Forcepoint

Bilgi Formu

Next Generation Firewall

Yerel SD-WAN özelliklerine sahip Kurumsal Ağ Güvenliği

Temel Avantajlar

İşletmeler için daima açık SD-WAN bağlantısı

Günümüzün işletmeleri, tümüyle esnek ağ güvenliği çözümleri talep ediyor. Forcepoint Next-Gen Firewall (NGFW), tüm seviyelerde yüksek ölçeklenebilirlik ve kullanılabilirlik sunar.

- **Aktif-aktif, karışık kümeleme.** Farklı sürümleri çalıştıran farklı modellerden 16'ya kadar düğüm birlikte kümelenebilir. Bu, üstün ağ performansı ve esnekliği sağlar ve derin paket denetimi ve VPN'ler gibi güvenlik özelliklerini etkinleştirir.
- **Sorunsuz politika güncellemeleri ve yazılım yükseltmeleri.** Forcepoint'in endüstri lideri kullanılabilirliği, politika güncellemelerinin (ve hatta yazılım yükseltmelerinin) hizmeti kesintiye uğratmadan sorunsuz bir şekilde bir kümeye iletilmesini sağlar.
- **SD-WAN ağ kümelendirmesi.** Ağ ve VPN bağlantılarında yüksek kullanılabilirlik sağlar. MPLS gibi pahalı kiralık hatları desteklemek veya değiştirmek için yerel geniş bant bağlantılarından yararlanma olanağı ile kesintisiz güvenliği birleştirir.

Forcepoint Next-Gen Firewall, insanları ve çeşitli ve gelişen kurumsal ağlarda kullandıkları verileri birbirine bağlamak ve korumak için hızlı, esnek SD-WAN bağlantısı ile endüstri lideri ağ güvenliği sunar. Forcepoint NGFW, fiziksel, sanal ve bulut sistemlerinde tutarlı güvenlik, performans ve çalışma sunar. Merkezi yönetim ve 360° görünürlük ile birlikte yüksek kullanılabilirlik ve ölçeklenebilirlik için sıfırdan tasarlanmıştır.

Forcepoint NGFW'ye geçen müşteriler Forcepoint NGFW'ye geçen müşteriler siber saldırılarda %86 düşüş, BT çözümünde %53 daha az yük ve %70 daha az bakım süresi bildiriyor.*

Değişen güvenlik ihtiyaçlarına ayak uydurun

Birleştirilmiş bir yazılım çekirdeği, Forcepoint'in dinamik iş ortamlarında güvenlik duvarı/VPN ve ZTNA Uygulama Bağlayıcısından Saldırı Önleme Sistemine (IPS) ve katman 2 güvenlik duvarına kadar birden fazla güvenlik rolünü üstlenmesini sağlar. Forcepoint, tamamen tek bir konsoldan yönetilir ve çeşitli şekillerde (örneğin, fiziksel, sanal, bulut cihazları) dağıtılabilir.

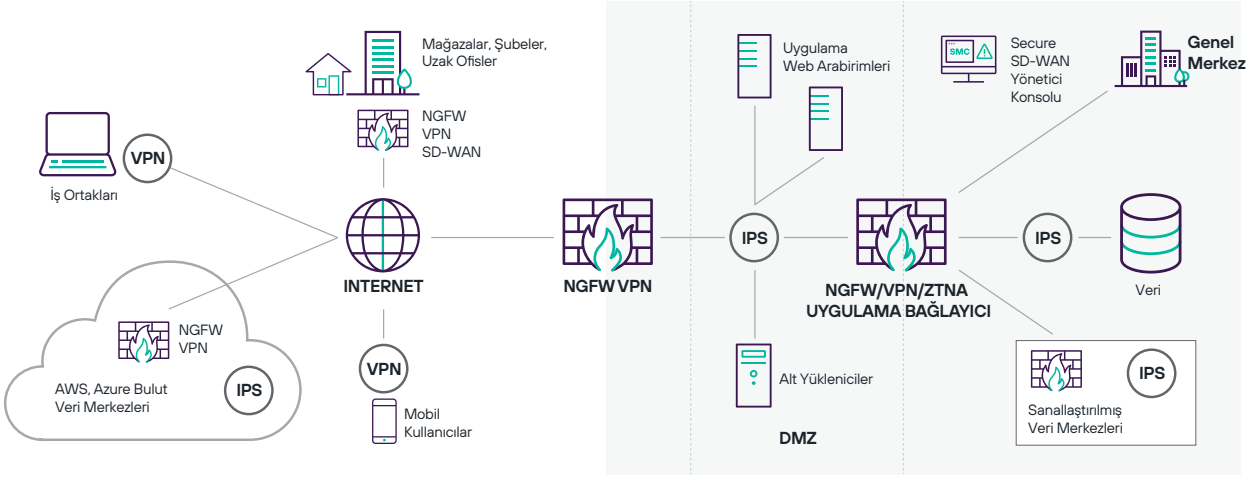
Forcepoint, yüksek performans ve güvenlik sunmak amacıyla her bağlantı için benzersiz bir şekilde erişim kontrolü ve derin denetim sağlar. Parçalı uygulama kontrolünü, IPS savunmalarını, yerleşik sanal özel ağ (VPN) kontrolünü ve görev açısından kritik uygulama vekil sunucularını verimli, genişletilebilir ve yüksek oranda ölçeklenebilir bir tasarımda bir araya getirir. Güçlü kaçınma önleme teknolojilerimiz, en gelişmiş saldırı yöntemlerini açığa çıkarmak ve engellemek için denetimden önce ve tüm protokol katmanlarında ağ trafiğini çözer ve normalleştirir.

Sofistike veri ihlali saldırılarını engelleyin

Büyük veri ihlalleri her sektördeki işletmeleri ve kuruluşları rahatsız ediyor. Uygulama katmanı sızma koruması ile bu tehditle mücadele edin. Forcepoint, son derece ayrıntılı uç nokta bağlamsal verilerine dayanarak PC'ler, dizüstü bilgisayarlar, sunucular, dosya paylaşımları ve diğer uç nokta cihazlarındaki belirli uygulamalardan kaynaklanan ağ trafiğine seçmeli ve otomatik olarak izin verir veya engeller. Tipik güvenlik duvarlarının ötesine geçerek, yetkisiz programlar, web uygulamaları, kullanıcılar ve iletişim kanalları aracılığıyla uç noktalardan hassas verilerin sızdırılma girişimlerini önler.

* "Forcepoint NGFW'ye Geçmenin Operasyonel ve Güvenlik Sonuçlarını Ölçümlendirme", R. Ayoub & M. Marden, IDC Research, Mayıs 2017.

Birçok dağıtım seçeneğine sahip tek bir platform—hepsi tek bir konsoldan yönetilir



Eşsiz koruma

Saldırganlar, kurumsal ağlara, uygulamalara, veri merkezlerine ve uç noktalara nüfuz etme konusunda uzmanlaştı. Bir kez içeri girdiklerinde fikri mülkiyet, müşteri bilgileri ve diğer hassas verileri çalarak işletmelere ve itibarlarına onarılamaz zararlar verir.

Yeni saldırı teknikleri, birçok tanınmış güvenlik duvarı ürünü de dahil olmak üzere geleneksel güvenlik ağı cihazları tarafından tespit edilmeyi atlatabilmekte ve böylece güvenlik açığı istismarlarının iletilmesinin önüne geçebilmektedir. Kaçınmalar, açıkları ve kötü amaçlı yazılımları kamufle etmek için birden fazla düzeyde çalışır ve bunları geleneksel imza tabanlı paket incelemesine karşı görünmez hale getirir. Yıllardır engellenen saldırılar bile iç sistemleri tehlikeye atacak saldırılarla yeniden paketlenebilir.

Forcepoint farklı bir yaklaşım benimser. Sektör lideri güvenlik motorumuz, ağ savunmasının üç kademesinde de çalışacak şekilde tasarlanmıştır: Kaçınmaları yenmek, güvenlik açıklarını tespit etmek ve kötü amaçlı yazılımları durdurmak. Kesinti olmadan koruma eklemek için mevcut güvenlik duvarlarının arkasına şeffaf bir şekilde veya hepsi bir arada güvenlik için tam özellikli bir Kurumsal Güvenlik Duvarı olarak dağıtılabilir.

Ek olarak, Forcepoint, HTTPS web bağlantıları da dahil olmak üzere şifrelenmiş trafiğin hızlı bir şekilde çözülmesini ve işletmenizi ve kullanıcılarınızı hızla değişen bir dünyada güvende tutan ayrıntılı gizlilik kontrolleriyle birlikte sunar. Cihazları kilitlemek veya savunmasız yazılımların kullanımını önlemek için belirli uç nokta uygulamalarından erişimi bile sınırlayabilir.

Ticari sonuçlar

- → Şubelerin, bulutların veya veri merkezlerinin daha hızlı kullanıma sunulması
- → Daha az kesinti
- → Kesinti olmadan daha fazla güvenlik
- → Daha az ihlal
- → BT ekipleri yeni düzeltme yamalarını dağıtmaya hazırlanırken yeni güvenlik açıklarına daha az maruz kalma
- → Ağ altyapısı ve güvenliği için daha düşük TCO

Başlıca özellikler

- → Kurumsal ölçekte SD-WAN bağlantısı
- → Web, bulut, özel uygulama güvenliği için SASE/SSE Entegrasyonu
- → Kaçınma önleme savunmalarına sahip yerleşik IPS
- → Cihazların ve ağların yüksek kullanılabilirlikte kümelendirilmesi
- → Otomatik, sıfır kesinti içeren güncellemeler
- → Politika odaklı merkezi yönetim
- → Eyleme dökülebilir, interaktif 360° görünürlük
- → Görev açısından kritik uygulamalar için Sidewinder güvenlik proxyleri
- → Kullanıcı ve uç nokta bağlamı
- → Granüler gizlilik kontrolleriyle yüksek performanslı şifre çözme
- → İstemci uygulamasına ve sürümüne göre izin verin/engelleyin
- → Uygulama durumunu izleme
- → CASB ve Web Güvenliği entegrasyonu
- → Kötü amaçlı yazılımlar için korumalı alan
- → Fiziksel, AWS, Azure, VMware dağıtımları için bütünleşik yazılım
- → BT ekipleri yeni düzeltme yamalarını dağıtmaya hazırlanırken yeni güvenlik açıklarına daha az maruz kalma
- → Ağ altyapısı ve güvenliği için daha düşük TCO

Forcepoint NGFW özellikleri

PLATFORMLAR	
Fiziksel Araç	Şube ofislerinden veri merkezi kurulumlarına kadar çok sayıda donanım cihazı seçeneği
Bulut Altyapısı	Amazon Web Services, Microsoft Azure, Google, Oracle, IBM
Sanal Cihaz	x86 64 bit tabanlı sistemler; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM ve Nutanix AHV
Uç Nokta	Uç Nokta Bağlam Aracısı (ECA), VPN İstemcisi
Sanal Bağlamlar	250'ye kadar
Merkezileştirilmiş Yönetim	Günlük analizi, izleme ve raporlama özelliklerine sahip kurumsal düzeyde merkezi yönetim sistemi. Ayrıntılar için Forcepoint Security Management Center veri sayfasına bakın.

GÜVENLİK DUVARI ÖZELLİKLERİ	
Derin Paket Denetleme	Çok Katmanlı Trafik Normalleştirme/Tam Akış Derin Denetleme, Kaçış Önleyici Savunma, Dinamik Bağlam Tespiti, Protokole Özel Trafik Yönetimi/Denetimi, SSL/TLS Trafiği Parçalı Şifre Çözme (TLS 1.2 ve 1.3 için), Güvenlik Açığı Suistimali Tespiti, Özel Parmak İzi Alma, Keşif, Anti-Botnet, Korelasyon, Trafik Kaydı, DoS/DDoS Koruma, Engelleme Yöntemleri, Otomatik Güncellemeler
Kullanıcı Tanımlama	Dahili kullanıcı veritabanı, Yerel LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, İstemci Sertifikaları
Yüksek Kullanılabilirlik	› 16 düğüme kadar aktif-aktif/aktif-bekleme güvenlik duvarı kümeleme › SD-WAN › Durum denetlemeli yük devri (VPN bağlantıları dahil) › Sunucu yükü dengeleme › Bağlantı birleştirme (802.3ad) › Bağlantı hatası tespiti
IP Adresi Uygulaması	› IPv4 statik, DHCP, PPPoA, PPPoE, IPv6 statik, SLAAC, DHCPv6 › Hizmetler: IPv4 ve IPv6 için DHCP sunucusu ve DHCP aktarıcısı
Yönlendirme	› Statik IPv4 ve IPv6 rotaları, politika tabanlı yönlendirme, statik çok noktaya yayın yönlendirmesi › Dinamik yönlendirme: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP vekil sunucusu › Uygulamaya duyarlı yönlendirme
IPv6	Çift yığınlı IPv4/IPv6, NAT64, ICMPv6, DNSv6, NAT, Tam NGFW özellikleri
Vekil Sunucu Yönlendirme	HTTP, HTTPS, FTP, SMTP protokollerinin şirket içi ve bulutta Forcepoint veya üçüncü taraf İçerik Denetleme Hizmetine (CIS) yönlendirilmesi
Coğrafi Koruma	Dinamik olarak güncellenen kaynak/hedef ülke veya kıta
IP Adresi Listesi	Önceden tanımlanmış IP kategorileri veya özel veya içe aktarılan IP adresi listelerini kullanarak
URL Filtreleme (Ayrı Abonelik)	Özel veya içe aktarılan URL listeleri; QUIC ve HTTP/3'ü destekler
Uç Nokta Uygulamaları	Uygulaması adı ve sürümü
Ağ Uygulamaları	7400+ ağ ve bulut uygulaması
Sidewinder Güvenlik Proxyleri	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS

SASE ENTEGRASYONU	
Web Trafiği Yönlendirme	Forcepoint ONE gibi Security Service Edge (SSE) platformlarına GRE ve IPsec tünelleme
ZTNA Application Connector	Dahili veri merkezlerindeki özel uygulamaların Forcepoint ONE'ın Zero Trust'ına bağlanmasını sağlar

SD-WAN	
Protokoller	IPsec ve TLS
Siteden Siteye VPN	› Politika ve rota tabanlı VPN › Toplama ve dağıtım, tam ağ, kısmi ağ, Hibrit topolojiler › Birden fazla ISP Bağlantısı için dinamik seçim › Yük paylaşımı, aktif/bekleme, bağlantı birleştirme › ISP'lerde bağlantı kalitesini canlı izleme ve raporlama (Gecikme, titreme, paket kaybı)
Uzaktan Erişim	› Microsoft Windows, Android ve Mac OS için Forcepoint VPN istemcisi › Herhangi bir standart IPsec istemcisi › Otomatik yük devri ile yüksek kullanılabilirlik › Müşteri güvenliği kontrolleri › TLS VPN portalına erişim

GELİŞMİŞ KÖTÜ AMAÇLI YAZILIM TESPİTİ VE DOSYA KONTROLÜ	
Protokoller	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
Dosya Filtreleme	Verimli aşağı seçim süreciyle politika tabanlı dosya filtreleme. 19 dosya kategorisinde 200'den fazla desteklenen dosya türü
Dosya Bilinirliği	Yüksek hızlı bulut tabanlı kötü amaçlı yazılım bilinirliği kontrolü ve engelleme
Anti-Virüs	Yerel antivirüs taraması motoru*
Sıfırıncı Gün Sandboxing Sistemi	Forcepoint Gelişmiş Kötü Amaçlı Yazılım Algılama ve Koruması hem bulut hem de şirket içi hizmet olarak mevcuttur

* Yerel kötü amaçlı yazılımlara karşı tarama 110/115 cihazlarda kullanılamaz.