Yeni Nesil Ağ Güvenliği

Labris UTM Serisi

Özelleşen İşinize, **Tam İhtiyacınız Olan Çözüm...**

Labris UTM, iş yapma biçiminize uyum sağlayacak esnekliği sunarken, sizi, gerekmeyen modülleri, donanımları almak zorunda bırakmaz. İşletmenizin mevcut ihtiyacı neyse onu alır ve yapınıza en uygun şekilde kullanırsınız.

Labris yeni nesil uygulama tanıma, merkezi kullanıcı dizini, IP itibar ağı, SMS'le misafir yetkilendirme, cihaza bütünleşik loglama ve raporlama, dağıtık cihazların izlenmesi, merkez politikaların uç cihazlarda uygulanması gibi sektörün ihtiyaç duyduğu konularda öncü duruşunu sürdürmektedir.

CWL Cyber Warfare Lab

Labris UTM ürün altyapısında kullanılan gelişmiş teknoloji ve güncel kritik savunma önlemleri, **Cyber Warfare Lab**'da, riskleri iyi tanıyan, yaratıcı bir ekip tarafından geliştirilmiştir.

CSS Close Security Support

Labris, teknolojik olarak gelişmiş özellikler sunmanın yanında, size bir çözüm ortaklığı da vaad eder. Kullanıcıların yakınında, onların isteklerine ve ihtiyaçlarına duyarlı bir ürün ve süreç yönetimi uygular. Bu kapsamda onların ihtiyaçlarına uygun SLA paketleri sunar.

EAL4+

Common Criteria (Ortak Kriterler) kritik güvenliğe sahip ağlarda kullanılan ürünler için düzenlenmiş dünyanın ortak kriteri, **ISO** standardıdır. Labris Networks **EAL4+** seviyesinde üretim yapan, dünyanın sayılı, Türkiye'nin tek ağ geçidi firmasıdır.

Labris® NETWORKS

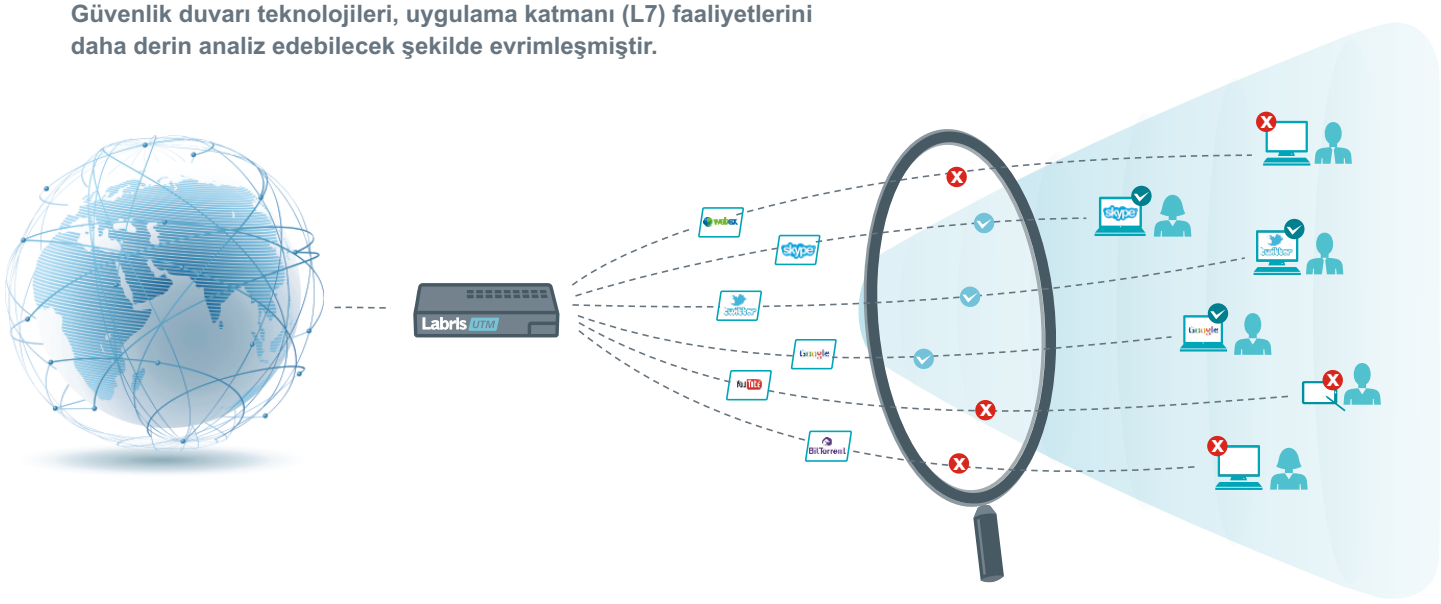
Yeni Nesil Firewall: Labris UTM

Labris UTM cihazları, güçlü ve sürekli geliştirilen uygulama kontrolü motoru ve merkezi kullanıcı dizini ile ağınız üzerinde üst düzey, kullanıcı bazlı hakimiyet sağlar.

Uygulama Kontrolü (2000+ Uygulama İmzası)

Internet ve intranet trafikleri, uygulamaların kullanıldığı portlara göre ayrıştırılamamaktadır. Bu durum uygulamalar üzerinde bir kontrol kurmak için port bağımsız uygulama tanıma teknolojilerinin gelişmesine yol açmıştır.

Güvenlik duvarı teknolojileri, uygulama katmanı (L7) faaliyetlerini daha derin analiz edebilecek şekilde evrimleşmiştir.



Uygulama Bileşenlerinde Hakimiyet

Uygulama İmza Kategorileri (15+)

Kullanılan derin paket ve akış inceleme (DPI) teknolojileri sayesinde, uygulamalar, uygulama fonksiyonları ve hatta uygulama içinde yer alan uygulama parçacıkları üzerinde hakimiyet kurarak, güvenlik duvarı politikalarında bu bilgilerden yararlanmak mümkündür.

- Collaboration
- Database
- File Transfer
- Games
- Messaging
- Network
- Monitoring
- Networking
- Proxy
- Remote Access
- Social Networking
- Streaming Media
- VPN and Tunneling
- Web Services
- Mail
- Others

Merkezi Kullanıcı Dizini

Yeni nesil güvenlik cihazlarının bir gereksinimi de gerekli olabilecek kullanıcı bilgisini dış sistemlerden sorgulayabilmek, bu bilgileri cihaz içi bir merkezi yetkilendirme sistemi kapsamında tek noktadan kullanabilmek ve uygulama veya uygulama parçacıklarını bu kullanıcı bilgisiyle kontrol altına alabilmektir.

Bu sayede güvenlik duvarı, web filtre ve benzeri bütünleşik uygulamaların loglarını da kullanıcı tabanlı görebilmek münkün olabilmektedir.

Kullanıcı Bilgileri Toplayan Dizin Modülleri

- **Kayıt Masası Modülü**
- **Aktif Dizin Entegrasyonu Modülü**
- **SMS Yetkilendirme ***
  - SMS Deposu **
  - Mobil Ödeme
  - Harici SMS Depo Entegrasyonu
- **Otel Yönetim Yazılımı Entegrasyonu ***
- **Kurumsal Uygulamalarla Entegrasyon Gereksinimleri ***

* Seçenek ** SMS yetkilendirme fonksiyonlarını kullanabilmek için ek bir sözleşmeye ya da prosedüre ihtiyaç yoktur.

Merkezi Kullanıcı Dizini Uygulama Örnekleri

Güvenlik Duvarı, Routing, Bandwidth Yönetimi, SSL VPN Client

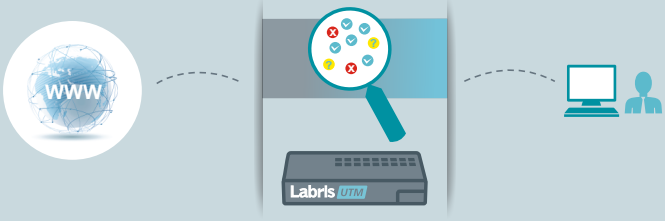
Birçok kaynaktan bir araya getirilerek oluşturulan merkezi kullanıcı dizini, isterseniz güvenlik duvarı ve routing kuralları içinde, isterseniz bandwidth yönetimi sırasında, isterseniz SSL VPN istemcilerin yetkilendirmesinde kullanabilirsiniz.

Bu sayede cep telefonundan SMS ile şifre almış bir kullanıcı için cep telefonu numarası kullanılarak güvenlik duvarı kuralı yazmak gibi daha önce düşünülemeyecek yetenekler sunulmaktadır.

Wauth+ Modulü (Hot Spot ve Ağ Yetkilendirme)

Labris UTM ve **Labris LOG** cihazlarında kullanılan **Labris Wauth+** modülü ile kullanıcılara hot spot yetkilendirmesi yapılabilmektedir. Merkezi kullanıcı dizini sayesinde SMS, Otel yazılımı gibi entegrasyonlar yanında, cihazın aktif dizin, LDAP gibi entegrasyonlar sonucu edindiği kullanıcı bilgileri de kullanılabilmektedir.
Bu sayede bu modül bir hotspot olmasının yanında iç ağların yetkilendirme ihtiyaçlarını da karşılayan bir **Ağ Yetkilendirme** uygulaması özelliğine de kavuşmuştur.

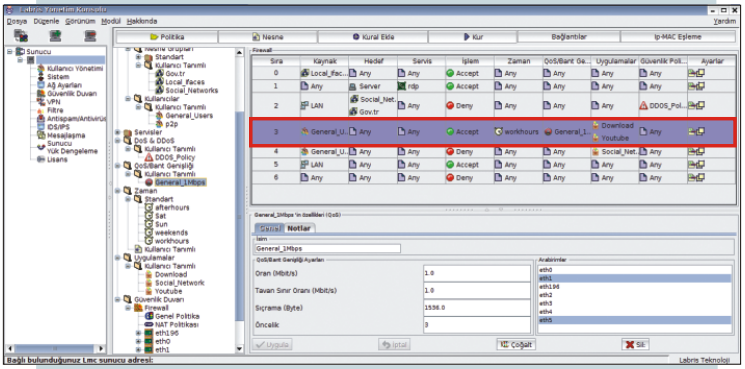
Labris Web Filtre



Labris Web Filtre içinde oluşturulan kullanıcı grupları içinde bu dizinde yer alan kullanıcılar ve kullanıcı gruplarının kullanılması mümkündür. Bu sayede web filtre politikaları oluşturulurken birçok yöntemle elde edilmiş kullanıcılar temel alınabilmektedir.

Firewall "Güvenlik Politika Nesneleri"

Firewall kuralları bazlı Güvenlik Politika (Security Policy) Nesneleri kullanılabilmektedir. Bu nesneler uygulama imzaları gibi önceden hazırlanmış olarak firewall kurallarında kullanılacak şekilde bekler.
İstenmesi halinde yeni nesneler de oluşturulabilmektedir.



En önemli kullanım alanı, belirlenmiş trafiklerde **DDOS ve benzeri anormalliklerin Firewall tarafından tespiti için terzi işi, çok önemli bir altyapı sağlamasıdır.**

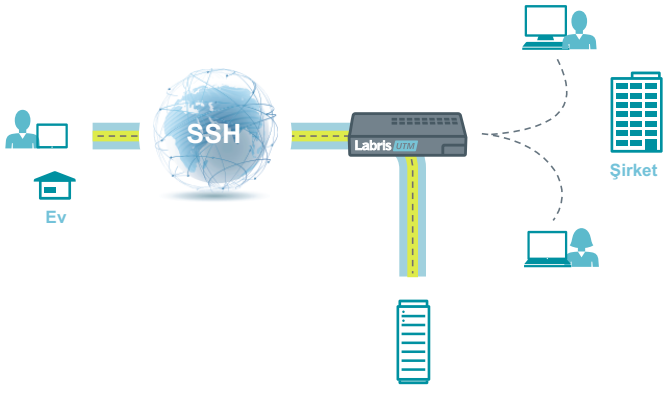
Örnek olarak; "A'dan B'ye giden trafiğin saniyede X kadar paketten fazla olmaması veya saniyede Y kadar SYN paketinden fazla olmaması" şeklinde hazırlanacak **Güvenlik Politika Nesneleri**, firewall kurallarında tanımlanabilmektedir.

SSH Denetim Motoru

SSH trafikleri üzerinden ağınızı tehdit edebilecek girişimleri engelleyebilmeniz için bir tanımlama ve engelleme altyapısı oluşturur.

SSH trafiklerinin kullanım alanları:

- Cihaz yönetim trafikleri
- SFTP/SCP ile dosya transferleri
- Tünelleme ile ileri-geri tüneller
- HTTP trafiğini tünelleme

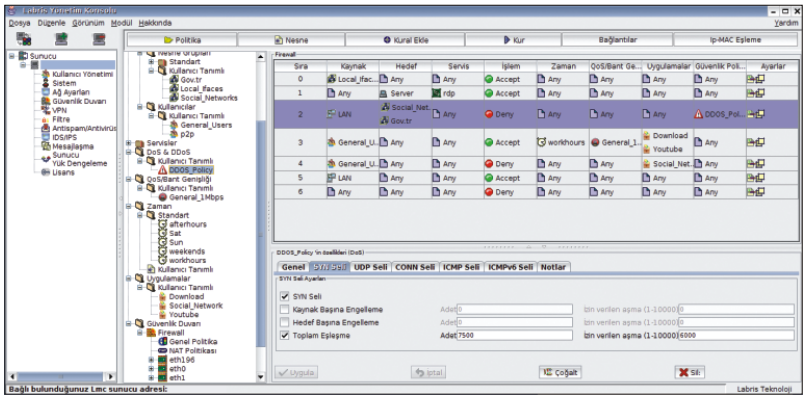


Güvenli ve Yedekli Erişim Yönetimi

- Labris UTM cihazları, dağıtık topolojilerde ve çoklu hatlarda güvenli ve yedekli erişim konfigürasyonları uygulayabilmenize olanak sağlar.

Bant Genişliği Yönetim Kıstasları

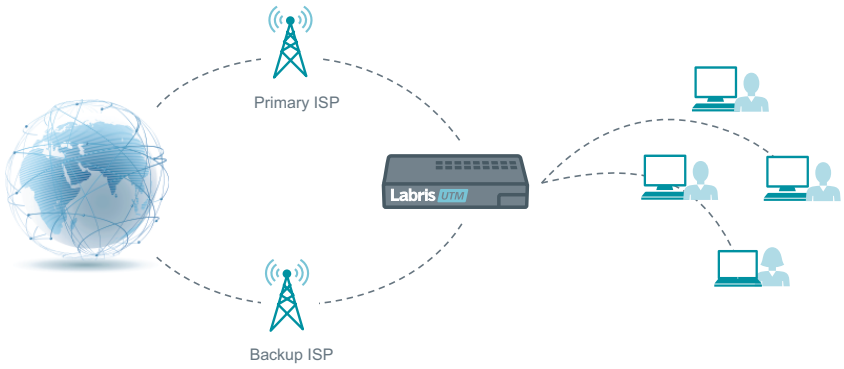
Bant Genişliği Yönetimi, Güvenlik Duvarı politika oluşturma ekranında yapılmaktadır. Bir firewall kuralında düşünülebilecek tüm bileşenler, kural koşulu olarak da kullanılabilmektedir.



Kim	Ne	Nereden	Nereye	Ne zaman
Kullanıcı* Kullanıcı Grubu*	Uygulamalar	Kaynak IP Kaynak Ağ	Hedef IP Hedef Ağ Port	Zaman Aralığı Tekrarlama Sıklığı Zaman sınırsız

* **Merkezi Kullanıcı Dizini**'nde seçilebilmektedir.

WAN / VPN Yedekleme



Gateway VPN Yedekliliği

Labris UTM cihazları tarafından yönetilen birden fazla internet hattı üzerinde, yedekli VPN bağlantıları tanımlanabilmektedir.

Bu bağlantılar üzerinde kurum politikaları uygulanabilmektedir. Bir hat koptuğunda "bağlantı ve VPN diğer hattan devam etsin" biçiminde düzenlemeler mümkün olabilmektedir.

- **Labris UTM** serisi cihazların tüm portları LAN/ WAN için kullanılabilir, bağımsız ethernet çipine sahiptir; switch ile çoklanmamıştır.
- **Labris UTM cihazlarının** USB portları 3G Modemler takıldığında otomatik olarak bir internet yolu olarak tanımlanmaktadır. Bu çıkışlar kurumların ihtiyacı çerçevesinde yedek acil durum hattı veya destek uzak erişim hattı olarak kullanılabilmektedir.
- **Labris UTM** cihazları birden fazla adette ve tipte internet bağlantısını ayrı portlarda veya switchle birleştirerek tek bir hat gibi kullandırabilmektedir.

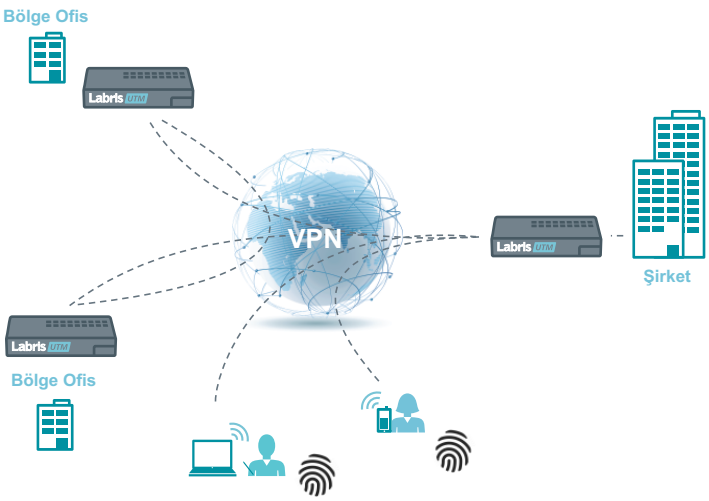
Çok Çıkışlı 3G Router Modu

Birden fazla 3G USB modemi yedekli ve koordineli biçimde kullanabilme

- 3G modemleri ayrı ayrı yönetebilme
- Modemleri gruplayabilme
- Yedekli çalıştırabilme

Güvenli Uzak İletişim (VPN / SSL VPN)

VPN teknolojileri, uzak kullanıcıların ve bölgelerin merkeze ve birbirlerine güvenli, şifrelenmiş yollardan erişebilmeleri için kullanılmaktadır. **Labris UTM** VPN özellikleri uluslararası standartlara tam uyumlu olup, farklı marka cihazlarla, yüksek trafiklerde uyumlu şekilde konumlanabilmektedir.



SSL VPN Client Yazılımı Kullanıcıların merkez ağa kurum dışından güvenli şekilde ulaşabilmesi için SSL VPN Client yazılımları kullanılmaktadır.	
Desteklenen İşletim Sistemleri	Windows, Linux, iPhone, Android, MacOS
Yetkilendirme Metodları	Merkezi Kullanıcı Dizini tarafından desteklenen tüm metodlar

E-İmza / Mobil İmza

E-İmza / Mobil İmza Entegrasyonu

E-imza ve mobil imza servisleri Merkezi Kullanıcı Dizini ile entegre çalışabilmektedir. Bu sayede dizinde, dolayısıyla cihazlar üzerindeki tüm uygulamalarda bu yetkilendirme metodlarıyla gelen kullanıcıları kullanabilmek, yönetebilmek mümkün olmuştur.

Labris WAUTH+ (Hotspot ve Ağ Yetkilendirme)

- Ağ bileşenlerinden bağımsız olarak, yetkilendirme yapılacak ağ bölümlerini belirleyebilme
- WAN üzerinden çalışarak uzak bölgelerdeki kullanıcıları merkezden yetkilendirebilme
- Kullanıcı ve ağ bazlı politika belirleyebilme

- Kurum kablosuz ağlarından SMS ile izinsiz internet kullanımını engellemek için Ortak Anahtar özelliği
- Süre kotası belirleyebilme
- Zaman aşımı süresi belirleyebilme
- İnternet tarayıcısı diline göre değişen Türkçe ve İngilizce arayüz desteği
- Özelleştirilebilir “Hoşgeldiniz” sayfası
- Kullanıcı için “Çıkış Yap” seçeneği

- SMS kullanımı için ek bir prosedüre gerek olmadan kontör yükleyebilme
- Kullanıcıları arama motoru
- Aktif bağlantıların izlenmesi, istenilen kullanıcı bağlantılarının kesilebilmesi
- T.C. 5651 ve e-imza kanunlarına uygun loglama

Misafir Yetkilendirme (Hot Spot)

Labris WAUTH+, pazardaki hotspot çözümlerinden farklıdır. Bu işi güvenliğin önemli bir parçası olarak ele alır ve her çeşit internet ağına entegre edilebilecek kapsamlı çözümler önerir.

- **Labris WAUTH+**, her kurumun misafir kullanıcı türü ve misafir yetkilendirme senaryosuna uygun çözümler sunar.

İmza Veritabanı

Labris sensor ağları, uluslararası açık ve lisanslı kaynaklar, yerel ekipler ve tarama robotları ile ürünlere bütünleşik veritabanları sürekli güncel ve verimli tutulmaktadır.

Anormallik tespit yöntemlerinin sürekli gelişmesine rağmen, güvenlik uygulamalarında sürekli güncellenen veritabanlarına ihtiyaç her zamankinden daha fazladır.

Bu veritabanlarıyla anormallik motorlarının daha az yükle çalışması sağlanırken, yerel bir bakışla ürünün verimliliği ve performansı, kurum/toplum davranışlarına uyumluluğu çok üst düzeylere çıkarılabilmektedir.

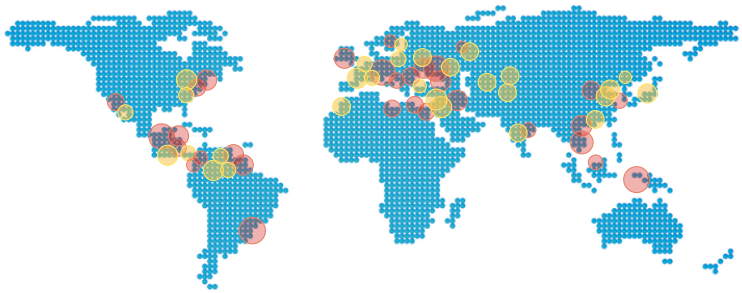
Spam Sensor Network

Bir noktadan başlayan çok hedefli zararlı yayılımların tespitinin, henüz cihazlara ulaşmadan yapılabilmesi önemlidir. Her bir cihazın anormallik yöntemleri ile tek başına karar vermesi sırasında elinde olmayan en önemli bilgi, bu trafiğin başka hangi hedeflere hangi sıklıkla yollandığıdır.

Yaygın şekilde konumlandırılan sensör ağı ile, kötü yayılımların kaynağının IP bilgisi yanında trafikle ilgili imza bilgisi de elde edilmekte ve hemen cihazlara dağıtılmaktadır.

IP İtibar Ağı (2000+ Nokta)

Labris Networks, sahip olduğu kurulu cihazlar ve sensör ağları ile yaygın ve kritik önemde ağlarda yoğun incelemeler yapmaktadır. Bu çalışmalar **Labris Networks**'ün güvenlik olayları araştırma merkezi olan **Cyber Warfare Lab** tarafından teknolojik altyapıya veya imzaya dönüştürülerek cihazlara dağıtılmaktadır.



Yerele inen itibar ağı	Sadece ISP'lerde değil, 50 kullanıcılı ağlara kadar uzanan IP itibar (reputation) ağı
IP belirleme için zararlı trafik inceleme	Spam, virus, kötü amaçlı yazılım yayılımı, açık proxy gibi zararlı trafikleri inceleme
IP Arşiv Verileri	Yıllara dayanan IP itibar (reputation) veritabanı

Standard İmza Sayıları

Firewall Uygulama : **2.000 +**
Uygulama Kategori: **15 +**
URL: **3 Milyon +**
URL Kategori: **85+ (18 adet TR)**
IPS : **9.000**

Ek Abonelik Seçenekleri

Web Filtre + Veritabanı Üyeliği
URL: **500 Milyon +**
Web Sayfası: **6 Milyar +**
Kategori: **150 +**
IPS+ Veritabanı Üyeliği
Dahili İmza : **20.000 +**
Kategori : **74 +**

Türkiye Özel

18 adet Türkiye özel URL Veritabanı Kategorisi

Türkiye'deki web sayfalarını çok detaylı şekilde 18 başlıkta inceleyen bir veritabanı ürünlere bütünleşik ve ücretsiz olarak sunulmaktadır.

T.C. URL Veritabanları Entegrasyonu

T.C. devlet kurumları tarafından kategorilendirilmiş, kullanımına izin verilen veritabanlarından ürün dahilinde yararlanılabilmektedir. İstendiğinde, bu kategoriler açılıp kapatılabilmektedir.

Loglama

Labris UTM ürünleri, dahili ve uzak loglama yetenekleriyle donatılmıştır. Cihazlar büyüklüklerine göre 8GB'tan 3TB'a kadar dahili log alanlarına sahiptir. Ek bir tedbire, yatırıma, cihaz ve yazılıma gerek olmadan ağ geçidinde tüm log saklama ve kanuni uyumluluk işlemleri gerçekleştirilmektedir.

Yedekli Loglama

Birden fazla loglama diskine sahip olan Labris UTM 62 ve üstü cihazlarda dahili logların RAID 1 yedekliliği sağlanabilmektedir.

Kanunlara Uygun Log Saklama

Bir logun değiştirilmediği logun zaman damgası ile damgalanarak saklanması ile ispat edilebilir. Labris ürünlerinde T.C. e-imza kanununda yetkilendirilmiş Türktrust tarafından üretilen nitelikli zaman damgası kullanılmaktadır.

Zaman Damgası Kullanım Sıklığı

Labris ürünlerinde ön tanımlı zaman damgası kullanım sıklığı, seçenek olarak sıklaştırılabilmekte, gereksinim halinde kurum ağında yer alan e-imza sertifika sunucusu kullanılabilmektedir.

Uzak Loglama

Labris UTM ürünleri cihaz loglarını, oluşması sırasında farklı yöntemlerle uzak bir noktaya gönderebilir.

Labris LOG Ürünlerine Uzak Loglama

Uzak Loglama bölümünde belirtilen tüm özelliklerle Labris UTM logları cihaza bağlı veya uzakta konumlandırılmış Labris LOG ürünlerine uzak loglama yapabilmektedir.

SIEM Ürünlerine Uzak Loglama

Ürün ailesinde oluşturulan loglar uluslararası standartlarda, SIEM ürünleri tarafından okunabilir ve korele edilebilir şekilde üretilmektedir. Loglar SIEM ürünlerine Syslog, ftp ve benzeri yöntemlerle aktarılabilmektedir.

Güvenli Loglama

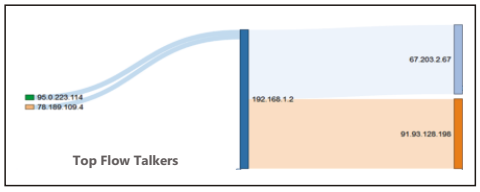
Logun ilk yazıldığı yerde saklanması, logun delil niteliğinin bozulmamasında ilk adımdır. Bu sayede logun yeniden yazılması sırasında logun değiştirilmediğinin ispatı ve logun yazılacağı yerle cihaz arasındaki bağlantının güvenliği, logun aktarıldığı donanımın fiziksel risk altında olması gibi konuların irdelenmesine gerek kalmaz.

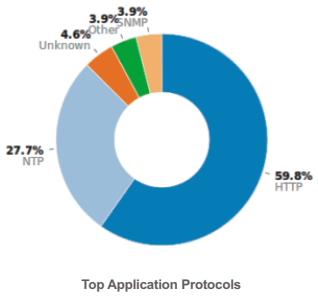
Log Yaşam Döngüsü

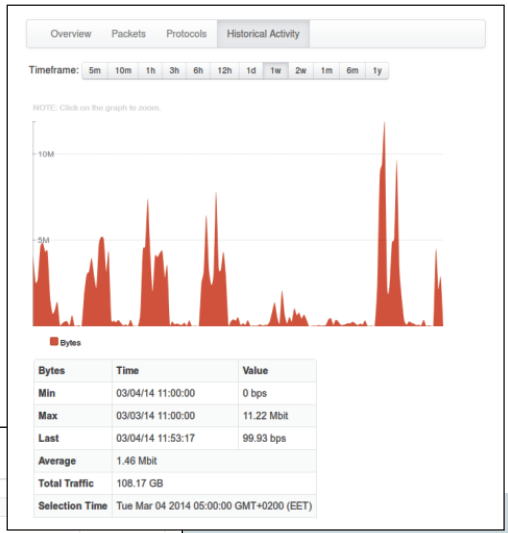
Dahili olarak tutulan loglar, yaşam döngüsü işlemleri kapsamında dahili log alanının büyüklüğüyle uyumlu olarak biriktirilir, uygun disk tiplerinde arşivlenir.

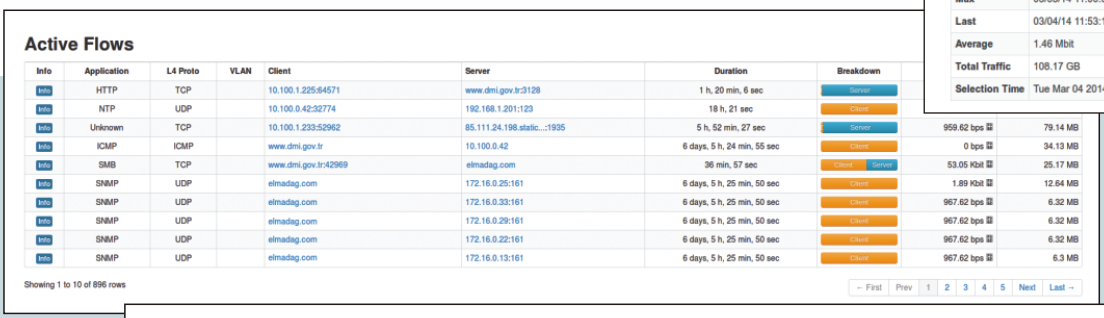
Anlık İzleme

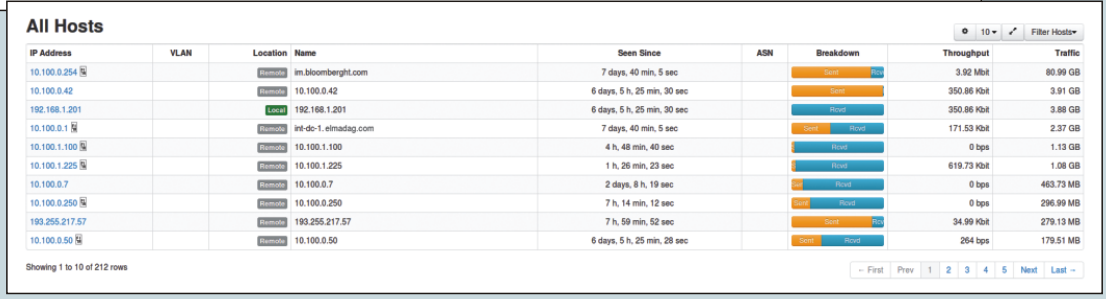
Anlık İzleme Modülü, mevcut trafiğinizin görsel analizini gerçek zamanlı olarak yapar.





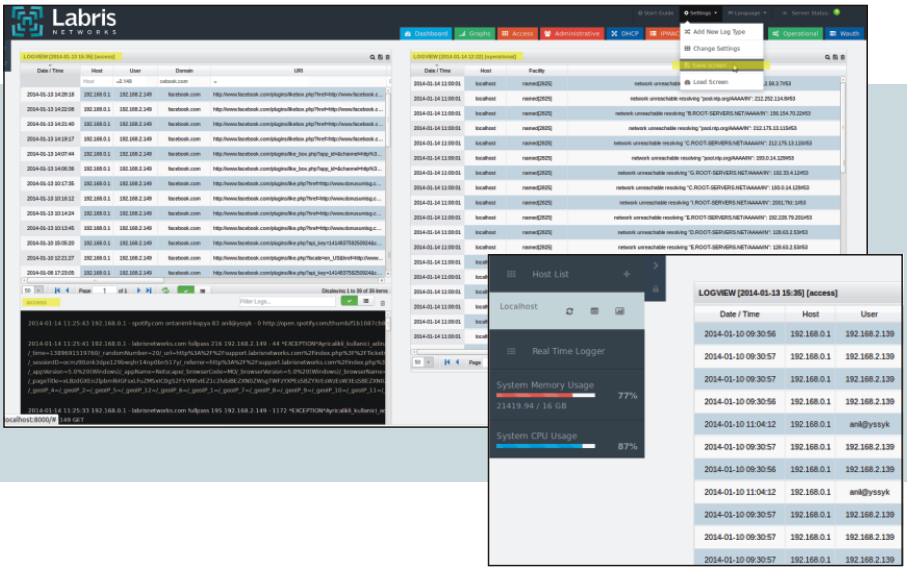






Log View

İzlenebilecek Log Tipleri	- Operasyonel Loglar - Güvenlik Duvarı (Firewall) Logları - UTM Fonksiyon Logları
Yönetim	- Anlık İzleme - Hiyerarşik Filtreleme - Birden fazla cihaz tanımlayabilme - Web tabanlı hızlı yönetim
Raporlama Formatları	PDF, XML, HTML, XLS, CSV



Entegre Raporlama

Cihazlar üzerinde toplanan loglar yine cihazlara bütünleşik entegre raporlama modülüyle grafiksel, idari yöneticilerin de kolaylıkla anlayabileceği, hızlı bir analiz aracı sunmaktadır.

Web Genel Görünüm

- Web Filtre Genel Görünüm
- WWW Trafiğinin Karakteristiği
- Filtreleme Politika İstatistikleri
- Risk Haritası

Anlık Raporlar

- Son Yarım Saat
- Anlık Kullanıcılar
- Anlık Siteler
- Anlık Adresler
- Anlık Engellenen Kategoriler

Web Kullanıcı Takibi

- Kullanıcı Web Erişim Özeti
- Kullanıcı Erişim Maliyeti
- Kullanıcı Favori Siteleri
- Kullanıcı Site Erişimleri

Web Özet Raporları

- Bağlantılara Göre Zirvedeki Siteler
- Bant Genişliğine Göre Zirvedeki Siteler
- Kullanım süresine Göre Zirvedeki Siteler
- Bağlantılara Göre Zirvedeki Kullanıcılar
- Kullanım süresine Göre Zirvedeki Kullanıcılar
- Zirvedeki Engellenmiş Siteler
- Zirvedeki Engellenmiş Kullanıcılar
- Zirvedeki Virüsler
- İçerik Tipi Dağılımı
- Engelleme Kategorisi Dağılımı
- Adedine Göre Zirvedeki Dosya İndirmeleri
- Boyutuna Göre Zirvedeki Dosya İndirmeleri
- Zirvedeki Dosya Tipleri
- Zirvedeki Arama Motorları
- Zirvedeki Arama Kalıpları
- Engellenmiş Kategorilerin Müdavimleri
- Engellenmiş Kategorilere Harcanan Bant Genişliği
- Site Bazında Maliyet Analizi
- Kategori Bazında Maliyet Analizi
- Yeşil Bilişim ve Tasarruflar

Detaylı Listeler (Web)

- Siteler
- Kullanıcılar
- Web Akışı
- Kullanıcı Başına Siteler
- Kullanıcı Başına Adresler (URL)
- Site Başına Kullanıcılar
- Site Başına Kullanıcı ve Adresler (URL)

E-posta Trafiği Genel Görünüm

- İleti Filtreleme Özet Raporu
- İleti Trafiğinin Genel Karakteri
- İletilerin Filtreleme Sonuç Dağılımı
- Yeşil Bilişim ve Tasarruflar

E-posta Rapor Özetleri

- Aktif Kullanıcılar
- Gelen İletilerin Dış Göndericileri
- Gelen İletilerin İç Alıcıları
- Gelen İletilerin İç Göndericileri
- Gelen İletilerin Dış Alıcıları
- Dahili İletilerin İç Göndericileri
- Dahili İletilerin İç Alıcıları
- Alıcı Alan Adları
- Gönderici Alan Adları
- Gelen Virüs Tipleri
- Giden Virüs Tipleri

E-postaların Zaman Dağılımı

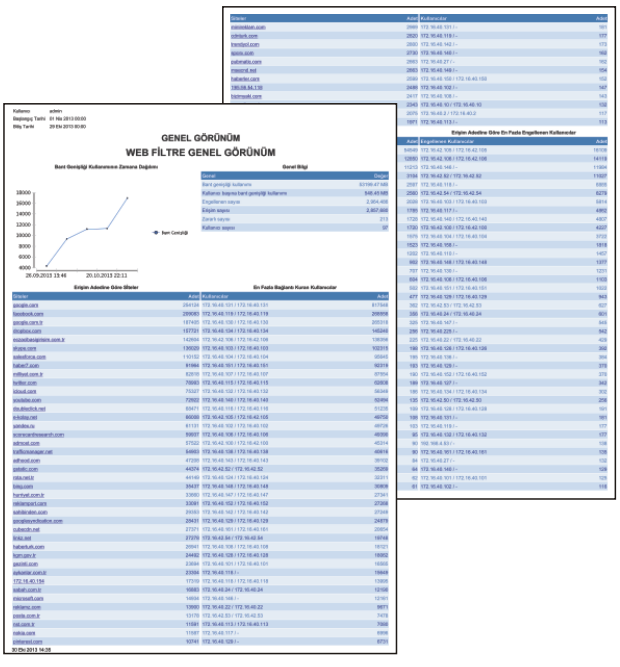
- Standart Dışı İletiler
- Kuyruğa Girmeden Reddedilen İletiler
- Spam ve Politika Filtresinde Engellenen İletiler
- Virüslü İletiler
- Temiz İletiler

Detaylı Listeler (E-posta)

- Standart Dışı İletiler
- Kuyruk Öncesi İletiler
- Spam İletiler
- Virüslü İletiler

Web Zaman Dağılımı

- Web Erişiminin Zamana Dağılımı
- Bant Genişliği Kullanımının Zamana Dağılımı
- Erişim Süresinin Zamana Dağılımı
- Filtreleme/Toplama Erişim Oranının Zamana Dağılımı
- Filtrelemenin Zamana Dağılımı
- Virüs Olaylarının Zamana Dağılımı



Yeni Nesil UTM Genel Özellikleri

Ağ Erişimi ve Servisleri
- TCP/IP
- IPv4 ve IPv6 desteği
- Hibrid IP (ipv4/ipv6) topoloji desteği
- PPPoE Desteği
- Dynamic Routing (OSPF, RIP, BGP, Multicast)
- Politika bazlı yönlendirme
- Real Multizone Desteği
- Link birleştirme (802.3ad)
- Saydam Köprü Modu
- VLAN'lar(802.1Q)
- DHCP Sunucu
- DHCP Proxy
- Caching DNS Sunucusu

İşletim/Yaşam Döngüsü
- Sıkılaştırılmış ve güvenli LabrisOS Firmware
- Parçalı firmware altyapısı
- Tüm firmware in yüklenmesi gerekmeden ve elle müdahale edilmesine gerek kalmadan firmware yükseltme işlemi
- Birden fazla cihazla yedekli, yüksek bulunur çalışabilme
- Otomatik güncellenen imza ve veritabanları

Kullanıcı Yetkilendirme
- Merkezi kullanıcı dizini ile tek bir noktadan tüm uygulama ve kullanıcıları yetkilendirme ve yönetim
- Ajanlı/Ajansız Aktif Dizin entegrasyonu (NTLM, LDAP)
- Wauth Hotspot yetkilendirmesi
- SMS ve kayıt masası ile misafir kullanıcı kabul edebilme
- GSM operatörlerinin mobil ödeme altyapılarına uygun yapı
- Radius/Tacacs yetkilendirme

WAN/LAN/ETHERNET
- Ürünlerin tüm portlarının WAN/LAN olarak kullanılabilmesi esnekliği
- Bağlantı yedekliliği desteği
- Bağlantı bazlı trafik politikası uygulayabilme
- WAN bağlantılarında yük dengeleme
- Bağlantı durumu bazlı eylemler tanımlayabilme
- 3G USB modemleri otomatik WAN çıkışı olarak tanımlayabilme
- Zengin metro ethernet, fiber, 10G sonlandırma seçenekleri
- Ethernet portlarının birleştirilerek kullanılabilmesi (Port Aggregation)

Güvenlik Duvarı (Firewall)
- Uygulama Tanıma (2000+ uygulama imzası)
- Uygulama bileşenlerine hakimiyet (Ör: facebook chat, facebook video, farmville, skype …)
- Bütünleşik http/https proxy motoru ile daha derin konfigürasyon yetenekleri (dosya tipi, mime tipi ve içerik bazlı kurallar kullanabilme)
- P2P engelleme
- Durum Korumalı (stateful) paket inceleme
- Zaman tabanlı dinamik kurallar
- Sınırsız kural ve oturumlar
- DoS ve DDoS önleme fonksiyonları
- Uygunsuz paket engelleme
- Politika bazlı esnek NAT/PAT
- Otomatik IP/MAC eşleme
- Bant genişliği, QoS yönetimi
- SSH denetim motoru ile şifreli SSH trafiklerinin kontrolü

Web Filtre
- URL filtreleme
- HTTPS filtreleme
- Beyaz listeler / Kara listeler
- İçerik tabanlı imzalar
- Hazır kategori veritabanı
- Türkçe'ye özel veritabanı işletimi
- Webfiltre+ aboneliği ile daha geniş bir veritabanından sıfırıncı dakika bilgileri için sorgulama yapabilme
- Engellemeden izleme ve raporlama özelliği
- Farklı kullanıcılara göre farklı politika grupları oluşturabilme
- IPler, IP aralığı, yerel kullanıcı ve grupları, aktif dizin kullanıcı ve grupları bazlı politika grupları
- Applet, Çerez(cookie), ActiveX engelleme
- Zaman tabanlı politikalar uygulayabilme
- İçerik değiştirebilme desteği
- Antispyware, antimalware, antitrojan, antiphishing desteği
- Arşiv dosyalarını inceleyebilme

Antivirüs
- Web (http/https) virüs koruması
- E-posta (sunucu, istemci) virüs koruması
- İmza tabanlı engelleme
- Heuristics tabanlı analiz
- Antivirüs motoruna bütünleşik sınırlandırılmış DLP
- Dosya türü/büyüklüğüne göre politika belirleyebilme
- Birden fazla türde ve katlı arşiv dosyaları desteği

Antispam
- Sürekli güncellenen imza veritabanı
- Heuristics tabanlı analiz
- Akıllı öğrenebilir spam motoru
- Spam sensor ağı geri beslemeleri
- Entegre resim OCR analizi
- Entegre PDF OCR analizi
- Kullanıcı ayarlı filtreleme desteği
- RBL desteği
- İçerik filtreleme
- Hazır içerik imzaları
- Beyaz listeler / Kara listeler
- Son kullanıcı spam karantinası
- Son kullanıcı spam rapor ekranı
- Son kullanıcı karantina bilgilendirme e-postası

Sunucu Yük Dengeleme
- L4 (Katman 4) yük dengeleme
- Bütünleşik reverse proxy ile SSL sonlandırma ve L7 yük dengeleme

İzleme ve Analiz
- Anlık kayıt izleme
- Grafiksel ağ kullanımı izleme
- Oturum detaylarını görebilme

Merkezi İzleme
- Labris MNG Merkezi Yönetim Sistemi ürün ailesine tam uygunluk
- Labris MNG eşliğinde Merkezi olarak tek noktadan politika alabilme
- Labris MNG eşliğinde Merkezi olarak izlenebilme
- Labris MNG eşliğinde Merkezi olarak yapılandırma ve kayıt yedekleme

Yönetim
- Sürükle bırak kolaylığında konfigürasyon arayüzü
- Web tabanlı izleme, raporlama arayüzü
- HTTPS/SSH/LMCCP yönetim desteği
- Son kullanıcı tarafından yönetilebilir virüs/spam karantinası
- SSL ile güvenli uzak bağlantı
- Yerel dil desteği (Türkçe,…) ve uyarlanabilme kolaylığı
- Nesne tabanlı yönetim
- Platform bağımsız yönetim altyapısı
- Rol tabanlı yönetim yetkilendirmesi
- Geçmişe dönük konfigürasyon yedeklerini kaydetme
- Eski politikalara geri dönebilme
- Sadece konfigürasyon yedeğinin yüklenmesiyle yeni bir cihazın ek bir işleme gerek olmadan eskisiyle değiştirilebilmesi

Kayıt Altına Alma
- Dahili olarak log tutabilme
- Uzak alanlara log yollayabilme (SYSLOG, ftp, uzak disk alanları,…)
- T.C. kanunlarına uygun nitelikli zaman damgası

Raporlama
- Grafik tabanlı raporlama motoru
- Bütünleşik güvenli ve hızlı veritabanı
- Dahili olarak ek bir sistem ihtiyacı olmadan rapor üretebilme
- Düzenli raporlama emirleri verebilme
- Üretilen raporları bir e-posta adresine yollayabilme
- Hazır rapor kategorileri ve şablonları
- Zamanlanmış veya anlık ihtiyaçlara uygun raporlama altyapısı

FLEX FIRMWARE SEÇENEKLERİ

Firmware FLEX	A	B	C	D
Güvenlik Duvarı	✓	✓	✓	✓
VPN/SSL VPN	✓	✓	✓	✓
IPS (Saldırı Önleme)	✓			✓
Web Filtre		✓	✓	✓
Antivirüs/Antispam Ağ Geçidi			✓	✓
Wauth+ (Hotspot ve Ağ Yetkilendirme)				

ETHERNET KART SEÇENEKLERİ

ÜRÜN	Kart Yuvası	GIGABIT (4 veya 8 port)	FIBER SFP (4 veya 8 port)	10G SFP+ (2 port)	10G SFP+ (4 port)
Labris UTM 52/56	1 Adet	✓	✓	✓	✓
Labris UTM 62/64	2 Adet	✓	✓	✓	✓
Labris UTM 150/155	3 Adet	✓	✓	✓	✓
Labris UTM 170/175	4 Adet	✓	✓	✓	✓

TAMAMLAYICI ÜRÜN AİLELERİ

Labris LOG

Labris LOG ürün ailesi, ağı dinleyerek logları toplayabilmesinin yanında, Labris UTM cihazlarının loglarını tek bir noktada toplayarak bu loglardan raporlar elde edebilmektedir.

Labris MNG

Labris MNG ürün ailesi ile Labris UTM cihazlarının tek bir merkezden izlenebilmesi, politikaların tek bir yerde düzenlenerek tüm cihazlara aynı anda uygulanabilmesi amacıyla kullanabilmektedir.

İLİŞKİLİ ÜRÜN AİLELERİ

Labris CLOUD

Labris UTM cihazları ile elde edebildiğiniz fonksiyonaliteyi, bulutta yer alan sunucu altyapılarınız için de edinebilmeniz mümkün. **Labris CLOUD** çözümleri hem cloud'da kurulu yapılarınızın güvenliğini hem de trafiğiniz henüz ISP üzerindeyken güvenlik hizmetlerini alabilmenizi sağlayabilmektedir.

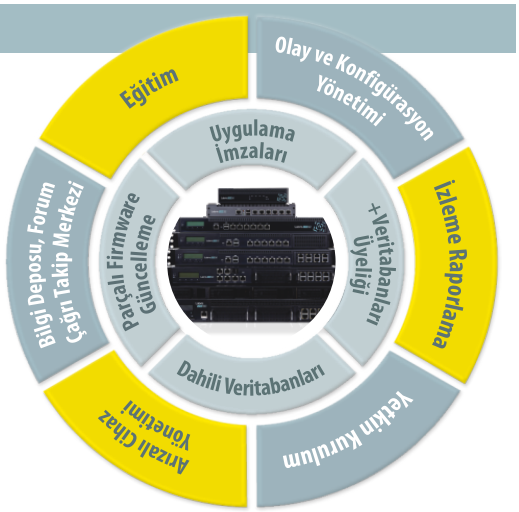
Labris Yazılım, VM Uyumu

Labris UTM firmware'i aynı zamanda **VM**'lerde çalışabilen yazılım olarak da edinilebilmektedir. Projede ihtiyaç olması halinde, Labris UTM içinde bulunan uygulamalar, tek tek yazılım olarak da edinilebilmektedir.

ÜRÜN YAŞAM DÖNGÜSÜ

Ürününüzle birlikte edinebileceğiniz uygun SLA paketleri için lütfen **Labris Destek Hizmetleri Datasheet**'ini inceleyiniz.

Ürününüz ve işleyişinize en uygun yaşam döngüsü için +90 **850 455 45 55**(pbx); **destek@labrisnetworks.com** iletişim bilgilerini kullanarak bize ulaşabilirsiniz.
http://labrisnetworks.com/tr/support-training/



Labris Networks
Galyum Blok, K1-1, Teknokent-ODTÜ,
ANKARA / TÜRKİYE

T + 90 312 2101490 (Pbx)
F + 90 312 2101492
bilgi@labrisnetworks.com

İstanbul İhracat Ofisi
Levent LOFT, İstanbul / TÜRKİYE
T + 90 212 2642200

twitter.com/labristeknoloji www.facebook.com/labristeknoloji www.linkedin.com/company/labris