ASA/PIX: Esempio di configurazione di BGP tramite ASA

Sommario

Introduzione

In questa configurazione di esempio viene mostrato come eseguire il protocollo BGP (Border Gateway Protocol) su un'appliance di sicurezza (PIX/ASA) e come ottenere la ridondanza in un ambiente BGP e PIX multihomed. Se si utilizza un diagramma di rete come esempio, questo documento spiega come instradare automaticamente il traffico al provider di servizi Internet B (ISP-B) quando AS 64496 perde la connettività all'ISP-A (o viceversa), tramite l'uso di protocolli di routing dinamico in esecuzione tra tutti i router in AS 64496.

Poiché BGP utilizza pacchetti TCP unicast sulla porta 179 per comunicare con i peer, è possibile configurare PIX1 e PIX2 per consentire il traffico unicast sulla porta TCP 179. In questo modo, è possibile stabilire il peering BGP tra i router connessi tramite il firewall. La ridondanza e le policy di routing desiderate possono essere ottenute tramite la manipolazione degli attributi BGP.

Prerequisiti

Requisiti

I lettori di questo documento devono avere familiarità con la configurazione di BGP e della configurazione base del firewall.

Componenti usati

Gli scenari di esempio riportati in questo documento si basano sulle seguenti versioni software:

- Cisco 2600 router con Cisco IOS? Software release 12.2(27)
- PIX 515 con Cisco PIX Firewall versione 6.3(3) e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- Cisco Adaptive Security Appliance (ASA) serie 5500 con versione 7.x e successive
- Cisco Firewall Services Module (FWSM) con software versione 3.2 e successive

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

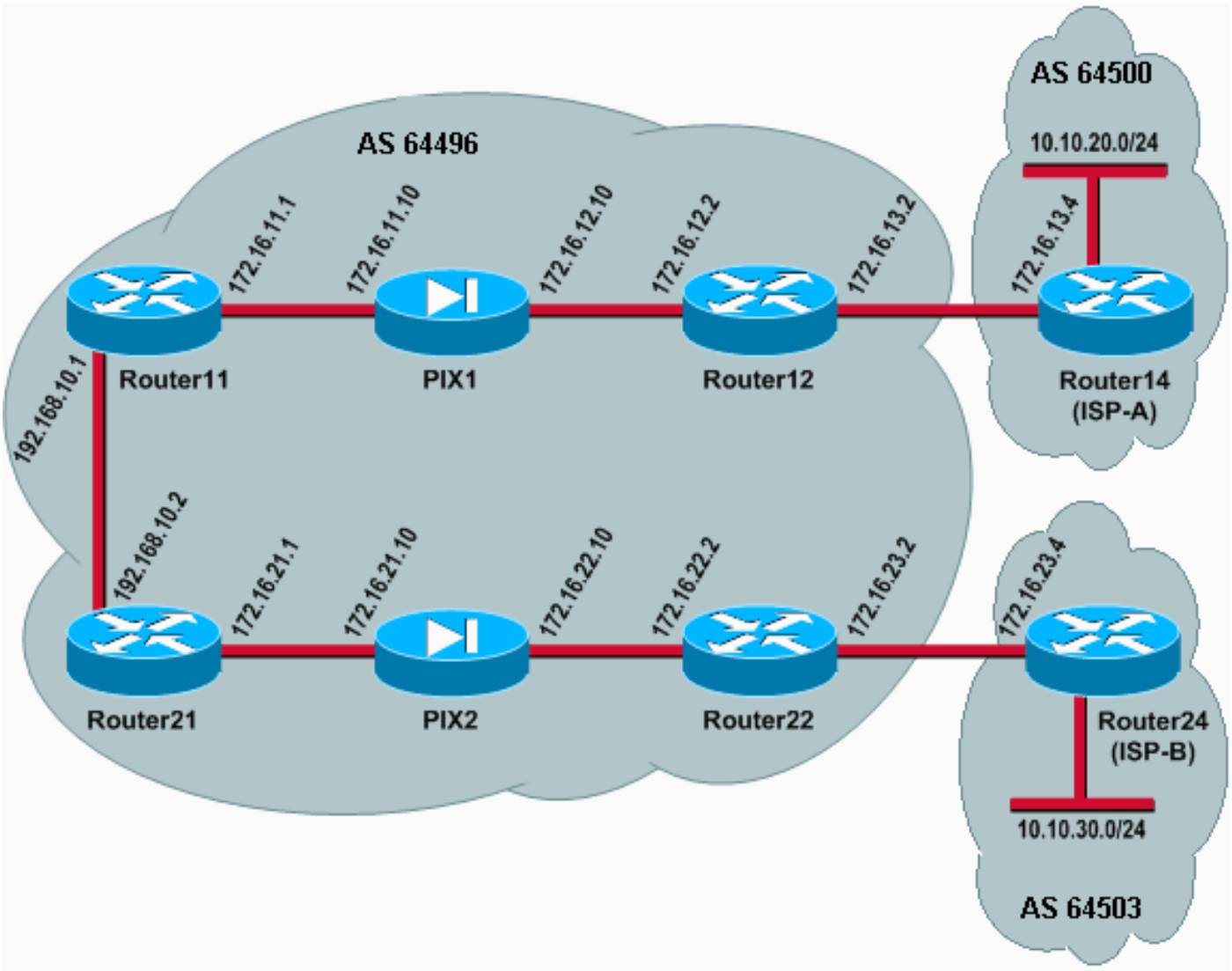
Configurazione

In questa sezione vengono fornite informazioni per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questa configurazione di rete, il router 12 e il router 2 (che appartengono allo standard AS 64496) sono multihomed rispettivamente al router 14 (ISP-A) e al router 24 (ISP-B), per motivi di ridondanza. La rete interna 192.168.10.0/24 si trova all'interno del firewall. I router 11 e 21 si connettono ai router 12 e 22 attraverso il firewall. PIX1 e PIX2 non sono configurati per eseguire Network Address Translation (NAT).

Scenario 1

In questo scenario, il router 12 in AS 64496 esegue il peering BGP (eBGP) esterno con il router 14 (ISP-A) in AS 64500. Il router 12 esegue anche il peering BGP (iBGP) interno con il router 11 tramite PIX1. Se sono presenti route apprese da ISP-A, il router 12 annuncia una route predefinita 0.0.0.0/0 su iBGP al router 11. Se il collegamento con ISP-A ha esito negativo, il router 12 si arresta il percorso predefinito.

Analogamente, Router22 in AS 64496 esegue il peering eBGP con Router24 (ISP-B) in AS 64503 e annuncia una route predefinita da iBGP a Router21 in base alla presenza di route ISP-B nella relativa tabella di routing.

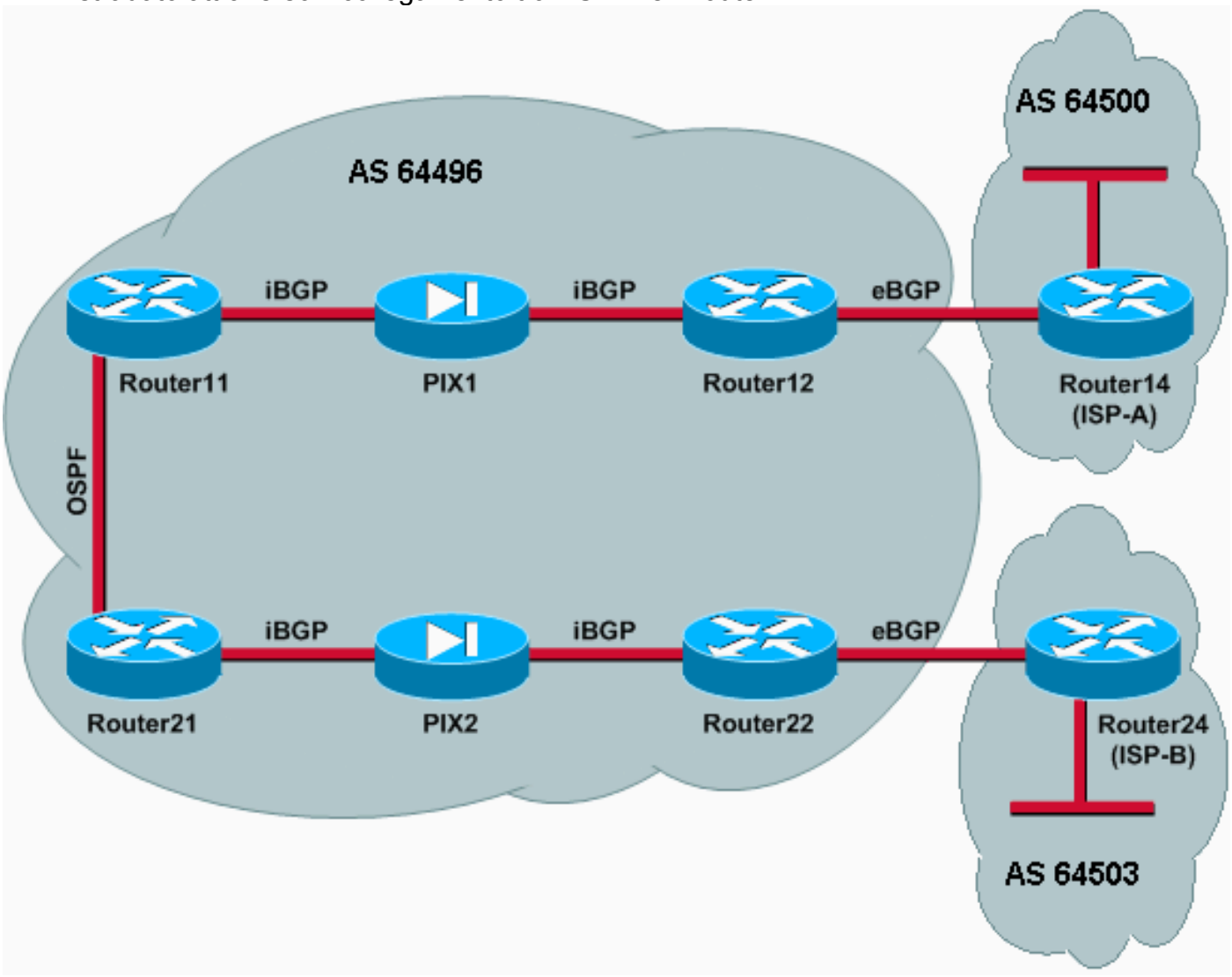
Tramite l'uso di un elenco degli accessi, PIX1 e PIX2 sono configurati per consentire il traffico BGP (TCP, porta 179) tra peer iBGP. Infatti alle interfacce PIX è associato un livello di sicurezza. Per impostazione predefinita, il livello di protezione dell'interfaccia interna (ethernet1) è 100 e quello dell'interfaccia esterna (ethernet0) è 0. Le connessioni e il traffico vengono in genere autorizzati dalle interfacce con un livello di protezione più alto a quelle con un livello di protezione

più basso. Tuttavia, per autorizzare il traffico tra un'interfaccia con un livello di sicurezza inferiore e un'interfaccia con un livello di sicurezza superiore, è necessario definire esplicitamente un elenco degli accessi sul PIX. Inoltre, è necessario configurare una conversione NAT statica su PIX1 e PIX2, per consentire ai router esterni di avviare una sessione BGP con i router all'interno di PIX.

Sia il router 11 che il router 21 annunciano in modo condizionale la route predefinita nel dominio OSPF (Open Shortest Path First) in base alla route predefinita appresa da iBGP. Il router 11 annuncia la route predefinita nel dominio OSPF con una metrica di 5, il router 21 annuncia la route predefinita con una metrica di 30, pertanto è preferibile la route predefinita dal router 11. Questa configurazione consente di propagare solo il percorso predefinito 0.0.0.0/0 al router11 e al router21, in modo da preservare il consumo di memoria sui router interni e ottenere prestazioni ottimali.

Di conseguenza, per riepilogare queste condizioni, questa è la politica di routing per AS 64496:

- AS 64496 preferisce il collegamento dal router 12 all'ISP-A per tutto il traffico in uscita (da 192.168.10.0/24 a Internet).
- Se la connettività all'ISP-A ha esito negativo, tutto il traffico viene instradato attraverso il collegamento tra il router 2 e l'ISP-B.
- Tutto il traffico proveniente da Internet e indirizzato a 192.168.10.0/24 utilizza il collegamento da ISP-A a Router12.
- Se il collegamento tra l'ISP-A e il router 12 ha esito negativo, tutto il traffico in entrata viene instradato attraverso il collegamento tra l'ISP-B e il router 22.



Configurazioni

In questo scenario vengono utilizzate le configurazioni seguenti:

- Router11
- Router12
- Router 14 (ISP-A)
- Router21
- Router22
- PIX1
- PIX2

Router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router ospf 1 log-adjacency-changes network
192.168.10.0 0.0.0.255 area 0 default-information
originate metric 5 route-map check-default !--- A
default route is advertised into OSPF conditionally
(based on whether the link !--- from Router12 to ISP-A
is active), with a metric of 5. router bgp 64496 no
synchronization bgp log-neighbor-changes network
192.168.10.0 neighbor 172.16.12.2 remote-as 64496 !---
Configures Router12 as an iBGP peer . distance bgp 20
105 200 !--- Administrative distance of iBGP learned
routes is changed from default 200 to 105. no auto-
summary ! ip route 172.16.12.0 255.255.255.0
172.16.11.10 !--- Static route to iBGP peer, because it
is not directly connected. ! access-list 30 permit
0.0.0.0 access-list 31 permit 172.16.12.2 route-map
check-default permit 10 match ip address 30 match ip
next-hop 31
```

Router12

```
hostname Router12
!
interface FastEthernet0/0
 ip address 172.16.13.2 255.255.255.0
!--- Connected to Router14 (ISP-A). ! interface
FastEthernet0/1 ip address 172.16.12.2 255.255.255.0 !--
- Connected to PIX1. ! router bgp 64496 no
synchronization neighbor 172.16.11.1 remote-as 64496
neighbor 172.16.11.1 next-hop-self neighbor 172.16.11.1
default-originate route-map check-ispa-route !--- A
default route is advertised to Router11 conditionally
(based on whether the link !--- from Router12 to ISP-A
is active). neighbor 172.16.11.1 distribute-list 1 out
neighbor 172.16.13.4 remote-as 64500 !--- Configures
Router14 (ISP-A) as an eBGP peer. neighbor 172.16.13.4
route-map adv-to-ispa out no auto-summary ! ip route
172.16.11.0 255.255.255.0 172.16.12.10 !--- Static route
to iBGP peer, because it is not directly connected. !
access-list 1 permit 0.0.0.0 access-list 10 permit
```

```
192.168.10.0 access-list 20 permit 10.10.20.0 0.0.0.255
access-list 21 permit 172.16.13.4 ! route-map check-
ispa-route permit 10 match ip address 20 match ip next-
hop 21 ! route-map adv-to-ispa permit 10 match ip
address 10
```

Router 14 (ISP-A)

```
hostname Router14
!
interface Ethernet0/0
 ip address 172.16.13.4 255.255.255.0
!
interface Ethernet0/1
 ip address 10.10.20.1 255.255.255.0
!
router bgp 64500
 network 10.10.20.0 mask 255.255.255.0
 neighbor 172.16.13.2 remote-as 64496
!--- Configures Router12 as an eBGP peer. !
```

Router21

```
hostname Router21
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.0
!--- Connected to Router11. ! interface FastEthernet0/1
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router ospf 1 network 192.168.10.0 0.0.0.255
area 0 default-information originate metric 30 route-map
check-default !--- A default route is advertised into
OSPF conditionally (based on whether the link !--- from
Router22 to ISP-B is active), with a metric of 30. !
router bgp 64496 no synchronization network 192.168.10.0
neighbor 172.16.22.2 remote-as 64496 !--- Configures
Router22 as an iBGP peer. ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 !--- Static route to iBGP
peer, because it is not directly connected. ! access-
list 30 permit 0.0.0.0 access-list 31 permit 172.16.22.2
route-map check-default permit 10 match ip address 30
match ip next-hop 31 !
```

Router22

```
hostname Router22
!
interface FastEthernet0/0
 ip address 172.16.23.2 255.255.255.0
!--- Connected to Router24 (ISP-B). ! interface
FastEthernet0/1 ip address 172.16.22.2 255.255.255.0 !--
- Connected to PIX2. ! router bgp 64496 no
synchronization bgp log-neighbor-changes neighbor
172.16.21.1 remote-as 64496 !--- Configure Router21 as
an iBGP peer. neighbor 172.16.21.1 next-hop-self
neighbor 172.16.21.1 default-originate route-map check-
ispb-route !--- A default route is advertised to
Router21 conditionally (based on whether the link !---
from Router22 to ISP-B is active). ! neighbor
172.16.21.1 distribute-list 1 out neighbor 172.16.23.4
remote-as 64503 neighbor 172.16.23.4 route-map adv-to-
ispb out ! ip route 172.16.21.0 255.255.255.0
172.16.22.10 !--- Static route to iBGP peer, because it
```

```
is not directly connected. ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.30.0 0.0.0.255 access-list 21 permit
172.16.23.4 ! route-map check-ispb-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispb permit 10 match ip address 10 set as-path prepend
10 10 10 !--- Route map used to change the AS path
attribute of outgoing updates.
```

Router24 (ISP-B)

```
hostname Router24
!
interface Loopback0
 ip address 10.10.30.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.16.23.4 255.255.255.0
!
router bgp 64503
 bgp log-neighbor-changes
 network 10.10.30.0 mask 255.255.255.0
 neighbor 172.16.23.2 remote-as 64496
!--- Configures Router22 as an eBGP peer. !
```

PIX1

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
!--- Configures the IP addresses for the inside and
outside interfaces. access-list acl-1 permit tcp host
172.16.12.2 host 172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !---
Allows ping to pass through for testing purposes only.

access-group acl-1 in interface outside
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
!--- No NAT translation, to allow Router11 on the inside
to initiate a BGP session !--- to Router12 on the
outside of PIX. static (inside,outside) 172.16.11.1
172.16.11.1 netmask 255.255.255.255 !--- Static NAT
translation, to allow Router12 on the outside to
initiate a BGP session !--- to Router11 on the inside of
PIX. route outside 0.0.0.0 0.0.0.0 172.16.12.2 1 route
inside 192.168.10.0 255.255.255.0 172.16.11.1 1
```

PIX2

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.22.10 255.255.255.0
ip address inside 172.16.21.10 255.255.255.0
!--- Configures the IP addresses for the inside and
outside interfaces. access-list acl-1 permit tcp host
172.16.22.2 host 172.16.21.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !---
Allows ping to pass through for testing purposes only.

access-group acl-1 in interface outside
```

```
route outside 0.0.0.0 0.0.0.0 172.16.22.2 1
route inside 192.168.10.0 255.255.255.0 172.16.21.1 1
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
!--- No NAT translation, to allow Router21 on the inside
to initiate a BGP session !--- to Router22 on the
outside of PIX. static (inside,outside) 172.16.21.1
172.16.21.1 netmask 255.255.255.255 ! -- Static NAT
translation, to allow Router22 on the outside to
initiate a BGP session !--- to Router21 on the inside of
PIX.
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Quando entrambe le sessioni BGP sono attive, tutti i pacchetti devono essere instradati tramite ISP-A. Prendere in considerazione la tabella BGP sul router 11. Apprende una route predefinita 0.0.0.0/0 dal router 12 con l'hop successivo 172.16.12.2.

```
Router11# show ip bgp

BGP table version is 14, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i0.0.0.0          172.16.12.2                  100      0 i
*> 192.168.10.0     0.0.0.0                  0         32768 i
```

Il percorso predefinito 0.0.0.0/0 appreso tramite BGP viene installato nella tabella di routing, come mostrato nell'output del comando **show ip route** sul router 11.

```
Router11# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.12.2 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 2 subnets
S       172.16.12.0 [1/0] via 172.16.11.10
C       172.16.11.0 is directly connected, FastEthernet0/1
B*   0.0.0.0/0 [105/0] via 172.16.12.2, 00:27:24
```

Ora consideriamo la tabella BGP sul router 21. Impara anche la route predefinita tramite il router 22.

```
Router21# show ip bgp

BGP table version is 8, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i0.0.0.0          172.16.22.2                   100      0 i
*> 192.168.10.0     0.0.0.0                  0         32768
```

Verificare ora se la route predefinita appresa da BGP viene installata nella tabella di routing del router21.

```
Router21# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.21.0 is directly connected, FastEthernet0/1
S       172.16.22.0 [1/0] via 172.16.21.10
O*E2 0.0.0.0/0 [110/5] via 192.168.10.1, 00:27:06, FastEthernet0/0
```

La route predefinita nel router 21 viene appresa tramite OSPF (notare il prefisso o sulla route 0.0.0.0/0). È interessante notare che esiste una route predefinita appresa tramite BGP dal router22, ma l'output **show ip route** mostra la route predefinita appresa tramite OSPF.

La route predefinita OSPF è stata installata nel router 21 perché il router 21 apprende la route predefinita da due origini: Router22 via iBGP e Router11 via OSPF. Il processo di selezione del percorso installa il percorso nella tabella di routing con una distanza amministrativa migliore. La distanza amministrativa di OSPF è 110, mentre la distanza amministrativa di iBGP è 200. Pertanto, la route predefinita appresa da OSPF viene installata nella tabella di routing, in quanto 110 è inferiore a 200. Per ulteriori informazioni sulla selezione della route, consultare il documento sulla selezione della route nei router Cisco.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Interrompere la sessione BGP tra il router 12 e l'ISP-A.

```
Router12(config)# interface fas 0/0

Router12(config-if)# shut

1w0d: %LINK-5-CHANGED: Interface FastEthernet0/0,
      changed state to administratively down
1w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
      changed state to down
```

Il router 11 non dispone della route predefinita appresa tramite BGP dal router 12.

```
Router11# show ip bgp

BGP table version is 16, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0     0.0.0.0                  0
```

Controllare la tabella di routing sul router 11. La route predefinita viene rilevata tramite OSPF (distanza amministrativa di 110) con un hop successivo di Router 21.

```
Router11# show ip route
!--- Output suppressed. Gateway of last resort is 192.168.10.2 to network 0.0.0.0 C
192.168.10.0/24 is directly connected, FastEthernet0/0 172.16.0.0/24 is subnetted, 2 subnets S
172.16.12.0 [1/0] via 172.16.11.10 C 172.16.11.0 is directly connected, FastEthernet0/1 O*E2
0.0.0.0/0 [110/30] via 192.168.10.2, 00:00:09, FastEthernet0/0
```

Questo output è previsto in base ai criteri predefiniti. A questo punto, tuttavia, è importante capire il comando di configurazione **bgp 20 105 200** per la **distanza** nel router 11 e come influisce sulla selezione del percorso sul router 11.

I valori predefiniti di questo comando sono **la distanza bgp 20 200 200**, dove le route eBGP-Led hanno una distanza amministrativa di 20, le route iBGP-Led una distanza amministrativa di 200 e le route BGP locali hanno una distanza amministrativa di 200.

Quando il collegamento tra il router 12 e l'ISP-A ricompare, il router 11 apprende la route predefinita tramite iBGP dal router 12. Tuttavia, poiché la distanza amministrativa predefinita di questa route iBGP-Led è 200, non sostituirà la route OSPF-Led (poiché 110 è inferiore a 200). In questo modo, viene forzato tutto il traffico in uscita verso il collegamento tra il router 21 e il router 22 e l'ISP-B, anche se il collegamento tra il router 12 e l'ISP-A è di nuovo attivo. Per risolvere questo problema, modificare la distanza amministrativa della route iBGP appresa in un valore inferiore al protocollo IGP (Interior Gateway Protocol) utilizzato. In questo esempio, l'IGP è OSPF, quindi è stata scelta una distanza di 105 (poiché 105 è inferiore a 110).

Per ulteriori informazioni sul comando **distance bgp**, consultare il documento sui comandi BGP. Per ulteriori informazioni sul multihoming con BGP, fare riferimento a Condivisione del carico con BGP in ambienti single e multihomed: Esempi di configurazione.

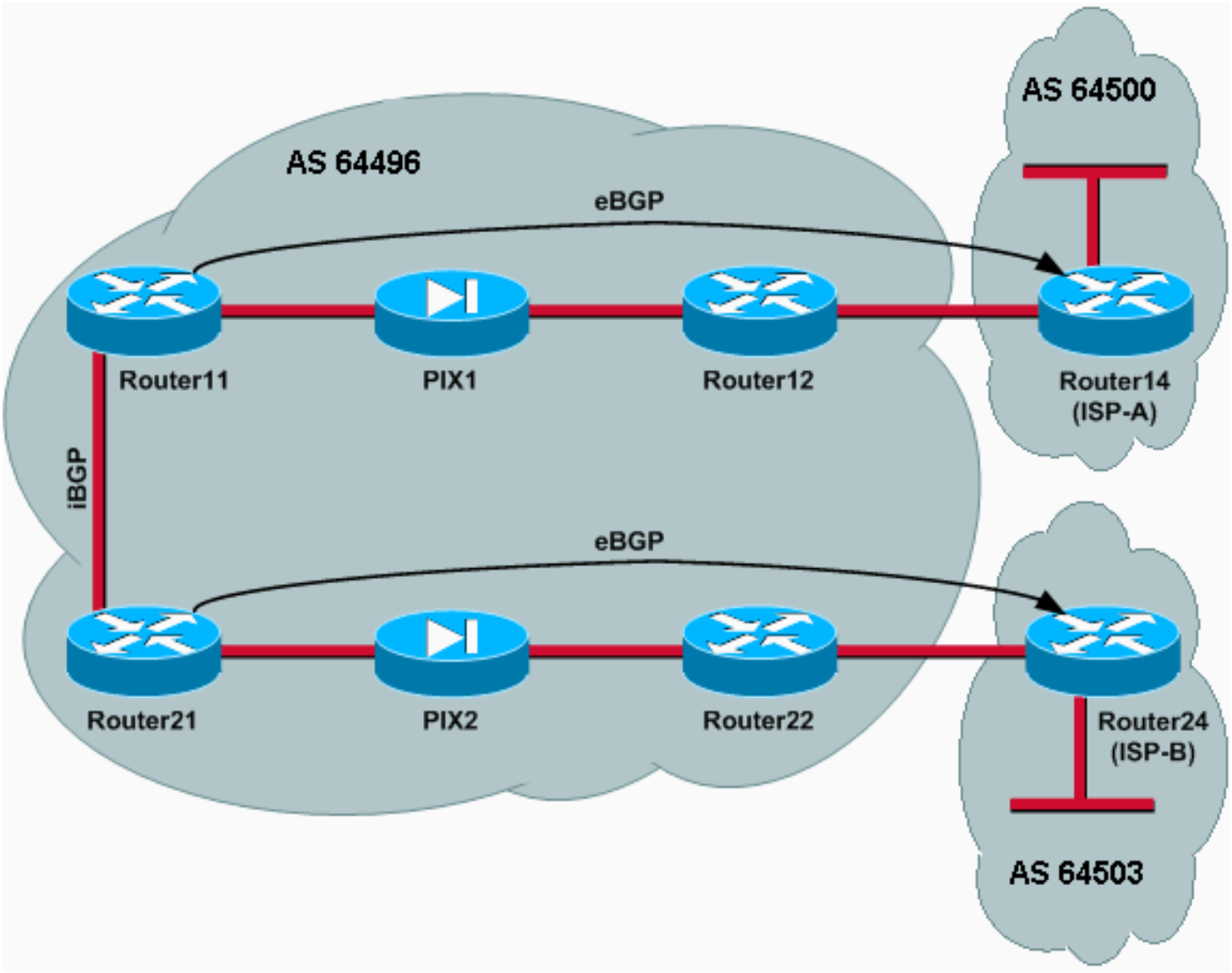
Scenario 2

In questo scenario, il router 11 è il peering eBGP diretto con il router 14 (ISP-A), mentre il router 21 è il peering eBGP diretto con il router 24 (ISP-B). Il router 12 e il router 22 non partecipano al peer BGP, ma forniscono la connettività IP agli ISP. Poiché i peer eBGP non sono vicini connessi direttamente, sui router partecipanti viene utilizzato il comando **neighbors ebgp-multihop**. Il comando **neighbors ebgp-multihop** consente a BGP di ignorare il limite eBGP predefinito di un hop perché modifica il valore TTL (Time to Live) dei pacchetti eBGP dal valore predefinito 1. In questo scenario, il router adiacente eBGP è a 3 hop di distanza, quindi il **router adiacente ebgp-multihop 3** è configurato sui router partecipanti in modo che il valore TTL venga modificato in 3. Inoltre, sui router e sul PIX vengono configurate route statiche per garantire che il router 11 possa eseguire il ping sull'indirizzo 14 (ISP-A) 17 1.16.13.4 e di assicurare che il router 21 possa eseguire il ping

sull'indirizzo 172.16.23.4 del router 24 (ISP-B).

per impostazione predefinita, il protocollo PIX non consente la trasmissione di pacchetti ICMP (Internet Control Message Protocol), inviati quando si esegue il comando **ping**. Per consentire i pacchetti ICMP, usare il comando **access-list** come mostrato nella successiva configurazione PIX. Per ulteriori informazioni sul comando **access-list**, consultare i comandi da A a B di PIX Firewall.

Il criterio di routing è lo stesso dello scenario 1: il collegamento tra il router 12 e l'ISP-A è da preferire al collegamento tra il router 22 e l'ISP-B e, quando il collegamento ISP-A è interrotto, il collegamento ISP-B viene utilizzato per tutto il traffico in entrata e in uscita.



Configurazioni

In questo scenario vengono utilizzate le configurazioni seguenti:

- Router11
- Router12
- Router 14 (ISP-A)
- Router21
- Router22
- PIX1
- PIX2

Router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.13.4 remote-as 64500 neighbor 172.16.13.4 ebgp-
multihop 3 !--- To accept and attempt BGP connections to
external peers that reside on networks that !--- are not
directly connected. neighbor 172.16.13.4 route-map set-
pref in !--- Sets higher local-preference for learned
routes. neighbor 172.16.13.4 route-map adv_to_ispa out
neighbor 192.168.10.2 remote-as 64496 neighbor
192.168.10.2 next-hop-self no auto-summary ! ip route
172.16.12.0 255.255.255.0 172.16.11.10 ip
route172.16.13.4 255.255.255.255 172.16.11.10 !---
Static route to eBGP peer, because it is not directly
connected. ! access-list 20 permit 192.168.10.0 ! route-
map set-pref permit 10 set local-preference 200 ! route-
map adv_to_ispa permit 10 match ip address 20 !
```

Router12

```
hostname Router12
!
interface FastEthernet0/0
 ip address 172.16.13.2 255.255.255.0
!--- Connected to ISP-A. ! interface FastEthernet0/1 ip
address 172.16.12.2 255.255.255.0 !--- Connected to
PIX1. ! ip route 172.16.11.0 255.255.255.0 172.16.12.10
ip route 192.168.10.0 255.255.255.0 172.16.12.10
```

Router 14 (ISP-A)

```
hostname Router14
!
interface Ethernet0/0
 ip address 172.16.13.4 255.255.255.0
!
interface Ethernet0/1
 ip address 10.10.20.1 255.255.255.0
!
router bgp 64500
no synchronization
network 10.10.20.0 mask 255.255.255.0
 neighbor 172.16.11.1 remote-as 64496
 neighbor 172.16.11.1 ebgp-multihop 3
!--- To accept and attempt BGP connections to external
peers that reside on networks that !--- are not directly
connected. neighbor 172.16.11.1 default-originate !---
Advertises a default route to Router11. no auto-summary
! ip route 172.16.11.1 255.255.255.255 172.16.13.2 !---
Static route to eBGP peers, because it is not directly
connected.
```

Router21

```
hostname Router21
```

```
 !
 interface FastEthernet0/0
  ip address 192.168.10.2 255.255.255.0
!--- Connected to Router11. ! interface FastEthernet0/1
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router bgp 64496 no synchronization network
192.168.10.0 neighbor 172.16.23.4 remote-as 64503
neighbor 172.16.23.4 ebgp-multihop 3 !--- To accept and
attempt BGP connections to external peers that reside on
networks that !--- are not directly connected. neighbor
172.16.23.4 route-map adv_to_ispb out neighbor
192.168.10.1 remote-as 64496 neighbor 192.168.10.1 next-
hop-self no auto-summary ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 ip route172.16.23.4
255.255.255.255 172.16.21.10 !--- Static routes
configured to reach BGP peer. ! access-list 20 permit
192.168.10.0 ! route-map adv_to_ispb permit 10 match ip
address 20 set as-path prepend 10 10 10
```

Router22

```
hostname Router22
!
interface FastEthernet0/0
 ip address 172.16.23.2 255.255.255.0
!--- Connected to Router24 (ISP-B). ! interface
FastEthernet0/1 ip address 172.16.22.2 255.255.255.0 !--
- Connected to PIX2. ! ip route 172.16.21.0
255.255.255.0 172.16.22.10 ip route 192.168.10.0
255.255.255.0 172.16.22.10
```

Router24 (ISP-B)

```
hostname Router24
!
interface Loopback0
 ip address 10.10.30.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.16.23.4 255.255.255.0
!--- Connected to Router22. ! router bgp 64503 no
synchronization bgp log-neighbor-changes network
10.10.30.0 mask 255.255.255.0 neighbor 172.16.21.1
remote-as 64496 neighbor 172.16.21.1 ebgp-multihop 3 !--
- To accept and attempt BGP connections to external
peers that reside on networks that !--- are not directly
connected. neighbor 172.16.21.1 default-originate !---
Advertises a default route to Router21. no auto-summary
! ip route 172.16.21.1 255.255.255.255 172.16.23.2 !---
Static route for BGP peer Router11, because it is not
directly connected.
```

PIX1

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!-- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !--
Allows ping to pass through for testing purposes only.
```

```
access-group acl-1 in interface outside
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.11.1 172.16.11.1 netmask
255.255.255.255
route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1
```

PIX2

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.22.10 255.255.255.0
ip address inside 172.16.21.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.23.4 host
172.16.21.1 eq bgp
!-- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !--
Allows ping to pass through for testing purposes only.

access-group acl-1 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.22.2 1
route inside 192.168.10.0 255.255.255.0 172.16.21.1 1
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.21.1 172.16.21.1 netmask
255.255.255.255
```

Verifica

Iniziare con la situazione in cui i collegamenti a ISP-A e ISP-B sono attivi. L'output del comando **show ip bgp summary** sul router 11 e sul router 21 conferma le sessioni BGP stabilite rispettivamente con ISP-A e ISP-B.

```
Router11# show ip bgp summary

BGP router identifier 192.168.10.1, local AS number 10
BGP table version is 13, main routing table version 13
4 network entries and 5 paths using 568 bytes of memory
7 BGP path attribute entries using 420 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 43/264 prefixes, 75/70 paths, scan interval 15 secs


Neighbor        V    AS     MsgRcvd  MsgSent   TblVer  InQ OutQ   Up/Down   State/PfxRcd
172.16.13.4     4    64500     1627     1623       13    0    0   02:13:36        2
192.168.10.2    4    64496      1596     1601       13    0    0   02:08:47        2

Router21# show ip bgp summary
!--- Output suppressed. Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
172.16.23.4 4 64503 1610 1606 8 0 0 02:06:22 2 192.168.10.1 4 64496 1603 1598 8 0 0 02:10:16 3
```

La tabella BGP sul router 11 mostra il percorso predefinito (0.0.0.0/0) verso l'hop successivo ISP-A 172.16.13.4.

```
Router11# show ip bgp

BGP table version is 13, local router ID is 192.168.10.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          172.16.13.4                  200      0 20 i
*> 10.10.20.0/24    172.16.13.4              0   200      0 64500 i
*>i10.10.30.0/24    192.168.10.2             0   100      0 64503 i
* i192.168.10.0     192.168.10.2             0   100      0 i
*>                  0.0.0.0                  0         32768 i
```

Controllare la tabella BGP sul router 21. Dispone di due route 0.0.0.0/0: uno ha appreso dall'ISP-B con un hop successivo di 172.16.23.4 su eBGP, l'altro ha appreso tramite iBGP con una preferenza local-priority di 200. Router21 preferisce le route iBGP-Led a causa dell'attributo di preferenza local più alto, quindi installa tale route nella tabella di routing. Per ulteriori informazioni sulla selezione del percorso BGP, fare riferimento all'algoritmo di selezione del miglior percorso BGP.

```
Router21# show ip bgp

BGP table version is 8, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete


Network          Next Hop                Metric LocPrf Weight Path
*  0.0.0.0          172.16.23.4                          0    64503 i
*>i                 192.168.10.1                 200      0    64500 i
*>i10.10.20.0/24    192.168.10.1             0   200      0    64500 i
*> 10.10.30.0/24    172.16.23.4              0            0    64503 i
*> 192.168.10.0     0.0.0.0                  0         32768       i
* i                 192.168.10.1             0   100      0 i
```

Risoluzione dei problemi

Interrompere la sessione BGP del router 11 e dell'ISP-A.

```
Router11(config)# interface fas 0/1

Router11(config-if)# shut

4w2d: %LINK-5-CHANGED: Interface FastEthernet0/1,
      changed state to administratively down
4w2d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
      changed state to down
4w2d: %BGP-5-ADJCHANGE: neighbor 172.16.13.4 Down BGP Notification sent
4w2d: %BGP-3-NOTIFICATION: sent to neighbor 172.16.13.4 4/0 (hold time expired)0 bytes
```

La sessione eBGP sull'ISP-A si interrompe quando scade il timer di attesa (180 secondi).

```
Router11# show ip bgp summary
!--- Output suppressed. Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
172.16.13.4 4 64500 1633 1632 0 0 0 00:00:58 Active 192.168.10.2 4 64496 1609 1615 21 0 0
02:18:09
```

Quando il collegamento all'ISP-A è inattivo, il router 11 installa il file 0.0.0.0/0 con l'hop successivo 192.168.10.2 (Router 21), che viene individuato tramite iBGP nella relativa tabella di routing. In questo modo tutto il traffico in uscita passa attraverso il router 21 e quindi all'ISP-B, come mostrato nell'output:

```
Router11# show ip bgp

BGP table version is 21, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i0.0.0.0          192.168.10.2                100      0 64503 i
*>i10.10.30.0/24    192.168.10.2             0    100      0 64503 i
* i192.168.10.0     192.168.10.2             0    100      0 i
*>                  0.0.0.0                  0         32768 i

Router21# show ip bgp

BGP table version is 14, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          172.16.23.4                            0 64503 i
*> 10.10.30.0/24    172.16.23.4              0             0 64503 i
*> 192.168.10.0     0.0.0.0                  0         32768 i
* i                 192.168.10.1             0    100      0 i
```

Autenticazione MD5 per router adiacenti BGP tramite PIX/ASA

Configurazione PIX 6.x

Come qualsiasi altro protocollo di routing, è possibile configurare il protocollo BGP per l'autenticazione. È possibile configurare l'autenticazione MD5 tra due peer BGP, in modo che venga verificato ciascun segmento inviato sulla connessione TCP tra i peer. L'autenticazione MD5 deve essere configurata con la stessa password su entrambi i peer BGP; in caso contrario, il collegamento tra di essi non sarà stabilito. La configurazione dell'autenticazione MD5 fa sì che il software Cisco IOS generi e controlli il digest MD5 di ogni segmento inviato sulla connessione TCP. Se l'autenticazione viene richiamata e un segmento non riesce, viene generato un messaggio di errore.

Quando si configurano i peer BGP con autenticazione MD5 che passano attraverso un firewall PIX, è importante configurare il PIX tra i vicini BGP in modo che i numeri di sequenza per i flussi TCP tra i vicini BGP non siano casuali. Infatti, la funzione TCP Random Sequence Number sul firewall PIX è abilitata per impostazione predefinita e modifica il numero di sequenza TCP dei pacchetti in arrivo prima di inoltrarli.

L'autenticazione MD5 viene applicata all'intestazione PSU-IP TCP, all'intestazione TCP e ai dati (consultare la RFC 2385). Il protocollo TCP utilizza questi dati, inclusi la sequenza TCP e i numeri ACK, insieme alla password dei nodi adiacenti BGP per creare un numero hash a 128 bit. Il numero hash viene incluso nel pacchetto nel campo delle opzioni dell'intestazione TCP. Per impostazione predefinita, il PIX sposta il numero di sequenza di un numero casuale, per flusso TCP. Sul peer BGP di invio, il protocollo TCP usa il numero di sequenza originale per creare il numero hash MD5 a 128 bit e include questo numero hash nel pacchetto. Quando il peer BGP ricevente riceve il pacchetto, il protocollo TCP usa il numero di sequenza modificato dal PIX per creare un numero hash MD5 a 128 bit e lo confronta con il numero hash incluso nel pacchetto.

Il numero hash è diverso perché il valore della sequenza TCP è stato modificato dal PIX e il protocollo TCP sul router adiacente BGP scarta il pacchetto e registra un messaggio di errore

MD5 simile al seguente:

```
%TCP-6-BADAUTH: Invalid MD5 digest from 172.16.11.1:1778 to 172.16.12.2:179
```

Per risolvere il problema, usare la parola chiave **norandomseq** con il comando **static (inside,outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq** e impedire che il PIX esegua l'offset del numero di sequenza TCP. Nell'esempio viene mostrato come usare la parola chiave **norandomseq**:

Router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router ospf 1 log-adjacency-changes network
192.168.10.0 0.0.0.255 area 0 default-information
originate metric 5 route-map check-default !--- A
default route is originated conditionally, with a metric
of 5. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.12.2 remote-as 64496 neighbor 172.16.12.2
password 7 08345C5A001A1511110D04

!--- Configures MD5 authentication on BGP. distance bgp
20 105 200 !--- Administrative distance of iBGP-learned
routes is changed from default 200 to 105. !--- MD5
authentication is configured for BGP. no auto-summary !
ip route 172.16.12.0 255.255.255.0 172.16.11.10 !---
Static route to iBGP peer, because it is not directly
connected. ! access-list 30 permit 0.0.0.0 access-list
31 permit 172.16.12.2 route-map check-default permit 10
match ip address 30 match ip next-hop 31
```

Router12

```
hostname Router12
!
interface FastEthernet0/0
 ip address 172.16.13.2 255.255.255.0
!--- Connected to ISP-A. ! interface FastEthernet0/1 ip
address 172.16.12.2 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization neighbor
172.16.11.1 remote-as 64496 neighbor 172.16.11.1 next-
hop-self neighbor 172.16.11.1 default-originate route-
map neighbor 172.16.11.1 password 7
08345C5A001A1511110D04
!--- Configures MD5 authentication on BGP. check-ispa-
route !--- Originate default to Router11 conditionally
if check-ispa-route is a success. !--- MD5
authentication is configured for BGP.

 neighbor 172.16.11.1 distribute-list 1 out
 neighbor 172.16.13.4 remote-as 64500
 neighbor 172.16.13.4 route-map adv-to-ispa out
 no auto-summary
!
ip route 172.16.11.0 255.255.255.0 172.16.12.10
!--- Static route to iBGP peer, because it is not
```

```
directly connected. ! access-list 1 permit 0.0.0.0
access-list 10 permit 192.168.10.0 access-list 20 permit
10.10.20.0 0.0.0.255 access-list 21 permit 172.16.13.4 !
route-map check-ispa-route permit 10 match ip address 20
match ip next-hop 21 ! route-map adv-to-ispa permit 10
match ip address 10
```

PIX1

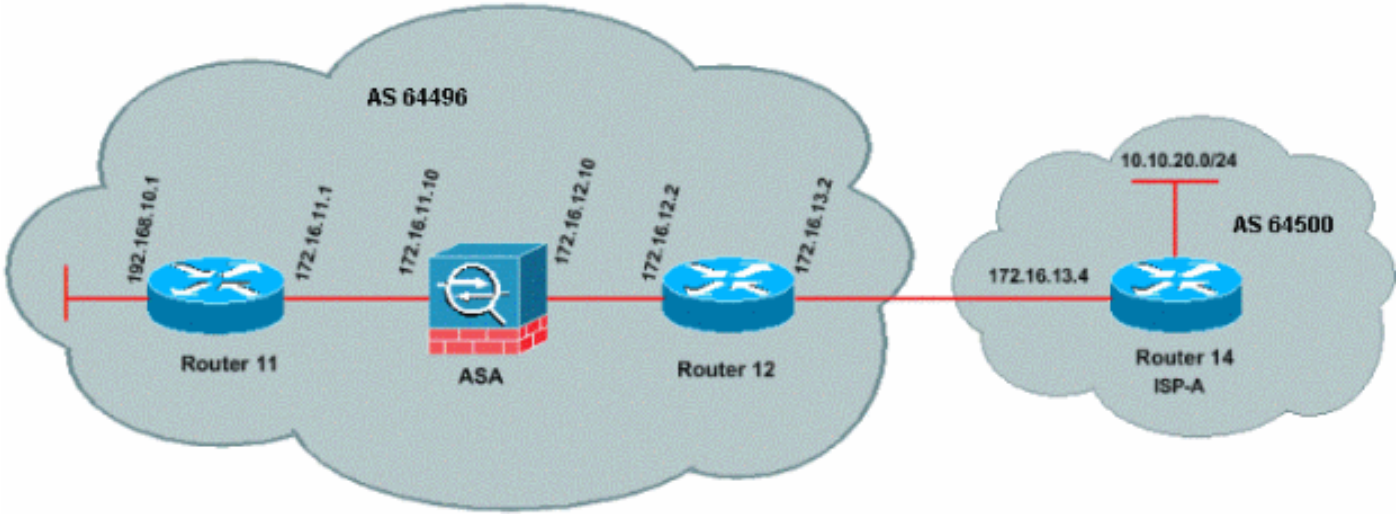
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !---
Allows ping to pass through for testing purposes only.

access-group acl-1 in interface outside
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.11.1 172.16.11.1 netmask
255.255.255.255 norandomseq

!--- Stops the PIX from offsetting the TCP sequence
number. route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1
```

PIX/ASA 7.x e versioni successive

Questa sezione utilizza questa configurazione di rete.



La versione 7.x di PIX/ASA e successive introducono un ulteriore problema quando si tenta di stabilire una sessione di peering BGP con autenticazione MD5. Per impostazione predefinita, PIX/ASA versione 7.x e successive riscrive qualsiasi opzione TCP MD5 inclusa in un datagramma TCP che passa attraverso il dispositivo e sostituisce il tipo, le dimensioni e il valore dell'opzione con byte dell'opzione NOP. L'autenticazione BGP MD5 viene interrotta e vengono visualizzati messaggi di errore come questo su ciascun router peer:

```
000296: 7 apr 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: Nessun digest MD5 da 172.16.11.1(28894) a
172.16.12.2(179)
```

Affinché una sessione BGP con autenticazione MD5 venga stabilita correttamente, è necessario

risolvere i tre problemi seguenti:

- Disabilita randomizzazione numeri di sequenza TCP
- Disattiva riscrittura opzione TCP MD5
- Disabilita NAT tra peer

Una mappa delle classi e un elenco degli accessi vengono utilizzati per selezionare il traffico tra i peer che devono essere entrambi esentati dalla funzionalità di casualizzazione del numero di sequenza TCP e autorizzati a trasportare un'opzione MD5 senza riscrittura. Una mappa TCP viene usata per specificare il tipo di opzione da consentire, in questo caso il tipo di opzione 19 (opzione TCP MD5). La class-map e la tcp-map sono entrambe collegate attraverso una policy-map, parte dell'infrastruttura Modular Policy Framework. La configurazione viene quindi attivata con il comando **service-policy**.

Nota: La necessità di disabilitare il protocollo NAT tra i peer è gestita dal comando **no nat-control**.

Nella versione 7.0 e successive, la natura predefinita di un'ASA è **no nat-control**, che indica che per impostazione predefinita ogni connessione tramite ASA non deve superare il test NAT. Si presume che l'impostazione predefinita per l'ASA sia **no nat-control**. Per ulteriori informazioni, fare riferimento a nat-control. Se l'opzione **nat-control** è applicata, è necessario disabilitare esplicitamente NAT per i peer BGP. A tale scopo, è possibile usare il comando **statico** tra le interfacce interne ed esterne.

```
static (inside, outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.255
```

PIX/ASA 7.x/8.x

```
ciscoasa# sh run
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
domain-name example.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface. interface
Ethernet0/0 nameif outside security-level 0 ip address
172.16.12.10 255.255.255.0 ! !--- Configure the inside
interface. interface Ethernet0/1 nameif inside security-
level 100 ip address 172.16.11.10 255.255.255.0 ! !--
Output suppressed. !--- Access list to allow incoming
BGP sessions !--- from the outside peer to the inside
peer access-list OUTSIDE-ACL-IN extended permit tcp host
172.16.12.2 host 172.16.11.1 eq  bgp


!--- Access list to match BGP traffic. !--- The next
line matches traffic from the inside peer to the outside
peer access-list BGP-MD5-ACL extended permit tcp host
172.16.11.1 host 172.16.12.2 eq  bgp
!--- The next line matches traffic from the outside peer
to the inside peer access-list BGP-MD5-ACL extended
permit tcp host 172.16.12.2 host 172.16.11.1 eq  bgp
```

```
!
!--- TCP-MAP to allow MD5 Authentication. tcp-map BGP-
MD5-OPTION-ALLOW
  tcp-options range 19 19 allow
!
!--- Apply the ACL that allows traffic !--- from the
outside peer to the inside peer access-group OUTSIDE-
ACL-IN in interface outside
!
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400

route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!
class-map inspection_default
 match default-inspection-traffic
class-map BGP-MD5-CLASSMAP
 match access-list BGP-MD5-ACL
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
 class BGP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options BGP-MD5-OPTION-ALLOW

!
service-policy global_policy global
prompt hostname context
```

```
Cryptochecksum:64ea55d7271e19eea87c8603ab3768a2
: end
```

Router11

```
Router11#sh run
hostname Router11
!
ip subnet-zero
!
interface Loopback0
 no ip address
 shutdown
!
interface Loopback1
 ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0
 ip address 172.16.11.1 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
router bgp 64496
 no synchronization
 bgp log-neighbor-changes
 network 192.168.10.0
 neighbor 172.16.12.2 remote-as 64496

!--- Configures MD5 authentication on BGP.  neighbor
172.16.12.2 password 7 123456789987654321

!--- Administrative distance of iBGP-learned routes is
changed from default 200 to 105. !--- MD5 authentication
is configured for BGP. distance bgp 20 105 200
 no auto-summary
!
ip classless
!--- Static route to iBGP peer, because it is not
directly connected. ip route 172.16.12.0 255.255.255.0
172.16.11.10
ip http server
!
!--- Output suppressed
```

Router12

```
Router12#sh run
hostname Router12
!
aaa new-model
!
```

```
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.13.2 255.255.255.0
!
interface Ethernet1
 ip address 172.16.12.2 255.255.255.0
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router bgp 64496
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.11.1 remote-as 64496

!--- Configures MD5 authentication on BGP. neighbor
172.16.11.1 password 7 123456789987654321
 neighbor 172.16.11.1 next-hop-self

!--- Originate default to Router11 conditionally if
check-ispa-route is a success

 neighbor 172.16.11.1 default-originate route-map check-
ispa-route
 neighbor 172.16.11.1 distribute-list 1 out
 neighbor 172.16.13.4 remote-as 64500
 no auto-summary
!
ip classless

!--- Static route to iBGP peer, because it is not
directly connected. ip route 172.16.11.0 255.255.255.0
172.16.12.10 ip http server ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.20.0 0.0.0.255 access-list 21 permit
172.16.13.4 route-map check-ispa-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispa permit 10 match ip address 10 ! !--- Output
suppressed
```

Router 14 (ISP-A)

```
Router14#sh run
hostname Router14
!
!
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.13.4 255.255.255.0
!
interface Ethernet1
 ip address 10.10.20.1 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
```

```
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router bgp 64500
 bgp log-neighbor-changes
 network 10.10.20.0 mask 255.255.255.0

!--- Configures Router12 as an eBGP peer. neighbor
172.16.13.2 remote-as 64496 ! !--- Output suppressed ip
classless
```

Verifica

L'output del comando **show ip bgp summary** indica che l'autenticazione ha esito positivo e che la sessione BGP è stata stabilita sul router 11.

```
Router11#show ip bgp summary
BGP router identifier 192.168.10.1, local AS number 64496
BGP table version is 8, main routing table version 8
3 network entries using 360 bytes of memory
3 path entries using 156 bytes of memory
2/2 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 764 total bytes of memory
BGP activity 25/22 prefixes, 26/23 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.13.2     4        64496     137     138        8    0    0 02:01:16        1
Router11#
```

Informazioni correlate

- Pagina di supporto BGP
- Algoritmo di selezione del miglior percorso BGP
- Condivisione del carico con BGP in ambienti singoli e multihome Esempi di configurazione
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Configurazione e test di PIX Firewall
- Documentazione e supporto tecnico – Cisco Systems