ASA/PIX: BGP com o exemplo de configuração ASA

Índice

Introdução

Esta configuração de exemplo demonstra como executar o Border Gateway Protocol (BGP) através de uma ferramenta de segurança (PIX/ASA) e como conseguir a Redundância em um BGP e em um ambiente PIX multihomed. Com um diagrama da rede como um exemplo, este documento explicar como distribuir automaticamente o tráfego ao provedor de serviço da Internet B (ISP-B) quando COMO 64496 perdem a Conectividade ao ISP-A (ou ao reverso), com o uso dos protocolos de roteamento dinâmico que se rodam entre todo o Roteadores COMO 64496.

Porque o BGP usa pacotes de TCP do unicast na porta 179 para se comunicar com seus pares, você pode configurar o PIX1 e o PIX2 para permitir o tráfego de unicast na porta TCP 179. Esta maneira, espreitar BGP pode ser estabelecida entre o Roteadores que é conectado com o Firewall. A Redundância e as políticas de roteamento desejadas podem ser conseguidas com a manipulação dos atributos de BGP.

Pré-requisitos

Requisitos

Os leitores deste documento devem ser familiares com configurar o BGP e a configuração de firewall básica.

Componentes Utilizados

Os exemplos de cenário neste documento são baseados nestas versões de software:

- Cisco 2600 Router com Cisco IOS? Software Release 12.2(27)
- PIX 515 com versão 6.3(3) e mais recente do Cisco PIX Firewall

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- 5500 Series adaptável da ferramenta de segurança de Cisco (ASA) com versão 7.x e mais tarde
- Módulo de serviços de firewall de Cisco (FWSM) essa versão de software 3.2 das corridas e mais atrasado

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

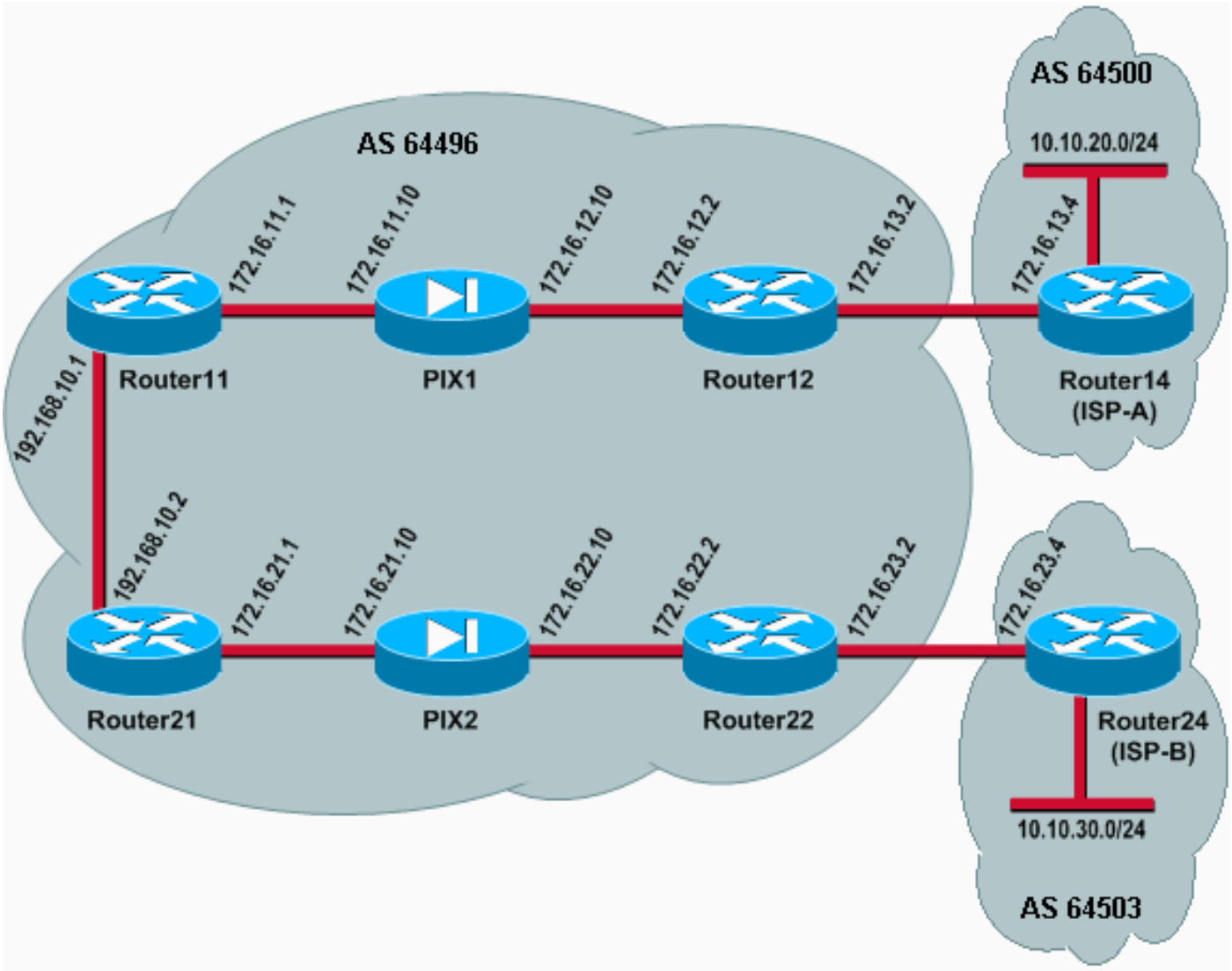
Configurar

Esta seção fornece a informação para configurar as características descritas neste documento.

Note: Para encontrar a informação adicional sobre os comandos neste documento, use a ferramenta de consulta de comandos (clientes registrados somente).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nesta instalação de rede, Roteador12 e Roteador22 (que pertencem COMO a 64496) são multihomed a Roteador14 (ISP-A) e a Roteador24 (ISP-B) respectivamente, para a Redundância. A rede interna 192.168.10.0/24 está no interior do Firewall. Roteador11 e Roteador21 conectam a Roteador12 e a Roteador22 com o Firewall. O PIX1 e o PIX2 não são configurados para executar o Network Address Translation (NAT).

Cenário 1

Nesta encenação, Roteador12 dentro COMO 64496 faz o external bgp (ebgp) peering com Roteador14 (ISP-A) dentro COMO 64500. Roteador12 igualmente faz o Internal BGP (iBGP) que espreita com Roteador11 com o PIX1. Se as rotas aprendidas do eBGP do ISP-A estam presente, Roteador12 anuncia uma rota padrão 0.0.0.0/0 no iBGP a Roteador11. Se o link ao ISP-A falha, Roteador12 para de anunciar a rota padrão.

Similarmente, Roteador22 dentro COMO 64496 faz o peering eBGP com Roteador24 (ISP-B) dentro COMO 64503 e anuncia uma rota padrão no iBGP a Roteador21 baseado condicionalmente na presença de rotas do ISP-B em sua tabela de roteamento.

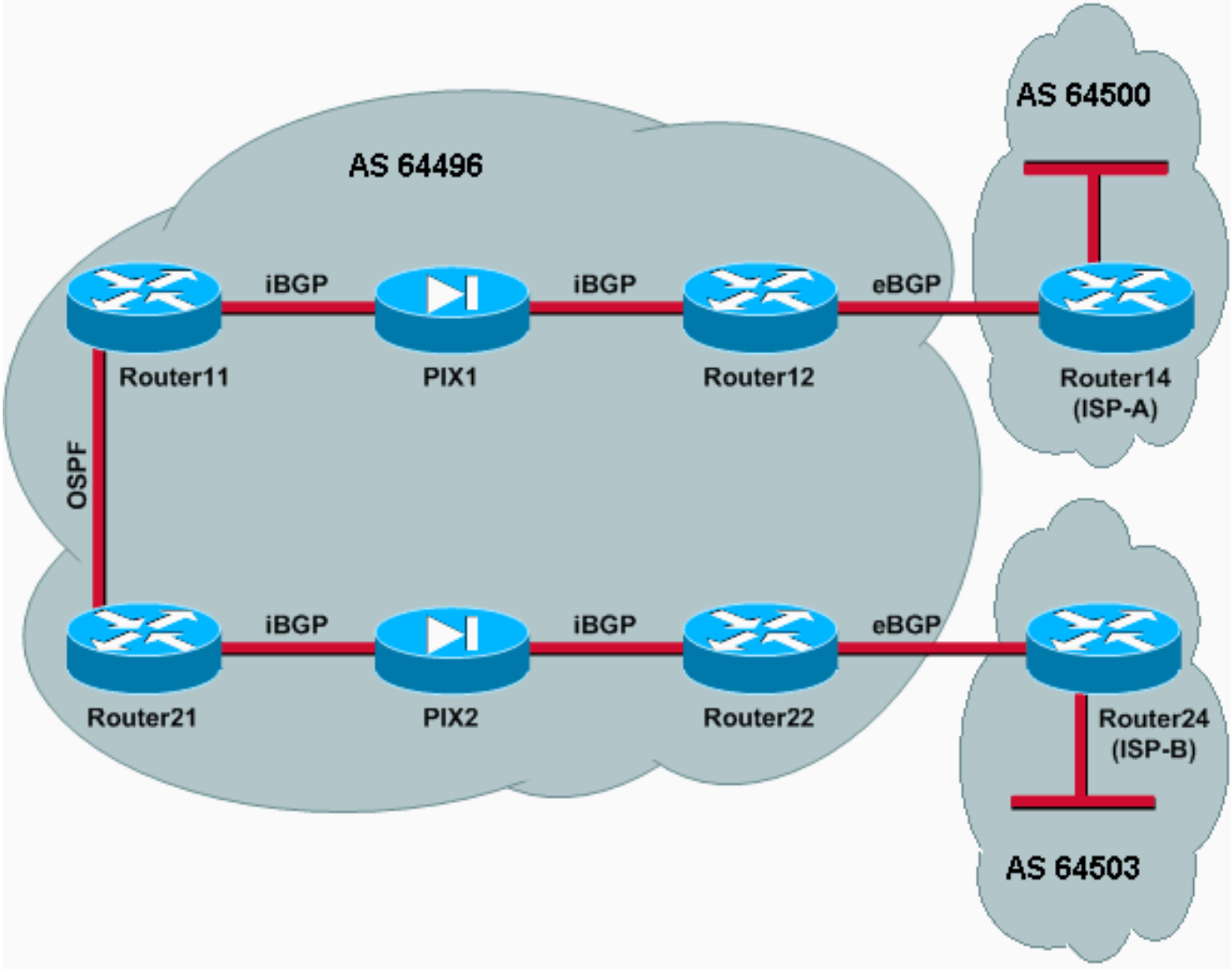
Com o uso de uma lista de acessos, o PIX1 e o PIX2 são configurados para permitir o tráfego BGP (TCP, porta 179) entre pares do iBGP. Isto é porque as interfaces de PIX têm um nível de segurança associado. À revelia, a interface interna (ethernet1) tem um nível de segurança 100 e a interface externa (ethernet0) tem conexões e tráfego do nível de segurança um 0. é permitida normalmente de mais altamente às interfaces de nível de seguranca mais baixo. Para permitir o

tráfego de uma interface de nível de seguranca mais baixo a uma interface do nível de segurança mais elevado, contudo, você deve explicitamente definir uma lista de acessos no PIX. Também, você deve configurar uma tradução NAT estática no PIX1 e no PIX2, para permitir que o Roteadores na parte externa inicie uma sessão de BGP com o Roteadores no interior do PIX.

Roteador11 e Roteador21 anunciam condicionalmente a rota padrão no domínio do Open Shortest Path First (OSPF) baseado na rota padrão iBGP-instruída. Roteador11 anuncia a rota padrão no domínio de OSPF com uma métrica de 5, Roteador21 anuncia a rota padrão com uma métrica de 30, e consequentemente a rota padrão de Roteador11 é preferida. Esta configuração ajuda a propagação somente a rota padrão 0.0.0.0/0 a Roteador11 e a Roteador21, que conserva o consumo de memória nos roteadores internos e consegue o desempenho ideal.

Assim, para resumir estas circunstâncias, esta é a política de roteamento para COMO 64496:

- COMO 64496 preferem o link de Roteador12 ao ISP-A para todo o tráfego de saída (de 192.168.10.0/24 ao Internet).
- Se a Conectividade ao ISP-A falha, todo o tráfego está distribuído através do link de Roteador22 ao ISP-B.
- Todo o tráfego que vem do Internet a 192.168.10.0/24 usa o link do ISP-à Roteador12.
- Se o link do ISP-à Roteador12 falha, todo o tráfego de entrada está distribuído através do link do ISP-B a Roteador22.



Configurações

Esta encenação usa estas configurações:

- Roteador11
- Roteador12
- Roteador14 (ISP-A)
- Roteador21
- Roteador22
- PIX1
- PIX2

Roteador11

```
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
```

Roteador12

```
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
```

Roteador14 (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. !
```

Roteador21

```
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 !
```

Roteador22

```
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.
```

Roteador24 (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.
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Quando ambas as sessões de BGP estão acima, você pode esperar todos os pacotes ser distribuído através do ISP-A. Considere a tabela de BGP em Roteador11. Aprende uma rota padrão 0.0.0.0/0 de Roteador12 com o salto seguinte 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
```

As 0.0.0.0/0 rotas padrão que é instruída através do BGP são instaladas na tabela de roteamento, segundo as indicações da saída da **rota da mostra IP em** Roteador11.

```
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
```

Considere agora a tabela de BGP em Roteador21. Igualmente aprende a rota padrão através de Roteador22.

```
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
```

Veja agora se esta rota padrão aprendido a rota de BGP obtém instalada na tabela de roteamento de Roteador21.

```
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
```

A rota padrão em Roteador21 é instruída através do OSPF (note o prefixo `O nas` 0.0.0.0/0 rotas). É interessante notar que há uma rota padrão aprendida através do BGP de Roteador22, mas a saída da **rota da mostra IP** mostra a rota padrão aprendida através do OSPF.

A rota padrão OSPF foi instalada em Roteador21 porque Roteador21 aprende a rota padrão de duas fontes: Roteador22 através do iBGP e Roteador11 através do OSPF. O processo de seleção de rota instala a rota com uma distância administrativa melhor na tabela de roteamento. A distância administrativa de OSPF é 110 quando a distância administrativa de iBGP for 200. Consequentemente, a rota padrão OSPF-instruída obtém instalada na tabela de roteamento, porque 110 são menos de 200. Para obter mais informações sobre da seleção de rota, refira a seleção de rota nos roteadores Cisco.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Derrube a sessão de BGP entre Roteador12 e o 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
```

Roteador11 não tem a rota padrão aprendida através do BGP de Roteador12.

```
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
```

Verifique a tabela de roteamento em Roteador11. A rota padrão é instruída através de OSPF (distância administrativa de 110) com um salto seguinte de Roteador21.

```
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
```

Esta saída é esperada conforme as políticas predefinidas. Neste momento, contudo, é importante compreender o **BGP 20 da distância o** comando configuration **105 200 em** Roteador11 e como influencia a seleção de rota em Roteador11.

Os valores padrão deste comando são **BGP 20 da distância 200 200**, onde as rotas eBGP-instruídas têm uma distância administrativa de 20, rotas ensinada pelo iBGP têm uma distância administrativa de 200, e as rotas de BGP locais têm uma distância administrativa de 200.

Quando o link entre Roteador12 e o ISP-A vem acima outra vez, Roteador11 aprende a rota padrão através do iBGP de Roteador12. Contudo, porque a distância administrativa padrão desta rota ensinada pelo iBGP é 200, não substituirá a rota OSPF-instruída (porque 110 são menos de 200). Isto força todo o tráfego de saída ao link de Roteador21 a Roteador22 ao ISP-B, mesmo que o link de Roteador12 ao ISP-A esteja acima outra vez. Para resolver esta edição, mude a distância administrativa da rota ensinada pelo iBGP a um valor menos do que o Interior Gateway Protocol (IGP) usado. Neste exemplo, o IGP é OSPF, assim que uma distância de 105 foi escolhida (porque 105 são menos de 110).

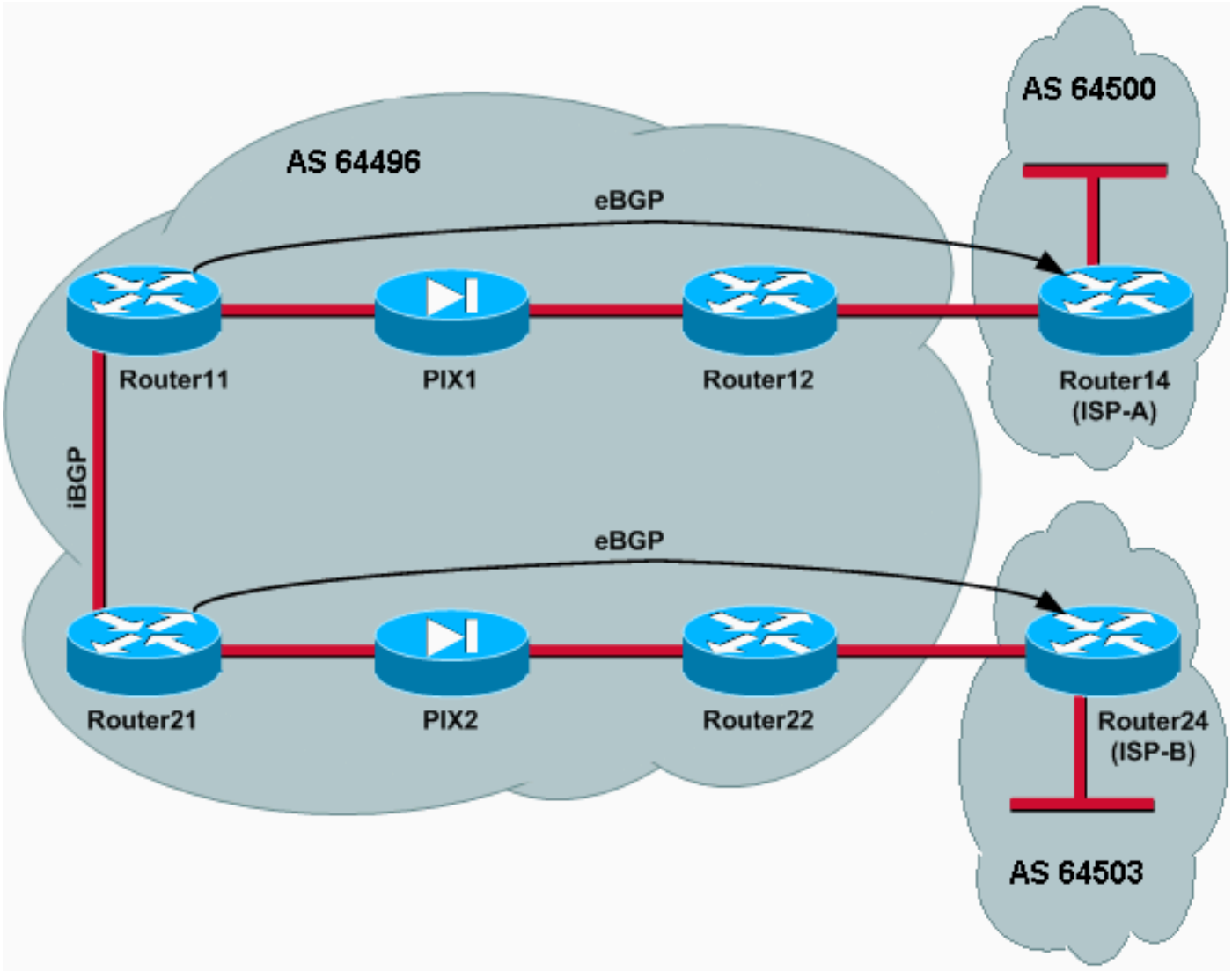
Para obter mais informações sobre do **comando distance bgp**, refira comandos bgp. Para obter mais informações sobre do hospedagem múltipla com BGP, refira o compartilhamento de carga com o BGP no ambientes únicos e multihomed: Configurações de amostra.

Cenário 2

Nesta encenação, Roteador11 é diretamente peering eBGP com Roteador14 (ISP-A), e Roteador21 é diretamente peering eBGP com Roteador24 (ISP-B). Roteador12 e Roteador22 não participam no BGP que espreita, mas fornece a conectividade IP aos ISP. Porque os pares do eBGP não são diretamente vizinhos conectados, o **comando neighbor ebgp-multihop** é usado nos roteadores participantes. **O comando neighbor ebgp-multihop** permite o BGP de cancelar o padrão um limite do eBGP do salto porque muda o Time to Live (TTL) de pacotes do eBGP do valor padrão de 1. Nesta encenação, o vizinho de ebgp é 3 saltos afastado, assim que **3 eBGP-multihop vizinhos** são configurados nos roteadores participantes de modo que o valor TTL seja mudado a 3. Também, as rotas estáticas são configuradas no Roteadores e no PIX para assegurar-se de que Roteador11 possa sibilar o endereço 172.16.13.4 de Roteador14 (ISP-A) e se assegurar de que Roteador21 possa sibilar o endereço 172.16.23.4 de Roteador24 (ISP-B).

Àrevelia, o PIX não permite que os pacotes do Internet Control Message Protocol (ICMP) (enviados quando você emite o **comando ping**) passem completamente. Para permitir pacotes ICMP, use o **comando access-list** segundo as indicações na configuração de PIX seguinte. Para obter mais informações sobre do **comando access-list**, refira o PIX Firewall A através dos comandos B.

A política de roteamento é a mesma que na encenação 1: o link entre Roteador12 e o ISP-A é preferido sobre o link entre Roteador22 e o ISP-B, e quando o link ISP-A vai abaixo do link do ISP-B usado para todo o tráfego de entrada e de saída.



Configurações

Esta encenação usa estas configurações:

- Roteador11
- Roteador12
- Roteador14 (ISP-A)
- Roteador21
- Roteador22
- PIX1
- PIX2

Roteador11

```
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
```

Roteador12

```
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
```

Roteador14 (ISP-A)

```
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
```

Roteador21

```
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
```

Roteador22

```
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
```

Roteador24 (ISP-B)

```
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
```

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
```

Verificar

Comece com a situação onde os links ao ISP-A e ao ISP-B estão acima. A saída do **comando show ip bgp summary em** Roteador11 e em Roteador21 confirma as sessões de BGP estabelecidas com ISP-A e ISP-B respectivamente.

```
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
```

A tabela de BGP em Roteador11 mostra a rota padrão (0.0.0.0/0) para o ISP-A 172.16.13.4 do salto seguinte.

```
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
```

Verifique agora a tabela de BGP em Roteador21. Tem dois 0.0.0.0/0 rotas: um aprendido do ISP-B com um salto seguinte de 172.16.23.4 no eBGP, e o outro aprendido através do iBGP com uma preferência local de 200. Roteador21 prefere rotas ensinada pelo iBGP devido ao atributo de preferência local mais alto, assim que instala que rota na tabela de roteamento. Para obter mais informações sobre da seleção de trajeto BGP, refira o algoritmo de seleção de caminho do melhors 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
```

Troubleshooting

Derrube Roteador11 e a sessão de BGP do 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
```

A sessão de eBGP ao ISP-A vai abaixo de quando o temporizador manter (180 segundos) expira.

```
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
```

Com o link ao ISP-A para baixo, Roteador11 instala 0.0.0.0/0 com um salto seguinte de 192.168.10.2 (Roteador21), que seja instruído através do iBGP em sua tabela de roteamento. Isto empurra todo o tráfego de saída com Roteador21 e então para o ISP-B, segundo as indicações desta saída:

```
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
```

Autenticação md5 para vizinhos de BGP com o PIX/ASA

Configuração PIX 6.x

Apenas como todo o outro protocolo de roteamento, o BGP pode ser configurado para a autenticação. Você pode configurar uma autenticação md5 entre dois bgp peer, assim que significa que cada segmento enviado na conexão de TCP entre os pares está verificado. A autenticação md5 deve ser configurada com a mesma senha em ambos os bgp peer; se não, a conexão entre eles não será feita. A configuração da autenticação md5 faz com que o Cisco IOS Software gerencia e verifique o resumo MD5 de cada segmento enviado na conexão de TCP. Se a autenticação é invocada e um segmento falha a autenticação, um Mensagem de Erro está gerado.

Quando você está configurando os bgp peer com autenticação md5 que passam com um PIX Firewall, é importante configurar o PIX entre os vizinhos de BGP de modo que os números de sequência para os fluxos de TCP entre os vizinhos de BGP não sejam aleatórios. Isto é porque a característica do número de sequência aleatória TCP no PIX Firewall é permitida à revelia, e mude o número de sequência TCP dos pacotes recebidos antes que ele para a frente eles.

A autenticação md5 é aplicada no encabeçamento, no cabeçalho de TCP e nos dados psuedo-IP TCP (refira o RFC 2385). O TCP usa estes dados — que incluem a sequência TCP e números ACK — junto com a senha do vizinho de BGP para criar um número da mistura do bit 128. O número da mistura é incluído no pacote em um campo de opção de cabeçalho de TCP. À revelia, o PIX desloca o número de sequência por um número aleatório, pelo fluxo de TCP. No bgp peer de emissão, o TCP usa o número de sequência original para criar 128 o número da mistura do bit MD5 e inclui este número da mistura no pacote. Quando o bgp peer de recepção obtém o pacote, o TCP usa o número de sequência PIX-alterado para criar 128 um número da mistura do bit MD5 e compara-o ao número da mistura que é incluído no pacote.

O número da mistura é diferente porque o valor da sequência TCP foi mudado pelo PIX, e o TCP no vizinho de BGP deixa cair o pacote e registra uma falha de mensagem MD5 similar a esta:

```
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
```

Use a palavra-chave do **norandomseq** com **(para dentro, fora) o comando norandomseq estático de 255.255.255.0 do netmask de 172.16.11.1 172.16.11.1** resolver este problema e parar o PIX de deslocar o número de sequência TCP. Este exemplo ilustra o uso da palavra-chave do **norandomseq**:

Roteador11

```
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
```

Roteador12

```
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

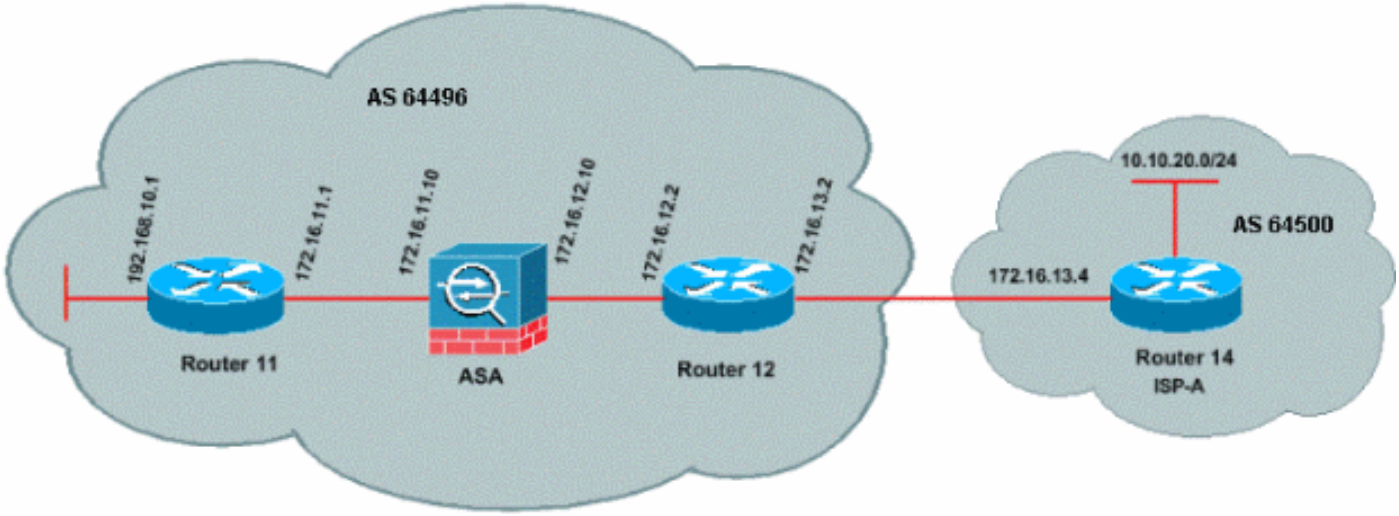
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. 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 ou posterior

Esta seção usa esta instalação de rede.



A versão 7.x e mais recente PIX/ASA introduz um desafio adicional quando você tenta estabelecer uma sessão de peer BGP com autenticação md5. À revelia, a versão 7.x e mais recente PIX/ASA reescreve toda a opção TCP MD5 incluída em uma datagrama TCP que atravesse o dispositivo e substitua o tipo da opção, o tamanho e o valor com os bytes de opção NOP. Isto quebra eficazmente a autenticação md5 BGP, e os resultados nos Mensagens de Erro como este em cada roteador peering:

```
000296: 7 de abril de 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: Nenhum resumo MD5 de
172.16.11.1(28894) a 172.16.12.2(179)
```

Para que uma sessão de BGP com a autenticação md5 a ser estabelecida com sucesso, estas três edições devem ser resolved:

- Randomization do número de sequência do desabilitação TCP
- Reescrita da opção do desabilitação TCP MD5
- Desabilitação NAT entre pares

Um mapa de classe e uma lista de acesso são usados para selecionar o tráfego entre os pares que devem ambos ser isentados da característica do randomization do número de sequência TCP e ser permitidos levar uma opção MD5 sem reescrever. Um tcp-mapa é usado para especificar o tipo da opção a ser reservado, neste caso, o tipo 19 da opção (opção TCP MD5). O mapa de classe e o TCP-mapa ambos são ligados junto com um mapa de política, parte da infraestrutura modular da estrutura de política. A configuração é ativada então com o **comando service-policy**.

Note: A necessidade de desabilitar o NAT entre os pares é segurada pelo **comando no nat-control**.

Na versão 7.0 e mais recente, que a natureza do padrão de um ASA não é **nenhum controle nat**, que indica que cada conexão com o ASA, à revelia, não precise de passar o teste NAT. Supõe-se que o ASA tem uma configuração padrão de **nenhum controle nat**. Refira o controle nat para mais informação. Se o **controle nat** é reforçado, você deve explicitamente desabilitar o NAT para os bgp peer. Isto pode ser feito com o **comando static** entre interfaces internas e externas.

```
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/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
```

Roteador11

```
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
```

Roteador12

```
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
```

Roteador14 (ISP-A)

```
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
```

Verificar

A saída do **comando show ip bgp summary** indica que a autenticação é bem sucedida e que a sessão de BGP está estabelecida em Roteador11.

```
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
```

Informações Relacionadas

- Página de suporte de BGP
- Algoritmo de seleção de melhor caminho BGP
- Compartilhamento de carga com o BGP no ambientes únicos e multihomed: Configurações de exemplo
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- PIX Firewall configurando e de teste
- Suporte Técnico e Documentação - Cisco Systems