Forcepoint

Çözüm Özeti

Forcepoint Next Generation Firewall ve Microsoft Azure

En güvenli ve etkili kurumsal güvenlik duvarı - merkezi yönetimli, her zaman açık ve amansız

Sorun

- Şirketlerin ve kurumların, bulut ve karma ortamlarda, geleneksel şirket içi altyapılarla aynı güvenlik seviyesini sürdürmeleri gerekir.
- Güvenli bir bulut altyapısı veya karma altyapı oluşturmak ve sürdürmek masraflı olabilir ve teknik zorluklar arz edebilir
- Düzenlemelere uyum zor olabilir ve teknik zorluklar arz edebilir

Çözüm

- Forcepoint Next Generation Firewall, minimum maliyet ve karmaşıklıkla maksimum güvenlik sağlamak üzere benzersiz bir şekilde tasarlanmış, yazılım tabanlı bir çözüm sunar
- Forcepoint Güvenlik Yönetimi Merkezi (SMC), ekiplerin binlerce güvenlik duvarını yönetmesini, süreçleri kolaylaştırmasını sağlar ve detaylı kontrollerle rakipsiz bir görünürlük sunar
- Çözümümüz, denetim raporlarına kolay erişim dahil olmak üzere sanal ve fiziksel ağlarda mevzuata uyum sağlanmasına imkan tanıyan hazır politikalar sunarak uyum çalışmalarını kolaylaştırır

Sonuç

- Minimum karmaşayla maksimum bulut ve karma ağ güvenliği
- Hızlandırılmış olay müdahaleleri
- Kolaylaştırılmış mevzuat uyumu, uygulama ve yönetimi
- Ağ altyapısı ve güvenlik için daha düşük toplam sahip olma maliyeti (TCO)

Forcepoint Next Generation Firewall zorlu ve dağınık kurumsal ağları bağlar ve korur Sıfır müdahaleli esnek kurulumlar ve ağ güvenliği konusundaki Sıfır Güven yaklaşımı, uç noktalarınızı korumak için ihtiyaç duyduğunuz etkinliği, güvenilirliği ve yüksek güvenlik verimliliğini sunar.

Dünya çapında binlerce müşterinin güvendiği ve Microsoft Azure pazar yeri üzerinden ulaşılabilen Forcepoint ağ güvenliği çözümleri, kurumların kritik sorunları etkin ve ekonomik bir şekilde ele almasını ve dolayısıyla ihlallere maruz kalmaktan kaçınmasını sağlar.

Halka Açık Bulut Ortamları için Forcepoint Güvenliği

Bulut tabanlı hizmetler ve sanal uygulamalar, her tür ve boyuttaki işletmeleri dönüştürüyor. Kurumlar, bakım ve genel masrafların getirdiği yükle uğraşmadan daha yüksek verim, çeviklik ve maliyet kontrolüne ihtiyaç duyduklarından, geleneksel şirket içi donanımlar hızla ortadan kaybolmakta. Forcepoint, müşterilerimizin rekabetçi kalmasına yardımcı olmak için stratejik olarak ağ güvenliği çözümlerimizi yazılım merkezli olacak şekilde tasarlanmıştır, dolayısıyla buluta geçiş yaptığınızda bu çözümleri kullanmaya devam edebilirsiniz. Bulut mimarilerinin geniş çaplı olarak benimsenmesi, güvenlik uzmanlarına ve BT liderlerine bu yeni ortamların fiziksel öncüleri kadar güvenli olmasını sağlamak gibi bir ek sorumluluk yükler.

Forcepoint Next Generation Firewall yazılım tabanlı çözümleri, minimum maliyet ve karmaşıklıkla maksimum güvenlik sağlamak üzere benzersiz bir şekilde tasarlanmıştır. Güvenlik Yönetimi Merkezimiz (SMC), fiziksel, sanal ortamlarda ve bulut ortamlarında mevzuata uymanızı sağlayan benzersiz bir görünürlük, kontrol ve tutarlı politika uygulamaları sağlayan birleşik bir platformdur.

Microsoft Azure Bulut Güvenliği

Forcepoint, bulut ortamlarında güvenliği sağlamak için ölçeklenebilirliği, operasyon verimi ve güvenliği kanıtlanmış, önde gelen yeni nesil güvenlik duvarı teknolojisini Azure'a taşıyor. Güvenli bir Sanal Özel Ağ (VPN) ağ geçidiyle veri merkezlerinden ve ağ uç noktalarından şubelere ve uzak tesislere kadar tüm kurumsal ağınızı kolayca ve güvenli bir şekilde Azure bulut ortamınıza taşıyın. Merkezi yönetimimiz, tüm sistemleriniz için politikaları hızla ve tutarlı bir şekilde oluşturup uygulayabilmenizi sağlamaktadır. Hem Azure ortamınızda hem de fiziksel ağınızda olup bitenleri hızla görebilirsiniz.

Forcepoint Next Generation Firewall'a geçen müşteriler, siber saldırılarda %86, BT üzerindeki iş yükünde %53 ve planlı bakım çalışmalarında %70 düşüş olduğunu bildiriyor.

Maksimum Güvenlik, Minimum Karmaşıklık

Forcepoint'in gelişmiş tehdit koruması, derin paket denetleme ve uygulama seviyesinde kontrol gibi güvenlik çözümlerinin yazılım tabanlı mimarisi, şirket içinde, sanal ortamda veya bulutta maksimum güvenlik sağlamak üzere kolayca kurulup uygulanacak şekilde tasarlanmıştır. Detaylı kullanıcı, uygulama ve protokol kontrolleri, güvenlik ekibinizin otomasyonun gücünden faydalanarak karmaşıklığı ve sıradan güvenlik hijyen görevlerine harcanan zamanı en aza indirmesini sağlamaktadır. Forcepoint'in kapsamlı ve entegre derinlemesine koruma yaklaşımı, tek veya çok sayıda güvenlik duvarı, VPN, IPS ve URL filtreleme koruması dahil olmak üzere her bir kişi, yer veya varlığın özel ihtiyaçlarına göre kişiselleştirilebilir. Kapsamlı yeni nesil güvenlik duvarımız, herhangi bir donanıma ihtiyaç duyulmadan, durum denetimi, detaylı politikalar ve erişim kontrolü ve yedek ISP bağlantıları da dahil olmak üzere gelişmiş bir donanım cihazındaki tüm özellikleri sunmaktadır.

Gerçek Zamanlı Görünürlük ve Kontrol

Forcepoint Next Generation Firewall, hem sanal ortamlarda hem de bulut ortamındaki trafik akışı üzerinde geleneksel yönetim konsollarının sağlayamadığı eksiksiz görünürlük ve kontrol sağlamaktadır. Ünlü SMC çözümümüz, hızlı raporlamanın yanı sıra sistem çökmek üzere olduğunda yöneticileri uyaran otomatik devir özelliklerini sunmakta ve kullanıcı deneyiminde kesintiler olmasını önlemek için önceden yapılandırılmış kurallara göre otomatik kararlar alabilmektedir. İstediğiniz sayı veya kombinasyondaki fiziksel veya sanal Forcepoint cihaz veya kümelerinin yanı sıra standart x86 donanım üzerinde çalışan yazılım tabanlı sürümleri de yönetin. SMC ayrıca tüm güvenlik uygulamaları üzerinde tam görünürlük ve detaylı kontrol sağlayan bütünsel bir takip panosuyla sanal sistem güvenliğini de artırır.

Düzenlemelere Uyumu Basitleştirin

Fiziksel dünyada PCI DSS, HIPAA, Sarbanes-Oxley ve FISMA gibi en son yasal düzenlemelere uyum sağlamak zor olsa da dijital ortamda uyumu sürdürmek daha da zordur. Uygulamalar için kullanılan geleneksel kontroller, sanal ortamlarda mevcut değildir. Bu da hangi bilgilere kimlerin, ne zaman eriştiğini belirlemeyi neredeyse imkansız hale getirir ve denetmenler için bir ikaz işareti oluşturabilir. Forcepoint SMC, sanal ve fiziksel ağlarda düzenlemelere uyum sağlayabilmeniz için ihtiyaç duyduğunuz takip, analiz ve raporlama seviyesini sunar. Tüm ağ olayları hakkında kapsamlı veriler toplar ve bu verileri açık ve kolayca anlaşılan denetim kayıtları şeklinde sunar. SMC, ayrıca tek bir düğmeye bastığınızda güvenlik ayarlarını listeler, sistem değişikliklerini bildirir ve ihtiyaç duyduğunuz doğru denetim raporlarını sunar.

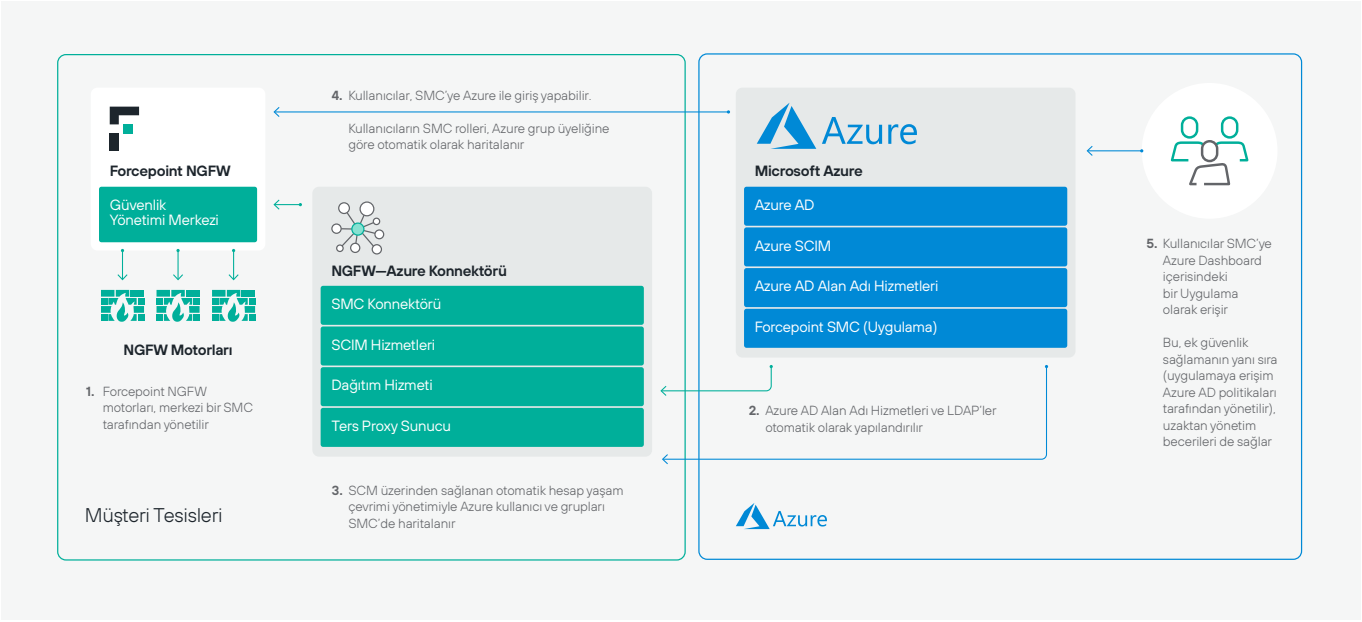
Hızlı ve Esnek Dağıtım

Forcepoint Next Generation Firewall'u Microsoft Azure ortamınızda kolayca kurmak için Microsoft Azure Pazar Yerini ziyaret edin.

→ Pazar Yerini Ziyaret Edin

Forcepoint Next Generation Firewall ve Microsoft Azure Çözümleri

Benzersiz entegrasyonlarımız sayesinde Azure yatırımınızdan maksimum fayda sağlayın ve Forcepoint çözümlerinizin yeteneklerini artırın. Adım adım uygulama talimatları da dahil olmak üzere entegrasyonlarımız hakkında daha fazla ayrıntı için: forcepoint.github.io



Azure Active Directory (AD) - Güvenli Karma Erişim Entegrasyonu

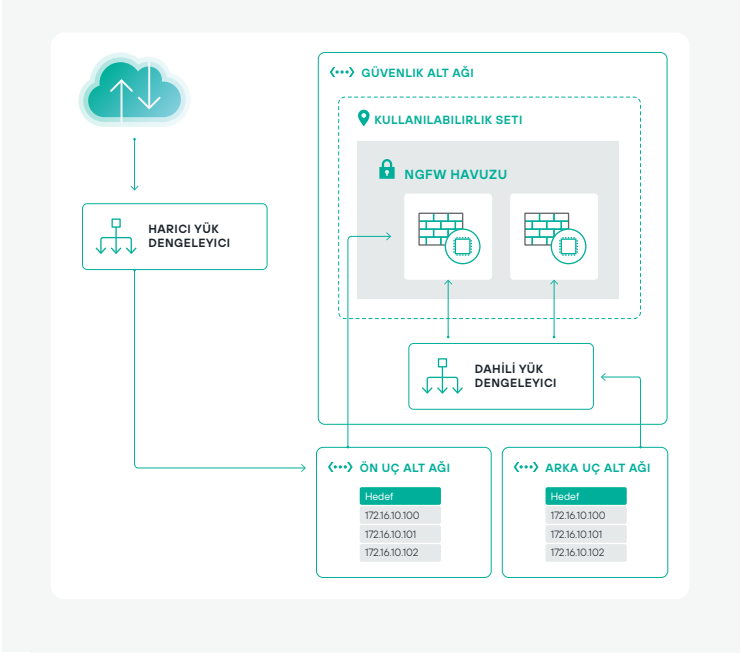
Azure AD kullanıcıları ve politikaları üzerinden Forcepoint SMC erişimi ve kimlik doğrulaması sağlar.

- → SMC'nin uzaktan yönetim özellikleri için bir Azure uygulaması olarak kullanılmasını sağlar
- → Seçilen Azure AD kullanıcılarına SMC içerisinde farklı erişim seviyeleri atanarak, tüm Yeni Nesil Güvenlik Duvarı motorları filosunda pek çok farklı uzaktan yönetim senaryosu uygulanabilir
- → Azure AD kimlik doğrulama politikalarının sağladığı ek güvenlikle SMC içerisinde merkezi yönetim ve kontrol sağlar

Azure Resource Manager (ARM) Entegrasyonuyla Yüksek Kullanılabilirlik Oranı

Tüm yapıyı kurmak için yapılandırılan bir ARM şablonundan faydalanarak Azure'da yedek bir Yeni Nesil Güvenlik Duvarı motorları setinin kurulmasını otomatik hale getirir.

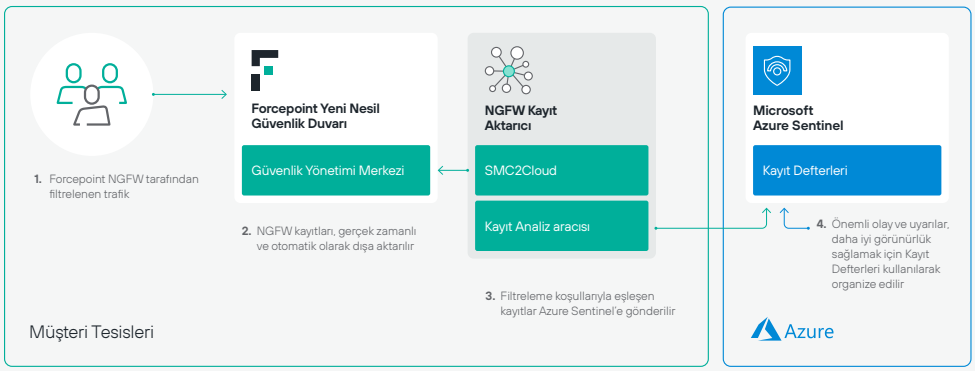
- → Dahili ve harici ağlar arasındaki trafiği yönetmek için 2 ağ yükü dengeleyici ve 3 alt ağ içeren bir yapıyı kurmak amacıyla yapılandırılan bir ARM şablonu
- → Kullanıcılar ve iş yükleri arasında kesintisiz bir ağ akışı sağlamak amacıyla Yeni Nesil Güvenlik Duvarı motorlarının yüksek kullanılabilirlik modunda çalışmasını sağlar



Azure Sentinel Entegrasyonu

Kullanıcı tarafından yapılandırılan filtrelere göre Yeni Nesil Güvenlik Duvarındaki ilgili kayıt verilerinin dışa aktarılmasını sağlar.

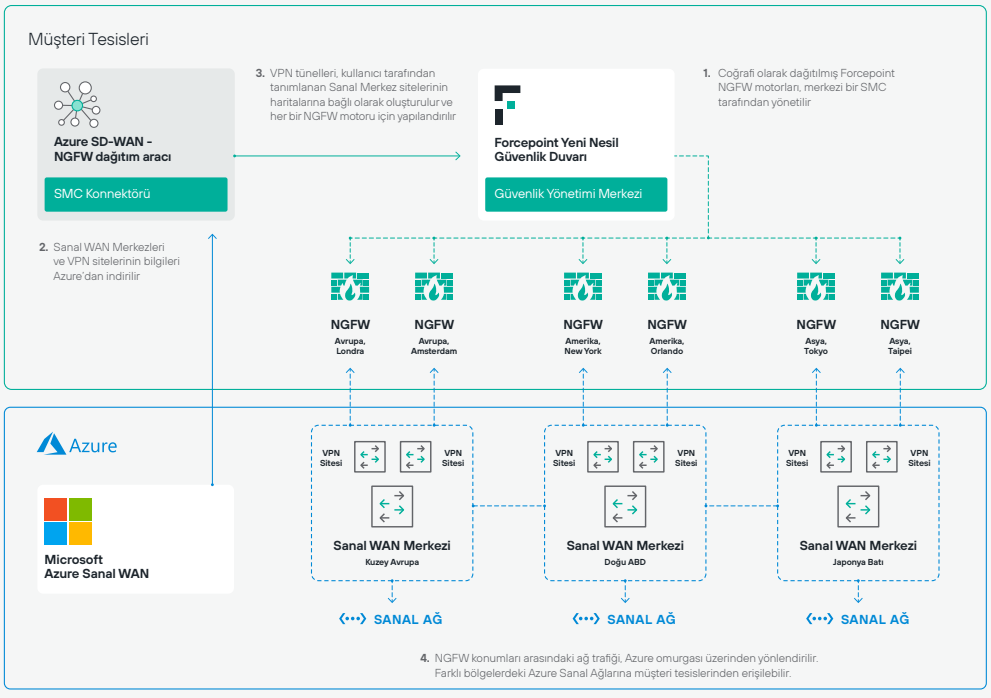
→ Forcepoint Yeni Nesil Güvenlik Duvarındaki olay kayıtlarını otomatik ve gerçek zamanlı olarak Azure Sentinel'e aktarın.
→ Kayıtları Azure Sentinel kayıt analizi özelliğiyle okuyun ve olayları Kayıt Defterlerini kullanarak görselleştirin



Azure Sanal WAN Entegrasyonu

Forcepoint SMC tarafından kontrol edilen bir Yeni Nesil Güvenlik Duvarı motorları filosuyla coğrafi Sanal WAN siteleri arasındaki IPsec tünellerinin otomatik olarak oluşturulup yapılandırılmasını sağlar.

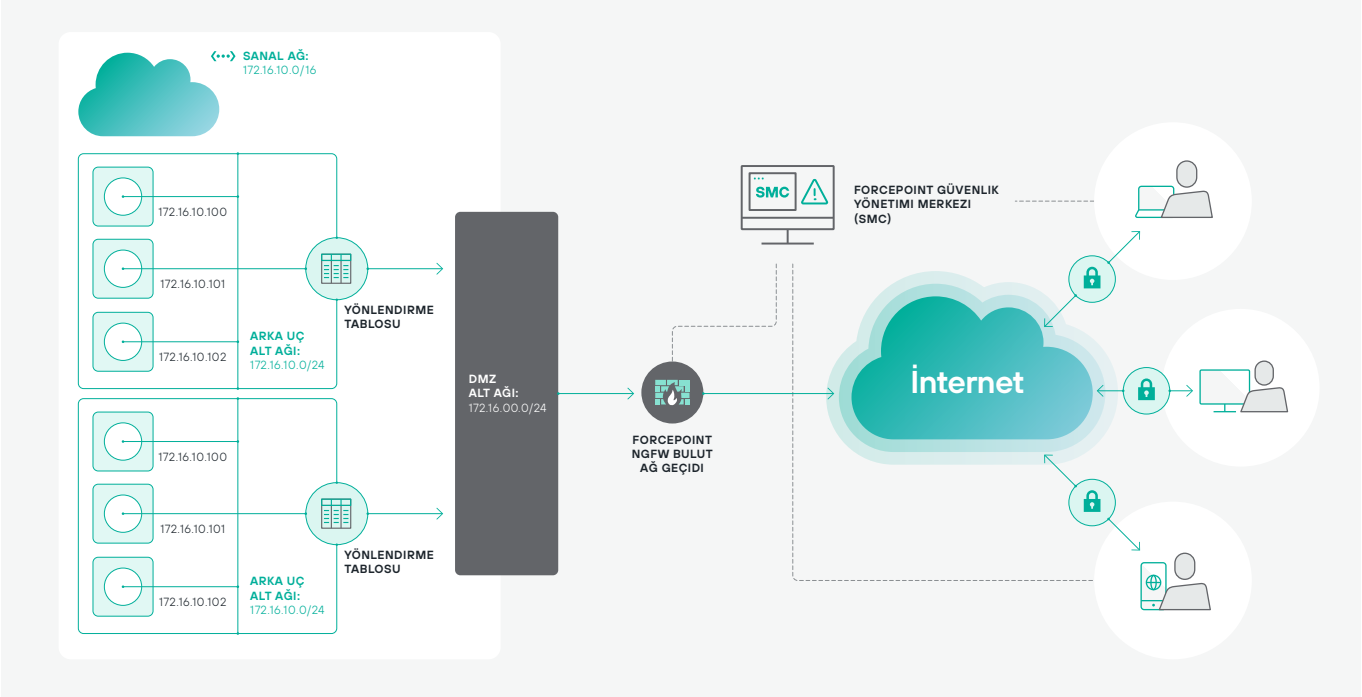
→ Azure Sanal WAN omurgası üzerinden siteler arasındaki trafiği yönlendirmek için kullanılabilecek bir SD-WAN katmanı oluşturur
→ Yöneticilerin, IPsec standardını kullanarak SMC tarafından kontrol edilen her Yeni Nesil Güvenlik Duvarı motorunda yedek VPN tünelleri oluşturmasını sağlar
→ Her bir Yeni Nesil Güvenlik Duvarı motorundaki VPN tünellerinin belirtilen Azure Sanal WAN bölgelerine bağlanmasını sağlar

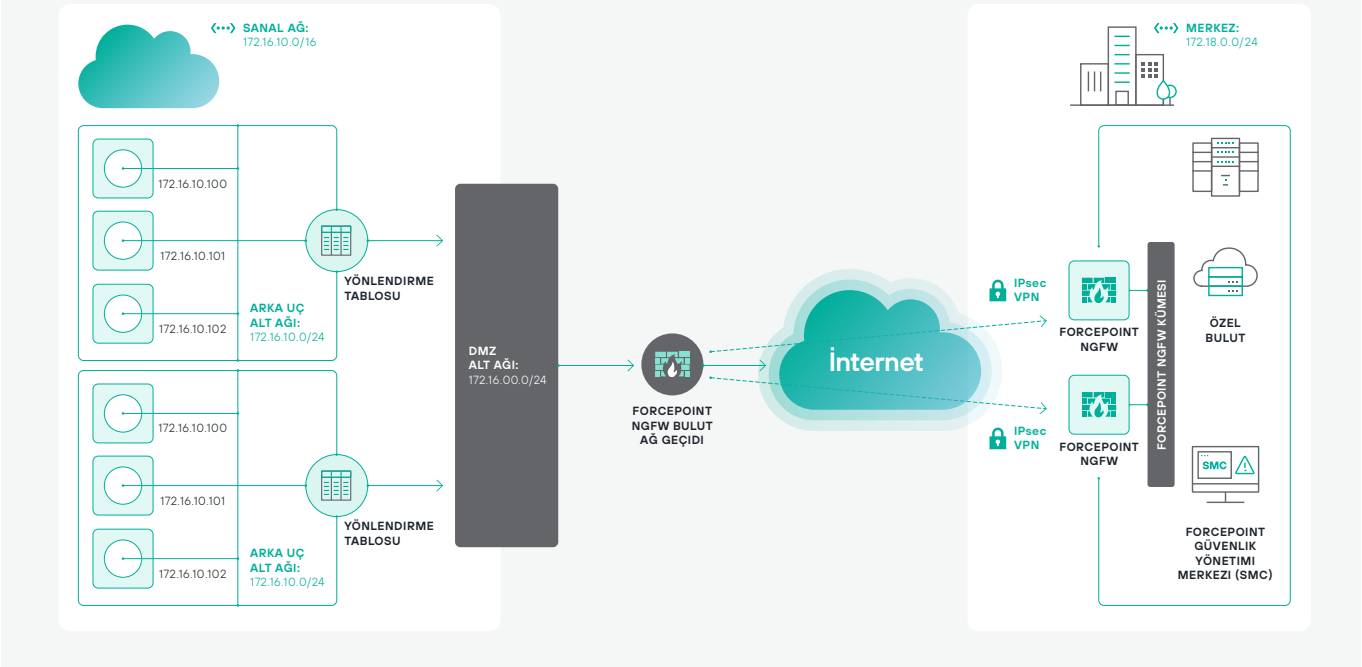


Kurumsal Veri Merkezi Bağlantıları

Forcepoint Next Generation Firewall fiziksel ve sanal ağ geçitleri, şirket içi veri merkezlerinizin, Azure bulutunda bulunan sanal veri merkezlerine güvenle bağlanmasını sağlar. Bu kullanım şekliyle şunları yapabilirsiniz:

- → Veri merkezi ağınızla Azure sanal ağınızda çalışmakta olan Forcepoint yazılım tabanlı VPN uygulaması arasında bir veya daha fazla VPN bağlantısı oluşturmak
- → SMC üzerinden hem yazılım tabanlı hem de fiziksel Forcepoint güvenlik duvarlarınızın tamamını VPN bağlantılarının her iki ucunda da yönetmek ve kontrol etmek
- → VPN bağlantısının merkez ofis tarafında iş sürekliliğinin sağlanması için, arıza durumunda devir amacıyla fiziksel güvenlik duvarlarından oluşan bir küme de kullanabilirsiniz.





Bölgeler arası VNET'ten VNET'e yönlendirme

Çok sayıda Azure bulut bölgesi içindeki ve arasındaki sanal ağları birbirine bağlamak için iki veya daha fazla Forcepoint yazılım tabanlı VPN uygulaması arasında güvenli VPN tünelleri oluşturun. Bu kullanım şekliyle şunları yapabilirsiniz:

→ Forcepoint SMC kullanarak, VPN bağlantılarının her iki ucunda da güvenlik politikalarını yönetmek, kontrol etmek ve uygulamak