



Labris™ Güvenlik Duvarı (Firewall)

Güvenlik duvarı (firewall) sunucusu

**ağınızı dışarıdan yalıtır
sanal IP adreslerinden oluşan ağlara olanak tanır
kurum iç ve dış güvenlik politikasında başı çeker**

Güvenlik duvarları oldukça uzun süreden beri varolmakla birlikte zaman geçtikçe çok önemli teknik ilerlemeler kaydettiler. En başta sınırlı sayıda arabirim desteği ile basit IP filtreleme yapan güvenlik duvarları bugün durumlu paket incelemeden (stateful inspection), ağ adres dönüşümüne(NAT) kadar birçok yeni özelliğe sahip olmuşlardır.

Güvenlik duvarları sayesinde giden ve gelen tüm erişimleri denetlemek yetisine sahip olmakla; hem dışarıya karşı ağınızı güven altına alır hem de kullanıcılarınızın çeşitli verim düşürücü erişimlerini kısıtlayabilme imkanına sahip olursunuz.

Uygulamalarınıza özel bölgeler (DMZ, MZ) oluşturabilir, birden fazla yerel ağınız arasındaki erişim kontrollerini gerçekleştirebilirsiniz. Güvenlik duvarları kullanıcıdan habersiz olarak belirli amaçla dışarı çıkan tüm paketler tespit edilmiş sunuculara yönlendirilebilir.

Güvenlik Duvarı Nasıl Çalışır?

Güvenlik duvarları görevleri gelişmiş IP filtreleme ve NAT'dan öte gitmeyen hafif ve basit sistemler olmak zorundadır. İşlevi yazacağımız kurallar ile tespit edilen, belli IP adresinden gelip belli IP adreslerine giden, belli bir tipi olan ve belli portları kullanan tüm paketlerin kabul edilmesinden ya da reddedilmesinden ibarettir.

Eğer iç ağda gerçek IP adresleri kullanılmıyorsa bunların hepsinin dışarıdan tek bir IP adresi olarak görülmesi, teknik ismiyle "ağ adres dönüşümü" de güvenlik duvarı üzerinde yapılır.

Kısıtlama, yönlendirme ve köprü gibi modlar ile güvenlik duvarı bulunduğu ağ topolojisine ayak uydurulamaktadır.

Özellikler

Güvenlik Duvarı (FIREWALL)

- Durum bilgisi tutarak paket inceleme (stateful packet inspection)
- Kural tabanlı erişim denetimi
- Kaynak adresleri, hedef adresleri, ağ adresleri ve servis/port bazında kural tanımlama
- IP, Kullanıcı, makine, domain, ağ ve gruplar bazında filtreleme
- MAC adreslerine bağlı kurallar tanımlayarak, IP değiştirerek gerçekleştirilebilecek yetki ihlallerinin ve IP-MAC eşleşmeleri dışında internete çıkışların engellenebilmesi
- Zamana bağlı olarak otomatik olarak değişebilen dinamik kurallar
- Kural tabanlı hat sığası(bandwidth) ve trafik düzenlemesi
- Uygulama katmanı seviyesinde filtreleme
- Kısıtlanmamış kural, profil ve oturum sayısı
- Durum Korunmalı işlem yeteneği ile minimum kural ile güvenli işletim
- Trafik Sayımı
- Kötü paket desteği
- TCP/IP seviyesinde paket yönlendirme
- Birden çok protokol kullanan uygulamalar ile çalışabilirlik
- Erişim denetim ve yetkilendirme: Çeşitli işletim sistemlerinde özel istemci yazılımı ile yetkilendirilen kullanıcılara, özel olarak belirlenmiş kuralların atanması
- One-to-many(adres aralığı, alt ağ adresi), one-to-one ağ adres dönüşümü (NAT, PAT)
- Birden fazla IP'ye Round-robin yönlendirme ile yük dengeleme
- Görünmez mod desteği(stealth bridge)
- Bulunduğu donanım üzerine veya uzak sunucuya kayıt tutabilme (logging)
- SNMP desteği
- Üçüncü parti ürünler ile entegrasyon



Labris™ Güvenlik Duvarı (Firewall)

SANAL ÖZEL GÜVENLİ AĞ (VPN-VIRTUAL PRIVATE NETWORK)

- IPSec, PPTP ve L2TP protokolleri desteği
- Açık anahtar (Public Key, X509) sertifika desteği
- Gizli anahtar (Shared Key) desteği
- AH ve ESP alt güvenlik protokolleri
- 3DES, AES şifreleme algoritmaları
- SHA1, SHA2, MD5 paket bütünlüğü kontrol algoritmaları
- IKE anahtar değişim protokolü
- IPCOMP ile veri sıkıştırma
- Otomatik ve el ile yeniden anahtarlama
- Perfect Forward Secrecy(PFS) desteği
- NAT geçişi desteği ile NAT arkası cihaz ve ağlara destek
- Windows ve Linux işletim sistemleri için ücretsiz VPN istemcileri
- Sabit olmayan istemcilerden VPN bağlantı için modem desteği
- SMP sistemlerde VPN işlemine tek CPU ayırma desteği

YÖNETİM

- Java tabanlı grafik yönetim arayüzleriyle kolay, Türkçe veya İngilizce yönetim
- Farklı yetkilere sahip birden fazla yönetici atayabilme
- Nesne bazlı politika oluşturma yapısı ve sürükle-bırak, kopyala-yapıştır yöntemleri ile hızlı ve verimli işlem
- Önceden hazırlanmış TCP, UDP, Ağ ve diğer servis nesneleri
- Tek ekrandan ağdaki veya uzak noktadaki tüm Labris servislerinin yönetimi ve ilişkilendirilebilmesi
- Tek arabirim ile diğer Labris güvenlik duvarı, saldırı tespit sistemi, vpn, antivirüs, antispam, web filtreleme ve zayıflık tespit sistemlerini yönetebilme
- Windows, Linux, Solaris ve diğer birçok platformdan uzaktan yönetim
- Yönetim konsollarında veri tutulmayarak tamamen mekan bağımsız yönetim
- Yönetim konsolu ve Labris ürünleri arasında özel LMCCP protokolü (SSL/TLS yüksek güvenlikli) ile erişim
- Yönetim konsoluna web arayüzü erişimi.
- Yönetim erişimlerinde sertifika ve şifreden oluşan çift yetkilendirme
- Log tutma ve yönetimi
- TFTP ile yazılımların güncellenebilmesi
- Yönetim platformundan belli kişilere çeşitli seviyelerde yetki dağıtımı (sadece izleme, ayar değiştirme vb.)
- SFTP ve LMCCP ile uzaktan güncelleme
- İstenilen tarihteki güvenlik politikalarına heran geri dönebilme, tekrar yükleyebilme

Güvenlik - Güvenilirlik

- ⊕ Hata-dayanıklı işletim
- ⊕ TCP SYN, spoofing gibi gelişmiş saldırı tiplerine bağışıklık
- ⊕ Yama ya da güncellemelerle hızlı tedbir alma