
Pristupne liste

Tehničko ime za pristupnu listu je *lista postupaka za nadzor pristupa* (engl. *access-control list*) ili ACL. Pojedinačne stavke zovu se *stavke nadzora pristupa* (engl. *access-control entries*) ili ACE-ovi. Izraz lista postupaka za nadzor pristupa ne koristi se često u praksi pa ćete obično čuti da ih se spominje jednostavno kao pristupne liste ili ACL-ove.

Pristupne liste čine više od samog nadziranja pristupa. One su sredstvo kojim Ciscovi uređaji kategoriziraju i uspoređuju pakete na brojne zanimljive načine. Pristupne liste se koriste kao jednostavni filtri za propuštanje prometa kroz sučelja. Također se koriste za definiranje „zanimljivog prometa“ za rasporede ISDN pozivača te se u nekim mapama smjerova koriste za uspoređivanje paketa.

Dizajniranje pristupnih lista

Ovo će se poglavlje usredotočiti manje na osnove sastavljanja pristupnih lista, a više na to da vas upozna s prednostima i zamkama njihovog dizajniranja. Savjeti i trikovi u ovom poglavlju trebali bi vam pomoći u pisanju boljih, učinkovitijih i moćnijih pristupnih lista.



Kad izrađujete pristupne liste (ili, što se toga tiče, bilo koju konfiguraciju), dobro ih je prvo izraditi u programu za obradu teksta i zatim, kad ste razradili sve detalje, iskušati ih u kontroliranom okruženju. Kad god radite na filtrima, riskirate prekid funkcioniranja mreže.

Zamjenske maske

Zamjenske maske (nazivaju ih i *obrnutim maskama*) mogu biti zbunjujuće jer su binarno inverzne normalnim maskama podmreže. Drugim riječima, zamjenska maska koju biste upotrijebili za usklađivanje s rasponom opisanim maskom podmreže 255.255.255.0 bila bi 0.0.0.255.

Evo jednostavnog pravila koje će riješiti većinu problema na koje ćete naići s maskama podmreže i zamjenskim maskama:

Zamijenite sve nule s 255, a sve 255 s nulama:

Tablica 23-1 prikazuje kako izgledaju zamjenske maske podmreža klase A, B i C.

Tablica 23-1. Zamjenske maske podmreža klase A, B i C

Maska podmreže	Odgovarajuća zamjenska maska
255.0.0.0	0.255.255.255
255.255.0.0	0.0.255.255
255.255.255.0	0.0.0.255

Iako ovo može izgledati očito, u stvarnom svijetu mreže često nisu projektirane sa klasnim ograničenjima. Ilustracije radi, uzmimo masku podmreže 255.255.255.224. Proizlazi da je odgovarajuća zamjenska maska 0.0.0.31.

Srećom, postoji trik za izračunavanje svih zamjenskih maski i lakši je nego što biste pomislili. Evo ga:

Zamjenska maska bit će derivacija broja adresa čvorova koje pruža maska podmreže minus jedan.

U prethodnom primjeru (maska podmreže 255.255.255.224) ima osam mreža s 32 čvora u svakoj od njih (pogledajte poglavlje 34 za pomoć pri izračunavanju koliko ima čvorova u mreži s podmrežama). $32 - 1 = 31$. Zamjenska maska je 0.0.0.31. Da, zaista je tako jednostavno.

Zapravo trebate samo misliti o jednom oktetu koji nije 0 ili 255. U slučaju zamjenske maske koja je na položaju različitom od zadnjeg okteta jednostavno upotrijebite istu formulu i smatrajte da je broj čvorova onaj koji bi bio da je oktet s kojim se dijeli bio zadnji oktet. Evo primjera koji koristi masku podmreže 255.240.0.0:

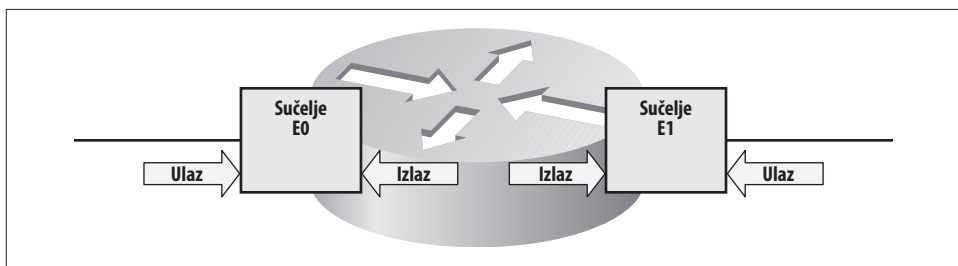
1. 240 u zadnjem oktetu maske podmreže (255.255.255.240) rezultirao bi sa 16 čvorova.
2. $16 - 1 = 15$.
3. Zamjenska maska je 0.15.255.255.

Što budete više u mislima vježbali rad s podmrežama, ovo će postajati sve lakše. Pokušajte sami s nekoliko primjera podmreža i ubrzo ćete vidjeti kako je to lako.

Gdje primijeniti pristupne liste

Jedno od najčešćih pitanja koje čujem od mlađih tehničara je „Primjenjujem li pristupnu listu dolazno ili odlazno?“. Odgovor je gotovo uvijek *dolazno*.

Slika 23-1 prikazuje jednostavni usmjerivač s dva sučelja, E0 i E1. Označio sam točke gdje bi se pristupna lista mogla primijeniti. Treba zapamtiti da su ovi pojmovi iz perspektive uređaja.



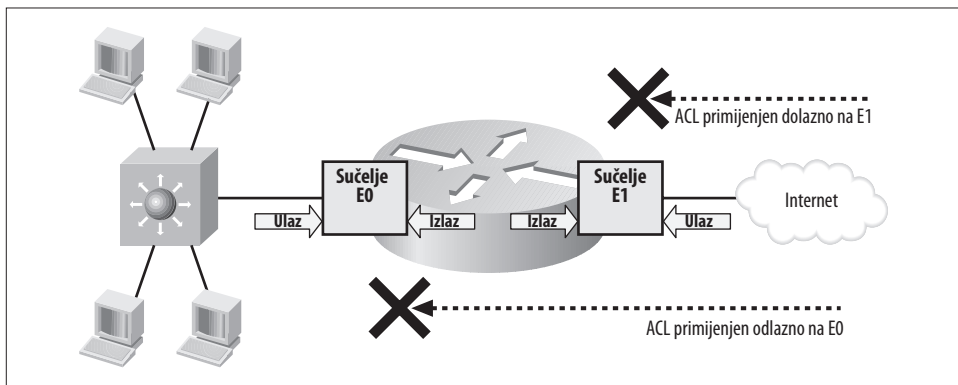
Slika 23-1. Točke primjene pristupnih lista

Kada pokušavate filtrirati promet želite spriječiti da doprije u mrežu ili da uopće doprije do uređaja. Primjena pristupnih lista na dolaznu stranu sučelja sprječava ulazak paketa u uređaj, štedeći na taj način vrijeme za obradu. Kad je paketu dopušten ulazak u uređaj i zatim je preklapljen na drugo sučelje da bi ga na kraju odbacio odlazni filter, resursi upotrijebljeni za prebacivanje paketa potrošeni su uzalud.



Refleksivne pristupne liste, opisane kasnije u ovom poglavlju, primjenjuju se u oba smjera.

Slika 23-2 prikazuje malu mrežu koja je usmjerivačem povezana s Internetom. Usmjerivač filtrira promet s Interneta da bi zaštitio uređaje u mreži. Kako promet dolazi s Interneta, putuje dolazno na E1, u usmjerivaču se preklapa na E0 i zatim se prosljeđuje u unutrašnju mrežu. Ako je ACL primijenjen dolazno na E1, paketi će biti odbijeni prije nego što ih usmjerivač bude morao dalje obraditi. Ako je ACL primijenjen odlazno na E0, usmjerivač mora utrošiti resurse na preklapanje paketa između sučelja samo da bi ih potom ispustio.



Slika 23-2. Primjena pristupnih lista u mreži



Budite oprezni kad brišete pristupne liste. Ako obrišete pristupnu listu koja je primijenjena na sučelje, sučelje će odbijati sav promet. Uvijek uklonite relevantne access-group naredbe prije brisanja pristupne liste.

Imenovanje pristupnih lista

Bilo bi u redu reći par riječi o imenovanju pristupnih lista. Imenovanje pristupnih lista na Ciscovim usmjerivačima korištenjem logičkih imena umjesto brojeva je moguće i preporučljivo jer olakšava čitanje konfiguracije. Nedostatak imenovanih pristupnih lista je taj što ne mogu biti korištene na mnoge načine na koje mogu biti korištene numerirane liste. Na primjer, mape smjerova podržavaju imenovane pristupne liste, ali rasporedi pozivača ne podržavaju. PIX vatrozidi podržavaju samo imenovane pristupne liste. To jest, čak i ako na PIX vatrozidu izradite listu pod imenom 10, bit će smatrana imenovanom listom umjesto standardnom (numeriranom).

Kad imenujete pristupne liste, preporučljivo je to učiniti dobro. Vidio sam mnoge instalacije PIX vatrozida u kojima je dolazna pristupna lista nazvana imenom poput „out“. Zamislite rješavanje problema s ovom naredbom:

```
access-group out in interface outside
```

Ako niste naviknuti na konfiguriranje PIX vatrozida ovu bi naredbu moglo biti teško protumačiti. Da je pristupna lista umjesto toga nazvana Inbound, naredba bi bila puno čitljivija:

```
access-group Inbound in interface outside
```

Mogućnost brzog utvrđivanja u koju je svrhu uređaj konfiguriran može uštedjeti vrijeme tijekom kvara, što vam doslovce može spasiti radno mjesto. Volim započinjati imena svojih pristupnih lista velikim slovima jer ih je lakše prepoznati u kodu. To je osobna sklonost koja može i ne mora odgovarati vašem stilu – radio sam s ljudima koji prigovaraju kad moraju pritisnuti tipku Shift.

Obrada od vrha prema dolje

Pristupne liste se obrađuju od vrha prema dolje, red po red. Kad se pronađe odgovarajuća stavka, obrada prestaje. Ovo je važno pravilo koje treba zapamtiti prilikom izrade i rješavanja problema s pristupnim listama. Uobičajena pogreška je dodavanje specifičnog reda za uspoređivanje s nečim što je već uspoređeno u manje specifičnom redu iznad toga:

```
access-list 101 permit tcp any 10.10.10.0 0.0.0.255 eq www
access-list 101 permit tcp any host 10.10.10.100 eq www
access-list 101 permit tcp any host 10.10.10.100 eq domain
```

U ovom primjeru drugi red neće nikada biti uspoređen jer su IP adresa i protokol već pronađeni u prvom redu. Osim toga, u slučaju da nema podudaranja s prvim redom, drugi red će ipak biti procijenjen, uzaludno trošeći vrijeme i energiju procesora. Ovaj se problem vrlo često može vidjeti u poslovnim mrežama. Na većim vatrozidima, gdje više osoba administrira uređaj, ovaj problem može biti ozbiljan. Također ga može biti teško uočiti jer ne sprječava rad protokola. Ovaj se tip problema obično otkriva tijekom kontrolnog pregleda mreže.

Najčešće korištene na vrhu

Pristupne liste trebale bi biti sastavljene tako da se redovi koji se najčešće uspoređuju nalaze na početku popisa. Sjetite se da se ACL obrađuje dok se ne pronađe odgovarajuća stavka. Nakon toga se ostatak ACL-a ne obrađuje. Ako ste radili samo na usmjerivačima s kratkim ACL-ovima, ovo vam se možda ne čini važno, ali u stvarnim poslovnim vatrozidima ACL-ovi mogu biti obimni. (Radio sam na PIX vatrozidima gdje su liste bile dugačke do 17 ispisanih stranica!)

Evo stvarnog primjera iz PIX vatrozida. Kad je moj tim sastavljao ovu malu pristupnu listu, jednostavno smo dodavali redove kako su nam padali na pamet. Ovo je razmjerno uobičajem pristup u stvarnim situacijama. Napravili smo popis poslužitelja (web1, lab, web2) i zatim naveli sve protokole kojima će biti dopušten pristup:

```
access-list Inbound permit tcp any host web1.gad.net eq www
access-list Inbound permit tcp any host web1.gad.net eq ssh
access-list Inbound permit udp any host web1.gad.net eq domain
access-list Inbound permit tcp any host web1.gad.net eq smtp
access-list Inbound permit tcp any host web1.gad.net eq imap4
access-list Inbound permit tcp any host lab.gad.net eq telnet
access-list Inbound permit tcp any host lab.gad.net eq 8080
access-list Inbound permit udp any host web2.gad.net eq domain
access-list Inbound permit tcp any host web2.gad.net eq smtp
access-list Inbound permit tcp any host web2.gad.net eq imap4
```

Nakon što smo mrežu ostavili da radi nekoliko dana, izvođenjem naredbe `show access-list` mogli smo vidjeti što se zbivalo s našom pristupnom listom:

```
PIX# sho access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
      alert-interval 300
access-list Inbound; 15 elements
access-list Inbound permit tcp any host web1.gad.net eq www (hitcnt=42942)
access-list Inbound permit tcp any host web1.gad.net eq ssh (hitcnt=162)
access-list Inbound permit udp any host web1.gad.net eq domain (hitcnt=22600)
access-list Inbound permit tcp any host web1.gad.net eq smtp (hitcnt=4308)
access-list Inbound permit tcp any host web1.gad.net eq imap4 (hitcnt=100)
access-list Inbound permit tcp any host lab.gad.net eq telnet (hitcnt=0)
```

```

access-list Inbound permit tcp any host lab.gad.net eq 8080 (hitcnt=1)
access-list Inbound permit udp any host web2.gad.net eq domain (hitcnt=10029)
access-list Inbound permit tcp any host web2.gad.net eq smtp (hitcnt=2)
access-list Inbound permit tcp any host web2.gad.net eq imap4 (hitcnt=0)

```

Pažljivo proučite stavke hitcnt na kraju svakog reda. One pokazuju koliko je puta pronađena podudarnost sa svakim redom u ACL-u. Zbrojevi pronađenih podudarnosti pokazuju da ovaj ACL nije sastavljen optimalno. Da bi bio sastavljen bolje, treba uzeti gornji rezultat i sortirati ga prema hitcnt, s najvećim brojem na početku. Rezultati izgledaju ovako:

```

access-list Inbound permit tcp any host web1.gad.net eq www (hitcnt=42942)
access-list Inbound permit udp any host web1.gad.net eq domain (hitcnt=22600)
access-list Inbound permit udp any host web2.gad.net eq domain (hitcnt=10029)
access-list Inbound permit tcp any host web1.gad.net eq smtp (hitcnt=4308)
access-list Inbound permit tcp any host web1.gad.net eq ssh (hitcnt=162)
access-list Inbound permit tcp any host web1.gad.net eq imap4 (hitcnt=100)
access-list Inbound permit tcp any host web2.gad.net eq smtp (hitcnt=2)
access-list Inbound permit tcp any host lab.gad.net eq 8080 (hitcnt=1)
access-list Inbound permit tcp any host lab.gad.net eq telnet (hitcnt=0)
access-list Inbound permit tcp any host web2.gad.net eq imap4 (hitcnt=0)

```

Ovo je optimalni sastav ove uistinu male pristupne liste. Stavke s najvećim brojem pristupanja sada su na vrhu liste, a one s najmanje su na dnu.



Čuvajte se pretpostavki. Mogli biste pomisliti da SMTP treba biti visoko na listi jer vatrozid štiti poslužitelj elektroničke pošte, ali ako pogledate prethodni rezultat vidjet ćete da DNS pokazuje daleko više povezivanja nego SMTP. Provjerite što se zaista događa na mreži i konfigurirajte pristupnu listu u skladu s tim.

Problem s ovim pristupom može biti gubitak čitljivosti. U ovom je slučaju izvorni ACL lakše čitati i razumjeti nego preoblikovanu inačicu. Drugi, učinkovitiji ACL ima stavku za web2 usred svih stavki za web1. To je lako previdjeti pa može otežati rješavanje problema. Samo vi kao administrator možete odlučiti u vezi s prednostima i nedostacima trenutnog oblika ACL-a. U manjim biste listama mogli učiniti ustupke radi čitljivosti, ali u slučaju liste od 17 stranica otkrit ćete da će smještanje često uspoređivanih redova na vrh imati značajan utjecaj na operativnu brzinu vrlo prometnog vatrozida.

Korištenje grupa u pristupnim listama PIX vatrozida

PIX vatrozidi sada omogućavaju korištenje *grupa* u pristupnim listama. Ovo je ogromna prednost pri izradi lista jer omogućava vrlo složene ACL-ove s vrlo jednostavnim konfiguracijama. Korištenje grupa u ACL-ovima također omogućava mijenjanje više ACL-ova mijenjanjem grupe – kad se grupa u upotrebi promijeni, PIX će automatski promijeniti svaku instancu gdje je grupa primijenjena. Kod složenih pristupnih lista korištenje grupa može pomoći pri sprječavanju pogrešaka jer je manje vjerojatno da ćete zaboraviti važnu stavku: ne morate je dodavati na više mjesta, već se samo trebate sjetiti da ju smjestite u grupu.

Pogledajmo primjer grupa na djelu. Evo izvornog ACL-a:

```
object-group service CCIE-Rack tcp
  description [< For Terminal Server Reverse Telnet >]
  port-object range 2033 2050

access-list Inbound permit tcp any host gto eq www
access-list Inbound permit tcp any host gto eq ssh
access-list Inbound permit tcp any host meg eq ssh
access-list Inbound permit tcp any host meg eq www
access-list Inbound permit tcp any host lab eq telnet
access-list Inbound permit tcp any host lab object-group CCIE-Rack
access-list Inbound permit udp any host PIX-Outside eq 5060
access-list Inbound permit tcp any host lab eq 8080
access-list Inbound permit udp any host meg eq domain
access-list Inbound permit udp any host gto eq domain
access-list Inbound permit tcp any host gto eq smtp
access-list Inbound permit tcp any host meg eq smtp
access-list Inbound permit tcp any host gto eq imap4
access-list Inbound permit tcp any host meg eq imap4
access-list Inbound permit esp any any
access-list Inbound permit icmp any any unreachable
access-list Inbound permit icmp any any time-exceeded
access-list Inbound permit icmp any any echo-reply
```

Primijetite da je grupa objekata već u upotrebi za CCIE-Rack. Ovo se možda ne čini potrebnim jer bi se ista stvar mogla postići s ključnom riječi range:

```
access-list Inbound line 3 permit tcp any host lab range 2033 2050
```

Ustvari, kao što ćete uskoro vidjeti, grupa objekata se svejedno pretvara u ovaj red. Neki smatraju da se grupa objekata ne bi trebala koristiti ako zauzima više redova konfiguracije od broja redova u koje se prevodi. Ja se ne slažem. Sviđa mi se činjenica da mogu dodati opis grupi objekata. Osim toga, kasnije lako mogu dodati servis grupi objekata a da ne moram mijenjati nijednu pristupnu listu.

Evo grupa koje sam izradio na temelju izvorne pristupne liste. Servise koji su zajednički za više poslužitelja uključio sam u grupu *Webserver-svcs*. Također sam izradio grupu *Webservers* koja sadrži sve Web poslužitelje, grupu *Webserver-svcs-udp* za servise koji se temelje na UDP-u kao što je DNS te grupu *ICMP-Types* za ICMP pakete. Grupa *ICMP-Types* namijenjena je povratnim paketima koji su rezultat naredbi ping i traceroute. Zagrade u poljima description mogle bi vam izgledati čudno, ali ja ih volim dodati kako bih istaknuo opise:

```
object-group service CCIE-Rack tcp
  description [< For Terminal Server Reverse Telnet >]
  port-object range 2033 2050
object-group service Webserver-svcs tcp
  description [< Webserver TCP Services >]
  port-object eq www
  port-object eq ssh
  port-object eq domain
  port-object eq smtp
  port-object eq imap4
```

```

object-group service Webserver-svcs-udp udp
  description [< Webserver UDP Services >]
  port-object eq domain
object-group network Webservers
  description [< Webservers >]
  network-object host gto
  network-object host meg
object-group icmp-type ICMP-Types
  description [< Allowed ICMP Types >]
  icmp-object unreachable
  icmp-object time-exceeded
  icmp-object echo-reply

```

Kad sam organizirao sve servise i poslužitelje u grupe, vrijeme je da prepisem pristupnu listu kako bi ih koristila:

```

access-list Inbound permit udp any object-group Webservers object-group Webserver-
svcs-udp
access-list Inbound permit tcp any object-group Webservers object-group Webserver-
svcs
access-list Inbound permit tcp any host lab eq telnet
access-list Inbound permit tcp any host lab object-group CCIE-Rack
access-list Inbound permit udp any host PIX-Outside eq 5060
access-list Inbound permit tcp any host lab eq 8080
access-list Inbound permit esp any any
access-list Inbound permit icmp any any object-group ICMP-Types

```

Pristupna lista se smanjila s 18 redova na 8. Ne zaboravite, ovo je samo vidljiva konfiguracija. Ovi će redovi biti prošireni u memoriji vatrozida na izvornih 18 redova.



Redovi možda nisu optimalno sortirani, što može biti problem kod složenih konfiguracija. Kao i kod većine stvari, potrebno je učiniti kompromis. Kod složenih instalacija svakako omogućite Turbo ACL-ove (opisane u sljedećem odjeljku).

Imajte na umu da grupe ne znače nužno manje tipkanja – zapravo, često vrijedi suprotno. Iako se ova pristupna lista smanjila s 18 na 8 redova, trebali smo napisati više redova nego što smo ih uštedjeli. Cilj je olakšati čitanje i održavanje pristupne liste. Vi trebate zaključiti hoće li konačne prednosti opravdati početni trud.

Rezultat konfiguracije može se vidjeti pomoću naredbe `show access-list`. Rezultat uključuje oba konfiguracijska reda `object-group` i same pristupne stavke u koje se prevode. Stavke `object-group` prikazane su podebljanim slovima:

```

GAD-PIX# sho access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
  alert-interval 300
access-list Inbound; 20 elements
access-list Inbound line 1 permit udp any object-group Webservers object-group
Webserver-svcs-udp

```

```

access-list Inbound line 1 permit udp any host gto eq domain (hitcnt=7265)
access-list Inbound line 1 permit udp any host meg eq domain (hitcnt=6943)
access-list Inbound line 2 permit tcp any object-group Webserver object-group
Webserver-svcs
access-list Inbound line 2 permit tcp any host gto eq www (hitcnt=21335)
access-list Inbound line 2 permit tcp any host gto eq ssh (hitcnt=4428)
access-list Inbound line 2 permit tcp any host gto eq domain (hitcnt=0)
access-list Inbound line 2 permit tcp any host gto eq smtp (hitcnt=1901)
access-list Inbound line 2 permit tcp any host gto eq imap4 (hitcnt=116)
access-list Inbound line 2 permit tcp any host meg eq www (hitcnt=23)
access-list Inbound line 2 permit tcp any host meg eq ssh (hitcnt=15)
access-list Inbound line 2 permit tcp any host meg eq domain (hitcnt=0)
access-list Inbound line 2 permit tcp any host meg eq smtp (hitcnt=1)
access-list Inbound line 2 permit tcp any host meg eq imap4 (hitcnt=0)
access-list Inbound line 3 permit tcp any host lab eq telnet (hitcnt=0)
access-list Inbound line 4 permit tcp any host lab object-group CCIE-Rack
access-list Inbound line 4 permit tcp any host lab range 2033 2050 (hitcnt=0)
access-list Inbound line 5 permit udp any host PIX-Outside eq 5060 (hitcnt=0)
access-list Inbound line 6 permit tcp any host lab eq 8080 (hitcnt=0)
access-list Inbound line 7 permit esp any any (hitcnt=26256)
access-list Inbound line 8 permit icmp any any object-group ICMP-Types
access-list Inbound line 8 permit icmp any any unreachable (hitcnt=359)
access-list Inbound line 8 permit icmp any any time-exceeded (hitcnt=14)
access-list Inbound line 8 permit icmp any any echo-reply (hitcnt=822)

```

Turbo ACL

Prirodno, ACL-ovi se moraju interpretirati svaki put kad se na njih upućuje. To može dovesti do značajnog opterećenja procesora, posebice na uređajima s velikim ACL-ovima.

Jedna od mogućnosti za poboljšanje performansi s velikim ACL-ovima je njihovo prevođenje. Prevedeni ACL naziva se *Turbo ACL*. Prevođenje mijenja ACL u strojni kod koji više ne treba interpretirati prije obrade. To može imati značajan utjecaj na izvedbu.

PIX vatrozidi i Ciscovi usmjerivači podržavaju Turbo ACL-ove. Na PIX vatrozidima naredba `access-list compiled` govori vatrozidu da prevede sve pristupne liste. Samo Ciscovi usmjerivači iz serije 7100, 7200, 7500 i 12000 (12.0(6)S i noviji) podržavaju Turbo ACL-ove. IOS naredba za omogućavanje te značajke također je `access-list compiled`.

Kad su Turbo ACL-ovi omogućeni, rezultat naredbe `show access-list` se mijenja, pokazujući činjenicu da su ACL-ovi prevedeni te koliko memorije svaki od njih zauzima:

```

PIX(config)# access-list comp
PIX(config)# show access-list

```

```

TurboACL statistics:
ACL                State          Memory(KB)
-----
Inbound
                Operational  2

```

Shared memory usage: 2056 KB

access-list compiled

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 1024)
alert-interval 300

access-list Inbound turbo-configured; 20 elements

```
access-list Inbound line 1 permit udp any object-group Webservers object-group
Webserver-svcs-udp
access-list Inbound line 1 permit udp any host gto eq domain (hitcnt=7611)
access-list Inbound line 1 permit udp any host meg eq domain (hitcnt=7244)
access-list Inbound line 2 permit tcp any object-group Webservers object-group
Webserver-svcs
access-list Inbound line 2 permit tcp any host gto eq www (hitcnt=22578)
access-list Inbound line 2 permit tcp any host gto eq ssh (hitcnt=4430)
access-list Inbound line 2 permit tcp any host gto eq domain (hitcnt=0)
access-list Inbound line 2 permit tcp any host gto eq smtp (hitcnt=2035)
access-list Inbound line 2 permit tcp any host gto eq imap4 (hitcnt=157)
access-list Inbound line 2 permit tcp any host meg eq www (hitcnt=23)
access-list Inbound line 2 permit tcp any host meg eq ssh (hitcnt=16)
access-list Inbound line 2 permit tcp any host meg eq domain (hitcnt=0)
access-list Inbound line 2 permit tcp any host meg eq smtp (hitcnt=1)
access-list Inbound line 2 permit tcp any host meg eq imap4 (hitcnt=0)
access-list Inbound line 3 permit tcp any host lab eq telnet (hitcnt=0)
access-list Inbound line 4 permit tcp any host lab object-group CCIE-Rack
access-list Inbound line 4 permit tcp any host lab range 2033 2050 (hitcnt=0)
access-list Inbound line 5 permit udp any host PIX-Outside eq 5060 (hitcnt=0)
access-list Inbound line 6 permit tcp any host lab eq 8080 (hitcnt=0)
access-list Inbound line 7 permit esp any any (hitcnt=26423)
access-list Inbound line 8 permit icmp any any object-group ICMP-Types
access-list Inbound line 8 permit icmp any any unreachable (hitcnt=405)
access-list Inbound line 8 permit icmp any any time-exceeded (hitcnt=14)
access-list Inbound line 8 permit icmp any any echo-reply (hitcnt=822)
```

Dozvoljavanje zadavanja naredbi traceroute i ping

Jedna od karakteristika vatrozida koje živciraju je i nemogućnost ispitivanja putanje paketa kroz mrežu (*engl. traceroute*) i mjerenje vremena potrebnog probnom paketu da stigne do određižnog računala i vrati se (*engl. ping*) kada su sigurnosna pravila stupila na snagu.

Pretpostavka da je ICMP opasan je opravdana ali ako razumijete kako se ICMP ponaša, možete propustiti samo tipove koje trebate i tako nastaviti uživati prednosti naredbi ping i traceroute.

Pod pretpostavkom da propuštate sav odlazni promet, možete primijeniti filtre paketa koji kao dolazni promet propuštaju samo one pakete s odgovorima koji su rezultat naredbi ping i traceroute. To će omogućiti da testovi rade kad se pokrenu iz unutrašnjosti mreže, dok će te iste testove onemogućiti kad im je izvor izvan mreže. Da biste omogućili rad ovih alata, morate dopustiti ulazak sljedećih tipova ICMP paketa:

ICMP Unreachable

Ima mnogo tipova ICMP Unreachable, uključujući Network Unreachable i Host Unreachable. Općenito je prihvatljivo propuštanje svih njih jer su to paketi s odgovorima.

Time Exceeded

Poruke Time Exceeded vraća naredba traceroute na svakom koraku staze kojom prolazi prema zadanom odredištu.

Echo Reply

Eho odgovor je odgovor probnog paketa.

Filtri paketa obično su uključeni na kraj dolaznih pristupnih lista koje su već primijenjene. Oni bi uglavnom trebali biti smješteni na dnu ACL-a, osim ako iz unutrašnjosti mreže ne potječe velika količina ICMP prometa. Evo nekih primjera primjene ovih filtara za Ciscove usmjerivače i PIX vatrozide:

- Ciscovi usmjerivači:

```
access-list 101 remark [< Allows PING and Traceroute >]
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any echo-reply
!
interface Ethernet1
ip access-group 101 in
```

- Vatrozidi:

```
object-group icmp-type ICMP-Types
description [< Allowed ICMP Types >]
icmp-object unreachable
icmp-object time-exceeded
icmp-object echo-reply
!
access-list Inbound permit icmp any any object-group ICMP-Types
!
access-group Inbound in interface outside
```

Propuštanje paketa za otkrivanje MTU staze

Otkrivanje MTU staze omogućava uređajima na udaljenim mrežama da vas obavještavaju o ograničenjima MTU-a. Da biste to omogućili, morate dopustiti ulazak još dva ICMP tipa: *Source-quench* i *Parameter-problem*. Možete ih propustiti na Ciscovim usmjerivačima i PIX vatrozidima na sljedeći način:

- Ciscovi usmjerivači:

```
access-list 101 remark [< Allows PING and Traceroute >]
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any parameter-problem
access-list 101 permit icmp any any source-quench
!
interface Ethernet1
ip access-group 101 in
```

- Vatrozidi:

```
object-group icmp-type ICMP-Types
description [< Allowed ICMP Types >]
```

```

icmp-object unreachable
icmp-object time-exceeded
icmp-object echo-reply
icmp-object source-quench
icmp-object parameter-problem
!
access-list Inbound permit icmp any any object-group ICMP-Types
!
access-group Inbound in interface outside

```

ACL-ovi u višeslojnim preklopnicima

Višeslojni preklopnici, prema prirodi svoje konstrukcije, omogućavaju neke sigurnosne značajke koje nisu dostupne na preklopnicima ili usmjerivačima sloja 2.

Preklopnik 3750 podržava IP ACL-ove i Ethernet (MAC) ACL-ove. Pristupne liste na preklopniku 3750 mogu se primijeniti na sljedeće načine:

ACL-ovi porta

ACL-ovi porta primjenjuju se na sučelja sloja 2 na preklopniku. Ne mogu se primijeniti na EtherChannel, SVI ili bilo koje drugo virtualno sučelje. ACL-ovi porta mogu se primijeniti na sučelja glavnih vodova i u tom će slučaju filtrirati svaku VLAN u glavnomvodu. Standardni IP, prošireni IP ili MAC ACL-ovi mogu biti dodijeljeni kao ACL-ovi porta. Oni se mogu primijeniti samo u *dolaznom* smjeru.

ACL-ovi usmjerivača

ACL-ovi usmjerivača primjenjuju se na sučelja sloja 3 na preklopniku. Mogu se primijeniti na SVI sučelja, fizička sučelja sloja 3 (konfigurirana s `no switchport`, na primjer) i EtherChannel sloja 3. Standardni IP i prošireni IP ACL-ovi mogu biti dodijeljeni kao ACL-ovi usmjerivača, dok MAC ACL-ovi ne mogu. ACL-ovi usmjerivača mogu se primijeniti i u *dolaznom* i u *odlaznom* smjeru.

VLAN mape

VLAN mape su po strukturi slične mapama smjerova. One se dodjeljuju VLAN mrežama i mogu se konfigurirati tako da prosljeđuju ili ispuštaju pakete na temelju brojnih testova. VLAN mape kontroliraju sav promet usmjeren u, iz ili unutar VLAN-a. One nemaju smjer.

Konfiguriranje ACL-ova porta

ACL-ovi porta su pridruženi specifičnom fizičkom sučelju. Oni se mogu koristiti za odbijanje pristupa čvoru unutar VLAN-a bilo kojem drugom čvoru unutar VLAN-a. Također se mogu koristiti za ograničavanje pristupa izvan VLAN-a.

Zamislite da u mreži VLAN 100 ima mnogo čvorova, uključujući čvor A. On ne bi trebao moći izravno komunicirati s bilo kojim drugim čvorom unutar iste VLAN mreže, već bi samo trebao moći komunicirati s podrazumijevanim prolazom radi komunikacije

s ostatkom svijeta. Pretpostavimo da je IP adresa čvora A 192.168.1.155/24, IP adresa podrazumijevanog prolaza je 192.168.1.1/24 i čvor A je povezan s portom G0/20 na preklopniku.

Prvi korak u ograničavanju komunikacija čvora A je izrada potrebnog ACL-a. Morate dopustiti pristup podrazumijevanom prolazu, zatim mu odbiti pristup ostalim čvorovima u mreži i, na kraju, dopustiti pristup ostatku svijeta:

```
access-list 101 permit ip any host 192.168.1.1
access-list 101 deny ip any 192.168.1.0 0.0.0.255
access-list 101 deny ip any any
```

Nakon što ste izradili ACL, možete ga primijeniti na fizičko sučelje:

```
3750(config)# int g0/20
3750(config)# switchport
3750(config-if)# ip access-group 101 in
```

Uočite da iako je ovo port preklopnika sloja 2, na njega se može primijeniti IP pristupna lista sloja 3. Činjenica da je IP pristupna lista primijenjena na port preklopnika čini je ACL-om porta.

ACL-ovi porta mogu se temeljiti i na MAC adresama. Evo male MAC pristupne liste koja odbija AppleTalk pakete, dok dopušta sve ostalo:

```
mac access-list extended No-Appletalk
deny any any appletalk
permit any any
```

Dodjela ove pristupne liste sučelju čini je ACL-om porta:

```
3750(config)# int g0/20
3750(config-if)# mac access-group No-Appletalk in
```

MAC ACL-ovi mogu se miješati s IP ACL-ovima u jednom sučelju. Ovdje možete vidjeti da su na sučelju aktivne MAC pristupna lista i IP pristupna lista:

```
3750# show run int g0/20
interface GigabitEthernet0/20
switchport mode dynamic desirable
ip access-group 101 in
mac access-group No-Appletalk in
end
```

Konfiguriranje ACL-ova usmjerivača

ACL-ovi usmjerivača vjerojatno su ono na što većina pomisli kad razmišlja o primjeni ACL-ova. Oni se primjenjuju na sučelja sloja 3. Stariji usmjerivači su imali samo sučelja sloja 3 pa su praktički svi ACL-ovi bili ACL-ovi usmjerivača.

Kad biste uzeli prethodni primjer i promijenili port iz sučelja sloja dva u sučelje sloja 3, ACL bi postao ACL usmjerivača:

```
3750(config)# int g0/20
3750(config)# no switchport
3750(config-if)# ip access-group 101 in
```

MAC pristupne liste ne mogu se dodijeliti kao ACL-ovi usmjerivača.

Kad konfigurirate ACL-ove usmjerivača, imate mogućnost da ih primijenite odlazno (iako ja nisam prevelik ljubitelj odlaznih ACL-ova):

```
3750(config-if)# ip access-group 101 out
```

Ne zaboravite da će primjena ACL-a na bilo koje sučelje sloja 3 učiniti da on postane ACL usmjerivača. Budite oprezni kad ACL-ove porta i ACL-ove usmjerivača primjenjujete zajedno:

```
3750(config)# int vlan 100
3750(config-if)# ip address 192.168.100.1 255.255.255.0
3750(config-if)# ip access-group 101 in
2w3d: %FM-3-CONFLICT: Input router ACL 101 conflicts with port ACLs
```

Ova poruka o pogrešci pokazuje da su primjenjeni ACL-ovi porta i ACL-ovi usmjerivača čiji se opsezi preklapaju (u ovom slučaju sadrže iste IP adrese). Ova poruka je generirana jer će oba ACL-a biti aktivna, ali će ACL porta imati prednost.

Kad je primijenjen ACL porta dok je primijenjen i ACL usmjerivača može doći do prilične zbrke ako niste svjesni da je primijenjen ACL porta.

Konfiguriranje VLAN mapa

VLAN mape omogućavaju kombiniranje pristupnih lista na zanimljive načine. One filtriraju sav promet *unutar* VLAN-a.

ACL porta samo filtrira dolazne pakete na jednom sučelju, a ACL usmjerivača samo filtrira pakete dok putuju u ili iz sučelja sloja 3. Međutim, VLAN mapa filtrira svaki paket unutar VLAN-a, bez obzira o kojem se tipu porta radi. Na primjer, kad biste izradili filtar koji sprječava da MAC adresa 1111.1111.1111 komunicira s 2222.2222.2222 i primijenili ga na sučelje, premještanje uređaja na drugo sučelje zaobišlo bi filtar. Ali kod VLAN mapa filtar bi bio primijenjen bez obzira koje se sučelje koristi (pod pretpostavkom da je u konfiguriranoj VLAN mreži).

Za ovaj ćemo primjer izraditi filtar koji će onemogućiti ulazak AppleTalk paketa u mrežu VLAN 100. Evo MAC pristupne liste:

```
mac access-list extended No-Appletalk
  permit any any appletalk
```

Primijetite da dopuštamo AppleTalk, iako nam je cilj da ga odbijemo. To je zbog prirode VLAN mapa, kao što ćete uskoro vidjeti.

Da bismo odbili AppleTalk unutar VLAN-a, trebamo izraditi VLAN mapu. VLAN mape sadrže izraze slično kao mape smjerova. Izrazi su numerirani, iako je za razliku od mapa smjerova akcija definirana unutar izraza, a ne u naslovu izraza.

Prvo trebamo definirati VLAN mapu. To se postiže pomoću naredbe `vlan access-map`. Ova će VLAN mapa sadržavati dva izraza. Prvi (10) uspoređuje MAC pristupnu listu `No-Appletalk` i ispušta pakete koji se podudaraju. To je razlog zašto pristupna lista treba sadržavati red `permit appletalk` umjesto reda `deny appletalk`. Stavka `permit` omogućava da se pronađe podudaranje s `AppleTalk`. Iskaz `action` u VLAN mapi ispušta pakete:

```
vlan access-map Limit-V100 10
  action drop
  match mac address No-Appletalk
```

Zatim ćemo dodati još jedan iskaz koji prosljeđuje sve ostale pakete. Budući da u ovom izrazu nema iskaza `match`, svi će paketi odgovarati:

```
vlan access-map Limit-V100 20
  action forward
```

Evo cijele VLAN mape:

```
vlan access-map Limit-V100 10
  action drop
  match mac address No-Appletalk
vlan access-map Limit-V100 20
  action forward
```

Kad smo izradili VLAN mapu, trebamo je primijeniti na VLAN. To se postiže globalnom naredbom `vlan filter`:

```
3750(config)# vlan filter Limit-V100 vlan-list 100
```



Da biste primijenili VLAN mapu na više VLAN mreža, na kraj naredbe dodajte broj svake VLAN mreže.

Možda se pitate nismo li jednostavno mogli izraditi običnu pristupnu listu poput sljedeće i primijeniti je na specifična sučelja?

```
mac access-list extended No-Appletalk
deny any any appletalk
permit any any
```

Odgovor je potvrđan, ali da bismo to učinili morali bismo znati koja bi sučelja mogla slati `AppleTalk` pakete i, prema tome, gdje ju primijeniti. Alternativno, mogli bismo ju primijeniti na sva sučelja unutar VLAN-a, ali tada bismo se trebali sjetiti primijeniti pristupnu listu na portove koji će biti dodani VLAN-u u budućnosti. Dodjeljivanje pristupne liste samoj VLAN mreži osigurava da će svi `AppleTalk` paketi koji pristignu u VLAN, bez obzira na njihov izvor ili odredište, biti odbačeni.

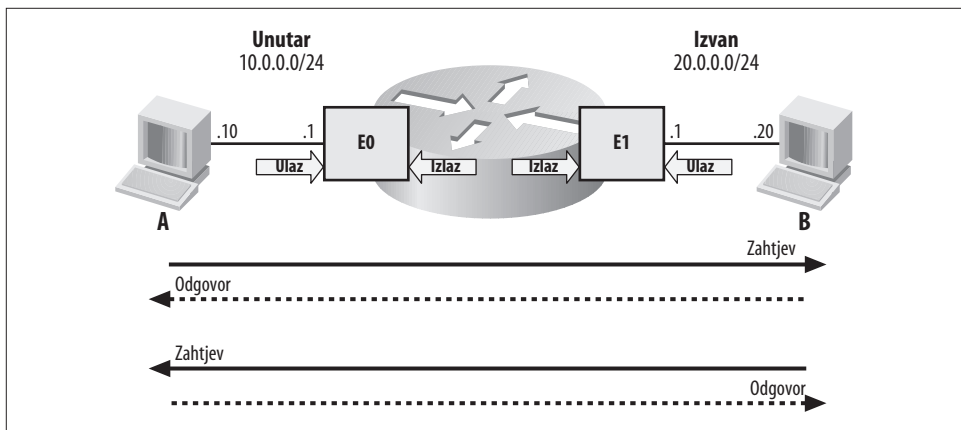
Da biste vidjeli koje su VLAN mape dodijeljene, upotrijebite naredbu `show vlan filter`:

```
SW2# sho vlan filter
VLAN Map Limit-V100 is filtering VLANs:
 100
```

Refleksivne pristupne liste

Refleksivne pristupne liste su dinamički filtri koji propuštaju promet na temelju smjera prometa u obrnutom smjeru. Jednostavan primjer mogao bi biti: „dolazni telnet promet propusti samo ako pokrenem odlazni telnet promet“. Kad ovo po prvi put objašnjavam mlađim tehničarima često primim reakciju poput „Ne radi li to tako u svakom slučaju?“ Ono što mnoge zbunjuje je sličnost ove značajke s Port Address Translation (PAT). PAT dopušta dolazni promet samo kao odgovor na odlazni promet kojem je izvor na mreži. To je zbog prirode PAT-a prema kojoj se mora napraviti prijevod da bi promet mogao proći. Refleksivne pristupne liste daleko su moćnije i mogu se primjenjivati iz mnogih razloga.

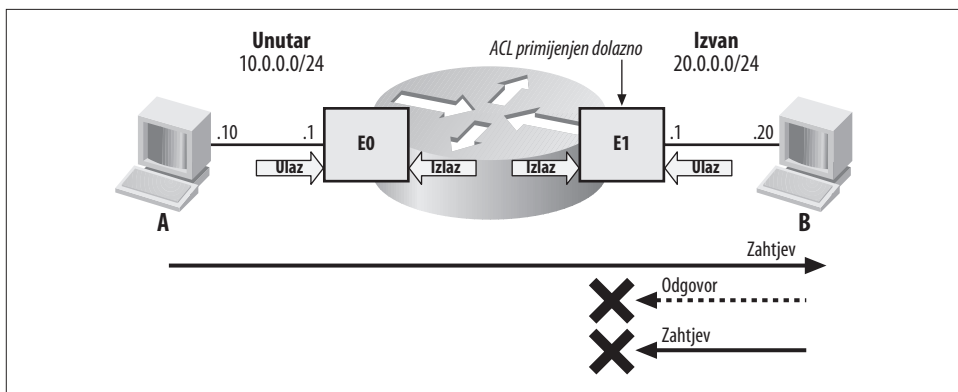
Bez PAT-a, filtar odbija promet bez obzira na drugi promet. Proučite mrežu na slici 23-3. Ima dva računala, A i B, spojena preko usmjerivača. Usmjerivač nema instaliranu pristupnu listu. Na zahtjeve računala A računalo B bit će odgovoreno, kao i na zahtjeve računala B računalo A.



Slika 23-3. Jednostavna mreža bez ACL-ova

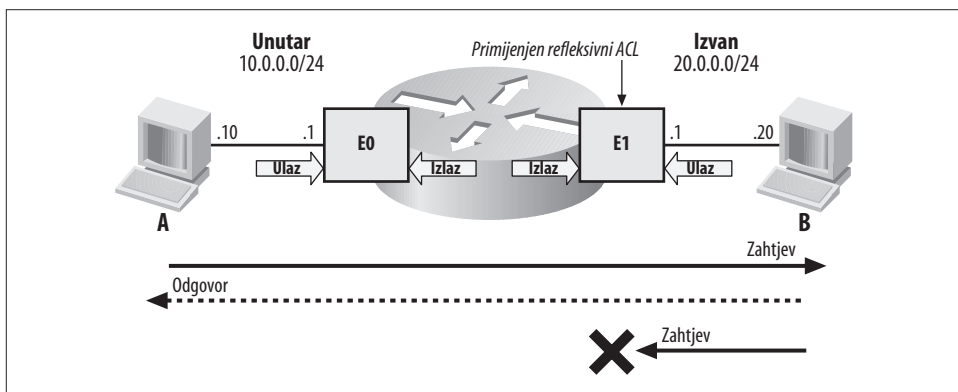
Recimo da želimo da se s računala A preko telnet-a možemo spojiti na računalo B, ali da se s računala B ne može spojiti na računalo A. Ako primijenimo običnu pristupnu listu primijenjenu dolazno na sučelje E1 na usmjerivaču, dopuštamo da A kontaktira B i sprječavamo da B kontaktira A. Na nesreću, također sprječavamo da B odgovori računalo A. Ovo ograničenje prikazano je na slici 23-4.

Ovo je previše ograničavajuće za naše potrebe. Osigurali smo računalo A od pokušaja komunikacije s računalo B, no također smo računalo A uskratili koristan promet od računala B. Potrebno nam je da usmjerivač postupa više kao vatrozid: želimo da usmjerivač odbija zahtjeve od računala B, ali da računalo B može odgovarati na zahtjeve računala A. Refleksivne pristupne liste rješavaju ovaj problem.



Slika 23-4. Jednostavna pristupna lista primijenjena dolazno na E1

Refleksivne pristupne liste izrađuju ACL-ove u trenutku potrebe kako bi dopustile odgovore na zahtjeve. U ovom bismo primjeru željeli dopustiti promet od B, ali samo ako se prvo otkrije promet od A. Ako B pokrene promet, ne želimo ga propustiti. Ova koncepcija prikazana je na slici 23-5.



Slika 23-5. Refleksivna pristupna lista primijenjena na E1

Refleksivne pristupne liste izrađuju privremene iskaze permit koji su refleksije izvornih iskaza. Na primjer, ako dopustimo spajanje telnetom na udaljena računala, privremeni iskaz permit bit će izrađen za dolazni telnet promet.

Refleksivne pristupne liste vrlo su korisne, ali imaju neka ograničenja:

- Privremena stavka je uvijek permit, a nikad deny.
- Privremena stavka je uvijek isti protokol kao i izvornik (TCP, UDP itd.).
- Privremena stavka imat će izvorišne i odredišne IP adrese obrnute od izvornog prometa.

- Privremena stavka imat će iste brojeve portova kao i izvorni promet, iako će izvor i odredište zamijeniti mjesta (ICMP, koji ne koristi brojeve portova, koristit će brojeve tipova).
- Privremena stavka bit će uklonjena nakon što je primijećen zadnji paket (obično FIN ili RST).
- Privremenoj stavci isteći će rok trajanja ako se ne primijeti nikakav promet u vremenskom periodu koji se može konfigurirati (podrazumijevani je pet sekundi).

Ne možete izraditi refleksivnu pristupnu listu koja dopušta jedan protokol kad je otkriven drugi. Na primjer, ne možete dopustiti dolazni HTTP promet jer je s udaljenog računala pokrenut telnet promet. Ako želite refleksivno dopustiti dolazni HTTP promet, morate testirati za odlazni HTTP promet.

Budući da su brojevi portova u privremenim stavkama uvijek obrnuti od brojeva portova iz izvornog prometa, nisu prikladni za protokole kao što je RPC koji mijenjaju brojeve izvornih portova. Refleksivni ACL-ovi također nisu prikladni za protokole koji izrađuju nove tokove kao što je FTP.



FTP se ipak može koristiti s refleksivnim pristupnim listama pod uvjetom da se koristi *pasivni režim*.

Konfiguriranje refleksivnih pristupnih lista

Refleksivne pristupne liste malo su kompliciranije od običnih jer morate ugnijezditi jedan ACL unutar drugog. Uzmite u obzir potrebu za testiranjem za dva tipa prometa: izvorni zahtjev i odgovor koji će uslijediti. ACL mora biti izrađen za svaki test. ACL za odgovor izrađuje se dinamički kad dođe do podudaranja s ACL-om za izvorni zahtjev.



Način na koji se konfiguriraju refleksivne pristupne liste Cisco naziva *ugnježđivanjem*, iako većini programera konfiguracija ne izgleda poput ugnježđenog koda.

Nastavljajući s prethodnim primjerom, izradimo refleksivnu pristupnu listu za telnet promet. Želimo da se s računala A preko telnet-a možemo spojiti na računalo B, ali ćemo sve ostalo odbiti. Ovo je pretjerano ograničavajuće za većinu primjena u stvarnom svijetu, ali pomoći će pri ilustriranju funkcionalnosti refleksivnih pristupnih lista.

Da bismo konfigurirali refleksivne pristupne liste, moramo izraditi jedan ACL za odlazni i jedan za dolazni promet.

Prvo ćemo izraditi imenovanu pristupnu listu TelnetOut:

```
ip access-list extended TelnetOut
 permit tcp host 10.0.0.10 host 20.0.0.20 eq telnet reflect GAD
 deny ip any any
```



Refleksivne pristupne liste mogu se izraditi samo korištenjem imenovanih pristupnih lista.

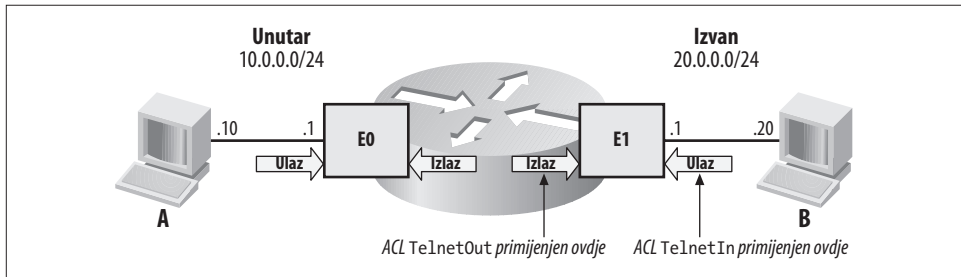
Ovaj ACL je prilično jednostavan, osim što je na kraju reda permit dodano reflect GAD. Ovo će biti ime privremene pristupne liste koju će izraditi usmjerivač kad dođe do podudaranja sa stavkom permit. Stavka deny ip any any nije potrebna jer to sve pristupne liste podrazumijevano dodaju, ali ja sam je ovdje dodao radi jasnoće i prikaza brojača čije se vrijednosti uvećavaju kako se promet kasnije odbija.

Sada ćemo izraditi imenovanu pristupnu listu TelnetIn:

```
ip access-list extended TelnetIn
evaluate GAD
deny ip any any
```

Ova pristupna lista nema iskaza permit, ali ima iskaz evaluate GAD. Ovaj red upućuje na red reflect u pristupnoj listi TelnetOut. GAD će biti ime nove pristupne liste koju će izraditi usmjerivač.

Da bi ove pristupne liste stupile na snagu, trebamo ih primijeniti na usmjerivač. Primijenit ćemo TelnetOut *odlazno* na sučelje E1, a TelnetIn *dolazno* na sučelje E1. Slika 23-6 to ilustrira.



Slika 23-6. Primjena refleksivnih pristupnih lista

Refleksivne pristupne liste primjenjuju se putem naredbe sučelja access-group:

```
interface Ethernet1
ip access-group TelnetIn in
ip access-group TelnetOut out
```

Čitava relevantna konfiguracija za usmjerivač glasi ovako:

```
interface Ethernet0
ip address 10.0.0.1 255.255.255.0
!
interface Ethernet1
ip address 20.0.0.1 255.255.255.0
ip access-group TelnetIn in
ip access-group TelnetOut out
!
```

```

ip access-list extended TelnetIn
  evaluate GAD
  deny ip any any
ip access-list extended TelnetOut
  permit tcp host 10.0.0.10 host 20.0.0.20 eq telnet reflect GAD
  deny ip any any

```

Promatrajući pristupne liste pomoću naredbe `show access-list`, obje vidimo točno onako kako smo ih konfigurirali:

```

Router# sho access-list
Reflexive IP access list GAD
Extended IP access list TelnetIn
  evaluate GAD
  deny ip any any
Extended IP access list TelnetOut
  permit tcp host 10.0.0.10 host 20.0.0.20 eq telnet reflect GAD
  deny ip any any (155 matches)

```

Ovdje možemo vidjeti da se sav promet koji nije telnet odbija odlazno. Zapravo nema stavki za dopuštanje ikakvog dolaznog prometa, ali to će se promijeniti kad se aktivira reflektivna pristupna lista.

Nakon što s računala A preko telnet-a pošaljemo zahtjev računalu B, rezultat se mijenja. Sada postoji dodatna pristupna lista pod imenom GAD:

```

Router# sho access-list
Reflexive IP access list GAD
  permit tcp host 20.0.0.20 eq telnet host 10.0.0.10 eq 11002 (12 matches)
Extended IP access list TelnetIn
  evaluate GAD
  deny ip any any
Extended IP access list TelnetOut
  permit tcp host 10.0.0.10 host 20.0.0.20 eq telnet reflect GAD
  deny ip any any (155 matches)

```

Ova privremena pristupna lista izrađena je u odgovor na odlazni promet koji se podudara sa stavkom `permit` koja sadrži iskaz `reflect GAD`. Broj odredišnog porta je 11002 i to je bio broj izvorišnog porta za odlazni telnet zahtjev.

Kad sesija završi ili nema aktivnosti koja se podudara s novom pristupnom listom, reflektivna pristupna lista se uklanja. Potreban period neaktivnosti može se konfigurirati pomoću globalne naredbe `ip reflexive-list timeout sekunde`. Ova naredba utječe na sve reflektivne pristupne liste na usmjerivaču. Podrazumijevana vrijednost za period neaktivnosti je pet sekundi.