**40**

**VPN Dağıtım ve**

**Değerlendirme Stratejisi**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Keith Pasley, CISSP**

VPN teknolojisi son yıllarda performans, kullanım kolaylığı, dağıtım ve yönetim aracı etkinliği alanlarında hızla gelişmiştir. Sanal özel ağ (VPN) teknolojisi için pazar talebi de hızla artmaktadır. Benzer şekilde, farklı VPN ürünlerinin sayısı artıyor. Maliyet tasarrufu vaadi yerine getiriliyor. Ancak, VPN’lere hem teknik hem de ticari açıdan yaklaşan yeni bir söz var. Günümüzün hızlı tempolu iş ortamında, VPN sistemlerinin yönetim kolaylığı, konuşlandırıla bilirlik ve ölçeklenebilirlik vaadi, doğru VPN sisteminin seçilmesi ve uygulanmasında kritik başarı faktörleridir. İş açısından bakıldığında, elde edilen faydalar şunları içerir:

* Muhataplar ve müşterilerle daha yakın ilişkiler kurarak rekabet avantajı
* Yeni hizmet sunumu kanalları
* Daha az maliyetle yeni pazarlara ulaşmak
* Bu çabayı engelleyen güvenlik kaygılarının giderilmesiyle daha değerli bilgiler sunmak.

Bu kadar çok seçenekle, kişi en uygun olanı nasıl belirler? Satıcı ürünü taleplerinin adil bir şekilde değerlendirilebilmesi için nesnel kriterlere ihtiyaç vardır. Satıcı ürünü taleplerinin adil bir şekilde değerlendirilmesini yapmak için nesnel ölçütler gerekli mi? VPN sistemlerine başka ne değer katabilir? Bazı durumlarda, yönetilen bir güvenlik servis sağlayıcısına dış kaynak kullanımı bir seçenektir. Yönetilen güvenlik servis sağlayıcıları, genellikle güvenlik uygulamalarını barındıran ve barındırılan güvenlik uygulamasının işlem tabanlı kullanımını sunan servis dış kaynak sağlayıcılarıdır. Artık birçok işletme, VPN'leri dağıtım ve yönetim sağlayabilen yönetilen güvenlik hizmeti sağlayıcılarına dış kaynak sağlamayı düşünüyor. Algı, yönetilen servis sağlayıcıların, büyük ölçekli VPN'leri şirket içi personelden daha iyi işletecek uzmanlık ve yönetim altyapısına sahip olmasıdır.

VPN performansı, VPN ürünlerinin daha yeni sürümlerinde sürekli olarak iyileşmiştir. Performans önemli olmasına rağmen, bir VPN çözümü seçiminde en önemli kriter bu mu? Hayır. Hızlı ama sömürülebilir bir VPN uygulama güvenliği geliştirmeyecektir. Performansı değerlendirmek de zordur ve birçok performans Testler gerçek dünyadaki durumları taklit eden kötü bir iş yapıyor. Satıcı performans talepleri, gerçek dünyadaki uygulamalarda göze çarpmayan aşırı iyimser pazarlama odaklı performans iddiaları nedeniyle çok yakından değerlendirilmelidir. Bu gibi performans taleplerinin temeli olarak satıcılar tarafından kullanılan test metodolojilerini anlamak önemlidir.

Bu bölüm, bilgi güvenliği uzmanlarının ne zaman karşılaştığı sorunlara cevaplar sunar.ürünleri seçmek ve VPN uygulamak.

**VPN Nedir?**

VPN'ler, özel bilgilerin İnternet gibi genel bir ağ üzerinden aktarılmasına izin verir. Bir VPN, ağ çevresinin bir uzantısıdır ve bu nedenle, ağ güvenliği politikasını tüm VPN giriş noktalarında eşit olarak uygulayabilmelidir. Kapsülleme ve şifreleme kullanımı sayesinde, verilerin gizliliği kamuya açık bir ağı geçerken korunur. Bu teknolojinin uygun şekilde kullanılmasının teknik yararları arasında işletme maliyetlerinin azaltılması, ağ erişim güvenliğinin arttırılması, transit veri bütünlüğü, kullanıcı ve veri kimlik doğrulaması ve veri gizliliği sayılabilir. Bununla birlikte, finansal yararların bazıları, VPN çözümünün satın alınmasından sonra, dağıtım sırasında, devam eden yönetim ve destek sırasında gerçekleşen VPN sisteminin gerçek maliyetleri ile ihmal edilebilir. Bu tür ürün farklılaşması Çoğu üreticinin VPN ürünleri aynı VPN protokolünü kullandığı için önemi giderek artmaktadır - IPSec - ve diğer temel teknolojiler. IPSec, İnternet’e güvenlik genişletmeleri tanımlayan uluslararası bir standarttır. İnternet protokolü. VPN'leri uygulamak için kullanılan başka güvenli tünel protokolleri olsa da, IPSec tercih edilen protokol olarak liderliğini üstlendi. Bu standart, minimum düzeyde satıcı birlikte çalışabilirliği sağlayan zorunlu özellikleri belirtir. Bu bölüm, bilgi güvenliği uzmanlarının IPSec VPN çözümlerini değerlendirirken kullanılabilecek bir dizi kriter belirlemelerine yardımcı olacaktır. Tartışma, VPN uygulamalarının incelenmesiyle başlar.

**IPSec VPN Uygulamaları**

İşletmeler, dört uygulama gereksinimini karşılamak için genellikle sanal özel ağları (VPN'ler) aradılar: uzaktan erişim, siteden siteye intranet, güvenli extranet ve güvenli iç ağ. Teknik amaç, çoğu durumda yetkili kullanıcılara korumalı ağ veri kaynaklarına (yani sunucu dosyaları, disk paylaşımları, vb.) Kontrollü erişim sağlamaktır. Ortak bir iş hedefi, ağ altyapısı maliyetlerini yönetmek ve iç ve dış iş bilgi akışının verimliliğini artırmak, kullanıcı verimliliğini, rekabet avantajını veya iş ortağı ilişkilerinin gücünü artırmaktır. Bir VPN değerlendirme projesinde yer alan görevleri tanımlamak iyi bir fikirdir. Bir görev listesi, değerlendirmeyi odaklı tutmaya yardımcı olacak ve değerlendirmeyi tamamlamak için gereken kaynakları öngörmeye yardımcı olacaktır. Sergi 40.1’de VPN değerlendirme projesi görevlerinin örnek listesi.

**Uzaktan Erişim VPN**

Uzaktan erişim VPN'in iki bölümü vardır: sunucu ve istemci. İki farklı rolleri var ve bu nedenle iki farklı değerlendirme kriteri.

* İş hedefi: daha düşük telekom maliyetleri, artan çalışan verimliliği
* Teknik hedef: Uzaktaki çalışanlara güvenli LAN erişimi ile aynı erişimi sağlamak.

Bu bölümde hem roller hem de kriterler tartışılmaktadır.

Uzaktan erişim IPSec VPN'leri, kullanıcıların ne zaman, nerede ve ne zaman isterlerse şirket kaynaklarına erişmelerini sağlar. Uzaktan erişim VPN'leri, mobil kullanıcıları ve telekomünikasyonları güvenli bir şekilde bağlamak için IPSec gibi güvenlik protokolleriyle birlikte analog, kadran, ISDN, dijital abone hattı (DSL), mobil IP ve kablolu İnternet erişim teknolojilerini içerir.

**EK 40.1** VPN değerlendirme projesi görevleri

Veri güvenliği gereksinimlerini değerlendirin.

Kullanıcıları sınıflandırın.

Kullanıcı konumlarını değerlendirin.

Ağ bağlantısı ve erişim gereksinimlerini belirleyin.

Ürün veya servis sağlayıcı seçin.

Donanım / yazılım ihtiyaçlarını değerlendirin.

Bir test laboratuvarı kurun.

Değerlendirme cihazları edinin.

Özellik gereksinimlerine göre ürünleri test edin.

Bir pilot program uygulayın.

**İstemci Yazılımı**

Uzaktan erişim kullanıcıları arasında telekomünikasyon cihazları, mobil çalışanlar, seyahat eden çalışanlar ve verilere erişilen şirketin çalışanı olan herhangi bir kişi bulunur. En sık kullanılan işletim sistemleri MS'dir. Windows tabanlı, kurumsal bir masaüstü standardı olarak pazar kabulünden dolayı. IPSec VPN sistem gereksinimleri Macintosh, UNIX, PalmOS veya Microsoft Pocket PC / gibi diğer işletim sistemleri için destek gösterebilir. Windows CE. Tercihen, IPSec VPN satıcısı, şirket tarafından istenen müşteri tiplerinin bir karışımını sunar. Mobil çalışanlar bazen satış tahminleri, gizli hasta veya yasal bilgiler, müşteri listeleri ve hassas ancak sınıflandırılmamış DoD veya yasa uygulama bilgileri gibi yüksek değerli / yüksek riskli kurumsal verilere erişmeye ihtiyaç duyarlar. Uzaktan erişim ayrıca İnternet üzerinden bilgi işbirliği için eşler arası erişim anlamına da gelebilir (örneğin, Microsoft NetMeeting) ve uzaktan teknik destek için de kullanılabilir.

Bu uygulama için istemci donanım platformları PDA'lar, dizüstü bilgisayarlar, ev masaüstü bilgisayarları, çağrı cihazları, verileri zaten içerir cep telefonları ve diğer kablolu ve kablosuz ağ bağlantılı cihazlar. Donanım platformu teknolojisi geliştikçe, şirket verilerine uzaktan erişmek için kullanılabilecek başka cihazlar olacağından emin olabilirsiniz. Popülerliği artıran ilginç bir fenomen, kişisel dijital asistanlar, cep telefonları ve diğer yüksek portatif ağ özellikli cihazlar gibi kablosuz cihazların uzaktan erişim IPSec VPN uygulamaları için erişim platformları olarak kullanılmasıdır. Kablosuz cihazların karşılaştığı sorunlar, kablolu IPSec VPN platformlarının karşılaştığı temel sorunları içerir. Fiziksel olarak güvenlik ve veri güvenliği gibi, işlemsel olarak zorlu cihazlarda şifreleme uygulama sorunu da eklendi.

PDA'lar gibi kablosuz IPSec VPN platformlarıyla ilgili başka bir sorun, kablolu dünya güvenliği ile uyumluluk protokolleridir. Kablosuz protokollerin standart bir organı olan Kablosuz Uygulama Protokolü (WAP) Forumu çalışıyor WAP tanımlı güvenlik protokolü arasındaki uyumluluğu geliştirmek için - Wireless Transport Layer Security (WTLS) - ve SSL gibi kablolu dünya güvenlik protokolleri. Endüstri gözlemcileri, PDA'lar ve verilere hazır cep telefonları gibi kablosuz cihazların, uzaktan işlemsel veri erişimi gerektiren uygulamalar için tercih edilen platform olacağını tahmin ediyor. Ancak, bu cihazlar küçüktür ve kolayca çalınabilir veya kaybolabilir. Bu, IPSec VPN istemci yazılımının özelliklerini analiz ederken, değerlendirme ölçütlerinin bir parçası olarak donanım platformu fiziksel güvenliğini dahil etme ihtiyacını vurgulamaktadır. Bu platformlar için fiziksel güvenlik kontrolleri kabloları içerebilir ve kilitler, seri numarası takibi, hareket sensörleri, konum tabanlı takip (Global Konumlandırma kullanımı ile (Sistemler) ve ses doğrulaması ile parmak taraması gibi biyometrik kimlik doğrulaması.

Uzaktan erişim için iletişim aktarımı ağırlıklı olarak çevirmeli bağlantı yoluyla olmaya devam ediyor. Kablosuz ve geniş bantlı erişim kullanımda büyümeye devam ediyor. Bununla birlikte, geniş bant uygulamalarındaki ve belirli coğrafi kısıtlamalardaki erken karmaşıklıklar son zamanlarda azaltılmıştır ve çevirmeli kullanımın ötesinde kullanımda geniş bant ve kablosuz kullanımın artması muhtemeldir.

Geniş bantlı (DSL, kablo modem) kullanımındaki bir sorun, meta haline geldiğinden, geniş bant sağlayıcılarının izin verilen hizmetleri ağlarında bölümlere ayırmaya çalışmalarıdır. İnternet erişimi sağlayan kablolu servisler tarafından kullanılan bir taktik, ev kullanıcıları tarafından IPSec VPN'lerin kullanılmasını yasaklamaktır. Bir kablo şirketine göre, ABD Batı Kıyısı'na dayanarak, konut IPSec VPN kullanıcılarının oluşturduğu genel gider ağı, diğer ev tabanlı kullanıcılar için mevcut bant genişliğini etkiliyordu. Bu nedenle, bu kablo şirketi, tüm VPN'lerin, kablo modemde port ve protokol paket filtre kuralları kullanılarak konut servis müşterileri tarafından kullanılmasını yasaklamıştı. Açıkçası, bu kablo şirketine fayda sağlıyor çünkü VPN'leri evden İnternet üzerinden yönlendirmek için daha yüksek işletme sınıfı ücretleri talep edebiliyor. Bazı tescilli VPN çözümleri satıcıları, örneğin bu kablo şirketi kısıtlamasını atlamak için VPN yüklerini izin verilen protokollere, örneğin HTTP paketlerinde kapsüllenerek kullanarak cevap verdiler. Bu sorunun nasıl çözüleceği hala görülmeye devam ediyor, ancak bir VPN seçerken başka bir kriter belirledi: Son kullanıcının ISS veya ağ erişim sağlayıcı ağı üzerinden mi çalışacak? Uzaktaki son kullanıcılar kendi mesken sınıfı ISS'lerini kullanır mı? Yoksa şirket satın alacak Tutarlı ve güvenilir bağlantı sağlamak için işletme sınıfı erişim?

Son kullanıcılar, yapmaları için para aldıkları işi yapmaya odaklanır. Genel olarak, kullanıcılar, uzaktan erişim bağlantılarının güvenliğini gerçekten önemsemeye teşvik edilmemektedir. Kullanıcılar, öncelikle bilgisayarlarındaki mevcut uygulamalarla kullanım kolaylığı, güvenilirlik ve uyumluluk ile ilgilenmektedir.

Bu nedenle, kapsamlı bir değerlendirme stratejisinin bir parçası, VPN istemcisinin tamamen test edilmesi gerektiğidir. kullanıcılar tarafından gerçek hayatta kullanılacak olan aynı uzak platform yapılandırması. Örneğin, bazı üreticilerin kişisel güvenlik duvarı başka bir satıcının IPSec VPN istemcisiyle çakışmaya neden olabilir. Bu tür bir uyumsuzluk, satıcıyla çalışarak çözülebilir olabilir veya olmayabilir ve listeden diskalifiye edilmesiyle sonuçlanabilir. potansiyel çözümler. IPSec VPN istemcisi uyumsuzluğunun bir başka örneği, bir satıcının IPSec VPN istemcisinin IPSec VPN sunucusu veya başka bir IPSec VPN ile aynı parametreleri desteklemediği durumdur. istemcisi. Burada akılda tutulması gereken şey, standartların genellikle asgari düzeyde zorunlu özellikler tanımlamasıdır. Satıcılar, ürünlerini farklılaştırmak amacıyla, bir standart tarafından açıkça belirtilmeyen özellikler gibi daha gelişmiş özellikler ekleyebilirler. Ayrıca, satıcılar IPSec VPN istemcilerini, kendi IPSec VPN sunucularıyla en etkili şekilde çalışacak şekilde optimize edebilirler. Bu, genel IPSec VPN sisteminin güvenlik seviyesini ve performansını düşürebilecek “en düşük ortak payda” konfigürasyonunu kullanmak için karışık bir satıcı yaklaşımı bırakır. Örneğin, bazı IPSec VPN sunucu satıcıları, standartta zorunlu olarak tanımlanmayan kimlik doğrulama protokollerini destekler. Açıkçası, seçilen IPSec VPN istemcisi, IPSec VPN sunucusuyla aynı satıcıdan gelmiyorsa ve kabul edilebilir bir birlikte çalışabilirlik sağlanamıyorsa, kriterlerde veya satıcı diskalifikasyonunda bir uzlaşma yapılması gereken karar olacaktır.

İnternet erişimi daha yaygın hale geldikçe ve aboneler daha uzun süre bağlı kaldıkça veya “her zaman”, uzak VPN kullanıcısının bilgisayarına yönelik saldırı fırsatlarında ortaya çıkan artışlar söz konusu. Bu nedenle, uzak kullanıcının bilgisayarında depolanan değerli veriler varsa, bir tür dosya veya disk şifreleme kullanmak mantıklı olabilir. Şifreleme, işlemci yoğun bir etkinlik olduğundan, uzak bilgisayar için kullanılabilen bilgi işlem kaynaklarının artırılması gerekebilir. Buradaki amaç, taşınabilir bir bilgisayar aygıtında saklanmış olsa bile değerli verileri yetkisiz görünümden korumaktır. Bazı VPN istemci yazılımı, virüs koruması, dağıtılmış masaüstü güvenlik duvarı, masaüstü izinsiz giriş koruması ve dosya / disk şifrelemesi içerir. Bu tür bir çözüm daha fazla olabilir . belirli uygulamalar için gerekenden daha fazla, ancak bir savunma alanında bile masaüstü seviyesi. Bu karışıma ek olarak, güçlü bir kimlik doğrulaması ve dijital imzalama ve iyi düşünülmüş bir politikanın uygulanmasının yanı sıra, politikanın doğru bir şekilde uygulanmasıyla güvenlik riski azalır. Yukarıda belirtilenler, çevirmeli bağlantı kullanıcıları için de geçerlidir; çevirmeli bağlantı ile ne zaman bağlanırsa, herkes kamuya açık ve dolayısıyla saldırıya açık bir IP adresi alır.

VPN istemcisi bütünlüğü sorunları da dikkate alınmalıdır. Örneğin, VPN istemcisinin VPN sunucusundan bir güvenlik politikası güncellemesi veya yapılandırma güncellemesi doğrulamak mı istiyorsunuz? Güncellemenin başarıyla tamamlanması için kullanıcı bir şekilde işbirliği yapmak zorunda mı? Kullanıcılar, VPN istemcisi güncelleme işlemine dahil olmaları gerekiyorsa zincirde zayıf bir bağlantı olabilir. Kullanıcı katılımı olmadan VPN istemcisi yapılandırmasının güvenli otomatik güncellemelerine izin veren VPN istemcilerini düşünün. Antivirüs koruması, örneğin bir VPN sisteminin yetkisiz manipülasyonunu gerçekleştirme potansiyeline sahip olan bir Truva atı veya virüsünün potansiyelinden kaynaklanmaktadır. VPN istemcisi masaüstü antivirüs programlarıyla uyumlu mu (veya içeriyor mu)? Bir artışa şahit oluyoruz Hedefe yönelik saldırılarda, saldırganın kör bir şekilde arama yapmak yerine belirli bir sebepten dolayı hedefleri seçtiği yer savunmasız bir ev sahibi için. Bu tür saldırılar, saldırganların VPN giriş noktaları aracılığıyla koordine etme ve saldırma yeteneklerini içerir. Bu, uzak VPN kullanıcı bağlantılarını sistematik olarak merkezi siteye yönlendiren kararlı bir saldırgan için olasıdır. Bu nedenle, VPN istemcisini dağıtılmış masaüstü güvenlik duvarları ve masaüstü izinsiz giriş tespit sistemleri kullanarak yıkılmaya karşı koruma gereksinimi olabilir.

Dağıtılmış bir masaüstü güvenlik duvarının ana ayırt edici özelliği, bir kuruluştaki tüm masaüstleri için güvenlik duvarı politikasının merkezi bir konsoldan yönetilmesidir. Kişisel güvenlik duvarları, adından da anlaşılacağı gibi, bireysel tüketicilere pazarlanmaktadır. Bireysel kullanıcı, kişisel güvenlik duvarlarındaki politikaların korunmasından sorumludur. Dağıtılmış bir güvenlik duvarı, uzak VPN kullanıcı bağlantısı da dahil olmak üzere, tüm giriş noktalarında dahili ağa tutarlı bir ağ güvenliği politikasını merkezi olarak uygulamak zorunda olan işletmelere pazarlanır. Bir IPSec VPN istemcisini, dağıtılmış bir güvenlik duvarı ve tekrar raporlayan izinsiz giriş tespit sistemi ile birlikte dağıtarak merkezi bir yönetim konsolu, devam eden ağ saldırıları, güvenlik duruşunun kurumsal bir görünümünü sağlamak için birleştirilebilir ve ilişkilendirilebilir. İdeal olarak, bir IPSec satıcısı antivirüs içeren bir VPN istemcisi sağlayabilir,masaüstü izinsiz giriş tespiti ve IPSec VPN istemcisi ile birlikte dağıtılmış bir güvenlik duvarı. Bu düzeyde bir entegrasyon sağlayan bir ürün, kesinlikle masaüstü güvenlik politikası yönetiminin etkinliğini artıracaktır.

**İstemciyi Dağıtma**

Uzaktan erişim VPN istemci yazılımı dağıtım sorunları, öncelikle herhangi biriyle ortaya çıkan operasyonel konulardır. dağıtılmış yazılım, bu tür SQL istemci yazılımı. Çok geniş bir yazılım yönetimi bilgisi vardır. ve uzaktan erişim VPN istemci yazılımını dağıtmaya uyarlanabilecek metodolojiler.

Bir VPN istemcisinin konuşlandırılabilirliğini incelerken birkaç sorunun çözülmesi gerekir. Böyle bir konu VPN istemci yazılımı dosya boyutu. Seçilen istemci yazılımı dağıtım modu, şu anda en yaygın kullanılan uzaktan erişim yöntemi olan düşük hızlı çevirmeli bağlantı üzerinden gerçekleştiriliyorsa, bu önemli bir sorun haline gelir. Dosyanın bir dağıtım FTP sunucusundan indirilmesi çok uzun sürerse, etkilenen kullanıcıların dosyayı veya gelecekteki güncellemeleri indirmeye dirençli olması olasıdır. Dayanıklı kullanıcılar, uzun süren uygulama olasılığını artırabilir VPN'in toplam uygulama maliyeti artar. Ancak, yaygın yüksek hızlı erişim vaadi ufukta. Bu sorunu çözebilecek bir dağıtım stratejisi, VPN istemcisini başlangıçta disket veya CD-ROM gibi taşınabilir ortamlar tarafından dağıtmaktır. Veri sıkıştırma, VPN istemcisi dağıtım boyutunu daraltmanıza yardımcı olabilir. Çoğu satıcı, yöneticinin bazı başlangıç ​​ayarlarını önceden yapılandırmasını ve ardından yükleme dosyasını her bir uzak kullanıcıya dağıtmasını sağlayan bir tür istemci yapılandırma yardımcı programı sağlar. Olası VPN müşteri dağıtımı yöntemler bir Web veya FTP sitesine göndermeyi içerir. Web, FTP veya başka bir çevrimiçi dosya aktarma yöntemi kullanılıyorsa, güvenlik uzmanının VPN istemcisi yükleme dosyasına yetkisiz erişim olgusu içeren olası senaryoları öngörmesi önemlidir. Bazı şirketler kurulum dosyalarını sadece şahsen dağıtmalarına karar verebilir. Diğerleri posta veya elektronik posta yoluyla dağıtım riskini kabul etmeye hazırdır. Diğerleri, güvenli bir dosya aktarım sitesi kurmayı, bir PIN veya özel bir parola kullanarak erişim sağlamayı seçebilir. Ne zaman VPN müşterisinin ilk dağıtımına gelince, olasılıklar ancak ihlal edildiğinde zararın değerine bağlı olarak kabul edilebilir risk seviyesi ile sınırlıdır. Bu, özellikle ilk VPN istemci yazılımının, saldırgan tarafından keşif bilgisi olarak kullanılabilecek bilgilerle önceden yapılandırılmış olması durumunda geçerlidir.

**Müşteri Yönetimi Sorunları**

VPN müşteri yönetimi, müşteri konfigürasyonunun operasyonel bakımı, VPN müşteri politikası güncelleme işlemi ve VPN istemci yazılımının güncellenmesi ile ilgilidir. Yine, bugün işletmeler tarafından dağıtılan diğer yazılım türlerini yönetmek için kullanılan genel bilgi ve yazılım yönetimi metodolojilerinden uyarlanabilecek birçok yaklaşım vardır. Ek faktörler güncellemelerin kullanıcı kimlik doğrulaması, VPN kullanılabilirlik, güncelleme dosyası bütünlüğü ve gizlilik. Kullanıcı kimlik bilgilerini yönetme yeteneği, VPN sunucusu yönetimi ile ilgili bölüm.

VPN istemcisi, iç ağda başka bir erişim noktasını temsil ettiğinden, bu erişim sıkı bir kullanıcı kimlik doğrulaması ve sıkı kontrol edilen VPN yapılandırma bilgileri gerektirir. Pek çok kişi, güçlü kimlik doğrulamanın en yüksek seviyesinin biyometrik tabanlı olduğunu iddia eder. Bir PIN birlikte kullanıldığında Biyometri ile iki faktörlü kimlik doğrulama olarak kabul edilebilir. Birçok güvenlik uzmanı tarafından bir sonraki seçenek PIN birleşimli bir akıllı kartta saklanan dijital sertifikadır. Zamana dayalı hesap kartı (jeton) ve basit parolaların kullanılması eski kullanımlara giriyor. Ancak, birçok IPSec satıcısı XAUTH uzantısını IKE / IPSec standardına uyguluyor. XAUTH uzantısı, IPSec tüneli kurulumu sırasında kullanıcı kimliğini doğrularken, şu anda kullanımda en yaygın kullanılan kimlik doğrulama yöntemi olan RADIUS gibi eski kullanıcı kimlik doğrulama yöntemlerinin kullanılmasına izin verir.

VPN güncelleme sunucusunu taklit etme ihtimaline bağlı olarak dikkat edilmesi gereken bir soru, “İstemci yazılımı, yapılandırma güncelleme dosyasını aldığını nasıl onaylar?” Şeklindedir. Birçok yapılandırma dağıtım biçimiyle, saldırganın göndermesi için bir fırsat vardır. kullanıcılara yetkisiz güncelleme dosyası. Bu tehdide karşı bir kontrol, güncellemeyi dijital olarak imzalamak için şifreleme ve dijital imza kullanımıdır kabul edilmeden önce VPN istemcisi tarafından doğrulanabilen bir dosya. Ek bir koruma Gerçek yapılandırma dosyasını, uzak kullanıcı bilgisayarında bulunan şekilde şifreleyin. Yaygın bir yöntem, güncellemeleri aktarmak için güvenli bir yol kullanmaktır; örneğin, SSL üzerinden LDAP (LDAP).

Ek 40.2, uzaktan erişim VPN istemci yazılımı için örnek bir değerlendirme profilini göstermektedir. Bu, bir VPN müşterisi için değerlendirme kriterleri geliştirirken göz önüne alınabilecek öğelerin bir listesidir.

**Uzaktan Erişim Sunucusu**

Şifreleme tüneli trafiğinin ana işlemesi uzaktan erişim (VPN) sunucusunda yapılır. VPN sunucusu tünel toplama noktası haline gelir: uzaktan erişim istemcisi sunucuyu tünel bitiş noktası olarak kullanır. VPN sunucusunun VPN trafiğini verimli bir şekilde işleme kapasitesine sahip olduğunu doğrulamanın iki yolu vardır. İlki, işlem kısıtlamalarının üstesinden gelmek için daha büyük, daha hızlı donanım cihazları kullanmaktır; yekpare donanıma dayalı çözümler doğrudan donanıma bağlı performans gelişmelerine bağlıdır. Performans geliştirmelerinin gelmesi yavaşsa, yukarı doğru ölçekleme yeteneği de artacaktır. Bu yaklaşım genellikle dikey ölçeklenebilirlik olarak adlandırılır. İkinci alternatif, bir VPN sunucusu grubundaki VPN bağlantılarını yük dengelemek veya dağıtmaktır. Yük dengeleme, özel yük dengeleme donanımı veya birden fazla VPN sunucusu arasında ilke ve durum çoğaltma yoluyla özel işlemciler ve yazılımlar gerektirir. Bağlantılar ve ekonomiler açısından, yük dengeli bir VPN sunucu grubu her zaman daha iyi ölçeklenebilirlik sunacaktır çünkü gerektiğinde daha fazla sunucu eklenebilir. Yük dengeleme aynı zamanda fazlalık da sağlayacaktır; Herhangi bir VPN sunucusu başarısız olursa, yük kalan VPN sunucuları arasında dağıtılacaktır.

**Ek 40.2** Uzaktan Erişim VPN İstemcisi için Değerlendirme Ölçütleri

Varsayım: VPN istemcisi merkezi sitenin yönetimine tabidir

Mobil kullanıcı masaüstünün güvenliği için dosya / disk şifrelemesi gerekebilir

Kapsamlı disk / dosya şifrelemesi kullanılıyorsa, yüksek performanslı dizüstü bilgisayarlar / dizüstü bilgisayarlar gerekebilir

Merkezileştirilmiş VPN yöneticisine entegre edilmiş uyarı ile masaüstü izinsiz giriş tespiti

Merkezi VPN yöneticisine entegre edilmiş uyarılı dağıtılmış masaüstü güvenlik duvarı

VPN istemcisi yapılandırmasını kilitleme yeteneği

Şeffaf kullanıcı VPN istemcisi güncellemesi

Şifrelenmiş bir bağlantı üzerinden kimliği doğrulanmış VPN istemcisi güncellemesi

Birlikte çalışabilirlik bir gereklilik ise, mevcut endüstri VPN standartlarına bağlılık

(Bazı HA çözümleri, oturumları kesintiye uğratmadan bunu yapabilir; diğerleri daha rahatsız edicidir.) Şifreleme hızlandırıcılar - donanım tabanlı şifreleme kartları - arttırmak için bir VPN sunucusuna eklenebilir. Sunucudaki tünel işleme hızı. Şifreleme ivmesi şimdi ağ arabirim kartlarının yonga düzeyinde de uygulanmaktadır. Şifreleme hızlandırması, VPN sunucusu için ayrı ayrı VPN istemci bilgisayarında olduğundan, yine tünellerin toplanmasından dolayı daha önemlidir.

VPN sunucusunun kapasitesini değerlendirirken, yönetim kolaylığını düşünün. Özellikle, bir yöneticinin operasyonel görevleri gerçekleştirmesi ve otomatikleştirmesi ne kadar kolaydır? Örneğin, yeni tüneller eklemek ne kadar kolay? Ek tünel yapılandırmaları VPN istemcisine otomatik olarak “itilebilir” veya “aşağı çekilebilir” mi? Günlük kaydı, raporlama ve uyarı VPN sunucu yönetimi arayüzüne entegre edilmesi gereken önemli bir özelliktir. VPN günlükleri mevcut veritabanlarına ve ağ yönetim sistemlerine aktarılabilir mi? VPN sunucusu gerçek zamanlı kayıt ve uyarı veriyor mu?

Kullanıcılar tarafından seçilebilen olayları görsel olarak vurgulamak için filtreler hemen sunucu günlüklerine uygulanabilir mi? Dijital sertifika kullanıyorsanız, hangi sertifika yetkilileri desteklenir? Sertifika talebi ve satın alma işlemi otomatik bir çevrimiçi prosedür mü? Yoksa manuel müdahale gerektiriyor mu? Sertifika talebi ve satın alma gibi tekrarlayan işler otomasyon için doğal adaylardır.

VPN sunucusu, kullanıcı sertifikalarının geçerliliğini kontrol etmek için otomatik olarak sertifika iptal listeleri talep ediyor mu? Sergi 40.3, uzaktan erişim VPN sunucuları için örnek bir değerlendirme profilini göstermektedir.

**Intranet VPN**

Bir intranet VPN, bir kurumsal WAN içindeki sabit konumları ve şube ve ev ofislerini birbirine bağlar. Bir intranet VPN bir siteden siteye veya VPN ağ geçidinden VPN ağ geçidine bir topoloji kullanır. Bir intranet VPN'in sağladığı faydalar arasında, ağ altyapısı maliyetlerinde düşüş ve kurum içinde bilgi akışında artış yer alıyor. Bir intranetin doğası siteden siteye olduğu için, son kullanıcı masaüstleri üzerinde çok az etki vardır. Bir intranet uygulaması için VPN çözümlerini değerlendirmedeki kilit kriterler performans, önceden var olan ağ altyapısıyla birlikte çalışabilirlik ve yönetilebilirliktir. Bir intranet VPN'in teknik avantajları arasında düşük WAN bant genişliği maliyetleri, daha esnek topolojiler (örneğin tamamen örülmüş) ve yeni sitelerin hızlı ve kolay bağlantısı bulunur.

**Ek 40.3 Uzaktan Erişim VPN Sunucusu için Değerlendirme Profili**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Ölçeklenebilirlik (sunucu bağlantı gereksinimlerini karşılayabilir mi?)

Yüksek kullanılabilirlik seçeneklerini destekler

Mevcut kullanıcı kimlik doğrulama sistemleri ile bütünleşir

Donanım tabanlı tünel işleme, şifreleme / şifre çözme hızlandırması

Otomatik kullanıcı doğrulama sürecinin yönetimi

Birlikte çalışabilirlik için endüstri VPN standartlarını destekler

Hangi kimlik doğrulama türleri desteklenir?

VPN sunucusu sertleştirilmiş bir işletim sisteminde çalışıyor mu?

Hem VPN istemcisi hem de sunucu tarafında güvenlik duvarı entegrasyonu mümkün mü?

Merkezi müşteri yönetimi özellikleri

Masaüstü işletim sistemleri için geniş istemci desteği

Satıcı tarafından sağlanan bir VPN donanım / yazılım sistemi olan uzaktan yapılandırılabilir VPN cihazlarının kullanımı, Yerinde yönetim eksikliği ve hızlı uygulama süresi olacağını belirtti. Değer Donanım, işletim sistemi ve VPN sunucu yazılımını daha geleneksel “kendin yap” yaklaşımını kullanarak entegre etmek için gereken zaman ve çabayı karşılaştırırken VPN cihazlarının kullanımı netleşti.

Hizmet sınıfı kontrolleri, diğerlerine göre belirli protokolleri önceliklendirmek için trafik mühendisliği yaparken yararlı olabilir. Bu, örneğin iş gereksinimleri belirli VPN trafiği türlerinin diğerlerinden daha az gecikme süresi gerektirmesi gerektiğini zorunlu kıldığı zaman, bir sorun haline gelir. Örneğin, video veya sesli trafik akışı, son kullanıcının beklentileri veya uygulama türünün özellikleri nedeniyle bir dosya aktarımından veya HTTP trafiğinden daha sürekli bir bit hızı gerektirir.

İnternet üzerinden tünel yapan intranet VPN'lerin genel kullanımı için iki sınırlayıcı faktör gecikme ve garantili bant genişliği eksikliğidir. Bu faktörler uluslararası olarak konuşlandırılmış özel WAN tabanlı intranet VPN'lerini de etkileyebilse de, çoğu şirket İnternet üzerinden düşük VPN maliyetine karşı rekabet edebilmek için yeterli uluslararası özel WAN bant genişliğine sahip olamaz. Bir maliyet / fayda analizi yapmak, özel bir WAN, Internet tabanlı bir intranet VPN veya dış kaynaklı bir VPN servisi kullanıp kullanmamaya karar vermede yardımcı olabilir. Çoklu Protokol Etiketi Anahtarlama (MPLS), veri trafiğini önceliklendirmek için standart bir yol sağlayan bir protokoldür.

VPN'nin topolojisi, intranet VPN'de önemli bir husustur. Birçok intranet VPN, bir kuruluşun bilgi akışının merkezden dağıtılmış doğası nedeniyle bir ağ topolojisi gerektirir. Diğer durumlarda, merkezileştirilmiş bir topoloji, merkezi bilgi akışı durumunda veya uygulanması gereken “merkez ofis” kavramı durumunda belirtilebilir. Ağ değişikliklerinin sık olacağı öngörülürse, dinamik yönlendirmeyi ve dinamik VPN yapılandırmasını destekleyen VPN çözümleri belirtilir. Dinamik yönlendirme, ağ adresleme güncellemelerinin VPN'de hızlı bir şekilde yayılması gerektiği, insan müdahalesine gerek kalmadan veya hiç müdahalesine gerek duyulmaması durumunda faydalıdır. Yönlendirme hizmetleri, VPN altyapılarına düşük maliyetli taşıma sağlar Mevcut ağ yapılandırmalarını etkilemeden sağlam bant genişliği yönetimi sağlayanlar. Dinamik VPN teknolojisi, spontan, kısa ömürlü VPN bağlantısının bir gereklilik olduğu tahmin edildiğinde faydalıdır. Büyük ölçekli dağıtımlarda VPN tünellerini kurmanın idari yükünü hafifletmeyi vaat eden dinamik VPN'ler konusunda halen devam etmekte olan araştırmalar var.

İnterneti kullanarak bir intranet VPN oluşturmak genel olarak en uygun maliyetli uygulama aracıdır. VPN teknolojisi Bununla birlikte, hizmet seviyeleri, daha önce de belirtildiği gibi, İnternette genellikle garanti edilmez. Hizmet düzeyi garantilerinin eksikliği genel IP trafiği için geçerli olsa da, intranet VPN'leri için evrensel olarak böyle değildir. Bazı ISS'ler ve özel etiketli IP sağlayıcıları (örneğin, Digital Island) hizmet düzeyi garantileri sunarken, bu teknoloji ancak şu anda olgunlaşıyor; ve bu tür hizmet tekliflerinden en iyi şekilde yararlanmak için, müşteriler genellikle intranetlerini tek bir ISS’nin IP ağının üzerine kurarlar. Bir intranet VPN'i uygularken, işletmelerin garantili hizmet seviyeleri, ağ erişiminin yaygınlığı ve taşıma maliyeti arasında ne gibi bir indirim yapmak istediklerini değerlendirmeleri gerekir. Garantili verim düzeyleri gerektiren işletmeler, VPN'lerini bir ağ servis sağlayıcısının özel uçtan uca IP ağı üzerinden dağıtmayı veya potansiyel olarak Frame Relay'i kurmayı veya kendi özel omurgasını oluşturmayı düşünmelidir.

Sergi 40.4, bir intranet VPN için bir dizi değerlendirme kriteri geliştirirken kullanılabilecek bir ürün listesi sunar.

**Ek 40.4** Siteden Siteye Intranet VPN için Değerlendirme Profili

Varsayım: yok

Otomatik politika dağıtımı ve yapılandırması desteği

Ağ topolojisi otomatik yapılandırma, hub ve konuştu topoloji desteği

Ağ ve servis izleme yeteneği

Heterojen ağda kullanılıyorsa VPN standartlarına bağlılık

Hizmet sınıfı kontrolleri

Dinamik yönlendirme ve tünel kurulum özelliği

Ölçeklenebilirlik ve yüksek kullanılabilirlik

**Extranet VPN**

Extranet VPN'ler, iş ortakları ve müşteriler arasında seçici bilgi akışı sağlar. Yüksek taneli erişim kontrolü ve güçlü kimlik doğrulaması üzerinde durulur. Örneğin, güvenlik yöneticileri, kaynak ve kodlar da dahil olmak üzere birden fazla parametre kullanarak bireysel uygulamalara kullanıcıya özel erişim yetkileri verebilir. Hedef adresler, kimliği doğrulanmış kullanıcı kimliği, kullanıcı grubu, kimlik doğrulama türü, uygulama türü (örneğin, FTP, Telnet), şifreleme türü, gün / saat penceresi ve hatta etki alanı tarafından.

Bir extranet VPN, tek bir şirketin tedarik zinciri ve iş ortakları ile bilgi paylaştığı veya Otomotiv Ağı Değişimi gibi bir siteden siteye modelini paylaştığı, merkezi bir site modeli kullanabilir. Kullanıcıdan siteye model kullanıyorsanız, değerlendirme kriterleri, kullanıcı masaüstünün merkezi sitenin kontrolü altında olmaması dışında, uzaktan erişim VPN'lerine benzer. Extranet kullanıcısının bilgisayarı kendi şirketin güvenlik politikasının kontrolü altında olduğundan, kullanıcıların bilgisayarında uygulanan güvenlik politikasında bir çatışma olabilir. Genel olarak, kullanıcı-site modelindeki extranet ortaklarının, kullanıcı masaüstünde güvenlik politikası uygulaması, VPN istemcisi yükleme sorunları, yardım masası, devam eden bakım için bir ortak kullanımı zorunlu kıldığı konusunda bir anlaşmaya varmak için birlikte çalışması gerekecektir. Belirli bir VPN müşterisi ve sorumluluk sorunları, bir ortağın ihmali diğer ortağın ağının uzlaşmasına yol açmalıdır. Bir satıcının VPN istemcisi tarafından desteklenen donanım platformları, uzak extranet ortaklarının kullanacağı olası platformların araştırılmasını gerektiren bir sorun olacaktır. Çoğunlukla, Web tabanlı erişim genellikle extranet ortamlarında tercih edilen yazılım istemcisi olarak kullanılır ve SSL genellikle güvenlik protokolü olarak seçilir. Bu, yüzleşilmesi gereken yapılandırma ve bakım sorunlarını büyük ölçüde basitleştirir. Bir extranet VPN ile gerçekten öyle Tüm katılımcıların aynı ISS'yi kullanıp kullanmadığı önemli değildir, kabul edilebilir hizmet kalitesinin, ISS'nin hangisi tarafından seçildiğine göre sağlandığı varsayılmaktadır. Gereken tek şey, grubun her bir üyesinin İnternet’e bir şekilde erişebilmesi. Her sitedeki VPN yazılımı veya ekipmanı, extranetin ana sitesindeki VPN ekipmanının IP adresiyle yapılandırılmalıdır.

Bir extranet VPN'in çekiciliği, büyük ölçüde pazarları genişletme ve iş ilişkilerinin gücünü artırma yeteneğinden biri olduğundan, pazarlama perspektifinden, extranet istemci yazılımını markalamak istenebilir. Bu, bazı extranet VPN yazılımı ve servis sağlayıcıları ile, extranet giriş noktası olan Web sayfasında (yazılım platformu olarak bir Web tarayıcısı kullanılıyorsa) veya VPN istemcisinin içinde (geleneksel istemci / sunucu yazılımı kullanılıyorsa) yapılabilir. modeli). Tüketici pazarında, extranet VPN'leri alternatif olarak kullanılabilir .Web tarayıcısı tabanlı SSL’ye IPSec VPN'lerin Web tarayıcı tabanlı SSL'ye tercih edileceği bir durum Müşterinin bilinmesi ve siteye birçok kez geri dönmesi muhtemeldir. Başka bir deyişle, bir extranet VPN, insanların bir kez gelebilecekleri bir tüketici katalog ortamında mutlaka çalışmayabilir. Kredi kartı ile alışveriş yapmak.

Web tarayıcısı tabanlı bir SSL kendiliğinden, basit işlem ilişkileri için iyidir, ancak bir IPSec VPN Dijital sertifika tabanlı karşılıklı kimlik doğrulama kullanan istemci / sunucu çözümü, yüksek değerli verilere erişim gerektiren kalıcı iş ilişkileri için daha uygun olabilir. İstemci tarafı sertifikalar kullanılıyorsa, tarayıcı tabanlı SSL bu tür bir uygulama için uygun olabilir. Ana fikir, kullanıcı bir dijital sertifika sayesinde bilindiğinde, VPN'in erişim kontrolü özelliklerinin bu kişiye şirketin ağındaki farklı kaynaklara erişimini sağlamak için kullanılabileceğidir. Bu kontrol seviyesi ve kullanıcının kim olduğu bilgisi, birçok şirketi dijital sertifika kullanmaya yönlendirmiştir. Açıkçası, bu büyük ölçekli extranet VPN uygulamalarında bir endişe kaynağıdır. Extranet VPN'deki PKI ile ilgili konular bu bölümün kapsamı dışındadır.

Varolan bir intranet VPN, extranet VPN uygulamak için temel olarak kullanılmalı mıdır? Bağlıdır risk kabul seviyesi ve ek maliyetler. Ekstranet bağlantılarını desteklemek için bir intranetin etkinleştirilmesi, ağ üzerinde sınırlı haklara sahip yeni bir kullanıcı sınıfını tanımlamak kadar basit olabilen oldukça basit bir işlemdir. Bununla birlikte, verilerin güvenliğini doğrudan etkileyebilecek bir extranet VPN tasarlamanın birkaç nüansı vardır. Örneğin bir extraneti etkinleştirmek için bir yaklaşım silahsızlaştırılmış bir bölge oluşturmaktır (örneğin dıştaki kullanıcıları desteklemek için çevre güvenlik duvarının üçüncü arayüzü). Bu çözüm intranet ve extranet kaynakları için güvenlik duvarı koruması ve VPN sunucusu üzerinden veri bütünlüğü ve gizliliği sağlar.

Ek 40.5, bir extranet VPN uygulaması için örnek bir değerlendirme profilini göstermektedir. Aşağıda listelenen öğelerin listesi extranet VPN için bir dizi değerlendirme kriteri geliştirilirken kullanılabilir.

**İç Ağın Güvenliğinin Sağlanması**

Veri gizliliğine yönelik sürekli içeriden tehdit nedeniyle, şirketler artık VPN ve güvenlik duvarları kullanarak iç ağ bölümlendirmesinin sadece daha fazla ürün satmaya çalışan güvenlik satıcıları tarafından yapılan bir satış aşaması olmadığını fark ediyorlar. Dış tehdit artıyor olsa da, veri güvenliğine yönelik iç tehdit sabit kalıyor. Bu nedenle, ortaya çıkan bir VPN uygulaması iç ağı güvence altına almaktır.

**Ek 40.5** Extranet VPN için Değerlendirme Profili

Basit kullanıcı adı / şifreler üzerinden güçlü karşılıklı kimlik doğrulamayı tercih edin

Erişim kontrolü ve günlüğe kaydetme çok önemlidir

Marka için müşteri özelleştirmesine izin veren çözümleri tercih edin

Minimum masaüstü ayak izi (masaüstü ortağın kontrolünde olmadığı için)

Normal uygulama kullanımına minimum müdahaleci olma

Önceden yapılandırılmış VPN istemcisi ve politikasının sessiz kurulumu

VPN istemcisinin kullanım kolaylığı anahtarıdır

Servis seviyesi izleme ve icra desteği

Bir ağın ağ güvenliği açısından bölümlenmesinin birçok yolu vardır. Tek bir yaklaşım iç ağı mantıksal olarak bölmektir. Diğer bir yaklaşım da ağı fiziksel olarak bölmektir. VPN teknoloji her iki yaklaşımda da kullanılabilir. Örneğin, fiziksel bölümlendirme bir hedef sunucuyu doğrudan bir VPN sunucusunun arkasına yerleştirerek sağlanabilir. Burada, hedef sunucuya erişmenin tek yolu VPN sunucusunun erişim kontrol politikasını sağlamaktır. Buradaki faydalar yönetimin basitliğini, açıkça tanımlanmış sınırları ve tek bir erişim noktasını içerir. Mantıksal bölümlendirmenin bir örneği, hedef sunucuya erişmesi gereken kullanıcılara VPN istemci yazılımı verilmesi durumudur. Kullanıcılar fiziksel olarak yerel veya uzak, iç ağda herhangi bir yere yerleştirilebilir. VPN istemci yazılımı, doğrudan veya dahili bir VPN ağ geçidi aracılığıyla otomatik olarak hedef sunucuyla şifrelenmiş bir oturum oluşturur. Böylece iç ağ, erişim kontrolü yoluyla mantıksal olarak “bölümlenir”. Başka bir mantıksal bölümleme senaryosu İç ağda eşler arası VPN oturumlarının kurulması gereken durum bu olacaktır. Bu durumda, iki veya daha fazla VPN istemcisi, geçici olarak gerektiğinde VPN bağlantısı kurar. Bu yapılandırmanın yararı, dinamik VPN'lerin veri gizliliğinin yanı sıra gerekli olan çok az kullanıcı yapılandırmasıyla kurulabilmesidir. VPN istemcileri, eşler arası VPN'de sağlam kullanıcı kimlik doğrulamasını desteklemiyorsa, bu yaklaşımın dezavantajı, kullanıcı kimlik doğrulama gücünü düşürür.

Ağ hiyerarşisinde VPN işlevselliğinin nerede uygulandığı ile ilgili yerleşim vurgusunda bir değişiklik olduğu görülüyor. Microsoft Windows 2000'in piyasaya sürülmesiyle, VPN teknolojisi, daha sonra özel donanım ve yazılım kullanılarak eklenmek yerine asıl işletim sistemine dahil ediliyor. Bu gelişmeyle birlikte, iç ağın güvenliğini sağlamak için kullanılabilecek VPN entegrasyon seviyesi, doğru şekilde uygulanırsa daha da derinleşir. VPN teknolojisi, sunucu düzeyinde, Microsoft Windows'ta ve UNIX'in çeşitli sürümlerinde uygulanmaktadır. Her ne kadar bu, VPN entegrasyon seviyesinin iç ağı güvence altına almak için gereken her şey olduğu anlamına gelmese de, güvenlikten bina inşa kavramını teşvik eder.başlayıp, baştan sona kullanarak. Bugüne kadar bir VPN'in doğrudan hedef uygulama sunucusunda uygulanması, performans üzerinde önemli bir etkiye sahiptir; bu nedenle, kriptografik işlevler için donanım ivmesi tipik olarak gereklidir.

İç ağ içinde veri gizliliği sağlama gerekliliği aynı şekilde karşılanabilir. uzaktan erişim VPN'in uygulanmasında kullanılan dağıtım ve yönetim yaklaşımları. Kullanıcı topluluğu genellikle aynıdır. Donanım platformu, özellikle çalışanlarına laptop ve diğer taşınabilir bilgisayarlar veren pek çok şirketle aynı olabilir. Dikkat edilmesi gereken bir fark, VPN istemcisine fiziksel olarak iç ağ içinde iken uygulanacak güvenlik politikasıdır; aynı donanım platformunu kullanırken iç ağa uzaktan erişim VPN üzerinden uzaktan erişmek için gereken politikadır. Durum, İnternet gibi bir toplu taşıma aracını geçerken, şirket verilerine yetkisiz erişim riskinin artması nedeniyle, kullanıcıların uzaktan giriş yaptıklarında daha sıkı bir güvenlik politikasına sahip olma konusunda temkinli olabilir. İç veya dış erişimde riskler aynı olsa da, uzaktan erişim VPN'i kullanırken saldırı olasılığı çok daha fazladır. Dahili ağlarda, LAN'lardaki iletişim için veri gizliliği sağlamak için VPN teknolojisinin başka bir uygulaması daha vardır. Potansiyel olarak yönetmenin operasyonel karmaşıklığı nedeniyle Microsoft Dosya Paylaşımı / SMB ortamındaki n-kare VPN bağlantıları, ancak, bazı şirketler tek bir "grup" veya LAN anahtarının yeterli olup olmadığını araştırıyor - bu tür dağıtımlarda, taşımadaki veri gizliliği kimlik doğrulamasından daha önemli.

Ek 9-6'daki dahili ağ VPN uygulamasını güvence altına almak için örnek bir değerlendirme profili.

**Ek 40.6** Dahili Ağ VPN Uygulamasının Güvenliğinin Sağlanması İçin Değerlendirme Profili

Güçlü kullanıcı kimlik doğrulaması

Güçlü erişim kontrolü

Gizlilik için politika temelli şifreleme

Transit veri bütünlüğü

Dahili ağ performansına düşük etki

Dahili ağ altyapısı üzerinde düşük etki

Kullanıcı masaüstüne düşük etki

Yönetim kolaylığı

Mevcut ağ bileşenleri ile entegrasyon

Operasyonel maliyetler (iş hedefine karşı tartıldığında büyük bir sorun olmayabilir)

VPN istemcisi sorunları:

Kullanıcı şeffaflığı (kullanıcı farklı bir şey yapmak zorunda mı?)

Uzaktan erişim ve dahili VPN poliçesi arasında otomatik fark (VPN istemcisi, dahili / harici güvenlik politikası değişikliklerine otomatik olarak uyarlanabilir mi?)

**VPN Dağıtım Modelleri**

Bu bölümde ele alınan dört VPN sunucusu dağıtım modeli vardır: özel donanım / cihaz, yazılım tabanlı, yönlendirici tabanlı ve güvenlik duvarı tabanlı. Kullanılan VPN platformunun türü, gereken güvenlik seviyesine, performans gereksinimlerine, ağ altyapısı entegrasyon çabalarına ve uygulama ve işletme maliyetlerine bağlıdır. Bu tartışma şimdi VPN olarak VPN sunucusu dağıtımıyla ilgili konulara yoğunlaşıyor müşteri dağıtımı önceki bölümlerde ele alınmıştır.

**Özel Donanım VPN Uygulaması**

Gelişmekte olan bir VPN sunucu platformu, özel bir donanım cihazına veya amaca yönelik yapılmış bir VPN'e aittir. Özel amaçlı donanım kullanımı, tek amaçlı, yüksek derecede optimize edilmiş tasarımının (bazı açılardan) kullanımının daha kolay, yönetilmesi kolay, anlaşılması daha kolay ve birçok durumda düşük maliyetli olduğu gerçeği nedeniyle popüler hale gelmiştir. Bu tür bir platformun arkasındaki fikir, yaygın ev aletleri örneğine benzemektedir. Örneğin, çok az kişi bir ekmek kızartma makinesi satın alır ve sonra eve getirdikten sonra değiştirmeyi dener. Burada kavrama kavramı anahtar teslimi

Bu birimler tipik olarak standart donanım konfigürasyonlarında satılmaktadır. Amaca yönelik üretilmiş VPN cihazları, genellikle yüksek olduğunda diğer platformlara göre avantaja sahiptir. Donanımda şifreleme gerçekleştirmenin hız verimliliği nedeniyle performans. En çok amaçlı VPN cihazlar özel olarak verimli bir şekilde çalıştırılmak üzere optimize edilmiş özel bir gerçek zamanlı işletim sistemine entegre edilmiştir tasarlanmış donanım. Birçok düşük kaliteli VPN cihazı, Intel platformunda çalışan, değiştirilmiş bir Linux veya BSD işletim sistemi kullanır. Birçok VPN cihazı önceden yapılandırılabilir, uzak bir siteye gönderilebilir ve kolayca kurulabilir ve uzaktan yönetilebilir. Buradaki avantaj, büyük ölçekli dağıtımlarda hızlı uygulamadır. Bu dağıtım modeli, birçok uzak ofis, büyük telekom operatörü, ISS ve yönetilen güvenlik hizmeti sağlayıcısı olan büyük işletmeler tarafından kullanılır. Bir kuruluşta BT personeli yetersizse, VPN cihazları yüksek oranda dağıtılmış bir VPN uygulamak için insan kaynakları gereksinimini büyük ölçüde azaltabilir.

Donanım VPN aygıtları kullanarak büyük ölçekli, yüksek oranda dağıtılmış bir VPN dağıtmaya yönelik bir yaklaşım:cihaz tarafından kullanılacak temel ağ parametrelerini önceden yapılandırın, (2) VPN'i önceden kurun cihazın dijital sertifikası, (3) cihazı uzak konumuna gönderir ve (4) sonra Uzak konum, cihazın temel fiziksel kurulumunu gerçekleştirir. Ünite elektrik prizine takıldıktan ve açıldıktan sonra, ağ kabloları bağlanabilir ve ünite daha sonra gerektiğinde yapılandırma görevlerini tamamlamak için uzaktan yönetim için hazır olmalıdır. VPN kullanımının sakıncaları ev aletleri yaklaşımı, VPN ev aletleri ürününün tek bedene uyan her tasarım konseptini içermez.daima bir VPN cihazında donanım değişikliklerini satıcının desteğine izin verin. Ek olarak, tescilli işletim sistemleri kullanan VPN cihazları başka bir işletim sisteminin öğrenilmesi anlamına gelebilir ve mevcut sistem yönetimi araçlarıyla net bir şekilde birlikte çalışmayabilir. Sonuç olarak: eğer bir VPN cihazının donanımını kendiniz değiştirmeyi planlıyorsanız, o zaman VPN cihazları gitmenin yolu olmayabilir.

Birçok taşıyıcı sınıfı VPN anahtarı - on binlerce kişiyi sağlayabilen VPN ağ geçitleri ayrı bağlantılar - telcos, ISS'ler veya büyük işletme işletme ağları gibi büyük ölçekli telekomünikasyon ağlarının gereksinimlerine uyan başka bir VPN bileşeni sınıfıdır. Taşıyıcı sınıfı VPN'in özellikleri ağ geçitleri daha az deneyimli personelin performans göstermesine olanak sağlayan hızlı ve kolay kurulum ve konfigürasyon içerir tesisatlar. Yüksek verimlilik, yani büyümekte olan bir işletmenin ihtiyaçlarını karşılayabilir ve dağıtımı kolay istemci yazılımı ayrıca taşıyıcı sınıfı VPN ağ geçitleri için farklılaştırıcılardır.

**Yazılım Tabanlı VPN**

Yazılım tabanlı VPN sunucuları genellikle VPN yazılımının genel amaçlı bir bilgisayara kurulmasını gerektirir. genel amaçlı bir işletim sisteminde çalışan. Desteklenen tipik işletim sistemleri olma eğilimindedir. Hangi işletim sistemi olursa olsun pazar lideridir. Bu, Microsoft Windows tabanlı ve UNIX tabanlı işletim sistemlerini de içeriyor. Bazı yazılım tabanlı VPN'ler kurulum sırasında işletim sistemini değiştirerek güvenlik sağlamlaştırması, bir miktar performans optimizasyonu veya ağ arayüz kartlarının ince ayarını yapacaktır. Yazılım tabanlı VPN'ler, VPN stratejisinin, cihazın anahtar teslimi konseptinden dolayı bir şekilde VPN donanımının ana bileşenlerini yükseltmesi veya "düzenlemesi" durumunda gösterilebilir. yaklaşım. Ayrıca, VPN yazılımı yaklaşımı, mevcut olanı kullanarak maliyetleri en aza indirmeyi planlıyorsa belirtilir.genel amaçlı bilgi işlem donanımı.

Yazılım tabanlı VPN sunucularının dezavantajları tipik olarak karşılaştırıldığında performans düşüşüdür. amaca yönelik inşa edilmiş VPN cihazları, sunucu donanımı ve işletim sistemi mevcut değilse edinilmelidir, donanım şifreleme kartları için ek ücret ve işlemi sertleştirmek için gereken ilave çaba sistemi. Yük dengeleme ve donanım şifrelemesi kullanma gibi uygun ölçeklenebilirlik tekniklerinin uygulanması Ek kartlar bu dezavantajları azaltabilir. Ayrıca, yalnızca VPN yazılımı yaklaşımı, genellikle daha düşük maliyetli bir peşin alım fiyatına sahiptir. Bazen, yazılım işletim sistemine yerleşiktir; örneğin, Microsoft Windows 2000 Server bir IPSec VPN sunucusu içerir.

Bazı üreticilerin yazılım VPN ürünleri, merkezi bir yönetim konsolu kullanılarak yönetilemeyen veya her platformda farklı bir görünüme sahip olan birden fazla platformda desteklenir. Tutarlı sağlamak için uygulama ve yönetilebilirlik, donanım platformlarında ve işletim sistemlerinde standardize olmak mantıklı geliyor. Platformlarda standardizasyon sağlayarak, öğrenme eğrisi en aza indirilebilir ve platform tabanlı özel durumlar ortadan kaldırılabilir.

**Router Tabanlı VPN'ler**

Bir VPN dağıtımı için düşük maliyetli bir giriş noktası, VPN işlevselliğine sahip mevcut yönlendiricileri kullanmaktır. Tarafından mevcut ağ kaynaklarından yararlanma, uygulama maliyetleri düşürülebilir ve ağa entegrasyon yönetim altyapısı daha kolay bir şekilde gerçekleştirilebilir. Bugün birçok yönlendirici VPN protokolünü ve daha yeni yönlendiriciler VPN trafiğini daha verimli bir şekilde işlemek için geliştirilmiştir. Ancak, bir yönlendiricinin birincil işlevi ağ paketlerini bir ağdan diğer bir ağa yönlendirmek; bu nedenle, yönlendirme performansı ve VPN işlevselliği arasında takas kararı verilmesi gerekebilir. Bazı yönlendirici modelleri, ek VPN işleme yeteneği eklemek için donanım yükseltmelerini destekler. Mevcut yönlendiricileri yükseltme yeteneği, VPN kullanıcı topluluğu büyüdükçe bir geçiş yolu sağlar. Birçok yönlendirici tabanlı VPN, dijital desteği içerir sertifikalar. Bazı durumlarda, dijital sertifikaların metin dosyalarının kesilmesi ve yapıştırılması yoluyla manuel olarak talep edilmesi ve edinilmesi gerekir. VPN düğümlerinin sayısına bağlı olarak, bu ölçeklenebilirliği etkileyebilir. VPN özellikli yönlendiriciler, güçlü güvenlik yönetimi araçları gerektirir - normalde donanım aracı ve yazılım VPN'leriyle birlikte verilen aynı tür araçlar

Yönlendirici tabanlı VPN tüneli nerede sonlandırılmalıdır? Tünel iki yerden birinde sonlandırılabilir: Bir erişim yönlendiricisine VPN eklerken veya arkadaki tünel trafiğini sonlandırırken şebeke çevresinin dışında Bir iç yönlendiriciye VPN eklerken güvenlik duvarı.

**Güvenlik Duvarı Tabanlı VPN'ler**

Güvenlik duvarları, bir ağa giren trafikle ilgili kararlara izin vermek / reddetmek için tasarlanmıştır. Birçok şirket zaten ağlarının çevresinde güvenlik duvarı uygulamaktadır. Birçok güvenlik duvarının VPN uç noktaları olarak kullanılmak üzere yükseltilmesi özelliği vardır. Bu durumda, bazı kuruluşlar için mevcut güvenlik duvarlarının VPN yeteneklerini araştırmak mantıklı olabilir. Bu, önceden oluşabilecek maliyetleri azaltmak için mevcut ağ altyapısından yararlanmanın bir başka örneğidir. Güvenlik duvarlarını VPN uç noktası olarak kullanmayla ilgili bir endişe performans olacaktır. Bir ağa giren veya çıkan tüm trafik bir güvenlik duvarından geçtiğinden, güvenlik duvarı zaten aşırı yüklenmiş olabilir. Ancak bazı güvenlik duvarı satıcıları donanım şifreleme eklentileri sunar. Herhangi bir yapılandırılabilir güvenlik cihazında olduğu gibi, herhangi bir Güvenlik duvarında yapılan değişiklikler güvenliğini tehlikeye atabilir. VPN yönetimi, güvenlik duvarı tarafından sağlanan ortak bir yönetim arayüzü kullanılarak geliştirilmiştir. Çevre güvenlik duvarı olarak bu, VPN için ideal bir konumdur, çünkü girişi / çıkışı tek bir noktaya ayırır. VPN sunucusunu güvenlik duvarına eklemek, donanım, yazılım ve yönlendirici VPN'lerle ilişkili yerleşim sorunlarını ortadan kaldırır; örneğin, şifreli paketler güvenlik duvarındaki bir delikten geçirilmelidir, güvenlik duvarı NAT vb. yaparsa ne olur?

Güvenlik duvarı / VPN yaklaşımı ayrıca güvenlik duvarındaki VPN tünellerinin sonlandırılmasına, şifre çözme ve verilerin denetlenmesine izin verir. Bu kabiliyetin avantajlı olduğu bir senaryo, güvenlik duvarı tabanlı anti-virüs yazılımının VPN tünelinden geçen verilere karşı çalıştırılması gerektiğidir.

**Herhangi bir VPN için Genel Yönetim Sorunları**

Yazılım tabanlı VPN'i kimin yönetmesi gerektiği sorusu ortaya çıkıyor. Yönetim arasında bölünebilir bir ağ işlemleri grubu, bir güvenlik grubu ve veri sahibi. Ağ işlemlerinin yapılması gerekecek uygulama ve tasarım kararları almaya dahil, çünkü bu grup genellikle bir şirketin veri ve veri bütünlüğünün kullanılabilirliğini korumakla yükümlüdür. Güvenlik grubunun, güvenlik politikasına uygunluğu sağlamak için genel sistem tasarımını ve kabiliyetini analiz etmesi gerekir. Veri sahibi, bu durumda, erişimi sınırlamak için VPN kullanan operasyonel gruba atıfta bulunur. Veri sahibi, erişim kontrolü ve kullanıcı hesabı kurulumundan sorumlu olabilir.

İdeal bir durumda, bu işbölümü VPN operasyonlarına dağıtılmış bir yönetim yaklaşımı sağlayacaktır. Uygulamada, bu yaklaşımın pratik olması için gereken işbirliği düzeyi nadiren görülür.

**VPN Performansını Değerlendirme**

Bu noktada, VPN’leri son kullanıcı ve yönetici bakış açılarından değerlendirme kriterlerini tartıştık. Ancak, VPN satıcılarının bir pazarlama aracı olarak performans için nasıl bir ölçüt oluşturduklarını anlamak da anlayışlıdır. Pek çok satıcı, eşzamanlı VPN bağlantısı sayısına, maksimum oturum sayısına veya verime göre sınıflandırdıkları VPN ürünleri sunar. Çoğu güvenlik uzmanı uygulamanın ne kadar güvenli olduğu ile ilgilenmektedir; çoğu ağ operasyon personeli, özellikle ISS personeli, kaç müşteri veya uzak kullanıcı tünelinin bir VPN ağ geçidi tarafından desteklenmesiyle ilgilenmektedir. Bir IPSec uzak kullanıcı tüneli olabilir. IKE faz 1 ve faz 2 anahtar değişimlerinin tamamlanması olarak tanımlanır. Bu aşamalar tamamlanmalı Her uzak iletişim oturumu için güvenli bir tünel oluşturarak dört güvenlik birliği sağlayın. Bu öznel bir tanım çünkü satıcılar tipik olarak performans iddialarını mümkün olan en iyi ışığa sokmak için çeşitli tanımlar oluştururlar.

Birçok satıcı VPN verimini karakterize etmek için tek bir numara vermesine rağmen, gerçek dünya dağıtımlarında, performans birçok koşullara bağlı olarak değişecektir. Bu bölüm, gerçek dünya dağıtımlarındaki verimi etkileyen faktörlerin bir özetini sunar.

**Paket Boyutu**

Veri şifreleme ve kimlik doğrulama gibi çoğu VPN işlemi paket başına gerçekleştirilir. İşlemci ek yük büyük ölçüde paket büyüklüğünden bağımsızdır. Bu nedenle, daha büyük paket boyutları genellikle daha yüksek verilere yol açar verim rakamları. İnternetteki ortalama IP paket büyüklüğü yaklaşık 300 bayttır. Ne yazık ki, çoğu satıcı, nispeten büyük ortalama 1000 baytlık paket boyutlarına dayanan VPN işlem hacmi özelliklerini belirtir. Sonuç olarak, kuruluşlar, satıcılardan beklenen performansı daha iyi ölçmek için bir dizi ortalama paket boyutunun üzerinde verim spesifikasyonları istemelidir.

**Şifreleme ve Kimlik Doğrulama Algoritmaları**

Daha güçlü şifreleme algoritmaları, matematik işlemlerini tamamlamak için daha büyük sistem kaynakları gerektirir, bu da daha düşük veri akışı sağlar. Örneğin, DES (56 bit güçlü) şifrelemeye dayalı VPN çıkışı, 3DES (168 bit güçlü) şifrelemeye göre daha büyük olabilir. Akış şifreleri tipik olarak blok şifrelere göre daha hızlıdır.

Veri kimlik doğrulama algoritmaları veri çıkışı üzerinde benzer bir etkiye sahip olabilir. Örneğin, MD5 kullanarak kimlik doğrulaması, SHA1 ile karşılaştırıldığında biraz daha büyük bir verime neden olabilir.

**Ana CPU**

Yazılım tabanlı VPN çözümleri, müşterilere sınıf ve saate göre değişen çeşitli merkezi işlemciler sunar. hız. Ana bilgisayar işleme gücü, isteğe bağlı donanım tabanlı bir seçenek sunmayan VPN ürünleriyle özellikle önemlidir hızlanma. VPN testi, VPN sunucularına ek genel amaçlı CPU'lar eklenerek performansın doğrusal olarak artmadığını göstermiştir. Bir satıcı, bir Windows NT sunucusunda, bir işlemci yüzde 100 yüklüyse, ikinci bir işlemci eklenmesinin CPU kaynaklarını yalnızca yüzde 5 serbest bıraktığını iddia ediyor. Satıcı, sunucuya genel amaçlı CPU'lar eklemek yerine şifreleme hızlandırma donanımı kullanırken, verimde yedi kat artış olduğunu iddia ediyor. Diğer durumlarda, genel amaçlı CPU'ların eklenmesi, donanım ivmesi eklenmesine kıyasla fiyat / performans esasına göre daha ağır basar. Bir durumda, genel amaçlı CPU eklemenin maliyeti donanım hızlandırma kartının fiyatının yaklaşık iki katı, esasen daha az performans artışıyla. Hız sadece bir CPU faktörü değil, aynı zamanda bir G / Ç veri yolu, RAM ve önbellek faktörüdür. Azaltılmış Komut Seti İşlemciler, RISC işlemcileri, genel amaçlı işlemcilerden daha hızlıdır ve Uygulamaya Özel Tümleşik Devreler, ASIC'ler genellikle yapmak için tasarlandıkları işlerde RISC işlemcilerinden daha hızlıdır.

**İşletim Sistemi ve Yama Seviyeleri**

Pek çok yazılım tabanlı VPN çözümü, müşterilere ticari işletim sistemi seçenekleri sunar. İşletim sistemlerinden elmadan elmaya karşılaştırmaların zor olmasına rağmen, müşteriler performans karşılaştırma ölçütlerinin hedef işletim sistemlerine özgü olduğundan emin olmalıdır. Ayrıca, işletim sistemi düzeltme eki düzeylerinin de önemli bir verimlilik etkisi olabilir. Genellikle, en güncel işletim sistemi düzeltme eki düzeyleri daha iyi performans sağlar. VPN gereksinimi işletim sistemi tabanlı VPN teknolojisini kullanmaksa, çoğu yazılım güvenlik duvarında olduğu gibi işletim sistemlerinin gerekli "sertleşmesini" sağlayan yazılım ürünlerini göz önünde bulundurun. Yazılım güncellemeleri, güvenlik uyarıları ve yama güncellemeleri sunan devam eden servis planlarına abone olmayı düşünün.

**Ağ Arabirim Kartı Sürücüleri**

Ağ arabirim kartı (NIC) sürüm seviyeleri verimi etkileyebilir. Genellikle, en güncel ağ arayüzü kart sürücüleri en iyi performansı sunuyor. Birkaç ağ arabirim kartı üreticisi şimdi IPSec tabanlı VPN'lere tamamlayıcı işlevler gerçekleştiren ürünler sunuyor. NIC'ler kullanıcı bilgisayarlarına veya şifreleme / şifre çözme gerçekleştiren IPSec VPN ağ geçitlerine kurulabilir, böylece CPU kullanımını azaltma. Bu işlem, doğrudan NIC'ye bir işlemci kurmak suretiyle gerçekleştirilir; bu, NIC'nin daha fazla ağ trafiği işleme yükünü paylaşmasını sağlar; böylece ana bilgisayar sistemi, hizmet uygulamalarına odaklanabilir.

**Hafıza**

Bir VPN'nin uzaktaki bir kullanıcı tüneli bazında ölçeklendirilebilmesi, ağ geçidi sunucusunda kurulu olan sistem belleği miktarına bağlıdır. Pek çok VPN cihazı çözümünden farklı olarak (sabit miktarda bellekle sınırlıdır), yazılım tabanlı bir VPN, eşzamanlı bağlantıları ve uzak kullanıcı tünellerini, çekirdeğin oluşturduğu maksimum eşzamanlı bağlantıları destekleyerek sınırlandırır. Bazı durumlarda, eşzamanlı bağlantılar, ana bilgisayarın çekirdek sınırlarından bağımsız olan VPN uygulaması proxy bağlantı sınırları ile sınırlıdır. Bununla birlikte, çoğu VPN dağıtımının, bağlantı sınırlamalarına ulaşmadan önce verimlilik sınırlamaları ile karşılaşabileceğini anlamak önemlidir. Yalnızca yazılım tabanlı VPN platformlarının bellek genişletilebilirliğini ve özel donanımın verimlilik avantajlarını birleştirerek her iki dünyanın da en iyisini elde edebilirsiniz. Aşağıdaki varsayımsal örneği ele alalım. Bir kuruluşta, donanım hızlandırıcılığının yüklü olduğu yazılım tabanlı bir VPN'e bağlı 30 Mbps İnternet bağlantısı vardır. Bu kuruluş için, tek bir uzak kullanıcı için gerekli ortalama veri hızı yaklaşık olarak 40K'dır. Bu senaryoda, VPN yaklaşık 750 eşzamanlı uzak kullanıcıyı destekleyecektir (30 MB / 40K). Kullanıcı sayısı 750 kullanıcının ötesine geçtiğinde, ortalama veri oranları ve ilgili kullanıcı deneyimi düşmeye başlayacaktır. Bu örnekten, güvenilir, eşzamanlı kullanıcı desteğinin, kurulan bağlantı sayısındaki sınırlamalardan ziyade, yazılım-tabanlı VPN ağ geçidi verimi tarafından sınırlandırılmasının daha muhtemel olduğu açıktır. Bu açıdan bakıldığında, şifreleme hızlandırıcı kartı, binlerce kullanıcıyı desteklemek için yazılım tabanlı bir VPN dağıtımını ölçeklendirmede önemli bir etkendir.

Tek bir sayı, VPN'in performans performansını etkili bir şekilde tanımlamaz. Örneğin, sistem tarafından aktarılan paketlerin büyüklüğü verimlilik üzerinde önemli bir etkiye sahiptir. Sistem performansı daha küçük paket boyutlarıyla azalır. Paket boyutu ne kadar küçük olursa, saniyede işlenen paket sayısı da o kadar fazla olur, ek yük de o kadar yüksek olur ve bu nedenle de etkili verim düşer. Bir şifreleme hızlandırıcı kart olabilir Performansın tüm paket boyutları için optimize edilmesini sağlamak için hem büyük hem de küçük paketler için ayarlanmıştır. Performansı etkileyebilecek diğer faktörler arasında sistem yapılandırması (CPU, bellek, önbellek vb.), Şifreleme algoritmaları, kimlik doğrulama algoritmaları, işletim sistemi ve trafik türleri. Bu faktörlerin çoğu tüm VPN ürünleri için geçerlidir. Bu nedenle, rekabetçi VPN ürünlerinin performans özelliklerinin, bu sayıların tüm ortamlarda doğrudan karşılaştırılabileceği veya elde edilebileceği anlamına geldiğini varsaymayın.

**Veri Sıkıştırma Yardımları**

Performansı artırmak ve son kullanıcılar arasındaki memnuniyeti artırmak için ulaşılması gereken bir amaç, gecikmeyi en aza indirmektir. VPN’de Gecikmeyi en aza indirmenin bir yolu daha az trafik göndermektir. Bu amaç, verileri VPN'ye koymadan önce sıkıştırarak başarılabilir. Sıkıştırmadan elde edilen performans kazancı, ne tür veri gönderildiğine bağlı olarak değişir; Ancak, genel olarak, veriler bir kez şifrelenmişse, şifrelenmemiş olduğu gibi sıkıştırılmaz. Veri sıkıştırma, özellikle düşük bant genişliğine sahip analog çevirmeli VPN erişimini optimize ederken, MTU boyutu ve parçalanmanın faktör olabileceği durumlarda, önemli bir performans arttırıcıdır.

**Ham Performans En Önemli Kriterler mi?**

Amacı, kullanıcıların hangi özellikleri VPN'leri değerlendirmede en önemli olduğunu düşündüklerini ve gelecekteki tekliflerde görmek istediklerini keşfetmek olan bir VPN kullanıcısı anketine göre, performans VPN'leri değerlendirirken öncelikli olarak güvenlikten daha yüksek olarak değerlendirildi. Bu, çok az kişinin VPN teknolojisinin güvenliğine ikna olduğu VPN'in ilk günlerinden düşünmede bir kaymaya işaret ediyor.

Bu özellikle VPN teknolojilerine ve ürünlerine aşinalıklarını “yüksek” olarak değerlendiren güvenlik profesyonelleri için geçerlidir. VPN’leri anlayanlar güvenlik ürünlerine güven duyuyorlar ve bunun farkındalar. performans ve yönetim sonraki büyük savaşlar. Anket sonuçlarına göre, birçok kullanıcı, temel güvenlik bileşenleri bir endişe kaynağı olsa da, VPN performansından ödün verilmemesi gerektiğini düşünüyor. Ankete göre, kullanıcılar performans, uygulama güvenliği ve kullanılabilirlik gibi üst düzey özellikler hakkında daha fazla endişe duyuyor ve VPN'in altında yatan teknolojiler ve protokoller hakkında daha az endişe duyuyorlar.

**VPN'yi Dış Kaynak Kullanımı**

Bilgili bir servis sağlayıcıya yapılan dış kaynak kullanımı, sorun giderme için bir uzmana sahip olmanın getirdiği bir güvenlik duygusu sunabilir. Dış kaynak kullanımı, şirket içi güvenlik yöneticilerini, şube ofisleri ağa eklenmesi gereken uzak kullanıcıları kurup test ederken VPN'lerini fiziksel olarak yükseltme ile ilgili sorunlardan kurtarır. Bir şirket coğrafi olarak dağınık bir omurgasına sahip olmadıkça, en azından VPN'in transit kısmının bir İnternet erişim servis sağlayıcısı veya özel IP ağ sağlayıcısı tarafından dış kaynaklı olması gerekir. Ancak, genel bir İnternet erişim hesabı, VPN trafiğinin yoğun saatlerde İnternet'teki trafiğin geri kalanıyla engellenmeyeceğinin güvencesini sağlamamaktadır. ISS veya VPN servis sağlayıcısı, gerekli donanım ve yazılımı seçip kurabilir, ayrıca teknik destek ve devam eden bakım görevlerini üstlenebilir.

Ek 40.7, bir VPN servis sağlayıcısını değerlendirirken göz önünde bulundurulması gereken bazı faktörleri listeler.

**Güvenilirlik**

Kullanıcılar ağa bağlanamıyorsa ve verimli bir bağlantı kuramıyorsa, güvenlik önemsizdir. VPN'nin hedefi mobil çalışanlara uzaktan erişim sağlamaksa, performansın kilit bir yönü, hizmet sağlayıcının ihtiyaç duyacağı coğrafi bölgelerde sahip olacağı nokta sayısı olacaktır. servisin yanı sıra, servis sağlayıcının çevirmeli bağlantı erişimindeki başarı oranları bakımından yapabileceği garantileri de içerir. Örneğin, bir VPN servis sağlayıcısı (ulaşım ve güvenlik hizmetleri sağlar), zamanın yüzde 99'u 26,4 KBps veya daha yüksek ilk modem bağlantı hızı ile yüzde 97 oranında meşgul arama veya uzaktan erişim sunar. Başka bir VPN servis sağlayıcısı (ulaşım ve güvenlik hizmetleri sağlar),% 100 ağ kullanılabilirliğini ve çevirmeli bağlantı hizmeti için yüzde 95 bağlantı başarı oranını desteklemektedir. Bu garantiler karşılanmadığında, servis sağlayıcı tipik olarak bir tür finansal tazminat veya hizmet kredisi vaat eder. VPN taşıma ve güvenlik hizmetleri bağımsız olarak dış kaynaklı olabilir.

**Ek 40.7** Bir VPN servis sağlayıcısının değerlendirilmesi

Bir VPN servis sağlayıcısını değerlendirirken göz önünde bulundurulacak faktörler şunlardır:

Hizmet kalitesi

Güvenlik

idare edilebilirlik

Sağlayıcının kendi ağlarının ve ağ operasyon merkezlerinin menkul kıymetleri

Sağlayıcının işe alım uygulamalarını araştırın (uzmanlık, geçmiş kontrolleri)

Sağlayıcı hangi dağıtım öncesi ve sonrası hizmetleri sunmaktadır (güvenlik açığı değerlendirmesi, adli tıp)

Ancak, asıl amaç şirket için geniş bir alan ağı sağlamaksa, genel ağ kullanılabilirliği hız birincil endişe olmalı. Sağlayıcılar şu anda bunu belirli bir seviyeyi garanti ederek ölçüyorlar. genel ağ ortalamalarına bağlı olarak verimlilik, gecikme ve kullanılabilirlik gibi performans. Kendi omurgalarını oluşturan sağlayıcılar, birçok müşteri VPN'sini desteklemek için bunları kullanır. Bazı VPN servis sağlayıcıları, müşteri VPN'leri için Asenkron Aktarım Modu veya Frame Relay aktarımı yoluyla özel WAN hizmeti sağlar. Bu şekilde, VPN trafiğinin bant genişliği için genel İnternet trafiğiyle rekabet etmesi gerekmez ve VPN servis sağlayıcısı, ağın uçtan uca performansını yönetmek için daha iyi bir iş yapabilir.

**Hizmet Kalitesi**

VPN servis sağlayıcıları, ses verileri gibi performansa duyarlı trafik için garantiler sunmaya başlıyor ve multimedya. Örneğin, bir ağ, akışlı bir video aktarımına dosya indirme yerine daha yüksek öncelik verebilir, çünkü videonun kullanılabilir olması için hızlı aktarım yapmasını gerektirir. Buradaki zorluk, bu garantiyi ağ sınırları içerisinde sunabilmektir. Şu anda tek bir ağ üzerinden seyahat eden trafik ile mümkün olsa da, birkaç ağ üzerinden geçmesi gereken trafik için neredeyse imkansızdır. Bunun nedeni, MPLS gibi standartların gelişmesine rağmen, bir ağ üzerinden trafiğe öncelik vermek için internetin çok daha az öncelikleri için mevcut tek bir standart bulunmamasıdır.

Daha iyi performans sağlamak için, birçok VPN servis sağlayıcısı servis seviyesi anlaşmaları sunar. Ek bir ücret karşılığında, servis kalitesi ile orantılı olarak bir VPN servis sağlayıcısı, müşterilerine verim, çevirmeli erişim ve ağ kullanılabilirliği konusunda garanti verebilir. Bazı VPN servis sağlayıcılarının, VPN trafiğinin büyük kısmının yönlendirildiği, kendi Özel Çerçeve Rölesi veya Asenkron Ttransfer modu şebekeleri vardır. arttırıcı performans

**Güvenlik**

Bir VPN, şifreleme, tünel oluşturma ve kimlik doğrulama / yetkilendirme kombinasyonu ile güvenlik sağlar. Güvenlik duvarı, yalnızca güvenilir, yetkili paketlere veya kullanıcıların erişmesine izin vererek çevre güvenliği savunması sağlar. kurumsal ağa. Şirketler VPN servis sağlayıcılarının güvenlik yöntemini seçmesini seçebilir VPN'leri için ve şirket içinde yönetebilir veya servis sağlayıcının bu işlevi yönetmesine izin verebilir. Diğer bir seçenek ise müşterinin VPN'in güvenlik politikası tanımını tamamen ele almasıdır. Çoğu güvenlik yöneticisi, özellikle son kullanıcı yönetimi, politika ve kimlik doğrulama alanlarında, ağlarının güvenliği üzerinde bir miktar kontrol sahibi olmayı tercih eder. Bir şirket kendi şifrelemesini yapmayı seçebilir, örneğin kendi güvenlik sunucusunu yönetebilir, ancak VPN servis sağlayıcısını, VPN yönetiminin uyarıları izlemek ve yanıtlamak gibi diğer yönleri için kullanabilir. Güvenliği bazılarının dış kaynaklardan sağlayıp sağlamama kararı, bir şirketin büyüklüğü ve BT kaynaklarıyla ilgili olmalıdır. Diğerleri için, dış kaynak kararlarının, kurumsal verilerin kritik niteliği ve BT yöneticisinin genel olarak dış kaynak sağladığı güven ile ilgisi vardır.

Sergi 40.7, dış kaynaklı VPN'leri değerlendirirken dikkate alınması gereken faktörleri sıralar.

**İdare Edilebilirlik**

Dikkate alınması gereken bir diğer husus, VPN servis sağlayıcısından ihtiyaç duyulan yönetim ve raporlama yetenekleridir. Birçok VPN servis sağlayıcısı, abonelere ağ performans verilerine ve müşteri kullanım raporlarına bir tür Web tabanlı erişim sunar. Web tabanlı araçlar, kullanıcıların yürütme gibi görevleri gerçekleştirmelerini sağlar uzaktan yapılandırma güncellemeleri, kullanıcı ekleme / silme, dijital sertifikaların verilişini kontrol etme ve performans düzeyindeki verilerin izlenmesi. VPN servis sağlayıcısının, müşterilerin kullanıcı ekleyip silebileceği ve politika değişikliklerini üst düzeyde gönderebilmesi için bölünmüş yönetime izin veren ürünler sunup sunmadığını kontrol edin.

**Özet**

Bir VPN değerlendirme stratejisi oluşturmak, güvenlik uzmanlarının bir şirketin kendi VPN sistem gereksinimlerini karşılayan gerçek özelliklerden satıcı yutturmacalarını belirlemelerini sağlar. Anahtar, ihtiyaç duyulan VPN uygulama türüyle eşleşen bir strateji ve ölçüt seti geliştirmektir. Değerlendirme kriterleri tam olarak neyin gerekli olduğunu tanımlamalıdır. Bir uygulamalı laboratuar değerlendirmesi, güvenlik uzmanının tam olarak neyin verileceğini anlamasına yardımcı olacaktır. VPN kurulumunun ayrıntılarına özellikle dikkat edin ve seçilen herhangi bir VPN servis sağlayıcısı veya ürün satıcısı ile dikkatli olun.

Benzer şekilde, iyi düşünülmüş bir VPN dağıtım stratejisi, uygulama maliyetlerini düşürmeye, artırmaya yardımcı olacak kullanıcı kabulü ve yatırım getirisini hızlandırmak. Dağıtım stratejisi, VPN uygulamasının türüne ve seçilen dağıtım modeline bağlı olarak değişecektir.

Satıcılar geleneksel olarak müşterilere mümkün olduğunca az karar noktası sunarak satış döngüsünü kolaylaştırmak istiyor. Bunu yapmanın bir yolu, VPN ürününün performans özelliklerini aşırı basitleştirmektir. Küçük, orta veya büyük boyutlu bir boyut mu istiyorsunuz? 10 kullanıcı VPN sunucusu, 100 kullanıcı VPN sunucusu veya mega kullanıcı VPN sunucusu ister misiniz? 100 MHz ya da 1 Gigabit modelini ister misiniz? VPN satıcılarının taleplerini doğrulamak için kullanılan parametreleri sağlamaları konusunda ısrar ediyorlar. Güvenlik uzmanlarının, satıcılar tarafından kullanılan ölçümleri ve doğrulama yöntemlerini anlamaları önemlidir. Bu bilgi ile donanmış güvenlik uzmanları ürün seçerken bilinçli kararlar alabilirler.

VPN uygulamak için birçok seçenek vardır. Yönetilen güvenlik servis sağlayıcıları kolaylaştırabilir yükün bir kısmı ve VPN’lerin hızlı bir şekilde uygulanmasına yardımcı olur. Bununla birlikte, güvenlik uzmanları bir servis sağlayıcı seçerken gerekli özeni göstererek iyi çalışacaktır.

**Sözlük**

**ATM** (Asenkron Aktarım Modu) Çok yüksek hızlara sahip dijital iletişim araçları; Verilerin yanı sıra görüntülerin veya sesin veya videonun iletimi için de uygundur. Yaygın olarak omurga içine yerleştirilmiş ağlar.

**DSL** (Dijital Abone Hattı) Abonelerine geniş bantlı erişim sağlamak için rekabetçi yerel değişim şirketleri ve yerel telefon şirketleri tarafından sağlanan, yüksek hızlı dijital hatlar ailesinin genel ismi.

**FTP** (Dosya Aktarım Protokolü) Kullanıcıların, yerel sistemleriyle bir ağda erişebilecekleri herhangi bir sistem arasında dosya kopyalamalarını sağlayan bir protokol. FTP istemcisi ve FTP sunucusundan oluşur.

**IKE** (İnternet Anahtar Değişimi) IPSec VPN'lerinde, bir IPSec VPN oturumu sırasında kullanılacak güvenlik parametrelerini belirlemek için kullanılan bir güvenlik protokolü (güvenlik birliği olarak adlandırılır).

**IPSec** (IP Güvenliği protokolü) VPN'lerde kullanılan ve güvenli IP paketlerinin formatını ve iletimini belirleyen şifreleme ve veri bütünlüğü algoritmalarını ve kurallarını tanımlayan standart bir protokol takımı.

**Kbps** Saniyedeki kilobit sayısı.

**Mbps** Saniyedeki megabitler.

**MSP** (Yönetilen Güvenlik Servis Sağlayıcısı) Varsaymayı öneren bir ağ altyapısı sağlayıcısı sınıfı müşterileri adına çeşitli ağ güvenliği görevleri. VPN servis sağlayıcıları VPN sunucusu / istemcisi sağlar dağıtım yardımı ve VPN’lerin operasyonel yönetimi.

**SSL** (Güvenli Yuva Katmanı) İlk olarak Netscape tarafından geliştirilen bir güvenlik protokolü. SSL oldu istemciler ve sunucular arasında kimliği doğrulanmış ve şifreli iletişim için evrensel olarak Web'de kabul edildi. SSL, genellikle tarayıcılarla ilişkilendirilir, ancak FTP gibi diğer TCP / IP protokollerini korumak için kullanılabilir. SSL, TLS'ye dönüşmüştür.

**TLS** (Aktarım Katmanı Güvenliği protokolü) Internet üzerinden iletişim gizliliği sağlayan bir IETF taslak standart protokolü. Protokol, istemci / sunucu uygulamalarının gizli dinlenmeyi, kurcalamayı ve mesaj sahteciliğini önleyecek şekilde iletişim kurmasını sağlar.

**VPN client** Bir bireysel kullanıcı bilgisayarında bulunan ve bir VPN sunucusuna VPN tüneli kuran yazılım.

**VPN server** Merkezi bir konumda bulunan ve VPN tünelini sonlandıran bir cihaz (IPSec güvenlik ağ geçidi). VPN istemcileri ve diğer VPN sunucuları ile iletişim kurar. Donanım veya yazılım tabanlı olabilir.

**VPN** (Sanal Özel Ağ) Gizlilik sağlayan verileri iletme imkanı sağlayan bir ağı, kimlik doğrulama ve veri bütünlüğü.

**41**

**BİR DENETİM NOKTASI**

**GÜVENLİK DUVARI GÜVENLİK**

**İNCELEMESİ NASIL YAPILIR**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Ben Rothke ,CISSP*

Değiştirilmiş Devletler, yalnızca deney yapan bir araştırma bilimcisi hakkındaki bilim kurgu filmi değildi.insan bilincinin değişmiş halleri; Aynı zamanda kurumsal işletmelerdeki birçok güvenlik duvarı için bir metafordur.

Genel olarak, bir güvenlik duvarı başlangıçta yüklendiğinde, bir kuruluşun güvenliği ile sıkı sıkıya bağlanır. Gereksinimler. Bir şirket ortamında kullandıktan sonra, güvenlik duvarı kural tabanı, yapılandırma ve temel işletim sistemi genellikle radikal olarak farklı bir düzenlemeye dönüşür. Bu değiştirilmiş güvenlik duvarı durumu, güvenlik duvarı incelemesini gerektiren şeydir.

Bir güvenlik duvarı yalnızca uygun şekilde yapılandırıldığı ölçüde etkilidir. Ve bugünün kurumunda ortamlarda, güvenlik duvarının yanlış yapılandırılmış olması kolaydır. Güvenlik duvarı kurulumunu gözden geçirerek yönetim, güvenlik duvarının ne beklediğini ve güvenli bir şekilde uygulanmasını sağlayabilir.

Bu bölüm, Checkpoint Firewall-1 için bir güvenlik duvarı incelemesi yapmaya odaklanmaktadır. Bu bilgilerin çoğu, Cisco PIX, NAI Gauntlet, Axent Raptor, vb. Dahil olmak üzere herhangi bir güvenlik duvarı için yeterince geneldir. Bir uyarı: güvenlik duvarı incelemesi bir sızma testi değildir. Bir güvenlik duvarı incelemesinin işlevi, istismarları bulmak ve güvenlik duvarına erişim sağlamak değildir; bunun yerine, tanımlamak yanlışlıkla güvenlik duvarı tarafından açılan riskler.

Son olarak, bir güvenlik duvarı incelemesinin aynı zamanda bir sertifikalandırma veya garanti vermediği anlaşılmalıdır. güvenlik duvarı işletim sistemi veya temel ağ işletim sistemi tamamen güvenlidir.

**Güvenlik Duvarı İncelemesi Gerekliliği**

İnsanlar gibi güvenlik duvarlarının da gözden geçirilmesi gerekiyor. İşyerinde buna performans değerlendirmesi denir. İçinde tıbbi arenada buna fiziksel denir. Yanlış yapılandırılmış bir güvenlik duvarı genellikle güvenlik duvarı olmamasından daha kötü olduğu için periyodik güvenlik duvarı incelemeleri için ihtiyaç çok önemlidir. Kuruluşlar güvenlik duvarına sahip olmadıklarında, ilgili riskleri anlarlar ve temel bir güvenlik mekanizmasına sahip olmadıkları gerçeğinin farkındadırlar. Ancak, yanlış yapılandırılmış bir güvenlik duvarı bir kuruluşa yanlış bir güvenlik hissi verir.

Ek olarak, güvenlik duvarı genellikle dağıtılan birincil bilgi güvenliği mekanizması olduğundan, güvenlik duvarındaki herhangi bir hata veya yanlış yapılandırma tüm şirkete yayılır. Bir güvenlik duvarı hiç gözden geçirilmezse, bu hatalardan herhangi biri denetlenmeden bırakılır.

**Gözden Geçirme, Denetim, Değerlendirme**

Güvenlik duvarı incelemeleri genellikle denetimler olarak adlandırılır. Bir denetim “metodik bir inceleme ve gözden geçirmeau” olarak tanımlanır. Ayrıca, “inceleme”, “değerlendirme” ve “denetim” terimleri de sıklıkla eşanlamlıdır. Big Five 2 muhasebe şirketlerinden güvenlik grupları güvenlik incelemesi yaptığında, özellikle “Denetim” terimini kullanmak yasaktır. Bu, Büyük Beşi denetleyen Amerikan Onaylı Kamu Hesapları Enstitüsü'nün (www.aicpa.org) “Beşli Terim” terimini yasaklamasından kaynaklanmaktadır. belirlenmiş çevrenin denetleneceği resmi bilgi güvenliği standartları.

Diğer taraftan, Genel Kabul Görmüş Kullanıcı İlkelerine aykırı mali denetimler yapılır. (GAAP) Generally Accepted Accounting Principles. Sabit bir kurallar dizisi olmasa da, GAAP yaygın olarak kabul edilen bir kurallar, standartlar ve finansal bilgilerin raporlanması için prosedürler. Finansal Muhasebe Standartları Kurulu (www.fasb.org), 1973 yılında GAAP'ı kurmuştur. Finansal Hesaplama Standartları Kurulu'nun misyonu, ihraççı, denetçiler, kamuoyunun rehberliği ve eğitimi için mali muhasebe ve raporlama standartlarını oluşturmak ve iyileştirmektir. ve finansal bilgi kullanıcıları.

Ocak 2001 itibariyle, Genel Kabul Görmüş Sistem Güvenlik İlkeleri (GASSP) Komitesi, Uluslararası Bilgi Güvenliği Vakfı'nı (IISF) kurma ve finanse etme planlarını yansıtan bir iş planı hazırlamanın ilk aşamalarındaydı. Halen, hiçbir güvenlik önlemi kabul edilmiş güvenlik ilkesi bulunmamakla birlikte (güvenlik duvarının gerçekten olabileceği karşı denetlenmiş), böyle bir standart oluşturmak için çalışmalar sürüyor. GASSP için çalışma grupları var. Halihazırda Yetkili Vakfı araştırmak ve tamamlamak, GASSP çerçevesini geliştirmek ve onaylamak için çalışmalar yapılmaktadır. Komite, GASSP Ayrıntılı Prensiplerini tamamlamak için ayrıntılı bir plan geliştirmiştir ve IISF fonunu güvence altına almak için bu planı uygulamak için planlar yapmıştır.

Bir GASSP’in olmayışı, korumanın korunmasına yönelik hiçbir yetkili referans olmadığı anlamına gelir.altyapısı. Bir GAASP olsaydı, GASSP'den makul bir şekilde belirlenmiş istisnaların veya ayrılmaların yetkili onayı için bir araç seviyesini zorlamanın ve bir aracı sağlamanın bir yolu olurdu.

Teoride GASSP'ye benzer şekilde Ortak Kriterler Projesi'dir (http: // csrc. Nist.gov/cc). Ortak Kriterler, bilgi teknolojisi (BT) ürünlerinin ve sistemlerinin güvenlik özelliklerini değerlendirmenin bir yolu olarak geliştirilen uluslararası bir çabadır. Böyle bir ortak ölçüt tabanı oluşturarak, BT güvenlik değerlendirmesinin sonuçları daha geniş bir kitleye anlam kazandıracak.

Ortak Kriterler, bağımsız güvenlik değerlendirmelerinin sonuçları arasında karşılaştırıla bilirliğe izin verecektir. BT ürünlerinin ve sistemlerinin güvenlik işlevleri ve güvenlik değerlendirmesi sırasında bunlara uygulanan güvence önlemleri için ortak bir dizi gereksinim sağlayarak bunu kolaylaştırır. Değerlendirme süreci, bu tür ürünlerin güvenlik işlevlerinin ve sistemler ve bunlara uygulanan güvence önlemleri bu gereksinimleri karşılar. Değerlendirme sonuçları bilişim teknolojisi ürününün veya sisteminin amaçlanan uygulaması için yeterince güvenli olup olmadığını ve kullanımında gizli güvenlik risklerinin tolere edilip edilemeyeceğini belirlemeye yardımcı olur.

**Güvenlik Duvarı İnceleme Adımları**

Güvenlik duvarı mimarisinin, güvenlik planlarının ve işlemlerin kapsamlı bir incelemesi şunları içermelidir:

* Çalışanlara ve iş ortaklarına altyapı erişimini yöneten prosedürler altyapı
* Altyapının fiziksel ve mantıksal mimarisi
* Altyapının ve altta yatan ağ işletim sistemlerinin donanım ve yazılım sürümleri
* Erişim kontrol bilgileri üzerinde altyapı kontrolleri
* Günlük olay seçimi ve bildirim kriterlerinin gözden geçirilmesi
* Bakım ve yönetim için sağlananlar dahil tüm erişim yolları
* Güvenlik politikaları ve idari prosedürler (yani, kullanıcıların ve hizmetlerin eklenmesi veya silinmesi, cihaz ve sistem denetim kayıtlarının gözden geçirilmesi, sistemin yedeklenmesi ve ortamın saklanması vb.)
* Kullanıcı hesapları, dosya sistemi izinleri dahil, ağ işletim sistemi üzerinden erişim kontrolleri,
* çalıştırılabilir dosyaların, ayrıcalıklı programların ve ağ yazılımının özniteliklerini
* Bir izinsiz giriş durumunda, hizmet dışı bırakma durumunda altyapı için Acil Müdahale Planları

saldırı vb.

* Yayınlanan güvenlik uyarısı bültenlerine erişim ve kullanım

Güvenlik duvarı incelemesi yapmanın birçok yöntemi vardır. Aşağıdaki altı adımda çoğu merkez:

1. Altyapı ve mimariyi analiz eder.
2. Kurumsal güvenlik duvarı politikasını inceleyin.
3. Ana bilgisayarları ve ağ değerlendirme taramalarını çalıştırın.
4. Güvenlik Duvarı-1 yapılandırmasını inceleyin.
5. Güvenlik Duvarı-1 Kural Tabanını inceleyin.
6. Hepsini bir rapora koyun.

Aşağıdaki tartışma her adımda genişlemektedir.

**Adım 1: Altyapı ve Mimariyi Analiz Edin**

Güvenlik duvarının ağı yeterince koruduğundan emin olmak için ağ altyapısını anlamak gerekir. İncelenecek öğeler şunlardır:

* İnternet erişim gereksinimleri
* İnternet / extranet erişimi için iş gerekçelerini anlama
* İzin verilen gelen ve giden hizmetlerin doğrulanması
* Güvenlik duvarı tasarımını gözden geçirme (yani, çift yönlü, çok yönlü, proxy)
* İç / dış ağlara bağlantıyı analiz etme:
* Çevre ağı ve dış bağlantılar
* Elektronik ticaret ağ geçitleri
* Şirketler arası veya şirket içi LAN-WAN bağlantısı
* Genel kurumsal güvenlik mimarisi
* Belirli bir sitedeki veya konumdaki tüm bilgisayar kurulumu
* Ağ ve güvenlik duvarı yöneticileriyle görüşme

Bilgi güvenliği mimarisinde şirket politikasının ne olduğunu yansıtmayan bir hata varsa, güvenlik duvarı bu eksikliğin yerini alamaz.

Güvenlik duvarı açısından, ölçeklenebilir ve dağıtılabilir bir güvenlik duvarı sistemi elde etmek için Checkpoint, Firewall-1 ürününün işlevselliğini iki bileşene ayırmıştır: bir Güvenlik Duvarı Modülü ve bir Yönetim Modülü. Bu bileşenlerin etkileşimi, standart Checkpoint Firewall mimarisinin tamamını oluşturur.

Yönetim modülü, diğer güvenlik duvarı modülleri için merkezi bir kontrol cihazıdır ve Güvenlik duvarı işlevselliğini tanımlayan nesneler ve kurallar mevcuttur. Kurallar ve nesneler, güvenlik duvarı modüllerinden birine veya tümüne uygulanabilir. Diğer güvenlik duvarı modülleri tarafından oluşturulan tüm günlükler ve uyarılar buna gönderilir. depolama, sorgulama ve inceleme için yönetim sistemi.

Güvenlik duvarı modülünün kendisi, ayrı bölgeler arasındaki tüm trafiğin geçmesi gereken gerçek ağ geçidi sistemidir. Güvenlik duvarı modülü, paketleri inceleyen, kuralları uygulayan ve günlükleri ve uyarıları üreten sistemdir. Kural tabanı ve günlük depolaması için bir veya daha fazla yönetim modülüne güvenir, ancak yönetim modülü çalışmıyorsa mevcut kural tabanı ile bağımsız olarak çalışmaya devam edebilir.

Güvenlik duvarı mimarileri tasarımında kullanmak için mükemmel bir referans İnternet Güvenlik Duvarı Oluşturma Elizabeth Zwicky (O'Reilly ve Doç. ISBN: 1565928717).

**Adım 2: Kurumsal Bilgi Sistemi Güvenlik Politikalarını Gözden Geçirin**

Politika, bir güvenlik duvarının etkin ve başarılı bir şekilde çalışmasının kritik bir unsurudur. Güvenlik duvarı, kullanımı ve yönetimi yöneten çalışma politikaları bağlamında konuşlandırmadıkça etkili olamaz.

Marcus Ranum bir güvenlik duvarını “İnternet güvenlik politikanızın uygulaması” olarak tanımlar. Bir güvenlik politikanız yoksa, bir güvenlik duvarınız yoktur. Bunun yerine, bir şeyler yapan bir şeye sahipsiniz, ancak ne yapmaya çalıştığını bilmiyorsunuz çünkü kimse size ne yapması gerektiğini söylemedi. ”Bir kuruluşun anlamlı bir güvenlik duvarı incelemesi yapmasını beklediği takdirde. Bir dizi güvenlik duvarı politikası yoksa, organizasyon kaba bir uyanış için içeride.

Güvenlik duvarı incelemesi sırasında sorulacak bazı politika temelli sorular şunlardır:

* Kuruluş için yayınlanmış bir güvenlik duvarı politikası var mı?
* Üst yönetim, güvenlik duvarı altyapısıyla ilgili politikaları gözden geçirdi ve onayladı mı?
* Kuruluşun bilgi güvenliğini kontrol etmekten kim sorumludur?
* Güvenlik duvarı politikalarını değiştirme prosedürleri var mı? Eğer öyleyse, süreç nedir?
* Bu politikalar kurum içinde nasıl iletilir?

Güvenlik duvarının yönetimi ile ilgili olarak ele alınması gereken sorunlardan bazıları şunlardır:

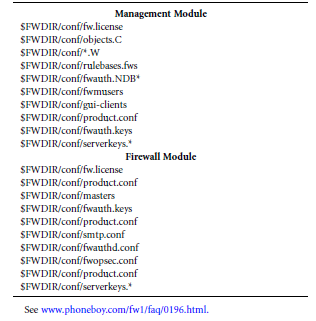
* Güvenlik duvarlarına kim sahip ve bu tanımlanmış mı?
* Her güvenlik duvarı için belirtilen politikaların uygulanmasından kim sorumludur?
* Güvenlik duvarının günlük yönetiminden kim sorumludur?
* Güvenlik duvarını belirtilen politikalara uygunluk açısından kim izler?
* Güvenlikle ilgili olaylar uygun bilgi güvenliği personeline nasıl bildirilir?
* Yeni güvenlik açıklarının varlığı için CERT, CIAC, satıcıya özel ve benzer öneriler izleniyor mu?
* Muhafaza etme ve raporlama prosedürleri dahil olmak üzere farklı olaylara nasıl tepki vereceğinizi belirten yazılı prosedürler var mı?

Değişim kontrolü bir güvenlik duvarı için kritik derecede önemlidir. Bazı değişiklik kontrolleri sorunları:

* Değişiklik kontrol prosedürü belgelerinin mevcut olduğundan emin olun.
* Test planlarının gözden geçirildiğinden emin olun.
* Düzeltmeleri güncelleme prosedürlerini gözden geçirin.
* Yönetim onay sürecini gözden geçirin.
* İşlem, aşağıdaki bileşenlerde yapılan değişikliklerin belgelenmesini sağlamalıdır:
  + Herhangi bir yükseltme veya düzeltme eki, arıza süresinin bildirilmesini ve zamanlanmasını gerektirir
  + Tüm değişikliklerin elektronik kopyaları
  + Basılı kopya formu tüm değişiklikler için dolduruldu

Son olarak, felaketler meydana geldiğinde yedekleme ve beklenmedik durum planlaması çok önemlidir. Bazı konular:

* *Güvenlik Duvarı-1'in altın kopyasını alın*. Altın kopya, ana bilgisayar ağa bağlanmadan önce tam yedeklenir. Bu kopya kurtarma için ve güvenlik duvarının bir şekilde tehlikeye girmesi durumunda referans olarak kullanılabilir.
* *Yedekleme prosedürlerini ve belgelerini* gözden geçirin. Yedekleme prosedürlerinin bir bölümü de içermelidir restorasyon prosedürleri. Yedekleme, yalnızca yapılan yedeklemelerden biri kurtarılabiliyorsa tamamlanmış sayılmalıdır. Ayrıca, yedeklerin güvenli bir yerde saklanması gerekir. Güvenlik duvarının yeniden yapılması veya değiştirilmesi gerektiğinde, geri yüklenmesi gereken birkaç dosya vardır (bkz. Ek 41.1). Bu dosyalar, bir teyp sürücüsü veya başka bir büyük depolama cihazı gibi harici bir cihaz kullanılarak tam bir sistem yedeklemesi yoluyla yedeklenebilir. Güvenlik duvarı işlevselliği için en kritik dosyalar diskete sığabilmelidir.

**Ek 41.1** Kritik Güvenlik Duvarı-1 Yapılandırma Dosyaları Yedeklenecek

* Yedekleme zamanlamasını inceleyin
* Güvenlik duvarı sistemini kurtarmak için prosedürlerin uygulanıp uygulanmadığını, hizmette bir kesinti olması durumunda belirleyin.
* Acil durum planını gözden geçirin.
* Acil durum planı dokümantasyonu

Bilgi Güvenliği Politikaları ve Prosedürleri (Thomas Peltier, Auerbach Publications) politika dağıtımına başlamak için iyi bir yerdir. Kapsamlı bir politika setinin olmayışı için her derde deva olmamasına rağmen, Bilgi Güvenliği Politikaları ve Prosedürleri bir kuruluşun, politikalarına boğulmadan politikaları hızla dağıtmasını sağlar.

Tüm bu analiz ve incelemelerin işletme kuruluşun amaçları bağlamında yapılması gerektiği belirtilmelidir. Bilgi sistemleri güvenliği risk yönetimi ile ilgili olmakla birlikte, kurumsal strateji çerçevesinde uygulanmazsa, güvenlik başarısızlıkla sonuçlanır.

**Adım 3: Ana Bilgisayar Yazılım Değerlendirme Taramasını Gerçekleştirin**

Güvenlik duvarı yanlış yapılandırması, güvenlik duvarının varlığına rağmen yetkisiz kişilerin (yabancıların) ağa girmesine izin verebilir. Tek tek güvenlik duvarı ana bilgisayarlarına karşı yazılım taramaları gerçekleştirerek, belirli güvenlik açıklarını tespit edilebilir. Bu tarama araçları güvenlik açıklarını tanımlayabilir, sistem zayıflıklarını detaylandırabilir, politikaları doğrulayabilir ve kurumsal güvenlik stratejilerini uygulayabilir. Bu tür araçlar sistem açıklarını kontrol etmek için çok önemlidir.

Tarayıcıların tanımlayabileceği sayısız kontrolün bazıları şunlardır:

* İşletim sistemi yanlış yapılandırması
* Uygunsuz güvenlik ve şifre ayarları
* Arabellek taşması
* SANS İlk 10 İnternet Güvenliği Tehditinin Tespiti
* FreeBSD'yi etkileyen segmentasyon hatası
* Parolasız NT konuk ve yönetici hesaplarının tespiti

Bazı popüler tarama araçları şunları içerir:

* NAI Cybercop, <http://www.pgp.com/products/cybercop-scanner>
* ISS İnternet Tarayıcı, http://www.iss.net/internet\_scanner/index.php
* SAINT, http://www.wwdsi.com/saint
* Symantec (formerly Axent) NetRecon, <http://enterprisesecurity.symantec.com/products>
* Netcat, <http://www.l0pht.com/~weld/netcat/>
* nmap, <http://www.insecure.org/nmap/index.html>

Bir güvenlik duvarı üzerinde bir ana bilgisayar yazılım değerlendirme taraması çalıştırmanın bir güvenlik duvarı incelemesinin yalnızca bir yönü olduğu belirtilmelidir. Cybercop gibi araçların kullanımı oldukça kolaydır; Bu nedenle, araçları çalıştırmak için profesyonel bir hizmet firması getirmeye gerek yoktur. Güvenlik uzmanı servis firmaları tarafından katma değer, kapsamlı mimari tasarım, analiz ve hata iyileştirme alanlarındadır. Bu araçları çalıştıracak ve müşteriye sadece ürünü teslim edecek herhangi bir firma müşteriye ciddi bir adaletsizlik yapıyor.

Bu, yalnızca bir güvenlik altyapısının başlangıçtan itibaren tasarlanması gerektiği noktasını yinelemeye hizmet eder. Bu mimari güvenlik, kapasite, yedeklilik ve yönetim gibi unsurları dikkate almalıdır. İyi bir mimari olmadan, sistemin yeniden tasarımı sürekli bir çaba olacaktır.

**Adım 4: Güvenlik Duvarı-1 Yapılandırmasını Gözden Geçirin**

Firewall-1 önemli bir güvenlik sağlarken, Firewall-1 yanlış yapılandırılmışsa bu güvenlik tehlikeye girebilir. İncelenecek daha önemli öğelerden bazıları aşağıda listelenmiştir (belirli bir sırada değil).

**IP Yönlendirme.**

IP Yönlendirmeyi Kontrol Et'e ayarlayın. İşletim sistemi çekirdeğinde IP Yönlendirme devre dışı bırakılmalıdır. Bu, Firewall-1 çalışmadığı sürece IP Yönlendirmenin hiçbir zaman etkinleştirilmemesini sağlar.

**Güvenlik Duvarı Yöneticileri.**

Güvenlik Duvarı-1 yöneticilerinin sayısının yalnızca gerçekten ihtiyacı olanlarla sınırlı olduğundan emin olun. Güvenlik duvarındaki her hesabın amacı (hem işletim sistemi hem de güvenlik duvarı işletim sistemi için) doğrulanmalıdır. Sergi 41.2, güvenlik duvarı yöneticilerinin ve izinlerinin bir listesini sağlar.

**Eğitilmiş çalışanlar.**

Güvenlik duvarı altyapısını yöneten personelin deneyimli olmadığı sürece bir güvenlik duvarı etkili olamaz. Güvenlik duvarı-1 işlemlerinde güvenlik ve eğitimli. Bir kişi güvenlik duvarından yalnızca ağ kurma konusunda tecrübe sahibi olduğu için sorumlu tutuluyorsa, güvenlik duvarının, rakiplerin güvenlik duvarını tehlikeye atmasını daha kolay hale getirecek şekilde yanlış yapılandırmalarla doldurulması beklenir.

**SYN Taşkın Koruması.**

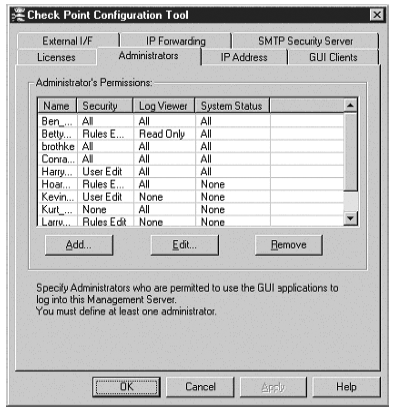
Hizmet reddi (DoS) saldırıları, saldırganın uzak bir ana bilgisayardaki kaynakları düzgün çalışamayacak derecede tüketmesini sağlar. SYN taşkın saldırıları en yaygın DoS saldırısı türlerinden biridir.

SYN taşkın korumasının uygun seviyede etkinleştirildiğinden emin olun: Yok, SYN Ağ Geçidi veya Pasif SYN Ağ Geçidi (bkz. Ek 41.3).

**İşletim Sistemi Versiyon Kontrolü.**

Hem Checkpoint yazılımı hem de ağ işletim sistemi için, güvenlik duvarının Güvenlik Duvarı-1'in güncel ve desteklenen bir sürümünü çalıştırdığından emin olun. En son sürümün özellikle yüklenmesi gerekmese de, geçerli yamaların yüklendiğinden emin olun.

**EXHIBIT 41.2** Güvenlik duvarı yöneticileri ve izinleri



**Fiziksel güvenlik.**

Güvenlik duvarı fiziksel olarak korunmalıdır. Tüm ağ işletim sistemlerinin kendi temellerini oluşturdukları belirtilmelidir. güvenli bir fiziksel altyapı üzerinde güvenlik modelleri. Erişimin olduğu alanlarda güvenlik duvarı bulunmalıdır.sadece yetkili personel ile sınırlıdır; özellikle:

* Yerel konsol güvenli olmalıdır.
* Yönetim konsolu harici ağa açık olmamalıdır.
* Güvenlik duvarı yapılandırması tamamen korunmalı ve kurcalamaya karşı korumalı olmalıdır. (yetkili yönetim istasyonu hariç).
* Yerel yönetim için yönetici için tam kimlik doğrulaması yapılmalıdır.
* Uzaktan yönetim için tam kimlik doğrulama ve şifreli bir bağlantı gereklidir.

**Gereksiz Sistem Bileşenlerini Çıkarın.**

Derleyiciler, hata ayıklayıcılar, güvenlik araçları vb. Gibi yazılımlar güvenlik duvarından kaldırılmalıdır.

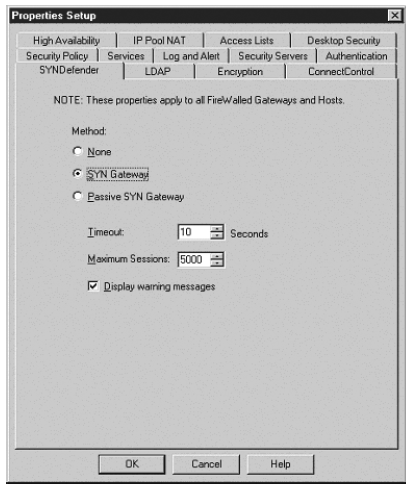
**Yeterli Yedek Güç Kaynakları.**

Güvenlik duvarında bir UPS yoksa, elektrik kesintisi durumunda güvenlik tamamen uygulanmayacaktır.

**Günlük İncelemesi.**

Hem güvenlik duvarı hem de ağ işletim sisteminin günlükleri gözden geçirilmeli ve analiz edilmelidir. Tüm olaylar, hata ayıklama ve adli analiz için kullanılabilecek günlüklere göre izlenebilir.

**EXHIBIT 41.3** SYN taşkın korumasını ayarlama.



İdeal olarak, günlükler uzaktaki bir günlük ana bilgisayarına veya ayrı bir disk bölümüne yazılmalıdır. Bir saldırı durumunda, Günlükler, olayın birkaç yönünü izlemek için kritik belgeler sağlayabilir. Bu bilgiler, sömürülen delikleri açmak, saldırının boyutunu keşfetmek, bir saldırının belgelenmiş kanıtını sağlamak ve hatta saldırının kaynağını izlemek için kullanılabilir. Bir saldırganın yapacağı ilk şey, günlük dosyalarını değiştirerek veya yok ederek izlerini örtmektir. Bu günlük dosyalarının imha edilmesi durumunda, olayı takip etmek için yedeklemeler gerekecektir. Bu nedenle, sık yedeklemeler zorunludur.

**Zaman Senkronizasyonu.**

Zaman senkronizasyonu iki amaca hizmet eder: zamana duyarlı olayların doğru şekilde yürütülmesini sağlamak. Zaman ve bu farklı günlük dosyaları ilişkilendirilebilir. Yanlış bir zamana atıfta bulunan günlükler, mahkemede kanıt olarak potansiyel olarak dışlanabilir ve bu, bir saldırganın kovuşturma çabalarını engelleyebilir.

Ağ Zaman Protokolü (NTP) RFC 1305, ana bilgisayarları senkronize etmek için yaygın olarak kullanılır. Ortamlar için daha yüksek dereceli ve denetlenebilir bir zaman senkronizasyonu yöntemi gerektiriyorsa, Sertifikalı Zaman'dan (www.certifiedtime.com) gelen zaman senkronizasyon teklifleri araştırılmalıdır.

**Bütünlük kontrolü**.

Bütünlük denetimi, dosya sistemindeki bir şey olduğunda sistem yöneticisine bildirimde bulunma yöntemidir. kritik bir dosyaya değiştirildi. En çok bilinen ve konuşlandırılmış bütünlük kontrolü uygulaması Tripwire (Www.tripwire.com).

**Hizmet Miktarını ve Protokolleri sınırlayın.**

Bir güvenlik duvarında, güvenlik duvarı tarafından kesinlikle gerekmeyen bir şey yüklü veya çalışıyor olmalıdır. Gereksiz protokoller gereksiz iletişim bağlantılarını açar. Hangi servislerin açık olduğunu görmek için port taraması kullanılabilir. Çok fazla hizmet güvenlik duvarının etkinliğini engelleyebilir, ancak her hizmete yetki verilmelidir; değilse, devre dışı bırakılmalıdır.

Tehlikeli bileşenler ve hizmetler şunları içerir:

* X veya GUI ile ilgili paketler
* NIS / NFS / RPC ile ilgili yazılım
* Derleyiciler, Perl, TCL
* Web sunucusu, yönetim yazılımı
* Masaüstü uygulamaları yazılımı (ör. Microsoft Office, Lotus Notes, tarayıcılar, vb.)

Bir NT güvenlik duvarında, yalnızca aşağıdaki hizmetler ve protokoller etkinleştirilmelidir:

• TCP/IP

• Firewall-1

• Protected Storage

• UPS

• RPC

• Scheduler

• Event log

• Plug-and-Play

• NTLM Security Support provider

Başka bir işlevselliğe ihtiyaç duyuyorsanız, bunları yalnızca gerektiği kadar ekleyin.

**İşletim Sistemini Sertleştirin.**

Temel ağ işletim sistemindeki herhangi bir zayıflık veya yanlış yapılandırma, Firewall-1'i azaltacaktır. Güvenlik duvarının, güvenlik kalesi olması için bir ana sunucu olarak korunması gerekir. Güvenlik duvarı hiçbir zaman genel amaçlı bir bilgi işlem aygıtı olarak değerlendirilmemelidir.

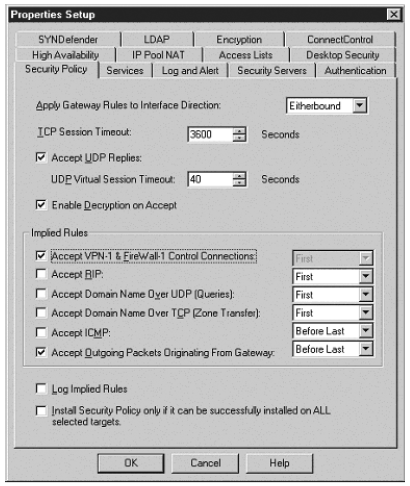
Bir işletim sisteminin nasıl sertleştirileceğine ilişkin mükemmel belgeler:

* Armoring Solaris, www.enteract.com/~lspitz/armoring.html
* Armoring Linux , www.enteract.com/~lspitz/linux.html
* Armoring NT , www.enteract.com/~lspitz/nt.html

Önceden sertleştirilmiş bir cihaza ihtiyaç duyanlar Nokia güvenlik duvarı cihazını dikkate almalıdır (www.nokia.com/securitysolutions / ağ / firewall.html). Nokia güvenlik duvarı, Firewall ile birlikte gelen bir donanım çözümüdür. Güvenlik duvarı işlevselliği için sertleştirilmiş ve optimize edilmiş IPSO işletim sisteminde çalışır.

**Firewall-1 Özellikleri.**

EXHIBIT 41.4 Güvenlik Politikaları sekmesini gösterir. Biri gerekli olmayan Kabul kutularının işaretini kaldırmalıdır:



**SERGİ 41.4** Güvenlik Politikası sekmesi.

* ICMP. Genel olarak, bir kişi bu özelliği devre dışı bırakabilir, ancak Checkpoint’in 4.0’da ICMP için Durumlu Denetimi’nden yararlanmak için etkin bırakması gerekebilir.
* Bölge aktarımı. Çoğu site, kullanıcıların DNS yüklemeleri gerçekleştirmesine izin vermez. Aynısı RIP ve DNS arama seçenekleri için de geçerlidir.

**Firewall-1 Ağ Nesneleri.**

Güvenlik Duvarı-1 incelemesinin merkezi bir yönü, tanımlanmış ağ nesnelerinin hepsinin analizini içerir. Güvenlik duvarı-1 ağ nesneleri, güvenlik politikasının bir parçası olarak gruplandırılmış mantıksal varlıklardır. Örneğin, bir grup Web sunucusu, kuralın uygulandığı basit bir ağ nesnesi olabilir. Her ağ nesnesinin, ağ adresi, alt ağ maskesi vb. Gibi bir dizi özniteliği vardır.

Bir ağ nesnesinin parçası olabilecek varlık örnekleri şunlardır:

* Ağlar ve alt ağlar
* Sunucular
* Yönlendiriciler
* Anahtarlar
* Ana bilgisayarlar ve ağ geçidi
* İnternet alanları
* Yukarıdakilerin grupları

Güvenlik duvarı-1, kaynak ve hedef alanlarda ağ nesnelerinin oluşturulmasına izin verir. Bu ağ nesneleri, tek bir cihazdan tüm ağlara kadar her yerde bulunabilir ve binlerce cihaz referans verebilir. İkincisi, bir Firewall-1 güvenlik duvarının güvenlik yapılandırmasını ve güvenlik seviyesini değerlendirmeye çalışırken önemli bir engel oluşturur. Kritik sorun nasıl belirlenir çok sayıda nesne içerdiğinde ağ nesnesinin güvenliğinin altında.

Güvenlik Duvarı-1'deki aygıtları yönetmeye yönelik bu nesne yönelimli yaklaşım, güvenlik duvarı yöneticisinin yönlendiricileri veya başka bir aygıtı ağ nesnesi olarak tanımlamasını ve ardından bu nesneleri güvenlik duvarı güvenlik ilkesi kuralları dahilinde kullanmasını sağlar. Ağ nesnelerinin temel kullanımları büyük bir referansta verimlilik içindir ağ aygıtı miktarı. Bu, ana bilgisayar adı, IP adresi gibi şeyleri hatırlama gereğini ortadan kaldırır konum, vb. Bu, ana bilgisayar adı, IP adresi, konum vb. Gibi şeyleri hatırlama gereksinimini ortadan kaldırır. Ağ nesneleri, bu tür nesneleri kullanarak önemli bir kullanım kolaylığı ve zaman tasarrufu sağlarken, bir kuruluşun, tümünün kendi kendine güvenip güvenmediğini belirlemesi gerekir. nesnede bulunan cihazların listesi. Sergi 41.5, mevcut nesnelerden bazılarını gösteren Ağ Nesneleri kutusunu gösterir. Exhibit 41.6, grupta çok sayıda iş istasyonu bulunan bir Ağ Nesnesinin bir örneğini gösterir.

Belirtildiği gibi, ağ nesnelerinin bu şekilde kullanılması idari açıdan zaman kazandırır; ancak güvenlik açısından, ağ nesnesiyle ilişkili olan yerleşik güvenlerin, bu ağ nesnesindeki her varlık için otomatik olarak oluşturulmasıyla ilgili bir sorun vardır. Bu büyük olması nedeniyle ağlarda, ağ nesnesinde tanımlanan her bir bireyi incelemek zaman alıcıdır. Böyle bir konfigürasyonun getirdiği zorluk, güvenlik duvarı kuralının sunduğu korumayı hassasiyet ve doğrulukla incelemek için ağ nesnesindeki her cihazı kontrol etmenin gerekli olduğu anlamına gelir.

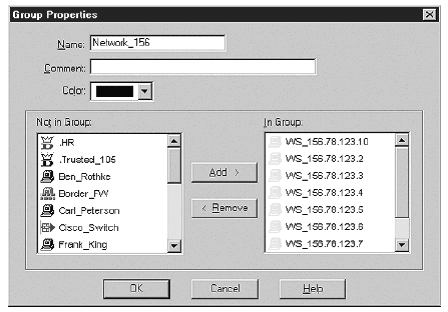
**Adım 5: Güvenlik Duvarı-1 Kural Tabanını Gözden Geçirin**

Bir kural tabanı incelemesinin amacı, güvenlik duvarının izin verdiği hizmetleri ve verilerini görmektir. Kural tabanının analizi ayrıca gereksiz, tekrarlayan veya yetkisiz kuralları tanımlamak içindir. Kural tabanı mümkün olduğunca basit yapılmalıdır. Kural sayısını azaltmanın bir yolu kuralları birleştirmektir, çünkü bazen tekrarlayan kurallar birleştirilebilir.

Bir kural tabanı incelemesinin amacı, güvenlik duvarının izin verdiği hizmetleri ve verilerini görmektir. Kural tabanının analizi ayrıca gereksiz, tekrarlayan veya yetkisiz kuralları tanımlamak içindir. Kural tabanı mümkün olduğunca basit yapılmalıdır. Kural sayısını azaltmanın bir yolu kuralları birleştirmektir, çünkü bazen tekrarlayan kurallar birleştirilebilir.



**EXHIBIT 41.5** Mevcut nesneler.



**EXHIBIT 41.6** Grupta çok sayıda iş istasyonu bulunan bir ağ nesnesi.

Bir kural tabanı incelemesinin işlevi, güvenlik duvarının beklenenleri zorladığından emin olmaktır. Lance Spitzner, Güvenlik Duvarı Kuralı Tabanı Oluşturma'da “sağlam bir kural tabanı oluşturmak kritik, önemli değilse de başarılı ve güvenli bir güvenlik duvarı uygulama adımı” olduğunu yazıyor. Güvenlik yöneticileri ve Uzmanların çoğu genellikle hangi platformların ve uygulamaların en iyi güvenlik duvarlarını yaptığını tartışıyor. Ancak, bunların hepsi güvenlik duvarı kural tabanı yanlış yapılandırılmışsa anlamsızdır. ”

Kural tabanı, bir Checkpoint güvenlik duvarının kalbi ve ruhudur. Bir kural tabanı, güvenlik duvarında depolanan ve her bir güvenlik duvarı için ayrı bir güvenlik politikası tanımlayan sıralı bir kurallar kümesi içeren bir dosyadır. Kural temel dosyasına erişim, fiziksel olarak güvenlik duvarında bulunanlarla veya yapılandırma ayarlarında belirtilen GUI istemci listesinin bir üyesi olanlarla sınırlıdır.

Bir kural, iletişimi kaynağı, hedefi ve servisi açısından açıklar. Kural ayrıca iletişimin kabul edilip edilmemesi veya reddedilmesi gerekip gerekmediği ve bir günlük girişi oluşturulmuş olup olmadığı.

Firewall-1 inceleme motoru, “en uygun” bir cihaza karşılık, “ilk kullanıma uygundur”. Bu, birinin 20 kural içeren bir kural tabanına sahip olması ve gelen paketin kural # 4 ile eşleşmesi durumunda, denetim motorunun derhal durması (kurallar, her paket için sırayla incelenmesi nedeniyle) ve kural tabanının geri kalanından geçmediği anlamına gelir.

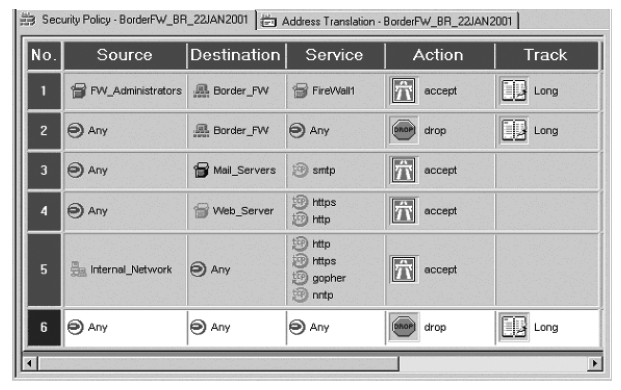
Kural tabanı incelemesine gelince, güvenlik uzmanı Lance Spitzer, hedefin 30'dan fazla kuralın bulunmamasını önermektedir. 30 kuraldan daha fazlası olduğunda, katlanarak işler karmaşıklaşır ve hatalar olur.

Her kural tabanının ayrı bir adı vardır. Ortak bir adlandırma kuralına standart hale getirmek yararlıdır. Önerilen bir biçim: firewallname\_administrators-initials\_date-of-change; for example, fw1\_am\_071298.

Bu adlandırma kuralının sonucu, güvenlik duvarı yöneticisinin kural tabanının tam olarak hangi güvenlik duvarına ait olduğunu bilmesidir; kural tabanı en son değiştirildiğinde; ve mevcut yapılandırmayı en son kim değiştirdi? Kural tabanı incelemesi için, her kural incelenmelidir.

Altı kuralı olan basit bir kural tabanına bir örnek Exhibit 41.7'de gösterildiği gibidir:

* **Kural 1 ve 2**, gizli kurallar kavramını yürürlüğe koyar; bu nedenle, GUI onaylı yöneticiler dışında hiçbir şey doğrudan güvenlik duvarına bağlanamaz. Kural 1, Firewall-1'e FW\_Administrators grubunun bir üyesinden olmadıkça herhangi bir paketi bırakmasını söyler. Firewall-1 hizmeti önceden tanımlanmıştır ve tüm Firewall-1 yönetim portlarını tanımlar. Gizli kural için, reddedilmek yerine, özellikle biri paketi bırakmak istiyor. Reddedilen bir paket, gönderene uzak tarafta bir şey olduğunu söylerken, bırakılan bir paket mutlaka bir uzaktaki bilgisayarı belirtmez. Ayrıca bu kural günlüğe kaydedilir; Böylece, kimin güvenlik duvarına doğrudan bağlantı kurmaya çalıştığı hakkında ayrıntılı bilgi toplanabilir.



**EXHIBIT 41.7** Basit bir kural tabanı.

* Kural 3, iç posta sunucularına herhangi bir ana e-posta bağlantısına izin verir.
* Kural 4, dahili Web sunucularına herhangi bir ana bilgisayar HTTP ve HTTPS bağlantısına izin verir.
* Kural 5, belirtilen dört protokol için İnternete dahili ana bilgisayar bağlantısına izin verir.
* Kural 6, temizleme kuralıdır. Bu noktada güvenlik duvarı tarafından işlenmeyen herhangi bir paket bırakılacak ve kaydedilecektir. Gerçek şu ki, bu noktada güvenlik duvarı tarafından işlenmeyen herhangi bir paketin bırakılması neyse. Bu temizleme kuralının avantajı, bu paketlerin günlüğe kaydedilmesidir. Bu şekilde, hangi paketlerin güvenlik duvarı tarafından kullanılmadığı görülebilir. Bu, daha ölçeklenebilir bir güvenlik duvarı mimarisi tasarlamada yardımcı olabilir.

Yukarıdaki kural temeli örneğinde sadece altı kural vardı ve oldukça basitti. Çoğu kurumsal kural tabanı daha ayrıntılı ve karmaşıktır. 50 kural ve binlerce ağ nesnesi içeren bir kural tabanından geçmek biraz zaman alabilir.

**Exhibit 41.8** biraz daha ilgili olan bir kural tabanı görüntüler:

* Kural 1, gizli kuralı uygular.
* Kural 2–4, posta sunucuları ve istemciler arasında posta trafiğine izin verir.
* Kural 5, iç Web sunucularına herhangi bir ana bilgisayar HTTP bağlantısına izin verir.
* Kural 6, DMZ ile bir intranet arasındaki trafiği durdurur.
* Kural 7-8, DMZ ile intranet arasında gelen ve giden trafiği durdurur.
* Kural 9 çok fazla trafiğe neden olan protokolleri bırakın - bu durumda, nbdatagram, nbname ve nbsession.
* Kural 10, temizleme kuralıdır.

Gözden geçirme yapılırken belirli bir kuralın gerekli olduğuna dair bir şüphe varsa, devre dışı bırakılabilir. Genel bir kural olarak, bir kural devre dışı bırakılırsa ve kimse şikayet etmezse, kural silinebilir. Exhibit 41.9, devre dışı bırakılmış bir kural örneğini gösterir.

**Kapalı Sözlü Kurallar**

Örtülü sahte kurallar normal kural tabanında görünmeyen ancak Güvenlik İlkesinin Özellikler Kurulumu ayarlarına göre Güvenlik Duvarı-1 tarafından otomatik olarak oluşturulan kurallardır. Bu kurallar Güvenlik Politikası GUI uygulamasında kural tabanı ile birlikte görüntülenebilir. Exhibit 41.10, bir kural tabanından gelen tek bir kuralla ima edilen sahte kurallara bir örnek gösterir.

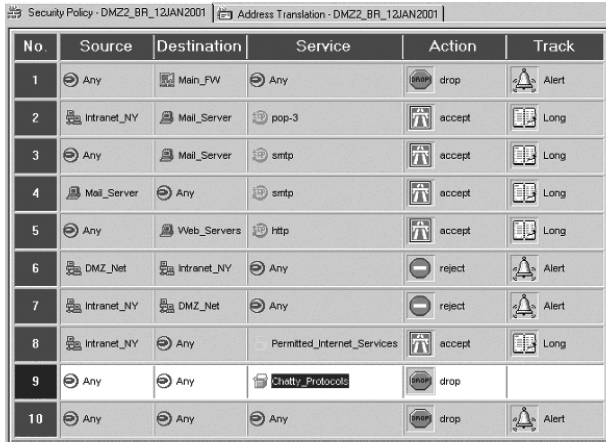
Tek ve tek kural tüm trafiği örtük olarak bıraksa da, güvenlik duvarından geçebilecek çok fazla trafik var. Bu zımni sözde kurallardan görüldüğü gibi, bağlantının çoğu güvenlik duvarının iç işlemleriyle ilgilidir.

**Adım 6: Hepsini Bir Raporda Birleştirin**

Tüm çalışmalar tamamlandıktan sonra, güvenlik duvarı incelemesinin belgelenmesi gerekir. Bir ön inceleme raporundaki değer, bulunan anomalileri düzeltmek için bir kaynak olarak kullanılabileceğidir.

Daha önce de belirtildiği gibi, tarama araçlarının sağladığı kullanım kolaylığı, çok büyük bir raporun oluşturulmasını zahmetsiz hale getirir. Ancak bir güvenlik duvarı incelemesinin bir müşterinin değerine sahip olması için, aşağıdakileri içermesi gerekir:

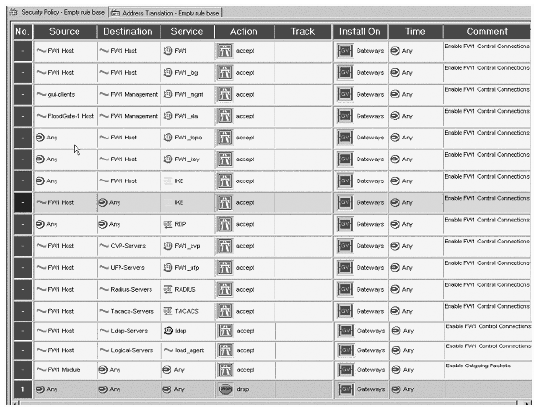
* Mevcut güvenlik durumu: mevcut ağ ortamının temelini ve mevcut güvenlik duruşunu detaylandırın; Bu, kuruluşun genel güvenlik hedefleriyle senkronizasyonu sağlamak için kurumsal risk değerlendirmesine atıfta bulunmalıdır.
* Tüm güvenlik açıklarının tespiti



**EXHIBIT 41.8** Karmaşık kural tabanı.



**EXHIBIT 41.9** Devre dışı bırakılmış kural



**EXHIBIT 41.10** Kapalı Sözde Kurallar

* Düzeltmeler, çözümler ve uygulama öncelikleri önerin; Tüm çözümlerin ve düzeltmelerin nasıl birleşeceğini gösteren ayrıntılı bir uygulama planı sunulmalıdır.
* Maliyet riskleri, kullanım kolaylığı, işletme gereklilikleri ve kabul edilebilir risk seviyeleri ile ilgili güvenlik takaslarının detaylı analizi
* Sistemlerin güvenli bir şekilde hayata geçirildiğinden emin olmak için gelecekteki referans ve karşılaştırma için temel veriler sağlayın

**Sonuç**

Bir güvenlik duvarı, doğru şekilde uygulanma derecesinde etkilidir. Ve bugünün kurumsal ortamlarında, Bir güvenlik duvarının yanlış yapılandırılmış olması kolaydır. Güvenlik duvarı kurulumunu inceleyerek, güvenlik duvarı yöneticileri Güvenlik duvarlarının beklediklerini güvenli bir şekilde uygulayabilmelerini sağlayabilir. Bu iyi yapar duyu ve iyi güvenlik.