Labris® LOG

Wauth+

Loglama

Raporlama

SOC (Security Operations Center) merkezimizde, cihazlarımız, siber saldırılar ve güvenlik olayları yakından izlenir. Olası güvenlik açıkları CWL (Cyber Warfare Lab) ilgililerinin de bulunduğu ekiplerce değerlendirilerek önlemler alınır. Bu sayede önlemlerimiz ve geliştirdiğimiz teknoloji ile sizin için değerli olanı yakından koruruz.*

SOC

Ekibimiz, 7 gün 24 saat sistemlerinizden gelen alarmları izler, altyapınızı en verimli şekilde kullanmanızda ihtiyacınız olan yakın desteği sağlar. Labris ürünü aldığınızda, işinize en uygun SLA standardından faydalanma avantajına sahip olursunuz.**

Close Security Support

Labris Networks, sahip olduğu kurulu cihazlar ve sensör ağları ile yaygın ve kritik önemdeki ağlarda yaptığı yoğun incelemeleri, Cyber Warfare Lab™'da teknolojik altyapıya veya imzaya dönüştürerek cihazlara dağıtmaktadır.

CWL cyber warfare lab

Labris NETWORKS

* SOC merkezinden yapılan bağlantılar, servis alınan SLA programına uygun olarak, son kullanıcı onayıyla gerçekleştirilmektedir.

**SLA programlarında verilen hizmet kapsamı için lütfen Satış Sonrası Destek Kataloğunu inceleyiniz.

Kullanıcı Yetkilendirme +

Farklı misafir tanımlarına farklı yetkilendirme senaryoları yaratabileceğiniz esnek çözümler +
Türkçe ve İngilizce arayüz desteğine sahip web tabanlı yönetim +
Active Directory, LDAP, Otel Yönetim Yazılımı ve diğer uygulama veritabanlarıyla entegrasyon +

5651 İçin En Doğru Çözüm +

Trafiği dinleyerek 5651'e tam uygun loglama kabiliyeti +
Kanuni Zaman Damgası +
Davalarda kanıtları hızlı, doğru, kanunlara uygun şekilde edinebilme +
Aynı anda birden fazla noktayı dinleyebilme +

Entegre Raporlama +

Detaylı web kullanım raporları +
Kolay anlaşılır, kullanıcı-dostu, grafiksel arayüz +
Günlük, haftalık, aylık veya istenilen zaman aralıkları için kullanıcı bazlı rapor desteği +
PDF, XLS gibi çeşitli formatlarda rapor desteği +
E-posta yoluyla otomatik raporlama +

Labris LOG, kanuni yükümlülüklerinizi yerine getirmenizi sağlayacak altyapıyı üst düzey teknoloji ve güvenlik bilgi birikimiyle sunuyor.

"Loglama hiçbir zaman sadece loglama olmadı" felsefesini taşıyan ürün, loglamayı güvenliğin önemli bir yapıtaşı olarak ele alıyor.

Entegre ve kolay yönetilebilir yetkilendirme (Hotspot) çözümü Wauth+ ile önemli güvenlik açıkları oluşturabilecek ve siber suç unsuru oluşturabilecek gezici veya misafir kullanıcıları yetkilendiriyor.

Labris LOG, kullanıcı SMS Yetkilendirmesi (SMS Depo ve Mobil Ödeme) ve elle kullanıcı kaydı seçeneklerinin yanında, Active Directory, LDAP, Otel programları vs. gibi mevcut veritabanlarınızı da tek tıkla kullanma şansı sunuyor.

Bütün bunların yanında, Labris LOG güçlü raporlama altyapısı ile ağınızda olup bitenlerle ilgili detaylı raporlar sunabiliyor, anlık izleme ekranı ile ağ trafiğini yakından denetleme imkanı veriyor.

Raporlama +

Entegre Raporlama *Modülü*

Ürün üzerinde toplanan kayıtlar için, cihazlara bütünleşik entegre raporlama modülüyle, grafiksel, yöneticilerin de kolaylıkla anlayabileceği, hızlı bir analiz aracı sunmaktadır.

Hızlı ve akıllı Matris Analiz altyapısı sayesinde, tek bir kritere göre değil, birçok kriteri sentezleyerek rapor üretebilir.

Anlık izleme özelliği ile anormal durumlarda, anında ve doğru noktaya müdahale edebilme yetkinliği kazandırır. Ağınızdaki kullanıcıların internet kullanım karakteristiklerini çıkarır, daha verimli politikalar oluşturmanız için yol gösterir.

Sistem Kullanımı
- Yük Ortalaması
- Bant Genişliği Kullanımı

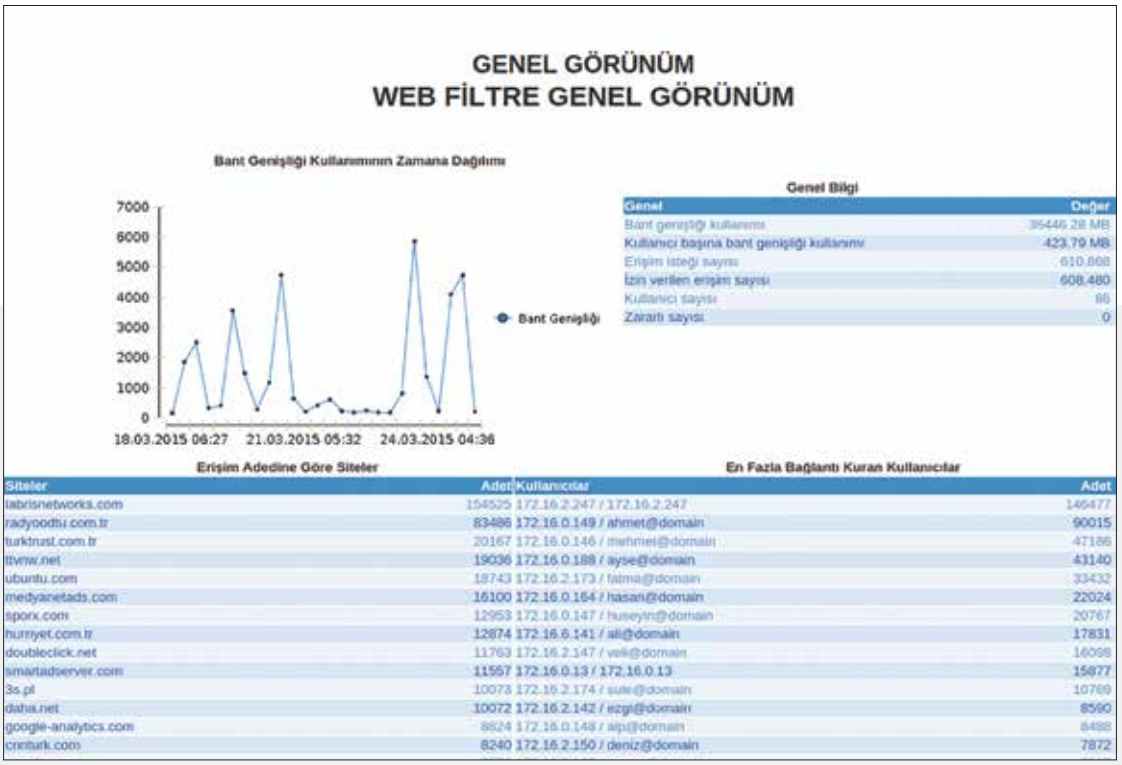
Zamana Göre Dağılım
- Erişim Sayısı
- Kullanım Süresi

Dosya İndirmeleri (Adedine Göre)
- Dosya Tipleri
- Arama Motorları
- Arama Kalıpları

Web Kullanımı
- Web Genel Görünüm
- Son Yarım Saat
- Şu Anki Siteler
- Şu Anki Adresler & Özetler
- Siteler (Bağlantılara Göre)
- Siteler (Kullanım Süresine Göre)
- Kullanıcılar (Bağlantılara Göre)
- Kullanıcılar (Kullanım Süresine Göre)

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

Ayrıntılı Listeleme
- Siteler
- Kullanıcılar
- Web Akışı
- Kullanıcı Başına Siteler
- Kullanıcı Başına Adresler (URL)
- Site Başına Kullanıcılar
- Site Başına Kullanıcı ve Adresler (URL)
- IP-MAC Listeleme



GENEL GÖRÜNÜM
WEB FİLTRE GENEL GÖRÜNÜM

Bant Genişliği Kullanımının Zamana Dağılımı

Genel Bilgi

Genel	Değer
Bant genişliği kullanımı	39446.28 MB
Kullanıcı başına bant genişliği kullanımı	423.79 MB
Erişim isteği sayısı	610.868
İzin verilen erişim sayısı	608.480
Kullanıcı sayısı	86
Zararlı sayısı	0

Erişim Adedine Göre Siteler

Siteler	Adet
tabrisnetworks.com	154525
radyoodtu.com.tr	83486
turktrust.com.tr	20167
ttvnw.net	19036
ubuntu.com	18743
medyanetads.com	16100
sporx.com	12953
hurriyet.com.tr	12874
doubleclick.net	11763
smartadserver.com	11557
3s.pl	10073
disha.net	10072
google-analytics.com	8624
cnnturk.com	8240

En Fazla Bağlantı Kuran Kullanıcılar

Kullanıcılar	Adet
172.16.2.247 / 172.16.2.247	146477
172.16.0.149 / ahmet@domain	90015
172.16.0.146 / mehmet@domain	47186
172.16.0.189 / ayse@domain	43140
172.16.2.173 / fatma@domain	33432
172.16.0.164 / hasan@domain	22024
172.16.0.147 / huseyin@domain	20767
172.16.6.141 / ali@domain	17831
172.16.2.147 / veli@domain	16098
172.16.0.13 / 172.16.0.13	15877
172.16.2.174 / sule@domain	10769
172.16.2.142 / ezgi@domain	8590
172.16.0.148 / alp@domain	8488
172.16.2.150 / deniz@domain	7872

Wauth +

Misafir Yetkilendirme *(Hotspot)*

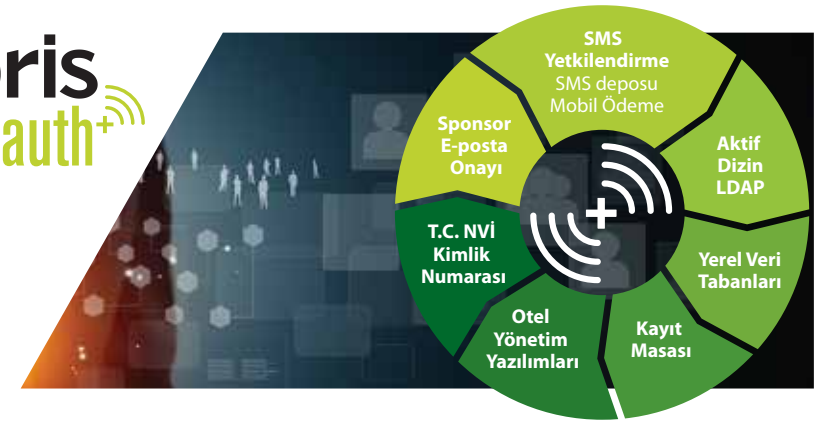
Labris WAUTH+, pazardaki hotspot çözümlerinden farklıdır. Bu işi güvenliğin önemli bir parçası olarak ele alır ve her çeşit internet ağına entegre edilebilecek kapsamlı çözümler önerir.

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

WAUTH+ ile yetkilendirdiğiniz kullanıcıların 5651 sayılı yasa kapsamında istenen tüm logları Labris LOG üzerinde kanuni zaman damgasıyla saklanarak, gerektiğinde raporlanabilir.

5651 Loglama ve Türktrust Kanuni Zaman Damgası +

Labris Wauth+



Hotspot ve Ağ Yetkilendirme

- Ağ bileşenlerinden bağımsız olarak, yetkilendirme yapılacak ağ bölümlerini belirleyebilme
- Birden fazla ağ arabiriminde aynı anda çalışabilme
- WAN üzerinden çalışarak uzak bölgelerdeki kullanıcıları merkezden yetkilendirebilme
- Yetkilendirme uygulanmayacak istisna ağ cihazlarını belirtebilme
- IPsec VPN ve MPLS gibi L3 ağlarda IP-Kullanıcı eşleşmesi ile yetkilendirilebilme
- Kullanıcı grubu ve ağ bazlı politika belirleyebilme
- Labris Wauth+ ile her bir ağ için ayrı ayrı yetkilendirme metodları seçilebilir ve kullanıcı giriş sayfası bu şekilde özelleştirilebilir
- Wauth+ kullanıcıları için uygulama kontrolü
- Kurum kablosuz ağlarından SMS ile izinsiz internet kullanımını engellemek için Ortak Anahtar özelliği
- Kota belirleyebilme
- İnternet tarayıcısı diline göre değişen Türkçe ve İngilizce arayüz desteği
- Misafir Giriş sayfasını tamamen özelleştirilebilme
- Kullanıcı giriş sözleşmesi onay süreci uygulayabilme
- Kullanıcı için "Şifre Değiştir", "Çıkış Yap" seçeneği
- Wauth+ ACL yapısı ile hangi kullanıcı ve grupların hangi ağlardan erişim sağlayabileceklerini ayarlayabilme
- Wauth+ kullanıcıları için bant genişliği kontrolü
- SMS kullanımı için ek bir prosedüre gerek olmadan kontör yükleyebilme
- Kullanıcı arama motoru
- Aktif bağlantıların izlenmesi, istenilen kullanıcı bağlantılarının kesilebilmesi
- T.C. 5651 ve e-imza kanunlarına uygun loglama

Loglama +

5651 İçin
En Doğru Çözüm

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

Zaman Damgası Alternatifleri: Gereksinim halinde kurum ağında yer alan e-imza sertifika sunucusu kullanılabilmektedir.

Labris LOG, topoloji ve ağda var olan yatırımınızı etkilemeden, kolayca ağa dahil edilerek, kanuna uygun şekilde kayıt tutmanızı sağlar.

Loglama Özellikleri

Tak ve Kullan Kolaylığı

Hiçbir konfigürasyon yapılmadan yönlendirilmiş trafiği kaydetmeye başlar. Dinlenecek trafiğin bir kopyası switch üzerinden (port mirroring veya span port), harici "tap dinleme cihazı" veya standart bir hub ile cihaza aktarılır. Bu anlamda bir kayıt sensörü olarak çalışır.

Köprü (Bridge) Modu

Dinlenmek istenen trafiğin üzerinden geçtiği hatta araya girerek, ağda hiçbir değişiklik yapmadan ve kullanıcılar farkına varmadan dinleme ve kayıt işlemleri yapabilir.

Çoklu Trafiği Çoklu Yöntemle Eş Zamanlı Dinleyebilme

Dinleme portlarının tamamı aynı anda kullanılabilir. Aynı anda birden fazla trafik için köprü modunda inceleme yaparken, yönlendirilmiş birden fazla trafiği de dinleyebilir.

Uzaktan Log Alma

Uzak Linux ve türevi sistemlerden syslog ve snmp ile, Windows sistemlerden Labris Kayıt Alma Yazılımı ile kayıtları kendi üzerine alır, damgalar ve sunar.

Vlan Tagged Dinleme

IEEE 802.1Q (VLAN Tagging) standardına göre birden fazla VLAN trafiğini aynı hat içinde barındıran dinlemelerde, standart uyumlu dinleme ve kayıt altına alabilme olanağı sağlar. Bu sayede gelişmiş ağlarda ağa dokunmadan kurulum ve yönetimi mümkün kılar.

Anlık Kayıt İzleme

İzleme sırasında akan trafiği IP ve hedef URL bazında filtreleyerek daha net ve detaylı bir izleme gerçekleştirilebilir.

Yönetim Profilleri

Yönetim arayüzünde, farklı yönetim profilleri tanımlanarak, farklı yetki ve erişim seviyelerinde yönetim mümkündür.

Aktif Dizin

Kayıtlarda Active Directory kullanıcı ismi ve hedef siteye ait IP adresini gösterir.

Arabirim Bölümleri

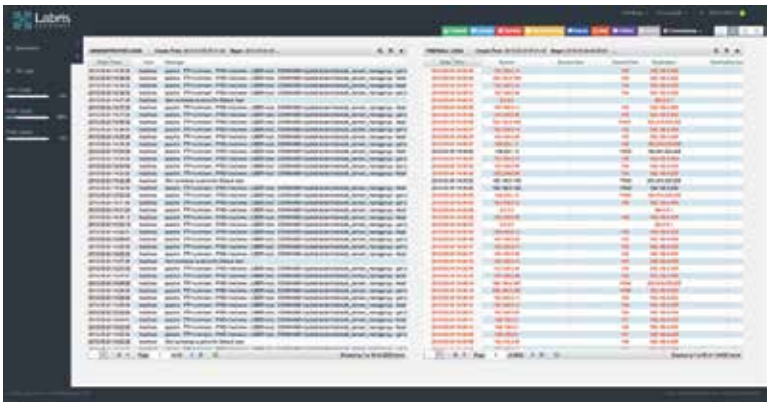
- Sensör ayarları
- Syslog Alma - Gönderme
- Windows üzerindeki kayıtların alınması. (Windows ajanı ile)
- Snmp log alma ayarları

Windows üzerinden Log alma ajanı

- Windows temel olay kayıtları
- DHCP Server kayıtları
- Exchange e-posta kayıtları
- IIS kayıtları
- Diğer bütün text içerikli loglar özel tanımlanarak alınabilir.

Uzak Loglama / Log Barındırma

Birden fazla uzak sunucuya yedek kayıt tutabilir, uzak syslog sunucularına log yazabilir. Harici Depolama Alan Ağlarına (SAN) bağlanarak kayıt tutabilir. Standartlara uyumlu tüm harici uygulamaların loglarını üzerinde barındırarak, kendi üretmiş olduğu loglarla birlikte zaman damgasıyla damgalanabilir.



Log Analizi (LOGVIEW)

İzlenebilecek Log Tipleri	Web, E-posta, Dhcp Kayıtları, Oturum Kayıtları, Diğer Sistemlerden Alınan Kayıtlar, Operasyonel Kayıtlar
Yönetim	Hiyerarşik Filtreleme Web Tabanlı Hızlı Yönetim Sistem genelindeki tüm kayıtların gerçek zamanlı izlenmesi Gerçek zamanlı filtreleme Ardışık filtreleme Geçmiş kayıtlarda kayıt arama Widget bazlı görünüm Pano (Dashboard) üzerinde kişiselleştirilmiş görünümler oluşturabilme ve kayıt edebilme Sistem kaynak izleme Servis yönetimi Değişken ekran desteği ile internet tarayıcısının ortam ve boyutuna göre biçim alabilme Farklı kaynakların izlenebilmesi Alanların görünürlüğünün özelleştirilebilmesi Sütun yeniden boyutlandırma Sütun yeniden sıralama
Dışa Aktarım	TXT, CSV

Loglamayla ilgili gereksinimleri yerine getirmek için topolojimizi, kullandığımız ürünleri değiştirmek istemiyoruz.

Kurulum gerektirmeyen tak çalıştır yeteneğiyle Labris LOG, hiçbir konfigürasyon yapılmadan, yönlendirilmiş trafiği kaydedebilir. Yani, ister köprü (bridge) modunda araya girerek, isterseniz switch üzerinden (port mirroring veya spanport), harici "tap dinleme cihazı" veya standart bir hub ile trafiği cihaz üzerine yönlendirmeniz yeterlidir.

Dağıttığım DHCP (IP dağıtım) loglarını alıp TIB'in yayınladığı programa vermem, operasyonel gereklilikler ve kanunlar karşısında yeterlidir.

TIB kanun tarafından yetkilendirilmiş bir zaman damgası sağlayıcı değildir. 5070 sayılı kanun sadece "Elektronik Sertifika Hizmet Sağlayıcı" olarak yetkilendirilen kuruluşların internetteki verilerin "değiştirilemezlik, bütünlük, gizlilik" ilkesini garanti ettiğini yazar.

Loglama ürününün ağıma, sunucularıma ve son kullanıcı bilgisayarlarıma müdahale etmesini, bir ajan kurmasını istemiyorum.

Labris LOG trafiği inline olarak dinler ve ajansız çalışır. PC lerinize ve sunucularınıza müdahale edilmesine gerek kalmaz.

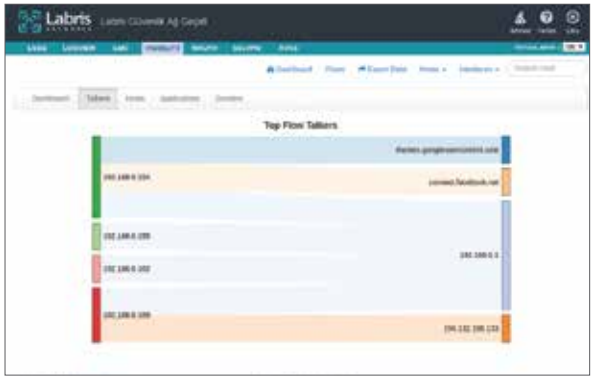
Misafir kullanıcıların kimliğini açıkça alabileceğim ve bana SMS ücreti gibi bir maliyeti olmayacak güvenilir bir yol bulamıyorum.

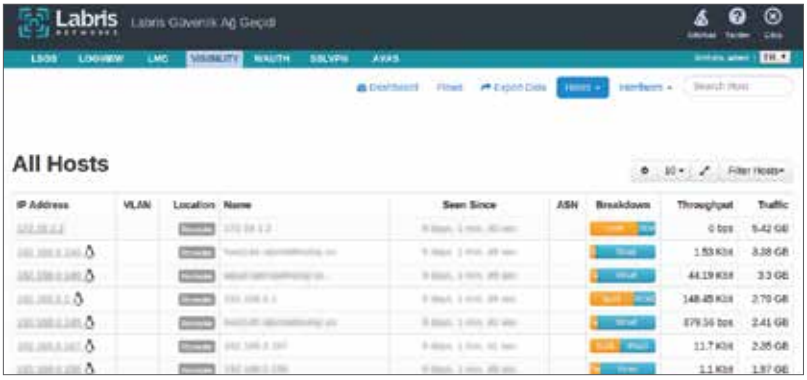
Labris LOG'a entegre olarak geren Wauth+ yetkilendirme modülünde aynı zamanda mobil ödeme entegrasyonu da bulunmaktadır. Bu yöntemle, yetkilendirme isteğinde bulunan cep telefonundan ilgili SMS ücreti alınabilmektedir. Size herhangi bir ek maliyet yansımayacaktır. Misafir kullanıcılarınız cep telefonu numarası ve şifre ile ağa dahil olduğunda, 5651 sayılı kanun kapsamında gerekli logları zaman damgasıyla cihaz üzerinde güvenli olarak tutulur ve saklanır.

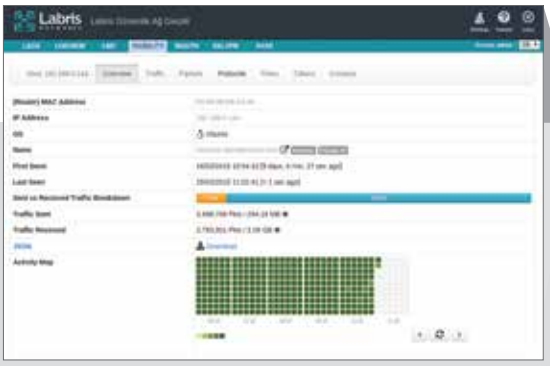
Network ***Visibility***

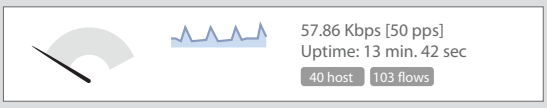
(Anlık Trafik İzleme, Kırılımlı Görsel Trafik Analizi)

- Ağınızda akan trafiğin detayını arabirim, uygulama ve IP bazlı görün.
- Kullanıcılarınızın internet kullanımını ve kullanım detayını gerçek zamanlı takip edin.
- Ağdaki yavaşlıkların sebeplerini görün.
- Geçmiş kullanım yoğunluklarının detayını görün.









Ürün Yaşam Döngüsü

Ürününüzle birlikte edinebileceğiniz uygun SLA paketleri için lütfen Labris Destek Hizmetleri Kataloğu'nu inceleyiniz.

Ürününüz ve işleyişinize en uygun yaşam döngüsü için
+90 850 455 4555; destek@labrisnetworks.com iletişim bilgilerini kullanarak bize ulaşabilirsiniz.

	Labris LOG 10	Labris LOG 14	Labris LOG 30	Labris LOG 60	Labris LOG 150	Labris LOG 155
Bant Genişliği	16 Mbps	60 Mbps	90 Mbps	150 Mbps	500 Mbps	1000 Mbps
Log Yazma Performansı *	600 Log/Sn	1200 Log/Sn	2500 Log/Sn	4000 Log/Sn	8000 Log/Sn	14000 Log/Sn
Dahili Loglama	450 GB	1 TB	1 TB	2 TB	2x3 TB	2x4 TB
Yedekli Loglama	-	-	Op (RAID 1)	Op (RAID 1)	Op (RAID 0, 1, 5)	Op (RAID 0, 1, 5)
Uzak Loglama	Syslog/SAN (iSCSI)	Syslog/SAN (iSCSI)	Syslog/SAN (iSCSI)	Syslog/SAN (iSCSI)	Syslog/SAN (iSCSI)	Syslog/SAN (iSCSI)
Dinleme Portları	3 adet 100/1000	5 adet 100/1000	5 adet 100/1000	7 adet 100/1000	7 adet 100/1000	7 adet 100/1000
Yönetim Portları	1 adet 100/1000	1 adet 100/1000	1 adet 100/1000	1 adet 100/1000	1 adet 100/1000	1 adet 100/1000
LCD Panel / VGA	-	20x2 LCD 4 tuş	20x2 LCD 4 tuş	20x2 LCD 4 tuş	20x2 LCD 4 tuş	20x2 LCD 4 tuş
SEÇENEKLER	IPS	IPS	IPS 2 TB Log Alanı Ek 100/1000 Port ve Fiber Port	IPS 2 TB Log Alanı Ek 100/1000 Port ve Fiber Port	IPS 4 TB Log Alanı Ek 100/1000 Port ve Fiber Port	IPS 4 TB Log Alanı Ek 100/1000 Port ve Fiber Port

* Tavsiye edilen trafik büyüklüğü (gelen, giden toplam) ve log yazma performansı trafiğin türü ve paket büyüklüğüne göre değişiklik gösterebilir.

Labris NETWORKS

Siber Savaşta Yakın Koruma

Galyum Binası No:27 K1-1
ODTÜ-Teknokent
Ankara/Türkiye
T . +90 312 2101490 (Pbx)
F . +90 312 9881798
bilgi@labrisnetworks.com
www.labrisnetworks.com

7 • 24 • 365
GLOBAL SUPPORT

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