EEE374 SİBER GÜVENLİK

Prof. Dr. Hasan Hüseyin BALIK

(9. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2 Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.8. İçerik

- Dikkate Değer Gelişmeler
- Güvenlik Duvarı İhtiyacı
- Güvenlik Duvarı Özellikleri ve Erişim Politikası
- Güvenlik Duvarı Türleri
- Güvenlik Duvarına dayalı hususlar
- Güvenlik Duvarı Konumu ve Konfigürasyonu
- Saldırı Önleme Sistemleri
- Örnek: BirleşikTehdit Yönetimi Ürünleri

Dikkate Değer Gelişmeler

- Bir dizi doğrudan bağlı terminali destekleyen merkezi bir ana bilgisayara sahip merkezi veri işleme sistemi
- PC'leri ve terminalleri birbirine ve ana bilgisayara bağlayan yerel alan ağları (LAN'lar)
- Bir dizi LAN'dan, birbirine bağlanan PC'lerden, sunuculardan ve belki bir veya iki ana bilgisayardan oluşan tesis içi ağ
- Özel bir geniş alan ağı (WAN) ile birbirine bağlanan birden çok coğrafi olarak dağıtılmış şirket içi ağdan oluşan kuruluş çapında ağ
- Çeşitli tesis ağlarının tamamının İnternet'e bağlandığı ve özel bir WAN ile bağlı olabileceği veya olmayabileceği İnternet bağlantısı
- Hem dahili kurumsal hem de harici İnternet erişilebilir hizmetler sağlayabilen bir veya daha fazla veri merkezinde bulunan sanallaştırılmış sunucularla kurumsal bulut bilgi işlem

Güvenlik Duvarı İhtiyacı

- İnternet bağlantısı önemlidir
  - Ancak tehdit oluşturur
- LAN'ları korumanın etkili yolları
- Kontrollü bir bağlantı kurmak için tesis ağı ile İnternet arasına eklenir
  - Tek bir bilgisayar sistemi veya birlikte çalışan iki veya daha fazla sistem kümesi olabilir
- Çevre savunması olarak kullanılır
  - Güvenlik ve denetim uygulamak için tek bağlantı noktası
  - Dahili sistemleri harici ağlardan yalıtır

Güvenlik Duvarı Özellikleri

Tasarım hedefleri

İçeriden dışarıya ve tersi yöndeki tüm trafik güvenlik duvarından geçmelidir.

Yalnızca yerel güvenlik politikası tarafından tanımlanan yetkili trafiğin geçmesine izin verilir.

Güvenlik duvarının kendisi sızmaya karşı bağışıktır

Güvenlik Duvarı Erişim Politikası

- Bir güvenlik duvarının planlanması ve uygulanmasındaki kritik bir bileşen, uygun bir erişim politikası belirlemektir.
  - Bu, güvenlik duvarından geçmesine izin verilen trafik türlerini listeler.
  - Adres aralıklarını, protokolleri, uygulamaları ve içerik türlerini içerir
- Bu politika, kuruluşun bilgi güvenliği risk değerlendirmesi ve politikasından geliştirilmelidir.
- Kuruluşun desteklemesi gereken trafik türlerine ilişkin geniş bir spesifikasyondan geliştirilmelidir
  - Ardından, uygun bir güvenlik duvarı topolojisi içinde uygulanabilen filtre öğelerini detaylandırmak için rafine edilir

Güvenlik Duvarı Filtre Özellikleri

- Bir güvenlik duvarı erişim politikasının trafiği filtrelemek için kullanabileceği özellikler şunları içerir:

IP adresi ve protokol değerleri

Bu tür filtreleme, paket filtresi ve durum denetimli güvenlik duvarları tarafından kullanılır

Genellikle belirli hizmetlere erişimi sınırlamak için kullanılır

Uygulama protokolü

Bu tür filtreleme, belirli uygulama protokolleri (ör. spam için e-posta) için bilgi alışverişini ileten ve izleyen uygulama düzeyinde bir ağ geçidi tarafından kullanılır

Kullanıcı kimliği

Genellikle kendilerini IPSec gibi bir tür güvenli kimlik doğrulama teknolojisi kullanarak tanımlayan dahili kullanıcılar içindir

Ağ etkinliği

Zaman veya istek, istek hızı veya diğer etkinlik kalıpları gibi hususlara dayalı olarak erişimi kontrol eder

Güvenlik Duvarı Yetenekleri ve Sınırları

Yetenekleri:

- Tek bir geçiş noktası tanımlar
- Güvenlik olaylarını izlemek için bir konum sağlar
- Güvenlikle ilgili olmayan çeşitli İnternet işlevleri için uygun platform (NAT)
- IPSec için platform görevi görebilir

Sınırları:

- Güvenlik duvarını (örn. çevirmeli) atlayarak yapılan saldırılara karşı koruma sağlanamaz
- İç tehditlere karşı tam koruma sağlayamayabilir
- Uygun şekilde güvenli olmayan kablosuz LAN'a kuruluş dışından erişilebilir
- Dizüstü bilgisayar, PDA veya taşınabilir depolama aygıtı, şirket ağının dışında virüs bulaştırabilir ve daha sonra şirket içinde kullanılabilir.

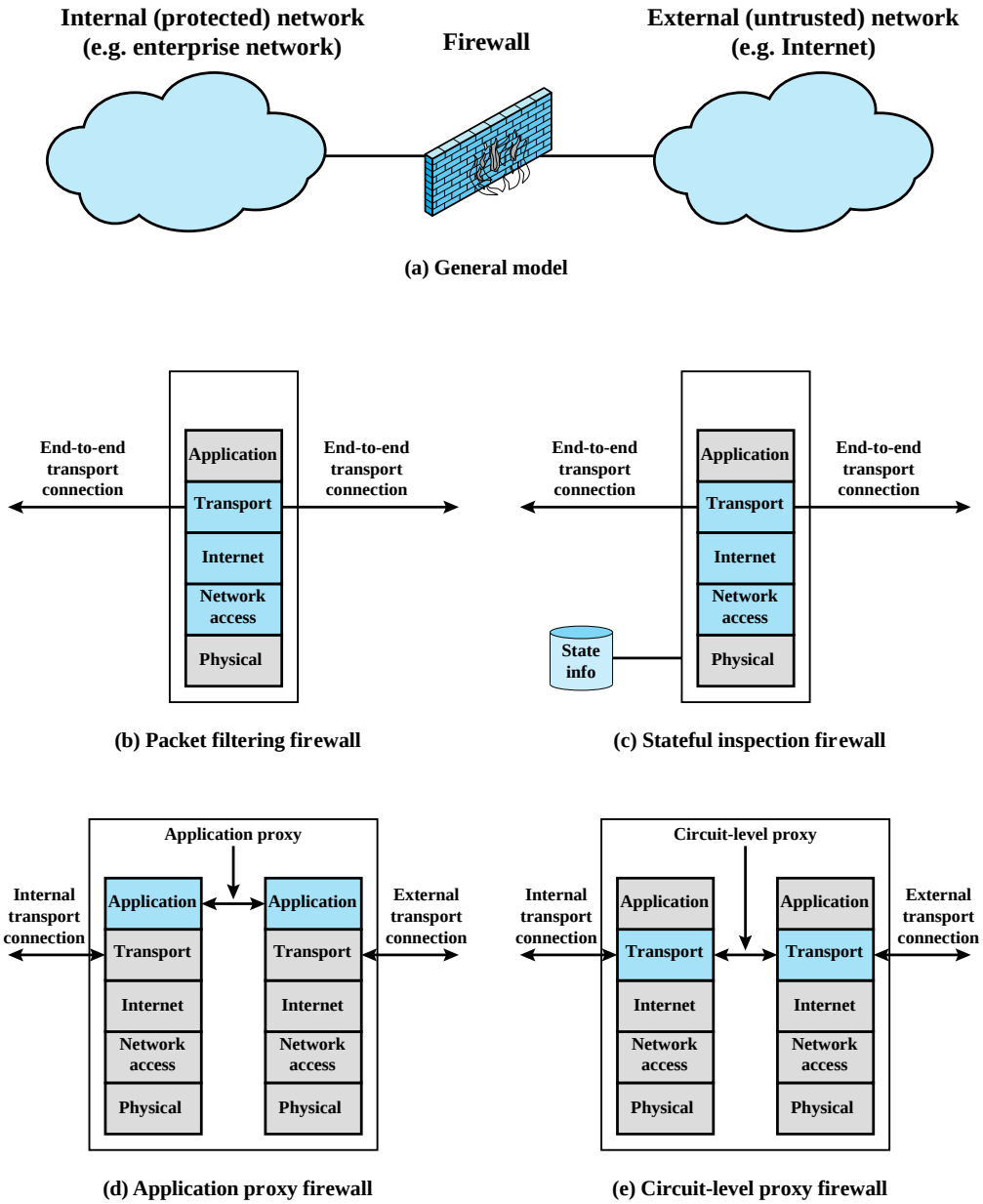


Figure 9.1 Types of Firewalls

Paket Filtreleme Güvenlik Duvarı

- Her gelen ve giden IP paketine kurallar uygular
  - Tipik olarak, IP veya TCP başlığındaki eşleşmelere dayalı bir kural listesi
  - Kural eşleşmesine göre paketi iletir veya atar

Filtreleme kuralları, bir ağ paketinde bulunan bilgilere dayalıdır.
• Kaynak IP Adresi • Hedef IP adresi • Kaynak ve hedef aktarım seviyesi adresi (örn. TCP/UDP bağlantı noktası numarası) • IP protokolü alanı • Arayüz

- İki varsayılan politika:
  - At - açıkça izin verilmedikçe yasakla
    - Daha muhafazakar, kontrollü, kullanıcılar tarafından görülebilir
  - İlet - açıkça yasaklanmadıkça izin ver
    - Yönetmesi ve kullanması daha kolay ancak daha az güvenli

Paket Filtreleme Örnekleri

Kural	Yön	Kaynak Adresi	Hedef Adresi	Protokol	Hedef Port	İşlem
1	Giriş	Harici	Dahili	TCP	25	İzin
2	Çıkış	Dahili	Harici	TCP	>1023	İzin
3	Çıkış	Dahili	Harici	TCP	25	İzin
4	Giriş	Harici	Dahili	TCP	>1023	İzin
5	Her biri	Herhangi	Herhangi	Herhngi	Herhangi	Red

Paket Filtreleme Güvenlik Duvarı Avantajları ve Zayıf Yönleri

- Avantajlar
  - Basitlik
  - Genellikle kullanıcılar için şeffaftır ve çok hızlıdır
- Zayıf yönler
  - Uygulamaya özgü güvenlik açıkları veya işlevleri kullanan saldırıları önleyemez
  - Sınırlı log kaydı işlevi vardır
  - Gelişmiş kullanıcı kimlik doğrulamasını desteklemez
  - TCP/IP protokolü hatalarına yönelik saldırılara karşı savunmasızdır
  - Yanlış yapılandırma güvenlik ihlallerine yol açabilir

Durum Denetimli Güvenlik Duvarı

Giden TCP bağlantılarından oluşan bir dizin oluşturarak TCP trafiği için kuralları sıkılaştırır

- **Halihazırda kurulan her bağlantı için bir giriş vardır**
- **Paket filtresi, yalnızca bu dizindeki girişlerden birinin profiline uyan paketler için yüksek numaralı bağlantı noktalarına gelen trafiğe izin verir**

Paket bilgilerini gözden geçirir, aynı zamanda TCP bağlantıları hakkındaki bilgileri de kaydeder

- **Sıra numarasına bağlı saldırıları önlemek için TCP sıra numaralarını takip eder**
- **FTP, IM ve SIPS komutları gibi protokoller için verileri inceler**

Örnek Durum Bilgili Güvenlik Duvarı Bağlantı Durumu Tablosu

Kaynak Adresi	Kaynak Port	Hedef Adresi	Hedef Port	İşlem
192.168.1.100	1030	210.9.88.29	80	Başlantı Kuruldu
192.168.1.102	1031	216.32.42.123	80	Başlantı Kuruldu
192.168.1.101	1033	173.66.32.122	25	Başlantı Kuruldu
192.168.1.106	1035	177.231.32.12	79	Başlantı Kuruldu
223.43.21.231	1990	192.168.1.106	80	Başlantı Kuruldu
219.22.123.32	2112	192.168.1.106	80	Başlantı Kuruldu
210.99.212.18	3321	192.168.1.106	80	Başlantı Kuruldu
24.102.32.23	1025	192.168.1.106	80	Başlantı Kuruldu
223.21.22.12	1046	192.168.1.106	80	Başlantı Kuruldu

Uygulama Düzeyinde Ağ Geçidi

- Uygulama proxy'si olarak da adlandırılır
- Uygulama düzeyinde trafik geçidi görevi görür
  - Bir TCP/IP uygulaması kullanan kullanıcı iletişim ağ geçididir
  - Kullanıcının kimliği doğrulanır
  - Ağ geçidi, uzak ana bilgisayardaki uygulamayla iletişim kurar ve sunucu ile kullanıcı arasında TCP segmentlerini aktarır
- Her uygulama için proxy kodu olmalıdır
  - Desteklenen uygulama özelliklerini kısıtlayabilir
- Paket filtrelerden daha güvenli olma eğilimindedir
- Dezavantajı, her bağlantıda ek işlem yüküdür.

Devre Düzeyinde Ağ Geçidi

Devre düzeyinde proxy

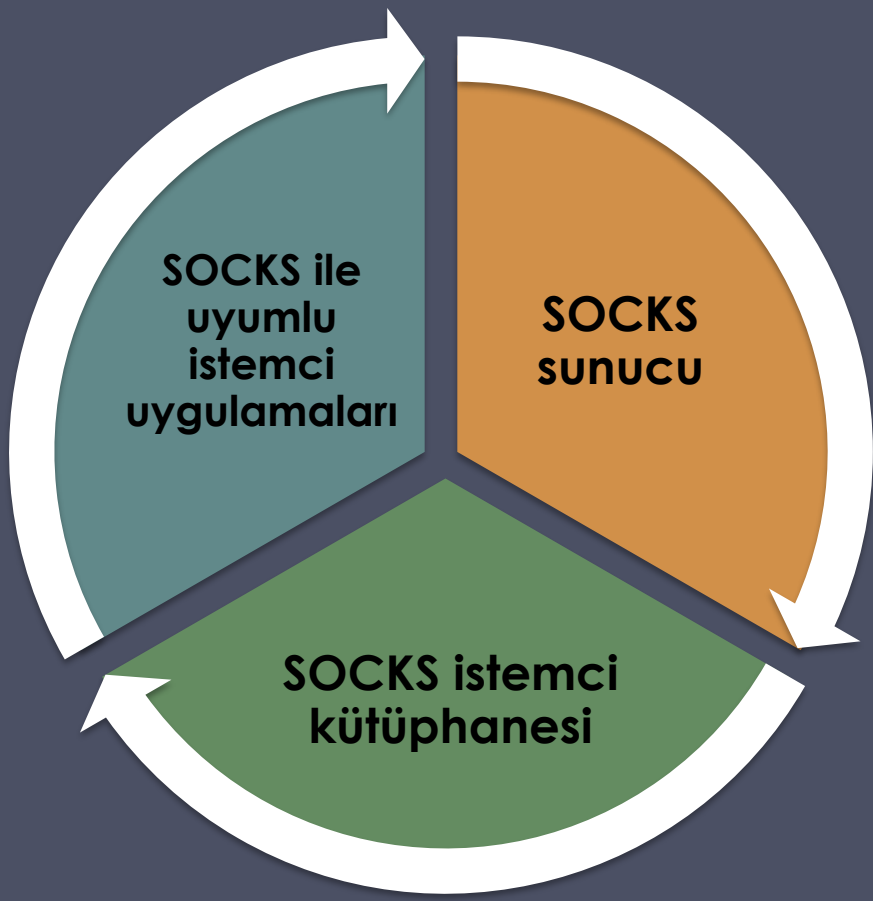
- Biri iç ana bilgisayardaki TCP kullanıcısı ile kendisi arasında ve diğeri dış ana bilgisayarda olmak üzere iki TCP bağlantısı kurar
- İçeriği incelemeden TCP segmentlerini bir bağlantıdan diğerine aktarır
- Güvenlik işlevi, hangi bağlantılara izin verileceğini belirlemekten oluşur

Genellikle içerideki kullanıcılara güvenildiğinde kullanılır

- Uygulama düzeyinde ağ geçidi gelen ve devre düzeyinde ağ geçidi giden yönde kullanılabilir
- Daha düşük işlem yükü vardır

SOCKS Devre Düzeyinde Ağ Geçidi

- SOCKS v5 RFC1928'de tanımlanır
- Bir ağ güvenlik duvarının hizmetlerini rahat ve güvenli bir şekilde kullanmak için TCP/UDP etki alanlarındaki istemci-sunucu uygulamaları için bir çerçeve sağlamak üzere tasarlanmıştır.
- İstemci uygulaması, SOCKS sunucusuyla bağlantı kurar, kimlik doğrulamasını yapar, aktarma isteği gönderir
    - Sunucu değerlendirir ve bağlantıyı kurar veya reddeder



Bileşenleri

Bastion (İyi Korunan) Ana Makina

- Güvenlik duvarı yöneticisi tarafından ağın güvenliğinde kritik bir güçlü nokta olarak tanımlanan sistemdir
- Uygulama düzeyinde veya devre düzeyinde ağ geçidi için bir platform görevi görür
- Ortak özellikleri:
  - Güvenli O/S çalıştırır, yalnızca gerekli hizmetler bulunur
  - Proxy veya ana bilgisayara erişmek için kullanıcı kimlik doğrulaması gerektirebilir
  - Her proxy, özellikleri, erişilen ana bilgisayarları kısıtlayabilir
  - Her proxy küçük, basit ve güvenlik açısından kontrol edilmiştir
  - Her proxy bağımsızdır, ayrıcalığı yoktur
  - Sınırlı disk kullanımı, dolayısıyla salt okunur kod

Ana Bilgisayar Tabanlı Güvenlik Duvarları

- Bireysel bir ana bilgisayarın güvenliğini sağlamak için kullanılır
- İşletim sistemlerinde bulunur veya eklenti paketi olarak sağlanabilir
- Paket akışlarını filtreleme ve kısıtlama işlevi görür
- Genellikle bir sunucuya kurulur

Avantajları
• Filtreleme kuralları ana bilgisayar ortamına göre uyarlanabilir • Topolojiden bağımsız koruma sağlanır • Ek bir koruma katmanı sağlar

Kişisel Güvenlik Duvarı

- Kişisel bir bilgisayar veya iş istasyonu ile İnternet veya kurumsal ağ arasındaki trafiği kontrol eder
- Hem ev hem de kurumsal kullanım için
- Tipik olarak kişisel bir bilgisayardaki bir yazılım modülüdür.
- Tüm ev bilgisayarlarını bir DSL, kablo modeme veya başka bir İnternet arabirimine bağlayan bir yönlendiriciye yerleştirilebilir
- Tipik olarak, sunucu tabanlı veya bağımsız güvenlik duvarlarından çok daha az karmaşık
- Birincil rol, yetkisiz uzaktan erişimi reddetmektir
- Solucanları ve kötü amaçlı yazılım etkinliğini tespit etmek ve engellemek için giden trafiği de izleyebilir

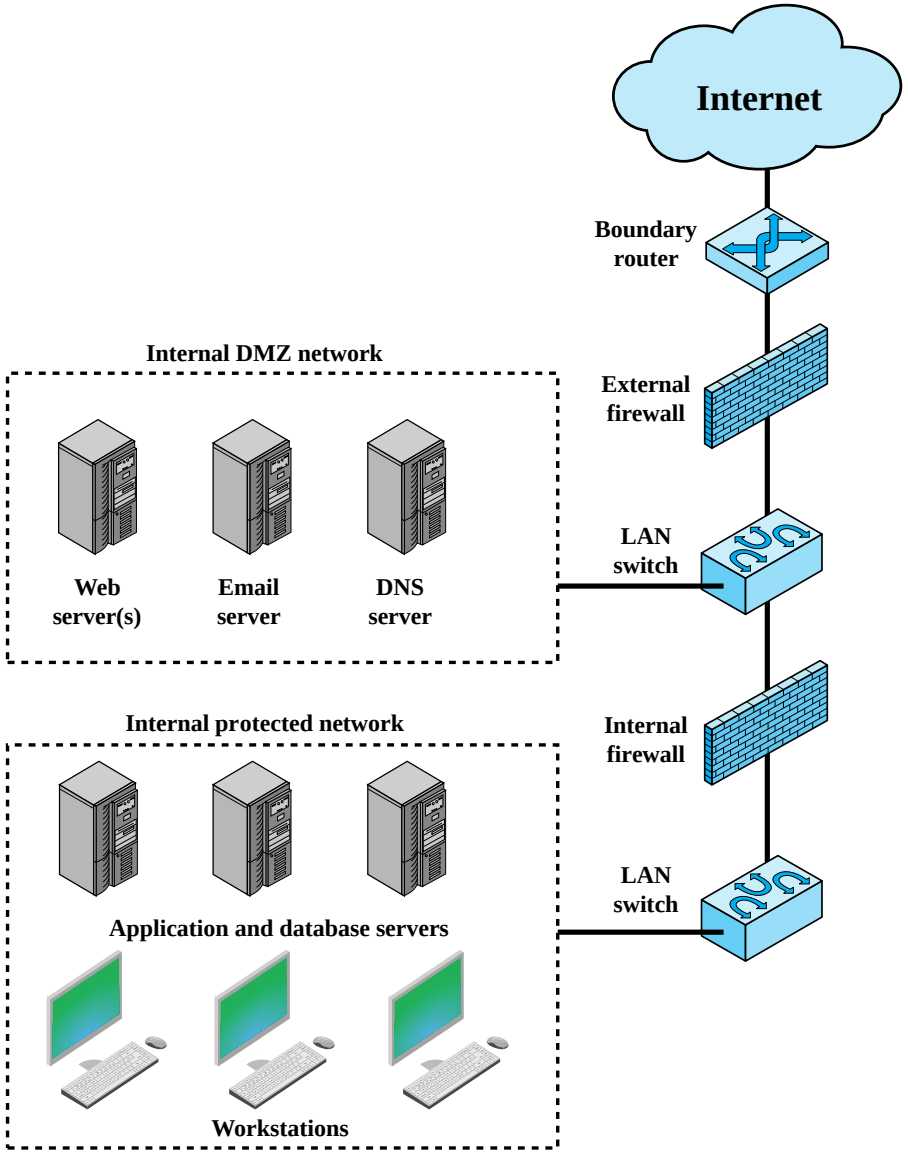


Figure 9.2 Example Firewall Configuration

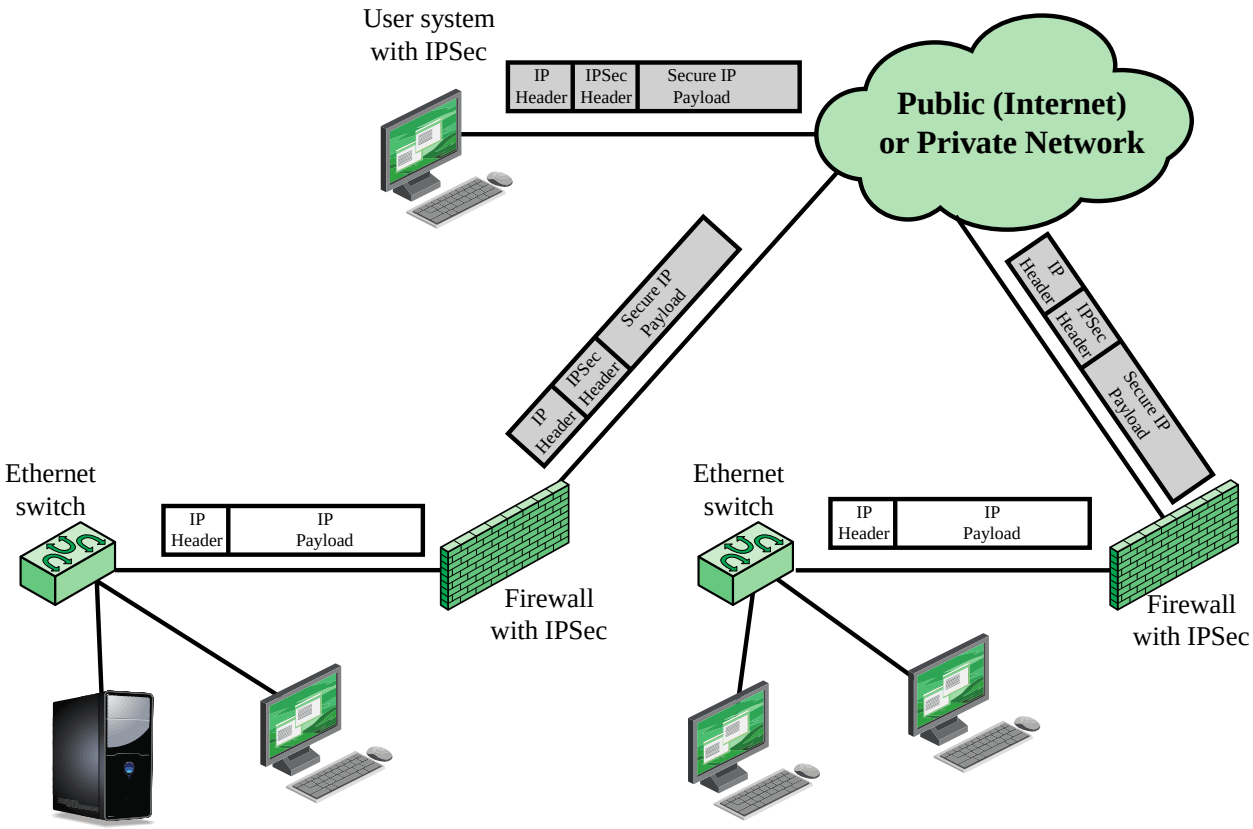


Figure 9.3 A VPN Security Scenario

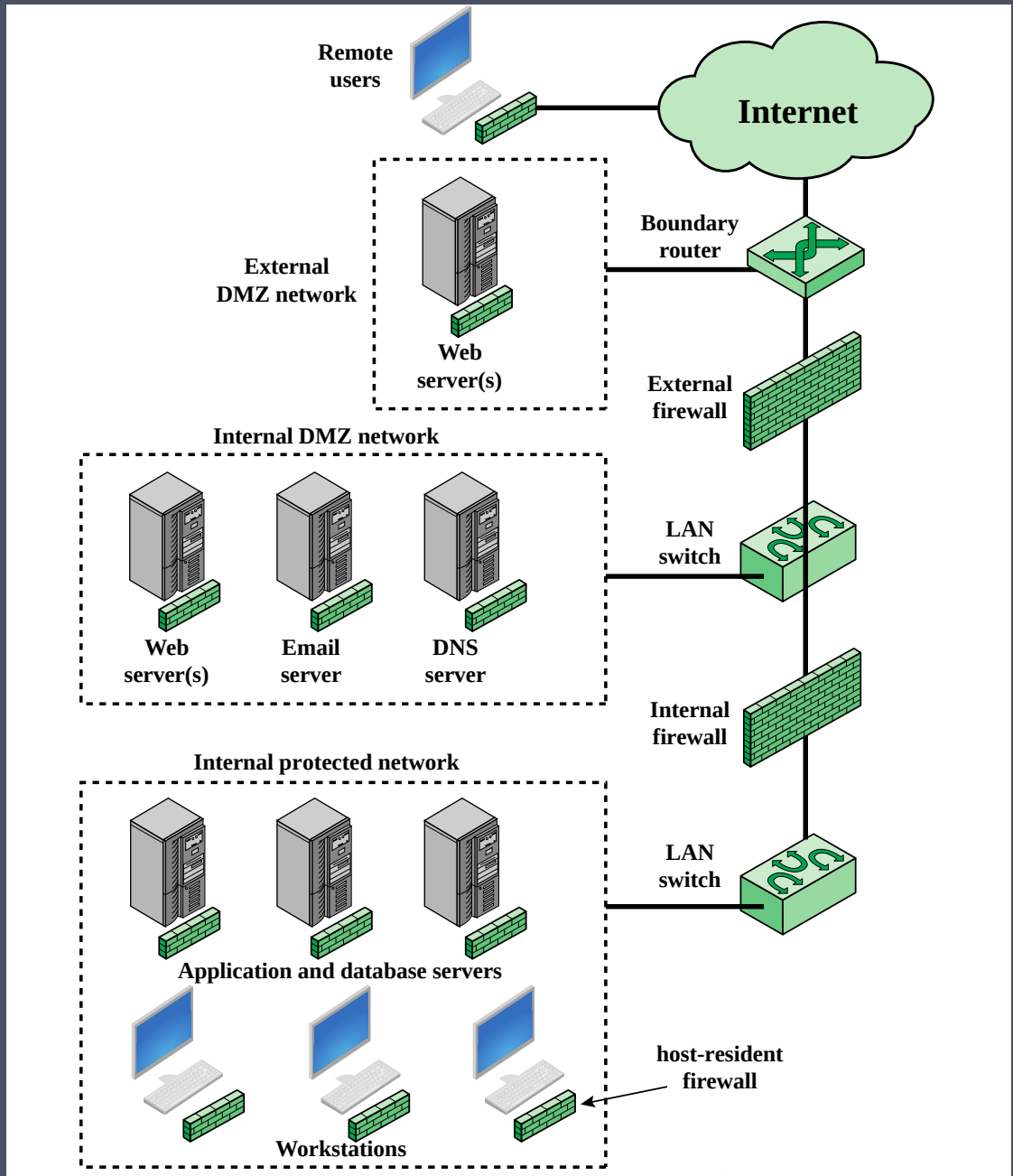


Figure 9.4 Example Distributed Firewall Configuration

Güvenlik Duvarı Topolojileri

Ana bilgisayar yerleşik güvenlik duvarı	•Sunucularda kişisel güvenlik duvarı yazılımı ve güvenlik duvarı yazılımı içerir
Tarama yönlendiricisi	•Durum bilgisiz veya tam paket filtrelemeli dahili ve harici ağlar arasında tek yönlendiricidir
Hatta tek kale	•Dahili ve harici yönlendirici arasında tek güvenlik duvarı cihazıdır
Tek kale T	•Harici olarak görülebilen sunucuların yerleştirildiği bir DMZ'ye bağlanan üçüncü bir ağ arabirimine sahiptir
Hatta çift kale	•DMZ, kale güvenlik duvarları arasına sıkıştırılmıştır
Çift kale T	•DMZ, kale güvenlik duvarında ayrı bir ağ arabirimindedir
Dağıtılmış güvenlik duvarı yapılandırması	•Büyük işletmeler ve devlet kurumları tarafından kullanılır

Saldırı Önleme Sistemleri (IPS)

- İzinsiz Giriş Tespit ve Önleme Sistemi (IDPS) olarak da bilinir
- Tespit edilen kötü amaçlı etkinliği engelleme veya engelleme girişiminde bulunma yeteneğini içeren bir IDS uzantısıdır.
- Ana bilgisayar tabanlı, ağ tabanlı veya dağıtılmış/hibrit olabilir
- Meşru kullanıcılara ait olmayan davranışları belirlemek için anormallik algılamayı veya bilinen kötü niyetli davranışları belirlemek için imza/bulgusal algılamayı kullanabilir, bir güvenlik duvarının yaptığı gibi trafiği engelleyebilir, ancak bunun ne zaman yapılacağını belirlemek için IDS'ler için geliştirilmiş algoritma türlerini kullanır.

Ana Bilgisayar Tabanlı IPS (HIPS)

- Saldırıları belirlemek için imza/sezgisel veya anormallik algılama tekniklerinden yararlanabilir
  - İmza: uygulama ağ trafiğinin veya sistem çağrılarının belirli içeriğine odaklanılır ve kötü amaçlı olarak tanımlanan kalıplar aranır
  - Anormallik: IPS, kötü amaçlı yazılıma işaret eden davranış kalıplarını arıyor
- Bir HIPS tarafından ele alınan kötü niyetli davranış türlerinin örnekleri şunları içerir:
  - Sistem kaynaklarının değiştirilmesi
  - Ayrıcalık yükseltme istismarları
  - Arabellek taşması istismarları
  - E-posta kişi listesine erişim
  - Dizin geçişi

HIPS

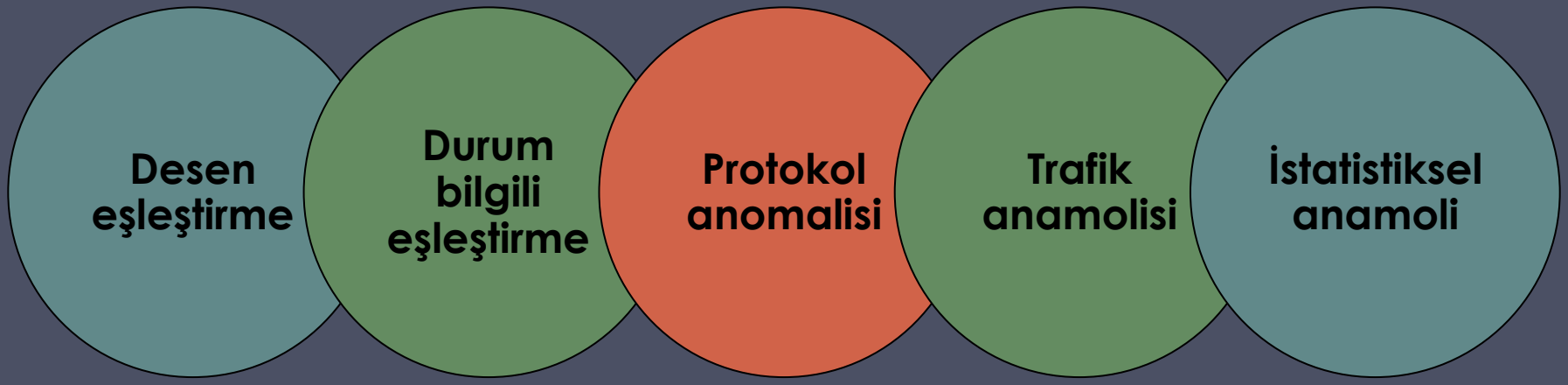
- Yetenek, belirli bir platforma göre uyarlanabilir
- Bir masaüstü veya sunucu sistemi için bir dizi genel amaçlı araç kullanılabilir.
- Bazı paketler, Web sunucuları ve veritabanı sunucuları gibi belirli sunucu türlerini korumak için tasarlanmıştır.
  - Bu durumda HIPS, belirli uygulama saldırılarını arar.
- Korumalı alan (sandbox) yaklaşımı kullanabilir
  - Korumalı alanlar özellikle Java uygulamaları ve scripting dilleri gibi mobil kodlar için uygundur.
  - HIPS, bu tür kodları yalıtılmış bir sistem alanında karantinaya alır, ardından kodu çalıştırır ve davranışını izler.
- Bir HIPS'nin tipik olarak masaüstü koruması sağladığı alanlar:
  - Sistem çağrıları
  - Dosya sistemi erişimi
  - Sistem kayıt defteri ayarları
  - Ana bilgisayar girişi/çıkışı

HIPS'in Rolü

- Birçok sektör gözlemcisi, masaüstü ve dizüstü bilgisayar sistemleri de dahil olmak üzere kurumsal son noktayı artık bilgisayar korsanları ve suçlular için ana hedef olarak görüyor.
  - Bu nedenle, güvenlik satıcıları daha çok uç nokta güvenlik ürünleri geliştirmeye odaklanıyor
  - Geleneksel olarak uç nokta güvenliği, antivirüs, casus yazılım önleme, istenmeyen e-posta önleme ve kişisel güvenlik duvarları gibi bir dizi farklı ürün tarafından sağlanır
- Yaklaşım, entegre, tek ürünlü bir işlev paketi sağlama çabasıdır.
  - Entegre HIPS yaklaşımının avantajları, çeşitli araçların yakın bir şekilde birlikte çalışması, tehdit önlemenin daha kapsamlı olması ve yönetimin daha kolay olmasıdır.
- İhtiyatlı bir yaklaşım, HIPS'i, güvenlik duvarları veya ağ tabanlı IPS'ler gibi ağ seviyesindeki cihazları içeren derinlemesine savunma stratejisinde bir unsur olarak kullanmaktır.

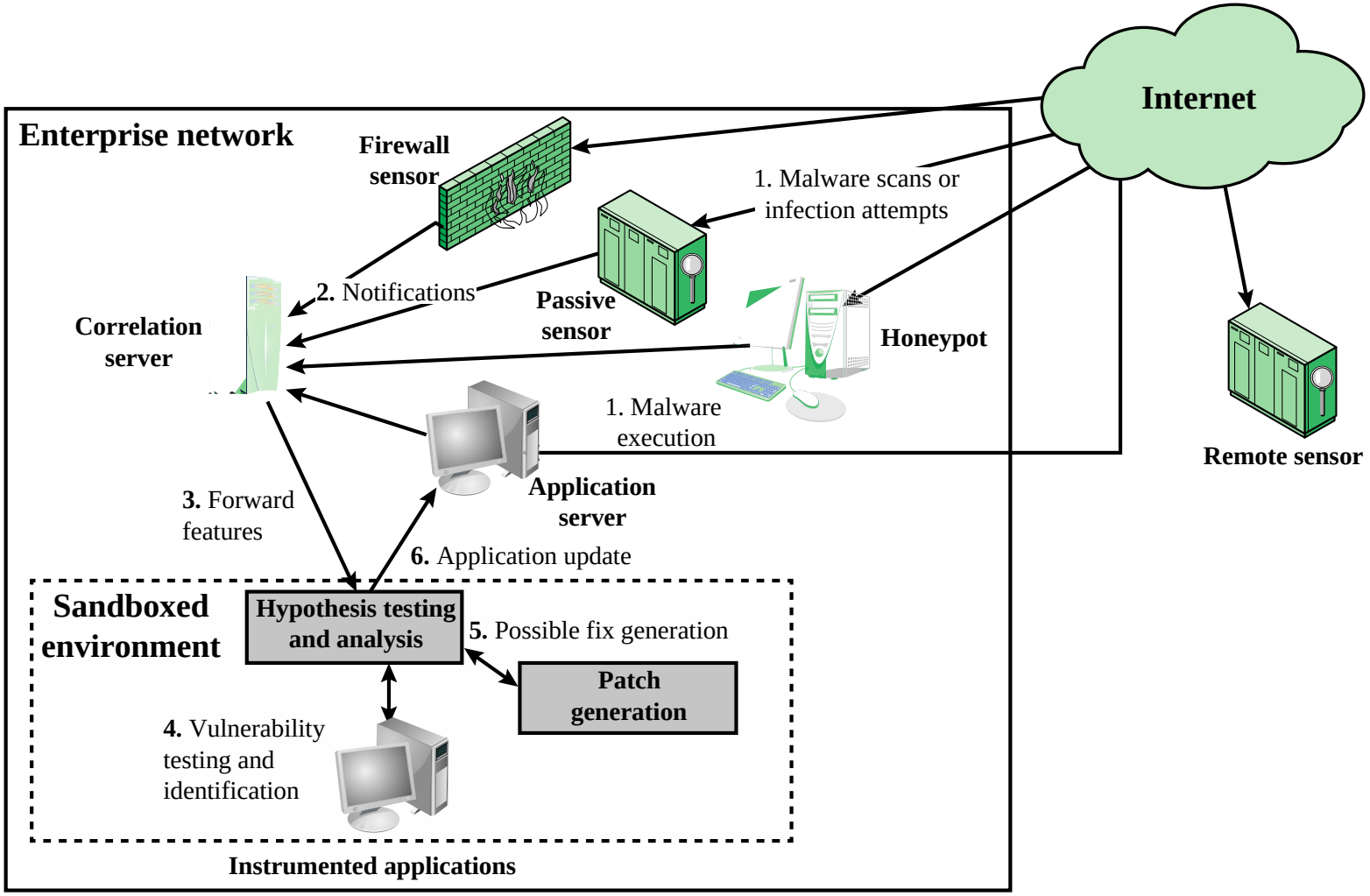
Ağ Tabanlı IPS (NIPS)

- Paketleri değiştirme veya atma ve TCP bağlantılarını koparma yetkisine sahip hat içi NIDS'dir.
- İmza/sezgisel algılama ve anormallik algılamayı kullanır
- Akış verilerinin korunmasını sağlar
  - Bir dizi paketteki uygulama yükünün yeniden birleştirilmesini gerektirir
- Kötü amaçlı paketleri belirlemek için kullanılan yöntemler:



Dijital Bağışıklık Sistemi (Digital Immune System)

- Kötü amaçlı yazılımların neden olduğu kötü niyetli davranışlara karşı kapsamlı savunma sağlar
- IBM tarafından geliştirilmiş ve Symantec tarafından rafine edilmiştir
- Bu gelişmenin motivasyonu, İnternet tabanlı kötü amaçlı yazılım tehdidinin artması, İnternet tarafından sağlanan yayılma hızının artması ve duruma küresel bir bakış açısı edinme ihtiyacıdır.
- Başarı, kötü amaçlı yazılım analiz sisteminin yeni ve yenilikçi kötü amaçlı yazılım türlerini algılama yeteneğine bağlıdır.



Şekil 9.5 Kötü Amaçlı Yazılım İzleyicilerinin Yerleştirilmesi

Snort Inline

- Snort'un izinsiz giriş önleme sistemi olarak işlev görmesini sağlar
- Snort kullanıcısının paketleri atmak (drop) yerine değiştirmesine izin veren bir değiştirme seçeneği içerir
  - Bal küpü uygulaması için kullanışlıdır
  - Saldırganlar hatayı görür ancak neden oluştuğunu anlayamaz

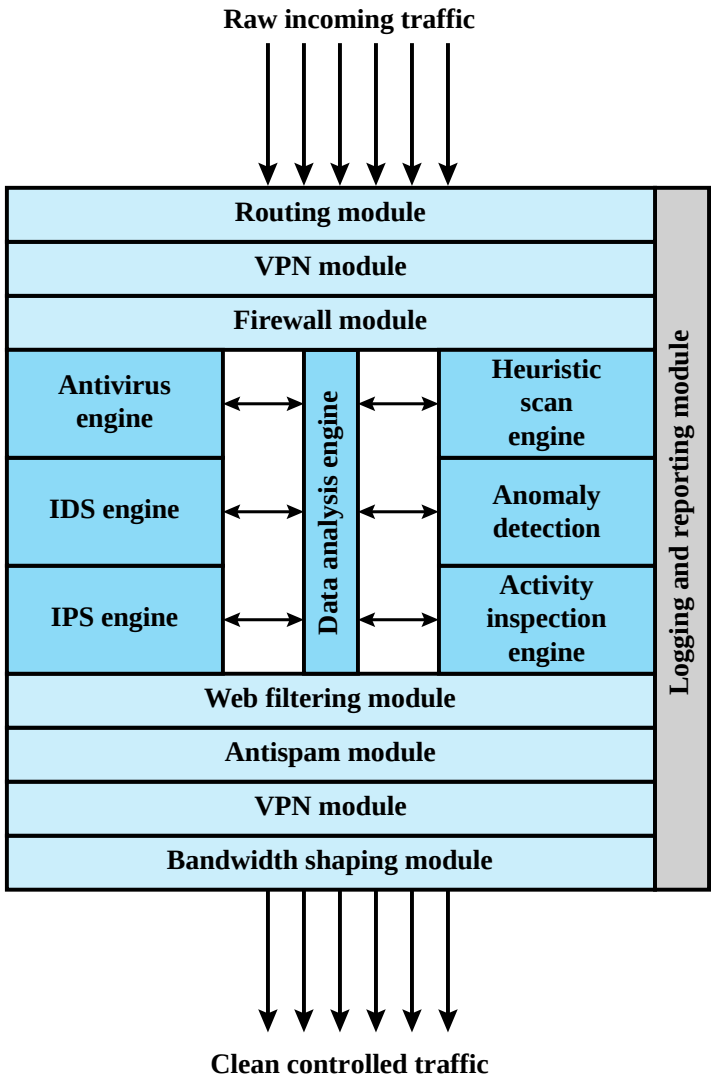


Figure 9.6 Unified Threat Management Appliance (based on [JAME06])

Sidewinder G2 Güvenlik Cihazı Saldırı Korumaları
Özet - Taşıma Katmanı Örnekleri

Saldırılar ve İnternet Tehditleri		Korumalar	
TCP			
• Geçersiz bağlantı noktası numaraları • Geçersiz sıra numaraları • SYN taşkınları • XMAS ağaç saldırıları • Geçersiz CRC değerleri • sıfır uzunluk • TCP Başlığı olarak rastgele veriler	• TCP kaçırma girişimleri • TCP kimlik sahtekarlığı saldırıları • Küçük PMTU saldırıları • SYN saldırısı • Kiddie saldırıları • Paket üretimi: farklı TCP seçenekleri seti	• Doğru TCP bayraklarını uygula • TCP başlık uzunluğunu zorunlu kıl • Uygun bir üç yönlü el sıkışmayı zorunlu kıl • TCP oturumunu doğru şekilde kapat • Biri içeride biri dışarıda olmak üzere 2 oturum aç • Doğru TCP bayrağı kullanımını zorunlu kıl • TCP oturum zaman aşımlarını yönet • SYN saldırısını engelle	• Doğruluğu sağlayan paketlerin yeniden birleştir • TCP zaman aşımlarını düzgün şekilde işle ve zamanlayıcıları yeniden ilet • Tüm TCP proxy'leri koru • Erişim listeleri aracılığıyla Trafik Kontrolü yap • Açık olmayan bağlantı noktalarına ait TCP paketlerini drop et (at) • Proxy'ler paket üretmeyi engeller
UDP			
• Geçersiz UDP paketleri • Kuralları atlamak için rastgele UDP verileri	• Bağlantı tahmini • UDP bağlantı noktası taraması	• Düzgün UDP paketini doğrula • Açık olmayan bağlantı noktalarına ait UDP paketlerini drop et (at)	

Sidewinder G2 Güvenlik Cihazı Saldırı Korumaları Özet - Uygulama Katmanı Örnekleri 1/3

Saldırılar ve İnternet Tehditleri	Korumalar
DNS	
AAAA sorgularından yanlış NXDOMAIN yanıtları, hizmet reddi koşullarına neden olur	• Negatif önbelleğe almaya izin verme • DNS önbelleği zehirlenmesini önle
9.2.1'den önceki ISC BIND 9, uzak saldırganların, message.c is not NULL'deki dns_message_findtype() işlevine ilişkin rdataset parametresi doğru şekilde işlenmediğinde bir hata koşulunu tetikleyen hatalı biçimlendirilmiş bir DNS paketi aracılığıyla hizmet reddine (kapatma) neden olur	• Sidewinder G2, yanlış biçimlendirilmiş DNS mesajlarının güvenlik duvarı işlemlerini etkilemek için kötü niyetli kullanımını engeller • DNS sorgusu saldırılarını önler • DNS yanıt saldırılarını önler
FTP	
• FTP sıçrama saldırısı • PASS saldırısı • FTP Bağlantı Noktası enjeksiyon saldırıları • TCP segmentasyon saldırısı	• Sidewinder G2, bu saldırıları önlemek için FTP komutlarını filtreleme özelliğine sahiptir. • Gerçek ağ ayrımı, segmentasyon saldırılarını önler.
SQL	
SQL Net ortadaki adam saldırıları	• Type Enforcement teknolojisi ile korunan akıllı proxy kullanır • Şeffaf olmayan bağlantılar yoluyla Dahili DB'yi gizler

Sidewinder G2 Güvenlik Cihazı Saldırı Korumaları Özet - Uygulama Katmanı Örnekleri 2/3

Saldırılar ve İnternet Tehditleri	Korumalar
Gerçek Zamanlı Akış Protokolü (RTSP)	
• Arabellek (Buffer) taşması • Hizmet reddi	• Type Enforcement teknolojisi ile korunan akıllı proxy kullanır • Protokol doğrulaması yapar • multicast trafiğini reddeder • Kurulum ve ayırma yöntemlerini kontrol eder • PNG ve RTSP protokolünü doğrular ve diğerlerini atar • Yardımcı bağlantı noktası izlemesi yapar
SNMP	
• SNMP taşma saldırıları • Varsayılan topluluk saldırısı • Kaba kuvvet saldırısı • SNMP put saldırısı	• SNMP sürüm trafiği 1, 2c'yi filtreler • Okuma, Yazma ve Bildirim mesajlarını filtreler • OID'leri Filtreler • PDU (Protokol Veri Birimi)'yu filtreler
SSH	
• Meydan Okuma Yanıtı arabelleği taşmaları • SSHD, kullanıcıların "İzin Verilen Kimlik Doğrulamaları"nı geçersiz kılmasına olanak tanıması • OpenSSH buffer_append_space arabellek taşması • OpenSSH/PAM sorgulaması Yanıt arabelleği taşması • Tek tek sunulan OpenSSH kanal kodu	Sidewinder G2 v6.x'in yerleşik Type Enforcement teknolojisi, Secure Computing'in OpenSSH arka plan programı kodunun değiştirilmiş sürümlerinin yeteneklerini kesinlikle sınırlar.

Sidewinder G2 Güvenlik Cihazı Saldırı Korumaları Özet - Uygulama Katmanı Örnekleri 3/3

Saldırılar ve İnternet Tehditleri	Korumalar
SMTP	
• Sendmail arabellek taşmaları • Sendmail hizmet reddi saldırıları • Sendmail'de uzak arabellek taşması • Sendmail adresi ayrıştırma arabelleği taşması • SMTP protokolü anormallikleri	• Type Enforcement teknolojisi ile korunan bölünmüş Sendmail mimarisi • Denetimler için özelleştirilmiş Sendmail • Type Enforcement teknolojisi ile arabellek taşmalarını önler • Sendmail, SMTP protokol anormalliklerini kontrol eder
• SMTP solucan saldırıları • SMTP posta taşması • Röle saldırıları • Virüsler, Truva atları, solucanlar • E-posta adresi sahteciliği • MIME saldırıları • Kimlik avı e-postaları	• Protokol doğrulama • Antispam filtresi • Posta filtreleri—boyut, anahtar kelime • Özel antivirüs • Antiröle • MIME/Antivirüs filtresi • Güvenlik duvarı antivirüs • Virüs taraması yoluyla kimlik avına karşı koruma
Casus Yazılım Uygulamaları	
• Pazarlama amacıyla bilgi toplamak için kullanılan reklam yazılımı • Atları takip etmek • Truva atları • Kötü amaçlı yazılım • Arka Kapı Noel Babaları	Sidewinder G2 ile yerleşik SmartFilter URL filtreleme özelliği, indirmeleri önleyerek Casus Yazılım URL'lerini filtrelemek üzere yapılandırılabilir