

Doküman Kodu: BGT-2003

YÖNLENDİRİCİ GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

12 EKİM 2007

P.K. 74, Gebze, 41470 Kocaeli, Türkiye
Tel: (0262) 648 1000
Faks: (0262) 648 1100
<http://www.bilgiguvenligi.gov.tr>
teknikdok@bilgiguvenligi.gov.tr

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geçen Ađ Güvenliđi personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Oktay ŞAHİN'e teşekkürü borç biliriz.

İÇİNDEKİLER

1. GİRİŞ	6
1.1 Amaç ve Kapsam.....	6
1.2 Hedeflenen Kitle.....	6
1.3 Kısaltmalar.....	6
1.4 Dokümanda Kullanılan Semboller	8
2. FİZİKSEL GÜVENLİK	8
3. ÇALIŞMA KOŞULLARI	9
4. YÖNLENDİRİCİNİN TOPOLOJİDEKİ YERİ	10
5. ERİŞİM KONTROLÜ	11
5.1 Kimlik Doğrulama	12
5.2 Yetkilendirme	13
5.3 Olay Kayıtları	14
5.4 Merkezi Kimlik Doğrulama, Yetkilendirme ve İzleme	15
6. İŞLETİM SİSTEMİ GÜNCELLİĞİ	16
7. SERVİS KONTROLÜ	16
8. UZAKTAN YÖNETİM KONTROLÜ	21
9. ERİŞİM KONTROL LİSTELERİ	21
9.1 Standart Erişim Kontrol Listeleri.....	22
9.2 Gelişmiş Erişim Kontrol Listeleri.....	24
10. YÖNLENDİRME PROTOKOLÜ GÜVENLİĞİ	26
10.1 Yönlendirme Tablosu ve Yönlendirme Protokolleri	26
10.2 Yönlendirme Kimlik Doğrulaması	29
10.2.1 RIP Kimlik Doğrulaması.....	29
10.2.2 OSPF Kimlik Doğrulaması	29
10.2.3 BGP Kimlik Doğrulaması	30
10.2.4 EIGRP Kimlik Doğrulaması	32

KAYNAKÇA 33

1. GİRİŞ

Bu dokümanda yerel alan ağlarının intranete veya internete bağlantısında kullanılan yönlendirme cihazlarının güvenli olarak yapılandırılması ve işletilmesi anlatılacaktır.

1.1 Amaç ve Kapsam

Bu dokümanda günümüzde yaygın olarak kullanılan ve ağın dış dünya ile bağlantısını sağlayan yönlendirme cihazı üzerinde alınabilecek güvenlik önlemleri anlatılacaktır. Bu çerçevede fiziksel güvenlik, çalışma koşulları, kimlik doğrulama, yetkilendirme, izleme, servis kontrolü, yama kontrolü, erişim listesi kontrolü, uzaktan yönetim kontrolü ve yönlendirme protokolü kontrolü anlatılacaktır.

1.2 Hedeflenen Kitle

Bu doküman bir ağın geniş alan bağlantısını yapılandıran, yöneten ya da bu konularda çalışmak isteyen kişiler tarafından kullanılabilir.

1.3 Kısaltmalar

UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
IP	: Internet Protocol
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
ICMP	: Internet Control Message Protocol
HTTP	: Hyper Text Transfer Protocol
FTP	: File Transfer Protocol
SNMP	: Simple Network Management Protocol
NTP	: Network Time Protocol
ARP	: Address Resolution Protocol
MAC	: Media Access Control
RIP	: Routing Information Protocol

OSPF	: Open Shortest Path First
IS-IS	: Intermediate System to Intermediate System
BGP	: Border Gateway Protocol
EIGRP	: Enhanced Interior Gateway Routing Protocol
AS	: Autonomous System
ISS	: İnternet Servis Sağlayıcı
RADIUS	: Remote Authentication Dial In User Service
TACACS	: Terminal Access Controller Access Control System
RFC	: Request For Comments
IETF	: Internet Engineering Task Force
AAA	: Authentication Authorization Accounting
DNS	: Domain Name System
CDP	: Cisco Discovery Protocol
SSH	: Secure Shell
HTTPS	: HTTP Secure
SSL	: Secure Socet Layer
QoS	: Quality of Service
CPU	: Central Processing Unit
RAM	: Random Access Memory

1.4 Dokümanda Kullanılan Semboller

Sembol	Açıklaması
(yabancı terim)	İngilizce terimleri belirtmek içindir.
<u>Vurgu</u>	Vurgu yapmak için kullanılır.
komut	Kod parçalarını ve betikleri belirtmek içindir.
<>	Komutlarda kullanılacak parametre ismi belirtmek için kullanılır.
	Komutlarda kullanılacak parametre seçeneklerini ayırmak için kullanılır.

2. FİZİKSEL GÜVENLİK

Herhangi bir ağ cihazına fiziksel erişim elde eden kişi o cihazın çalışmasını engelleme, yapılandırmasını değiştirme veya dinleme imkanına da sahip olabilir. Bu sadece ağ cihazlarıyla sınırlı olmayıp, pek çok bilgisayar elemanı için geçerlidir. Yönlendirici ağın dış dünya ile bağlantısını sağladığı için sürekliliği ve üzerinden geçen trafik çok önemlidir. Bu yüzden de üzerinden geçen trafiğin dinlenmesi, çalışmasının engellenmesi veya devre dışı kalmasını sağlayacak etkilerden uzak tutulması gerekmektedir. Bu çerçevede birinci önlem olarak yönlendiricinin fiziksel güvenliği sağlanmalıdır. Yönlendiricinin fiziksel güvenliği için aşağıdaki önlemler alınmalıdır:

- Yönlendirici, fiziksel çarpma veya düşme gibi olaylara maruz kalmaması için kabinet içerisinde muhafaza edilmelidir.
- Eğer yönlendirici 19” kabinete monte edilebilirse edilmeli edilemezse de kabinet içerisinde sabit raf üzerine uygun bir şekilde konulmalıdır.
- Yönlendiricinin bulunduğu sistem odasına sadece yetkili kişilerin girmesine izin verecek kilit, manyetik kart, parmak izi gibi kimlik doğrulama mekanizması konulmalıdır.

- Yönlendiriciler çalışma koşullarından dolayı eğer mümkünse insanların bulunduğu ofislerde konumlandırılmamalıdır. Eğer yönlendirici zorunlu olarak ofislerde konumlandırılıyorsa kilitli kabinetler içerisinde tutularak yetkisiz kişilerin doğrudan erişimi engellenmelidir.

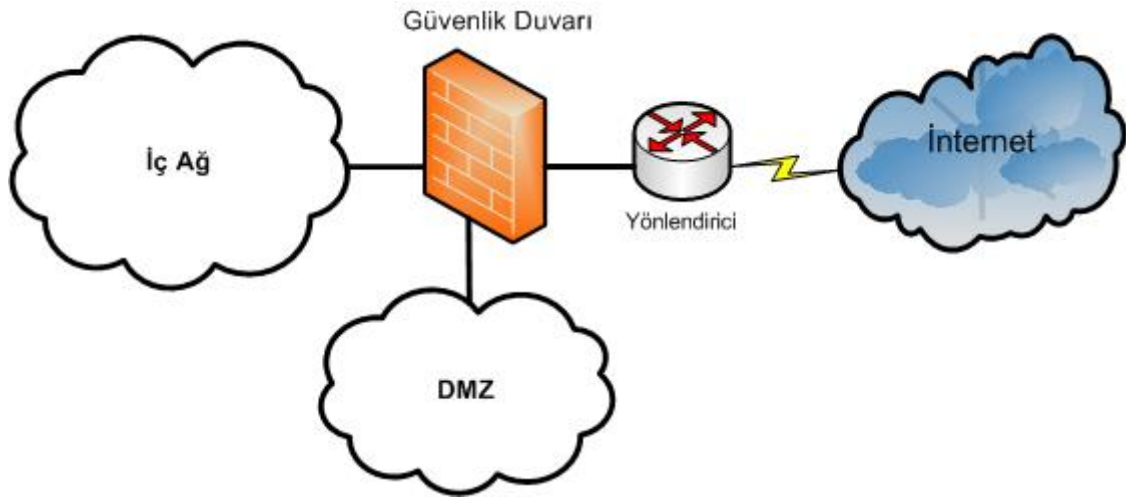
3. ÇALIŞMA KOŞULLARI

Yönlendiriciler ağda sürekli olarak ya da uzun süre çalışması gereken cihazlardır. Çoğunlukla bir yönlendirici yapılandırıldıktan sonra uzun süre problemsiz olarak çalışabilir. Bu süre içerisinde yönlendiricinin mekanik ya da elektriksel problemlerden kaynaklanan nedenlerden dolayı devre dışı kalmaması için çalışma koşullarının uygun olarak ayarlanması gerekmektedir. Yönlendiricinin uzun süre çevresel ya da elektriksel etkilerden dolayı bozulmaması için aşağıdaki önlemler alınmalıdır:

- Yönlendiricinin bulunduğu ortama toz girmemeli ve toz yapıcı etkenler bulunmamalıdır.
- Yönlendiricinin şebekeden kaynaklanabilecek gerilim değişikliklerinden etkilenmemesi için kesintisiz güç kaynağı ile beslenmelidir.
- Yönlendirici, çalışmasını olumsuz yönde etkileyecek elektromanyetik işaretlerin bulunduğu bir ortamda tutulmamalıdır.
- Yönlendiricinin bulunduğu ortamda nem ya da yüksek ısı olmamalı ve bunlar klima gibi cihazlarla sürekli belli değerlerde tutulmaya çalışılmalıdır. Ortamın çeşitli cihazlarla kontrol edilmesi yanında ısı ölçer, nem ölçer gibi aygıtlarla sürekli ortama ait değerler ölçülmeli ve sınır değerlerin dışına çıkılması durumunda gerekli uyarılar yapılarak sisteme müdahale edilmesi sağlanmalıdır.
- Yönlendirici üretim koşullarına uygun olarak kullanılmalıdır. Yani kapağı açık, modül yuvalarından birinin veya birkaçının kapağı çıkarılmış durumlarda çalıştırılmamalıdır.

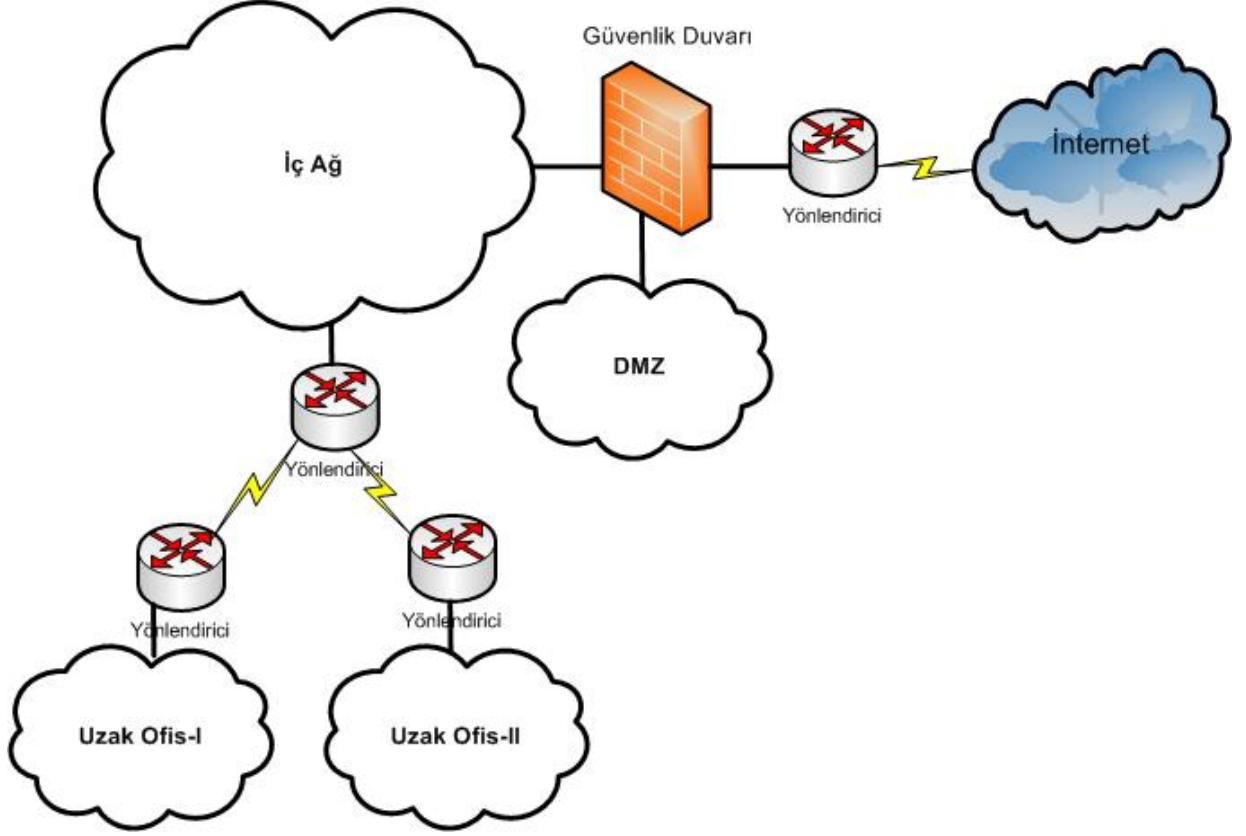
4. YÖNLENDİRİCİNİN TOPOLOJİDEKİ YERİ

Yönlendirici ağın dış dünyaya bağlantısını sağlayan cihaz olup ağın en dış kısmında bulunur. Günümüz ağlarında çoğunlukla Güvenlik duvarından hemen sonra yer alır ve güvenlik duvarından gelen paketleri dış dünyaya, dış dünyadan gelen paketleri de güvenlik duvarına iletir. Tipik bir ağ topolojisi Şekil 4-1’de görülmektedir. Yönlendiricinin bu topolojide kullanılması durumunda önünde yönlendiriciyi koruyan herhangi bir güvenlik mekanizması olmadığından yönlendiricinin güvenli olarak yapılandırılması oldukça önemlidir.



Şekil 4-1 – Yönlendiricinin topolojideki yeri

Bazı durumlarda iç ağda da yönlendiricinin bulunması gerekebilir. Özellikle büyük bir geniş alan ağına sahip şirkette kurumun internet çıkışı tek bir noktadan yapılmak istenirse ya da kuruma erişimin tek bir noktadan yapılması gerektiği durumlarda iç ağa da bir yönlendirici konulabilir. Bu yönlendirici kurumun kendi bağlantıları ile iletişimini sağlar. Bu yönlendiricinin topolojik yapısı Şekil 4-2 görülmektedir. Bunun yanında kurumun bağlantıları bir yönlendiricide sonlandırıldıktan sonra, bir güvenlik duvarı aracılığı ile iç ağa ve oradan da internete çıkabilir ya da yönlendiricide sonlandırıldıktan sonra güvenlik duvarının bir arayüzüne bağlanarak iç ağa ve internete erişimleri kontrol altına alınabilir.



5. ERİŞİM KONTROLÜ

Erişim kontrolü, nesnelerin objelere erişimlerini düzenler. Buradaki nesne cihaz, yazılım, dosya gibi araçları, özne ise bunlara erişim yapacak kullanıcı, program gibi şeyleri ifade etmektedir[2]. Yönlendiriciye bağlanarak ayar yapmak, yönlendirici üzerindeki yapılandırmayı görmek veya sonradan yönlendirici üzerindeki değişiklikleri izlemek, bir bilgisayar ağının düzgün işlemesi ve kontrolü için oldukça önemlidir. Gizlilik ve sürekliliğin sağlanması için bu işlemlerin yetkili kişiler tarafından yapılması ve sonuçlarının kayıt altına alınması gerekmektedir. Erişim kontrolünün sağlanabilmesi için yönlendirici üzerinde temel olarak kimlik doğrulama, yetkilendirme ve izleme mekanizmalarının çalıştırılması gerekir.

5.1 Kimlik Doğrulama

Kimlik doğrulama, iddia edilen kimliğin test edilmesini ya da doğrulanmasını sağlayan işlemdir. Yönlendirici üzerinde zaman zaman bazı ayarların yapılması ya da görülmesi gerekebilir. Bu ayarların yapılması veya görülmesi için yönlendiriciye erişim, lokal olarak konsol porttan ya da telnet, SSH (**Secure Shell**), HTTP (**Hyper Text Transfer Protocol**), SNMP (**Simple Network Management Protocol**), HTTPS gibi protokollerle uzaktan yapılabilir. Yönlendiriciye yapılan bu erişimlerin sadece doğru kişiler tarafından yapılmasını sağlamak için kimlik doğrulaması gerekmektedir.

Çoğunlukla yönlendiricilerin, varsayılan fabrika ayarlarında, kullanıcı isimleri ve parolaları olmaz. Yönlendiriciye doğrudan erişim yapılabilir. Bazı yönlendiricilerde kullanıcı adı ve parolası tanımlanmış olsa da bu bilgiler kullanıcı kılavuzlarında yer aldığından ciddi bir güvenlik önlemi oluşturmazlar. Bu yüzden yönlendirici ilk yapılandırılmaya başlandığında kullanıcı adı ve parolası tanımlanarak yönlendiriciye erişim, kontrol altına alınmalıdır. Yönlendiriciye lokalden erişim yapılmak istendiğinde, kimlik doğrulaması yapacak şekilde yapılandırılmalıdır. Ayrıca lokal erişimlerin güvenliğini artırmak için fiziksel güvenlik önlemleri de alınmalıdır.

Yönlendiriciye uzaktan erişime izin verilmesi, yönlendiricinin uzaktan yapılandırılması, ağ ile ilgili bilgilerin alınması, yönlendiricinin durumu hakkında bilgi alınması gibi çeşitli yönetim kolaylıkları getirmesi yanında ciddi güvenlik risklerini de beraberinde getirmektedir. Çünkü yönlendiriciye uzaktan erişim izni verildiğinde ağda bulunan herkese erişim imkanı doğar. Yönlendiriciye gerekmiyorsa uzaktan erişim izni verilmemelidir. Eğer uzaktan erişim izni veriliyorsa uzaktan erişimlerin denetim altına alınması için telnet, SSH, HTTP, SNMP protokolleri için aşağıdaki güvenlik önlemleri alınmalıdır:

- Telnet, HTTP, SSH, SNMP, HTTPS servislerinden kullanılmayanlar kapatılmalıdır.
- Kullanılan uzak erişim protokolleri için yönlendirici üzerinde kimlik doğrulaması etkinleştirilmelidir.
- Kimlik doğrulamalarında mümkün olduğunca kullanıcı isimleri kullanılarak sisteme yapılan erişimlerin izlenmesi sağlanmalıdır.
- Yönlendiricilerde kimlik doğrulaması genellikle kullanıcı adı ve parolası ya da genel bir parola yapısında olduğu için parola yeterince karmaşık seçilmelidir. (Örneğin sekiz karakter uzunluğunda büyük harf küçük harf ve rakamlardan oluşan bir parola)
- Yönlendirici üzerinde tanımlanmış olan parolalar periyodik olarak değiştirilmelidir.

- Yönlendiriciyi artık yönetmeyecek bir kullanıcı varsa ivedi olarak ona ait hesap kapatılmalı ve parolası iptal edilmeli.
- Yönlendirici destekliyorsa uzaktan erişim için öncelikle SSH, HTTPS gibi güvenli protokoller tercih edilmelidir.
- Yönlendiriciye uzaktan erişim yapacak IP adresleri erişim kontrol listeleriyle sınırlandırılmalıdır.
- Yönlendirici üzerindeki kimlik doğrulama kayıtları başarılı da olsa başarısız da olsa kayıt altına alınmalıdır.

5.2 Yetkilendirme

Yetkilendirme ağ cihazı üzerinde tanımlanan herhangi bir kullanıcının neler yapabileceğinin tanımlanmasıdır. Yönlendiriciler de diğer birçok ağ cihazında olduğu gibi üzerinde birden çok kullanıcının tanımlanmasına izin verirler. Yönlendirici üzerinde tanımlı tüm kullanıcıların yetkileri aynı değildir. Bazı kullanıcılar yönlendirici üzerindeki tüm komutları işletebilmesine karşın bazı kullanıcılar sadece belli komutları işletebilir ya da belli ayarları görebilirler. Bunun sebebi yönlendiricinin birden çok kişi tarafından yönetilmesi ya da izlenmesidir. Bu özellik sistemin sürekliliğini ve gizliliğini sağlamaya yöneliktir. Yönlendirici üzerinde gerçekleştirilecek olayların tamamı aynı öneme sahip değildir. Bu yüzden de farklı yetkilere sahip kullanıcılara ihtiyaç duyulmaktadır. Yönlendirici üzerinde yetkilendirme yapılırken aşağıdaki güvenlik önlemleri alınmalıdır:

- Yönlendirici üzerinde mümkün olan en az sayıda kullanıcı oluşturulmalıdır.
- Kullanıcılara işlerini yapabilecekleri en düşük haklar verilmelidir.
- Kullanıcıların genel kullanıcı adı ve parolası ile sisteme girişine izin verilmemelidir.
- Yetkilendirme yapıldıktan sonra kullanıcıların sistem üzerindeki aktiviteleri izlenmeli ve kayıt altına alınmalıdır.

5.3 Olay Kayıtları

Yönlendirici üzerindeki önemli olayların nedenlerinin araştırılması ve geriye doğru izinin sürülebilmesi için yönlendirici üzerindeki önemli olayların kayıtlarının tutulması gerekmektedir. Yönlendirici üzerindeki önemli olayların kayıtları yönlendirici üzerinde veya kayıt sunucusu üzerinde tutulmalıdır. Kayıtların yönlendirici üzerinde tutulması durumunda yönlendiricinin enerjisinin kesilmesi veya yönlendiricinin yeniden başlatılması durumunda kayıtlar RAM (**Read Only Memory**)’de tutulduğu için olayların geriye doğru izini sürmek mümkün olamaz. Eğer mümkünse yönlendiriciye ait olaylar yönlendirici dışında ayrı bir kayıt sunucusunda tutulmalıdır.

Yönlendirici üzerinde meydana gelen olayların sistem yöneticileri tarafından kolay bir şekilde anlaşılabilmesi için olaylar sınıflandırılmıştır. Tablo 5.1’de yaygın olarak kullanılan sınıflandırma değerleri görülmektedir. Bu tabloda olaylar çok önemliden az önemliye doğru sıralanmıştır. Yönlendiricide tutulacak kayıt seviyesinin belirlenmesinde bu derecenin büyük önemi vardır. Eğer çok önemli olaylara ait kayıtların görülmesi isteniyorsa sıfır seviyesi seçilmelidir. Daha az önemli kayıtların görülmesi isteniyorsa bu seviye yediye doğru yükseltilmelidir. Kayıt seviyesi yükseldikçe yönlendiriciden gelecek bilgi artacaktır. Bu durumda da gelen kayıtların incelenmesi ve oradan anlamlı bilgilerin çıkarılması zor olabilir. O yüzden kayıt seviyesi seçilirken yönlendiriciden beklediğimiz bilgiler göz önüne alınmalıdır.

Seviye	Seviye İsmi	Açıklama	Örnek
0	Emergency	Yönlendirici kullanılamaz halde	İşletim sistemi yüklenemiyor
1	Alert	İvedi müdahale gerekir	Isı çok yüksek
2	Critical	Kritik koşul	Bellek ayıramama
3	Errors	Hata koşulu	Geçersiz bellek boyutu
4	Warnings	Uyarı koşulu	Hatalı kripto işlemi
5	Notifications	Normal fakat önemli olay	Arayüz durumu değişmesi
6	Informational	Bilgi mesajı	Erişim kontrol listesi paket engelledi
7	Debugging	Hata ayıklama mesajı	Hata ayıklama etkinleştirildiğinde kullanılır

Tablo 5.1 Olay kayıt kritiklik dereceleri

Tutulacak kaydın kritiklik seviyesi etkin bir biçimde belirlendikten sonra kayıtların düzenli olarak incelenmesi de önemli bir konudur. Çünkü kayıtlar düzenli olarak incelenmezse yönlendirici üzerinde meydana gelen önemli olaylar fark edilmeyebilir. Örneğin yönlendiricinin bir portundaki aşırı trafik, bir portunun **up down** olması gibi ağın sürekliliğini etkileyen olaylar zamanında fark edilmeyebilir. Bunun sonucunda da ağ kaynaklarından etkin bir şekilde faydalanılmamış olur. Ağdaki kaynakların etkin kullanılması, problemlerin zamanında fark edilip ivedi olarak çözülmesi, güvenlik ihlallerinin tespit edilmesi için yönlendirici üzerindeki kayıtlar düzenli olarak incelenmeli ve uygunsuz bir durum varsa gerekli önlemler alınmalıdır.

5.4 Merkezi Kimlik Doğrulama, Yetkilendirme ve İzleme

Kimlik doğrulaması, yetkilendirme ve izleme yönlendirici üzerinde yerel olarak yapılmasının yanında merkezi bir AAA(**Authentication Authorization, Accounting**) sunucusu tarafından da yapılabilir. Merkezi bir sunucu tarafından yapılmasının temel avantajı ağda çok sayıda yönlendirici varsa bunlarının her birinin üzerinde kullanıcı, tanımlama, onların yetkilerini belirleme olay kayıtlarının tutulması çok zor olacağı için bu işlemin merkezi olarak yapılmasını sağlamaktır. Çoğu zaman bu AAA sunucuların sunduğu güvenlik hizmetleri bir yönlendiricinin sunacağı güvenlik hizmetlerinden daha fazladır. Bu güvenlik hizmetleri kimlik doğrulama, yetkilendirme ve izlemeyi içerirler. Diğer bir avantajı ise herhangi bir şekilde yönlendiricinin yapılandırmasının kaybolması, silinmesi ya da arızalanması durumunda yönlendiriciye AAA sunucudan kimlik doğrulama, yetkilendirme ve izleme ile ilgili ayarlar kolay bir şekilde yeniden yüklenebilir.

Günümüzde yaygın olarak kullanılan iki tane AAA sunucu vardır. Bunlar RADIUS (**Remote Authentication Dial In User Service**) ve TACACS+ (**Terminal Access Controller Access Control System plus**)'dır.

RADIUS, RFC 2865 numarası ile IETF (**Internet Engineering Task Force**) tarafından tanımlanmış bir endüstri standardıdır [1]. RADIUS erişim noktası ve merkezi sunucu arasında güvenlik bilgilerini taşıyan dağıtık istemci/sunucu mimarisine dayalı bir mimaridir. RADIUS paylaşılan gizli anahtarla haberleşmeyi korur. RADIUS kimlik doğrulama, yetkilendireme ve izlemeyi sağlamak için kullanılır. RADIUS sunucular ücretsiz olarak elde edilebilir. Eski olanlar kimlik doğrulamak için 1645 numaralı portu yeni olanlar ise 1812 numaralı portu kullanırlar. Daha çok ISS (Internet Servis Sağlayıcı)'lar tarafından kullanılmakla birlikte büyük bir ağa sahip olan ve cihazlarını merkezi olarak yönetmek isteyen herkes tarafından kullanılabilirler.

TACACS esnek bir izleme, kimlik doğrulaması ve yetkilendirme sağlamak için geliştirilmiştir [1]. TACACS+ Cisco tarafından AAA sistemi kullanılarak merkezi erişim kontrolü için geliştirilmiştir. Cisco açık kaynak kodlu olan sistem üzerine eklemeler yaparak TACACS+'ı geliştirmiştir. TACACS+ paylaşılan gizli anahtarla sunucu ve istemci arasındaki haberleşmeyi korur.

Eğer ağda çok sayıda yönlendirici ve bunları kullanan farklı yetkilerde kullanıcılar varsa merkezi kimlik doğrulaması yapılmalıdır.

6. İŞLETİM SİSTEMİ GÜNCELLİĞİ

Yönlendiriciler çoğunlukla kendilerine özgü işletim sistemleri üzerinde çalışırlar. Diğer yazılım ve donanımlarda olduğu gibi yönlendiriciler üzerinde de açıklıklar çıkmaktadır. Yönlendiricilerin işletim sistemlerinde çıkan bu açıklıklar sonucu yönlendiricilerin ve hizmet sunduğu ağın süreklilik, gizlilik ve bütünlüğünün zarar görmemesi için işletim sistemleri güncel olmalıdır. Güncelleme işlemi üreticinin sayfası periyodik aralıklarla kontrol edilerek veya güvenlik sayfaları izlenerek yapılmalıdır. Fakat yönlendiricinin en son çıkan sürümü geniş bir çevre tarafından test edilmediği için bazı işlevsel ve fonksiyonel eksiklikleri bulunabilir. Bu yüzden kullanılmadan önce mümkünse test edilmeli ya da bazı çevreler tarafından bir süre kullanılması beklenmelidir.

7. SERVİS KONTROLÜ

Yönlendirici üzerinde varsayılan olarak birçok servis çalışmaktadır. Yönlendirici üzerinde yaygın çalışan servisler aşağıda verilmiştir.

TCP small servers

UDP small servers

Finger
HTTP server
Bootp server
Configuration auto-loading
IP source routing
Proxy ARP
IP directed broadcast
Classless routing behavior
IP unreachable notifications
IP mask reply
IP redirects
NTP service
Simple Network Mgmt. Protocol (SNMP)
Domain Name Service (DNS)
Cisco Discovery Protocol (CDP)
SSH (Secure Shell)

TCP ve UDP Small Server

TCP ve UDP protokol standartları, ip servisi veren cihazların **daytime, chargen echo, discard** gibi basit servisleri sunmasını tavsiye ederler. Fakat günümüzde yönlendiricilerin bu servisleri sunmasına gerek yoktur. Bu yüzden de yönlendirici üzerinde bu servisler kapatılmalıdır.

Finger Server

Finger servisi, Unix sistemlerde sisteme bağlı olan kullanıcıları listeleyen bir komuttur. Birçok yönlendirici üzerinde bu servis varsayılan olarak açık gelmektedir. Bu servisin kontrol edilerek kapatılması gerekmektedir.

HTTP Server

Yönlendiricilerin birçoğu http protokolünü desteklemektedir. Yani http protokolü kullanılarak yönlendiriciye bağlanılabilmekte, onun yapılandırması ve izlenmesi yapılabilmektedir. Diğer taraftan yönlendiricinin yönetimi için bu servis kullanılmıyorsa ataklar için açıklık oluşturmaktadır. Yönlendirici HTTPS, SSL gibi daha güvenli bir protokolle yönetiliyorsa ya da HTTP servisi kullanılmıyorsa bu servis kapatılmalıdır. Eğer zorunlu olarak bu servisin kullanılması gerekiyorsa erişim kontrol listesi ile yönlendiriciye olan erişimler kontrol altına alınmalıdır.

Bootp Server

Bootp protokolü bir yönlendiricinin işletim sistemini ağdaki başka bir cihazdan yüklemesini sağlar. Aynı zamanda birçok yönlendirici ağdaki cihazlara kendi işletim sistemini Bootp servisi aracılığıyla sunar. Pratikte Bootp servisi nadir kullanılan bir servistir. Kullanılmadığında yönlendiricinin işletim sisteminin başkaları tarafından alınmasına sebep olur. Bu yüzden bu servis kapatılmalıdır.

Configuration Auto-Loading

Yönlendiriciler başlangıç yapılandırmalarını yerel bellekten veya ağdan yapabilirler. Başlangıç yapılandırmasının ağdan yükleniyor olması ciddi açıklıklara sebep olabilir. Eğer ağ tamamen güvenilir değilse bu servis kapatılmalıdır.

IP Source Routing

Kaynak Yönlendirme (**Source Routing**) IP'nin bir özelliğidir. Bu özellik etkinleştirilirse paket kendi yolunu belirleyebilir. Bu da birçok atak yapılmasına sebep olabilir. Yönlendiriciler genellikle kaynak yönlendirmeyi desteklerler. Eğer paketler QoS (**Quality of Service**) gibi özel bir amaçlar için belirli yollardan gönderilmiyorsa bu servis kapatılmalıdır.

Proxy ARP

Ağ cihazları ağ adresini fiziksel adrese çevirmek için ARP'ı (**Address Resolution Protocol**) kullanırlar. Normal koşullarda ARP protokolü bir yerel alan ağında çalışır. Ama yönlendiriciler farklı yerel alan ağlarında bulunan cihazların ikinci katmanda haberleşmesini bu Proxy ARP servisini kullanarak sağlarlar. Bu da iki farklı yerel alan ağ segmenti arasında güvenliğin ortadan kalkması anlamına gelir. Ancak iki ağın güvenlik seviyesi de aynı ise Proxy ARP servisi kullanılabilir. Proxy ARP servisi kapatılmalıdır.

IP Directed Broadcast

IP Directed Broadcast servisi yönlendiriciye bağlı herhangi bir yerel alan ağından genelyayın (**broadcast**) yapılması durumunda bu genelyayının tüm diğer yerel alan ağlarından yayınlanmasını sağlar. Bu bazı eski yönlendiricilerde servis dışı bırakma atağı için kullanılabilir. Bu servis yönlendirici üzerinde kapatılmalıdır.

IP Unreachables, Redirect, Mask Replies

ICMP (**Internet Control Message Protocol**) verdiği cevapta ağın yolu, yönlendirmesi ve koşulları hakkında bilgi verir. Yönlendiriciler gelen ICMP paketlerine geniş bir yelpazede cevap verirler bu da ağa ait bilgilerin dış dünyaya gönderilmesi, yönlendiricinin işletim sisteminin tespit edilmesi gibi önemli bilgilerin istenmeyen kişilerin eline geçmesine sebep olabilir. “**Host unreachable**”, “**Redirect**”, “**Mask Reply**” mesajları saldırganlar tarafından yaygın olarak kullanılır. Yönlendiriciler tarafından otomatik olarak üretilen bu mesajların engellenmesi gerekmektedir.

NTP Service

Yönlendiriciler, tarih ve saat bilgisini güncel tutmak için NTP protokolünü kullanırlar. Eğer yönlendirici büyük bir sistem içindeyse, cihazların her birinden olay kayıtları toplanıyorsa doğru bir analiz yapılabilmesi için yönlendiricilerin zaman bilgisinin merkezi güvenilir bir sunucudan alınması gerekir. NTP sunucusu cihazlar bu zaman bilgisini sağlayan sunucudur. NTP protokolü çoğunlukla açık kaynak kodlu ya da bir üreticiden alınarak yönlendirici içerisine gömülen bir servis olduğu için içerisinde birçok açıklığı da barındırmaktadır. Bu yüzden NTP servisi kullanılıyorsa servise olan erişim, erişim kontrol listeleriyle kontrol altına alınmalıdır. NTP servisi kullanılmıyorsa da kapatılmalıdır.

SNMP Servisi

SNMP ağ yönetimi ve izlemesi için kullanılan standart protokoldür. SNMP protokolünün üç sürümü mevcuttur. Bu sürümlerin her biri farklı güvenlik özelliklerine sahiptir. SNMP V1 ve V2 kimlik doğrulama ve gizlilik güvenlik özelliklerindeki eksiklerden dolayı tercih edilmemelidir. Eğer ağ içerisindeki yönlendiricilerin yönetimi SNMP protokolü ile yapılıyorsa yapılandırma güvenli bir şekilde yapılmalıdır. Çünkü ağ yönetim yazılımı yönlendiricinin, yapılandırmasını, yönlendirme tablosunu, trafik yükünü ve daha birçok bilgiyi yönlendiriciden alabilir. Eğer ağda SNMP servisi kullanılmıyorsa yönlendiriciler üzerinde aşağıdakiler yapılmalıdır:

- Kesinlikle tüm topluluk isimleri silinmeli
- SNMP servisi kapatılmalı ve SNMP trap özellikleri kapatılmalı

Eğer yönlendirici üzerinde SNMP protokolü kullanılacaksa öncelikle daha güvenli olan SNMP V3 sürümü tercih edilmeli ve aşağıdaki güvenlik önlemleri alınmalıdır:

- Güvenli bir sürüm tercih edilmelidir.
- Kullanılan ortak isim (**Community name**) varsayılan değerden değiştirilmeli ve tahmin edilmesi güç olan bir kelime seçilmelidir.
- Erişim yapacak IP adresleri erişim kontrol listesi ile sınırlandırılmalıdır.
- Başarısız SNMP sorgulama denemeleri kayıt altına alınmalıdır.

DNS Servisi

DNS (**Domain Name System**) servisi isim ve IP dönüşümü yapmaktadır. Yönlendirici üzerinde istendiğinde isimle iletişim kurulmak isteniyorsa DNS tanımlanarak isim çözümlleme işlemi gerçekleştirilebilir.

CDP Servisi

CDP (**Cisco Discovery Protocol**) Cisco'ya özgü bir protokoldür. Temel işlevi ağda bulunan diğer cihazları tanıma ve onlara üzerinde çalıştığı cihaz hakkında bilgi göndermek ve diğer cihazlar hakkında bilgi toplamaktır [4]. Bu protokol ikinci katmanda çalışan bir protokoldür. Bu yüzden kontrol edilmesi daha üst katmanlarda çalışan protokollere göre daha zordur. Eğer ağ dışarıya kapalı bir ağ ise kullanılabilir. Fakat ağ dış dünyaya bağlanan bir ağ ise bu servis yönlendiriciye ait önemli bilgileri dış dünyaya göndereceği için kapatılmalıdır.

Bu servislerin hepsi her zaman kullanılmamaktadır. Bu servislerden kullanılmayanlar kapatılmalıdır. Kullanılması zorunlu servislere olan erişimler ise denetim altına alınmalıdır. Aynı görevi yerine getiren iki servis var ise sadece daha güvenli olan servis çalıştırılmalıdır (Telnet ve SSH gibi).

8. UZAKTAN YÖNETİM KONTROLÜ

Yönlendiricinin uzaktan yönetilmesi, yapılandırmasının incelenmesi veya çalışma parametrelerine ait bilgilerin alınması genellikle telnet, SSH, HTTP, SNMP gibi protokollerle yapılmaktadır. Yönlendiricinin konsol dışında bu tür protokollerle uzaktan yönetilmesi, yönlendiricinin ele geçirilmesi, yönlendiricinin devre dışı bırakılması, yönlendiriciye ve ağa ait bilgilerin kötü niyetli kişilerin eline geçmesi gibi birçok riski de beraberinde getirmektedir. Yönlendirici için uzaktan erişim izni verilecekse aşağıdaki güvenlik önlemleri alınmalıdır:

- Uzaktan yönetim kullanılmıyorsa ilgili servisler kapatılmalıdır.
- Uzaktan erişim için mümkünse SSH, HTTPS gibi güvenli servisler tercih edilmelidir.
- Uzaktan erişime izin veren servisleri kullanacak IP adresleri erişim kontrol listeleri ile sınırlandırılmalıdır.
- Uzaktan yönetim için SNMP kullanılması durumunda topluluk ismi varsayılan değer olan **“public”** ve **“private”** değerlerinden başka bir değere değiştirilmelidir. SNMP sorgulaması yapabilecek cihazlar erişim kontrol listesi ile sınırlandırılmalıdır.
- Uzaktan başarısız bağlantı yapma istekleri kayıt altına alınmalıdır.
- Mümkün olduğunca yönlendirici tek bir servisle yönetilmelidir.

9. ERİŞİM KONTROL LİSTELERİ

Yönlendirici ağın en dış kısmında bulunması nedeniyle öncelikle kendisini koruması daha sonra da gerekiyorsa ağı koruması gerekir. Bu koruma işlemini genellikle ağa giren ve ağdan çıkan paketleri filtreleyerek yapar. Bu işlem içinde erişim kontrol listelerini kullanır. Bu erişim kontrol listeleri yönlendiriciye ya da ağa gelen ve ağdan çıkan paketleri denetim altına alır.

Birçok ağ cihazında da erişim kontrol listesi yaygın olarak kullanılmaktadır. Fakat bunların formatları arasında farklılıklar mevcuttur. Burada Cisco firmasına ait erişim kontrol listeleri anlatılacaktır. Diğerlerinde format olarak farklılıklar göstermekle birlikte mantık olarak aynıdır.

Erişim kontrol listelerinin genel özellikleri aşağıda verilmiştir:

- Erişim kontrol listeleri genellikle numaralarla ifade edilirler. Bazen isimle de ifade edilebilir.

- Erişim kontrol listesindeki satırlar yukarıdan aşağı doğru işlenirler. En son satır her şeyi durdur şeklindedir ve yazılmayabilir.
- Yazılan her bir erişim kontrol listesi bir arayüze giriş ya da çıkış yönünde uygulanmalıdır. Yoksa erişim kontrol listesinin bir anlamı olmaz.
- Erişim kontrol listeleri standart ve gelişmiş olarak ikiye ayrılmaktadır. Standart erişim kontrol listeleri sadece kaynak adresine göre sorgulama yapabilmekte gelişmiş erişim kontrol listeleri ise kaynak, hedef ve port adresine göre sorgulama yapabilmektedir. Bunların yanında bazı cihazlarda oturumları da kontrol eden dönüşlü (**Reflexive**) erişim kontrol listeleri mevcuttur.

9.1 Standart Erişim Kontrol Listeleri

Standart erişim kontrol listesi sadece kaynak adrese bakarak filtreleme yapar. Kaynak adresi kısmında ağ adresi de kullanılabilir. Yönlendiricinin herhangi bir arayüzüne standart erişim kontrol listesi **in** ya da **out** yönüne uygulandığında bu erişim kontrol listesinde belirtilen kaynak adreslerine ait paketlere erişim kontrol listesinde belirtildiği gibi izin verilir ya da düşürülür [5].

Standart erişim kontrol listesi aşağıdaki yapıdadır:

access-list sayı işlem kaynak [aralık] | herhangi log

sayı : 1-99 arasında olmak zorunda

işlem : **Permit** veya **Deny** olmak zorunda

kaynak: karşılaştırılacak kaynak adresi

aralık : Belli bir aralık verilebilir

log : Erişim listesine ait

herhangi: **any** değeri olursa herhangi bir adres olabilir anlamına gelir

Aşağıda standart erişim kontrol listesine ait bir örnek verilmiştir.

```
access-list 20 permit 192.168.1.0 0.0.0.255
access-list 20 deny any any
```

Buradaki 20 rakamı erişim kontrol listesinin sayı numarasını göstermektedir. **Permit** bu satırdaki kaynak adresine sahip IP'lere izin verileceğini göstermektedir. 192.168.1.0 0.0.0.255 ise bu erişim kontrol listesinin aralığını göstermektedir. İkinci kısım **wildcard** olarak ifade edilmektedir. Maskede bulunan bir bitlerinin olduğu kısımlardaki IP adreslerini kapsar.

Aşağıda başka bir örnek verilmektedir;

```
Access-list 10 permit host 212.174.45.12
Access-list 10 permit host 212.174.45.20
Access-list 10 permit host 212.174.45.22
Access-list 10 deny any any
```

Bu örnekte sadece 212.174.45.12, 212.174.45.20 ve 212.174.45.22 kaynak IP adreslerine sahip bilgisayarlara izin verilir diğerleri ise düşürülür. En son satırda kullanılan ifade **deny any any** ifadesine gerek yoktur. Çünkü erişim kontrol listelerinin yazılmayan son satırı her şeyi otomatik olarak engeller.

Engellemelerin kullanılacağı başka bir örnek verilecek olursa

```
Access-list 30 deny host 212.174.45.12
Access-list 30 deny host 212.174.45.20
Access-list 30 deny 175.45.70.0 0.0.0.255
Access-list 30 permit any any
```

Bu örnekte kaynak IP adresleri 212.174.45.12, 212.174.45.20 olan ve 175.45.70.0/24 ağında bulunan cihazların erişimi engellenir. Bu IP adresleri dışında olan tüm IP adreslerinin erişimine izin verilir. Bu tür erişim kontrol listesi genellikle bir ağdan veya bir bilgisayardan gelen saldırının veya erişimin engellenmesi için kullanılır.

Yazılan erişim kontrol listesinin geçerli olabilmesi için bir arayüze uygulanması gerekmektedir. Standart erişim kontrol listeleri de **in** ya da **out** yönünde uygulanır.

```
ip Access-group 30 in
```

Burada erişim kontrol listesinin bir arayüze **in** uygulanması görülmektedir. Arayüzün yapılandırmasına girildikten sonra erişim kontrol listesi uygulanabilir.

Standart erişim kontrol listesi yaygın olarak kullanılmasına karşın erişim yapılacak hedefin belirtilmemesi kullanımını kısıtlar.

9.2 Gelişmiş Erişim Kontrol Listeleri

Gelişmiş erişim kontrol listesi kaynak, hedef adrese ve porta bakarak filtreleme yapar. Kaynak ve hedef adresi kısmında ip adresi, aralık veya ağ adresi de kullanılabilir. Yönlendiricinin herhangi bir arayüzüne **in** ya da **out** yönüne uygulandığında erişim kontrol listesinin yaptığı kısıtlamaların çerçevesinde paket iletilir ya da düşürülür.

Gelişmiş erişim kontrol listesi aşağıdaki yapıdadır:

access-list sayı işlem protokol kaynak [aralık] [kaynakport] hedef [aralık] [hedefport] [diğer-seçenekler]

Sayı: 100 – 199, 2000-2699 arasında bir sayı veya isim olabilir.

İşlem: **permit** veya **deny** olmalı

Protokol: Protokolün ismi veya numarası. Örneğin IP, TCP, UDP, ICMP, vb...

Kaynak: Karşılaştırılacak kaynak adresi

Kaynak portu: **TCP** veya **UDP** kaynak portu

Hedef: Karşılaştırılacak hedef adresi

Hedef portu: **TCP** veya **UDP** hedef portu

Diğer seçenekler: **log**, **log-input**, **established**

Aşağıda gelişmiş erişim kontrol listesine örnek verilmiştir:

```
access-list 101 deny ip any host 10.1.1.1
```

Bu erişim kontrol listesinde IP adresleri kontrol edilmektedir. Erişim kontrol listesi kaynağı ne olursa olsun hedefi 10.1.1.1 olan bilgisayara erişimi kısıtlamaktadır. Standart erişim kontrol listelerinde olduğu gibi gelişmiş erişim kontrol listelerinde de en son satır **deny any any** şeklindedir ve bu yazılmaz. Ama istenirse **any any deny** yazılabilir.

Başa bir örnek aşağıda verilmiştir:

```
access-list 110 permit tcp any host 172.16.3.10 eq ftp
access-list 110 permit tcp host 172.16.2.10 host 172.16.1.100 eq telnet
```

110 numaralı erişim kontrol listesinin birinci satırında 172.16.3.10 IP adresine sahip FTP sunucusuna her yerden 21 numaralı porta erişim izni verilmiştir. Aynı erişim kontrol listesinin ikinci satırında ise 172.16.2.10 adresli cihazdan 172.16.1.100 IP adresli cihaza 23 numaralı porttan erişim izni verilmiştir. Geri kalan tüm paketler düşürülecektir.

Bazı erişimlerin engellediği bir örnek aşağıda verilmiştir:

```
access-list 120 deny tcp host 194.170.1.10 195.16.10.0 0.0.0.255 eq ftp
```

```
access-list 120 deny tcp host 194.170.1.10 host 195.16.10.100 eq http
```

```
access-list 120 permit any any
```

120 numaralı erişim kontrol listesinin birinci satırında 194.170.1.10 IP adresli cihazdan 195.16.10.0/24 ağına 21 numaralı porttan erişimler engellenmiştir. İkinci satırda ise 194.170.1.10 IP adresli cihazdan 195.16.10.100 IP adresli cihaza 80 numaralı porttan erişim engellenmiştir. Üçüncü satırda ise tüm IP'lerden tüm IP'lere her şeye izin veren kural görülmektedir.

Standart erişim listelerinde olduğu gibi gelişmiş erişim listelerinde de **log** ifadesi kullanılarak erişim listesine ait kayıtların tutulması sağlanabilir. Aynı şekilde yazılmış olan erişim listesinin çalışabilmesi için bir ara yüze **in** ya da **out** yönünde uygulanması gerekmektedir. Aşağıdaki örnekte 110 numaralı gelişmiş erişim kontrol listesi **serial 0** arayüzüne **in** yönünde uygulanmıştır. Yani **serial 0** arayüzünden içeriye giren paketler bu kurallara uyuyorsa geçer yoksa da düşürülür.

```
interface Serial 0
```

```
ip access-group 110 in
```

10. YÖNLENDİRME PROTOKOLÜ GÜVENLİĞİ

Protokol iki cihazın bilgi değişebilmesi için uyması gereken kurallar kümesidir[3]. Protokoller yönlendirilen (**Routed**) ve yönlendirici (**Routing**) olmak üzere ikiye ayrılır. Yönlendirilen protokoller, yönlendiriciler tarafından sadece iletilen paketlerdir. Bu protokoller yönlendiriciler üzerinden sadece kullanıcı ve cihazlara ait bilgileri taşırlar. IP, IPX, AppleTalk, DECNet yönlendirilen paketlere örnek olarak verilebilir. Yönlendirici protokoller ise ağ içerisinde karşı hedefe olan en kısa yolun bulunmasını sağlarlar. Yönlendiriciler üzerlerinde bu protokolleri çalıştırarak ya komşularından aldığı bilgilerle ya da kendisi doğrudan her bir hedefle konuşarak ağda bulunan tüm hedeflere olan en kısa yolu belirler ve yönlendireceği paketleri bu yoldan gönderir. RIP (**Routing Information Protocol**), OSFP (**Open Shortest Path First Protocol**), BGP (**Border Gateway Protocol**), IS-IS (**Intermediate System to Intermediate System**), EIGRP (**Enhanced Interior Gateway Routing Protocol**) protokolleri yaygın kullanılan yönlendirme protokollerine örnek olarak verilebilir.

10.1 Yönlendirme Tablosu ve Yönlendirme Protokolleri

Yönlendiricinin birincil görevi paketleri hedefe göndermektir. Bu işlemi yapabilmek için her bir yönlendiricinin bir yönlendirme tablosu vardır. Bu yönlendirme tablosu yönlendiricinin kendisi, sistem yöneticisi ve komşularından alınan bilgilerle oluşturulur. Yönlendiriciler, en iyi yolu belirlemek için bulunan yönleri belli metriklere göre kıyaslarlar. Yönlendirme protokollerinde yönü bulmak için belli algoritmalar kullanılır.

Yönlendiriciler kendi yönlendirme tablosunu oluşturmak için dört yöntem kullanır:

- Doğrudan Bağlantı: Yönlendiriciye doğrudan bağlı olan herhangi bir arayüz. Bu arayüz otomatik olarak yönlendirme tablosuna eklenir.
- Statik Yönlendirme: Ağ yöneticisi herhangi bir hedef için kendisi bir yön atayabilir. Yani herhangi bir hedef için paketin hangi arayüzden çıkacağını belirleyebilir.
- Dinamik Yönlendirme: Yönlendirici ağ içerisindeki diğer yönlendiricilerle yönlendirme protokolleri aracılığıyla konuşarak yönlendirme tablosunu otomatik olarak oluşturur. Yönlendirme tablosu oluşturma yöntemleri içerisinde en etkin olanı budur. Çünkü ağdaki değişimlere otomatik olarak ayak uydurur.

- Varsayılan Yönlendirme: En son karar için el ile girilir. Hedef için bir tabloda bir yer bulunmaz ise paketler bu varsayılan hedefe yönlendirilir. Bu yönlendirici kenar yönlendiriciler için önemli çünkü orada birkaç yönlendirme dışında tüm paketler varsayılan hedefe yönlendirilir.

Yönlendiricilerde RIP, OSPF, BGP, IS-IS, ve EIGRP protokolleri yaygın olarak kullanılır. Bunlardan RIP, OSPF ve BGP IETF standardı, IS-IS ISO standardı, EIGRP ise Cisco firması tarafından tanımlanmış bir standarttır.

Yönlendirmede önemli konulardan birisi de yönlendirme protokolleri kullanıldığında ağın ne kadar bir süre içerisinde öğrenildiğidir. Bu protokole göre değişmektedir. Örneğin OSPF, RIP'e göre çok daha hızlı bir şekilde ağı öğrenebilir.

Yönlendirme protokollerine ait birçok parametre bulunmakla birlikte bu dokümanın kapsamı dışındadır. Bu dokümanda sadece güvenlik penceresinden bakılacaktır.

Protokol	Çalışması
RIP	Distance Vector Protocol: Diğer ağlara olan uzaklığı sıçrama sayısı ile ölçer. Buradaki sıçrama sayısı hedefe ulaşılırken kaç tane yönlendirici geçildiğini gösterir. RIP küçük ağlar için uygun bir protokoldür. Çünkü en fazla 15 sıçrama uzaklığa gidebilmektedir. Komşularla olan bütünlüğü sağlamak için her 30 saniyede bir yönlendirme tablosunun tamamı komşularla paylaşılır.
OSPF	Link State Protocol: Diğer ağlara olan uzaklığı bulmak için bandgenişliğini bir parametre olarak kullanır. Her bir yönlendirici ağın basitleştirilmiş bir haritasını tutar. Güncellemeler çokluyayın paketleri ile gönderilir. Bu paketlerde yönlendirme tablosunun tamamı değil sadece değişiklikler gönderilir. OSPF geniş ağlar için uygun bir protokoldür.
IS-IS	Link State Protocol: Hedefe olan en kısa yolu bulmak için maliyet tabanlı bir metrik kullanır. Metrikleri gecikme, gider(expense) ve hatadır. Yönlendiriciler komşularına her on saniyede bir bilgilendirme paketi gönderirler. Tüm link state database'in gönderilmesi atanmış yönlendiriciler tarafından genel yayın olarak gönderilirler. IS-IS geniş alan ağları için uygun bir yönlendirme algoritmasıdır.
BGP	Diğer ağlara ait komşulukları tutmak için bir takım kurallar kullanır. Gelişmiş distance vector exterior gateway protokolünü kullanır. Güncellemeler çiftler arasında bir TCP bağlantısı ile yapılır. BGP-4 çok geniş ağlar için kullanılır.
EIGRP	Distance vector protocol: Diğer ağlara olan uzaklığı modellemek için karmaşık bir metrik kümesi kullanır ve bazı link state protokol

Protokol	Çalışması
	parametrelerini de kullanır. Güncellemeleri her bir 90 saniyede tüm EIGRP komşularına gönderirler. Gönderilen güncellemeler sadece değişiklikleri içerir. EIGRP geniş ağlar için uygun bir protokoldür.

Tablo 10.1 Yönlendirme protokolleri

Yaygın Yönlendirme Problemleri

Yönlendirme ve yönlendirme protokolleri yönlendiriciler için çok önemlidir. Aşağıda belirtilen konuları önemseyen ağ yöneticileri için yönlendirme protokolleri çok önemlidir:

- Ağdaki kaynaklara yetkisiz erişimi engellemek,
- Önemli bilgilerin yetkisiz kişiler tarafından kötüye kullanılmasını ve değiştirilmesini engellemek,
- Servislerdeki ağ hatalarını ve kesintilerini önlemek.

Korumasız bir yönlendirici veya yönlendirme etki alanı kötü niyetli ve bu konuda biraz tecrübeli kişiler için kolay bir hedef olabilir. Örneğin bir saldırgan yanlış bir güncelleme paketi göndererek yönlendiricinin yönlendirme tablosunu kolayca bozabilir. Saldırgan bu bilgileri kullanarak ağdaki paketleri istediği bir yere yönlendirebilir. Yönlendiricinin, yönlendirme tablosu üzerinde aşağıdaki önlemler alınarak bu tür saldırganların yetkisiz erişimleri ve kötü niyetli değiştirmeleri engellenebilir.

- Sadece statik yönlendirme kullanılabilir. Küçük ağlar için uygulanabilir fakat büyük ağlarda kullanılması yönlendirmeyi çok zorlaştırır ve çok büyük bir işgücü gerektirir.
- Yönlendirme tablosu güncellemeleri kimlik doğrulaması ile yapılabilir. Sadece bilinen ve güvenilen yönlendiricilerden gelen yönlendirme bilgileri değerlendirilir. Diğerleri ise elemine edilir.

Diğer gelebilecek atak türü servis dışı bırakma atakları. Örneğin güvensiz bir ağdan sürekli gelen güncelleme mesajları ağın bir kısmının devre dışı kalmasına neden olabilir. Bu tür atakların önüne geçilmesi için hızlı birleşme zamanı (**convergence**) ve yedek yönler olmalıdır.

ARP protokolü IP adresi bilinen bir cihazın MAC adresinin elde edilmesini için kullanılır. Proxy ARP ise IP adresi yerine MAC adresini kullanarak yönlendirme yapmaya yarar. Hem ARP protokolü hem de Proxy ARP protokolünde herhangi bir güvenlik önlemi yoktur. Yerel alan ağında bulunan herhangi bir kolayca yönlendiricinin ARP tablosunu değiştirebilir. Eğer yönlendirici üzerinde varsayılan ağ geçidi yerine Proxy ARP kullanılırsa hatalı veya yanlış yönlendirmeye sebep olabilir. Proxy ARP günümüzde yaygın olarak kullanılmamasına karşın kullanılması durumunda dikkatli olunmalıdır.

10.2 Yönlendirme Kimlik Doğrulaması

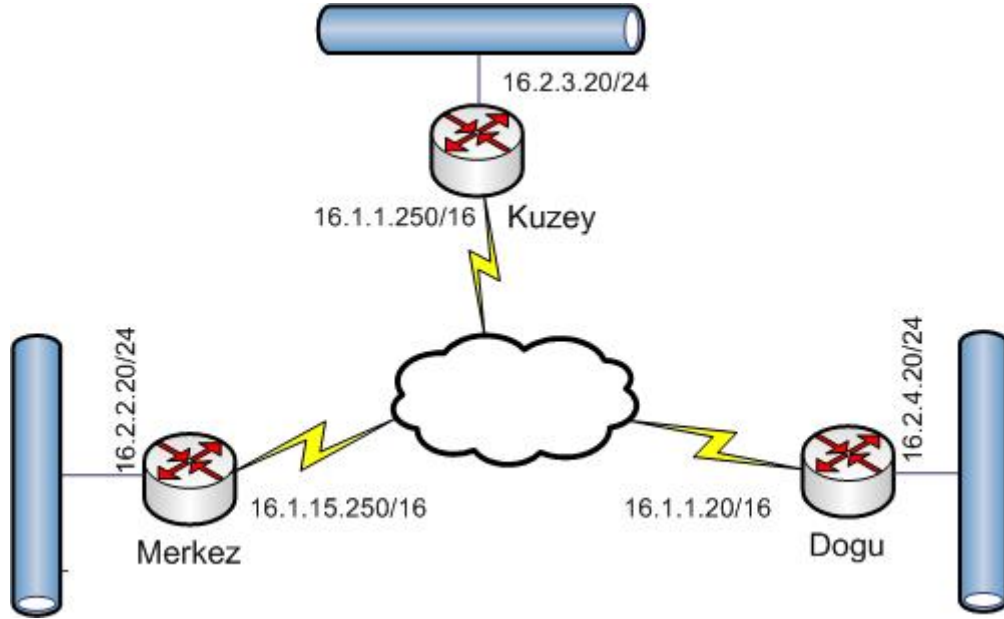
Yönlendirici kimlik doğrulamasının birincil amacı yönlendirme etki alanının bütünlüğünü korumaktır. Bu yönlendirme etki alanı bütünlüğünü sağlama işlemi yönlendiricilerin komşularıyla yönlendirme tablosunu değiştirken kimlik doğrulaması yapmasıyla sağlanır. Kimlik doğrulaması sayesinde güvensiz olan yönlendiricilerden gelebilecek hatalı yönlendirme güncellemeleri engellenmiş olur.

10.2.1 RIP Kimlik Doğrulaması

RIP protokolü yönlendirme ataklarını engellemek için kimlik doğrulamayı destekler. Komşu olan RIP yönlendiriciler paylaşılan gizli anahtarlar kullanır. Yönlendirme güncellemesi gönderen her bir yönlendirici, RIP güncelleme paketini bu anahtarla özetleyerek gönderir. Yönlendirme paketini alan yönlendirici de paylaşılan gizli anahtarı kullanarak paketin özetini kontrol eder. Eğer doğrudur paketi kabul eder. Sadece RIP Sürüm 2 kimlik doğrulamayı destekler. Bu yüzden kimlik doğrulamadan önce RIP Sürüm 2'nin kullanılacağı belirlenmelidir. RIP Protokolünde açık metin (**plaintext**) ve MD5 (**Message Digest**) özetleme kimlik doğrulaması olmak üzere iki yöntemle kimlik doğrulaması yapılır. Bunlardan MD5 kimlik doğrulaması daha güvenli olduğu için tercih edilmelidir.

10.2.2 OSPF Kimlik Doğrulaması

OSPF kimlik doğrulamasında kimlik doğrulaması anahtarla sağlanır. Yönlendirici güncelleme paketlerini gönderirken bu anahtarla imzalar. Paketi alan yönlendirici anahtarla paketin doğruluğunu paylaşılan anahtarla kontrol eder. Eğer gelen paket doğrudur kabul eder değilse paketi reddeder. OSPF de RIP gibi açık metin ve MD5 kimlik doğrulamasını kullanır.



Şekil 10.1 OSPF kimlik doğrulaması

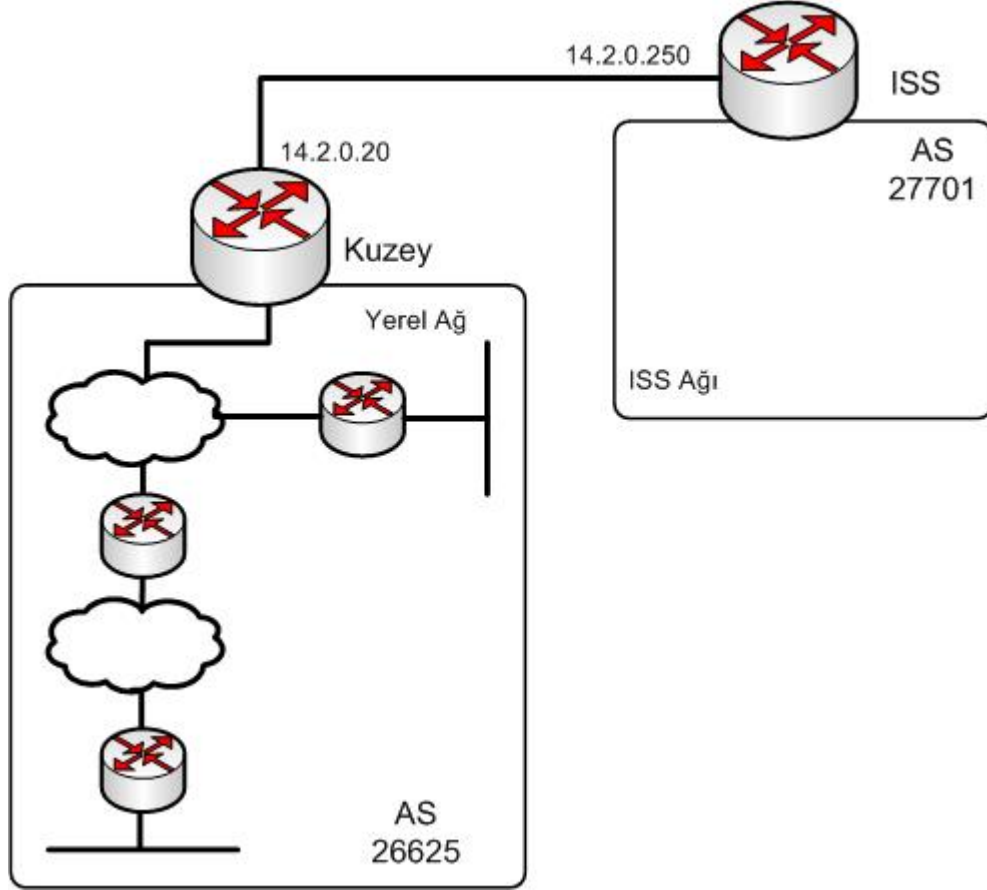
Kuzey, Doğu ve Merkez yönlendiricileri “yönlendirici-3-hepsi” gizli anahtarını paylaşıyorlar ve anahtar ID değerleri 1. Her bir yönlendirici bir birini MD5 kimlik doğrulama yöntemiyle doğrular. Şekil 10.1’de Doğu yönlendiricisinin Kuzey yönlendiricisi ile nasıl kimlik doğruladığı görülmektedir. Doğu birinci olarak başlık ve gövdeden oluşan bir OSPF paketi olarak üretir. Sonra ağ segmentinde kullanılmak üzere bir birincil anahtar alır. Bu durumda anahtar “yönlendirici-3-hepsi” kullanılmıştır. Uygun anahtar ID 1 başlıkta yer alır. Doğu yönlendiricisi başlık alanında 32 bit sıra numarası yer alır. Bu sıra numarası sıralı olarak artırılarak tekrarlama ataklarına karşı koruma sağlanır. Bu işlem sonucunda da iki paketin özetleme değeri aynı olmaz. Sonuç olarak gizli anahtar her bir pakete uygulanır.

Alıcı yönlendirici Kuzey hangi anahtarın özetleme veya imzalama için kullanıldığını belirlemek üzere anahtar ID’sine bakar. Sonra yönlendirici gönderilen paketteki özet değerini üretmek için kendi anahtarını kullanır. Eğer yeni üretilen özet değeri paketle gelenle aynı ise alıcı pakete güvenir diğer türlü ise paket reddedilir.

10.2.3 BGP Kimlik Doğrulaması

BGP protokol yapılandırması oldukça karmaşık ve bu kılavuzun kapsamı dışındadır. Bu kılavuzda BGP protokolü için komşu kimlik doğrulaması ve yönlendirme dalgalanmasının absorbe edilmesi anlatılacaktır.

Şekil 10.2, servis sağlayıcı ve bir ağ arasındaki ilişkiyi göstermektedir. Bu örnekte AS numarası 26625 olan tek bir otonom sistem var. Bu ağ otonom sistem numarası 27701 olan ISS servis sağlayıcısına bağlıdır. Bu örnekte sadece BGP'nin kimlik doğrulaması anlatılacaktır. Yön dağıtma ve diğer ayarlardan bahsedilmeyecektir.



Şekil 10.2 BGP komşuları ve otonom numarası

Kuzey ve ISS yönlendiricileri arasındaki BGP MD5 kimlik doğrulaması güncelleme trafiğini koruyacak, BGP yönlendirme saplama (**injection**) ataklarını ve TCP yeniden başlatma ataklarını engelleyecektir.

Aşağıdaki örnekte Cisco yönlendiriciler için gizli anahtar olarak “yOnlendir04” kelimesi kullanılarak yönlendirici ve ISS yönlendiricisi arasında MD5 kimlik doğrulaması yapılmıştır.

```
Kuzey(config)# router bgp 26625
Kuzey(config-router)# neighbor 14.2.0.250 remote-as 27701
Kuzey(config-router)# neighbor 14.2.0.250 password yOnlendir04
Kuzey(config-router)# end
```

```
Kuzey #
```

Kuzey yönlendiricisinin bağlandığı ISS yönlendiricisinin ayarları ise aşağıdaki şekilde olacaktır.

```
ISS(config)# router bgp 27701
ISS(config-router)# neighbor 14.2.0.20 remote-as 26625
ISS(config-router)# neighbor 14.2.0.20 password yOnlendir04
ISS(config-router)# end
```

BGP yönlendirme dalgalarının absorbe edilmesi yönlendirici BGP yönlendirme tablosunu oluştururken CPU kullanımını ve ağ kararlılığının kontrol edilmesidir. Yön dalgalanması yönlendiricideki bir arayüzün **down-up** sonra **up-down** olması durumudur. Bu da çok sayıda BGP yön güncellenmesine sebep olur. Yönlendirme arayüzünde yapılan ayarlarla yön dalgalanması kontrol edilebilir.

10.2.4 EIGRP Kimlik Doğrulaması

EIGRP protokolünde kimlik doğrulaması MD5 kullanılarak sağlanır. Bu da komşulardan alınan paketin bütünlüğünün garanti altına alınmasını sağlar. EIGRP kimlik doğrulamasını yapılandırmak için aşağıdakiler yapılmalıdır:

- MD5 kimlik doğrulama modu seçilmeli
- EIGRP mesajlar için kimlik doğrulaması etkinleştirilmeli
- Kullanılacak anahtar karakter dizisi, anahtar numarası, anahtar zinciri belirlenmeli
- Anahtar yönetimi yapılandırılmalı (Seçenek)

KAYNAKÇA

- [1] Vanessa Antoine, Raymond Bongiorno, Patricia, Bosmajian, Daniel Duesterhaus, Michael Dransfield, Brian Eppinger, Kevin Gallicchio, Stephen Hamilton, James Houser, Andrew Kim, Phyllis Lee, Tom Miller, David Opitz, Florence Richburg, Michael Wiacek, Mark Wilson, Neal Ziring, *Router Security Configuration Guide*, December 2003, NSA
- [2] J. Michael Stewart, Ed Tittel, Mike Chapple, *Certified Information System Security Professional*, 3. Editron, 2005, Sybex Inc.
- [3] William Stallings, *Data and Computer Communications*, 4. Edition, 1994, Prentice Hall
- [4] Todd Lammle, *Cisco Certified network Associate Study Guide*, 6. Edition, 2007, Wiley Publishing,
- [5] Wendell Odom, *CCNA ICND2*, Second Editon, 2007, Cisco Press
- [6] Juniper Network, *J Series Services Router User Guide*, Version 7.0, 2004, Juniper Inc.
- [7] Pejhan Peymani, Matt Colon, *Junos Router Security*, 2002, Juniper Networks Inc,
- [8] DISA Field Security Operations, *Juniper JUNOS Router Checklist Procedure Guide*, 2005, Defence Information System Agency