ASA/PIX: Exemplo de configuração de BGP através do ASA

Contents

Introduction

Esta configuração de exemplo demonstra como executar o Border Gateway Protocol (BGP) em um Security Appliance (PIX/ASA) e como obter redundância em um ambiente de BGP e PIX multihomed. Com um diagrama de rede como exemplo, este documento explica como rotear automaticamente o tráfego para o provedor de serviços de Internet B (ISP-B) quando o AS 64496 perde a conectividade com o ISP-A (ou o inverso), através do uso de protocolos de roteamento dinâmico que são executados entre todos os roteadores no AS 64496.

Como o BGP usa pacotes TCP unicast na porta 179 para se comunicar com seus pares, você pode configurar PIX1 e PIX2 para permitir o tráfego unicast na porta TCP 179. Dessa forma, o peering BGP pode ser estabelecido entre os roteadores que estão conectados pelo firewall. A redundância e as políticas de roteamento desejadas podem ser obtidas através da manipulação dos atributos BGP.

Prerequisites

Requirements

Os leitores deste documento devem estar familiarizados com Configuração de BGP e Configuração Básica de Firewall.

Componentes Utilizados

Os cenários de exemplo neste documento são baseados nas seguintes versões de software:

- Roteadores Cisco 2600 com Cisco IOS? Software versão 12.2(27)
- PIX 515 com Cisco PIX Firewall versão 6.3(3) e posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

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

- Cisco Adaptive Security Appliance (ASA) 5500 Series com versão 7.x e posterior
- Cisco Firewall Services Module (FWSM) que executa a versão de software 3.2 e posterior

Conventions

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

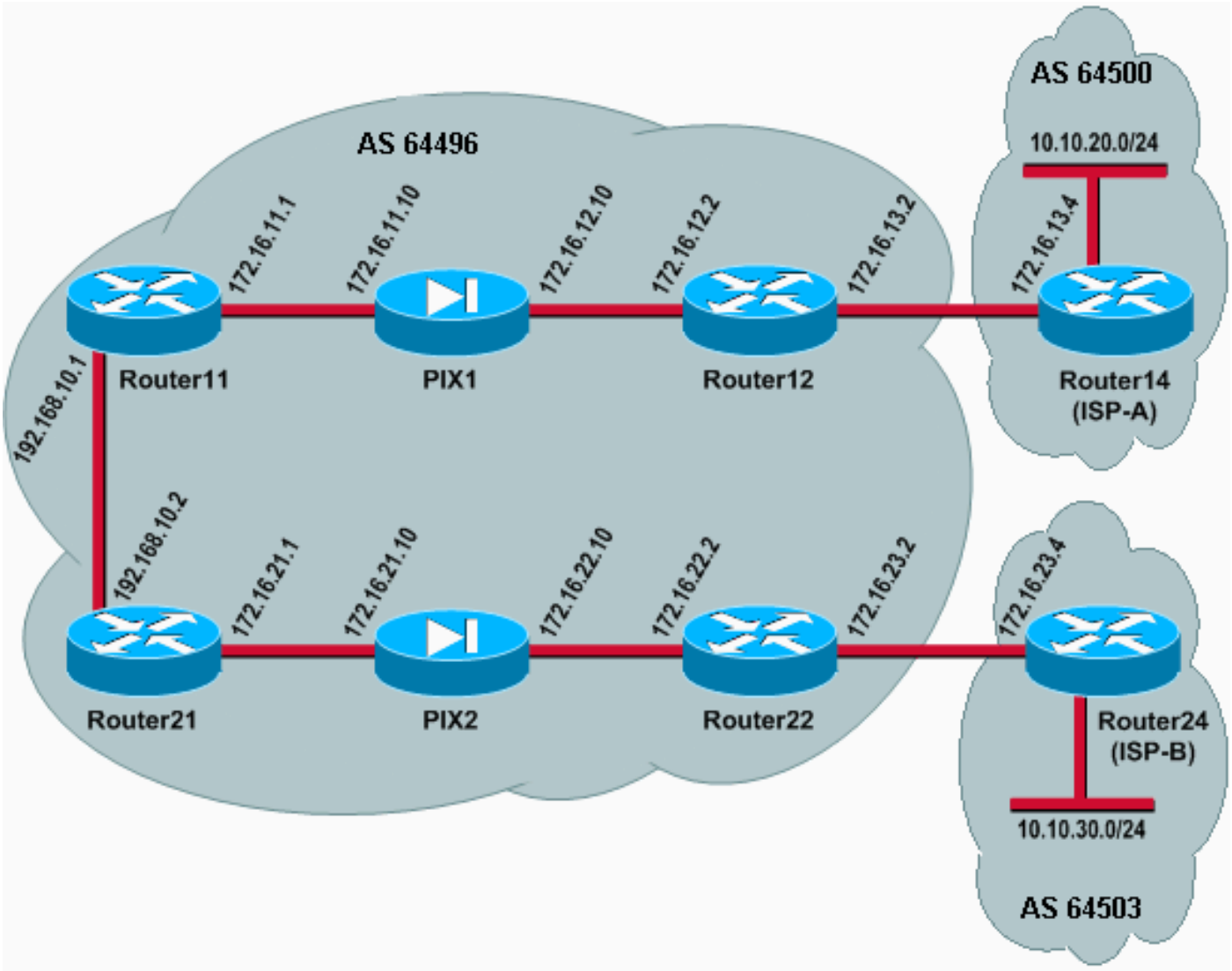
Configurar

Esta seção fornece informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos neste documento, use a Command Lookup Tool (somente clientes registrados) .

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nesta configuração de rede, Router12 e Router22 (que pertencem ao AS 64496) são multihomed para Router14 (ISP-A) e Router24 (ISP-B), respectivamente, para redundância. A rede interna 192.168.10.0/24 está no interior do firewall. Router11 e Router21 se conectam ao Router12 e ao Router22 por meio do firewall. PIX1 e PIX2 não estão configurados para executar a NAT (Network Address Translation Conversão de Endereço de Rede).

Cenário 1

Neste cenário, o Router12 no AS 64496 faz peering de BGP externo (eBGP) com o Router14 (ISP-A) no AS 64500. O Router12 também faz peering de BGP interno (iBGP) com o Router11 através do PIX1. Se as rotas aprendidas do eBGP do ISP-A estiverem presentes, o Router12 anuncia uma rota padrão 0.0.0.0/0 no iBGP para o Router11. Se o link para o ISP-A falhar, o Roteador12 para de anunciar a rota padrão.

Da mesma forma, o Router22 no AS 64496 faz o peering do eBGP com o Router24 (ISP-B) no AS 64503 e anuncia uma rota padrão no iBGP para o Router21 condicionalmente baseada na presença de rotas ISP-B em sua tabela de roteamento.

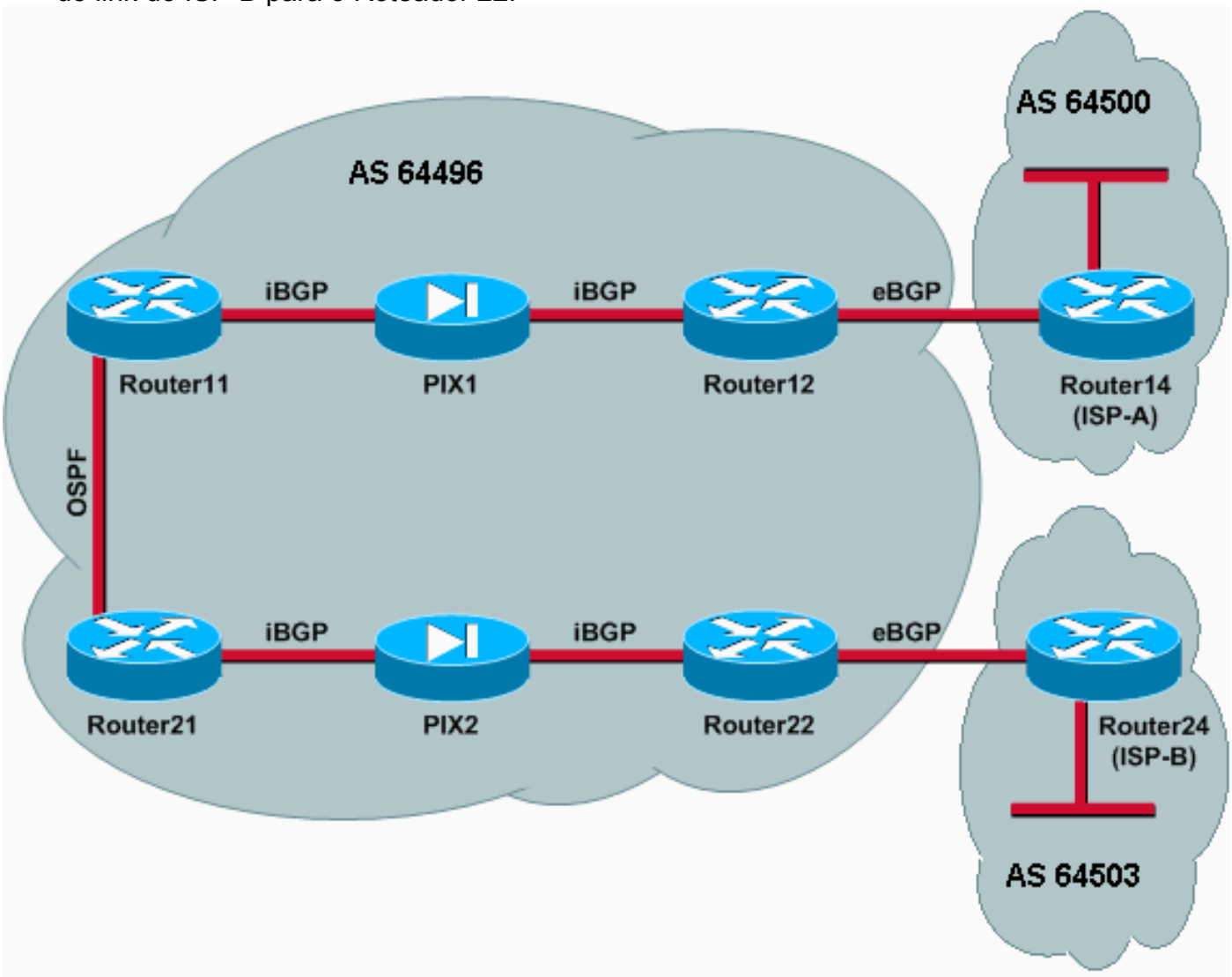
Através do uso de uma lista de acesso, PIX1 e PIX2 são configurados para permitir o tráfego BGP (TCP, porta 179) entre os peers iBGP. Isso ocorre porque as interfaces PIX têm um nível de segurança associado. Por padrão, a interface interna (ethernet1) tem um nível de segurança 100 e a interface externa (ethernet0) tem um nível de segurança 0. As conexões e o tráfego são normalmente permitidos de interfaces de nível de segurança mais alto a mais baixo. Para permitir

o tráfego de uma interface de nível de segurança mais baixo para uma interface de nível de segurança mais alto, no entanto, você deve definir explicitamente uma lista de acesso no PIX. Além disso, você deve configurar uma conversão de NAT estático em PIX1 e PIX2, para permitir que os roteadores externos iniciem uma sessão de BGP com roteadores no interior do PIX.

O Router11 e o Router21 anunciam condicionalmente a rota padrão no domínio OSPF (Open Shortest Path First) com base na rota padrão aprendida pelo iBGP. O Router11 anuncia a rota padrão no domínio OSPF com uma métrica de 5, o Router21 anuncia a rota padrão com uma métrica de 30 e, portanto, a rota padrão do Router11 é preferencial. Essa configuração ajuda a propagar somente a rota padrão 0.0.0.0/0 para o Roteador11 e o Roteador21, que conserva o consumo de memória nos roteadores internos e alcança o desempenho ideal.

Assim, para resumir essas condições, esta é a política de roteamento para AS 64496:

- O AS 64496 prefere o link do Roteador12 ao ISP-A para todo o tráfego de saída (de 192.168.10.0/24 para a Internet).
- Se a conectividade com o ISP-A falhar, todo o tráfego é roteado através do link do Roteador 22 para o ISP-B.
- Todo o tráfego que vem da Internet para 192.168.10.0/24 usa o link do ISP-A para o Roteador12.
- Se o link do ISP-A para o Roteador 12 falhar, todo o tráfego de entrada será roteado através do link do ISP-B para o Roteador 22.



Configurações

Este cenário 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 (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Quando ambas as sessões de BGP estão ativas, você pode esperar que todos os pacotes sejam roteados via ISP-A. Considere a tabela BGP no Router11. Ele aprende uma rota padrão 0.0.0.0/0 do 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
```

A rota padrão 0.0.0.0/0 que é aprendida via BGP é instalada na tabela de roteamento, como mostrado na saída de **show ip route** no Router11.

```
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
```

Agora, considere a tabela BGP no Roteador21. Ele também aprende a rota padrão via Router22.

```
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
```

Agora, veja se essa rota padrão aprendida por BGP é instalada na tabela de roteamento do 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
```

A rota padrão no Router21 é aprendida via OSPF (observe o prefixo `O` na rota 0.0.0.0/0). É interessante observar que há uma rota padrão aprendida via BGP do Roteador22, mas a saída **show ip route** mostra a rota padrão aprendida via OSPF.

A rota padrão OSPF foi instalada no Roteador21 porque o Roteador21 aprende a rota padrão de duas fontes: Roteador22 via iBGP e Roteador11 via OSPF. O processo de seleção de rota instala a rota com uma distância administrativa melhor na tabela de roteamento. A distância administrativa do OSPF é 110, enquanto a distância administrativa do iBGP é 200. Portanto, a rota padrão aprendida com OSPF é instalada na tabela de roteamento, porque 110 é menor que 200. Para obter mais informações sobre a seleção de rotas, consulte Seleção de rotas em Cisco Routers.

Troubleshoot

Use esta seção para resolver problemas de configuração.

Reduza a sessão BGP entre o 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
```

O Router11 não tem a rota padrão aprendida via BGP do Router12.

```
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 no Roteador11. A rota padrão é aprendida via OSPF (distância administrativa de 110) com um próximo salto do 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
```

Essa saída é esperada de acordo com as políticas predefinidas. Neste ponto, no entanto, é importante entender o comando de configuração **distance bgp 20 105 200** no Router11 e como ele influencia a seleção de rota no Router11.

Os valores padrão desse comando são **distance bgp 20 200 200**, onde as rotas aprendidas pelo eBGP têm uma distância administrativa de 20, as rotas aprendidas pelo iBGP têm uma distância administrativa de 200 e as rotas locais do BGP têm uma distância administrativa de 200.

Quando o link entre o Router12 e o ISP-A é ativado novamente, o Router11 aprende a rota padrão via iBGP do Router12. No entanto, como a distância administrativa padrão dessa rota aprendida com iBGP é 200, ela não substituirá a rota aprendida com OSPF (porque 110 é menor que 200). Isso força todo o tráfego de saída para o link do Roteador 21 para o Roteador 22 para o ISP-B, mesmo que o link do Roteador 12 para o ISP-A esteja ativo novamente. Para resolver esse problema, altere a distância administrativa da rota aprendida pelo iBGP para um valor menor que o IGP (Interior Gateway Protocol) usado. Neste exemplo, o IGP é o OSPF, portanto foi escolhida uma distância de 105 (porque 105 é menor que 110).

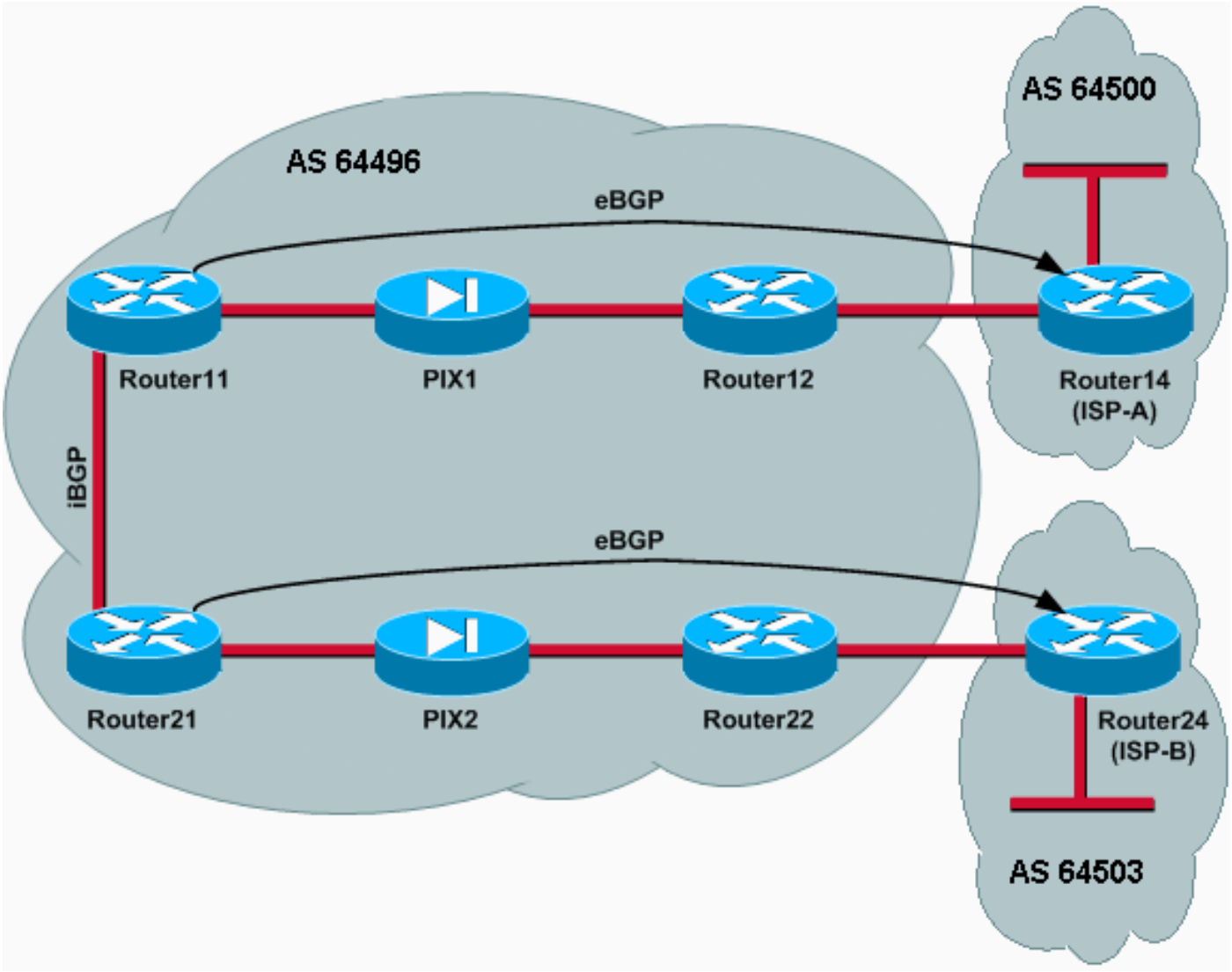
Para obter mais informações sobre o comando **distance bgp**, consulte Comandos BGP. Para obter mais informações sobre multihoming com BGP, consulte Compartilhamento de Carga com BGP em Ambientes Single e Multihomed: Exemplo de configurações.

Cenário 2

Neste cenário, o Router11 é diretamente o peering eBGP com o Router 14 (ISP-A), e o Router21 é diretamente o peering eBGP com o Router24 (ISP-B). Router12 e Router22 não participam do peering de BGP, mas fornecem a conectividade IP aos ISPs. Como os peers do eBGP não são vizinhos diretamente conectados, o comando **neighbor ebgp-multihop** é usado nos roteadores participantes. O comando **neighbor ebgp-multihop** permite que o BGP substitua o limite padrão de eBGP de um salto porque altera o Tempo de Vida (TTL) dos pacotes de eBGP do valor padrão de 1. Nesse cenário, o vizinho eBGP está a 3 saltos de distância, portanto, o **vizinho ebgp-multihop 3** é configurado nos roteadores participantes para que o valor TTL seja alterado para 3. Além disso, as rotas estáticas são configuradas nos roteadores e no PIX para garantir que o Router11 possa fazer ping no endereço 172.16.13.4 do Router14 (ISP-A) e para garantir que o Router21 possa fazer ping no endereço 172.16.23.4 do Router24.

Por padrão, o PIX não permite a passagem de pacotes ICMP (Internet Control Message Protocol) (enviados quando você emite o comando **ping**). Para permitir pacotes ICMP, use o comando **access-list** conforme mostrado na próxima configuração do PIX. Para obter mais informações sobre o comando **access-list**, consulte os Comandos PIX Firewall A a B.

A política de roteamento é a mesma do cenário 1: o link entre o Router12 e o ISP-A é preferencial em relação ao link entre o Router22 e o ISP-B, e quando o link ISP-A é desativado, o link ISP-B é usado para todo o tráfego de entrada e saída.



Configurações

Este cenário 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 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 !
```

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. ! 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
```

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
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.
```

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 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
```

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. ! 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
```

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
!--- 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
```

Verificar

Comece com a situação em que os links para ISP-A e ISP-B estão ativos. A saída do comando **show ip bgp summary** no Router11 e Router21 confirma as sessões 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 no Router11 mostra a rota padrão (0.0.0.0/0) em direção ao próximo salto 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
```

Agora, verifique a tabela BGP no Roteador21. Ele tem duas rotas 0.0.0.0/0: um aprendeu com o ISP-B com um salto seguinte de 172.16.23.4 no eBGP, e o outro aprendeu através do iBGP com uma preferência local de 200. O Router21 prefere rotas aprendidas pelo iBGP devido ao atributo de preferência local mais alto, de modo que ele instala essa rota na tabela de roteamento. Para obter mais informações sobre a seleção de caminho BGP, consulte o algoritmo de seleção de melhor caminho 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
```

Troubleshoot

Desative a sessão do Roteador11 e do 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 eBGP para ISP-A cai quando o temporizador holddown (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 para ISP-A inativo, o Roteador11 instala 0.0.0.0/0 com um salto seguinte de 192.168.10.2 (Roteador21), que é aprendido via iBGP em sua tabela de roteamento. Isso envia todo o tráfego de saída através do Roteador21 e depois para o ISP-B, como mostrado nesta 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 BGP através do PIX/ASA

Configuração do PIX 6.x

Assim como qualquer outro protocolo de roteamento, o BGP pode ser configurado para autenticação. Você pode configurar a autenticação MD5 entre dois peers BGP, o que significa que cada segmento enviado na conexão TCP entre os peers é verificado. A autenticação MD5 deve ser configurada com a mesma senha em ambos os peers BGP; caso contrário, a conexão entre eles não será feita. A configuração da autenticação MD5 faz com que o software Cisco IOS gere e verifique o resumo MD5 de cada segmento enviado na conexão TCP. Se a autenticação for chamada e um segmento falhar na autenticação, uma mensagem de erro será gerada.

Quando você está configurando peers BGP com autenticação MD5 que passam por um firewall PIX, é importante configurar o PIX entre os vizinhos BGP para que os números de sequência para os fluxos TCP entre os vizinhos BGP não sejam aleatórios. Isso ocorre porque o recurso TCP random sequence number no PIX firewall está ativado por padrão e altera o número de sequência TCP dos pacotes recebidos antes de encaminhá-los.

A autenticação MD5 é aplicada no cabeçalho TCP psuedo-IP, no cabeçalho TCP e nos dados (consulte RFC 2385). O TCP usa esses dados—que incluem a sequência TCP e os números ACK—juntamente com a senha do vizinho BGP para criar um número de hash de 128 bits. O número de hash é incluído no pacote em um campo de opção de cabeçalho TCP. Por padrão, o PIX compensa o número de sequência por um número aleatório, por fluxo TCP. No peer BGP emissor, o TCP usa o número de sequência original para criar o número de hash MD5 de 128 bits e inclui esse número de hash no pacote. Quando o peer BGP receptor recebe o pacote, o TCP usa o número de sequência modificado pelo PIX para criar um número de hash MD5 de 128 bits e o compara ao número de hash que está incluído no pacote.

O número de hash é diferente porque o valor da sequência TCP foi alterado pelo PIX, e o TCP no vizinho BGP descarta o pacote e registra uma mensagem de falha MD5 semelhante a esta:

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

Use a palavra-chave **norandomseq** com o **comando static (inside,outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq** para resolver esse problema e parar a sequência PIX de desconfigurar o TCP número. Este exemplo ilustra o uso da palavra-chave **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

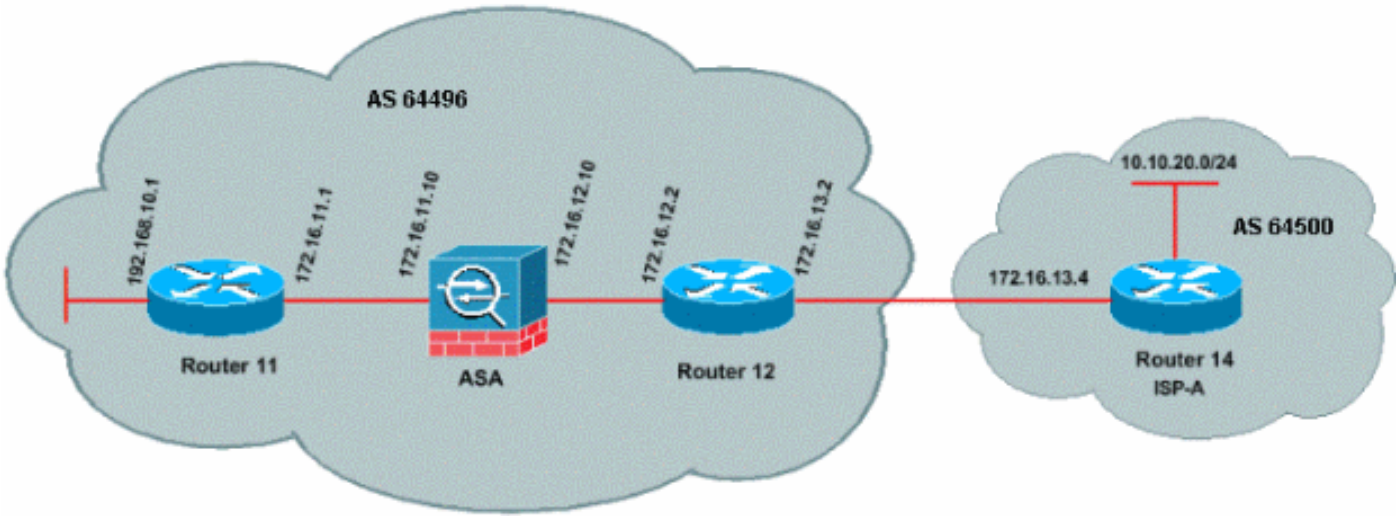
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

Essa seção utiliza esta configuração de rede.



O PIX/ASA versão 7.x e posterior apresenta um desafio adicional quando você tenta estabelecer uma sessão de peering BGP com autenticação MD5. Por padrão, o PIX/ASA versão 7.x e posterior regrava qualquer opção TCP MD5 incluída em um datagrama TCP que passa pelo dispositivo e substitui o tipo, o tamanho e o valor da opção por bytes de opção NOP. Isso efetivamente quebra a autenticação MD5 do BGP e resulta em mensagens de erro como essa em cada roteador de peering:

```
000296 : Abr 7 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 BGP com autenticação MD5 seja estabelecida com êxito, esses três problemas devem ser resolvidos:

- Desativar aleatorização do número de sequência TCP
- Desativar a reescrita da opção TCP MD5

- Desativar NAT entre pares

Um mapa de classe e uma lista de acesso são usados para selecionar o tráfego entre os peers que devem estar isentos do recurso de aleatorização do número de sequência TCP e ter permissão para transportar uma opção MD5 sem reescrever. Um mapa tcp é usado para especificar o tipo de opção a ser permitida, nesse caso, o tipo de opção 19 (opção TCP MD5). O mapa de classes e o mapa tcp estão vinculados por meio de um mapa de políticas, parte da infraestrutura da Estrutura de Política Modular. A configuração é ativada com o comando **service-policy**.

Observação: a necessidade de desabilitar o NAT entre os peers é tratada pelo comando **no nat-control**.

Na versão 7.0 e posterior, a natureza padrão de um ASA **não** é **nenhum controle de nat**, que afirma que cada conexão através do ASA, por padrão, não precisa passar no teste de NAT. Pressupõe-se que o ASA tem uma configuração padrão de **sem controle de nat**. Consulte nat-control para obter mais informações. Se **nat-control** for imposto, você deve desativar explicitamente o NAT para os peers BGP. Isso pode ser feito com o comando **static** entre interfaces internas e externas.

```
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
```

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)

```
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
```

Verificar

A saída do comando **show ip bgp summary** indica que a autenticação foi bem-sucedida e que a sessão BGP foi estabelecida no Router11.

```
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#
```

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
- Configurando e Testando o Firewall PIX
- Suporte Técnico e Documentação - Cisco Systems