T.C.
MİLLİ EĞİTİM BAKANLIĞI

MEGEP

(MESLEKÎ EĞİTİM VE ÖĞRETİM SİSTEMİNİN GÜÇLENDİRİLMESİ PROJESİ)

BİLİŞİM TEKNOLOJİLERİ

ERİŞİM DENETİM LİSTELERİ

ANKARA 2008

Milli Eğitim Bakanlığı tarafından geliştirilen modüller;

- Talim ve Terbiye Kurulu Başkanlığının 02.06.2006 tarih ve 269 sayılı Kararı ile onaylanan, Mesleki ve Teknik Eğitim Okul ve Kurumlarında kademeli olarak yaygınlaştırılan 42 alan ve 192 dala ait çerçeve öğretim programlarında amaçlanan mesleki yeterlikleri kazandırmaya yönelik geliştirilmiş öğretim materyalleridir (Ders Notlarıdır).
- Modüller, bireylere mesleki yeterlik kazandırmak ve bireysel öğrenmeye rehberlik etmek amacıyla öğrenme materyali olarak hazırlanmış, denenmek ve geliştirilmek üzere Mesleki ve Teknik Eğitim Okul ve Kurumlarında uygulanmaya başlanmıştır.
- Modüller teknolojik gelişmelere paralel olarak, amaçlanan yeterliği kazandırmak koşulu ile eğitim öğretim sırasında geliştirilebilir ve yapılması önerilen değişiklikler Bakanlıkta ilgili birime bildirilir.
- Örgün ve yaygın eğitim kurumları, işletmeler ve kendi kendine mesleki yeterlik kazanmak isteyen bireyler modüllere internet üzerinden ulaşılabilirler.
- Basılmış modüller, eğitim kurumlarında öğrencilere ücretsiz olarak dağıtılır.
- Modüller hiçbir şekilde ticari amaçla kullanılamaz ve ücret karşılığında satılamaz.

İÇİNDEKİLER

AÇIKLAMALAR

DERSİN KODU	**481BB0062**
DERSİN ADI	**Ağ Sistemleri ve Yönlendirme**
ALAN	**Bilişim Teknolojileri**
MESLEK/DAL	**Ağ İşletmenliği**
DERSİN OKUTULACAĞI SINIF / YIL	11. sınıf
SÜRE	40/24
DERSİN AMACI	Bu modülün genel amacı: Öğrenci bu modül ile gerekli ortam sağlandığında erişim kontrol listelerini yönetmektir. **Amaçlar** **1.**Erişim denetim listelerinin işlevlerini kavrayıp, erişim denetim listelerini oluşturabilecektir. **2.**Erişim denetim listelerinin çeşitlerini kavrayarak, erişim denetim listelerini yapılandırabilecektir.
DERSİN ÖN KOŞULLARI	TCP/IP iletim katmanı modülünü almış olmak
EĞİTİM ÖĞRETİM ORTAMI VE DONATIM	Ortam: Ağa bağlı İnternet erişimi olan bilgisayar laboratuvarı Donatım: Yönlendirici, Güvenlik duvarı
ÖLÇME VE DEĞERLENDİRME	Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. Modül içinde ve sonunda verilen öğretici sorularla edindiğiniz bilgileri pekiştirecek, uygulama örneklerini ve testleri gerekli süre içinde tamamlayarak etkili öğrenmeyi gerçekleştireceksiniz. Sırasıyla araştırma yaparak, grup çalışmalarına katılarak ve en son aşamada alan öğretmenlerine danışarak ölçme ve değerlendirme uygulamalarına gerçekleştirin.

GİRİŞ

Sevgili öğrenci,

Büyük bir işletmede ağ kullanıcıların gerekli ağ kaynaklarının kullanılmasına izin verileceği gibi birtakım kaynakların da erişiminin kısıtlanması gereklidir. Parolalar, fiziksel güvenlik aygıtları ve bazı yazılımlar, yardımcı birer unsur olmuştur. Ancak temel anlamda ağ yöneticilerinin tercih ettiği temel filtreleme esnekliğinden yoksundurlar. Örneğin ağ yöneticisi İnternet erişimine izin verirken msn Messenger programının kullanımına izin vermeyebilir.

Yönlendiriciler, erişim denetim listeleriyle (EDL) bir tür internet trafiğini denetleme gibi temel trafik filtrelemesi yeteneği sağlarlar. Bir erişim denetim listesi (EDL), üst katman protokolleri ya da adreslere uygulanan izin ya da red durumlarının yer aldığı ardışık bir listedir. Bu modülde ağ trafiğini kontrol amaçlı standart ve uzatılmış EDL'ler tanıtılacak ve onların güvenlik çözümümün bir parçası olarak nasıl kullanılacağı gösterilecektir.

Ek olarak bu bölüm ipuçları, değerlendirmeler, öneriler ve EDL'lerin nasıl kullanılacağına yönelik genel kılavuzlar ile EDL oluşturmada gereksinim duyulan yapılandırma ve komutları içermektedir. Son olarak yine bu bölümde standart ve uzatılmış EDL örnekleri ve onların router arabirimine nasıl uygulandığı gösterilmiştir.

EDL'ler belirli bir host'dan gönderilen paketlere izin verme doğrultusunda tek bir satır kadar yalın olabileceği gibi router erişiminin performansını etkileyen ve trafiği kesin bir şekilde tanımlamaya yönelik son derece karmaşık bir kurallar ve koşullar kümesi de olabilir. Bu bölümde EDL'nin ileri düzey kullanımlarının çoğu, konu dışı bırakılmış olup standart ve uzatılmış EDL hakkında ayrıntı, EDL'nin düzgün yapılandırılması ve bazı özel uygulamalar yer verilmiştir.

ÖĞRENME FAALİYETİ–1

AMAÇ

Erişim denetim listelerinin işlevlerini kavrayıp erişim denetim listelerinin oluşturulma sebeplerini, kurallarını öğreneceksiniz.

ARAŞTIRMA

- Ağlarda filtreleme konusu inceleyiniz
- Ağlarda trafik akışını kontrol etmek neden önemlidir?

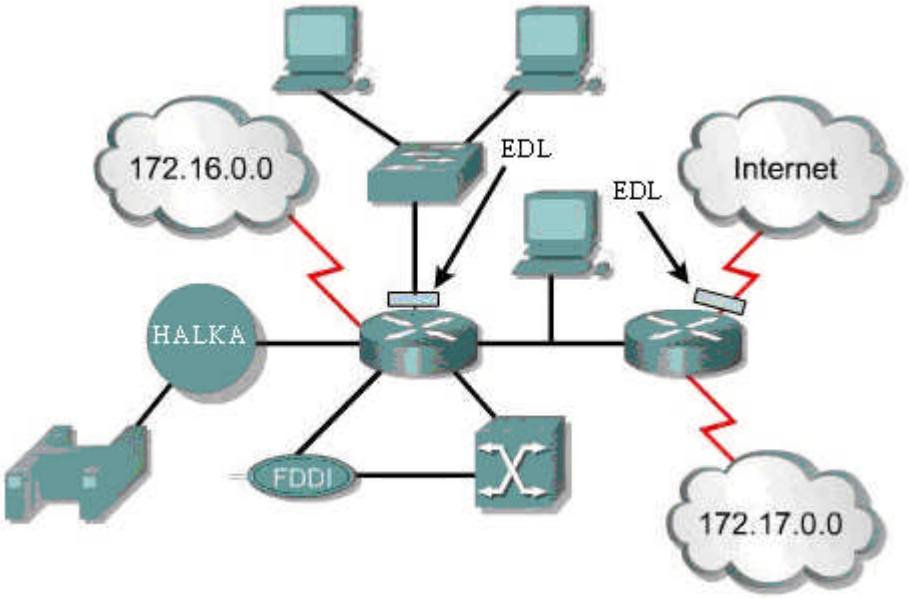
1. ERİŞİM DENETİM LİSTELERİ OLUŞTURMA

1.1. Erişim Denetim Listesi

EDL (ACL, Access Control List)'ler bir yönlendirici arabirimi üzerinde geçiş yapan veri trafiğine uygulanacak koşullar listesidir.

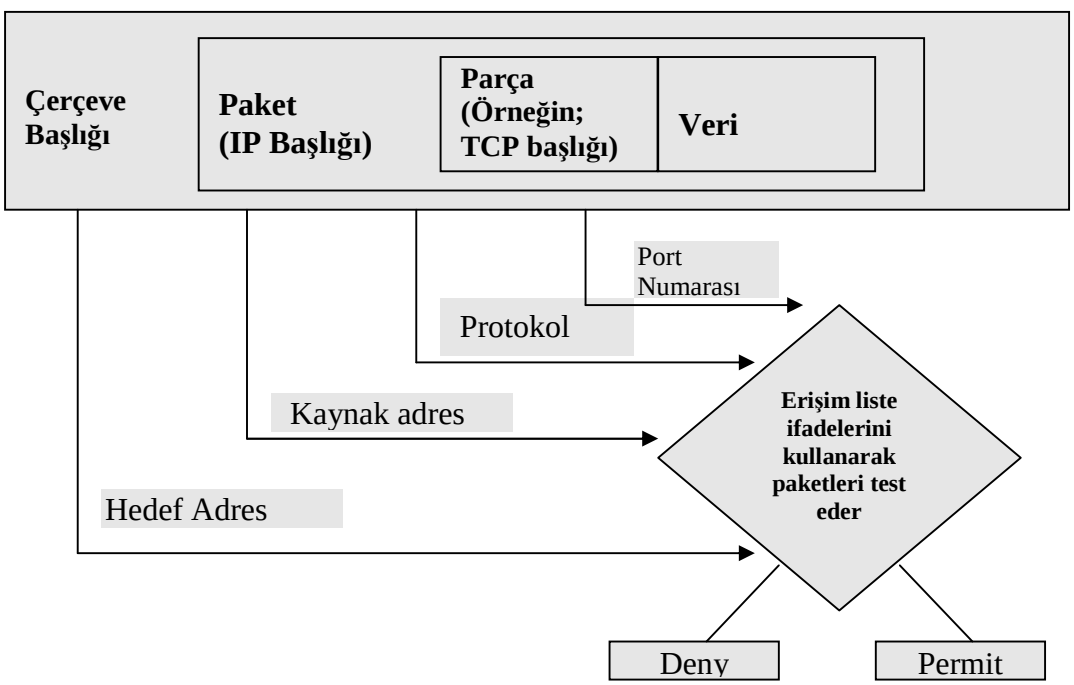
Bu listeler, yönlendiriciye hangi tip veri paketlerinin kabul ya da red edileceğini söyler. Kabul ya da red listelerdeki koşullara bağlıdır. EDL'ler trafiğin yönetimini mümkün kılar ve bir ağa ya da ağdan yapılacak erişimi güvenli hâle getirir.

EDL'ler, İnternet Protokolü (IP) ve İnternet İş Paket Değişimi (IPX) gibi her tür yönlendirilmiş ağ protokolleri için oluşturulabilir. EDL'leri bir ağa ya da alt ağa erişimini kontrol için yönlendirici üzerinde yapılandırılırlar.



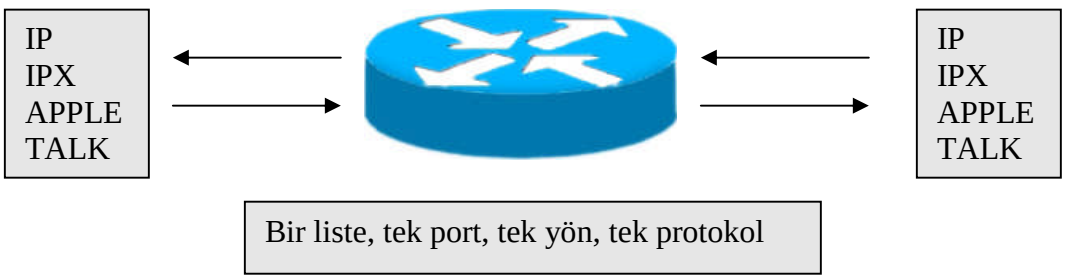
Resim 1.1: Erişim denetim listesi

EDL'leri yönlendirilmiş paketlerin gönderilmiş ya da bir yönlendirici arabiriminde bloke edilmiş olup olmadığını kontrol etmek suretiyle ağ trafiğini filtreler. Yönlendirici, EDL'de belirtilen koşullara dayalı olarak gönderilmiş mi yoksa düşmüş mü olduğunu saptama amacıyla her paketi inceler. EDL'nin karar vereceği noktalarından bazıları, veri paketinin gideceği adresin, protokollerin ve üst katman portun numaralarıdır.



Şekil 1.1: IP Paketi

EDL'ler protokol, yön ya da port temelli olarak tanımlanmalıdır. Bir arabirim üzerindeki trafik akışını kontrol etmek için arabirim üzerinde çalışır durumdaki her bir protokol için bir EDL tanımlanmalıdır. EDL'ler trafiği arabirim üzerinde, tek bir yönde ve tek zamanda kontrol ederler. Her farklı yön için ayrı ayrı bir EDL oluşturulmalıdır; giriş trafiği için bir tane, çıkış trafiği için bir tane. Sonuç itibarıyla her bir arabirim çok sayıda protokole ve tanımlanmış yöne sahip olabilir. Eğer yönlendirici IP ve IPX için konfigüre edilmiş iki arabirime sahip ise 12 farklı EDL gerekecektir. Her protokol için bir EDL, giriş ve çıkış doğrultusu için iki defa ve port sayısı için iki defa gerekecektir.



Şekil 1.2: Liste

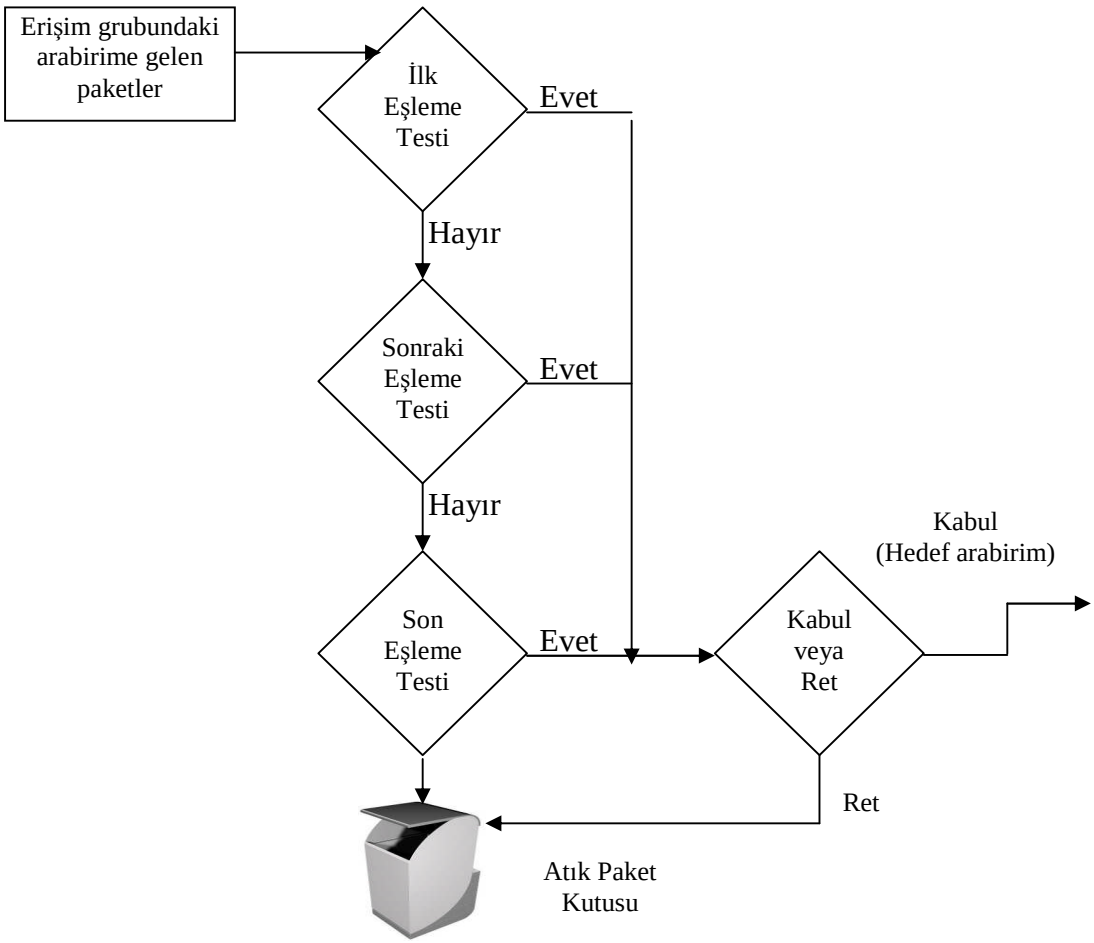
EDL oluşturmanın birincil nedeni şunlardır:

- Ağ trafiğini sınırlamak ve ağ performansını artırmak. Örneğin EDL'ler video trafiğini sınırlamak suretiyle ağdaki yükü büyük ölçüde azaltır ve neticede ağ performansını artırır.
- Trafik akışı kontrolünü sağlamaktır. EDL'leri gönderi yenilemelerinin dağıtımını sınırlayabilir. Eğer yenilemeler ağ koşulları nedeniyle gerekli değilse bant genişliği muhafaza edilir.
- Ağ erişiminde temel bir güvenlik düzeyi sağlamak. EDL'leri bir host'un ağın bir kısmına erişmesine izin verebilir ve diğer bir host'un aynı bölgeye erişimini engelleyebilir. Örneğin, host A'nın insan kaynakları ağına erişimine izin verilirken, host B'nin oraya erişimi engellenebilir.
- Yönlendirici arabirimlerinde hangi tip trafiğe yol verileceği ya da bloke edileceğine karar verir. E-Posta trafiğinin gönderime izinli olması ama tüm telnet trafiğine blokludur.
- Bir yöneticiye, bir istemcinin ağa hangi alanda erişebileceğini kontrol etmek iznini verir.
- Ağın belli bir kısmına erişim izni olsun ya da olmasın bazı hostları ekranda görüntüler. Sadece FTP ya da HTTP gibi belli başlı dosyalarda erişim için kullanıcı iznini onaylar ya da reddeder.

Eğer EDL'leri yönlendirici üzerinde konfigüre edilmezlerse yönlendirici içinden geçen her pakete, ağın her yanına ulaşması için izin verilecektir.

1.1.1. Erişim Denetim Listelerinin Çalışması

Bir EDL, bir verinin giriş ve çıkış arabirimi sınırlarında kabul ya da reddedileceğini tanımlayan bildirimler grubudur. Bu kararlar, bir erişim listesindeki koşul bildirimlerinin karşılaştırılması ile gerçekleşir ve ardından bildirimde tanımlanan kabul ya da ret eylemi uygulanır.



Şekil 1.3: Paketlerin eşlenmesi

EDL'leri hangi sırada konumlandırılacağı önemlidir. ROS yazılımı, paketleri her koşul bildirimi karsısında en tepeden en alta kadar test eder. Listede bir eşleşme olduğunda kabul ya da ret eylemi icra edilir ve diğer EDL bildirimleri kontrol edilmez. Tüm trafiğe topyekûn izin veren bir koşul bildirimi listenin en basında yer alıyorsa daha alttaki bildirimler asla kontrol edilemeyecektir.

Eğer bir erişim listesinde ilaveten koşul bildirimleri gerekiyorsa, tüm EDL listesi silinmeli ve yeni koşul bildirimleriyle tekrar oluşturulmalıdır. Bir EDL'lerini yenilemeyi kolaylaştırma konusunda Notepad gibi bir editör kullanmak ve EDL'sini yönlendirici yapılandırmasına yapıştırmak iyi bir fikirdir.

EDL'ler kullanılsın ya da kullanılmasın, yönlendirici işlemlerinin başlangıcı aynıdır. Bir çerçeve gibi arabirim girer, yönlendirici iki adres katmanının eşleşip eşleşmediğini ya da gösterim çerçevesi olup olmadığını kontrol eder. Eğer çerçeve adresi kabul edilirse çerçeve bilgisi çıkartılır ve yönlendirici inbound bir arabirim üzerinde EDL olup olmadığını kontrol eder. Eğer mevcut bir EDL varsa, paket o anda listede yer alan bildirimler doğrultusunda test edilir. Eğer paket bir bildirimle eşleşirse paketi kabul ya da ret işlemi gerçekleşir. Eğer paket arabirimde kabul edilirse bu durumda alıcı, arabirimin saptanması ve arabirime yöneltilmesi için paket gönderi tablosu girişleri doğrultusunda kontrol edilir. Sonrasında yönlendirici, alıcı arabirimin bir EDL'si olup olmadığını kontrol eder. Eğer mevcut bir EDL varsa, paket o anda listede yer alan bildirimler doğrultusunda test edilir. Eğer paket bir bildirimle eşleşirse paketi kabul ya da ret işlemi gerçekleşir. Eğer EDL yoksa ya da paket kabul edilmiş ise paket ikinci yeni katman protokolüne alınır ve bir sonraki aygıta gönderilmek üzere arabirim dışına yönlendirilir.

Genel görünüş itibarıyla EDL bildirimleri ardışık ve mantıksal bir düzende çalışır. Eğer bir koşulun doğruluğu eşleşiyorsa pakete izin verilir ya da tam tersi reddedilir ve EDL bildirimlerinin diğerleri kontrol edilmez. Eğer EDL bildirimlerinin hiçbiri eşleme göstermiyorsa listenin en sonuna varsayılan bir değer olarak gizli bir "hepsi ret" bildirimi yerleştirilir. Liste sonundaki bu bildirim, EDL'nde eşleşme sağlamayan hiçbir paketin kabulüne olanak sağlamayacaktır. "hepsi ret" değeri bir EDL'sinin son satırı gibi görünür olmamasına karşın orada olacaktır. EDL'de eşleşme göstermeyen hiçbir paketin kabulüne izin vermeyecektir. EDL' lerin nasıl oluşturulacağını ilk öğrenirken komut satırının dinamik varlığını güçlendirmek için EDL'nin sonuna gizli bir ret eklemek iyi bir fikirdir.

1.2. Erişim Denetim Listelerinin Oluşturulması

EDL'ler dünya çapında yapılandırma modunda oluşturulur. Standart, uzatılmış, IPX, Apple Talk ve başka diğerlerini de içeren çok farklı tiplerde EDL'ler vardır. Bir yönlendirici üzerinde EDL'leri konfigüre ederken her EDL kendisine atanan bir rakamla kendine özerk tanımlanmalıdır. Bu rakam, oluşturulan erişim listesinin tipini tanımlar.

ACL Tipleri	ACL NUMARALARI
IP Standard	1–99, 1300–1999
Standard Vines	1–99
IP Extended	100–199, 2000–2699
Extended Vines	100–199
Bridging type code (layer–2)	200–299
DECnet	300–399
Standard XNS	400–499
Extended XNS	500–599
AppleTalk	600–699
Bridging MAC address and vendor code	700–799
IPX Standard	800–899
IPX Extended	900–999

IPX SAP filters	1000–1099
Extended transparent bridging	1100–1199
IPX NLSP	1200–1299

Tablo 1.1: ACL tipleri ve numaraları

Doğru komut moda girildikten ve liste tip numarasına karar verildikten sonra, kullanıcı uygun parametreleri takiben, **access-list** anahtar sözcüğünü kullanarak erişim listesi bildirimlerini girer. Erişim listesi oluşturma işi onları yönlendirici üzerinde kullanmanın ilk yarısıdır. İşlemin ikinci yarısı ise onların doğru arabirimlere atanmasıdır.

1.2.1. Erişim Denetim Listelerinin Genel Yazım Biçimi

Router(config)# **access-list** ACL_# **permit|deny koşul**

Genel bir EDL tanımlama adımı bu şekildedir. Özellikle 1–99 ve 1300–1999 arası kullanılan numaralar tablo da görüldüğü gibi standart erişim listelerini tanılamada kullanılır. Bu adımdaki koşul yönlendirici tarafından kabul veya red işlemi yürütüldüğünde paketlerin içeriklerinin nelere göre eşleme yapılması gerektiğini yönlendiriciye söyler.

Router(config-if)# **ip access-group** ACL_# **in|out**

EDL'ler bir ya da daha fazla arabirime atanabilir ve **access-group** (erişim-küme) komutu kullanılarak giriş ve çıkış trafiğini filtreleyebilir. İn ve out parametresi yönlendirici arabirimine giriş ve çıkış trafiğini simgeler.

```
Router(config)#
Router(config)# access-list 2 deny    192.168.1.2
Router(config)# access-list 2 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 2 deny     192.168.0.0 0.0.255.255
Router(config)# interface serial 0
Router(config-if)# ip access-group 2 in
```

Access-group komutu arabirim yapılandırmasına iletilir. Bir giriş ya da çıkış arabirimine herhangi bir EDL atandığında konumlandırma özelleştirilmelidir. Filtreleme yönü içeri ya da dışarı giden paketleri kontrol için ayarlanabilir. EDL'nin giriş trafiği mi yoksa çıkış trafiğine mi adreslenmiş olduğunu saptarken ağ yöneticisi yönlendiricinin içinden gelen arabirimlere göz atma gereği duyabilir. Bu çok önemli bir düşüncedir. Bir arabirimden gelen trafik giriş erişim listesince, arabirimden çıkan trafik de çıkış erişim listesince filtrelenir. Numaralandırılmış bir EDL oluşturulduktan sonra bir arabirime ataması yapılmalıdır. Numaralandırılmış EDL bildirimleri içeren bir EDL değiştirilecekse içindeki tüm bildirimler **no access-list** / liste no komutu kullanılarak silinmelidir.

Router(config)# **no access-list 2**

Erişim listeleri oluşturulurken ve uygulanırken şu temel kurallar takip edilmelidir:

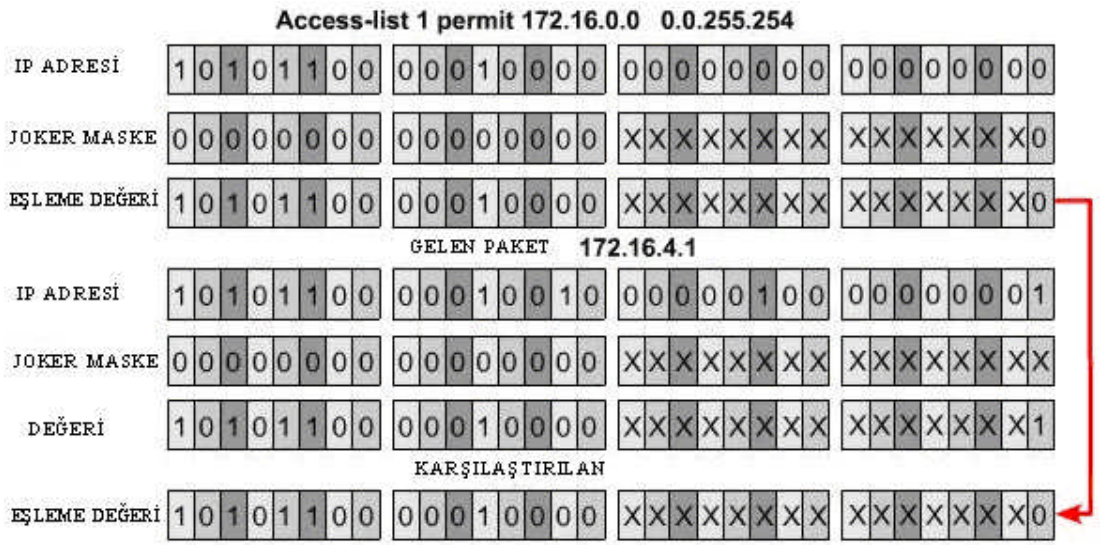
- Protokol ve yön temelli bir erişim listesi olmalıdır.
- Standart erişim listesi alıcı adresine en yakın olmalıdır.
- Uzatılmış erişim listesi kaynağa en yakın olmalıdır.
- Giriş ve çıkış arabirim referansları yönlendiricinin içinden sanki "porta bakıyormuş" gibi kullanılmalıdır.
- Bildirimler, bir eşleme gerçekleşene kadar listenin en başından en sona kadar ardışık olarak gerçekleşecektir. Eğer eşleşme olmaz ise paket reddedilecektir.
- Erişim listesinin sonunda gizli bir ret olacaktır. Bu normal olarak yapılandırma listelemesinde ekranda görüntülenmez.
- Erişim listesi girişleri özelden genele bir sıra içinde filtrelenmelidir. Önce özel hostlar reddedilmeli ve sonrada gruplar ya da genel filtrelemeler gelmelidir.
- Eşleşme koşulu ilk önce incelenir. İzin ya da ret sadece eşleşme doğru ise incelenir.
- Bir erişim listesi aktif olarak uygulamadayken üzerinde asla çalışmayın.
- Mantıksal çıkış yorumları oluştururken bir metin editörü kullanın ve ardından mantıksal koşulu icra eden bildirimleri tamamlayın.
- Erişim listesinin sonuna daima yeni satırlar eklenir. **No access-list x** komutu tüm listeyi silecektir. Numaralandırılmış bir EDL'si seçerek silme ya da ekleme mümkün değildir.
- Bir erişim listesi silinirken dikkatli olunmalıdır. Eğer erişim listesi bir ürünün arabirimine uygulanır ve silinirse ROS'un sürümüne bağlı olarak arabirime default (varsayılan) bir ret uygulanır ve dolayısıyla tüm sistem durur.
- Çıkış filtrelemesi yerel yönlendiriciden kaynaklanan trafiği etkilemez.

1.2.2. (wildcard mask) Joker Maske'nin İşlevi

Joker maske (wildcard mask), dört sekizliğe bölünmüş bir 32 bittir. Joker maskesi bir IP adresi ile eşleşir. Maskedeki sıfır ve birler, IP adres bitleriyle nasıl haberleşeceğini tanımlamak için kullanılır. Wildcard maskelemesi terimi tıpkı bir arama işleminde tüm karakterler yerine kullanılabilen joker karakterler mantığında olup EDL' nin mask-bit eşleşmesi için bir tür takma addır (nickname). Joker maskelerinin alt ağ maskeleriyle işlevsel bir ilişkisi yoktur. Onlar farklı amaçlar ve farklı kurallar doğrultusunda kullanılır. Alt ağ maskeleri IP adresinin sol tarafından başlar ve host alanından ödünç bitler almak suretiyle ağda genişlemek için sağ tarafa doğru ilerler. Joker maskeleri, adrese bağlı olarak kaynaklara erişimi kabul ya da red eden bireysel veya grup IP adreslerini filtrelemek için tasarlanmıştır. Joker maskelerinin alt ağ maskeleriyle nasıl ilişkilendirilip çalıştırılacağını düşünmek sadece kafa karıştır. Joker maske ile alt ağ maskesi arasındaki tek benzerlik her ikisinin de otuz iki bit uzunlukta olması ve maskelemede sıfır ve birleri kullanıyor olmasıdır.

Diğer bir açıdan, joker maskesindeki sıfır ve birler, alt ağ maskesindekilerden çok farklıdır. (2); Bu karışıklığı gidermek için, grafikte joker maskesindeki 1'lerin yerine X'ler konmuştur. Bu maskeleme 0.0.255.255 olarak yazılabilirdi. Buradaki sıfırın anlamı, kontrol

edilecek değerlere izin vermek, X'lerin (yani 1'lerin) anlamı ise karşılaştırılan değerlerin bloklanmasıdır.



Resim 1.2: joker maske eşleme

Joker maskesi işleminde, erişim listesi bildiriminde yer alan ip adresi kendisine uygulanmış bir joker maskesine sahiptir. Bu, bir paketin EDL tarafından işleme konup konmayacağını görmede ve karşılaştırmada kullanılacak bir değer üretir ya da bir sonraki bildirimi kontrol amacıyla gönderir. EDL işleminin ikinci kısmı, belli bir EDL bildirimince kontrol edilmiş olan herhangi bir IP adresinin bildirim tarafından ona uygulanacak olan joker maskesinin alınmasıdır. IP adresinin ve joker maskesinin sonucu EDL'nin değerini eşlemede eşit olmalıdır. Bu işlem çizimde gösterilmiştir.

IP Adresi	Joker maske	Eşleme
0.0.0.0	255.255.255.255	Bütün adresi eşler (any)
172.16.1.1	0.0.0.0	Sadece 172.16.1.1 adresini eşler.
172.16.1.0	0.0.0.255	Sadece 172.16.1.0/24 adresini eşler. (172.16.1.0–172.16.1.255)
172.16.2.0	0.0.1.255	172.16.2.0/23 deki adresleri eşler. (172.16.2.0–172.16.3.255)
172.16.0.0	0.0.255.255	172.16.0.0/16 deki adresleri eşler. (172.16.0.0–172.16.255.255)

Tablo 1.2: joker maske örneği

EDL'lerde kullanılan iki özel anahtar sözcük vardır. Bunlar; any ve host seçenekleridir. Basit şekliyle, any seçeneği IP adresi için 0.0.0.0 in yerini, joker maskesi için de 255.255.255.255'in yerini tutar. Bu seçenek, karşılaştırılmış olan herhangi bir adresi eşleştirecektir. Host seçeneği, 0.0.0.0 maskesinin yerini tutar. Bu maske, EDL adresinin tüm

bitlerine ve paket adresinin eşleşmiş olmasına gerek duyar. Bu seçenek tek bir adresi eşleştirecektir.

Router(config)# **access-list 2 permit 0.0.0.0 255.255.255.255**

Yukarıdaki adım yerine

Router(config)# **access-list 2 permit any** yazılabilir.

Router(config)# **access-list 2 permit 192.168.1.2 0.0.0.0**

Komut adımı yerine de aşağıdaki adım yazılabilir

Router(config)# **access-list 2 permit host 192.168.1.2**

Yönlendirici üzerinde EDL'lerin yerleşimini ve içeriğini doğrulamak için pek çok **show** komutu vardır.

Show ip interface komutu, IP arabirim bilgilerini görüntüler ve herhangi bir EDL' nin kurulu olup olmadığını belirtir. **Show access-list** komutu yönlendirici üzerindeki tüm EDL'lerin içeriğini görüntüler. Özel bir listeyi görmek için, bu komutla birlikte seçenek olarak EDL adını ya da numarasını eklemek gerekir. **Show running-config** komutu da yine yönlendirici üzerindeki erişim listesini ve arabirim atama bilgilerini ortaya çıkaracaktır.

```
Router#show access-lists
Standard IP access list 2
 deny   172.16.1.1
 permit 172.16.1.0, wildcard bits 0.0.0.255
 deny   172.16.0.0, wildcard bits 0.0.255.255
 permit 172.0.0.0, wildcard bits 0.255.255.255
Extended IP access list 101
 permit tcp 192.168.6.0 0.0.0.255 any eq telnet
 permit tcp 192.168.6.0 0.0.0.255 any eq ftp
 permit tcp 192.168.0.0 0.0.0.255 any eq ftp-data
Router#
```

Resim 1.3: Show access-lists komutu

Bu show komutları, liste içeriklerini ve yapılanmalarını doğrulayacaktır. Erişim listesi mantığını kavramak için örneksel bir trafik üzerinde çalışmak yararlı olacaktır.

1.3. Erişim Denetim Listelerinin Düzenlenmesi

Bir EDL'nin oluşturulması ve yürütülmesi karmaşık işlem olabilir. Bu kısımda EDL ifadesinin eklenmesi, değiştirilmesi veya silinmesi üzerine düzenlemeleri öğreneceksiniz.

İlk olarak EDL'nin belirli bir bölümünü silemezsiniz, sadece giriş listesini silebilirsiniz. Bu ifade numaralı EDL'ler için geçerlidir fakat adlandırılmış EDL' ler için geçerli değildir. Bir EDL'yi silmek için **no access-list** komutunu kullanmanız gerekir. Bu giriş listesini siler. Eğer ki listenin belirli bir bölümünü silmeyi denediğinizde yönlendirici komut parametrelerinin sadece ilk üçünü çalıştıracak, **no access-list** ACL# . İkinci olarak erişim listesinin başına veya ortasına kontrol ekleyemezsiniz. Komut adımına bir giriş yaptığınızda bu komut listenin sonuna eklenecektir. Üçüncü olarak bir EDL'de var olan bir denetimi değiştiremezsiniz. Yönlendirici üzerinde zamanla bazı noktalarda EDL girişlerinin eklenmesi, silinmesi veya değiştirilmesi ihtiyacı duyacaksınız. Aşağıdaki adımları yerine getirdiğinizde liste işlemlerini kolaylıkla yönetebileceksiniz.

1. **show running-config** komutunu girin ve scroll down ile EDL girişlerini bulunuz.
2. Farenizle EDL komutlarını seçin ve kopyalayın.
3. EDL komutlarını Notepad benzeri bir yazı editörüne yapıştırın.
4. Yazı editöründeki EDL'yi düzenleyin; (ekleme,silme ve değiştirme girişlerini)
5. Yazı editöründeki EDL'yi seçin ve kopyalayın.
6. Yönlendiricideki arabirime EDL uygulamasını kaldırın.

   no ip access-group ACL# in/out

7. Eski erişim listesini silin.

   no access-list ACL_#

8. EDL'yi yapılandırma moduna kopyalayın. Bunu yaptığınızda, yönlendirici her ifadeyi ayrı olarak kabul edecek ve işleyecek. EDL komutlarında bir yazım hatası ile karşılaşırsa yönlendirici size uyarı verecektir. Bu durumda 4. adıma dönünüz.
9. Yönlendiricideki EDL'yi harekete geçirmek için:

   ip access-group *Interface Subconfiguration* modu komutunu kullanınız.

Bunun yerine EDL'yi silip el ile tekrardan listeyi girmeye kalktığınızda liste başında yaptığınız bir hata yüzünden bütün hepsini silmek zorunda kalabilirsiniz.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ (Komut Satırına Aşağıdaki Adımları Sırasıyla Giriniz) Router(config)# **access-list 1 deny 88.226.104.1**	➢ Daha önce liste 1'in kayıtlı olmaması gereklidir. ➢ **Show running-config** komutunu kullanarak kontrol edin. ➢ **Eğer varsa;** ➢ **no ip access-group 1'in** ➢ **komutunu kullanarak listeyi silin.**
➢ Router(config)# **access-list 1 permit 88.226.104.0 0.0.0.255**	
➢ Router(config)# **interface serial 0**	
➢ Router(config-if)# **ip access-group 1 in**	

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki soruları cevaplayarak faaliyette kazandığınız bilgi ve becerileri ölçünüz.

Aşağıdaki cümleleri doğru ifade olacak şekilde kelime veya sayılarla doldurunuz.

1) Bir EDL, arabirimin giriş ve çıkış sınırlarında _____ ya da _____edebileceğini tanımlayan bildirim grubudur.

2) EDL'de en son satıra gizli bir _____ _____ bildirimi yerleştirilir.

3) Joker maske _____ sekizliğe bölünmüş _____ bitliktir.

4) Bir adresteki bütün bitlerin hepsini eşleyecek değeri giriniz _____

Aşağıdaki soruların cevaplarını "doğru" ve "yanlış" olarak değerlendiriniz.

5) Erişim denetim listelerini hangi arabirime atandığı önemli değildir. ( )

6) Yeni bir EDL oluşturulmadan, önce eski liste silinmelidir. ( )

7) EDL'ler protokol, yön ya da port temelli tanımlanmalıdır. ( )

Aşağıdaki sorularda doğru olan seçeneği işaretleyerek değerlendiriniz.

8) Aşağıdakilerden hangisi EDL oluşturmanın nedenlerinden değildir?

A) Ağ trafiğini sınırlamak
B) Ağ trafiğinin performansını artırmak
C) Ağ erişiminde temel güvenlik düzeyini sağlamak
D) Uzaktaki ağları yönetmek

9) Aşağıdaki ifadelerden hangisi EDL'ler için doğrudur?

A) Adımların düzenlenmesi otomatiktir.
B) Bütün adımlar işlenir.
C) Eşleme bulunmaz ise paket kabul edilir.
D) Adlandırılmış bir listede istenilen adımı silebilirsiniz.

10) Aşağıdakilerden hangi komut yönlendirici arabirimindeki bir IP EDL'sini aktifleştirir?

A) access-list
B) ip access-group
C) access-class
D) access-group

ÖĞRENME FAALİYETİ–2

AMAÇ

Bu faaliyette EDL'lerin çeşitlerini ayrıntılı bir şekilde öğrenecek ve aralarında temel farklılıkları kavrayacaksınız. Ayrıca erişim denetim listelerinin nasıl yerleştirilmesi gerektiği hakkında bilgi edineceksiniz. Son olarak sanal terminalin kısıtlanmasını öğreneceksiniz.

ARAŞTIRMA

- 1.UDP ve TCP'de kullanılan port isimlerini ve numaralarını araştırınız?
- 2.Sanal port nedir? Nerelerde kullanılır?

2. ERİŞİM DENETİM LİSTELERİ

2.1 ERİŞİM DENETİM LİSTELERİ ÇEŞİTLERİ

Bu bölümde, numaralı ve adlandırılmış EDL'lerin yapılandırılmasını öğreneceksiniz. İlk olarak iki kısımdan meydana gelen standart ve genişletilmiş olarak adlandırılan numaralı EDL'lerin yapılandırılmasını öğreneceksiniz. Daha sonra adlandırılmış EDL'lerin yapılandırılmasını inceleyeceğiz.

2.1.1 Standart Erişim Listeleri

Standart EDL'ler yönlendirilmiş IP paketlerinin kaynak adresini kontrol ederler. Ağa, alt ağa ve host adreslerine bağlı olarak topyekûn protokol için karşılaştırma izin ya da red ile sonuçlanacaktır. Örneğin, Fa0/0'dan gelen paketler kaynak adresi ve protokolü için kontrol edilecektir. Eğer izin verilmişse paketler yönlendiricide doğru bir çıkış arabirimine yönlendirilecektir. Eğer izin verilmemişse daha giriş arabirimindeyken düşeceklerdir.

2.1.1.1 Standart Erişim Listelerinin Genel Yazım Biçimi

Access-list [liste numarası] [permit | deny] [IP adresi] [joker maske(isteğe bağlı)]

Bileşenler:
Liste numarası
Erişim liste numarası 1'den 99 ve 1300 den 1999'a kadar olabilir.

Permit | deny
Her ikisi de olabilir. Permit belirttiğiniz ip adresini, bir eşleme girişini içerir.

IP adresi
Bir IP adresi, belirlenmiş kuralları içeren IP adreslerini eşlemede ve kararlaştırmada kullanılır.

Joker maske
İsteğe bağlı olarak kullanılan joker maske eşlemede bir IP adresindeki bitlerin değerlerini (0/1) kontrol eder.

Şu ana kadar standart erişim listesi oluşturmada ve aktifleştirmek için iki komut ile tanıştık (permit= kabul, deny=red). Bunları kullanarak daha iyi kavramanıza yardımcı olacaktır. Aşağıdaki örneğe bakalım.

Router(config)# **access-list 1 permit 192.168.1.1**
Router(config)# **access-list 1 deny 192.168.1.2**
Router(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**
Router(config)# **access-list 1 deny any**
Router(config)# **interface serial 0**
Router(config-if)# **ip access-group 1 in**

Bu örnekte EDL'nin en başında bulunan permit işlemi düzenli bir şekilde yürütüldüğünde IP paketinde kaynak adresin 192.168.1.1 olmalıdır. Eğer değilse yönlendirici ikinci adıma geçecektir. Standart EDL'de joker maskesi kullanmadığınızda varsayılan olarak 0.0.0.0 idi ve EDL satırındaki adreste tam olarak eşleştirme yaptığını hatırlayın. EDL'nin ikinci satırı deny işlemi yürütüldüğünde IP paketinde kaynak adres 192.168.1.2 olmalı, değilse yönlendirici üçüncü satıra geçecek. EDL deki üçüncü satırda permit işlemi yürütüldüğünde IP paketinde kaynak adres 192.168.1.0 ile 192.168.1.255 arasında olmalıdır. Değilse dördüncü satıra geçecektir. Dördüncü satır genelde gerekli değildir, çünkü bütün IP paketlerini düşürecektir. Bu adıma her EDL'nin sonunda gizli olarak belirtilen bir red işlemi olmadığı sürece ihtiyacınız yok demektir. Yukarıdaki EDL örneğinde son iki komut serial0' dan arabirime gelen trafiği EDL#1'de aktifleştirecektir. Aslında aşağıdaki gibi yazılmış olması gerekirdi.

Router(config)# **access-list 1 deny 192.168.1.2**
Router(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**
Router(config)# **interface serial 0**
Router(config-if)# **ip access-group 1'in**

Bu düzenleme listeniz dört satır olacak ve iki satır düşmüş olacaktır. Bu da yönlendiricinizin performansını artıracaktır. Şimdi aşağıdaki başka bir örneğe bakalım:

Router(config)# **access-list 2 deny 192.168.1.0**
Router(config)# **access-list 2 deny 172.16.0.0**
Router(config)# **access-list 2 permit 192.168.1.1**
Router(config)# **access-list 2 permit 0.0.0.0 255.255.255.255**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 1 out**

Bu örnekte birkaç problem var; üzerinde düşünün ve arkadaşlarınızla belirlemeye çalışın.

İlk adımda 192.168.1.0/24'den gelen bütün trafiği red edecek diye görünüyor. Gerçekte, başarıya ulaşamayacak. Joker maskeyi atladığınızda varsayılan olarak 0.0.0.0 olarak tam bir eşleme yapıldığını hatırlayın. 192.168.1.0 bir ağ adresi, numarası veya tek kullanıcı adresi değilse kaynak adresten hiçbir paket alınamayacak ve problem olacaktır. İkinci adımda da aynı problem mevcuttur. 3 ve 4. adımlar normaldir.

Görüldüğü gibi EDL yapılandırması büyük bir hassasiyet gerektirmektedir. Yukarıdaki EDL'nin güncelleştirilmiş hâli aşağıdaki gibi olmalıdır.

Router(config)# **access-list 2 deny 192.168.1.0 0.0.0.255**
Router(config)# **access-list 2 deny 172.16.0.0 0.0.255.255**
Router(config)# **access-list 2 permit 192.168.1.1**
Router(config)# **access-list 2 permit 0.0.0.0 255.255.255.255**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 1 out**

Yukarıda ki örnekte kaynak IP adresi 92.168.1.0/24 ağından olan her paket düşecektir. İkinci adımda 172.16.0.0/16 ağındaki B sınıfı trafiğinden her biri düşecektir. Üçüncü adımda 192.168.1.1'deki trafiğe izin verilecektir. Dördüncü adımda her yerden trafiğe izin verilecektir. Aslında birinci ve üçüncü adıma bakıldığında hâlen bir problem vardır. Üçüncü adım yürütüldüğünde işlem yapacak mıdır? "Hayır" derseniz; ayağınızı kaldırın, bildiniz. Bu durumda özel girişlerden önce daha detaylı olanları yapmalısınız. Bir diğer nokta, listenin dördüncü adımını önemsiz yapan adreste **any** anahtar kelimesinin kullanılmamasıdır. Aşağıda yapılandırmanın güncellenmiş hâline bakalım.

Router(config)# **access-list 2 permit 192.168.1.1**
Router(config)# **access-list 2 deny 192.168.1.0 0.0.0.255**
Router(config)# **access-list 2 deny 172.16.0.0 0.0.255.255**
Router(config)# **access-list 2 permit any**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 1 out**

Aslında EDL'de bir tane daha sorunumuz var. Arabirim üzerinde kullanılan EDL numarasını yanlış tahmin ettiyseniz sonra doğru düzeltebilirsiniz. Uyarı: Arabirimdeki EDL uygulaması 1'i kullanıyorsa EDL 2 numarasını meydana getirecektir. Bunu düzeltmek için aşağıdaki yapılandırmayı kullanın:

Router(config)# **interface ethernet 0**
Router(config-if)# **no ip access-group 1 out**
Router(config-if)# **ip access-group 2 out**

Yeni EDL'yi uygulamadan önce arabirim üzerinde eski EDL'yi kaldırmak zorunda olduğunuzu unutmayın.

2.1.2 Genişletilmiş Erişim Denetim Listeleri

Uzatılmış EDL'ler, geniş bir kontrol aralığı sağladığı için standart EDL'lerden daha sık kullanılırlar. Uzatılmış EDL'ler port numaraları ve protokolleri de kontrol edebileceği gibi paketin kaynağını ve alıcı adresini de kontrol eder. Bu, EDL'nin neyi kontrol edeceğini tanımlama konusunda büyük bir esneklik sağlar. Erişim izni ya da reddi verilen paketler, protokol tipi ve port adresinin yani sıra, paketin nereden çıktığı ve nereye yollandığına dayalıdır. Uzatılmış bir EDL, Fa0/0'dan özel bir S0/0 adresine yapılacak olan mail trafiğine dosya transferi ve web tarayıcı reddi olma koşuyla izin verir. Paketler göz ardı edildiğinde, bazı protokoller göndericiye alıcı adresine ulaşılamadığını bildiren bir yankı paket yollar.

Tek bir EDL için, birden çok bildirim düzenlenebilir. Bu bildirimlerin her biri, bildirimi aynı EDL' ye ilintilendirmek için aynı erişim listesi numarası içermelidir. Gerektiği ölçüde koşul bildirimlerinin sayısı artabilir, bu sayıyı sınırlayan sadece yönlendiricinin kullanılabilir belleğidir. Doğal olarak bildirimlerin artırılması EDL'nin yönetimini ve anlaşılmasını daha bir zorlaştıracaktır.

2.1.2.1 Genişletilmiş Erişim Listelerinin Genel Biçimi

Şimdi genişletilmiş erişim listelerinin tipik olarak kullanımlarının genel biçimini tanımlayalım. Genişletilmiş erişim listeleri aşağıdaki biçimi alır:

Access-list [liste numarası] [permit | deny] [protokol] [kaynak belirtme] [hedef belirtme] [protokol niteleme] [logging]

Bileşenler:

Liste numarası
Erişim liste numarası 100'den 199'a ve 2000'den 2699'a kadar olabilir.

Permit | deny
Her ikisi de olabilir. Permit belirttiğiniz ip adresini bir eşleme girişini içerir.

Protokol belirtme
Paket protokolüdür. Burası, IP,TCP,EDP veya ICMP ve diğer IP protokollerinden biri olabilir. Bununla birlikte İP protokol numarası da olabilir.

Kaynak belirtme
[Ip adresi] [joker maske] [port numarası belirtme (sadece UDP ve TCPiçin kullanılır)] biçiminde belirtilir.

Hedef belirtme
[Ip adresi] [joker maske] [port numarası belirtme (sadece UDP ve TCP çin kullanılır)] biçiminde belirtilir.

IP adresi
Bir IP adresini eşlemek için kullanılır.

Joker maske
İsteğe bağlı olarak kullanılan joker maske eşlemede bir IP adresindeki bitlerin değerlerini 0/1) kontrol eder.

Port numarası belirtme
İsteğe bağlı belirtme, port için bir dizi numaralara karar verir.

Protokol niteleme
İsteğe bağlı belirtme, protokol numaralarına daha fazla özellik tanımlar.

Logging (Kayıtlama)
Logging anahtar kelimesi. Erişim liste girişlerinin eşlendiğinde paket bilgilerini hepsini kayıt altına alır.

Uzatılmış EDL bildirimlerin için yazım formatı oldukça uzun olabilir ve çoğu kez terminal ekranını hepten kaplayabilir. Joker kartlar da komutlarda host ve anahtar sözcüklerinin kullanımında seçenekler içerir.

Uzatılmış EDL bildiriminin sonunda, opsiyonel TCP ya da UDP port numaralarının özelleştiği bir alandan kazanılan ilave bir kesinlik vardır.

Operatörler TCP ve UDP ile birlikte kaynak ve hedefi veya her ikisinin numara ve ismini açıkça belirtebilirsiniz. Yapılandırmada operatör kullandığınız takdirde eşlemede açıkça belirtmiş olursunuz. Operatörler yönlendiriciye port numaralarında veya numaralarda nasıl eşleme yapacağınızı söyler. Aşağıdaki tabloda operatörlerin açıklamalarını görebilirsiniz. Bu operatörler sadece TCP ve UDP bağlantılarda uygulanabilir. Diğerleri kullanmaz.

OPERATÖR	TANIM
lt	Küçüktür
gt	Büyüktür
neg	Eşit değil
eq	Eşit
range	Port numara sırası

Tablo 2.1: TCP ve UDP operatörleri

Port numaraları ve isimleri TCP ve UDP bağlantılarda port numarasını ve port isminden her ikisini de listeleyebilirsiniz. Örneğin, telnet trafiğini eşleme yapmak için **telnet** anahtar kelimesini ve 23 numarasından birisini kullanabilirsiniz. Tablo da TCP bağlantılarından genel olarak kullanılan port numarası ve isimlerini görebilirsiniz. Kullanılan TCP port isimlerinin tamamı: **bgp**, **chargen**, **daytime**, **discard**, **domain**, **echo**, **finger**, **ftp**, **ftp-data**, **gopher**, **hostname**, **irc**, **klogin**, **kshell**, **lpd**, **nntp**, **pop2**, **pop3**, **smtp**, **sunrpc**,**syslog**, **tacacs-ds**, **talk**, **telnet**, **time**, **uucp**, **whois**, and **www**. **Pop3** ismi bir e-posta

kullanıcısının e-posta sunucusundan postalarına erişmesi için kullanılır. www http web sunucusuna web bağlantısıdır. Bu listede port ismini bulamadıysanız port numarası ile belirtebilirsiniz. Port numarasını ve adını atladığınızda EDL bütün TCP bağlantısına eşleme için bakacaktır.

PORT İSMİ	KOMUT PARAMETRESİ	PORT NUMARASI
Ftp Data	ftp-data	20
Ftp Control	ftp	21
Telnet	telnet	23
SMTP	Smtp	25
WWW	www	80

Tablo 2.2: Genel TCP port isimleri ve numaraları

Tablo 2.3'de genel kullanılan UDP port adlarını ve numaralarını göstermektedir. Kullanabileceğiniz UDP port isimlerinin tamamı şunlardır: **biff, bootpc, bootps, discard, dns, dnsix, echo, mobile-ip, nameserver, netbios-dgm, netbios-ns, ntp, rip, snmp, nmptrap, sunrpc, syslog, tacacs-ds, talk, tftp, time, who, and xdmcp.** Listede olmayan port ismini port numarası kullanarak belirtebilirsiniz. Eğer port ismini ve numarasını atladığınızda, EDL eşleme için bütün UDP bağlantılarına bakacaktır.

PORT İSMİ	KOMUT PARAMETRESİ	PORT NUMARASI
DNS Query	Dns	53
TFTP	Tftp	69
SNMP	Snmp	161
IP RIP	Rip	520

Tablo 2.3: Genel UDP port isimleri ve numaraları

Genişletilmiş bir EDL'yi oluşturmak için yönlendiricinin arabirimini aşağıdaki yapılandırma gibi aktifleştirmelisiniz.

Router(config)# **interface** type [module_#]port_#
Router(config-if)# **ip access-group** ACL_# **in**|**out**

Not: Standart EDL için yapılandırma aynıdır. Yönlendirici arabirim üzerindeki trafiği filtrelemeye başlayacaktır.

Şu ana kadar genişletilmiş EDL'yi oluşturmak için söz diziminin nasıl olması gerektiğini gördük. Birkaç tane yapılandırma örneğine bakarak öğrendiklerimizi pekiştirelim.

Router(config)# **access-list 100 permit udp any host 172.16.1.1 eq dns log**
Router(config)# **access-list 100 permit tcp 172.17.0.0 0.0.255.255 host 172.16.1.2 eq telnet log**
Router(config)# **access-list 100 deny ip any any log**

Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 100 in**

Bu örnekteki gaye ağdan gelen trafiği sınırlamaktır. Bir dahili DNS sunucusuna (172.16.1.1) herhangi bir kaynak cihaz tarafından gönderilen DNS sorgusuna izin verecektir. 0.0.0.0 joker maske kaldırılmış ve **host** anahtar kelimesi IP adresinin önüne konmuştur. Bu adımda diğer bir eşlemde **log'**dur. İkinci adımda 172.17.0.0/16 ağındaki herhangi bir cihaza hedef cihaz 172.16.1.2 ise izin verecektir. Aslında üçüncü adıma gerek yoktur çünkü önceki adımda bütün trafik eşlemesi kabul (permit) edilmediğinden düşecektir. Bununla birlikte ne düşürüldüğünü bilmek istiyorsanız, örnekte yapıldığı gibi, **log** parametresi ile yapılandırma yapmanız gerekmektedir. Yapılandırmanın en son kısmında EDL ethernet0 üzerinde sınırlama yapacaktır.

Örneğin 192.168.1.100 bilgisayarının 212.1.1.8 bilgisayarına 80. porttan erişmemesini, aynı bilgisayara 25. porttan erişebilmesini, diğer bilgisayarlar için herhangi bir kısıtlama olmamasını istiyoruz (Söz konusu portlar TCP'de çalışır). Bu durumda komut satırına;

Router(config)#**access-list 101 deny tcp host 192.168.1.100 host 212.1.1.8 eq 80**
Router(config)#**access-list 101 permit tcp host 192.168.1.100 host 212.1.1.8 eq 25**
Router(config)#**access-list 101 permit ip any any**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 101 in**

2.1.3 Adlandırılmış Erişim Denetim Listeleri

Diğer erişim listelerinden sadece yapılandırma sırasında farklılık gösterir. Adlandırılmış erişim listeleri acces-list numarası vermek yerine, akılda kalması daha kolay olacak isimler kullanılır. Adlandırılmış erişim listelerinde satırlar tek tek silinebilir veya yeni satır eklenebilir. Çünkü listenin Standart ve Extended olmasına göre uygun modlar oluşturulur ve yapılandırma bu modlar altında yapılır.

2.1.3.1 Adlandırılmış Erişim Denetim listelerinin Genel Biçimi

Bir adlandırılmış erişim listesi oluşturmak için aşağıdaki biçimi kullanın:

Router(config)# **ip access-list Standard | Extended** ACL_name

İlk düşünmeniz gereken EDL tipini belirtmek; standart veya genişletilmiş. İkincisi kullanacağınız EDL adımları grubuna vereceğiniz bir EDL adı. Yalnız bu adı sadece bir kez kullanmalısınız. Bu adıma takiben EDL Subconfiguration moduna alınırsınız. Aşağıda görüldüğü gibi:

Router(config-std-acl)# veya Router(config-ext-acl)#

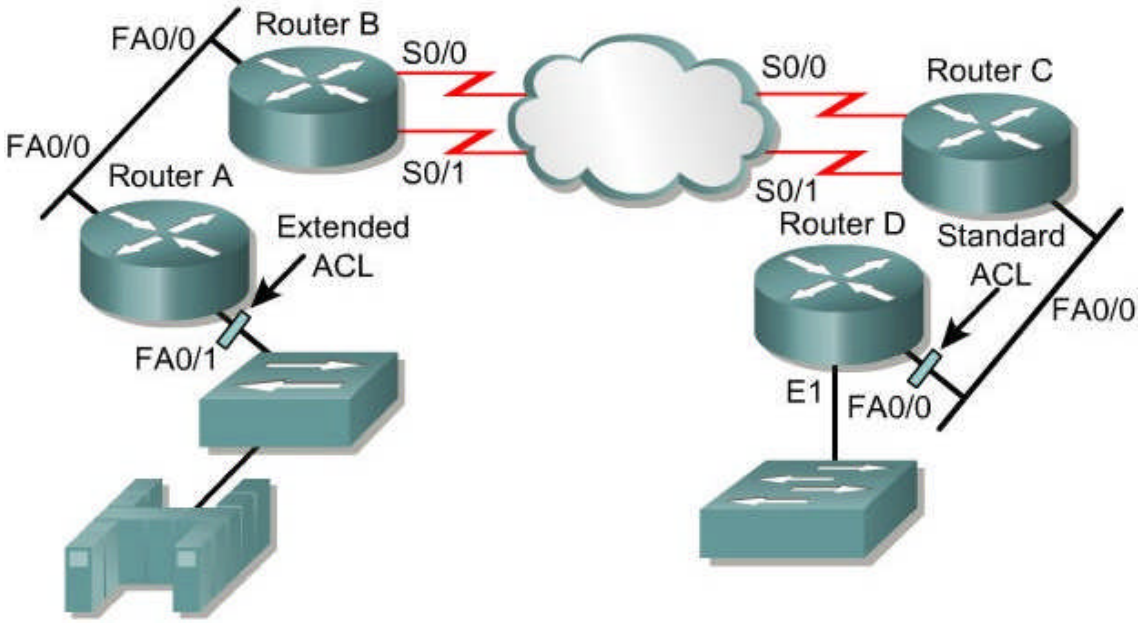
Bu moda alındıktan sonra standart ve genişletilmiş EDL'ler tanımlayabilirsiniz.

Genişletilmiş erişim Listesinde üzerinde çalıştığımız aynı senaryoyu adlandırılmış erişim listesi ile yapılandırmak istersek komut satırına;

Router(config)# **ip Access-list extended cilinkit**
Router(config-ext-nacl)# **deny tcp host 192.168.1.100 host 212.1.1.8 eq 80**
Router(config-ext-nacl)# **permit tcp host 192.168.1.100 host 212.1.1.8 eq 25**
Router(config-ext-nacl)# **permit tcp any any**

Yazmamız yeterli olacaktır. Burada 1. satırda belirtilen cilinkit bizim belirleyeceğimiz bir isimdir ve erişim listelerinin standart numaraları yerine kullanılır. Bu yapılandırmada hatalı bir satır yazıldığında başına "no" yazılarak satır iptal edilebilir.

2.2 Erişim Denetim Listelerinin Yerleştirilmesi



Resim 2.1: Erişim denetim listelerinin yerleştirilmesi

EDL'ler, ağ üzerindeki istenmeyen trafiği azaltmak ve paketleri filtrelemek suretiyle trafiği kontrol amaçlı kullanılırlar. EDL'lerin uygulanışında göz önünde bulundurulması gereken bir diğer önemli nokta erişim listelerinin nerede konumlandırılacağıdır. Eğer erişim listeleri doğru yerde bulunursa sadece trafik filtrelenmekle kalmaz aynı zamanda tüm ağın daha verimli çalışması sağlanır. Eğer trafiğin filtrelenmesi düşünülüyorsa EDL ağ performansının artışında en çok hangi noktada etki yapıyorsa oraya yerleştirilmelidir.

İşletme politikasının amacının D yönlendirici üzerindeki Fa/01 ağ kartına bağlı A yönlendiricisinin ağ kartı biriminden FTP ya da telnet trafiğini engellemeye yönelik olduğunu düşünmek gerekir. Aynı zamanda diğer trafiğe izin verilecektir. Bu politikayı farklı

yaklaşımlar tamamlar. Önerilen politika, hem kaynağı hem de alıcı adresini belirleyen uzatılmış EDL kullanılmasıdır. Bu uzatılmış EDL'yi A yönlendiricisine yerleştirin. Bu durumda A yönlendiricisinin ethernetindeki paketler kesişmez, B ile C yönlendiricinin seri arabirimi kesişmez ve D yönlendiricisine girilmez. Farklı kaynak ve alıcı adresi içeren trafiğe hâlâ izin veriliyor olacaktır.

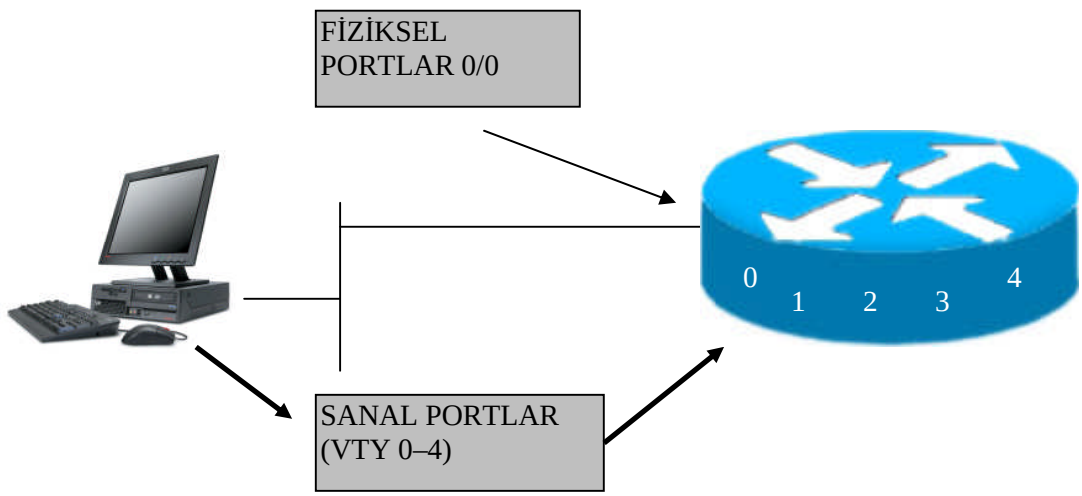
Genel kural, uzatılmış EDL' yi engellenecek trafik kaynağına mümkün olduğunca yakın yere koymaktır. Standart EDL'ler alıcı adresini belirlemez. Dolayısıyla mümkün olduğunca alıcı adresine yakın yerde olmalıdır.

Örneğin, A yönlendiricisinden gelen bir trafiği engellemek için standart bir EDL D yönlendiricinin Fa0/0 i üzerinde konumlandırılmalıdır.

Bir yönetici, bir aygıt üzerine kontrol edebileceği tek bir erişim listesi yerleştirebilir. Bu yüzden erişim listelerinin konumları ağ yöneticisinin kontrol yoğunluğu olan noktalarda belirtilmelidir.

2.3 Sanal Terminal Erişimlerinin Kısıtlanması

Standart ve uzatılmış erişim listeleri yönlendiricide yol alan paketlere uygulanır. Onlar yönlendiriciden gelen paketleri bloklamak için tasarlanmamıştır. Uzatılmış bir telnet çıkış erişim listesi, telnet oturumunu başlatmış bir yönlendiriciyi default olarak engellemez.

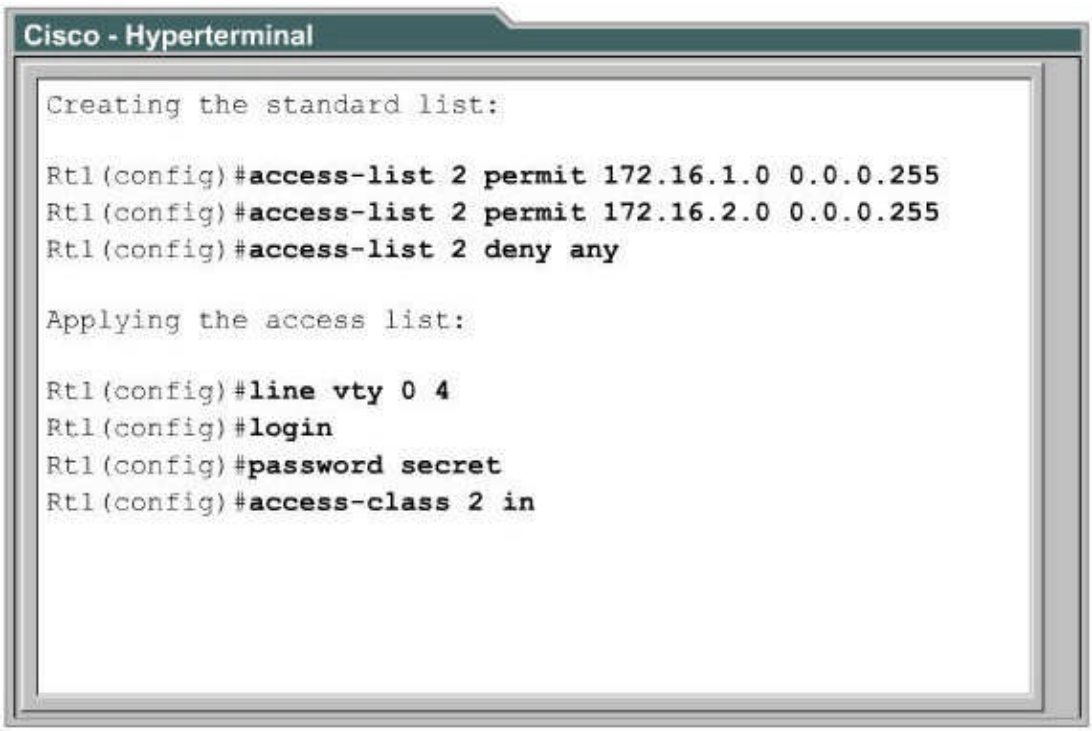


Şekil 2.1: Portların karşılaştırılması

Yönlendirici üzerinde Fa0/0 ve S0/0 gibi fiziksel portlar ya da arabirimler olduğu gibi sanal portlar da vardır. Bu sanal portlar vty hatları olarak adlandırılır. Sekil 2.1'de gösterildiği gibi, 0'dan 4'e kadar numaralandırılan beş tür vty hattı vardır. Güvenlik önerisi olarak kullanıcıların yönlendiriciye yönelik sanal terminal erişimlerine izin verilebilir ya da reddedilebilir, fakat yönlendiriciden alıcı adresine erişim reddedilmiştir.

Vty erişiminin yasaklanması düşüncesi ağ güvenliğini artırır. Vty'ye erişim, yönlendiriciye fiziksel olmayan bir bağlantı yapmak için telnet protokolünü kullanarak tamamlanır. Sonuç olarak sadece bir vty erişim listesi tipi vardır. Kullanıcının hangi hattan bağlandığını kontrol etmek mümkün olmadığından tüm vty hatlarına tanımsal yasaklar yerleştirilmelidir.

Vty erişim listesi oluşturma işlemi bir arabirim için tarif edilenle aynıdır. Bununla birlikte, EDL'yi bir terminal hattına bağlamak **access-group** komutu yerine **access-class** komutunu gerektirir.

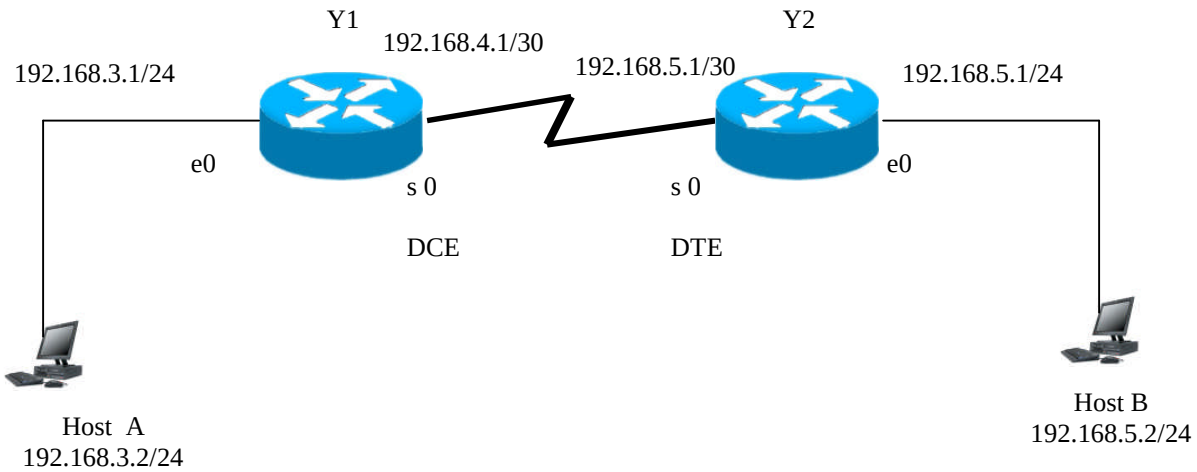


Resim 2.2: Sanal terminal kısıtlanması

Vty hatlarında erişim listelerini konfigüre ederken aşağıdakiler göz önünde bulundurulmalıdır:

- Bir arabirime erişim kontrolünde isim ya da numara kullanılmış olmalı.
- Sadece numaralandırılmış erişim listeleri sanal hatlara uygulanabilir.
- Sanal terminal hatlarına tanımsal yasaklar yerleştirilmeli, çünkü bir kullanıcı onlardan herhangi birine bağlanmaya teşebbüs edebilir.

UYGULAMA FAALİYETİ



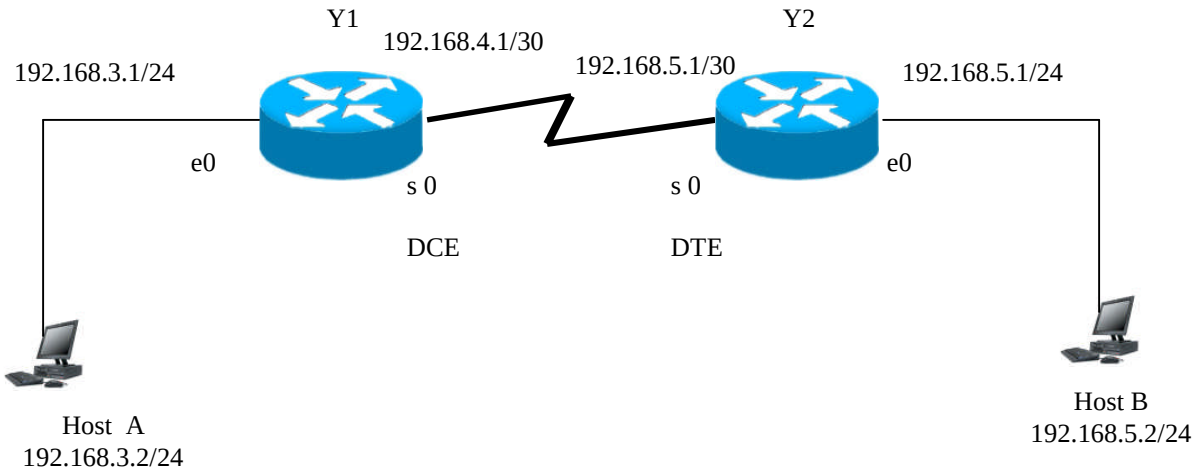
Yukarıdaki resimde Host B' den çıkan paketlerin 192.168.3.0 ağına erişmesini engellemek için.

Y1 Yönlendiricisinde;
Y1(config)#access-list 1 deny 192.168.5.2 0.0.0.0
Y1(config)#access-list 1 permit any
Y1(config)#inter serial 0
Y1(config-if)#ip access-group 1 in

veya

Y2 yönlendiricisinde;
Y2(config)#access-list 1 deny 192.168.5.2 0.0.0.0
Y2(config)#access-list 1 permit any
Y2(config)#inter ethernet 0
Y2(config-if)#ip access-group 1 in

UYGULAMA FAALİYETİ



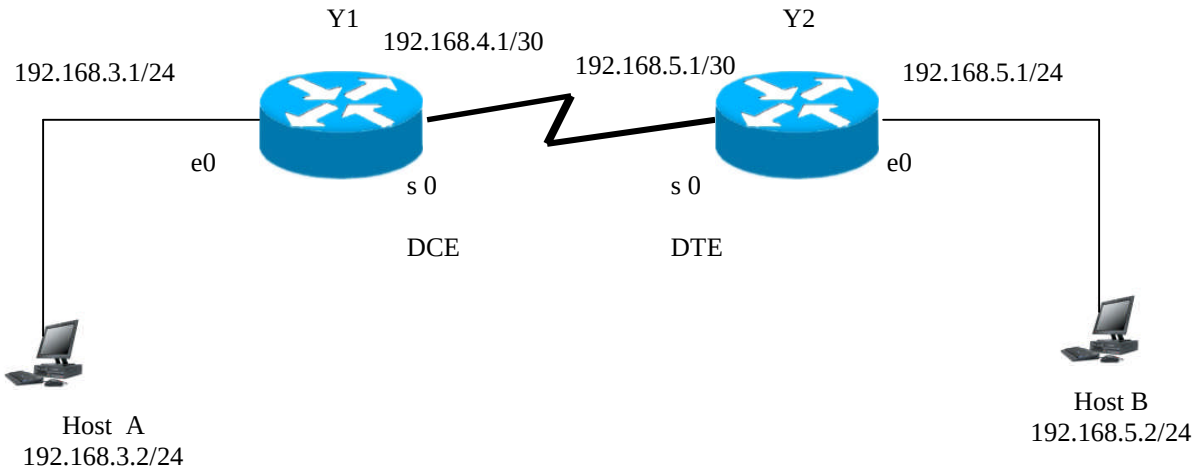
192.168.5.0 networkunun tamamının 192.168.3.0 networkuna erişmesini engellemek için.

Y1 yönlendiricisinde;
Y1 (config)#access-list 1 deny 192.168.5.2 0.0.0.255
Y1 (config)#access-list 1 permit any
Y1 (config)#inter serial 0
Y1 (config-if)#ip access-group 1 in

veya

Y2 yönlendircisinde;
Y2 (config)#access-list 1 deny 192.168.5.2 0.0.0.255
Y2 (config)#access-list 1 permit any
Y2 (config)#inter ethernet 0
Y2 (config-if)#ip access-group 1 in

UYGULAMA FAALİYETİ



Host A da bulunan FTP Server ve Web Server'a 192.168.5.2 bilgisayarının erişmesini engellemek (Kalan trafik akışı normal devam etmeli) için.

```
Y1(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 80
Y1(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 21
Y1(config)#access-list 101 permit ip any any
Y1(config)#
Y1(config)#inter serial 0
Y1(config-if)#ip access-group 101 in
Y1(config-if)#
```

veya

```
Y2(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 80
Y2(config)#access-list 101 deny tcp host 192.168.5.2 host 192.168.3.2 eq 21
Y2(config)#access-list 101 permit ip any any
Y2(config)#
Y2(config)#inter ethernet 0
Y2(config-if)#ip access-group 101 in
Y2(config-if)#
```

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki soruları cevaplayarak faaliyette kazandığınız bilgi ve becerileri ölçünüz.

Aşağıdaki cümleleri doğru ifade olacak şekilde kelime ve sayılarla doldurunuz.

1) Liste numarası 10 kullanılacak şekilde, 192.168.1.0/24 tarafından gelen trafiği kabul edecek standart EDL komutunu girin _____

2) Arabirimden giren adı cilinkit olan EDL'yi aktifleştirecek yönlendirici komutunu girin _____

3) 100 numaralı erişim listesindeki bütün adımları silecek komutu yazınız. _____

4) Uzatılmış EDL'yi engelleyecek trafiğe kaynağından mümkün olduğunca _____ yere konmalıdır.

5) Aşağıdakilerden hangisine göre standart EDL'ler eşler?
   A) Hedef Adres
   B) IP Protokol
   C) IP Protokol bilgileri
   D) Hiçbiri

6) Aşağıdakilerden hangisi cilinkit adında bir adlandırılmış standart EDL oluşturur.
   A) ip access-list cilinkit
   B) access-list cilinkit
   C) ip access-list standard cilinkit
   D) access-list Standard cilinkit

7) Aşağıdaki eşlemelerden hangisi <u>yanlıştır</u>?
   A) ftp Control 21
   B) telnet 23
   C) smtp 29
   D) www 80

8) Aşağıdakilerden hangisi erişim denetim listesi <u>değildir</u>?
   A) Joker maske
   B) Standart erişim listesi
   C) Genişletilmiş erişim listesi
   D) Adlandırılmış erişim listesi

MODÜL DEĞERLENDİRME

PERFORMANS TESTİ

Bir arkadaşınızla birlikte yaptığınız uygulamayı değerlendirme ölçeğine göre değerlendirerek, eksik veya hatalı gördüğünüz davranışları tamamlama yoluna gidiniz.

DEĞERLENDİRME ÖLÇÜTLERİ(YETERLİLİK)	**Evet**	**Hayır**
Erişim denetim listelerinin önemi kavradım.		
Erişim denetim listesi oluşturabilirim.		
Joker maske kullanabilirim.		
Yönlendiricide erişim denetim listelerini gösterebilirim.		
Erişim denetim listeleri çeşitlerini tanımlayabilirim.		
Standart erişim listesi oluşturma /silme		
Genişletilmiş erişim listesi oluşturabilirim/silebilirim.		
Erişim listesinde kullanılan port isimleri ve numaraları		
Adlandırılmış erişim listesi oluşturma/silme		
Erişim denetim listesi yerleştirme kriterleri		
Sanal terminal erişimlerinin kısıtlanması		

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ–1

1	**Kabul ya da ret**
2	**Hepsi ret**
3	**4 sekizliğe bölünmüş32**
4	**0.0.0.0**
5	**Yanlış**
6	**Doğru**
7	**Doğru**
8	**D**
9	**D**
10	**B**

ÖĞRENME FAALİYETİ–2

1	**access-list 10 permit 192.168.1.0 0.0.0.255.**
2	**ip access-group cilinkit in.**
3	**no access-list 100.**
4	**Yakın**
5	**D**
6	**C**
7	**C**
8	**A**

Cevaplarınızı cevap anahtarları ile karşılaştırarak kendinizi değerlendiriniz.

KAYNAKÇA

- SEDAYAO Jeff, Cisco IOS Access List, 2001
- KOLUKISAOGLU Hayrullah, CCNA Dokümantasyon Çalışması
- www.hasanbalik.com
- www.cisco.com
- www.olympos.org
- www.belgeler.org