VMWARE NSX

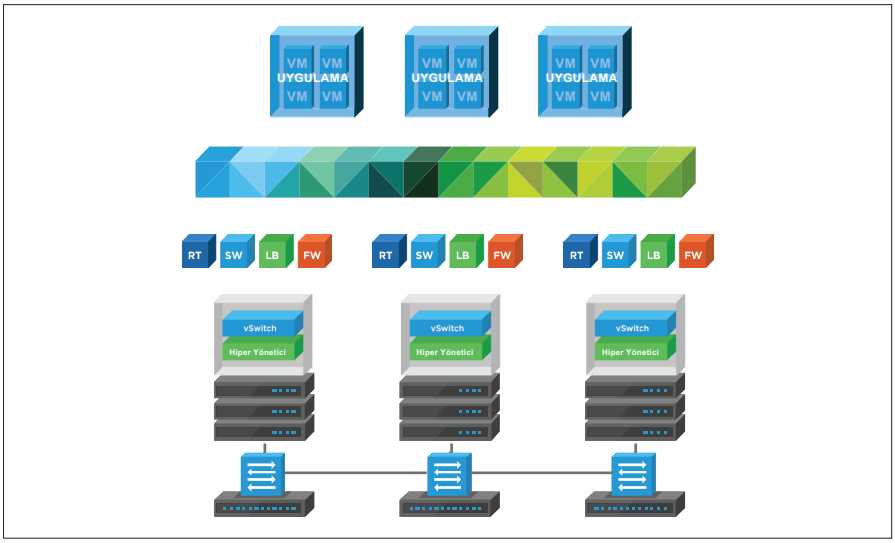
Ağ Sanallaştırma ve Güvenlik Platformu

BİR BAKIŞTA

VMware NSX®, Yazılım Tanımlı Veri Merkezi (SDDC) için ağ sanallaştırma ve güvenlik platformudur ve tüm ağlar için bir sanal makinenin işletim modelini sunar. NSX ile, anahtarlama, yönlendirme ve güvenlik duvarı dahil olmak üzere ağ işlevleri, hiper yöneticiye eklenir ve ortam genelinde dağıtılır. Bu, sanal ağ ve güvenlik hizmetleri için bir platform görevi gören bir "ağ hiper yöneticisi"ni etkili bir şekilde oluşturur. Sanal makinelerin işletim modeline benzer şekilde, sanal ağlar programlı olarak sağlanır ve temel donanımdan bağımsız olarak yönetilir. NSX, tüm ağ modelini yazılım içinde yeniden oluşturarak, basit ve karmaşık çoklu iletişim ağları dahil herhangi bir ağ topolojisinin saniyeler içinde oluşturulmasını ve sağlanmasını mümkün kılar. Kullanıcılar, daha güvenli ortamlar oluşturmak için NSX aracılığıyla sunulan hizmetlerin bir kombinasyonundan yararlanarak çeşitli gereksinimlere sahip birden çok sanal ağ oluşturabilir.

TEMEL AVANTAJLARI

- Münferit iş yükü için sağlanan mikro segmentasyon ve parçalı güvenlik
- Otomasyon yoluyla günlerden saniyelere düşen azaltılmış ağ sağlama süresi ve daha iyi işletim verimliliği
- Veri merkezleri içinde ve arasında fiziksel ağ topolojisinden bağımsız iş yükü mobilitesi
- Önde gelen üçüncü taraf sağlayıcıların ekosistemi aracılığıyla iyileştirilmiş güvenlik ve gelişmiş ağ hizmetleri



Ağ Sanallaştırma, Güvenlik ve SDDC

VMware NSX, Yazılım Tanımlı Veri Merkezinin temelini oluşturan ağ iletişimi için tamamen yeni bir işletim modeli sunar. NSX, ağları yazılımlarda kurduğundan, veri merkezi operatörleri daha önce fiziksel ağlarda ulaşılamamış olan çeviklik, güvenlik ve ekonomi düzeylerine ulaşabilirler. NSX, mantıksal anahtarlama, yönlendirme, güvenlik duvarı oluşturma, yük dengeleme, VPN, hizmet kalitesi (QoS) ve izleme dahil olmak üzere eksiksiz bir dizi mantıksal ağ elemanı ve hizmeti sunar. Bu hizmetler, NSX API'lerini kullanan herhangi bir bulut yönetim platformu aracılığıyla sanal ağlarda sağlanır. Sanal ağlar, mevcut herhangi bir ağ donanımı üzerinde kesilmeden dağıtılır.

NSX'in Temel Özellikleri

Anahtarlama	Veri merkezi sınırları içinde ve arasında yönlendirilmiş (L3) bir yapı üzerinde mantıksal katman 2 yer paylaşımı eklentilerini etkinleştirir. VXLAN tabanlı ağ yer paylaşımları için destek.
Yönlendirme	Hiper yönetici çekirdeğinde dağıtılmış bir şekilde sanal ağlar arasında gerçekleştirilen dinamik yönlendirme, fiziksel yönlendiricilerle aktif-aktif yük devretme ile ölçek genişletme yönlendirmesi. Statik yönlendirme ve dinamik yönlendirme (OSPF, BGP) protokolleri desteklenir.
Dağıtılmış Güvenlik Duvarı Oluşturma	Hiper yönetici ana bilgisayar başına 20 Gbps'ye kadar güvenlik duvarı kapasitesi için hiper yönetici çekirdeğine eklenmiş, durum bilgisi içeren, dağıtılmış güvenlik duvarı. Active Directory ve etkinlik izleme desteği. Ayrıca NSX, NSX Edge™ aracılığıyla kuzey-güney güvenlik duvarı kapasitesi de sağlayabilir.
Yük Dengeleme	SSL yük boşaltma ve doğrudan geçiş, sunucu sistem durumu denetimleri, programlanabilirlik ve trafik manipülasyonu için Uygulama Kurallarına sahip L4 – L7 yük dengeleyici.

VPN	Siteden siteye ve uzaktan erişim VPN özellikleri, bulut ağ geçidi hizmetleri için yönetilmeyen VPN.
NSX Ağ Geçidi	Fiziksel iş yüklerine sorunsuz bağlantı için VXLAN ile VLAN köprüleme desteği. Bu özellik, NSX'e özgüdür ve bir ekosistem ortağının sunduğu raf üstü anahtarları tarafından sağlanır.
NSX API	Herhangi bir bulut yönetimi platformuna veya özel otomasyona entegrasyon için RESTful API.
Operasyonlar	Sorun gidermek ve altyapıyı proaktif olarak izlemek için merkezi komut satırı arabirimi, iz akışı, SPAN ve IPFIX gibi yerel operasyon özellikleri. Gelişmiş analiz ve sorun giderme için VMware vRealize® Operations™ ve vRealize Log Insight™ gibi araçlarla entegrasyon. NSX Uygulama Kural Yöneticisi ve Uç Nokta İzleme, uygulama ekiplerinin hem intra hem de iç veri merkezi uç noktalarını tanımlamasına ve uygun güvenlik kurallarını oluşturarak yanıt vermesine olanak sağlayan, Katman 7'ye kadar uçtan uca ağ trafik akışı görselleştirmesine imkan verir.
Bağlama Duyarlı Mikro Segmentasyon	NSX, uygulamanın içeriğine göre mikro segmentasyon yapılabilmesi için, dinamik güvenlik gruplarının ve ilgili ilkelerin sadece IP adresi ve MAC'e göre değil, VMware vCenter™ nesneleri ve etiketleri, işletim sistemi türü ve Katman 7 uygulama bilgisi dahil olmak üzere diğer faktörlere göre oluşturulmasını sağlar. VM'lerden, Active Directory'den ve Mobil Aygıt Yönetimi entegrasyonundan gelen giriş bilgilerini kullanan kimlik temelli ilke, uzak ve sanal masaüstü ortamlarında oturum düzeyinde güvenlik dahil olmak üzere kullanıcıyı baz alan güvenlik sağlar.
Bulut Yönetimi	vRealize Automation™ ve OpenStack ile yerel entegrasyon.
Üçüncü Taraf Ortak Entegrasyonu	Yeni nesil güvenlik duvarı, IDS/IPS, aracısız antivirüs, uygulama teslim denetleyicileri, anahtarlama, operasyonlar ve görünürlük, gelişmiş güvenlik ve daha fazlası gibi çok çeşitli kategorilerde yönetim ve üçüncü taraf ortaklarla kontrol düzlemi ve veri düzlemi entegrasyonu desteği.
Çapraz vCenter Ağ İletişimi ve Güvenlik	Temel fiziksel topolojiden bağımsız olarak vCenter ve veri merkezi sınırları genelinde ağ ve güvenliği genişleterek, olağanüstü durum kurtarma ve aktif-aktif veri merkezleri gibi özellikleri etkinleştirir.
Günlük Yönetimi	vRealize Log Insight for NSX'ten gelen ek görünürlük ile sorunların daha hızlı çözülmesine yardımcı olur. Etkinlik eğilimlerini, tetik uyarılarını ve daha fazlasını gerçek zamanlı olarak görselleştirir.

Kullanım Durumları

Güvenlik

NSX, kurumların veri merkezini, iş yükünün ağ alt ağından veya VLAN'dan bağımsız olarak, münferit iş yükü seviyesine kadar, mantıksal şekilde farklı güvenlik bölümlerine ayırmalarına olanak tanır. BT ekipleri daha sonra dinamik güvenlik gruplarına göre her iş yükü için güvenlik ilkelerini ve denetimlerini tanımlayabilir, bu da veri merkezi içindeki tehditlere anında yanıt vermeyi ve münferit sanal makineye kadar zorlama yapılmasını sağlar. Geleneksel ağlarda olduğundan farklı şekilde, bir saldırgan veri merkezi çevre savunmasını ele geçirirse tehditler veri merkezi içinde yana doğru hareket edemez.

Otomatikleştirme

NSX, iş gücü ihtiyacı yüksek, hataya açık görevleri otomatikleştirerek uzun ağ sağlama, yapılandırma hataları ve maliyetli işlemlerin çıkardığı zorluğu ortadan kaldırır. NSX, ağları yazılımda oluşturur ve donanım tabanlı ağlarla ilişkilendirilen çıkmazları ortadan kaldırır.

NSX'in vRealize Automation veya OpenStack gibi bulut yönetim platformlarıyla yerel entegrasyonu daha fazla otomasyon sağlar.

Uygulama Sürekliliği

NSX, ağ oluşturmayı temeldeki donanımdan soyutladığından, ağ ve güvenlik politikaları ilişkili iş yüklerine eklenmektedir. Kuruluşlar, tüm uygulama ortamlarını olağanüstü durum kurtarma için uzak veri merkezlerine kolayca çoğaltabilir, bunları bir kurumsal veri merkezinden diğerine taşıyabilir veya hibrit bulut ortamına dağıtabilir, üstelik tamamı birkaç dakika içinde, uygulamaları kesmeden ve fiziksel ağa dokunmadan yapılabilir.

VMware NSX Sürümleri

Standard

Ağda çevikliğe ve otomasyona ihtiyaç duyan kuruluşlar için

Advanced

Standard sürümünün yanı sıra mikro segmentasyonla birlikte daha güvenli bir veri merkezine gereksinim duyan kuruluşlar için

Enterprise

Advanced sürümün yanı sıra birden çok etki alanında ağ iletişimine ve güvenliğe gereksinim duyan kuruluşlar için

ROBO

Uzak ofis veya şubede uygulamaları sanallaştırmak ve güvenli hale getirmek isteyen kuruluşlar için

DAHA FAZLA BİLGİ

Daha fazla bilgi için www.vmware.com/go/nsx adresini ziyaret edin.

NSX lisansı sürüm özellikleri hakkında daha fazla ayrıntıyı https://kb.vmware.com/kb/2145269 adresinde bulabilirsiniz.

Tüm VMware ürünleri hakkında daha fazla bilgi almak veya alışveriş yapmak için 877-4-VMWARE numaralı telefonu arayın (Kuzey Amerika dışındaysanız +1-650-427-5000 numaralı telefonu arayın), www.vmware.com/tr/products adresini ziyaret edin ya da internette yetkili bir satıcı bulun.

	STANDARD	ADVANCED	ENTERPRİSE	ROBO
Dağıtılmış Anahtarlama	•	•	•	•*
Dağıtılmış Yönlendirme	•	•	•	
NSX Edge güvenlik duvarı	•	•	•	•
NAT	•	•	•	•
Fiziksel ortama köprü oluşturan yazılım L2	•	•	•	
ECMP ile dinamik yönlendirme (aktif-aktif)	•	•	•	•
API temelli otomasyon	•	•	•	•
vRealize ve OpenStack ile entegrasyon	•	•	•	•
vRealize Log Insight for NSX ile günlük yönetimi	•	•	•	•
vRealize ile güvenlik ilkelerinin otomasyonu		•	•	•
NSX Edge yük dengeleme		•	•	•
Dağıtılmış güvenlik duvarı oluşturma (Active Directory ile entegrasyon dahil)		•	•	•
Sunucu etkinliği izleme		•	•	•
Servis ekleme (üçüncü taraf entegrasyonu)		•	•	•
VMware AirWatch® ile entegrasyon		•	•	•
Uygulama Kural Yöneticisi		•	•	•
Çapraz vCenter NSX			•	
Çoklu site NSX optimizasyonları			•	
VPN (IPSEC ve SSL)			•	•
Uzak ağ geçidi			•	
Donanım VTEP'leri ile entegrasyon			•	
Uç Nokta İzleme			•	
Katman 7 ile dağıtılmış güvenlik duvarı oluşturma			•	

*VLAN destekli

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 ABD Tel 877-486-9273 Faks 650-427-5001 www.vmware.com