0	212.37 MB	74.125.13.39	19:08	Send	0 bit/s	215.19 MB	
192.168.10.30	Local	41	15.94 MB		03:04:04	Recv	41.02 kbit/s	844.02 MB	
157.240.9.52	Remote	5	3.28 GB	157.240.9.52	03:02:38	Send	0 bit/s	3.31 GB	
192.168.10.73	Local	71	147.12 MB		02:35:57	Recv	43.7 kbit/s	1.81 GB	
192.168.11.57	Local	44	42.77 MB	192.168.11.57	03:22:24	Recv	52.6 kbit/s	503.52 MB	
192.168.10.38	Local	51	223.78 MB		19:46:44	Recv	30.31 kbit/s	1.05 GB	
173.194.15.135	Remote	1	230.77 MB	173.194.15.135	01:00:04	Send	0 bit/s	235.16 MB	
20.10.16.51	Remote	2	3.24 MB	20.10.16.51	42:40	Recv	26.64 kbit/s	52.34 MB	
34.36.216.83	Remote	1	64.91 KB	34.36.216.83	00:22	Recv	52.6 kbit/s	3.8 MB	

1	Detay	Cihazların oluşturduğu trafik akışının detayları görüntülenir.
2	IP Adresi	Cihazların IP adresleri görüntülenir.
3	Yer	Cihazların ağ üzerindeki konum bilgileri görüntülenir.
4	Akış	Cihazın toplam akış sayısı görüntülenir.

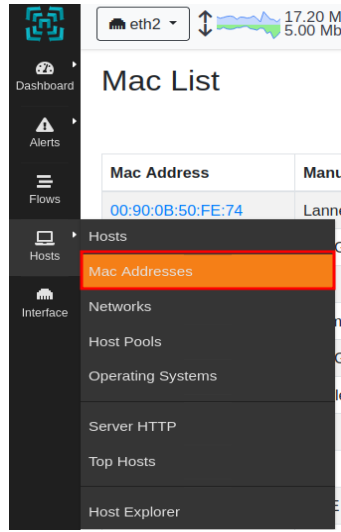
5	Toplam Gönderilen Byte	Cihazların toplam gönderilen byte boyutu görüntülenir.
6	İsim	İstemcinin belirli bir hedefe doğru yarattığı süre görüntülenir.
7	Son Görünme Zamanı	Cihazların yarattığı trafikteki son görülme zamanı görüntülenir.
8	Breakdown	Cihazların gelen ve giden paketlere ilişkin grafikleri gösterir.
9	Bantgenişiği	Cihazların bantgenişiği kullanımı görüntülenir
10	Toplam Byte	Cihazların toplam byte boyutu görüntülenir.

-Cihazın trafiğini detaylı olarak incelemek için detay butonuna basılır. Detay butonuna basıldıktan sonra gelen ekranda seçilen cihaza göre trafik, paket, DSCP, port, eşlenen IP adreslerini, ICMP isteklerini, uygulama, dns, tls, http ve akış detayları görüntülenir.

Host: 192.168.11.20									
Traffic Packets DSCP Ports Peers ICMP Applications DNS TLS HTTP Flows									
Active Flows [Host 192.168.11.20]									
10 Hosts Status Severity Direction Applications Categories IP Version Protocol									
	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
	Facebook	UDP	192.168.11.20:51956	157.240.9.52:443	00:41	Server	5.60 Mbit/s	9.95 MB	
	DNS.DeH_DoT	UDP	192.168.11.20:55614	8.8.8.8:53	< 1 sec	Client Server	0 bps	216 Bytes	dns.google
	MDNS	UDP	192.168.11.20:5353	_companion-link_tcp.loc...:5353	00:12	Client	0 bps	1.09 KB	_companion-link_tcp.loc...
	Unknown	UDP	192.168.11.20:50687	172.224.106.196:443	00:01	Client Server	0 bps	9 KB	
	DNS.Apple	UDP	192.168.11.20:58777	8.8.8.8:53	< 1 sec	Client Server	0 bps	241 Bytes	mask.apple-dns.net
	Facebook	UDP	192.168.11.20:58576	157.240.234.63:443	00:40	Client Server	0 bps	60.09 KB	
	DNS.Apple	UDP	192.168.11.20:52883	8.8.8.8:53	< 1 sec	Client Server	0 bps	284 Bytes	mask.apple-dns.net
	Facebook	TCP	192.168.11.20:55234	157.240.234.175:5222	00:01	Client Server	0 bps	3.98 KB	
	Facebook	UDP	192.168.11.20:60155	157.240.234.15:443	< 1 sec	Client Server	0 bps	10.87 KB	
	Facebook	UDP	192.168.11.20:62315	185.60.218.52:443	00:40	Client Server	0 bps	5.56 KB	

18.5.2 Mac Adres

Trafik akışının MAC adreslerine göre analizinin yapıldığı bölümdür.



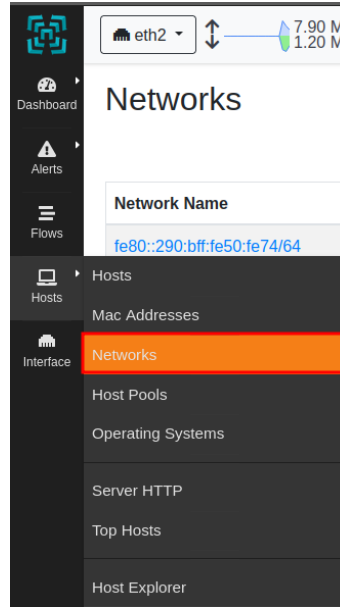
Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
00:90:0B:...	...	Router/Switch	...	857	230.830	21:42:40	...	35.24 Mbit/s	92.88 GB
1C:69:7A:...	...	Unknown	...	1	209	05:07:37	...	0 bit/s	1.26 MB
E4:54:E8:...	...	Computer	...	3	208.923	21:42:37	...	21.41 kbit/s	860.29 MB
00:21:B7:...	...	Printer	...	2	604	21:42:34	...	0 bit/s	7.12 MB
1C:69:7A:...	...	Computer	...	2	6.618	04:47:58	...	824.25 kbit/s	795.8 MB
48:BA:4E:...	...	Printer	...	2	39	21:42:34	...	0 bit/s	6.97 MB
EA:4D:02:...	...	Unknown	...	2	683	04:45:03	...	0 bit/s	344.6 MB
E4:54:E8:...	...	Unknown	...	2	6.028	21:42:26	...	2.38 Mbit/s	209.03 MB
1C:FD:08:...	...	Unknown	...	2	6.253	21:42:38	...	9.3 kbit/s	179.72 MB
E4:54:E8:...	...	Computer	...	1	3.050	04:03:13	...	1.84 kbit/s	382.48 MB

1	Mac Adres	Mac Adres bilgisi görüntülenir.
2	Üretici	Üretici firmanın bilgisi görüntülenir.(MAC adresine bakarak tespit yapılır.)
3	Cihaz Tipi	MAC adresine bakarak cihazın tipi görüntülenir.
4	İsim	Cihazın ismi görüntülenir.
5	Cihaz	Cihazın, cihazlar modülündeki toplam sayısı görüntülenir.
6	Arp	Cihazın arp isteğinin toplam sayısını görüntülenir.

7	Son Görülme Zamanı	MAC adresleri tarafından gönderilen/alınan ilk paketin gözlemlenmesinden bu yana geçen sürenin görüntülediği bölümdür.
8	Breakdown	Gelen ve giden pakete ilişkin grafikleri gösterir.
9	Bantgenişliği	Cihazların bantgenişliği kullanımı görüntülenir
10	Trafik	Cihazların toplam byte boyutu görüntülenir.

18.5.3 Ağlar

Trafik akışının ağ adreslerine göre analizinin yapıldığı bölümdür.

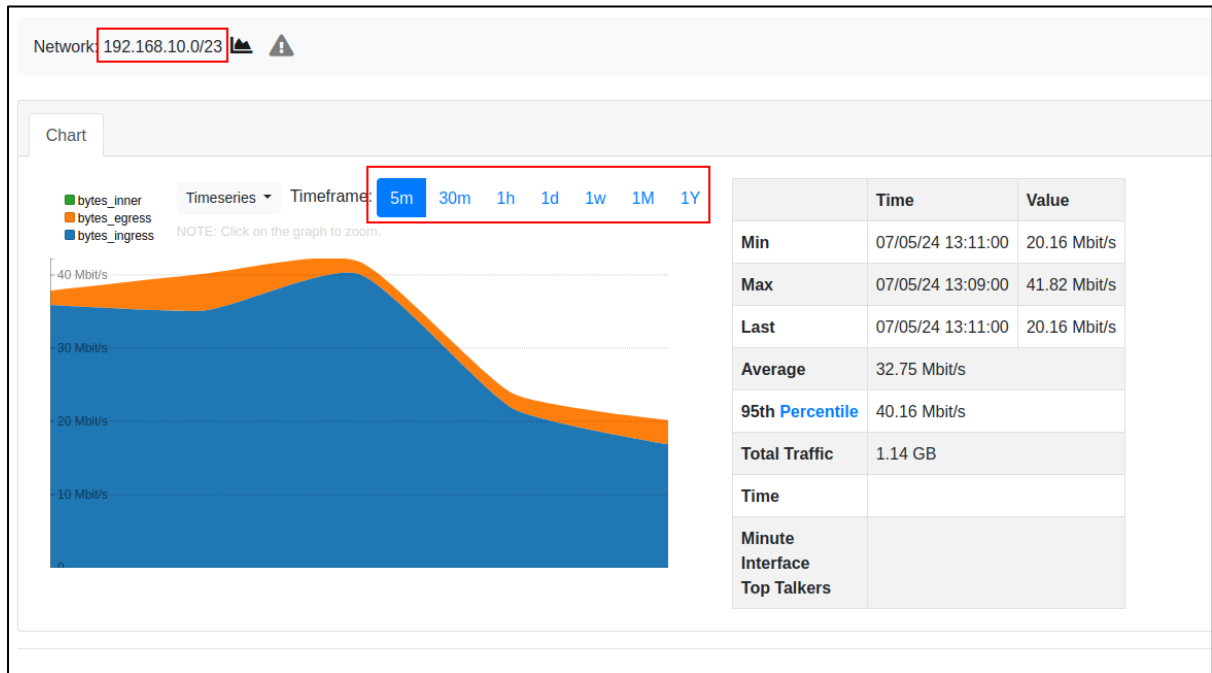


Network Name	Chart	Hosts	Breakdown	Throughput	Traffic
fe80::290:bff:fe50:fe74/64		86	Send	33.96 kbit/s	132.47 MB
192.168.10.0/23		131	Send	46.04 Mbit/s	107.65 GB

1	Ağ İsmi	Ağ isminin görüntülediği bölümdür.
2	Tablo	Ağ adresleri ile ilgili trafiğin tablo olarak görüntülediği bölümdür.

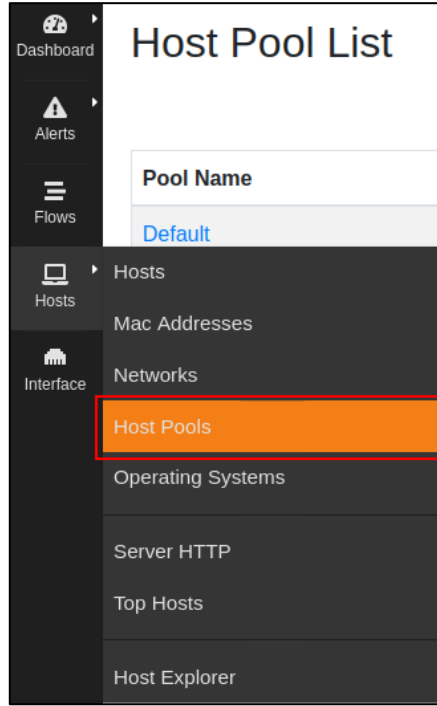
3	Breakdown	Ağ adresi ile ilişkili gelen ve giden paketlere ilişkin grafikleri gösterir.
4	Bantgeniřliđi	Ağ adresine ait bant geniřliđi görüntülenir.
5	Trafik	Ağ adreslerine ait trafiđin paket boyutu görüntülenir.

-Ağ adresi ile ilgili trafiđi 5dk, 30dk ,1 saat, 1gün,1hafta, 1 ay ve 1 yıl řeklinde detayları görüntülenir.



18.5.4 Cihaz Havuzları

Tanımlanmış ve aktif olan cihaz havuzlarının listesini gösterir.



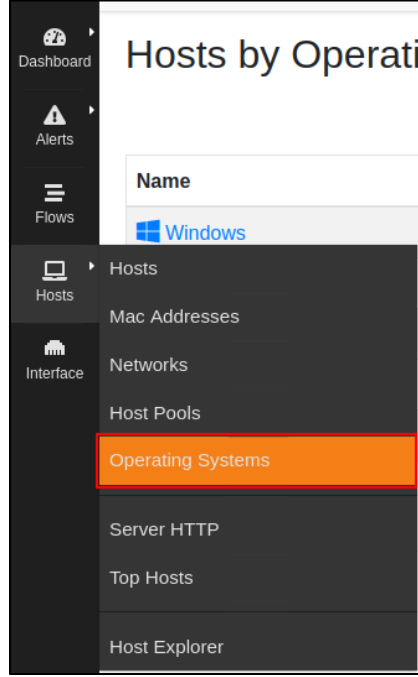
Pool Name	Hosts	Seen Since	Breakdown	Throughput	Traffic
Default	779	1 Day, 08:12		42.47 Mbit/s	127.0 GB

Showing 1 to 1 of 1 rows

1	Havuz İsmi	Cihaz havuzunun isminin görüntülediği bölümdür.
2	Cihazlar	Havuzda dahil olan cihazların sayısının görüntülediği bölümdür.
3	Breakdown	Cihaz Havuzuyla ilişkili gelen ve giden paketlere ilişkin grafikleri gösterir.
4	Bantgenişliği	Cihaz havuzlarına ait bant genişliği görüntülenir.
5	Trafik	Cihaz havuzlarına ait trafiğin paket boyutu görüntülenir.

18.5.5 İşletim Sistemi

Trafik akışında Labris UTM cihazı tarafından tespit edilen işletim sistemleri görüntülediği bölümdür.



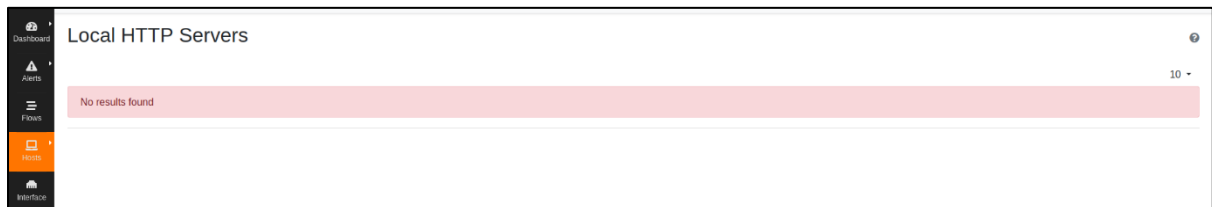
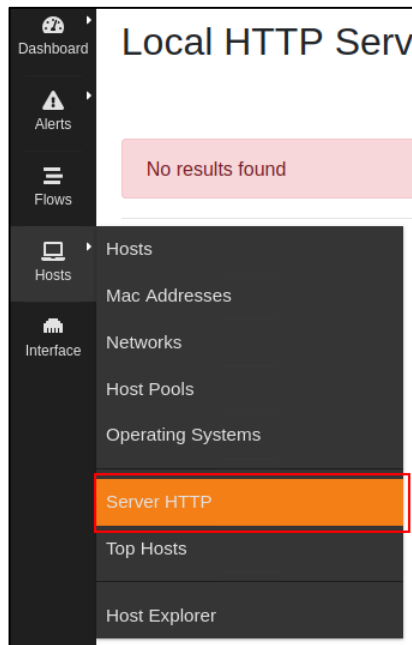
Name	Hosts	Alerts	Seen Since	Breakdown	Throughput	Traffic
Windows	31	0	1 Day, 16:15	Send Recd	124.86 Mbit/s	63.1 GB
Unknown	925	1	1 Day, 16:15	Send Recd	133.67 Mbit/s	35.42 GB
Linux	12	0	08:05:07	Send Recd	38.93 kbit/s	5.69 GB
Android	9	0	08:16:57	Send Recd	69.79 kbit/s	5.05 GB
iOS	1	0	07:14:23	Send Recd	0 bit/s	632.56 MB

1	İsim	Labris UTM cihazı tarafından tespit edilen işletim sisteminin görüntülediği bölümdür.
2	Cihazlar	İşletim sistemini kullanan cihaz sayısı görüntülenir.
3	Uyarılar	İşletim sistemindeki cihazların uyarı sayısı görüntülenir.
4	Son Görülme Zamanı	İşletim sistemi tarafından gönderilen/alınan ilk paketin gözlemlenmesinden buy ana geçen sürenin görüntülediği bölümdür.

5	Breakdown	İşletim sistemi ile ilişkili gelen ve giden paketlere ilişkin grafikleri gösterir.
6	Bant genişliği	Labris UTM cihazı tarafından tespit edilen işletim sistemine sahip cihazların toplam kullandığı bantgenişliğini gösterir.
7	Trafik	Labris UTM cihazı tarafından tespit edilen işletim sistemine sahip cihazların toplam yarattığı trafiğini gösterir.

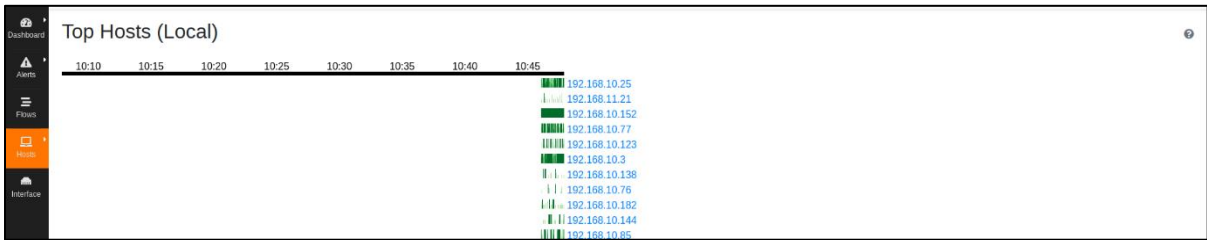
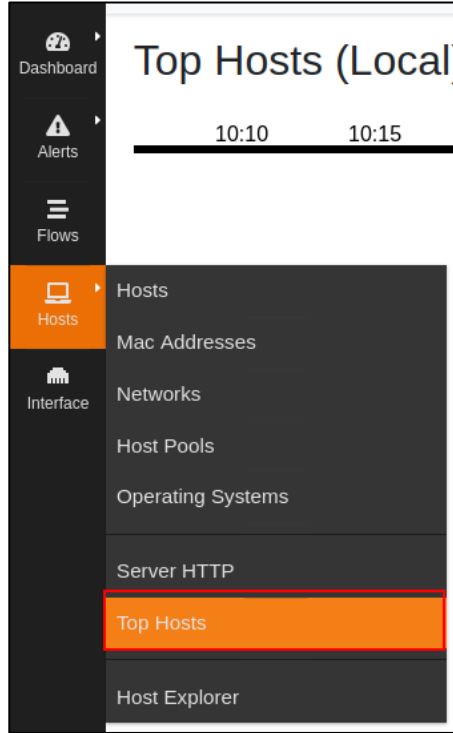
18.5.6 HTTP Sunucu

Yerel ağda bulunan HTTP sunucuların listesi görüntülenir. Eğer Trafik Analizinin açıldığı arabirimde http sunucu yok ise sayfa 'herhangi bir sonuç bulunamadı' şeklinde hata verir.



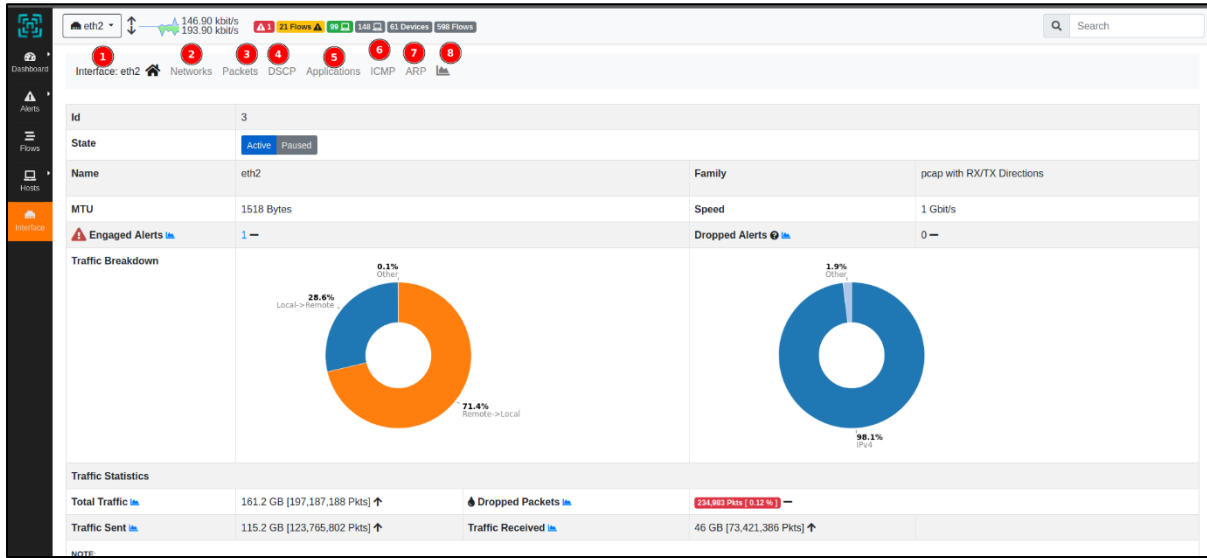
18.5.7 Top cihazlar

Bu modülde ise en çok trafik oluşturan yerel ağda bulunan cihazların listesi görüntülenir.



18.6 Arabirim

Trafik analizinin açıldığı arabirime ait bilgilerin detaylarının görüntülediği bölümdür.



1	Arabirim	İncelenen arabirimin görüntülediği bölümdür.
2	Ağ	Seçilen arabirime ait ağ adresleri görüntülenir.
3	Paketler	Seçilen arabirime ait paket boyutu dağılımının pasta grafiğini gösterir.
4	DSCP	Arabirime ait DSCP paker bilgileri görüntülenir.
5	Uygulama	Arabirimden geçen uygulamaa bilgileri görüntülenir.
6	ICMP	Arabirime ait ICMP trafiği görüntülenir.
7	Arp	Arabirime ait ARP trafiği görüntülenir.
8	Grafik	Arabirime ait trafik grafik halinde görüntülenir.

18.6.1 Ağ

Arabirimdeki ağ trafiğinin detayları görüntülenir.

Interface: eth2 🏠 Networks Packets DSCP Applications ICMP ARP 📊

IP Address 1	<ul style="list-style-type: none"> • 192.168.10.1/32 • fe80::290:bff:fe50:fe74/128
Broadcast Domain 2	<ul style="list-style-type: none"> • 192.168.1.0/24 🚫 • 192.168.10.0/23 • 95.3.35.160/28 🚫

1	IP Adresleri	İncelenen arabirimin IP adres bilgileri yer alır.
2	Broadcast Domain	ARP trafiği incelenilir ve arabirime ait broadcast domainler tespit edilir.

18.6.2 Paketler

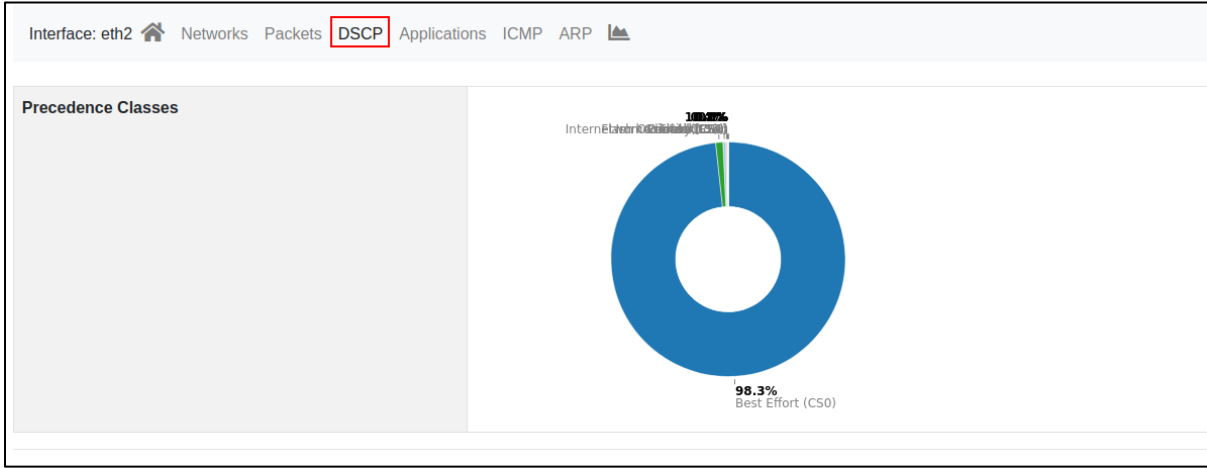
Trafikteki paket boyutunun dağılımını pasta grafiği şeklinde görüntülenir.

Interface: eth2 🏠 Networks Packets DSCP Applications ICMP ARP 📊

TCP Packets Analysis	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Retransmissions</td> <td style="text-align: right;">121,558 Pkts</td> </tr> <tr> <td>Out of Order</td> <td style="text-align: right;">666,746 Pkts</td> </tr> <tr> <td>Lost</td> <td style="text-align: right;">449,855 Pkts</td> </tr> </table>	Retransmissions	121,558 Pkts	Out of Order	666,746 Pkts	Lost	449,855 Pkts	
Retransmissions	121,558 Pkts							
Out of Order	666,746 Pkts							
Lost	449,855 Pkts							
Size Distribution								
IP version vs TCP Flags Distribution								

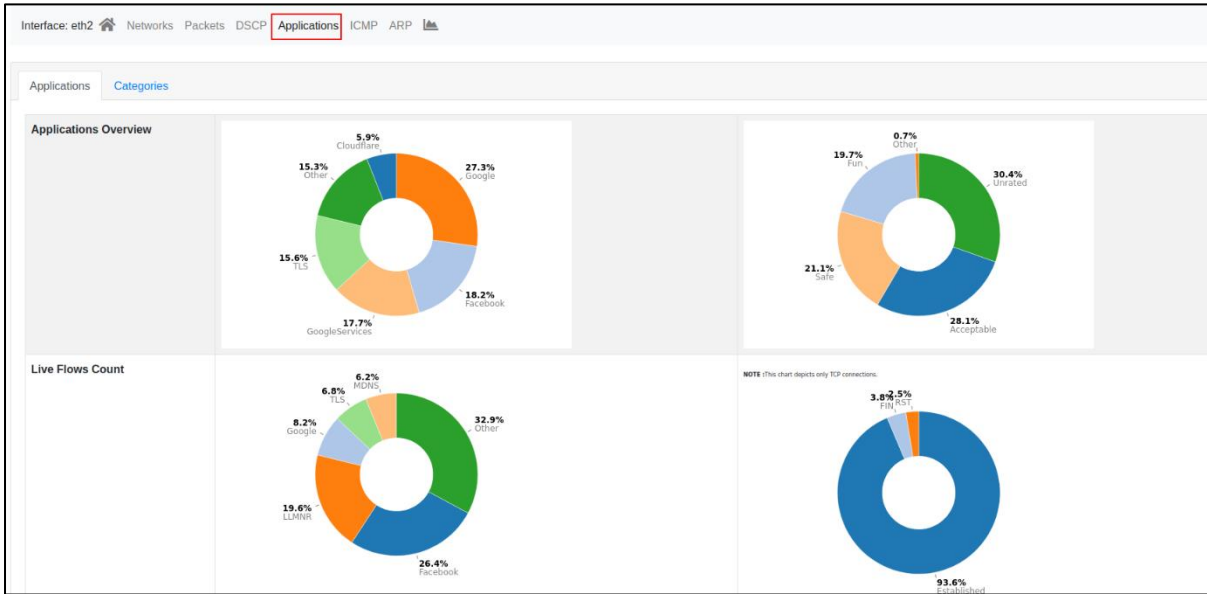
18.6.3 DSCP

DSCP, internet üzerinde veri iletiminde kullanılan bir kalite hizmet mekanizmasıdır. Bu bölümde ise DSCP dağılımını pasta grafiği şeklinde görebilir.



18.6.4 Uygulamalar

Arabirime ait ağ trafiğindeki uygulama kullanım detaylarını pasta grafiği şeklinde görebildiğimiz bölümdür.



18.6.5 ICMP

Arabirime ait ICMP istatistikleri görüntülediği bölümdür.

ICMP Message	Type	Code	Packets
Echo Reply	0	0	746 Pkts
Unassigned	1	177	1 Pkt
Host Unreachable	3	1	2,584 Pkts
Communication with Destination Host is Administratively Prohibited	3	10	17 Pkts
Communication Administratively Prohibited	3	13	5 Pkts
Destination Unreachable	3	135	1 Pkt
Protocol Unreachable	3	2	3 Pkts
Port Unreachable	3	3	42,365 Pkts

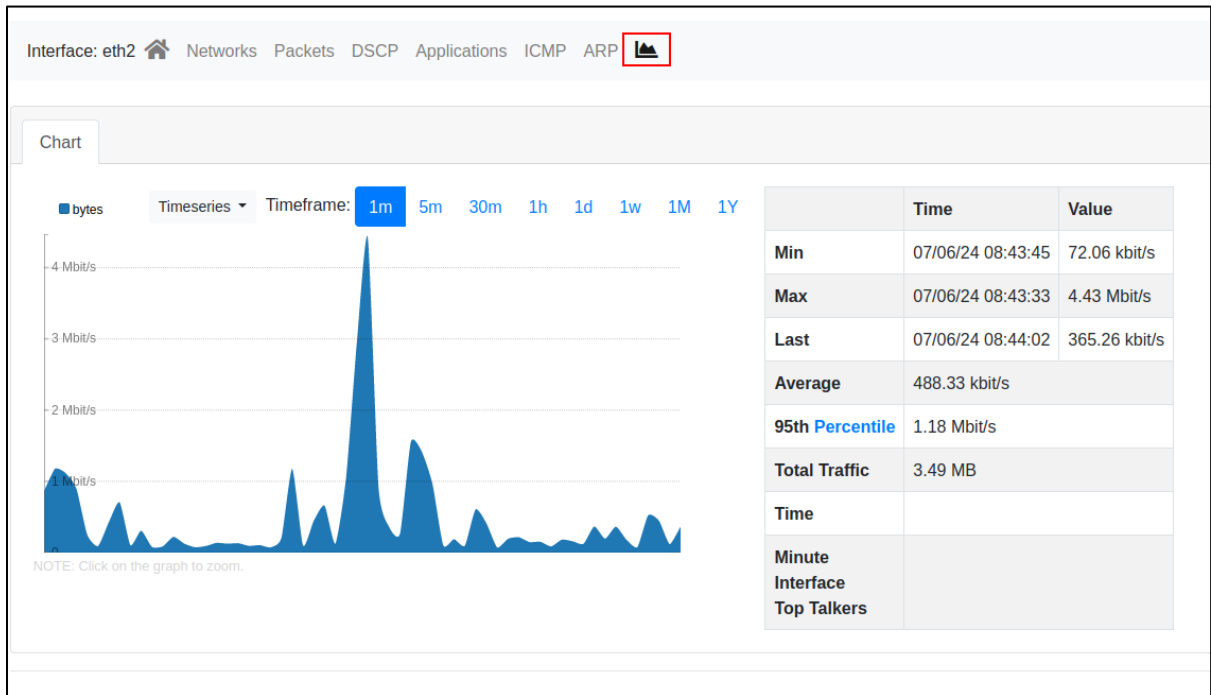
18.6.6 ARP

Arabirime ait ARP istatistiklerinin görüntülediği bölümdür.

ARP Type	Packets
ARP Requests	1988967
ARP Replies	218251

18.6.7 Grafik

Seçilen arabirime ait detaylarının görüntülediği bölümdür. 1 dakika, 5 dakika, 30 dakika, 1 saat, 1 gün, 1 hafta, 1 ay ve 1 yıllık trafik raporu görüntülenir.



19. Kayıtlar ve Raporlar

Labris UTM cihazında tutulan kayıtların görüntülediği ve tutulan kayıtların raporlandığı modüldür. Kayıtlar ve Raporlar modülünde kayıtlar, raporlar ve zaman damgaları loglar bulunur. Tutulan logları anlık olarak olarak izlenebilir ya da arşivde tutulan loglar görüntülenir. Kayıtlar ve raporlar sayfasını açmak için Kayıtlar ve Raporlara tıklanır.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Category	
2024-06-03 09:23:59	172.16.10.17	-	5222	172.16.10.118	-	5222	INVALID_PACKET	DROP	TCP	0x00000000	-	
2024-06-03 09:23:59	172.16.10.17	-	64369	172.16.10.118	-	443	R1	LOG	TCP	SSL_SSL	Web Services	
2024-06-03 09:23:59	172.16.10.17	-	64369	172.16.10.118	-	443	RS	ACCEPT	TCP	SSL_SSL	Web Services	
2024-06-03 09:23:59	172.16.10.63	-	59309	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.63	-	59309	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.63	-	61207	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.63	-	61207	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	64803	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	64803	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	52909	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	52909	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	48895	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	48895	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	50055	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	50055	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	68	255.255.255.255	-	67	APP	APP	UDP	DHCP_DHCP	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.10.10	-	53	APP	APP	UDP	ICMP_ICMP	Networks Monitoring	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.10.17	-	65525	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.10.17	-	59391	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.10.17	-	65311	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.11.17	-	64621	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.11.48	-	64803	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.11.48	-	52909	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.11.48	-	48895	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.1	-	53	172.16.11.48	-	50055	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	52370	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.11.48	-	52370	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.157	-	45988	92.122.192.234	-	443	INVALID_PACKET	DROP	TCP	0x00000000	-	
2024-06-03 09:23:59	172.16.10.157	-	53	172.16.10.118	-	52370	APP	APP	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.157	-	443	172.16.10.17	-	64368	APP	APP	UDP	TCP	CLOUD_Cloud	File Transfer
2024-06-03 09:23:59	172.16.10.157	-	443	172.16.10.17	-	64368	APP	APP	UDP	TCP	CLOUD_Cloud	File Transfer
2024-06-03 09:23:59	172.16.10.157	-	65303	52.183.220.149	-	443	R1	LOG	TCP	SSL_SSL	Web Services	
2024-06-03 09:23:59	172.16.10.157	-	65303	52.183.220.149	-	443	RS	ACCEPT	TCP	SSL_SSL	Web Services	
2024-06-03 09:23:59	172.16.11.178	-	65406	54.54.54.92	-	443	INVALID_PACKET	DROP	TCP	0x00000000	-	
2024-06-03 09:23:59	172.16.10.157	-	57165	172.16.10.118	-	53	R1	LOG	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.157	-	57165	172.16.10.118	-	53	RS	ACCEPT	UDP	DNS_DNS	Networking	
2024-06-03 09:23:59	172.16.10.157	-	443	172.16.10.17	-	64368	APP	APP	UDP	TCP	CLOUD_Cloud	File Transfer
2024-06-03 09:23:59	172.16.10.157	-	443	172.16.10.17	-	64368	APP	APP	UDP	TCP	CLOUD_Cloud	File Transfer

19.1 Kayıtlar

Labris UTM cihazında tutulan kayıtların görüntülediği modüldür. Bu modülde anlık olarak tutulan kayıtlar ve arşivde tutulan loglar görüntülenir. Tutulan kayıtlar; güvenlik duvarı, web filtre, servis, yönetimsel, wauth, mail, IPMAC, DHCP, SSLVPN, ataklar, IPsec ve bağlantı kayıtları görüntülenir.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Category
2024-05-17 09:01:52	192.168.1.10	-	44360	192.168.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x00000000	-
2024-05-17 09:01:52	192.168.1.10	-	44376	192.168.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x00000000	-
2024-05-17 09:01:18	192.168.0.2	-	138	192.168.0.255	-	138	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:01:18	192.168.1.254	-	138	192.168.1.255	-	138	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:01:18	192.168.2.1	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:01:18	10.0.0.1	-	138	10.0.0.255	-	138	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:01:18	10.14.15.2	-	138	10.14.15.255	-	138	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:01:18	192.168.1.10	-	37652	192.168.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x00000000	-
2024-05-17 09:01:18	192.168.1.10	-	37656	192.168.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x00000000	-
2024-05-17 09:01:06	192.168.1.1	-	98228	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:01:07	192.168.1.254	-	39468	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:01:04	192.168.1.254	-	39468	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:00:58	192.168.2.1	-	55163	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:55	192.168.1.10	-	57652	192.168.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x00000000	-
2024-05-17 09:00:48	192.168.2.1	-	38524	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:20	192.168.2.1	-	35295	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:13	192.168.1.254	-	39383	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:00:10	192.168.2.1	-	58823	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:04	192.168.1.254	-	39333	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:00:04	192.168.1.2	-	137	192.168.0.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:04	192.168.0.2	-	137	192.168.0.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:04	192.168.1.254	-	137	192.168.1.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:04	192.168.2.1	-	137	192.168.2.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:04	10.0.0.1	-	137	10.0.0.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:04	10.14.15.2	-	137	10.14.15.255	-	137	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:03	192.168.2.1	-	69452	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.1.10	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.2.1	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.1.254	-	138	192.168.1.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.2.1	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	10.14.15.2	-	138	10.14.15.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.1.10	-	138	10.0.0.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:00:02	192.168.1.254	-	39304	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:00:02	192.168.1.254	-	39304	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:00:02	192.168.1.10	-	59149	255.255.255.255	-	1124	RO	ACCEPT	UDP	0x00000000	-
2024-05-17 09:00:02	192.168.1.10	-	49811	255.255.255.255	-	3789	RO	ACCEPT	UDP	0x00000000	-

19.1.1 Anlık İzleme

Labris UTM cihazına tutulan logların anlık olarak gösterildiği modüldür. Anlık olarak güvenlik duvarı, web filtre, servis, yönetimsel, wauth, mail, IPMAC, DHCP, SSLVPN, ataklar, IPsec ve bağlantı kayıtları görüntülenir.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Category
2024-05-17 09:06:09	192.168.2.1	-	39210	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:29	192.168.2.1	-	37655	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:28	169.254.1.10	-	42954	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:06:22	169.254.1.2	-	138	169.254.255.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:22	192.168.0.2	-	138	192.168.0.255	-	138	RO	ACCEPT	UDP	0x30000000	-
2024-05-17 09:06:22	192.168.1.254	-	138	192.168.1.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:22	192.168.2.1	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:22	192.168.23.1	-	138	192.168.23.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:22	10.0.0.1	-	138	10.0.0.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:22	10.14.15.2	-	138	10.14.15.255	-	138	RO	ACCEPT	UDP	0x10000000	-
2024-05-17 09:06:22	192.168.2.1	-	39471	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:18	169.254.1.2	-	137	169.254.255.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:18	192.168.0.2	-	137	192.168.0.255	-	137	RO	ACCEPT	UDP	0x30000000	-
2024-05-17 09:06:18	192.168.1.254	-	137	192.168.1.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:18	192.168.2.1	-	137	192.168.2.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:18	10.0.0.1	-	137	10.0.0.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:18	10.14.15.2	-	137	10.14.15.255	-	137	RO	ACCEPT	UDP	0x10000000	-
2024-05-17 09:06:10	192.168.2.1	-	39051	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:06:08	192.168.1.254	-	39676	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:06:06	192.168.1.254	-	39676	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:04:08	192.168.1.254	-	39647	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:04:05	192.168.1.254	-	39647	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:03:18	169.254.1.2	-	138	169.254.255.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:03:18	192.168.0.2	-	138	192.168.0.255	-	138	RO	ACCEPT	UDP	0x30000000	-
2024-05-17 09:03:18	192.168.1.254	-	138	192.168.1.255	-	138	RO	ACCEPT	UDP	-	-
2024-05-17 09:03:18	192.168.2.1	-	138	192.168.2.255	-	138	RO	ACCEPT	UDP	-	-

19.1.1.1 Güvenlik Duvarı

Labris UTM cihazında tutulan güvenlik duvarı loglarının görüntülediği bölümdür. Güvenlik Duvarı modülünde yazılan kuralların kayıtları görüntülenir.

Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Category
2024-05-17 09:15:38	192.168.2.1	-	41907	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:28	192.168.2.1	-	57602	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:20	192.168.2.1	-	40515	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:18	192.168.2.1	-	39643	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:11	192.168.1.254	-	40346	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:15:10	192.168.2.1	-	32940	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:08	192.168.1.254	-	40346	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:15:08	192.168.2.1	-	59110	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	169.254.1.2	-	137	169.254.255.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	192.168.0.2	-	137	192.168.0.255	-	137	RO	ACCEPT	UDP	0x30000000	-
2024-05-17 09:15:04	192.168.1.254	-	137	192.168.1.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	192.168.2.1	-	137	192.168.2.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	192.168.23.1	-	137	192.168.23.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	10.0.0.1	-	137	10.0.0.255	-	137	RO	ACCEPT	UDP	-	-
2024-05-17 09:15:04	10.14.15.2	-	137	10.14.15.255	-	137	RO	ACCEPT	UDP	0x10000000	-
2024-05-17 09:14:58	192.168.2.1	-	56662	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:48	192.168.2.1	-	54015	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:38	192.168.2.1	-	44677	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:30	169.254.1.10	-	36796	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:14:30	169.254.1.10	-	36812	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:14:30	169.254.1.10	-	36826	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:14:30	169.254.1.10	-	36840	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:14:30	169.254.1.10	-	36846	169.254.1.2	-	81	IN_CONSOLE	ACCEPT	TCP	0x20000000	-
2024-05-17 09:14:28	192.168.2.1	-	56432	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:18	192.168.2.1	-	53523	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:08	192.168.1.254	-	40231	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:14:08	192.168.2.1	-	36537	192.168.2.6	-	53	RO	ACCEPT	UDP	-	-
2024-05-17 09:14:05	192.168.1.254	-	40231	192.168.1.100	-	389	RO	ACCEPT	TCP	-	-
2024-05-17 09:13:58	192.168.1.254	-	36735	192.168.1.100	-	63	RO	ACCEPT	UDP	-	-

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Kaynak	Kayıttaki kaynak IP Adresi bilgisi görüntülenir.

3	Kaynak Kullanıcı	Kayıttaki kaynak kullanıcı bilgisi görüntülenir. Eğer kaynak kullanıcı yok ise '-' işareti ile gösterilir.
4	Kaynak Port	Kayıttaki kaynak port bilgisi görüntülenir.
5	Hedef	Kayıttaki hedef IP adresi bilgisi görüntülenir.
6	Hedef Kullanıcı	Kayıttaki hedef kullanıcı bilgisi görüntülenir. Eğer hedefte kullanıcı bilgisi yok ise '-' işareti ile gösterilir.
7	Hedef Port	Kayıttaki hedef port bilgisi görüntülenir.
8	Kural	Trafiğin geçtiği güvenlik duvarı kuralını gösterir. R3 yazması durumunda trafiğin 3 numaralı Güvenlik Duvarı kuralından geçtiğini gösterir.
9	İşlem	Trafiğin işlem bilgisi görüntülenir. Genellikle bu bölümdür 'ACCEPT, DROP ve APP LOG' görüntülenir.
10	Protokol	Kayıttaki protokol bilgisi görüntülenir. Protokoller TCP, UDP, ICMP 'dir.
11	Uygulama	Kayıttaki uygulama bilgisi görüntülenir. Uygulamalar Labris UTM cihazında tutulan uygulamalardır.
12	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.
13	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
14	Sil	Tutulan logların silindiği bölümdür.

-Güvenlik duvarı kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek IP adresi, kullanıcı, port vb. bilgileri yazılarak filtreleme yapılır.



Date / Time	Source	Source User	Source Port	Destination	Destination User	Destination Port	Rule	Action	Protocol	Application	Category
2024-06-03 10:12:35	172.16.10.12	-	45042	195.175.98.83	-	443	R5	ACCEPT	TCP	0x30000000	Web Services
2024-06-03 10:12:35	172.16.10.12	-	35456	157.240.238.175	-	5222	APP	LOG	TCP	TCP_TCP	Networking
2024-06-03 10:12:35	172.16.10.12	-	45049	195.175.98.83	-	443	R1	LOG	TCP	0x30000000	Web Services
2024-06-03 10:12:35	172.16.10.12	-	45040	195.175.98.83	-	443	R5	ACCEPT	TCP	0x30000000	Web Services
2024-06-03 10:12:35	172.16.10.12	-	45042	195.175.98.83	-	443	R1	LOG	TCP	0x30000000	Web Services
2024-06-03 10:12:34	172.16.10.12	-	43974	195.175.196.18	-	443	APP	LOG	TCP	FBCDN_Web	Streaming Media
2024-06-03 10:12:34	172.16.10.12	-	45054	157.240.238.14	-	443	R1	LOG	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	49524	157.240.238.14	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	45042	195.175.98.83	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	34208	157.240.238.35	-	443	R1	LOG	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	45040	195.175.98.83	-	443	R1	LOG	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	45040	195.175.98.83	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	59277	195.175.98.83	-	443	R1	LOG	UDP	UDP_UDP	Networking
2024-06-03 10:12:34	172.16.10.12	-	34208	157.240.238.35	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:34	172.16.10.12	-	59277	195.175.98.83	-	443	R5	ACCEPT	UDP	UDP_UDP	Networking
2024-06-03 10:12:34	172.16.10.12	-	45042	195.175.98.83	-	443	R1	LOG	TCP	SSL_SSL	Web Services
2024-06-03 10:12:33	172.16.10.12	-	7415	172.16.10.1	-	53	R1	LOG	UDP	DNS_DNS	Networking
2024-06-03 10:12:33	172.16.10.12	-	7415	172.16.10.1	-	53	R5	ACCEPT	UDP	DNS_DNS	Networking
2024-06-03 10:12:33	172.16.10.12	-	33240	195.175.98.21	-	443	APP	LOG	TCP	TCP_TCP	Networking
2024-06-03 10:12:33	172.16.10.12	-	28272	172.16.10.1	-	53	R1	LOG	UDP	DNS_DNS	Networking
2024-06-03 10:12:33	172.16.10.12	-	28272	172.16.10.1	-	53	R5	ACCEPT	UDP	DNS_DNS	Networking
2024-06-03 10:12:33	172.16.10.12	-	33240	195.175.98.21	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:32	172.16.10.12	-	43554	195.175.98.21	-	443	R1	LOG	UDP	UDP_UDP	Networking
2024-06-03 10:12:32	172.16.10.12	-	30088	195.175.98.83	-	443	APP	LOG	TCP	TCP_TCP	Networking
2024-06-03 10:12:32	172.16.10.12	-	19850	172.16.10.1	-	53	R1	LOG	UDP	DNS_DNS	Networking
2024-06-03 10:12:32	172.16.10.12	-	19850	172.16.10.1	-	53	R5	ACCEPT	UDP	DNS_DNS	Networking
2024-06-03 10:12:32	172.16.10.12	-	13915	8.8.8.8	-	53	R1	LOG	UDP	DNS_DNS	Networking
2024-06-03 10:12:32	172.16.10.12	-	13915	8.8.8.8	-	53	R5	ACCEPT	UDP	DNS_DNS	Networking
2024-06-03 10:12:32	172.16.10.12	-	43554	195.175.98.21	-	443	R5	ACCEPT	UDP	UDP_UDP	Networking
2024-06-03 10:12:32	172.16.10.12	-	33240	195.175.98.21	-	443	R1	LOG	TCP	SSL_SSL	Web Services
2024-06-03 10:12:32	172.16.10.12	-	49265	195.175.196.18	-	443	R1	LOG	UDP	UDP_UDP	Networking
2024-06-03 10:12:32	172.16.10.12	-	60848	195.175.99.21	-	443	R5	ACCEPT	TCP	SSL_SSL	Web Services
2024-06-03 10:12:32	172.16.10.12	-	56915	195.175.99.146	-	443	R1	LOG	UDP	UDP_UDP	Networking
2024-06-03 10:12:32	172.16.10.12	-	56915	195.175.99.146	-	443	R5	ACCEPT	UDP	UDP_UDP	Networking
2024-06-03 10:12:32	172.16.10.12	-	60850	195.175.99.21	-	443	R1	LOG	TCP	SSL_SSL	Web Services

19.1.1.2 Web Filtre

Labris UTM cihazı tutulan web filtre kayıtları anlık olarak görüntülenir. Web Filtre kayıtlarının görüntülenmesi için NAT modülünde http veya https filtreleme kurallarının yazılması gerekmektedir. HTTPs filtreleme kuralı yazılması durumunda kullanıcıların ağ cihazlarına sertifika yüklenmesi gerekir.

Date / Time	User	Source	Mac Address	Destination	Domain	Decision	File Name	File Type	Category	Filter Group
2024-06-03 10:21:42	-	172.16.10.41	-	leasring	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:39	-	172.16.10.96	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:39	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:38	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:38	-	172.16.10.47	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:36	-	172.16.10.47	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:36	-	172.16.10.53	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:34	-	172.16.11.190	-	windowsupdate.com	-	ALLOWED	diskwecdnatf.cab	cab	-	Default
2024-06-03 10:21:33	-	172.16.10.50	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:33	-	172.16.10.50	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:33	-	172.16.11.190	-	windowsupdate.com	-	ALLOWED	diskwecdnatf.cab	cab	-	Default
2024-06-03 10:21:33	-	172.16.11.53	-	google.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:33	-	172.16.10.41	-	digicert.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:31	-	172.16.10.57	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:31	-	172.16.10.96	-	google.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:30	-	172.16.10.57	-	3.77.1.187	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:29	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:25	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:24	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:23	-	172.16.10.249	-	leasring	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:22	-	172.16.10.97	-	digicert.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:21	-	172.16.10.123	-	wordreference.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:20	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:20	-	172.16.11.198	-	whatsapp.net	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:20	-	172.16.10.123	-	wordreference.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:19	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:17	-	172.16.10.123	-	wordreference.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:17	-	172.16.10.192	-	microsoft.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:15	-	172.16.11.84	-	icofe.com	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:15	-	172.16.11.151	-	windowsupdate.com	-	ALLOWED	diskwecdnatf.cab	cab	-	Default
2024-06-03 10:21:15	-	172.16.10.47	-	3.76.113.134	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:14	-	172.16.11.123	-	whatsapp.net	-	ALLOWED	-	-	-	Default
2024-06-03 10:21:12	-	172.16.11.151	-	windowsupdate.com	-	ALLOWED	diskwecdnatf.cab	cab	-	Default
2024-06-03 10:21:12	-	172.16.11.123	-	windowsupdate.com	-	ALLOWED	diskwecdnatf.cab	cab	-	Default
2024-06-03 10:21:11	-	172.16.10.180	-	microsoft.com	-	ALLOWED	-	-	-	Default

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Kullanıcı	Web Filtre kayıtlarındaki kullanıcı bilgisi görüntülenir.

3	Kaynak	Web Filtre kayıtlarındaki kaynak IP bilgisinin görüntülenir.
4	Mac Adresi	Mac adres bilgisinin görüntülenir. Mac Adres bilgisi yok ise '-' işareti görüntülenir.
5	Hedef	Kayıttaki hedef IP bilgisi görüntülenir.
6	Domain	Kayıttaki domain adresi görüntülenir.
7	Karar	Kayıttaki karar bilgisi görüntülenir. Kararlar 'ALLOWED ve DENIED' şeklindedir.
8	Dosya İsmi	Web Filtre kaydındaki dosya isminin görüntülenir. Kayıttaki dosya ismi yoksa '-' şeklinde gösterilir.
9	Dosya Tipi	Web Filtre kaydındaki dosya tipi görüntülenir. Kayıttaki dosya tipi yoksa '-' şeklinde görüntülenir.
10	Kategori	Web Filtre kayıtlarındaki kategori tipi görüntülenir. Kayıttaki kategori tipi yoksa '-' şeklinde görüntülenir.
11	Filtre Grubu	Web Filtre modülünde oluşturulan Filtre grubunun görüntülediği bölümdür.
12	Filtre	Kayıtların filtrelediği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.
13	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
14	Sil	Tutulan logların silindiği bölümdür.

-Web Filtre kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek kaynak IP adresi, kullanıcı, domain, karar vb. bilgileri yazılarak filtreleme yapılır.



3	Mesaj	Servis kayıtlarının mesajı görüntülenir.
4	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.
5	Dışa Aktar	Tutulan logların dışarı aktarıldığı butondur. TXT ve CVS formatında loglar dışarı aktarılır.
6	Sil	Tutulan kayıtların temizlendiği butondur.

-Servis kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek tarih, host ismi ve mesaj bilgileri yazılarak filtreleme yapılır.



Date / Time	Host	Message
2024-06-04 08:58:02	localhost	labris-servant status
2024-06-04 08:56:03	localhost	labris-servant status
2024-06-04 08:54:03	localhost	labris-servant status
2024-06-04 08:52:02	localhost	labris-servant status
2024-06-04 08:50:03	localhost	labris-servant status
2024-06-04 08:48:03	localhost	labris-servant status
2024-06-04 08:46:02	localhost	labris-servant status
2024-06-04 08:44:02	localhost	labris-servant status
2024-06-04 08:42:03	localhost	labris-servant status
2024-06-04 08:40:03	localhost	labris-servant status
2024-06-04 08:38:02	localhost	labris-servant status
2024-06-04 08:36:03	localhost	labris-servant status
2024-06-04 08:34:02	localhost	labris-servant status
2024-06-04 08:32:03	localhost	labris-servant status
2024-06-04 08:30:06	localhost	labris-servant status
2024-06-04 08:28:02	localhost	labris-servant status
2024-06-04 08:26:02	localhost	labris-servant status
2024-06-04 08:24:03	localhost	labris-servant status
2024-06-04 08:22:03	localhost	labris-servant status
2024-06-04 08:20:03	localhost	labris-servant status
2024-06-04 08:18:02	localhost	labris-servant status
2024-06-04 08:16:02	localhost	labris-servant status
2024-06-04 08:14:02	localhost	labris-servant status
2024-06-04 08:12:03	localhost	labris-servant status
2024-06-04 08:10:03	localhost	labris-servant status
2024-06-04 08:08:03	localhost	labris-servant status
2024-06-04 08:06:03	localhost	labris-servant status
2024-06-04 08:04:03	localhost	labris-servant status
2024-06-04 08:02:02	localhost	labris-servant status
2024-06-04 08:00:06	localhost	labris-servant status
2024-06-04 07:58:02	localhost	labris-servant status
2024-06-04 07:56:03	localhost	labris-servant status
2024-06-04 07:54:03	localhost	labris-servant status
2024-06-04 07:52:02	localhost	labris-servant status
2024-06-04 07:50:03	localhost	labris-servant status

-Web filtre kayıtlarını indirmek için indirme butonuna basılır. İndirilecek dosya türü ve dosya ismi girilerek indirme işlemi yapılır.



Export

Export Type: TXT CSV

File Name:

Export

19.1.1.4 Yönetimsel

Labris UTM cihazı üzerindeki yönetimsel kayıtların görüntülenir. Web arayüzünde bağlanan kullanıcıların yaptıkları değişikliklerin kayıtları tutulur.

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Host	Labris UTM cihazının ismi görüntülenir.
3	Mesaj	Yönetimsel logların açıklaması görüntülenir.
4	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.

5	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
6	Sil	Tutulan logların silindiği butondur.

-Yönetimsel kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek tarih, host ismi ve mesaj bilgileri yazılarak filtreleme yapılır.



Date / Time	Host	Message
2024-06-04 09:56:39	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:39	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:38	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:37	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:37	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:37	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:35	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:35	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:34	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:33	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:33	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:33	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:32	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:32	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:29	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:29	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:27	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports/static/img/ddn.png, ...
2024-06-04 09:56:27	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:27	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports, method: POST, res...
2024-06-04 09:56:26	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports/static/img/up.png, m...
2024-06-04 09:56:26	localhost	LMC ACL - username: admin, ip: 178.251.45.176, user_id: 3242597576797267919, path: /logs_reports/static/img/ddn.png, ...

-Yönetimsel kayıtlarını indirmek için indirme butonuna basılır. İndirilecek dosya türü ve dosya ismi girilerek indirme işlemi yapılır.



Export

Export Type: TXT CSV

File Name:

Export

19.1.1.5 Wauth

WAUTH' a bağlanan kullanıcı ile ilgili kayıtlar görüntülenir.

Date / Time	Host	Facility	Action	Mac Address	User	User IP	IP
2024-06-04 09:44:56	localhost	wauth	User logged in	4C:CC:6A:0C:BE:D0		192.168.5.92	192.168.5.185
2024-06-04 09:40:17	localhost	wauth	User logged in	1C:6F:65:65:78:4D		192.168.2.45	192.168.0.185
2024-06-04 09:37:03	localhost	wauth	User logged in	F4:39:09:35:58:F5		192.168.2.193	192.168.0.185
2024-06-04 09:35:37	localhost	wauth	User logged out intentionally	4:c0cc:6a:32:f0:53		192.168.10.87	192.168.10.185
2024-06-04 09:33:56	localhost	wauth	User logged in	B4:85:2F:BB:0F:E7		192.168.2.137	192.168.0.185
2024-06-04 09:33:36	localhost	wauth	User logged in	B4:85:2F:BB:E3:57		192.168.2.182	192.168.0.185
2024-06-04 09:33:16	localhost	wauth	User logged in	B6:CA:3A:8C:79:93		192.168.2.78	192.168.0.185
2024-06-04 09:32:54	localhost	wauth	User logged in	C8:60:80:6A:2A:D4		192.168.2.95	192.168.0.185
2024-06-04 09:31:44	localhost	wauth	User logged in	1C:6F:65:66:9E:DB		192.168.5.93	192.168.5.185
2024-06-04 09:30:59	localhost	wauth	User logged out intentionally	b4:85:2f:bb:e6:6e		192.168.2.143	192.168.0.185
2024-06-04 09:28:47	localhost	wauth	User logged in	50:46:5D:4E:CB:C1		192.168.0.81	192.168.0.185
2024-06-04 09:26:53	localhost	wauth	User logged in	7C:57:58:36:FC:9C		192.168.0.93	192.168.0.185
2024-06-04 09:22:43	localhost	wauth	User logged in	50:46:5D:4D:1E:96		192.168.2.85	192.168.0.185
2024-06-04 09:22:12	localhost	wauth	User logged in	50:46:5D:4E:CC:1D		192.168.2.166	192.168.0.185
2024-06-04 09:18:51	localhost	wauth	User logged in	4C:CC:6A:0C:BF:66		192.168.5.72	192.168.5.185
2024-06-04 09:17:41	localhost	wauth	User logged in	BC:EE:7B:9E:74:D1		192.168.0.53	192.168.0.185
2024-06-04 09:13:57	localhost	wauth	User logged in	B8:CA:3A:8C:8C:CA		192.168.5.84	192.168.0.185
2024-06-04 09:13:33	localhost	wauth	User logged in	B8:CA:3A:8C:52:7A		192.168.2.93	192.168.0.185
2024-06-04 09:13:28	localhost	wauth	User logged in	50:46:5D:4C:8D:CA		192.168.2.220	192.168.0.185
2024-06-04 09:12:29	localhost	wauth	User logged in	B4:85:2F:BB:E2:D0		192.168.2.134	192.168.0.185
2024-06-04 09:10:49	localhost	wauth	User logged in	60:02:92:22:4F:98		192.168.0.82	192.168.0.185
2024-06-04 09:10:24	localhost	wauth	User logged in	A0:D3:C1:4D:50:04		192.168.2.109	192.168.0.185
2024-06-04 09:09:59	localhost	wauth	User logged in	74:D4:35:6D:59:23		192.168.2.54	192.168.0.185
2024-06-04 09:09:49	localhost	wauth	-	-		0.0.0.0	0.0.0.0
2024-06-04 09:08:57	localhost	wauth	User logged in	1C:87:2C:5A:F0:BA		192.168.2.53	192.168.0.185
2024-06-04 09:08:08	localhost	wauth	User logged in	18:60:24:71:DD:8D		192.168.2.21	192.168.0.185
2024-06-04 09:07:04	localhost	wauth	User logged out (auto deleted due to timeout)	60:02:92:22:4F:98		192.168.0.82	127.0.0.1
2024-06-04 09:06:06	localhost	wauth	User logged in	A0:D3:C1:4D:50:1A		192.168.2.49	192.168.0.185
2024-06-04 09:05:33	localhost	wauth	User logged in	F4:6D:04:94:3F:FF		192.168.2.242	192.168.0.185
2024-06-04 09:04:23	localhost	wauth	User logged in	A0:D3:C1:4D:4F:FD		192.168.2.68	192.168.0.185
2024-06-04 09:03:48	localhost	wauth	User logged in	60:02:92:21:91:65		192.168.2.171	192.168.0.185
2024-06-04 09:01:04	localhost	wauth	User logged in	00:50:9D:50:84:F6		192.168.2.190	192.168.0.185
2024-06-04 09:01:26	localhost	wauth	User logged in	6C:F0:49:E7:20:D5		192.168.10.38	192.168.10.185
2024-06-04 09:00:45	localhost	wauth	User logged in	F4:4D:30:86:61:9C		192.168.0.47	192.168.0.185
2024-06-04 08:59:13	localhost	wauth	User logged in	54:BE:F7:91:08:D7		192.168.0.50	192.168.0.185
2024-06-04 08:57:53	localhost	wauth	User logged in	60:02:92:21:4B:45		192.168.2.72	192.168.0.185
2024-06-04 08:57:18	localhost	wauth	User logged in	60:02:92:22:55:98		192.168.2.212	192.168.0.185

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Host	Labris UTM cihazının ismi görüntülenir.
3	Facality	Kayıdın tutulduğu modülü gösterir.
4	İşlem	Wauth'a bağlanan kullanıcının işlem bilgisi görüntülenir.
5	MAC Adresi	Wauth'a bağlanan kullanıcının MAC adres bilgisi görüntülenir.
6	Kullanıcı	Wauth'a bağlandığı kullanıcı adının görüntülediği bölümdür.
7	Kullanıcı IP	Wauth'a bağlanan kullanıcının IP adresinin görüntülediği bölümdür.
8	IP	Wauth'un açıldığı arabirim IP adresi görüntülenir.
9	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrenir.

10	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
11	Sil	Tutulan logların silindiği butondur.

19.1.1.6 Mail

Labris UTM cihazında mail kayıtlarının tutulduğu ve kayıtların görüntüldüğü bölümdür.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Date / Time	Host	Reason	Code	Recipient	Destination	Size	Sender	Duration	Hits	Source	Infection	Mail ID	Category
2024-06-04 10:18:01	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	106	0.0	-	-	5E4Y9A3Q9L3	clean
2024-06-04 10:14:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	117	0.0	-	-	ZPTTA-12u6	clean
2024-06-04 10:12:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	137	0.0	-	-	FS9aQY9dG	clean
2024-06-04 10:10:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	128	0.0	-	-	NB-8K9W9dQ	clean
2024-06-04 10:08:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	131	0.0	-	-	wC9Y9W9d5n	clean
2024-06-04 10:06:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	115	0.0	-	-	zMusKalerMg	clean
2024-06-04 10:04:03	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	134	0.0	-	-	X56nL3J3BK	clean
2024-06-04 10:02:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	121	0.0	-	-	JhD9GZvewk	clean
2024-06-04 10:00:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	175	0.0	-	-	VgTwiDEZuHl	clean
2024-06-04 09:58:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	122	0.0	-	-	RCrmb99zI	clean
2024-06-04 09:56:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	117	0.0	-	-	k8llyW9d9Yk	clean
2024-06-04 09:54:01	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	121	0.0	-	-	TeukWm69WQ	clean
2024-06-04 09:52:01	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	119	0.0	-	-	uzZQ9F01888	clean
2024-06-04 09:50:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	116	0.0	-	-	YNZ9uP9RnAI	clean
2024-06-04 09:48:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	121	0.0	-	-	map9U9d9E	clean
2024-06-04 09:46:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	111	0.0	-	-	J8514H7HAA6	clean
2024-06-04 09:44:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	108	0.0	-	-	FkZ-0869eyKy	clean
2024-06-04 09:42:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	123	0.0	-	-	IO9h4f-3Q9	clean
2024-06-04 09:40:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	127	0.0	-	-	BV7OH9Z9P2	clean
2024-06-04 09:38:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	124	0.0	-	-	M81-Qk9Wm9dM	clean
2024-06-04 09:36:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	116	0.0	-	-	Cv8Z6vT9m3p	clean
2024-06-04 09:34:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	115	0.0	-	-	XhD9e8P9d48	clean
2024-06-04 09:32:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	119	0.0	-	-	UCOR9w-9p9Hu	clean
2024-06-04 09:30:03	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	176	0.0	-	-	Y8u9H9d9dM	clean
2024-06-04 09:28:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	128	0.0	-	-	W9P9V9OR9WV	clean
2024-06-04 09:26:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	113	0.0	-	-	wV3Q9p06dED	clean
2024-06-04 09:24:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	117	0.0	-	-	I9d9T9e95C9	clean
2024-06-04 09:22:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	121	0.0	-	-	Z9-C9U9d9PQ	clean
2024-06-04 09:20:03	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	125	0.0	-	-	ZH9Z9Y7FA	clean
2024-06-04 09:18:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	123	0.0	-	-	u8C9J9e9dCI	clean
2024-06-04 09:16:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	131	0.0	-	-	H9G9E9h9n9C9	clean
2024-06-04 09:14:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	117	0.0	-	-	h9N9d9V9ew	clean
2024-06-04 09:12:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	134	0.0	-	-	99h9q9e9d8L	clean
2024-06-04 09:10:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	121	0.0	-	-	J9D939q979ep	clean
2024-06-04 09:08:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	129	0.0	-	-	AN9K-E9d9M9w9d	clean
2024-06-04 09:06:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	120	0.0	-	-	ngC9w9h9W9dM	clean
2024-06-04 09:04:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	115	0.0	-	-	9R9v9W9d9dR	clean
2024-06-04 09:02:02	localhost	-	0	noreply@labristeknoloji.com	-	581	sorun@labristeknoloji.com	123	0.0	-	-	9N9S9O9TER9h9a	clean

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Host	Labris UTM cihazının ismi görüntülenir.
3	Sebeup	Mail'in gönderilme sebebinin görüntüldüğü bölümdür.
4	Kod	Mail'in kodunun görüntüldüğü bölümdür.
5	Alıcı	Mail'in alıcı adresinin görüntüldüğü bölümdür.
6	Hedef	Mail hedef adresinin görüntüldüğü bölümdür.
7	Boyut	Mail boyutu görüntülenir.

8	Gönderen	Maili gönderen adres görüntülenir.
9	Süre	Mail gönderim süresi görüntülenir.
10	İsabet	Mail'in gönderim değeri görüntülenir.
11	Kaynak	Mailin kaynağı görüntülenir.
12	Infection	Mailin infection değeri görüntülenir
13	Mail Kodu	Mail kodu görüntülenir.
14	Kategori	Mail kategorisi görüntülenir.
15	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.
16	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
17	Sil	Tutulan logların silindiği butondur.

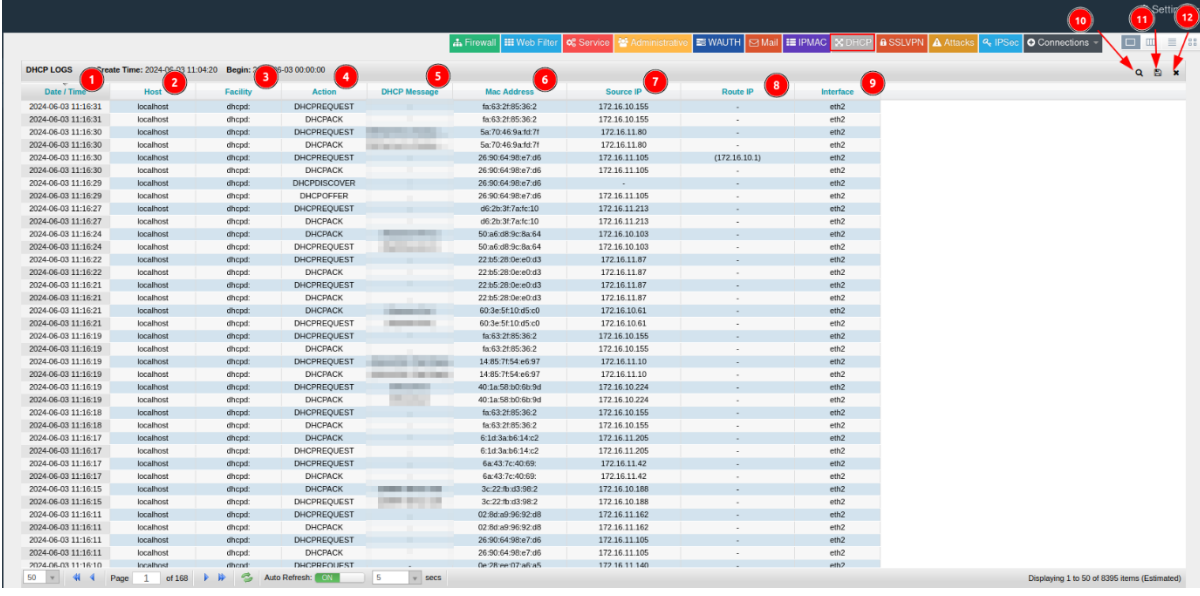
19.1.1.7 IPMAC

Labris UTM cihazında IPMAC kayıtları görüntülenir.



19.1.1.8 DHCP

Labris UTM cihazı DHCP sunucusu görevinde kullanılıyorsa DHCP kayıtları görüntülenir.



1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Host	Labris UTM cihazının ismi görüntülenir.
3	Facality	Kayıdın tutulduğu modülün görüntülenir.
4	İşlem	DHCP Kaydının işlem adımının görüntülediği bölümdür.
5	DHCP Mesajı	Kayıttaki DHCP mesajı görüntülenir.
6	MAC Adresi	DHCP isteği atan Mac adres görüntülenir.
7	Kaynak IP	DHCP'den IP alan IP adresi görüntülenir.
8	Yönlendirici IP	Yönlendirici IP adresi görüntülenir.

9	Arabirim	DHCP'nin çalıştığı arabirim görüntülenir.
10	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrelenir.
11	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
12	Sil	Tutulan logların silindiği bölümdür.

-DHCP kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek tarih, host ismi ve mesaj bilgileri yazılarak filtreleme yapılır.



Date / Time	Host	Facility	Action	DHCP Message	Mac Address	Source IP	Route IP	Interface
2024-06-04 11:12:02	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 11:12:02	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 11:09:59	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 11:09:59	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:39	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:39	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	(172.16.10.1)	eth2
2024-06-04 10:57:38	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:34	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:34	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:31	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:31	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:06	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:06	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:05	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:57:05	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:43	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:43	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:41	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:41	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:40	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:56:40	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:17:25	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:17:25	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:15:45	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:15:45	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:14:37	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	(172.16.10.1)	eth2
2024-06-04 10:14:37	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:14:36	localhost	dhcpd	DHCPREQUEST	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2
2024-06-04 10:14:36	localhost	dhcpd	DHCPACK	-	1a:e7:2a:1f:2e:1	172.16.11.67	-	eth2

-DHCP kayıtlarını indirmek için indirme butonuna basılır. İndirilecek dosya türü ve dosya ismi girilerek indirme işlemi yapılır.



Export

Export Type: TXT CSV

File Name:

Export

19.1.1.9 SSL VPN

SSLVPN'e bağlı olan kullanıcıların kayıtları görüntülenir.

1	2	3	4	5	6	7	8	9	10	11	12
Date / Time	Action	Username	Client IP	Remote IP	Sent Bytes	Received Bytes	Connect Date / Time	Disconnect Date / Time	Duration(sec)	Auth Type	Login
2024-06-04 08:10:33	client-connect		10.8.3.27				2024-06-04 08:10:32			user	Success
2024-06-04 07:48:21	client-connect		10.8.3.10				2024-06-04 07:48:20			user	Success
2024-06-04 07:47:25	client-connect		10.8.3.29				2024-06-04 07:47:24			user	Success
2024-06-04 07:29:26	client-connect		10.8.3.15				2024-06-04 07:29:25			user	Success
2024-06-04 07:09:12	client-disconnect		10.8.3.10		342866	192789	2024-06-04 06:43:53	2024-06-04 07:09:12	1519		
2024-06-04 07:02:30	client-disconnect		10.8.3.30		52959	97356	2024-06-04 06:23:51	2024-06-04 07:02:30	2319		
2024-06-04 06:55:00	client-connect		10.8.3.15				2024-06-04 06:54:59			user	Success
2024-06-04 06:43:55	client-connect		10.8.3.10				2024-06-04 06:43:53			user	Success
2024-06-04 06:23:52	client-connect		10.8.3.30				2024-06-04 06:23:51			user	Success
2024-06-04 06:01:50	client-connect		10.8.3.11				2024-06-04 06:01:46			user	Success
2024-06-04 05:51:38	client-disconnect		10.8.3.30		342969	371104	2024-06-04 04:25:15	2024-06-04 05:51:38	5183		
2024-06-04 05:46:15	client-connect		10.8.3.19				2024-06-04 05:46:13			user	Success
2024-06-04 05:44:59	client-connect		10.8.3.18				2024-06-04 05:44:58			user	Success
2024-06-04 05:34:00	client-connect		10.8.3.14				2024-06-04 05:33:58			user	Success
2024-06-04 05:11:48	client-connect		10.8.3.3				2024-06-04 05:11:47			user	Success
2024-06-04 05:06:01	client-connect		10.8.3.22				2024-06-04 05:06:00			user	Success
2024-06-04 05:05:38	client-connect		10.8.3.13				2024-06-04 05:05:37			user	Success
2024-06-04 05:03:55	client-connect		10.8.3.18				2024-06-04 05:03:54			user	Success
2024-06-04 04:25:15	client-connect		10.8.3.30				2024-06-04 04:25:15			user	Success

1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	İşlem	Tutulan kaydın işleminin görüntülediği bölümdür. İşlem olarak 'client-connected ve client-disconnect' dir.
3	Kullanıcı Adı	SSLVPN'e bağlanan kullanıcıların kullanıcı adları görüntülenir.
4	İstemci IP	SSLVPN'e bağlı olan kullanıcının IP adresini görüntülediği bölümdür. SSLVPN'e bağlandığında Labris UTM tarafından verilen IP adresleridir.
5	Uzak IP	SSLVPN'e bağlı olunan Genel IP adresleri görüntülenir.
6	Gönderilen Byte	SSLVPN bağlantısındaki gönderilen byte boyutu görüntülenir.
7	Alınan Byte	SSLVPN bağlantısındaki alınan byte boyutu görüntülenir.
8	Bağlanma Tarihi/Saati	SSLVPN'e bağlanma tarihi ve saati görüntülenir.
9	Bağlantıyı Kesme Tarihi/Saati	SSLVPN'den bağlantıyı kesme tarihi ve saati görüntülenir
10	Bağlı Kalınan	SSLVPN'e bağlı kalınan süre görüntülenir.

	Süre	
11	Giriş Yapma Tipi	SSLVPN'e giriş yapan kullanıcıların giriş yapma türü görüntülenir.
12	Giriş	SSLVPN'e bağlantısında giriş kaydının tutulduğu bölümdür.

-SSLVPN kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek tarih, host ismi ve mesaj bilgileri yazılarak filtreleme yapılır.



Date / Time	Action	Username	Client IP	Remote IP	Sent Bytes	Received Bytes	Connect Date / Time	Disconnect Date / Time	Duration(sec)	Auth Type	Login
2024-06-04 08:40:41	client-connect		10.8.3.13				2024-06-04 08:40:40			user	Success
2024-06-04 08:37:24	client-connect		10.8.3.31				2024-06-04 08:37:23			user	Success
2024-06-04 08:10:33	client-connect		10.8.3.27				2024-06-04 08:10:32			user	Success
2024-06-04 07:48:31	client-connect		10.8.3.10				2024-06-04 07:48:30			user	Success
2024-06-04 07:47:25	client-connect		10.8.3.29				2024-06-04 07:47:24			user	Success
2024-06-04 07:20:26	client-connect		10.8.3.5				2024-06-04 07:20:25			user	Success
2024-06-04 06:55:00	client-connect		10.8.3.15				2024-06-04 06:54:59			user	Success
2024-06-04 06:43:55	client-connect		10.8.3.10				2024-06-04 06:43:53			user	Success
2024-06-04 06:23:52	client-connect		10.8.3.30				2024-06-04 06:23:51			user	Success
2024-06-04 06:01:50	client-connect		10.8.3.11				2024-06-04 06:01:46			user	Success
2024-06-04 05:46:15	client-connect		10.8.3.19				2024-06-04 05:46:13			user	Success
2024-06-04 05:44:59	client-connect		10.8.3.8				2024-06-04 05:44:58			user	Success
2024-06-04 05:34:00	client-connect		10.8.3.14				2024-06-04 05:33:58			user	Success
2024-06-04 05:11:48	client-connect		10.8.3.3				2024-06-04 05:11:47			user	Success
2024-06-04 05:06:01	client-connect		10.8.3.22				2024-06-04 05:06:00			user	Success
2024-06-04 05:05:38	client-connect		10.8.3.13				2024-06-04 05:05:37			user	Success
2024-06-04 05:03:55	client-connect		10.8.3.18				2024-06-04 05:03:54			user	Success
2024-06-04 04:25:15	client-connect		10.8.3.30				2024-06-04 04:25:15			user	Success

-SSLVPN kayıtlarını indirmek için indirme butonuna basılır. İndirilecek dosya türü ve dosya ismi girilerek indirme işlemi yapılır.



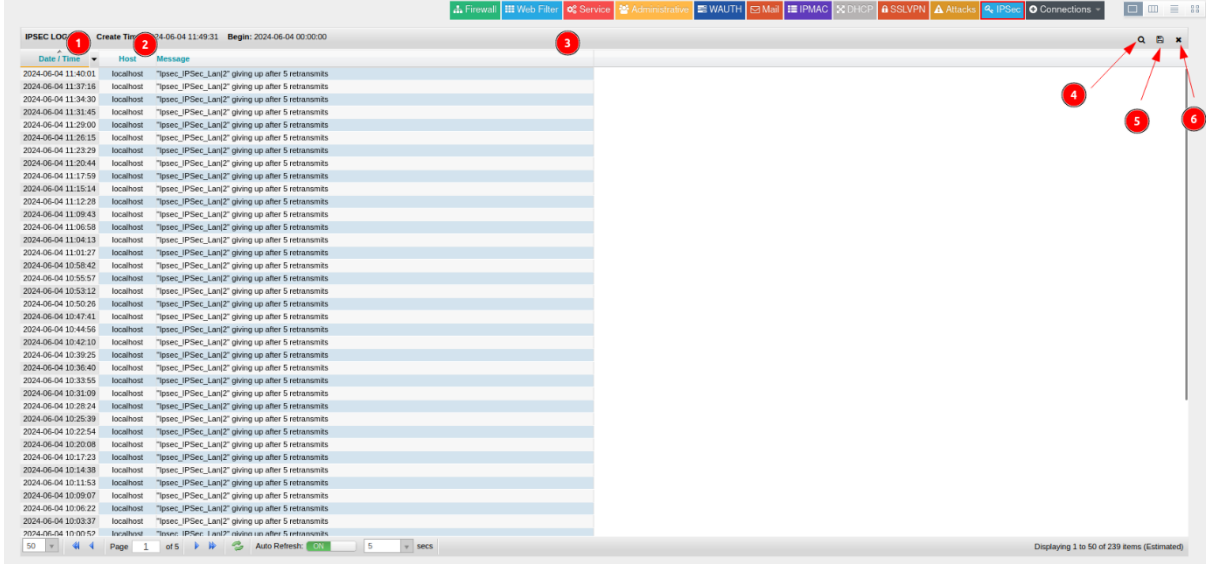
Export

Export Type: TXT CSV

File Name:

19.1.1.10 IPsec

Labris UTM cihazı üzerinde tutulan IPsec kayıtları görüntülenir.



1	Tarih/Zaman	Kayıdın tutulduğu tarih ve saat görüntülenir.
2	Host	Labris UTM cihazının ismi görüntülenir.
3	Mesaj	IPsec logların açıklaması görüntülenir.
4	Filtre	Kayıtların filtrelendiği bölümdür. Filtrelemek istenilen bölüme filtrelemek istenilen değer yazılarak filtrenir.
5	Dışa Aktar	Tutulan logların dışarı aktarıldığı bölümdür. TXT ve CVS formatında loglar dışarı aktarılır.
6	Sil	Tutulan logların silindiği butondur.

-IPSec kayıtlarını filtrelemek için filtreleme butonuna tıklanır. Filtrelenecek tarih, host ismi ve mesaj bilgileri yazılarak filtreleme yapılır.



Date / Time	Host	Message
2024-06-04 11:40:01	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:37:16	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:34:30	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:31:45	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:29:00	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:26:15	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:23:29	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:20:44	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:17:59	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:15:14	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:12:28	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:09:43	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:06:58	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:04:13	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 11:01:27	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:58:42	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:55:57	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:53:12	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:50:26	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:47:41	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:44:56	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:42:10	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:39:25	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:36:40	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:33:55	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:31:09	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:28:24	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:25:39	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:22:54	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:20:08	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:17:23	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:14:38	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:11:53	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:09:07	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits
2024-06-04 10:06:22	localhost	"Ipsec_IPSec_Lan[2]" giving up after 5 retransmits

-IPSec kayıtlarını indirmek için indirme butonuna basılır. İndirilecek dosya türü ve dosya ismi girilerek indirme işlemi yapılır.



Export

Export Type: TXT CSV

File Name:

Export

19.1.1.11 Bağlantı

Labris UTM cihazında tutulan bağlantı logları görüntülenir. Cihaza gelen trafikteki gelen ve giden paketlerin detayları bulunur.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Date / Time	Start Time	End Time	Duration	Source	Destination	Application	Category	Protocol	Source Port	Destination Port	Transmitted Pa...	Received Pack...	Transmitted B...	Received Bytes
2024-06-04 12:57:56	2024-06-04 12:57:36	2024-06-04 12:57:56	20	172.16.106.123	213.74.1.3	DNS_DNS	Networking	UDP	63686	53	1	1	63	189
2024-06-04 12:57:56	2024-06-04 12:57:36	2024-06-04 12:57:56	20	192.0.2.254	8.8.4.4	0x30000000		UDP	53433	53	1	1	84	84
2024-06-04 12:57:56	2024-06-04 12:57:36	2024-06-04 12:57:56	20	172.16.106.123	213.74.1.3	DNS_DNS	Networking	UDP	65252	53	1	1	69	395
2024-06-04 12:57:56	2024-06-04 12:57:36	2024-06-04 12:57:56	20	192.0.2.254	8.8.4.4	0x30000000		UDP	59054	53	1	1	84	84
2024-06-04 12:57:56	2024-06-04 12:57:36	2024-06-04 12:57:56	20	192.0.2.254	8.8.4.4	0x30000000		UDP	40969	53	1	1	76	195
2024-06-04 12:57:55	2024-06-04 12:57:34	2024-06-04 12:57:55	21	172.16.106.94	161.117.98.205	XIAOMI_Xiaomi	Web Services	TCP	41110	443	19	11	2738	6913
2024-06-04 12:57:55	2024-06-04 12:57:03	2024-06-04 12:57:55	52	172.16.106.108	77.92.138.118	BLOOMBERGHT_Bo...	Web Services	TCP	52754	443	16	18	2984	7127
2024-06-04 12:57:55	2024-06-04 12:56:45	2024-06-04 12:57:55	70	192.168.5.56	2.22.248.8	MICROSOFT_Microsof...	Web Services	TCP	59236	443	10	11	969	7536
2024-06-04 12:57:55	2024-06-04 12:57:38	2024-06-04 12:57:55	17	172.16.106.94	8.219.159.97	SSL_SSL	Web Services	TCP	51154	443	12	10	1721	5222
2024-06-04 12:57:55	2024-06-04 12:54:50	2024-06-04 12:57:55	185	172.16.106.49	8.8.4.4	UDP_UDP	Networking	UDP	51663	443	15	15	5397	6276
2024-06-04 12:57:55	2024-06-04 12:57:35	2024-06-04 12:57:55	20	172.16.106.189	213.74.0.3	DNS_DNS	Networking	UDP	52298	53	1	1	79	157
2024-06-04 12:57:55	2024-06-04 12:57:35	2024-06-04 12:57:55	20	172.16.106.189	213.74.0.3	DNS_DNS	Networking	UDP	53496	53	1	1	79	95
2024-06-04 12:57:54	2024-06-04 12:57:13	2024-06-04 12:57:54	41	172.16.106.111	17.8.136.52	APPLE_Apple	Networking	TCP	65348	443	15	13	2010	4605
2024-06-04 12:57:54	2024-06-04 12:57:44	2024-06-04 12:57:54	10	172.16.106.127	172.16.106.1	KCMP_KCMP	Network Monitoring	KCMP	53134	443	1	1	84	84
2024-06-04 12:57:54	2024-06-04 12:57:34	2024-06-04 12:57:54	20	172.16.106.123	213.74.1.3	DNS_DNS	Networking	UDP	63916	53	1	1	64	115
2024-06-04 12:57:54	2024-06-04 12:57:34	2024-06-04 12:57:54	20	172.16.106.94	213.74.1.3	DNS_DNS	Networking	UDP	24782	53	1	1	73	89
2024-06-04 12:57:54	2024-06-04 12:57:34	2024-06-04 12:57:54	20	172.16.106.132	213.74.1.3	DNS_DNS	Networking	UDP	59580	53	1	1	60	76
2024-06-04 12:57:54	2024-06-04 12:57:34	2024-06-04 12:57:54	20	172.16.106.132	213.74.0.3	DNS_DNS	Networking	UDP	47135	53	1	1	60	76
2024-06-04 12:57:54	2024-06-04 12:56:22	2024-06-04 12:57:54	332	172.16.106.104	142.251.140.34	GOOGLE_Google...	Web Services	TCP	53134	443	23	97	3785	2884
2024-06-04 12:57:54	2024-06-04 12:57:34	2024-06-04 12:57:54	20	172.16.106.94	213.74.1.3	DNS_DNS	Networking	UDP	32242	53	1	1	72	362
2024-06-04 12:57:53	2024-06-04 12:57:29	2024-06-04 12:57:53	24	172.16.106.161	172.16.106.255	0x20000000		UDP	138	138	3	0	606	0
2024-06-04 12:57:53	2024-06-04 12:57:12	2024-06-04 12:57:53	41	172.16.106.111	17.253.73.207	SSL_SSL	Web Services	TCP	65344	443	13	12	1570	5354
2024-06-04 12:57:53	2024-06-04 12:57:33	2024-06-04 12:57:53	20	172.16.106.216	213.74.0.3	DNS_DNS	Networking	UDP	65373	53	1	1	61	121
2024-06-04 12:57:53	2024-06-04 12:57:33	2024-06-04 12:57:53	20	172.16.106.216	213.74.0.3	DNS_DNS	Networking	UDP	56039	53	1	1	61	77
2024-06-04 12:57:53	2024-06-04 12:57:43	2024-06-04 12:57:53	10	172.16.106.188	46.31.149.220	SSL_SSL	Web Services	TCP	55812	443	13	12	3281	9068
2024-06-04 12:57:53	2024-06-04 12:57:43	2024-06-04 12:57:53	10	172.16.106.188	46.31.149.220	SSL_SSL	Web Services	TCP	55811	443	12	12	3187	9068
2024-06-04 12:57:53	2024-06-04 12:52:21	2024-06-04 12:57:53	332	172.16.106.104	142.250.187.162	SSL_SSL	Web Services	TCP	45462	443	22	109	3174	23763
2024-06-04 12:57:53	2024-06-04 12:57:33	2024-06-04 12:57:53	20	172.16.106.187	213.74.1.3	DNS_DNS	Networking	UDP	63159	53	1	1	90	345
2024-06-04 12:57:53	2024-06-04 12:57:33	2024-06-04 12:57:53	20	172.16.106.187	213.74.0.3	DNS_DNS	Networking	UDP	63159	53	1	1	90	348
2024-06-04 12:57:53	2024-06-04 12:57:13	2024-06-04 12:57:53	40	172.16.106.111	17.8.136.52	APPLE_Apple	Networking	TCP	65346	443	15	12	2002	4595
2024-06-04 12:57:53	2024-06-04 12:57:43	2024-06-04 12:57:53	10	192.168.5.169	157.240.238.61	WHATSAPP_WhatsApp	Messaging	TCP	51839	5222	20	24	1990	3308
2024-06-04 12:57:52	2024-06-04 12:23:33	2024-06-04 12:57:52	2059	172.16.106.32	46.31.149.220	SSL_SSL	Web Services	TCP	56617	443	147	147	14801	24662
2024-06-04 12:57:52	2024-06-04 12:56:41	2024-06-04 12:57:52	71	192.0.2.254	104.18.20.226	0x30000000		TCP	40613	80	6	4	730	2123
2024-06-04 12:57:52	2024-06-04 12:56:41	2024-06-04 12:57:52	71	192.0.2.254	104.18.20.226	0x30000000		TCP	40614	80	6	4	731	2134
2024-06-04 12:57:52	2024-06-04 12:56:41	2024-06-04 12:57:52	71	192.0.2.254	104.18.20.226	0x30000000		TCP	40615	80	6	4	731	2134
2024-06-04 12:57:52	2024-06-04 12:56:41	2024-06-04 12:57:52	71	192.0.2.254	104.18.20.226	0x30000000		TCP	40616	80	6	4	730	2123
2024-06-04 12:57:52	2024-06-04 12:56:48	2024-06-04 12:57:52	184	172.16.106.221	916.68.919.14	UDP_UDP	Networking	UDP	57683	443	20	20	11118	11612

1	Tarih/Zaman	Kaydın tutulduğu tarih ve saat görüntülenir.
2	Başlanma Zamanı	Bağlantının kurulma başlama zamanının görüntülenir.
3	Bitiş Zamanı	Bağlantının bitiş zamanı görüntülenir.
4	Süre	Bağlantı süresinin görüntülediği bölümdür.
5	Kaynak	Kaynak IP bilgisinin görüntülediği bölümdür.
6	Hedef	Hedef IP bilgisinin görüntülediği bölümdür.
7	Uygulama	Bağlantı kaydındaki uygulama türlerinin görüntülenir.
8	Kategori	Bağlantı kaydındaki kategori türleri görüntülenir.
9	Protokol	Bağlantı kaydındaki protokol türü görüntülenir.
10	Kaynak Port	Kaynak Port bilgisi görüntülenir.

11	Hedef Port	Hedef Port bilgisi görüntülenir.
12	Alınan Paket	Bağlantıdaki alınan paket boyutu görüntülenir.
13	Gönderilen Paket	Bağlantıdaki gönderilen paket boyutu görüntülenir.
14	Alınan Byte	Bağlantıdaki alınan byte boyutu görüntülenir.
15	Gönderilen Byte	Bağlantıdaki gönderilen byte boyutu görüntülenir.

19.1.2 Arşiv

Labris UTM cihazında arşivlenen kayıt dosyalarında kayıt sorgulaması yapılır. Seçilen kayıt türüne göre arşivden kayıtlar gösterilir.

Date / Time	Start Time	End Time	Duration	Source	Destination	Application	Category	Protocol	Source Port	Destination Port	Transmitted Pa...	Received Pack...	Transmitted B...	Received Bytes
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	56054	53	1	1	86	152
2024-06-04 13:56:47	2024-06-04 13:56:26	2024-06-04 13:56:47	21	172.16.11.20	192.167.249.29	NTPDATA_InData	Web Servers	TCP	55309	443	14	13	6041	2209
2024-06-04 13:56:47	2024-06-04 13:56:26	2024-06-04 13:56:47	21	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	34754	53	1	1	96	230
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	49224	53	1	1	72	396
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	51394	53	1	1	64	264
2024-06-04 13:56:47	2024-06-04 13:56:37	2024-06-04 13:56:47	10	172.16.10.235	142.250.167.131	PSIPHON_Pushon	Proxy	TCP	51606	80	5	5	495	498
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	37270	53	1	1	79	238
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	57340	53	1	1	81	145
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.76	172.16.10.1	DNS_DNS	Networking	UDP	54568	53	1	1	85	223
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	62282	53	1	1	77	215
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	30997	53	1	1	95	188
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.89	172.16.10.1	DNS_DNS	Networking	UDP	34321	53	1	1	61	622
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.76	172.16.10.1	DNS_DNS	Networking	UDP	56748	53	1	1	72	396
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	40094	53	1	1	69	404
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	42252	53	1	1	80	238
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	53078	53	1	1	83	136
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	54090	53	1	1	77	345
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	54968	53	1	1	69	260
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	31565	53	1	1	80	152
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	54388	53	1	1	77	215
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	53765	53	1	1	86	194
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.76	172.16.10.1	DNS_DNS	Networking	UDP	62885	53	1	1	77	345
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.76	172.16.10.1	DNS_DNS	Networking	UDP	56550	53	1	1	78	343
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	51152	53	1	1	77	435
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	50503	53	1	1	78	343
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	64525	53	1	1	73	537
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	61711	53	1	1	75	402
2024-06-04 13:56:47	2024-06-04 13:56:35	2024-06-04 13:56:47	12	172.16.10.210	17.249.236.86	KLOOK_Cloud	File Transfer	TCP	58802	443	77	60	91047	11429
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.76	172.16.10.1	DNS_DNS	Networking	UDP	60788	53	1	1	81	239
2024-06-04 13:56:47	2024-06-04 13:53:47	2024-06-04 13:56:47	180	172.16.10.79	216.58.212.35	UDP_UDP	Networking	UDP	57126	443	16	18	4516	5606
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	1052	53	1	1	88	154
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	61844	53	1	1	73	255
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	58590	53	1	1	70	405
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.185	172.16.10.1	DNS_DNS	Networking	UDP	64101	53	1	1	77	143
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	59229	53	1	1	73	213
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	172.16.11.82	172.16.10.1	DNS_DNS	Networking	UDP	52345	53	1	1	92	422
2024-06-04 13:56:47	2024-06-04 13:56:27	2024-06-04 13:56:47	20	192.0.2.254	8.8.8.8	0x00000000	Networking	UDP	51629	53	1	1	79	177

-Arşiv'e tıklandığında gelen ekrandaki alınması istenilen kayıt seçilerek arşivden istenilen kayıtlar gelmektedir.

The screenshot shows the 'Table' configuration page in the Labris UTM management interface. It is divided into several sections:

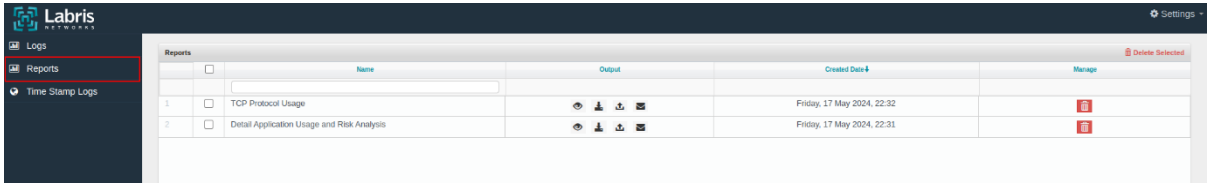
- 1 Select Log Source:** A list of log sources with radio buttons. 'Firewall Logs' is selected.
- 2 Select Log Fields:** A list of log fields with checkboxes. 'Date / Time', 'Source', 'Source User', 'Destination User', 'Action', 'Protocol', 'Application', 'Category', 'Mac Address', 'Host', 'Message', 'Sequence Number', 'Type', 'TTL', 'Packet ID', 'Urgent Pointer', 'Outbound Interface', 'Ack Number', 'Inbound Interface', 'Precision', 'Window Size', 'TCP Flag', 'Packet Length', and 'SID' are checked.
- 3 Default Ranges:** A dropdown menu showing '1 day', '3 days', and '1 week'.
- 4 From:** A text input field containing '2024-06-01 13:48:01'.
- 5 To:** A text input field containing '2024-06-04 13:48:01'.
- 6 CREATE TABLE:** A green button.
- 7 Exit:** A red button.

1	Log Kaynağını Seç	Log kaynağının seçildiği bölümdür. Labris UTM cihazında tutulan kayıt kaynaklarından seçilir.
2	Log Alanlarını Seç	Seçilen log kaynağına göre değişiklik gösterir.
3	Standart Zaman Aralıkları	Labris UTM cihazında standart olarak zaman aralıklarıdır.
4	Başlangıç(Tarih)	Arşivden alınan kaydın başlangıç tarihi seçilir.

5	Bitiş(Tarih)	Arşivden alınan kaydın bitiş tarihi seçilir.
6	Tabloyu Oluştur	Seçilen değerlere göre tablonun oluşturulduğu butondur.
7	Çıkış	Arşiv'e tıklanarak açılan ekranın kapatıldığı butondur.

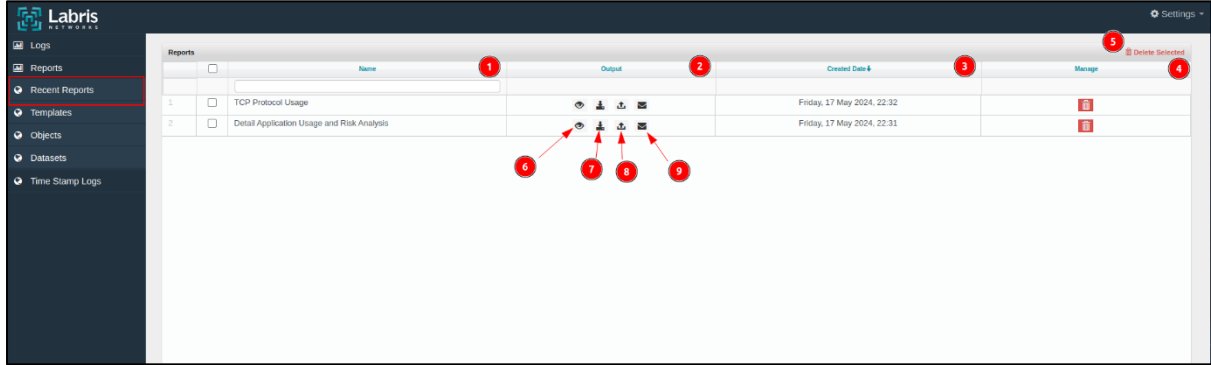
19.2 Raporlar

Labris UTM cihazında tutulan kayıtlar üzerinde raporların oluşturulduğu bölümdür.



19.2.1 Alınan Raporlar

Raporlar modülünde alınan raporların görüntülediği, indirildiği, alınan raporların FTP sunucusuna veya mail yoluyla gönderildiği bölümdür.



1	İsim	Alınan raportlarının isimleri görüntülenir.
2	Çıktı	Alınan raporların indirildiği, görüntülediği, FTP sunucusuna gönderildiği ve mail olarak iletildiği bölümdür.
3	Oluşturulma Tarihi	Raporun oluşturulma tarihinin görüntülenir.
4	Yönet	Alınan raporun silindiği bölümdür.

5	Seçilenleri Sil	Seçilen raporların silindiği bölümdür.
6	Görüntüle	Alınan raporun görüntülediği bölümdür.
7	İndir	Oluşturulan raporun indirildiği bölümdür.
8	Gönder	Oluşturulan rapor FTP sunucusuna gönderilir.
9	Mail Sunucusuna Gönder	Oluşturulan raporun Mail sunucusuna gönderilir.

19.2.2 Şablonlar

Labris UTM cihazında varsayılan olarak gelen şablonlardan kayıt raporları oluşturulur.

ID	Name	Category	Type	Created Date	Reports	Manage
1	236	All Prevented Attacks Against Specific User	IPS Report Templates	Predefined	Friday, 1 December 2017, 12:00	
2	206	All Prevented Attacks From Specific User	IPS Report Templates	Predefined	Friday, 1 December 2017, 12:00	
3	38	Allowed And Blocked Applications	Application Report Templates	Predefined	Friday, 1 December 2017, 12:00	
4	46	Apple Applications Usage	Application Report Templates	Predefined	Friday, 1 December 2017, 12:00	
5	47	Application Bandwidth Usage	Application Report Templates	Predefined	Friday, 1 December 2017, 12:00	
6	245	Attacks of Last 24 Hours	Attack Report Templates	Predefined	Tuesday, 21 June 2022, 12:00	
7	39	Category Based Bandwidth Usage	Application Report Templates	Predefined	Friday, 1 December 2017, 12:00	
8	1	Detail Application Usage and Risk Analysis	Detail Analysis Report Templates	Predefined	Friday, 1 December 2017, 12:00	
9	55	Detail Logs for Firewall	Firewall Report Templates	Predefined	Friday, 1 December 2017, 12:00	
10	249	Detected Attacks From Specific Category	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
11	251	Detected Attacks From Specific Date	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
12	247	Detected Attacks From Specific Destination IP	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
13	248	Detected Attacks From Specific Protocol	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
14	250	Detected Attacks From Specific Signature ID	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
15	246	Detected Attacks From Specific Source IP	Attack Report Templates	Predefined	Tuesday, 5 July 2022, 12:00	
16	26	Downloaded Files Report	Web Report Templates	Predefined	Friday, 1 December 2017, 12:00	
17	2	Email Report	Detail Analysis Report Templates	Predefined	Friday, 1 December 2017, 12:00	
18	7	Filtering Policy Overview	Web Report Templates	Predefined	Friday, 1 December 2017, 12:00	
19	41	(Same, Applications, Icons)	Application Report Templates	Predefined	Friday, 1 December 2017, 12:00	

1	ID	Şablonların ID numarasının görüntülediği bölümdür.
2	İsim	Şablonların isminin görüntülediği bölümdür.
3	Kategori	Şablonların kategori tiplerinin görüntülediği bölümdür.
4	Tip	Şablonların tipinin görüntülediği bölümdür.
5	Oluşturulma	Şablonun oluşturulma tarihinin görüntülediği

	Tarihi	bölümdür.
6	Raporla	Şablona bağlı olarak raporun oluşturulduğu, şablonun oluşturulduğu rapor tablosu ve oluşturulan son raporun görüntülediği bölümdür.
7	Yönet	Oluşturulan Şablonların kopyalandığı veya silindiği bölümdür.
8	Oluştur	Şablon oluşturma işleminin yapıldığı butondur.
9	Rapor Tablosunda Görüntüle	Şablonu raport tablosunda görüntülenir.
10	Rapor Oluştur	Şablona bağlı olarak rapor oluşturulur.
11	Oluşturulan Son Raporu Görüntüle	Şablondaki oluşturulan son raporun görüntülediği bölümdür.

-Şablon eklemek için 'oluştur' butonuna tıklanır.

The screenshot shows the 'Create New Report Template' interface. It includes a header with a hamburger menu icon and the title 'Create New Report Template'. Below the header, there are several input fields and buttons, each marked with a red circle and a number from 1 to 12. The fields are: 'Template Name' (1) with the value 'labrisrapor', 'Description' (2) with a text area and 'Max. 500 character' note, 'Date Filter' (3) with a checkbox, 'Output Format' (4) with a dropdown set to 'PDF', 'Template Category' (5) with a dropdown set to 'User Defined', 'Report Language' (6) with a dropdown set to 'English', 'Object List' (7) with a dropdown set to 'Session History Graph of User Web Usage' and an 'Add Obj' button, 'Schedule Settings' (8), 'Email Settings' (9), and 'FTP Settings' (10). At the bottom, there are 'Create Template' (11) and 'Exit' (12) buttons.

1	Şablon İsmi	Şablona verilecek ismin girildiği bölümdür.
2	Açıklama	Şablona dair açıklamanın girildiği bölümdür.
3	Tarih Filtresi	Şablona tarih filtresinin girildiği butondur.
4	Şablon Kategorisi	Şablonun kategorisinin seçildiği bölümdür.
5	Rapor Dili	Şablona ait rapor dilinin seçildiği bölümdür.
6	Obje Listesi	Obje modülünde eklenen veya varsayılan olarak bulunana objelerin seçildiği bölümdür.
7	Tarih Ayarları	Şablona tarih filtresi uygulandığı bölümdür.

8	Email Ayarları	Eklenecek şablonun mail sunucusuna gönderildiği bölümdür. Bu bölümde mail konusu, mail gönderilecek adres ve mesaj girilir.
9	FTP Ayarları	Eklenecek Şablonun FTP sunucusuna gönderildiği bölümdür. Bu bölümde FTP sunucusunun bulunduğu IP adresi, FTP Sunucusundaki kullanıcı adı ve şifre bilgisi ve FTP sunucusundaki izin bilgileri girilir.
10	Şablonu Oluştur	Şablona bağlı olarak rapor oluşturulur.
11	Kapat	'ekle' butonuna tıkladıktan sonra gelen ekranın kapatıldığı butondur.

19.2.3 Objeler

Labris UTM cihazında varsayılan olarak gelen objelerden kayıt raporları oluşturulur. Eklenecek objeler şablonlarda kullanılır.

ID	Name	Object Type	Dataset	Type	Created Date	Length	Manage
22	Allowed Requests Summary	Line Chart	ACCESS ALLOWED	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
315	Attack Prevention History Graph	Line Chart	NETWORK IPS	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
328	Attack Prevention History Graph of Destination IPs	Line Chart	NETWORK IPS	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
368	Attack Prevention History Graph of Destination Users	Line Chart	NETWORK IPS USER	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
325	Attack Prevention History Graph of Source IPs	Line Chart	NETWORK IPS	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
319	Attack Prevention History Graph of Source Users	Line Chart	NETWORK IPS USER	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
364	Attack Prevention History Graph of User	Line Chart	NETWORK IPS USER	Prefdefined	Friday, 1 December 2017, 12:00	20	[Manage]
394	Attacks by Priority	Pie Chart	ATTACKS	Prefdefined	Tuesday, 21 June 2022, 12:00	20	[Manage]
395	Attacks by Protocol	Pie Chart	ATTACKS	Prefdefined	Tuesday, 21 June 2022, 12:00	20	[Manage]
129	Before Queue Rejected Mails	Grid	MAIL REJECT	Prefdefined	Friday, 1 December 2017, 12:00	200	[Manage]
28	Blocked Request Summary	Line Chart	ACCESS DENIED	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
25	Browsing Time Summary	Line Chart	ACCESS	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
16	Database Applications Session History	Line Chart	CONNECTION DATABASE	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
113	Destination Ip Session History Graph	Line Chart	CONNECTION TRACK	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
406	Detected Attacks Details	Grid	ATTACKS	Prefdefined	Tuesday, 21 June 2022, 12:00	10000	[Manage]
10	E-mail Applications Session History	Line Chart	CONNECTION MAIL	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
19	File Sharing Applications Session History	Line Chart	CONNECTION FILE SHARING	Prefdefined	Friday, 1 December 2017, 12:00	-	[Manage]
47	Filter Policy Group Allowed Count	Grid	ACCESS ALLOWED	Prefdefined	Friday, 1 December 2017, 12:00	50	[Manage]
48	Filter Policy Group Denied Count	Grid	ACCESS DENIED	Prefdefined	Friday, 1 December 2017, 12:00	50	[Manage]
168	Firewall Logs With Time Stamp	Grid	NETWORK ALL	Prefdefined	Friday, 1 December 2017, 12:00	200	[Manage]

1	ID	Varolan objenin ID'si görüntülenir.
2	İsim	Objenin isminin görüntülediği bölümdür.
3	Obje Tipi	Objenin tipinin görüntülediği bölümdür.
4	Veri Seti	Objenin veri seti görüntülenir.

5	Tip	Obje tipi görüntülenir.
6	Oluşturma Tarihi	Objenin oluşturma tarihinin görüntülediği bölümdür.
7	Uzunluk	Objenin içeriğinin uzunluğu görüntülenir.
8	Yönet	Objenin kopyalandığı veya silindiği bölümdür.
9	Oluştur	Objenin oluşturulduğu butondur.

-Objeye eklemek için **'oluştur'** butonuna tıklanır.

1	Objeye İsmi	Eklenecek objenin isminin girildiği bölümdür.
2	Veri Seti	Objenin veri setinin seçilir.
3	Tip	Objenin oluşturulma tipi belirtilir. Tip seçimine göre oluşturulacak obje değişiklik gösterecektir.
4	Objeye Oluştur	Girilen değerlere göre objenin oluşturulduğu butondur.
5	Çıkış	'oluştur' butonuna tıklandıktan sonra açılan ekranın kapatıldığı butondur.

19.3.4 Veri Setleri

Obje oluştururken kullanılacak veri setlerinin oluşturulduğu modüldür. Labris UTM cihazında varsayılan olarak veri setleri bulunur.

ID	Name	Source	Type	Period	Created Date	Order by	Manage
17	ACCESS	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
18	ACCESS ALLOWED	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
23	ACCESS CATEGORY	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
19	ACCESS DENIED	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
41	ACCESS FILE NAME	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
42	ACCESS FILE TYPE	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
24	ACCESS SEARCH ENGINE	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
40	ACCESS VIRUS	access	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
30	APPLICATION ACCEPT	network	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
29	APPLICATION DROP	network	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
150	ATTACKS	attacks	Preddefined	This Week	Tuesday, 21 June 2022, 12:00	Date / Time	[C] [D]
15	CONNECTION DATABASE	conntrack	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
16	CONNECTION FILE SHARING	conntrack	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
13	CONNECTION MAIL	conntrack	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]
10	CONNECTION PROXY	conntrack	Preddefined	This Week	Friday, 1 December 2017, 12:00	Date / Time	[C] [D]

1	ID	Veri seti ID'sinin görüntülediği bölümdür.
2	İsim	Verisetlerinin isminin görüntülediği bölümdür.
3	Kaynak	Verisetinin kaynak bilgisinin görüntülediği bölümdür.
4	Tip	Verisetinin tipinin görüntülediği bölümdür.
5	Periyod	Verisetinin periyod bilgisi görüntülenir.
6	Oluşturulma Tarihi	Verisetinin oluşturma tarihi görüntülenir.
7	Sırala	Verisetinin sıralama türünün görüntülediği bölümdür.
8	Yönet	Verisetinin kopyalandığı ve oluşturulan verisetinin silindiği bölümdür.
9	Oluştur	Verisetinin oluşturulduğu butondur.

-Veriseti oluşturmak için **'oluştur'** butonuna tıklanır.

1	Veriseti İsmi	Verisetinin isminin girildiği bölümdür.
2	Kaynak	Verisetinin kaynağının seçildiği bölümdür. Labris UTM cihazında tutulan kayıtlarından veriseti oluşturmak istenilen seçilir.
3	Periyod	Oluşturulacak verisetinin periyodu seçilir.
4	Sıralama	Oluşturulacak verisetinin sıralama tipi seçilir.
5	Filter	Verisetinin filtrelendiği bölümdür.
6	Kural	Verisetinin kuralının yazıldığı bölümdür.
7	Verisetini Oluştur	Verisetinin oluşturulduğu butondur.
8	Çıkış	'oluştur' butonuna tıklandıktan sonra açılan ekranın kapatıldığı butondur.

19.3 Zaman Damgalı Kayıtlar

Labris UTM cihazında tutulan kayıtların zaman damgalı olarak tutulduğu bölümdür.

1	Tarih	Zaman Damgalı olarak tutulan kayıtların tarihinin görüntülendiği bölümdür.
2	Hash	Zaman Damgalı kayıtların hashının görüntülendiği bölümdür.
3	Yönet	Zaman Damgalı kayıtların indirildiği bölümdür.