Bilgi Güvenliği ve Kriptografi

Temel Güvenlik Teknolojileri ve Güvenli Ağ Mimarileri

- Bu bölümde genel olarak ağ güvenliğini sağlamaya yönelik kullanılan araçlar ve protokoller ele alınacaktır.

- **TEMEL GÜVENLİK MEKANİZMALARI**

Bilgi güvenliği kavramı etrafında sorulabilecek önemli sorulardan biri şu şekilde olabilir:

"Bilgisayarımızı, ağımızı veya ağımızdaki bir servisimizi korumak için ne kadar güvenlik önlemi almalıyız?"

- Cevap:

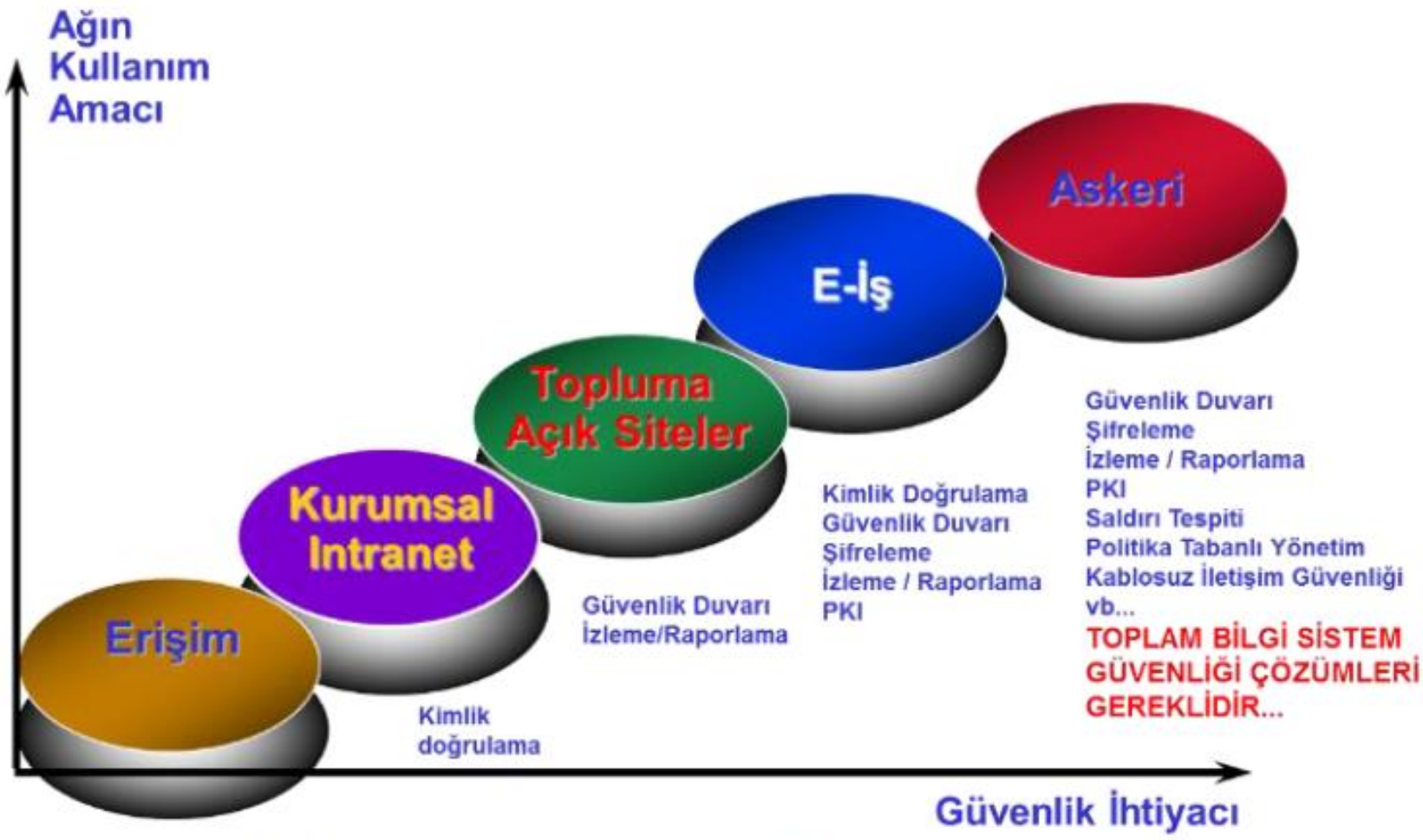
"Ne kadar değerli bilgi varsa o kadar önlem almalıyız. Eğer yayınladığımız veri değerli değilse büyük güvenlik önlemleri almaya da gerek yoktur."

- Örneğin kurum içerisinde sadece açık bilgileri yayınlamak için kullanılacak bir sunucu üzerinde güvenlik önlemi almaya gerek yoktur.

- Kuruma özgü bilgilerin bulunduğu bir web sayfası söz konusu ise kimlik doğrulama yeterli olacaktır.

- Topluma açık siteler için ise sistemi dış saldırılardan koruyacak bir güvenlik duvarı vb. önlemler ile ve sunucu üzerindeki önemli olayları izlemeye yardımcı olacak izleme sistemleri kullanılmalıdır.

- Bu durum e-ticaret ve askeri amaçlı kullanılan sistemler için farklılık arz edebilir.



Ağın Kullanım Amacı ve Güvenlik İhtiyacı

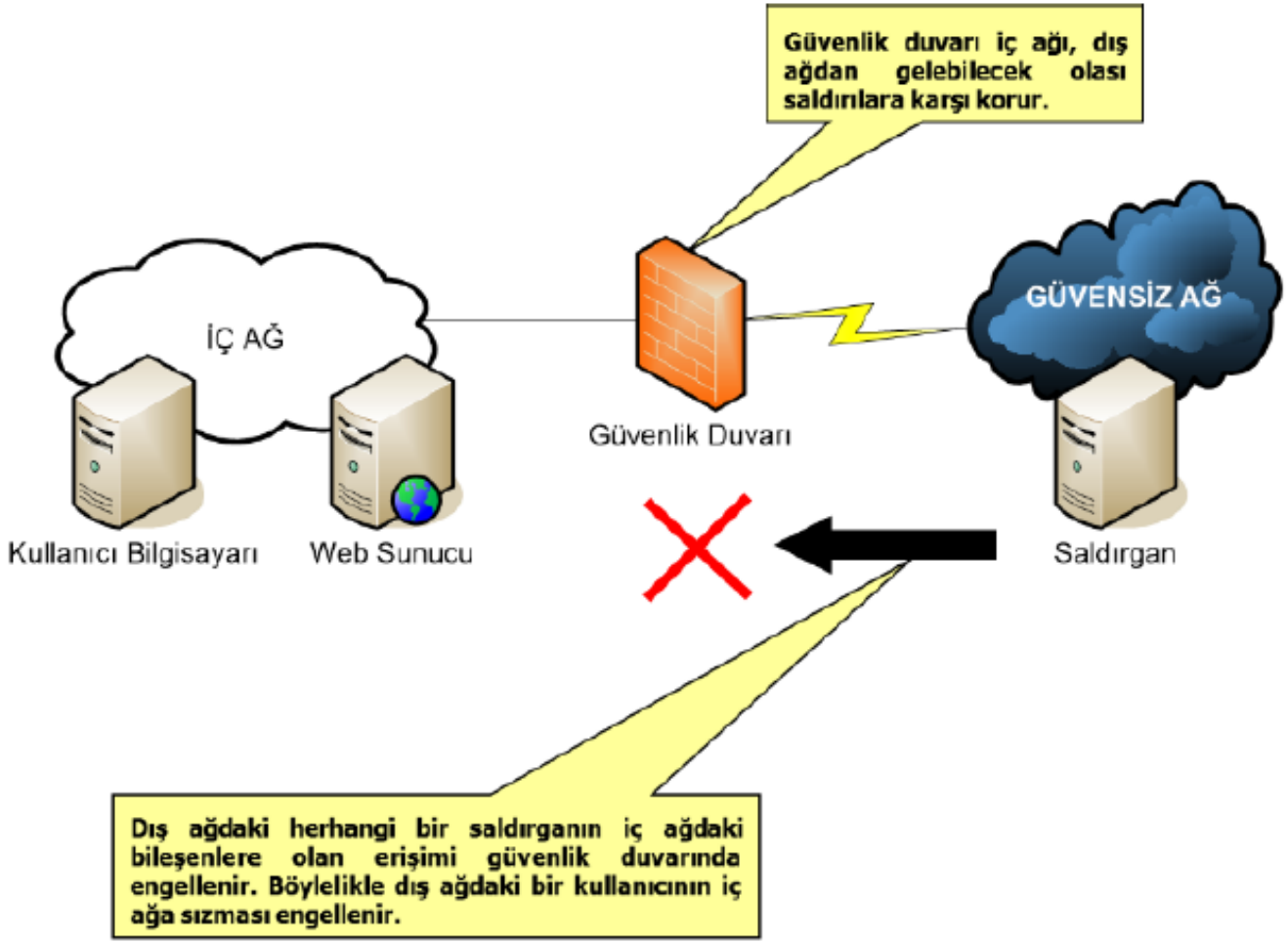
Güvenlik Duvarı - Firewall

- **Güvenlik duvarının temel görevi ağ trafiğini kontrol altına almaktır. Bu çerçevede iç ağdan dış ağa giden ya da dış ağdan iç ağa gelen trafiği kontrol ederek istenmeyen paketlerin ağa girmesini ve ağdan çıkmasını engeller.**

- Ağ üzerinde ve kendi üzerinde çalışan servisleri kontrol eder. Güvenlik duvarına takılmış olan ağ bağdaştırıcı kartları üzerinde farklı güvenlik özelliklerini etkinleştirerek farklı güvenlik seviyesine sahip ağlar oluşturur.

- Ağda bulunan cihazlar ve kendisinin yönetimi için gerekli erişim kontrolünü sağlayarak ağın güvenli bir şekilde erişim ve yönetimini sağlar. Kural tablosu ve servislere ilişkin önemli olayların kayıtlarını kendi üzerinde ya da kayıt sunucuda tutarak ağa ait önemli olayların sonradan incelenebilmesini sağlar.

Güvenlik Duvarı - Firewall



Güvenlik Duvarı - Firewall

- **Güvenlik duvarı iç ağ ile dış ağ arasında konumlandırılır.**

- **Dış ağdan gelebilecek olası saldırılara karşı iç ağın önemli ölçüde korunmasını sağlar.** Bununla birlikte iç ağdan dış ağa ve dış ağdan iç ağa yapılan erişimler güvenlik duvarı tarafından denetlenerek sadece gerekli erişimlere izin verilir. Bunun dışında kalan erişimler yetkisiz erişim olarak değerlendirilir ve bu erişimlere izin verilmez.

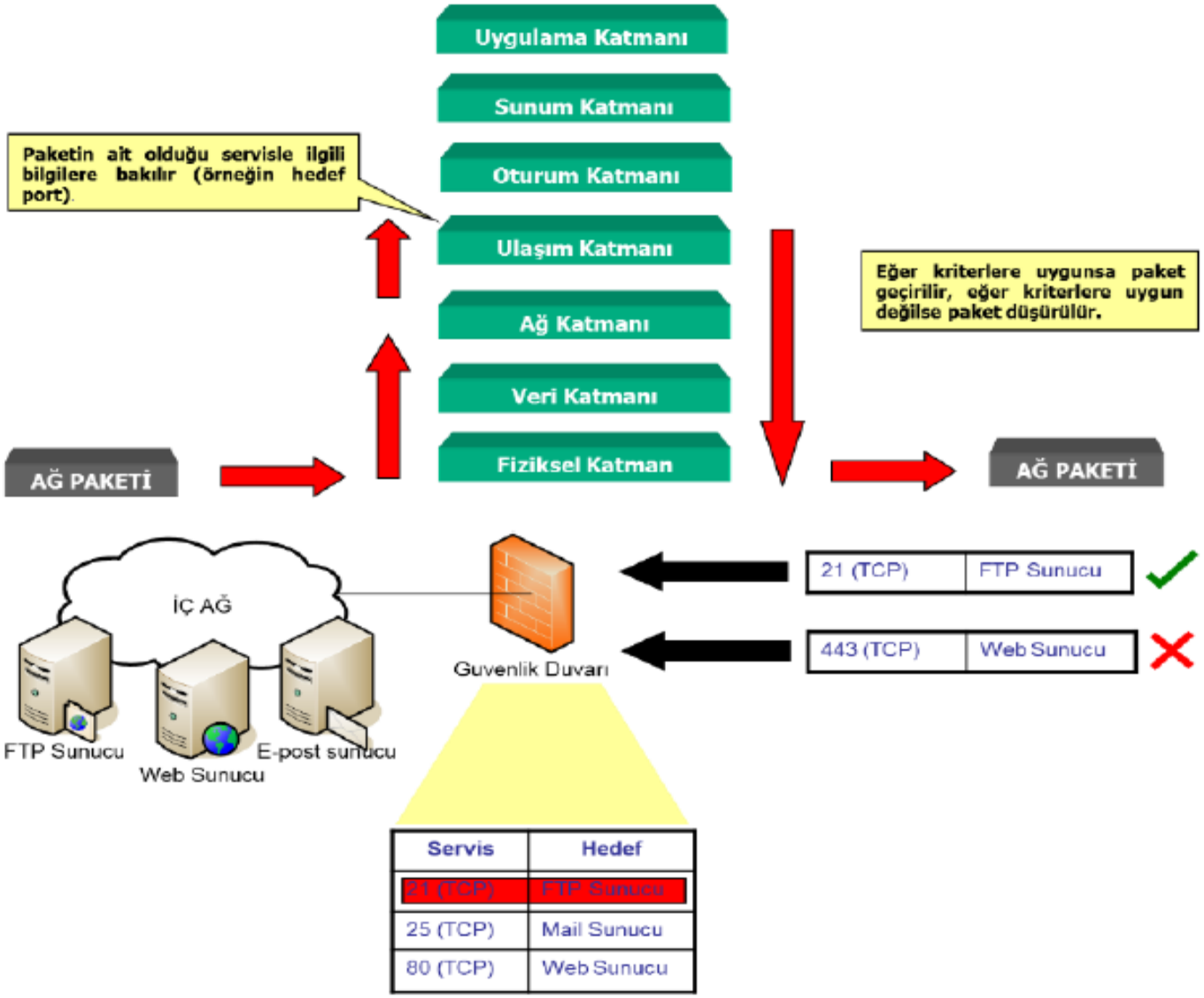
- **Ayrıca yapılan her türlü erişim ile ilgili detay bilgiler güvenlik kayıtları olarak tutulur. Bu güvenlik kayıtları, çoğunlukla, sonradan herhangi bir güvenlik sorunu olduğunda incelenerek kaynağını bulmak için kullanılır.**

Güvenlik Duvarı - Firewall

- **Paket filtreleme her güvenlik duvarında bulunan en temel özelliklerden biridir.** Paket filtrelemede, gelen ve giden paketlerin bilgilerine bakılır ve söz konusu paketin geçirilip geçirilmeyeceğine karar verilir.

- Genellikle bir güvenlik duvarı gelen ve giden paketleri incelerken paketin **ulaşım katmanı bilgilerine** kadar ulaşabilir. Paket filtrelemede bir IP paketinin aşağıdaki alanlarına bakılır:
  - Kaynak IP adresi
  - Hedef IP adresi
  - Gömülü protokol (TCP, UDP, ICMP, vb…)
  - Hedef port (Erişilmeye çalışılan servis, örneğin web servisi - 80 no'lu port)

Güvenlik Duvarı - Firewall



Open Systems Interconnection (OSI) Modeli

- **Open Systems Interconnection** (**OSI**) modeli ISO (International Organization for Standardization) tarafından geliştirimiştir. Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır.
-
- OSI Modeli herhangi bir donanım ya da bilgisayar ağı tipine göre değişiklik göstermemektedir. OSI'nin amacı ağ mimarilerinin ve protokollerinin bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır.
-
- OSI modeli sayesinde bir cihazın ağ içinde veya ağ dışında nasıl görevlendirildiği kolaylıkla anlatılabilir. Gerek ağ içinde gerek ağ dışında veri iletimi için verinin mutlaka her katmandan geçmesi gerekir. Geçtiği her katmanda da veriye belli görevler yüklenir.

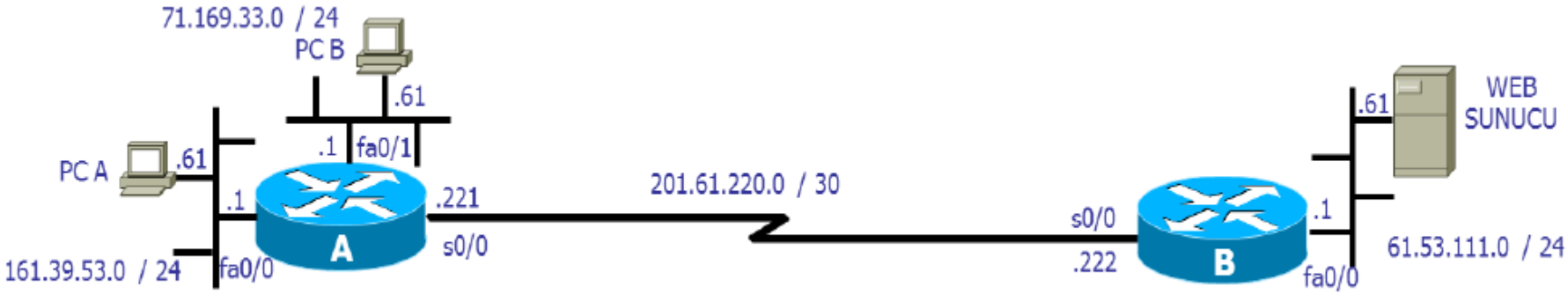
- OSI katmanlarında veri iletimi için uygulama katmanından donanım katmanına(fiziksel katman) doğru giderken veriye her bir katmanda ayrı bir başlık eklenir. Veri karşıdaki bilgisayara ulaştığında donanım katmanından(fiziksel katman) uygulama katmanına doğru bu başlıklara göre gider. En son uygulama katmanına ulaştığında veri karşı bilgisayara ulaşmış olur.

OSI Modeli				
Katman		Veri birimi	İşlevi[5]	Örnekler
Sunucu katmanları	7. Uygulama	Veri	Kaynak paylaşımı, uzaktan dosya erişimi, dizin hizmetleri veya sanal uçbirimler gibi üst seviye APIler	NFS, SMB, AFP, FTAM, NCP
	6. Sunum		Ağ hizmeti ve uygulama arasında veri çevirisi, örneğin karakter kodlaması, veri sıkıştırma ve şifreleme/şifre çözme	CSS, GIF, HTML, XML, JSON, S/MIME,
	5. Oturum		İletişim oturumlarının, yani iki düğüm arasında ileri ve geri aktarımlar şeklinde sürekli olarak gerçekleşen veri takası.	RPC, SCP, PAP, TLS, FTP, HTTP, HTTPS, SMTP, SSH, Telnet
	4. Taşıma	Bölüt	Veri bölümlerinin, bölütleme, alıntılama ve çoğullama gibi işlemlerle ağ üzerinde noktalara güvenli bir şekilde iletilmesi.	NBF, TCP, UDP
Ortam katmanları	3. Ağ	Paket/Datagram	Çok düğümlü bir ağın, adreslendirme, yönlendirme (routing) ve trafik denetimi gibi süreçler kullanılarak yapılandırılması ve yönetilmesi.	AppleTalk, ICMP, IPsec, IPv4, IPv6
	2. Veri bağlantısı	Bit/Çerçeve (Frame)	Fiziksel bir katman aracılığıyla birbirine bağlı iki düğüm arasında veri çerçevelerinin güvenli bir şekilde iletilmesi	IEEE 802.2, L2TP, LLDP, MAC, PPP, ATM, MPLS
	1. Fiziksel	Bit	İşlenmemiş bit akışlarının fiziksel bir ortam üzerinden gönderilmesi ve teslim alınması	DOCSIS, DSL, Ethernet physical layer, ISDN, RS-232

Yönlendiriciler ile Paket Filtreleme

- Erişim kontrolü politikası bir takım kısıtlayıcı kuralın bir araya getirilmesiyle oluşturulur. Bir erişim kontrolü politikasındaki kurallarda en azından aşağıdaki üç kıstas bulunmalıdır:
  - Erişimi sağlayacak bilgisayar
  - Erişilecek bilgisayar
  - Erişim sağlanacak servisler

Yönlendiriciler ile Paket Filtreleme



Gelişmiş Erişim Kontrol Listeleri

- 161.39.53.0 ağı ve B bilgisayarı WEB sunucuya 80 ve 443 numaralı TCP portlarından erişebilecektir,
- PC A, B yönlendiricisine 23 numaralı TCP portundan erişebilecektir.

```
ROUTERA(config)#access-list 161 permit tcp 161.39.53.0 0.0.0.255 host 61.53.111.61 eq 80
ROUTERA(config)#access-list 161 permit tcp 161.39.53.0 0.0.0.255 host 61.53.111.61 eq 443
ROUTERA(config)#access-list 113 permit tcp host 71.169.33.61 host 61.53.111.61 eq 80
ROUTERA(config)#access-list 113 permit tcp host 71.169.33.61 host 61.53.111.61 eq 443
ROUTERA(config)#access-list 190 permit tcp host 161.39.53.61 host 201.61.220.222 eq 23
ROUTERA(config)#interface FastEthernet0/0
ROUTERA(config-if)#access-group 161 in
ROUTERA(config-if)#access-group 190 in
ROUTERA(config-if)#exit
ROUTERA(config)#interface FastEthernet0/1
ROUTERA(config-if)#access-group 113 in
```

L7 (Layer 7) Firewall

- Bir saldırı imzası, güvenlik duvarının herhangi bir saldırıyı tanımasına yetebilecek düzeyde bilgi içerir.

- Bu özelliğe sahip bir güvenlik duvarı gelen paketleri uygulama düzeyinde inceler. Yani, paketin daha üst katman bilgilerini inceleyebilir.

- Daha sonra bu bilgileri saldırı imzaları ile karşılaştırır. Eğer herhangi bir uyuşma söz konusu ise ilgili paketin geçişine izin verilmez. İmzası bulunmayan saldırılar güvenlik duvarı tarafından tespit edilemez.

L7 (Layer 7) Firewall

- Bununla birlikte gelişmiş güvenlik duvarlarında bilgisayar virüsleri ve zararlı içerikler de taranabilmekte ve eğer gerekirse ilgili trafik durdurulabilmektedir.

- İçerik kontrolü yapan güvenlik duvarları bu özelliğe sahiptir. Ancak bu güvenlik duvarları, içerik kontrolcülere göre çok daha kısıtlı yeteneklere sahiptir. Yani, ancak sınırlı sayıdaki zararlı içerik ve virüsler bu güvenlik duvarları tarafından engellenebilmekte ve bu işlem sınırlı sayıda protokol için yapılabilmektedir.

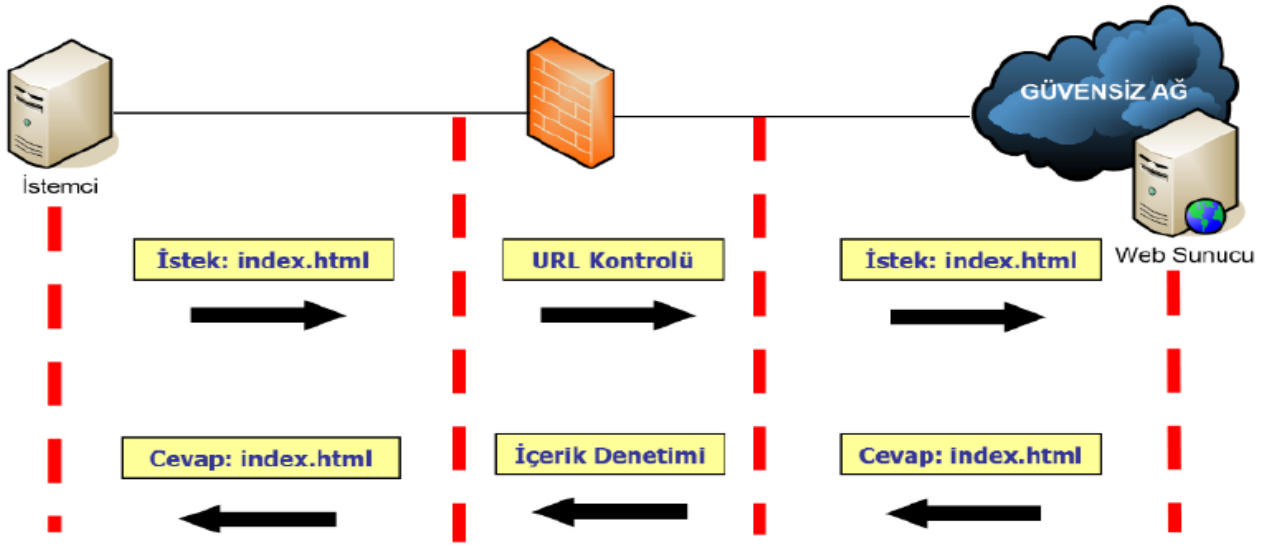
- Ama yine de içerik kontrolü sağlayan güvenlik duvarları paketleri uygulama katmanı seviyesinde inceleyebildiği için normal güvenlik duvarlarına göre daha üst seviyede güvenlik sağlamaktadır.

Uygulama Seviyesi Ağ Geçidi (Proxy)

- Dışarıdan ağa gelen saldırıların çoğu belli uygulamaların verileri içerisinde gelebilmektedir.
- İçerik kontrolcüsü, verilerin içerisinde gelen bu zararlı içerikleri tespit ederek bu içeriklerin ağa girmesini engellemektedir.
- Zararlı içeriklerin engellenmesi yanında gelen verilerin içerisinde belli başlıkları, belli kelimeleri veya konuları tespit ederek bu tür verilerin ağa girmesini de engelleyebilmektedir. Bu verileri filtreleme işlemini doğal olarak belli protokoller için yapmaktadır. Bu protokoller HTTP, FTP, SMTP ve POP3 olabilir.
- İçerik kontrolcüsü ağ tabanlı ya da sunucu tabanlı olabilir. Ağ tabanlı olanlar genellikle donanım tabanlıdır. Sunucu tabanlı olanlar ise yazılım tabanlıdır.

Uygulama Seviyesi Ağ Geçidi (Proxy)

- **Proxy**, (vekil sunucu), internete erişim sırasında kullanılan bir ara sunucudur. Bu durumda, örneğin bir ağ sayfasına erişim sırasında doğrudan bağlantı yerine: Tarayıcı vekil sunucuya bağlanır ve hangi sayfayı istediğini söyler. Vekil sunucu gerekiyorsa o sayfaya bağlanır ve içeriği alır.



İçerik kontrolcüsünün iletişim altyapısı güvenliğindeki yeri

Uygulama Seviyesi Ağ Geçidi (Proxy)

- İç ağdaki bir istemci dış ağdaki bir web sunucuya erişmek istemektedir. Bu amaçla istemci tarafından istek paketi oluşturulup güvenlik duvarına gönderilir.
- Güvenlik duvarı öncelikle bu isteğe izin verilip verilmeyeceğine karar verir. Bunun için erişilmeye çalışılan web sayfasının URL'sinin izin verilen URL'ler listesinde olup olmadığına bakar. Eğer sonuç olumlu ise, yani erişilmeye çalışılan URL'ye izin varsa, söz konusu istek güvenlik duvarı tarafından yeniden oluşturulup web sunucuya iletilir.
- Web sunucudan gelen cevap paketi tekrar güvenlik duvarına gelir. Güvenlik duvarı öncelikle gelen paketin içeriğinin zararlı olup olmadığını kontrol eder. Bunun için gelen paketin içerik denetimi yapılır. Zararlı bir içeriğe rastlanmadığı takdirde gelen cevap paketi güvenlik duvarında yeniden oluşturulup istemci bilgisayara gönderilir.
- Aksi takdirde, eğer gelen paket zararlı içeriğe sahipse, güvenlik duvarı tarafından düşürülür. Tanımlanmamış zararlı içerikler tespit edilemez ve bu nedenle durdurulamaz

Uygulama Seviyesi Ağ Geçidi (Proxy)- SOCKS Proxy

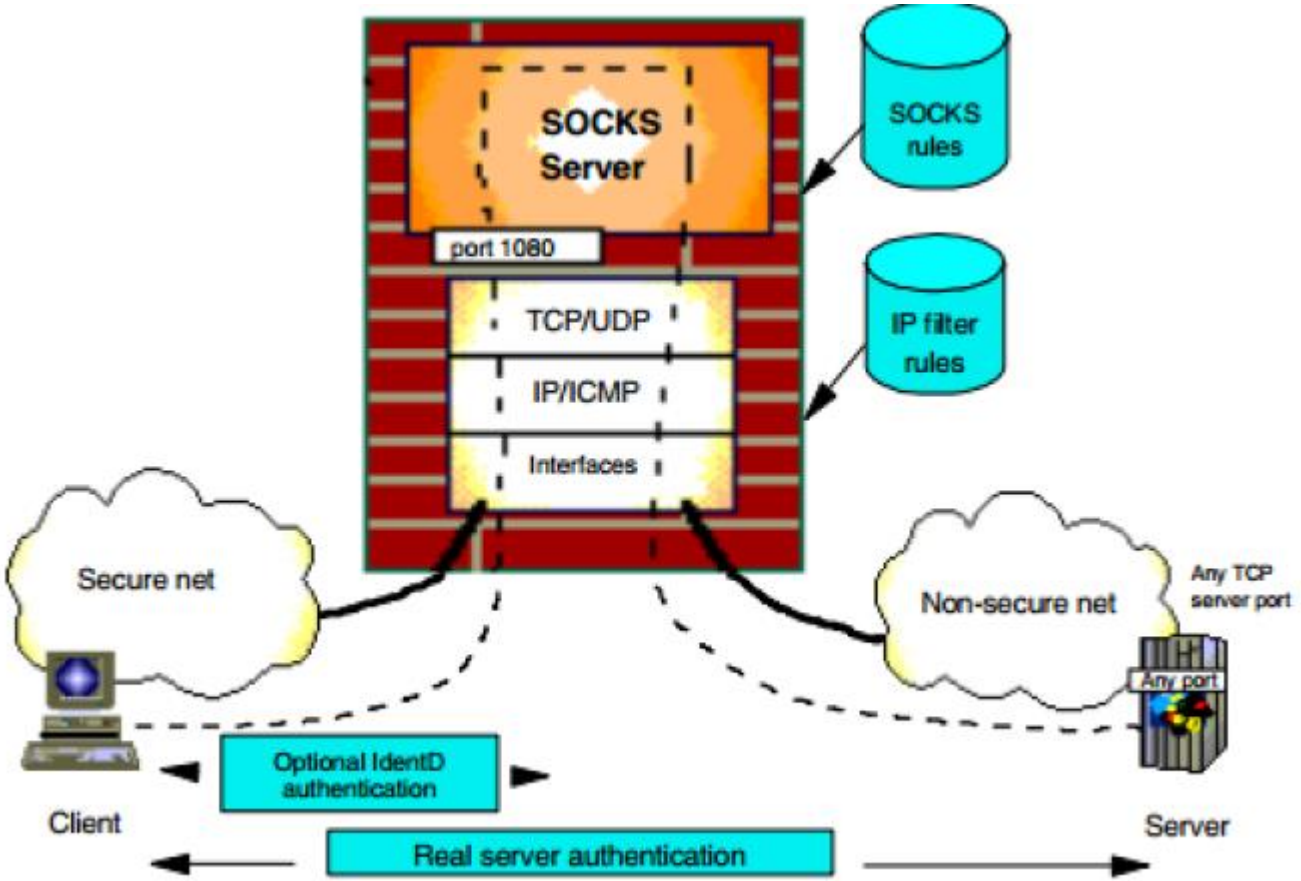
- SOCKS, OSI modelinin 5. katmanında çalışır. Devre seviyesindeki ağ geçitleri için bir standart olup geleneksel Proxy sunucular gibi ekstra başlık gerektirmez.

- Kullanıcı doğrudan hedef sunucu ile oturum kurmak yerine öncelikle SOCKS sunucu ile oturum başlatır.

- SOCKS sunucu kaynak adresi ve kullanıcı kimliğini doğruladıktan sonra hedef sunucuya bağlantı kurulmasına izin vererek ikinci bir oturum başlatır.

- RFC 1928'te belirtildiği şekli ile SOCKSv5; kullanıcı adı/parola doğrulaması, OTP (One time password) üreteçleri, Kerbereos, RADIUS ve IPSec kimlik doğrulama gibi farklı kimlik doğrulama mekanizmalarını desteklemektedir.

Uygulama Seviyesi Ağ Geçidi (Proxy)- SOCKS Proxy



SOCKS vekil sunucusu

Uygulama Seviyesi Ağ Geçidi (Proxy)-SOCKS Proxy

- Örneğin istemci bilgisayarlarındaki yönlendirme bilgileri tamamen kaldırılıp sadece vekil sunucunun dış dünyaya erişimine izin verilebilir. Böylece iç ağdaki bir istemcinin dış ağa erişmesi için mutlaka vekil sunucu üzerinden geçmesi gerekecektir.

- Bu durumda iç ağdaki bir istemci bilgisayar ele geçirilse bile dış dünyaya doğrudan erişim yapamayacaktır.

- Ayrıca vekil sunucu üzerinde kimlik doğrulama yapılarak güvenlik daha da arttırılabilir.

- Bununla birlikte vekil sunucuya yönlendirilen ağ trafiği şifrelenerek yerel ağda yapılabilecek ağ dinleme saldırılarına karşı önlem alınabilir.

IDS/IPS (Intrusion Detection/Prevention System)

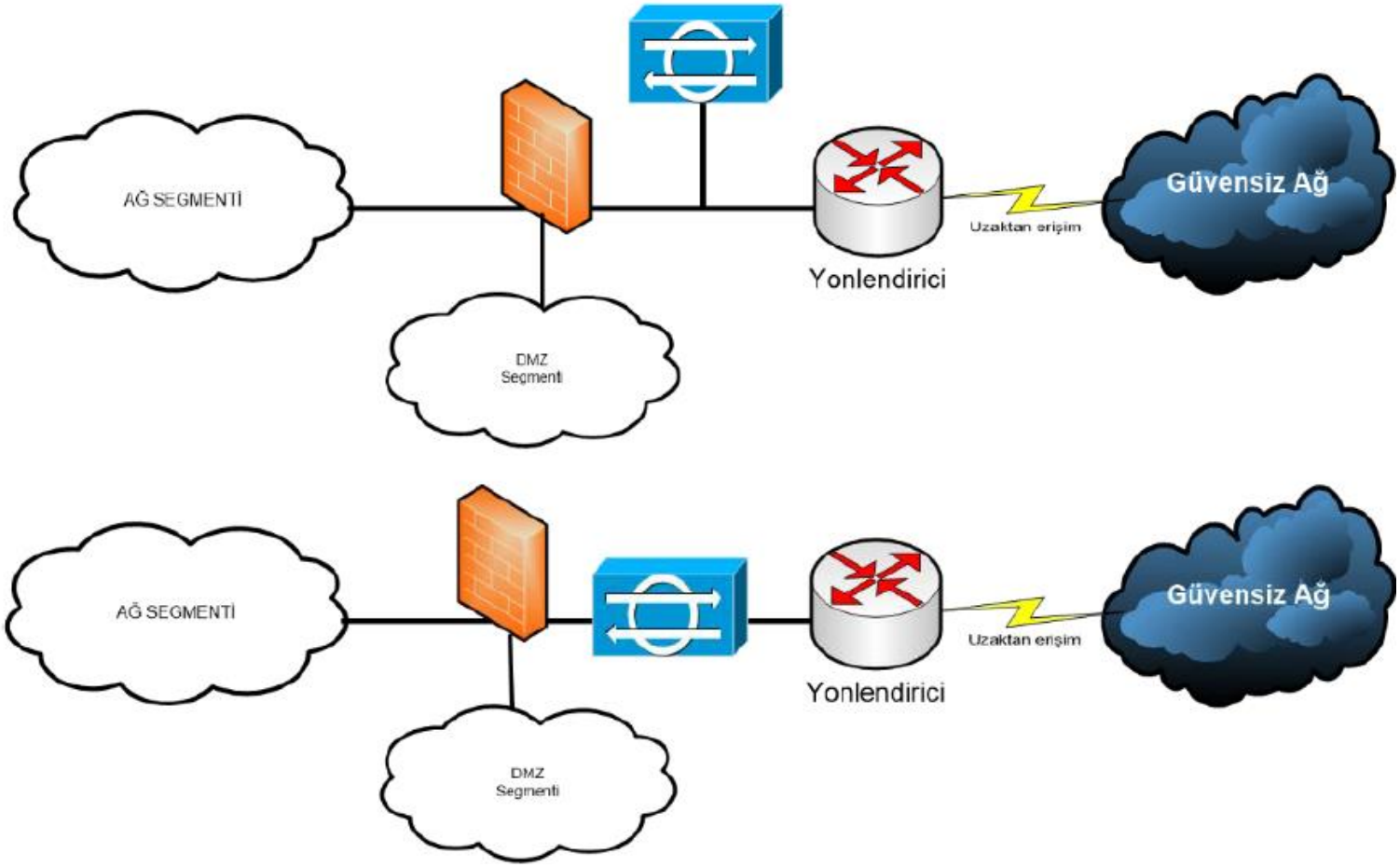
- Saldırı tespit sistemlerinin temel amacı ağa yapılan saldırıları tespit edip kayıt altına almak ve sistem yöneticisine gerekli uyarılarda bulunarak saldırıya karşı zamanında gerekli önlemlerin alınmasını sağlamaktır. Bu uyarma mekanizması olay kayıtları tutma, e-posta gönderme, çağrı bırakma, belli programları çalıştırma veya diğer şekillerde olabilir.

- Saldırı engelleme sistemi ise saldırıları tespit etme yanında bu saldırıların durdurulmasını da sağlayarak saldırının ağ sistemini etkilemesini engellemektedir. Saldırı tespit/engelleme sistemleri hem yazılım hem de donanım tabanlı olabilir.

IDS/IPS (Intrusion Detection/Prevention System)

- Ağa yapılan saldırıların anlaşılabilmesi için saldırı tespit sistemi, yönlendirici ve güvenlik duvarı arasında konumlandırılır.
- Yönlendirici ve güvenlik duvarı arasındaki bağlantı iki şekilde yapılabilir. Birincisinde güvenlik duvarı ile yönlendirici arasına bir HUB yerleştirilir ve STS de bu HUB'a bağlanır.
- HUB, herhangi bir portuna gelen bilgiyi diğer portlarına genel yayınla gönderdiği için STS ağa giren ve ağdan çıkan tüm bilgileri dinleyebilir.
- İkincisinde ise araya bir anahtarlama cihazı yerleştirilir. Yönlendirici, güvenlik duvarı ve STS bu anahtara bağlanır.

IDS/IPS (Intrusion Detection/Prevention System)



STS'nin İletişim Altyapısı Güvenliğindeki Yeri

IDS/IPS (Intrusion Detection/Prevention System)

- Yönlendiriciden güvenlik duvarına bilgi aktaran port STS'ye aynalanır (mirroring). Bu şekilde yönlendiriciden çıkan tüm bilgiler STS'ye gönderilmiş olur. STS de gelen paketleri inceleyerek bir saldırı varsa gerekli uyarıları yapar.

- Sunucular üzerine kurulmuş olan saldırı tespit sistemi ise sadece o sunucuya yapılan saldırıları algılar ve gerekli uyarı mesajlarını oluşturur.

- **Inline Mode:** Bu mimari daha çok saldırı engelleme sistemleri için uygulanır. Saldırı engelleme sistemleri köprü (*bridge*) modunda çalışır. Saldırı tespit/engelleme sistemi kendisine gelen paketleri inceleyerek saldırı varsa tespit eder ve gerekli uyarıları verir. Bu tür çalışan cihazların önemli bir özelliği herhangi bir şekilde elektrik kesilmesi ya da arızalanması durumunda girişini ve çıkışını kısa devre ederek ağın iletişimini durdurmamasıdır. Bu yapı daha çok saldırı engelleme cihazlarında görülür.

IDS/IPS (Intrusion Detection/Prevention System)-Snort

- Snort, hem imza tabanlı hem de protokol anormalliğini kontrol ederek çalışabilen açık kaynak kodlu olarak geliştirilen bir tehdit gözetleme sistemi yazılımıdır. Snort, imza tabanlı çalışma sisteminde daha önceden belirlenen imza kurallarının eşleşmesini temel alarak, protokol anormalliği çalışma sisteminde ise ağ trafiğinin gözlemlenmesi ve buna göre anormallik durumunun ortaya çıkartılmasını temel alarak çalışmaktadır.

- Snort açık kaynak kod dünyasında en çok tercih edilen tehdit gözetleme sistemi olarak göze çarpmaktadır. Tehdit gözetleme sisteminin yanı sıra ağ trafiğini monitör etmek için paket dinleyici modunda da çalışabilmektedir. Her ne kadar wireshark, tcpdump gibi paket dinleyiciler popüler olsalar da Snort'da bir iyi bir alternatif olarak bu işi üstlenebilmektedir.

- Nmap ile gerçekleştirilebilecek bir SYN taramasını önleyebilecek örnek bir Snort kuralı aşağıdaki gibidir.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN synscan portscan"; id:
39426; flags: SF;reference:arachnids,441; classtype:attempted-recon; sid:630; rev:1
```

Suricata

- Suricata açık kaynak kodlu olarak geliştirilen gelişmiş bir tehdit gözetleme sistemi uygulamasıdır. Göze çarpan özellikleri olarak;
  - Yüksek Uygulanabilirlik: Suricata birden fazla kopyasını (thread) çıkartarak çalışabilmektedir. Bu şekilde dağıtık yapıda yük dağıtma özelliği ile oldukça efektif olarak çalışabilecektir.
  - Protokol Tanımlama: Yaygın olarak kullanılan birçok protokol veri akışı gözlemlenmeye başladığında Suricata tarafından tanımlanabilecektir. Özellikle bu özelliği ile kötücül yazılım tanımlama işleminde oldukça kolaylık sağlamaktadır.
  - Dosya Tanımlama, MD5 Kontrolü ve Dosya Çıkartımı: Bu özelliği ile ağ üzerinden akış sağlanan dosya türlerinin birçoğu Suricata tarafından tanımlanabilecek ayrıca önceden tanımlanmış md5 değerleri de anlık olarak tespit edilen dosyalar için kontrol edilebilecektir.