YÖNLENDİRİCİ GÜVENLİĞİ

Sedat Kulduk, Enis Karaarslan,
kulduk@bornova.ege.edu.tr, enis@bornova.ege.edu.tr
Ege Üniversitesi Kampüs Network Güvenlik Grubu

ÖZET

Bu bildiride, bilgisayar ağlarının kısa tanımından başlayarak, bu ağlar içinde yönlendiricide (router) alınması gereken güvenlik önlemlerinden bahsedilmiş, ayrıca yönlendirici ile yapılabilecek ağ güvenliğine değinilerek önemli ipuçları verilmiştir. Bu cihazın güvenliği, kurumun dış bağlantılarının (internet) etkinliği için kritik önem taşımaktadır.

Anahtar Kelimeler: yönlendirici güvenliği, ağ güvenliği, erişim listesi (access list), snmp, rat

GİRİŞ

Günümüzde bilgisayar ağları denince iki veya daha fazla bilgisayarın bilgi ve kaynak paylaşımı için belirli protokollere uygun olarak, kablolu veya kablosuz, birbiriyle haberleşmesi akla gelmektedir. İki bilgisayar aralarında veri transfer ederken bazı temel protokollere göre bu transferi gerçekleştirmek zorundadırlar. OSI modeline göre veri, Uygulama seviyesinden Fiziksel seviye kadar inip daha sonra elektriksel sinyal olarak yoluna devam etmektedir. Fakat bu yolculuk sırasında sinyaller direkt olarak kaynak (source) bilgisayardan hedef (destination) bilgisayara doğru değildir. Arada bu sinyalleri gidecekleri yerlere yönlendiren cihazlar vardır. Bu cihazlar yerel ağlarda switch, hub gibi cihazlarken; geniş alan ağlarında (WAN) yönlendirici (router) cihazları kullanılmaktadır. Yönlendiricilerin görevi, yerel ağdan gelen paketleri filitrelemek ve paketlerin nereye gideceğine karar vermektir. Böylece yerel ağları birbirine bağladığı gibi kurumun WAN'a bağlantı noktasını da oluşturmakta ve internet erişimini de sağlamaktadır. Yönlendiricinin temel parçaları aşağıdaki gibidir:

- İşlemci: Yönlendiricinin ana beynidir. RISC işlemci(ler)den oluşur.
- Anakart: Anakart, yönlendirici elemanlarını birbirine bağlayan ana birimdir. Üzerinde uygulamaya özgü geliştirilmiş özel devreler (ASIC) bulunmaktadır.
- Bellek: Kullanılan bellekler işlevlerine göre farklı birimler olarak bulunmaktadır. Bunlar aşağıdaki gibidir:
    - Flash: Kalıcı hafıza birimidir. Her yönlendirici belirli bir İşletim Sistemine (Operating System) ihtiyaç duyar. İşletim sistemi imgeleri (image) ise Flash bölgesinde tutulur. İstenildiği taktirde ve donanım elverdiği sürece daha yeni versiyonu ile değiştirilebilir.
    - NVRAM: Kalıcı hafıza birimidir. Burada başlangıç (startup) ve yedek(backup) konfigürasyon dosyaları tutulur. Elektrik kesilse bile bu bilgiler bu bölgede kalmaktadır.
    - (Boot)ROM: Fiziksel olarak sinyal yollayıp donanımları test eden ve cihazı başlatmaya yarayan program olan Bootstrap'ı içerir. Eğer ki bu program değiştirilmek istenirse, rom çipi yenisiyle değiştirilmek zorundadır.
    - DRAM/SRAM (Memory): Cihazın aktif bilgilerinin tutulduğu geçici hafıza birimidir. Cihaz açılırken bootstrap flash'tan işletim sistemi imgelerini ve nvram'den başlangıç konfigürasyonunu ram bölgesine yükler. Çalışan

konfigürasyon (running config) bu bölgede tutulur. Ayrıca bu bölgede routing tablolarını ve gelen henüz iletilmemiş verileri de tutmaktadır (buffering).

- I/0 Interface (Arayüz): Her yönlendiricinin kendisine gelen bilgileri alması, göndermesi ve konfigürasyonunun yapılması için kullanılan bağlantı noktalarına arayüz (interface) denir (Örneğin ethernet 0, consol). Arayüz her zaman fiziksel bir olgu değildir. Bir fiziksel arayüz, birden fazla sanal alt arayüz olarak da kullanılabilir.

Yönlendiricinin görevleri aşağıdaki gibi sınıflandırılabilir:

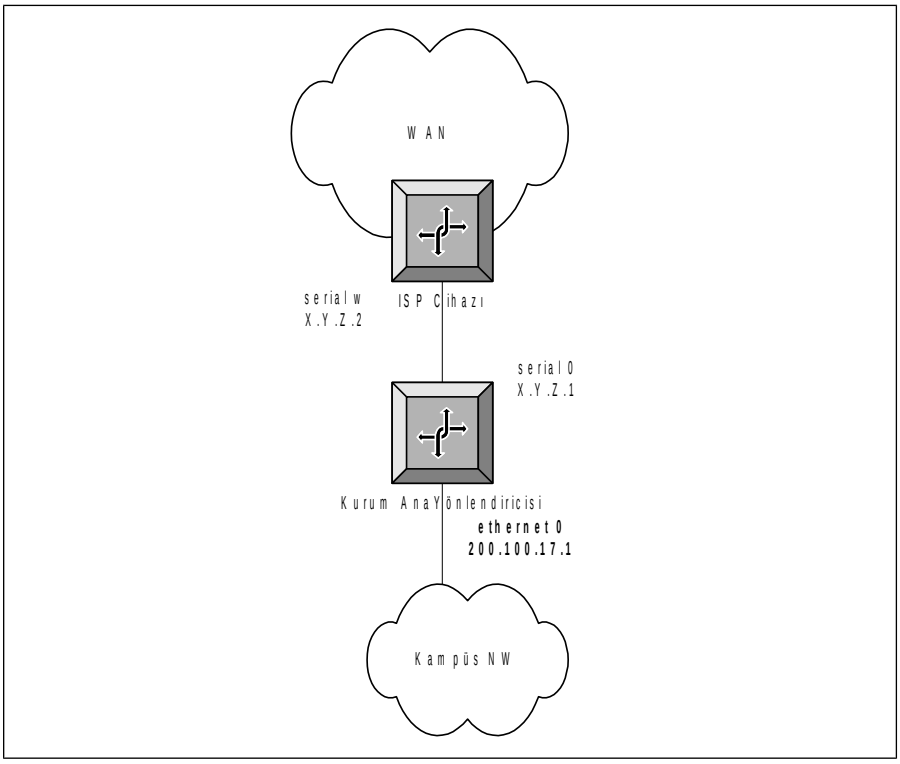
- Yol Seçmek(Routing): Yönlendirici, kendine bağlı olan bilgisayarların network adreslerini tuttuğu gibi, kendisine bağlı veya kullanılan protokole göre bağımsız yönlendiricilerin network adreslerini de routing tablolarında tutmaktadır. Yönlendirici kendisine gelen paketlerin nereye gideceğini öğrendikten sonra bu adresi routing tablolarıyla karşılaştırarak hangi port'undan yollayacağına karar vermektedir.
- Paket Filitreleme: Paket filtreleme, network adresi(IP), servisi ve protokolüne göre bilgi transferini kontrol etmektir. Yönlendirici bu kontrolleri ACL'ler (Access-Control List – Erişim Listesi) yardımı ile sağlar. ACL'ler kendisine gelen verinin kaynak, hedef ip adreslerine, bilginin gideceği port adresine veya kullanılmak istenen protokole göre kısıtlamalar yapabilmektedir. Bu kısıtlamalar yapılırken iki şekilde yapılabilir. Birincisi sadece izin verilen servisler ve protokoller yazılarak servise açılmakta ve geri kalanı kapatılmaktadır. İkincisinde ise sadece kapatılan servisler yazılmakta ve diğerleri açılmaktadır. ACL yazarken komutların yukarıdan aşağıya doğru işleneceği ve gelen paketin yazdığımız herhangi bir kuralla takıldığı anda işlemin bitirilip alttaki kurallara bakılmayacağıda akıldan çıkartılmamalıdır [1] [2] [3]. Aşağıdaki ACL'de bütün bilgisayarlara 80. port (http) erişimi serbest bırakılmış ve diğer bütün servisler kısıtlanmıştır.

```
access-list 101 permit ip any any eq 80
access-list 101 deny any any
```

  Erişim listeleri, yönlendiricinin belirli bir arayüze uygulanmadan aktif olmazlar. Erişim listeleri uygulandıkları yön açısından iki türlü olmaktadır. Arayüzün içten gelen trafiğine ("in" - inbound) ya da dıştan gelen trafiğine ("out" - outbound) uygulanabilir. Örneğin aşağıdaki örnekte 101 numaralı erişim listesi, "ethernet 0" arayüzünün inbound'una uygulanmıştır.

```
Interface ethernet 0
      access-group 101 in
```

Dökümanda örneklerin üzerinde uygulanacağı kurum ağının bir C sınıfı IP adres alanına (200.100.17.0\24) sahip olduğu varsayılacak ve örnekler buna göre verilecektir. Şekil 1'de de görüldüğü üzere, kurum ağı "ethernet 0" arayüzü ile kurumun yerel ağına, "serial 0" arayüzü ile de genel ağa (WAN) bağlıdır.



Şekil 1: Kurum Ağ Şeması

Yönlendirici güvenliği dört ana başlıkta işlenecektir:

1. Yönlendirici Cihazının Güvenliği
2. Yönlendirici Cihazla Ağ Güvenliği
3. Sistemi Takip Etmek
4. Sistemde Güvenlik Testleri Uygulamak

Türkiye'de özellikle kurumsal bağlantılarda Cisco marka yönlendiriciler kullanıldığı için uygulamalar Cisco marka cihazlar üzerinde gösterilmiştir. Diğer firmaların ürünlerinde de benzer prensipler geçerlidir, sadece bazı komutlarda yazım farklılıkları bulunmaktadır.

YÖNLENDİRİCİ CİHAZININ GÜVENLİĞİ

Router'in, ağa bağlı bir cihaz olarak kendisinin güvenliğinin sağlanması gerekmektedir.
Yönlendirici cihazının güvenliği şu alt başlıklarda işlenebilir:
1. Fiziksel Güvenlik
2.Yönlendiriciye Erişim Hakları
3.Şifrelerin Güvenliği,
4.Erişim Protokolleri Güvenliği
5.İşletim Sistemi Güvenliği

1.Fiziksel Güvenlik

Fiziksel güvenliği saglamanın birkac yolu vardır. Bunlardan biri yönlendiricilerin bulunduğu odaların kapılarını kilitli tutarak yetkisiz kişilerin girişilerine izin vermemektir. Ayrıca bu odalarda cok fazla elektrik ve manyetik alan olmamasına; sıcaklık ve nemin de kontrol altında

tutulmasına özen gösterilmelidir. Yönlendiriciler için ayrı bir oda ayırılamıyorsa en azından kilitli dolaplar (kabinet) içine koyulmalıdır. İkincisi bu odaya gelen elektriğin hiç kesilmemesidir . Bu UPS (Uninterupted power supply) kullanarak sağlabilmektedir. Bir üçüncüsü; yönlendirici yakınlarına şifre veya ip bilgileri gibi bilgileri yazmaktan kaçınmaktır. [4]

2.Yönlendiriciye Erişim Hakları

Yönlendiriciye kimlerin erişeceğinin bir politikayla belirlenmesi ve erişimlerin loglanması gerekmektedir. Bu politikada; kimin konfigürasyon yedeklerini alacağının, kimin yeni bir parça alımında yönlendiriciye yerleştireceğinin, kimin logları düzenli takip edileceğinin açık bir şekilde belirtilmesi gerekmektedir. [5]

Temelde yönlendiricilere, kullanıcı (user) ve yönetici (enable) olarak iki çeşit erişim hakkı vardır. Kullanıcı modunda sadece kontroller yapılabilirken, yönetici modda ek olarak cihaz konfigürasyonu da yapılabilmektedir. Bu iki erişim hakkı, 15 seviyeli erişim mekanizmasıyla desteklenmiştir ve varsayılan (default) olarak üç adet erişim seviyesi vardır. Seviye 0'da sadece *disable*, *enable* ,*help* ,*logout* komutlarını; seviye 1'de kullanıcı modundaki komutları (router>); seviye 15'de exec modu (router#) diye tabir ettiğimiz yönetici komutlarını kullanma hakkına sahiptirler [6]. Bu erişim seviyeleri, kişiler ve komutlar bazında yöneticinin isteğine göre ayarlanabilir. Mesela yönetici kullanıcının *ping* komutunu kullanmasını fakat `snmp-server community` komutunu kullanmamasını isterse buna göre ayarlama yapabilmektedir. Bu seviyeler yönlendiricide komut bazında veya TACACS+, RADIUS doğrulama(authentication) sunucuları bazında ayarlanabilmektedir. Ayrıntı için bakınız [7].

3.Şifrelerin Güvenliği

Günümüzde büyük oranda kırma(hacking) işlemi "password quessing" (parola tahmin etme) yöntemiyle yapılmaktadır bu sebepten şifre seçimine gerektiği önem verilmelidir. [4]

Cisco yönlendiricilerde kullanıcı adı ve parolasının konfigürasyon dosyasında gözükmemesi için "*service password-encription*" komutu kullanılmalı. Zayıf şifreleme algoritması kullanan "*enable password*" kaldırılmalı, MD5-tabanlı algoritmayla şifreyi koruyan "*enable secret*" komutu kullanılmalıdır. "*no enable pass*word" komutu kullanılarak enable password'ler silinmeli yerine "*enable secret yeni_şifreniz*" ile yeniden şifreler girilmelidir [4].

4.Erişim Protokollerinin Güvenliği

Yönlendiricilere fiziksel erişim konsol portundan yapılmaktadır. Bunun için fiziksel güvenliğin sağlanması gerekmektedir. Diğer erişim yöntemleri olan HTTP, Telnet, SSH, TFTP, ve FTP kullanıldığında TCP/IP protokolünün zayıflıklarına karşı önlem alınması gerekmektedir. Alınması gereken önlemler aşağıdaki gibidir.

Belirli IP'lerin Cihaza Erişimine İzin Vermek:
Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu da erişim listesi (access-list) yazılarak sağlanır. Örneğin Cisco IOS'de sadece 200.100.17.2 ve 200.100.17.3 IP'lerin erişimine izin verilmesi ve diğer ip'lerin engellenmesi ve bu erişimlerin kaydının tutulması aşağıdaki erişim listesi ile sağlanmaktadır

```
access-list 7 permit 200.100.17.2
access-list 7 permit 200.100.17.3
access-list 7 deny any log
```

Örnekte verilen 7 numaralı erişim listesinin devreye girmesi için erişimin geleceği arayüzlerde etkin hale getirilmesi gerekmektedir. Telnet (veya ssh) için uygulanması da aşağıdaki gibi olmaktadır[8]:

```
line vty 0 4
access-class 7 in
```

Http erişimi için kısıtlanması da aşağıdaki gibi olmaktadır:

```
ip http access-class 7
```

SNMP erişimine belirtilen IP'lerin izin verilmesi ise aşağıdaki gibi olmaktadır:

```
snmp-server host 200.100.17.2 snmp_şifresi
snmp-server host 200.100.17.3 snmp_şifresi
```

HTTP Erişimi:

HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir. Daha önceden de belirtildiği gibi HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IP'lere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir. Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin *"ip http server port 500"* komutuyla 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

Şifrenin Ağda Düz Metin Olarak İletilmesini Engellemek:

HTTP, Telnet, SNMP protokolleri ile cihaza erişimde, doğrulama mekanizması ağda şifrenin düz metin (clear text) şeklinde gönderimi ile sağlandığı için güvenlik açığı oluşmaktadır. Özellikle hub bulunan ortamlarda saldırganın ağ üzerinden dinleme (sniff) yoluyla iletilen bilgiyi elde etmesi mümkün olabilmektedir. Bunu engellemek için aşağıdaki önlemler alınabilir :

- Konsol Kablosunu Yönetim Bilgisayarına Çekmek: Eğer cihaz tek bir makinadan yönetiliyorsa, o makinanın com portundaki arabirime çekilen bir utp kablo ile konsol erişimi sağlanabilir. Böylece erişim tek bir kablo üzerinden sağlanacaktır.
- Telnet yerine Secure Shell (SSH) Erişimi Vermek: İletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmalıdır. SSH'i desteklemek için cihazın işletim sisteminin güncellenmesi gerekebilmektedir. SSH, şu anda bütün cihazlar ve cihaz işletim sistemleri tarafından desteklenmemektedir. Bu konuda üretici firmanın cihaz dökümantasyonu incelenmelidir.
- Güncel SNMP Versiyonlarını Kullanmak: SNMP Versiyon 1, düz metin doğrulama dizileri (string) kullandığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz (*digest*) doğrulama şeması kullanan ve çeşitli yönetim verilerine kısıtlı erişim sağlayan SNMP Versiyon 2 veya 3'ün kullanılması gerekmektedir. Mümkünse her cihaz için ayrı bir MD5 gizli (*secret*) değeri kullanılmalıdır.
- Hub olan ortamlardan cihaza erişim yapmamak: Hub olan ortamlardan yönlendiriciye erişim yapılmamalıdır. Böyle erişimin zorunlu olduğu durumlarda ssh'i destekleyen bir linux/unix sunucuya bağlanarak onun üzerinden yönlendiriciye telnet erişimi yapılmalıdır.
- Doğrulama Mekanizmaları Sağlamak : HTTP protokolünde doğrulama mekanizması ağda şifrenin düz metin şeklinde gönderimi ile sağlandığı için efektif değildir ama farklı üreticilerin değişik çözümleri bulunmaktadır. Doğrulama mekanizması, onay sunucuları (Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması "*ip http authentication*" komutuyla sağlanmaktadır.

Acil Durum Erişimini Ayarlamak:
Yönlendiricilere erişimin sağlanamadığı acil durumlarda telefon hatları üzerinden modem kullanılarak erişmek için "Auxiliary port" bulunmaktadır. Bu tür bir erişim için PPP (Point to Point Protocol) üzerinde PAP (Password Authentication Protocol) yerine CHAP (Challenge Handshake Authentication Protocol) doğrulama methodu kullanılmalıdır. CHAP, dial-up ve uçtan uca (point to point) bağlantılarda uç noktayı engelleyerek izinsiz erişimleri engellemektedir.

Bütün bu önlemlere karşı saldırganlar yönlendiriciyi ele geçirebilmektedir. Bu sebeble en azından yönlendirici açılışına yasal haklarla erişebilinecek bir cihaza erişildiğini izinsiz erişimlere kanuni işlem yapılacağını belirten yazı yazılmalıdır. Cihaza erişim yapıldığında bir uyarı gözükmesi için, "*banner motd*" komutu kullanılmaktadır. Örneğin aşağıdaki şekilde bir uyarı cihaza eklenebilir:

```
---------------------------------------------------------------------
Bu cihaza yetkisiz erisim yasaktir. Erisim bilgileriniz kayitlanmistir.
Unauthorized access to this device is prohibited. All access has been
logged.
---------------------------------------------------------------------
```

5.İşletim Sistemi

Yönlendirici için işletim sistemi (Operating System) seçilirken ağın ihtiyaclarına uygun ve aynı zamanda donanımın desteklediği bir versiyon olmasına dikkat edilmelidir. Her ne kadar işletim sistemleri güvenlik testlerine tabi tutulup daha sonra piyasaya sürülüyorsa da daha sonradan güvenlik açıkları bulunabilmektedir. Bu nedenden dolayı çıkan yamaları takip edip upgrade yapmak gerekebilmektedir. Şuda unutulmamalıdır ki; işletim sisteminin en son versiyonu her zaman en iyi versiyon olmayabilmektedir. Bu nedenlerden dolayı, düzgün calıştıgı denenmiş en son versiyon tercih edilmeli ve kesinlikle eski versiyon yedeklenmelidir. [14]

Cisco yönlendirici cihazlarının IOS larının güvenliği için [15] referansından ayrıntılı olarak yararlanabilirsiniz. Eğer başka marka yönlendirici kullanıyorsanız en son işletim versiyonlarını üretici sitelerinden bulabilirsiniz.

AĞI YÖNLENDİRİCİLERLE KORUMAK

Bu bölümde yönlendirici ile ağdaki bilgisayarlara gelebilecek saldırıların engellenmesi için ipuçları verilecektir.

1. Riskli portları kapatmak:

İnternet üzerindeki servisler, kullanıcılara hizmet götürebilmek için bazı sanal port numaraları kullanırlar (örn: http için 80 numaralı port kullanılmaktadır). Saldırganlar veya kötü yazılımlar servislerin açıklarını kullanarak hizmet verilen port numarası üzerinden bilgisayar ağına sızabilirler. Bunu önlemenin bir yolu riskli portları yönlendirici ile kısıtlamaktır. Riskli portların listesi [17] nolu referansının 38 ve 39 sayfalarında listelenmiştir. Bu liste, ağ yöneticisi tarafından çeşitli güvenlik sitelerini takip ederek sürekli olarak güncellenmelidir. Aşağıdaki örnekte 445 nolu UDP portu ile finger servisi bloklanmaktadır:

```
access-list 101 deny udp any any eq 445
```

```
access-list 101 deny tcp any any eq finger
access-list 101 permit ip any any
```

Yönlendiriciye fazla yük getirmediği sürece bu erişim listesini genişletmek mümkündür. Tanımlı mail ve web sunucularını belirlemek ve bu sunucular dışında bu tür protokolleri engellemek de mümkündür. Erişim listesi ne kadar kapsamlı olursa o kadar fazla işlemci gücü gerektirecek ve performans azalacaktır. O yüzden sık gelen paket türlerini erişim listesinde daha önde tutmak performansı arttıracaktır.

2.Bazı saldırı tekniklerine karşı önlemler

IP spoofing : IP kandırmacası anlamına gelmektedir. Kötü niyeli kişi hattı dinler giden paketlerin kaynak ve hedef adresini alır. Hedef adresini kendi ip'si yaparak kaynak adrese cevap verir. Böylece erişim listesine takılmadan bilgisayar ağına sızmış olur. Bunu önlemenin yolu, yönlendiricinin kaynak adresi hedef makinaya varmadan kimseye göstermemesidir. Cisco cihazlarda "*No ip source route*" komutuyla yapılabilmektedir [18].

Routing Protokole olan saldırılar: Bilindiği üzere yönlendiriciler kendi aralarında interior veya exterior routing protokollere göre haberleşmektedirler [8][19]. Saldırgan yönlendiricinin routing protokolünü bozmadan yollanan paketlerin bir kopyasının kendine de yollanmasını sağlayabilir(kredi kart numaraları gibi verileri almak için) veya protokolleri kaldırarak yönlendiricinin diğer yönlendiricilerle haberleşmesini kesebilir. Haberleşmenin yok olması, yönlendiricinin aldığı paketleri nereye göndereceğini bilmemesi ve servis dışı kalması(DoS) anlamını taşımaktadır. Bunu önlemenin yolu ise gönderilen ve alınan routing protokolu paketlerini de filitrelemektir. Örneğin IGRP routing protokolünü filitrelemek için yazılmış ACL aşağıda verilmiştir.

```
router eigrp
network 200.100.17.0
distribute list 20 out ethernet 0
distance 255
distance 90 200.100.17.0 0.0.0.255

access-list 20 permit 200.100.17.0 0.0.0.255
```

Çıkış (Egress) ve Giriş (Ingress) Erişim Listeleri

Bu erişim listeleriyle yönlendiriciye gelen paketlerdeki kaynak IP adresleri kontrol edilmektedir.

Dış ağdan iç ağa gelen paketlerde, gelen ip'lerin kontrolüne giriş (ingress) filtreleme denmektedir. Ağ adresimiz 200.100.17.0/24 ise, dış dünyadan böyle bir IP aralığına ait bir paket gelmemesi gerekmektedir. O zaman ingress kısıtlamaları aşagıdaki gibi olacaktır.

```
access-list 102 deny ip 200.100.17.0 0.0.0.255 any
access-list 102 permit ip any any
```

İç ağdan dış ağa giden paketlerde, gelen ip'lerin kontrolüne çıkış (egress) filtreleme denmektedir. Kendi ağ ip adresi aralığında olmayıp da internete çıkmak isteyen "ip"ler kısıtlanmalıdır [17]. Bu kontrolde gelen paketlerdeki ip'lerde internet ortamında

kullanılmayan (rezerve edilmiş) adresler bulunduğunda bu paketler kabul edilmeyecektir[20]. Bazı reserve edilmiş IP lerin kısıtlanması aşağıdaki gibidir:

```
access-list 101 deny ip 10.0.0.0  0.255.255.255 any
access-list 101 deny ip 191.255.0.0 0.0.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 223.0.0.0 0.255.255.255 any
access-list 101 permit ip any any
```

Bu erişim listesi yönlendiricinin Ethernet arayüzünün içerden gelen trafiğine veya serial arayüzünün dışardan gelen trafiğine uygulanabilir. Örnekte dışardan gelen

```
interface serial 0
ip access-group 101 out
```

Egress ise:

```
interface ethernet 0
ip access-group 102 in
```

“Reverse Path” Kontrolü: Gönderdiğimiz paket “ethernet 0” arayüzünden gönderiliyor fakat cevabı “ethernet 1”den geliyorsa bu işte bir yanlışlık var demektir. Bu önlemek için geliş gidiş istatiğini tutan CEF routing tablolarından yararlanmak gerekmektedir. Bu sağlamak için de seri arayüzde bu komutun uygulanması gerekmektedir.[21]

```
İp cef disributed
!
interface serial 0
      ip verify unicast reverse-path
```

“CAR Rate”i Güvenlik için Kısıtlamak: Bir çeşit QOS(“Quality of Service” – Servis Kalitesi) sağlayarak belli protoldeki verilerin belli ip adresleri veya mac adresleri için politikaya göre belirlenmiş belli oran ve miktarlarda kurumsal ağa gelmesini veya kurumsal ağdan gitmesini sağlayabiliriz [22]. Bu da bizim trafiğimizi boşu boşuna işgal eden ve kurumsal ağın yavaşlamasını sağlayan paketlerden kurtulmamızı sağlar. Mesela örnekte xy arayüzündeki TCP SYN paketlerini 8 Kbps’a indirmek gösterilmiştir.

```
interface xy
rate-limit output access-group 102 256000 8000 8000
      conform-action transmit exceed-action drop [ikisi bir satırda]
!
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

SYN saldırılarından korunmak: Eğer kötü kullanıcı belli bir sunucuya (server) belli sayıdan daha fazla bağlantı kurma isteğini gönderir fakat nerden bağlanmak istediğini göndermeyerek bağlantıları boşa açarsa buna “SYN flooding attack” denmektedir. Böylece o sunucunun iş görmesini engelliyerek servis dışı bırakmaktadır. Çözümü için [23] referansındaki adres incelenebilir.

Smurf attack: IP adresi kandırmacası ve broadcast (aynı subnetteki herkese yollama) ilkelerine dayanır. Saldırgan, saldırmayı hedeflediği bilgisayarın IP’sini kendi IP’si yapar ve bu IP’yle bir broadcast ping atar. Gönderilen ping paketlerinin cevabı gerçekte bu IP’ye sahip

olan bilgisayara gider ve orada gereksiz trafik yaratarak bilgisayarın internete ulaşması engellenir. Bu olayı yönlendiriciden önlemenin bir yolu router'daki arayüzlere "*no ip directed- broadcast*" komutunu girmektir.[24]

SİSTEMİ TAKİP ETMEK

Ağ cihazlarını takip etmek için kullanılan bir veya birden fazla bilgisayar olabilir. Bu bilgisayarlara Ağ Yönetim İstasyonu - Merkezi (AYM) denmektedir. AYM, ağdaki cihazlara ait SNMP şifre dizileri gibi doğrulama bilgileri ve saldırı girişimi kayıtlarını bulundurdukları için doğal bir saldırı hedefi durumuna gelmektedir. Bu yüzden bu makinaların fiziksel, yazılımsal ve ağ güvenlikleri sağlanmalıdır. Sistemi takip etme (monitor) aşağıdaki yöntemlerle gerçekleştirilebilir:

- Kayıtlama (logging)
- SNMP

Kayıtlama (Logging)

Ağ cihazları çeşitli hadiseler (*event*) hakkında kayıtlama özelliğine sahiptir. Bu kayıtlar, güvenlik hadiselerinin belirlenmesinden ve önlem alınmasında kritik önem taşıyabilmektedir. Arayüzlerin durum değişikliği, sistem konfigürasyon değişikliği, erişim listelerine takılan (*match*) bağlantılar gibi güvenlik açısından önemli olan bilgilerin kayıtı tutulabilmektedir. Cihazda kayıtlama aşağıdaki şekillerde yapılabilmektedir:

- SNMP Trap Logging: Sistem durumunda (*status*) karakteristik (*significant*) değişikliklerde Ağ Yönetim İstasyonuna uyarı (*notification*) göndermektedir. Bu işlem cisco cihazlarda aşagıdaki gibi yapılmaktadır. [9]

```
snmp-server community community_kelimesi ro 10
!
!  SNMP yi göreceklere izin verilir
access-list 10 permit host snmp_mgmt_ip
access-list 10 deny any
!
! "community" adlarıyla "trap"lar gönderilir.
snmp-server trap-authentication
! Bütün "trap"lar içerdeki arayüzde bulunan yönetim cihazına gönderilir.
snmp-server trap-source Ethernet0
snmp-server host snmp_mgmt_ip community_kelimesi
!
interface Ethernet0
 ip access-group e0-in in
!
ip access-list extended e0-in
! İçerdeki belirli bir makinanın erişimine izin verilir
permit udp host snmp_mgmt_ip host 200.100.17.2 eq snmp
```

- Sistem Kayıtlaması: Sistem konfigürasyonuna bağlı olarak hadiselerin kayıdını tutmaktadır. Sistem kayıtlaması farklı yerlere yapılabilmektedir [4]:
  - Sistem konsoluna bağlı ekrana "*logging console*" komutuyla,
  - Üzerinde UNIX'in syslog protokolü çalışan ağdaki bir sunucuya "*logging ip-address*", "*logging trap*" komutlarıyla,
    Ör: *logging 200.100.17.2*
  - Telnet veya benzeri protokolle açılan VTY remote oturumlara (session) "*logging monitor*", "*terminal monitor*" komutlarıyla,

- Yerel buffer olan RAM'ine "*logging buffered*" komutuyla yapılabilmektedir.

Kayıtlar düzenli olarak takip edilmeli ve sistemin düzgün çalışıp çalışmadığı kontrol edilmeldir. Farklı cihazlardan Ağ Yönetim İstasyonu'na gönderilen mesajların zamana göre senkronize olması için cihazlarda Network Time Protokol (NTP) çalıştırılmalıdır [10].

SNMP

Simple Network Management Protokol (SNMP), cihaz ve yönlendirici için vazgeçilmez bir protokoldür. Trafik istatistiklerinden bellek ve CPU kullanımına kadar bir cihaz hakkında çok detaylı bilgiler edinilebilmektedir.

Bir veya daha fazla AYM, üzerlerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan (server) bu istatistikleri toparlayacak (poll) şekilde ayarlanmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Router Traffic Grapher (MRTG) gibi programlar bulunmaktadır [11].

SNMP kullanılırken dikkat edilmesi gerekenler aşağıdaki gibi özetlenebilir:

- SNMP protokolünün, özellikle SNMP Version 1'in birçok uygulamasında zayıflık (vulnerability) olduğu CERT[1] 'in raporlarında belirtilmiştir[12] . Versiyon 2 veya 3'ün kullanılması önerilmektedir. Daha detaylı bilgi için [13] incelenebilir.
- Sadece Oku (*Read only*) ve Oku-Yaz (*Read-Write*) erişimleri için kullanılan varsayılan SNMP şifre (*community*) adları değiştirilmeli ve bu iki parametre birbirinden farklı olmalıdır.
- SNMP şifrelerine kritik bir UNIX makinasındaki root şifresi gibi davranılmaldır.
- SNMP erişimi hakkı sadece belirli güvenilir IP'lere sağlanmalıdır.
- AYM tarafından SNMP erişimi yapılırken "Sadece Oku" parametresi kullanılmalıdır. Mümkünse cihazlarda "Oku-Yaz" parametresi iptal edilmelidir.
- Ağ Yönetimi için yerel ağda ayrı bir alt ağ (subnet), mümkünse VLAN[2] yaratılmalıdır. Erişim listesi ve Ateş Duvarı (*firewall*) kullanılarak bu ağa dış ağlardan gelen trafik kısıtlanmalıdır.

SİSTEMDE GÜVENLİK TESTLERİ UYGULAMAK

Kurumun sisteminin ne kadar güvenli olup olmadığının test edilmesi gereklidir. Bunun için sistemde yapılan güvenlik geliştirmelerinin düzgün çalışıp çalışmadığını kontrol eden ve güvenlik açıklarını size belirten bazı araçlara gereksinim duyulmaktadır. Aşağıda bu araçların bazılarından kısaca bahsedilecektir:.

- RAT (Router Audit Tool): CIS (the Center for Internet Security) tarafından geliştirilmiş ve http://www.cisecurity.org/bench_cisco.html adresinden ücretsiz olarak temin edilebilen bir kontrol ve karşılaştırma (benchmark) aracıdır. Kullanılan Cisco marka yönlendiricinin işletim sistemi ve üzerindeki konfigürasyonunu çeşitli güvenlik özelliklerine göre karşılaştırmaya, eksik olan yanlarını bir rapor olarak düzeltebilmeye olanak sağlayan bir araçtır [16]. Web sitesindeki dökümanlarda kullanımı hakkında detaylı bilgi bulunmaktadır.

[1] CERT: Computer Emergency Response Team – http://www.cert.org

[2] VLAN: Virtual Local Area Network

- Tarayıcılarla Ağı Denetlemek: Nessus (http://www.nessus.org) gibi tarayıcılarla kurum dışından bağlantılar yaparak, örneğin bir ISP'den internet erişiminde kurumun ağına ulaşma ve erişim listelerinin çalışıp çalışmadığını kontrol etme aşamaları yerine getirilmektedir.
- Yönlendiricide IOS tabanlı kontrol: Tablo1'deki komutlar kullanılarak sistemin düzgün çalışıp çalışmadığı kontrol edilebilir.

Komut	Açıklaması
show processes cpu	CPU kullanımı kontrol
show processes memory	Bellek kullanımı kontrol
show ip access-list	Erişim listesi kontrolü

Tablo1: IOS Tabanlı Kontrol Komutları

SONUÇ

Yönlendirici, kurumun dış bağlantılarında kilit bir cihazdır. Cihazın güvenliğini sağlamak ve yapılacak ayarlarla ağın güvenliğini sağlamak çok önemlidir. Bu dökümanda bu işlemler için gerekli temel işlemler örneklerle anlatılmıştır.

Bu bildiri, Ege Üniversitesi Network Güvenlik Grubu tarafından hazırlanmakta olan "Yönlendirici Güvenlik Raporu" nun bir özetidir. Halen alt başlıkları yazılmakta olan bu raporun en son versiyonuna http://security.ege.edu.tr/dokumanlar.php adresindeki "network" altbaşlığından veya http://bornova.ege.edu.tr/~enis/bildiri adresinden ulaşabilirsiniz.

KAYNAKÇA

[1] 2001, Mehmet Uğursoy, Router access-list bölüm1, http://www.olympos.org/article/articleview/246/1/10/

[2] 2001, Mehmet Uğursoy, Router access-list bölüm2, http://www.olympos.org/article/articleview/247/1/10/

[3] Cisco ACL Example, http://www.ja.net/CERT/JANETCERT/prevention/cisco/cisco_acls.html

[4] 2002, Enis Karaaslan, Ağ Cihazlarının Güvenliğinin Sağlanma Yöntemleri, Inet-tr 2002, http://bornova.ege.edu.tr/~enis/bildiri/NwCihazGuvenligi2002.doc

[5] NSA/SNAC Router Security Configuration Guide: http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf

[6] Cisco - Why Some IOS Privilege Levels Cannot See Complete Running Configuration, http://www.cisco.com/warp/public/63/showrun.pdf

[7] Cisco - How to Assign Privilege Levels with TACACS+ and RADIUS, http://www.cisco.com/warp/public/480/PRIV.pdf

[8] Choosing Interior Gateway Protocol, http://www.networkcomputing.com/1021/1021ws2.html

[9] 99, Building Bastion Routers Using Cisco IOS : http://www.phrack.org/show.php?p=55&a=10

[10] 2000, Convery S., Trudel B., SAFE: A *Security* Blueprint for *Enterprise* Networks, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

[11] Multi Router Traffic Grapher, http://people.ee.ethz.ch/~oetiker/webtools/mrtg

[12] CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP), http://www.cert.org/advisories/CA-2002-03.html
[13] SNMP version 3 linkleri, http://www.ibr.cs.tu-bs.de/ietf/snmpv3/
[14] Jason Riddle: Four Steps to the Right IOS http://www.cisco.com/warp/public/784/packet/title
[15] Cisco IOS Security, http://www.cisco.com/warp/public/732/Tech/security/
[16] IOS Karşılaştırması, http://www.cisecurity.org/bench_cisco.html
[17] Router Security Guide, http://www.nsa.gov/snac/cisco/guides/cis-2.pdf
[18] IP Source Route http://www.avici.com/documentation/HTMLDocs/0222306_revBA/IP_Commands10.html
[19] Exterior Gateway Protocolu RFC 904 Exterior Gateway Protocol Formal Specification, http://www.faqs.org/rfcs/rfc904.html
[20] Reserve edilmiş ip adresleri, http://spamid.servebeer.com:8081/utils/include/spamid/reserved_blocks.jsp
[21] Enable Unicast Reverse Path-Forwarding Check, http://www.juniper.net/techpubs/software/junos/junos61/swconfig61-routing/html/routing-generic-config11.html#1016980
[22] Quality of Service, http://www.cisco.com/en/US/tech/tk543/tech_topology_and_network_serv_and_protocol_suite_home.html
[23] Defining Strategies to Protect Against TCP SYN Denial of Service Attacks, http://www.cisco.com/warp/public/707/4.html#unwittinglyhost
[24] Preventing Smurf Attacks, http://www.nordu.net/articles/smurf.html