ASA/PIX: BGP durch ASA - Konfigurationsbeispiel

Inhalt

Einführung

Diese Beispielkonfiguration zeigt, wie Border Gateway Protocol (BGP) über eine Security Appliance (PIX/ASA) ausgeführt wird und wie Redundanz in einer multihomed BGP- und PIX-Umgebung erreicht wird. In einem Netzwerkdiagramm als Beispiel wird in diesem Dokument erläutert, wie Datenverkehr automatisch an den Internetdienstanbieter B (ISP-B) weitergeleitet wird, wenn die Verbindung zum ISP-A (oder umgekehrt) des AS 64496 durch die Verwendung dynamischer Routing-Protokolle, die zwischen allen Routern des AS 6496 ausgeführt werden, unterbrochen wird.

Da das BGP Unicast-TCP-Pakete an Port 179 für die Kommunikation mit seinen Peers verwendet, können Sie PIX1 und PIX2 so konfigurieren, dass Unicast-Datenverkehr an TCP-Port 179 zugelassen wird. Auf diese Weise kann BGP-Peering zwischen den Routern hergestellt werden, die über die Firewall verbunden sind. Die Redundanz und die gewünschten Routing-Richtlinien können durch Manipulation der BGP-Attribute erreicht werden.

Voraussetzungen

Anforderungen

Leser dieses Dokuments sollten mit der Konfiguration von BGP und der grundlegenden Firewall-

Konfiguration vertraut sein.

Verwendete Komponenten

Die Beispielszenarien in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco 2600 Router mit Cisco IOS? Softwareversion 12.2(27)
- PIX 515 mit Cisco PIX Firewall Version 6.3(3) und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Version 7.x oder höher
- Cisco Firewall Services Module (FWSM) für die Softwareversion 3.2 und höher

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

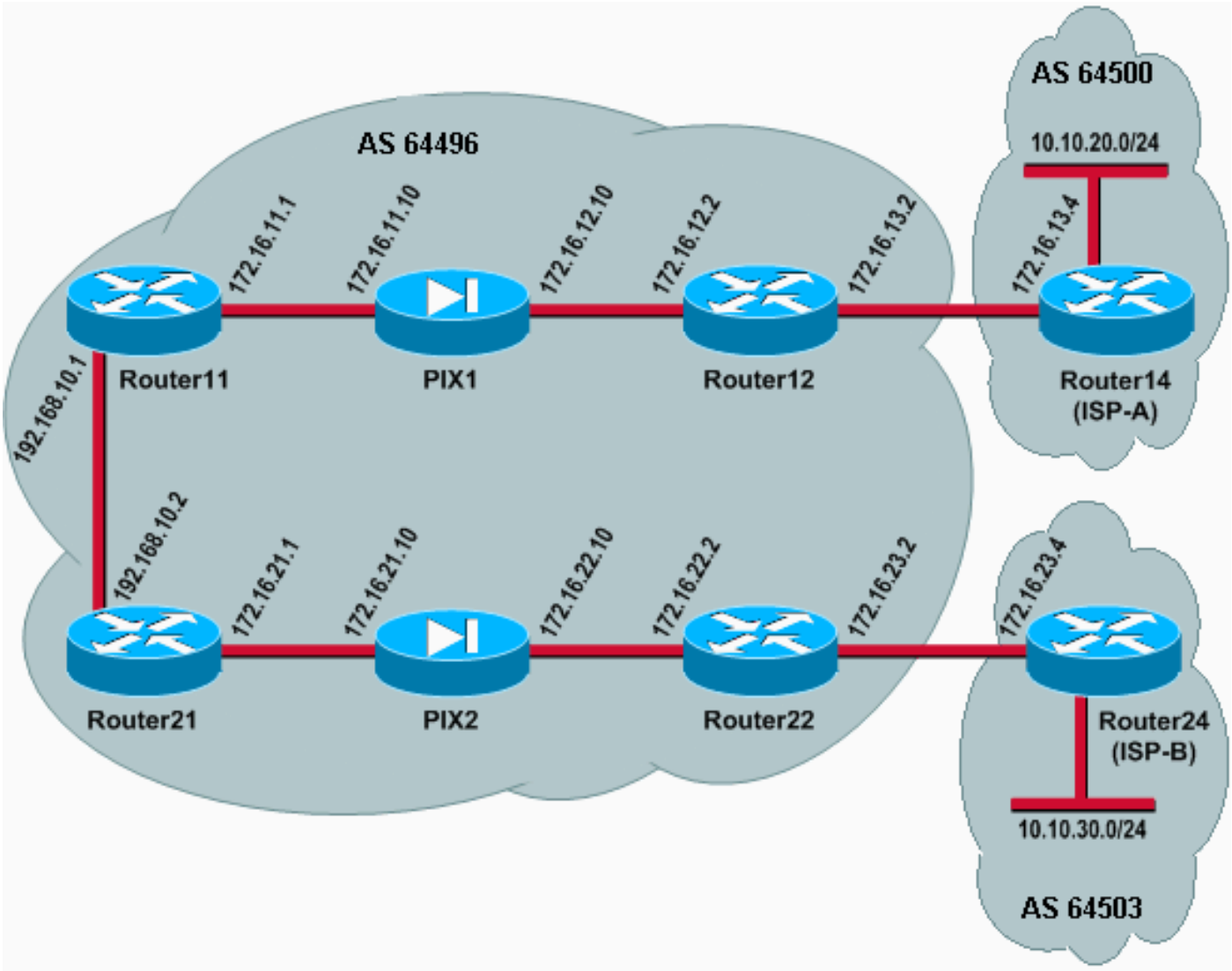
Konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den Befehlen in diesem Dokument zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In dieser Netzwerkeinrichtung werden Router12 und Router22 (die zum AS 64496 gehören) aus Redundanzgründen jeweils mit Router14 (ISP-A) bzw. Router24 (ISP-B) verbunden. Das interne Netzwerk 192.168.10.0/24 befindet sich in der Firewall. Router11 und Router21 verbinden sich über die Firewall mit Router12 und Router22. PIX1 und PIX2 sind nicht für die NAT (Network Address Translation) konfiguriert.

Szenario 1

In diesem Szenario führt Router12 im AS 64496 ein externes BGP (eBGP)-Peering mit Router14 (ISP-A) im AS 64500 durch. Router12 führt auch internes BGP (iBGP)-Peering mit Router11 bis PIX1 durch. Wenn eBGP Routen von ISP-A erfasst hat, kündigt Router12 ein Standard-Routing 0.0.0.0/0 für iBGP zu Router11 an. Wenn die Verbindung zum ISP-A fehlschlägt, beendet Router12 die Ankündigung der Standardroute.

Ebenso führt Router22 im AS 64496 eBGP-Peering mit Router24 (ISP-B) im AS 64503 durch und kündigt eine Standardroute im iBGP zu Router21 bedingt an, basierend auf dem Vorhandensein von ISP-B-Routen in der Routing-Tabelle.

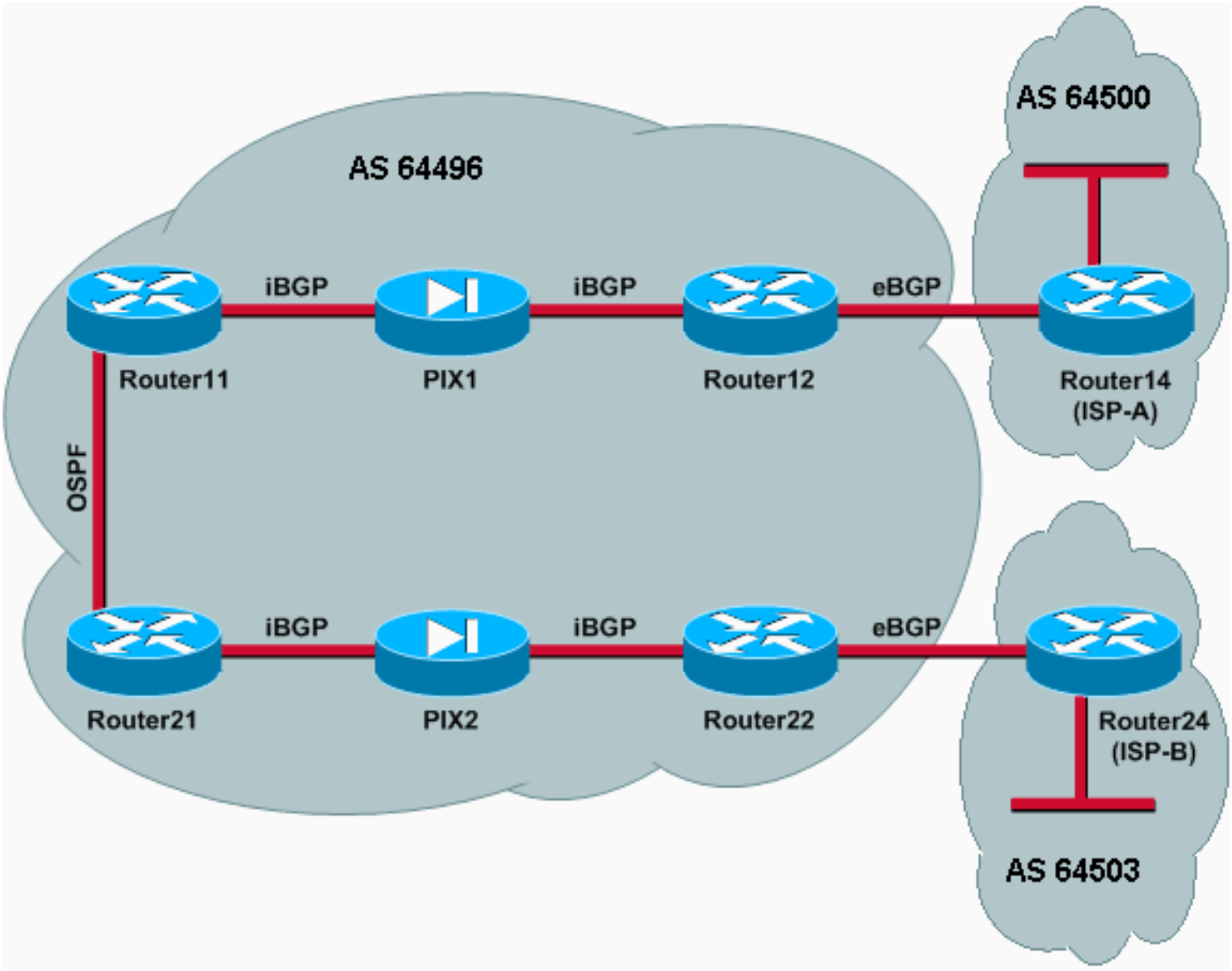
Mithilfe einer Zugriffsliste werden PIX1 und PIX2 so konfiguriert, dass der BGP-Datenverkehr (TCP, Port 179) zwischen iBGP-Peers zugelassen wird. Der Grund hierfür ist, dass PIX-Schnittstellen eine zugehörige Sicherheitsstufe aufweisen. Standardmäßig hat die interne Schnittstelle (Ethernet1) die Sicherheitsstufe 100 und die externe Schnittstelle (Ethernet0) die Sicherheitsstufe 0. Verbindungen und Datenverkehr sind normalerweise von Schnittstellen auf

höherer und niedrigerer Sicherheitsstufe zulässig. Um Datenverkehr von einer Schnittstelle mit niedrigerer Sicherheitsstufe zu einer Schnittstelle mit höherer Sicherheitsstufe zuzulassen, müssen Sie jedoch explizit eine Zugriffsliste auf dem PIX definieren. Außerdem müssen Sie eine statische NAT-Übersetzung auf PIX1 und PIX2 konfigurieren, damit Router an der Außenseite eine BGP-Sitzung mit Routern in PIX-Umgebungen initiieren können.

Sowohl Router11 als auch Router21 geben bedingt die Standardroute in die OSPF-Domäne (Open Shortest Path First) auf Basis der vom iBGP ermittelten Standardroute bekannt. Router11 kündigt die Standardroute in die OSPF-Domäne mit der Metrik 5 an, Router21 kündigt die Standardroute mit der Metrik 30 an. Daher wird die Standardroute von Router11 bevorzugt. Diese Konfiguration unterstützt die Übertragung der Standardroute 0.0.0.0/0 auf Router11 und Router21, wodurch der Speicherverbrauch der internen Router gesenkt und eine optimale Leistung erzielt wird.

Um diese Bedingungen zusammenzufassen, folgt die Routing-Richtlinie für AS 64496:

- Der AS 64496 bevorzugt die Verbindung von Router12 zu ISP-A für den gesamten ausgehenden Datenverkehr (von 192.168.10.0/24 zum Internet).
- Wenn die Verbindung zum ISP-A fehlschlägt, wird der gesamte Datenverkehr über die Verbindung von Router22 zum ISP-B weitergeleitet.
- Der gesamte Datenverkehr, der aus dem Internet an die Adresse 192.168.10.0/24 stammt, verwendet die Verbindung von ISP-A zu Router12.
- Wenn die Verbindung zwischen ISP-A und Router12 fehlschlägt, wird der gesamte eingehende Datenverkehr über die Verbindung zwischen ISP-B und Router22 weitergeleitet.



Konfigurationen

In diesem Szenario werden folgende Konfigurationen verwendet:

- Router11
- Router12
- Router14 (ISP-A)
- Router21
- Router22
- PIX1
- PIX2

Router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router ospf 1 log-adjacency-changes network
192.168.10.0 0.0.0.255 area 0 default-information
originate metric 5 route-map check-default !--- A
```

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

Router12

```
hostname Router12
!
interface FastEthernet0/0
 ip address 172.16.13.2 255.255.255.0
!--- Connected to Router14 (ISP-A). ! interface
FastEthernet0/1 ip address 172.16.12.2 255.255.255.0 !--
- Connected to PIX1. ! router bgp 64496 no
synchronization neighbor 172.16.11.1 remote-as 64496
neighbor 172.16.11.1 next-hop-self neighbor 172.16.11.1
default-originate route-map check-ispa-route !--- A
default route is advertised to Router11 conditionally
(based on whether the link !--- from Router12 to ISP-A
is active). neighbor 172.16.11.1 distribute-list 1 out
neighbor 172.16.13.4 remote-as 64500 !--- Configures
Router14 (ISP-A) as an eBGP peer. neighbor 172.16.13.4
route-map adv-to-ispa out no auto-summary ! ip route
172.16.11.0 255.255.255.0 172.16.12.10 !--- Static route
to iBGP peer, because it is not directly connected. !
access-list 1 permit 0.0.0.0 access-list 10 permit
192.168.10.0 access-list 20 permit 10.10.20.0 0.0.0.255
access-list 21 permit 172.16.13.4 ! route-map check-
ispa-route permit 10 match ip address 20 match ip next-
hop 21 ! route-map adv-to-ispa permit 10 match ip
address 10
```

Router14 (ISP-A)

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

Router21

```
hostname Router21
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.0
```

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

Router22

```
hostname Router22
!
interface FastEthernet0/0
 ip address 172.16.23.2 255.255.255.0
!--- Connected to Router24 (ISP-B). ! interface
FastEthernet0/1 ip address 172.16.22.2 255.255.255.0 !--
- Connected to PIX2. ! router bgp 64496 no
synchronization bgp log-neighbor-changes neighbor
172.16.21.1 remote-as 64496 !--- Configure Router21 as
an iBGP peer. neighbor 172.16.21.1 next-hop-self
neighbor 172.16.21.1 default-originate route-map check-
ispb-route !--- A default route is advertised to
Router21 conditionally (based on whether the link !---
from Router22 to ISP-B is active). ! neighbor
172.16.21.1 distribute-list 1 out neighbor 172.16.23.4
remote-as 64503 neighbor 172.16.23.4 route-map adv-to-
ispb out ! ip route 172.16.21.0 255.255.255.0
172.16.22.10 !--- Static route to iBGP peer, because it
is not directly connected. ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.30.0 0.0.0.255 access-list 21 permit
172.16.23.4 ! route-map check-ispb-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispb permit 10 match ip address 10 set as-path prepend
10 10 10 !--- Route map used to change the AS path
attribute of outgoing updates.
```

Router24 (ISP-B)

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

PIX1

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

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

PIX2

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

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Wenn beide BGP-Sitzungen aktiv sind, können Sie erwarten, dass alle Pakete über ISP-A weitergeleitet werden. Betrachten Sie die BGP-Tabelle auf Router11. Es wird eine Standardroute 0.0.0.0/0 von Router12 mit dem nächsten Hop 172.16.12.2 abgerufen.

```
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
```

Die 0.0.0.0/0-Standardroute, die über BGP abgerufen wird, wird in der Routing-Tabelle installiert, wie in der Ausgabe von **show ip route** auf Router11 gezeigt.

```
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
```

Betrachten Sie jetzt die BGP-Tabelle auf Router21. Außerdem wird die Standardroute über Router22 erkannt.

```
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
```

Prüfen Sie jetzt, ob diese vom BGP bezogene Standardroute in die Routing-Tabelle von Router21 installiert wird.

```
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
```

Die Standardroute in Router21 wird über OSPF erfasst (beachten Sie das `O`-Präfix auf der Route 0.0.0.0/0). Es ist interessant festzustellen, dass über BGP vom Router22 eine Standardroute abgerufen wird. Die Ausgabe von **show ip route** zeigt jedoch die über OSPF bezogene Standardroute.

Die OSPF-Standardroute wurde in Router21 installiert, da Router21 die Standardroute von zwei Quellen bezieht: Router22 über iBGP und Router11 über OSPF. Beim Routenauswahlprozess wird die Route mit einer besseren administrativen Distanz in die Routing-Tabelle installiert. Die administrative Distanz von OSPF beträgt 110, die administrative Distanz von iBGP 200. Aus diesem Grund wird die vom OSPF ermittelte Standardroute in der Routing-Tabelle installiert, da 110 weniger als 200 ist. Weitere Informationen zur Routenauswahl finden Sie unter Routenauswahl in Cisco Routern.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Deaktivieren Sie die BGP-Sitzung zwischen Router12 und 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
```

Router11 hat nicht die Standardroute, die über BGP von Router12 abgerufen wurde.

```
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
```

Überprüfen Sie die Routing-Tabelle auf Router11. Die Standardroute wird über OSPF (administrative Distanz von 110) mit einem Next Hop of Router21 erfasst.

```
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
```

Diese Ausgabe wird gemäß den vordefinierten Richtlinien erwartet. An diesem Punkt ist es jedoch wichtig, den Konfigurationsbefehl **bgp 20 105 200** in Router11 zu kennen und zu verstehen, wie er die Routenauswahl auf Router11 beeinflusst.

Die Standardwerte dieses Befehls sind **Distanzbgp 20 200 200**, wobei vom eBGP bezogene Routen eine administrative Distanz von 20 haben, vom iBGP bezogene Routen eine administrative Distanz von 200 haben und lokale BGP-Routen eine administrative Distanz von 200 haben.

Wenn die Verbindung zwischen Router12 und ISP-A wieder hergestellt wird, erfährt Router11 vom Router12 die Standardroute über iBGP. Da die standardmäßige administrative Distanz dieser vom iBGP bezogenen Route jedoch 200 beträgt, wird die vom OSPF erfasste Route nicht ersetzt (da 110 weniger als 200 ist). Dadurch wird der gesamte ausgehende Datenverkehr an die Verbindung zwischen Router21 und Router22 und ISP-B gezwungen, obwohl die Verbindung zwischen Router12 und ISP-A wieder aktiv ist. Um dieses Problem zu beheben, ändern Sie die administrative Distanz der vom iBGP bezogenen Route in einen Wert, der kleiner ist als der Wert des verwendeten Interior Gateway Protocol (IGP). In diesem Beispiel ist das IGP OSPF. Daher wurde eine Entfernung von 105 gewählt (da 105 weniger als 110 ist).

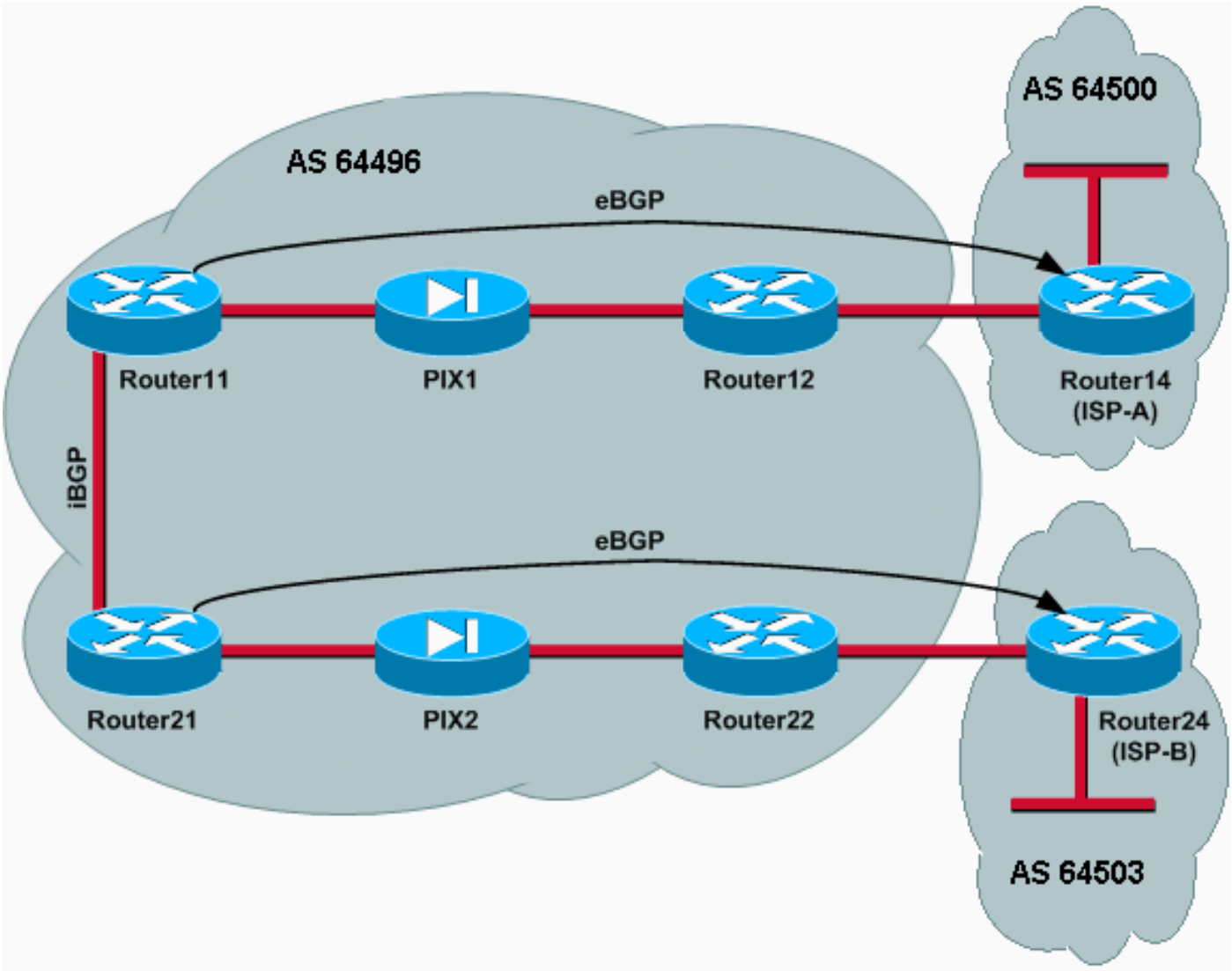
Weitere Informationen zum Befehl **distanzieren** bgp finden Sie unter BGP-Befehle. Weitere Informationen zum Multihoming mit BGP finden Sie unter Lastverteilung mit BGP in Single- und Multihomed-Umgebungen: Beispielkonfigurationen.

Szenario 2

In diesem Szenario ist Router11 direkt eBGP-Peering mit Router 14 (ISP-A) und Router21 direkt eBGP-Peering mit Router24 (ISP-B). Router12 und Router22 sind nicht am BGP-Peering beteiligt, stellen aber die IP-Verbindung zu den ISPs bereit. Da die eBGP-Peers nicht direkt mit Nachbarn verbunden sind, wird der Befehl **bgp-multihop** für die teilnehmenden Router verwendet. Der Befehl **bgp-multihop neighbor** ermöglicht es BGP, die standardmäßige eBGP-Obergrenze für einen Hop zu überschreiben, da er die Time to Live (TTL) von eBGP-Paketen vom Standardwert 1 ändert. In diesem Szenario ist der eBGP-Nachbar 3 Hops entfernt, daher wird der **Nachbarn ebgp-multihop 3** auf den teilnehmenden Routern konfiguriert, sodass der TTL-Wert auf 3 geändert wird. Darüber hinaus werden auf den Routern und PIX statische Routen konfiguriert, um sicherzustellen, dass Router11 den Router14 (ISP-A) der Adresse 172.16.13.4 pingen kann, und um sicherzustellen, dass Router21 die Router24 (ISP-B)-Adresse 172.16.23.4 pingen kann.

In der Standardeinstellung lässt PIX keine ICMP-Pakete (Internet Control Message Protocol) zu (die gesendet werden, wenn Sie den **Ping-**Befehl ausgeben). Um ICMP-Pakete zuzulassen, verwenden Sie den Befehl **access-list**, wie in der nächsten PIX-Konfiguration gezeigt. Weitere Informationen zum Befehl **access-list** finden Sie unter PIX Firewall A bis B Commands.

Die Routing-Richtlinie entspricht der in Szenario 1: Die Verbindung zwischen Router12 und ISP-A wird gegenüber der Verbindung zwischen Router22 und ISP-B bevorzugt. Wenn die ISP-A-Verbindung ausfällt, wird die ISP-B-Verbindung für den gesamten ein- und ausgehenden Datenverkehr verwendet.



Konfigurationen

In diesem Szenario werden folgende Konfigurationen verwendet:

- Router11
- Router12
- Router14 (ISP-A)
- Router21
- Router22
- PIX1
- PIX2

Router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.13.4 remote-as 64500 neighbor 172.16.13.4 ebgp-
```

```
multihop 3 !--- To accept and attempt BGP connections to
external peers that reside on networks that !--- are not
directly connected. neighbor 172.16.13.4 route-map set-
pref in !--- Sets higher local-preference for learned
routes. neighbor 172.16.13.4 route-map adv_to_ispa out
neighbor 192.168.10.2 remote-as 64496 neighbor
192.168.10.2 next-hop-self no auto-summary ! ip route
172.16.12.0 255.255.255.0 172.16.11.10 ip
route172.16.13.4 255.255.255.255 172.16.11.10 !---
Static route to eBGP peer, because it is not directly
connected. ! access-list 20 permit 192.168.10.0 ! route-
map set-pref permit 10 set local-preference 200 ! route-
map adv_to_ispa permit 10 match ip address 20 !
```

Router12

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

Router14 (ISP-A)

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

Router21

```
hostname Router21
 !
 interface FastEthernet0/0
  ip address 192.168.10.2 255.255.255.0
!--- Connected to Router11. ! interface FastEthernet0/1
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router bgp 64496 no synchronization network
192.168.10.0 neighbor 172.16.23.4 remote-as 64503
neighbor 172.16.23.4 ebgp-multihop 3 !--- To accept and
attempt BGP connections to external peers that reside on
networks that !--- are not directly connected. neighbor
172.16.23.4 route-map adv_to_ispb out neighbor
192.168.10.1 remote-as 64496 neighbor 192.168.10.1 next-
```

```
hop-self no auto-summary ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 ip route172.16.23.4
255.255.255.255 172.16.21.10 !--- Static routes
configured to reach BGP peer. ! access-list 20 permit
192.168.10.0 ! route-map adv_to_ispb permit 10 match ip
address 20 set as-path prepend 10 10 10
```

Router22

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

Router24 (ISP-B)

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

PIX1

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

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

PIX2

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

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

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

Überprüfen

Beginnen Sie mit der Situation, in der die Links zu ISP-A und ISP-B verfügbar sind. Die Befehlsausgabe **show ip bgp summary** auf Router11 und Router21 bestätigt die etablierten BGP-Sitzungen mit ISP-A bzw. ISP-B.

```
Router11# show ip bgp summary

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


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

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

Die BGP-Tabelle auf Router11 zeigt die Standardroute (0.0.0.0/0) zum nächsten Hop-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
```

Überprüfen Sie jetzt die BGP-Tabelle auf Router21. Es verfügt über zwei 0.0.0.0/0-Routen: einer lernte von ISP-B mit einem nächsten Hop von 172.16.23.4 für eBGP, der andere mit iBGP mit einer lokalen Präferenz von 200. Router21 bevorzugt vom iBGP erfasste Routen aufgrund des

Attributs mit höherer lokaler Präferenz. Daher wird diese Route in der Routing-Tabelle installiert. Weitere Informationen zur BGP-Pfadauswahl finden Sie unter BGP Best Path Selection Algorithm.

```
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
```

Fehlerbehebung

Deaktivieren Sie die Router11- und ISP-A-BGP-Sitzung.

```
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
```

Die eBGP-Sitzung mit ISP-A wird unterbrochen, wenn der Hold-Down-Timer (180 Sekunden) abläuft.

```
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
```

Wenn die Verbindung zum ISP-A unterbrochen ist, installiert Router11 0.0.0.0/0 mit dem nächsten Hop von 192.168.10.2 (Router21), der über iBGP in der Routing-Tabelle erfasst wird. Dadurch wird der gesamte ausgehende Datenverkehr über Router21 und anschließend über ISP-B weitergeleitet, wie in der folgenden Ausgabe gezeigt:

```
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
```

MD5-Authentifizierung für BGP-Nachbarn über PIX/ASA

Konfiguration von PIX 6.x

Wie jedes andere Routing-Protokoll kann auch BGP für die Authentifizierung konfiguriert werden. Sie können die MD5-Authentifizierung zwischen zwei BGP-Peers konfigurieren. Das bedeutet, dass jedes Segment, das über die TCP-Verbindung zwischen den Peers gesendet wird, verifiziert wird. Die MD5-Authentifizierung muss für beide BGP-Peers mit demselben Kennwort konfiguriert werden. Andernfalls wird keine Verbindung zwischen ihnen hergestellt. Durch die Konfiguration der MD5-Authentifizierung generiert und überprüft die Cisco IOS-Software den MD5-Digest jedes Segments, das über die TCP-Verbindung gesendet wird. Wenn Authentifizierung aufgerufen wird und ein Segment die Authentifizierung nicht erfolgreich beendet, wird eine Fehlermeldung generiert.

Wenn Sie BGP-Peers mit MD5-Authentifizierung konfigurieren, die eine PIX-Firewall passieren, ist es wichtig, das PIX zwischen den BGP-Nachbarn so zu konfigurieren, dass die Sequenznummern für die TCP-Flüsse zwischen den BGP-Nachbarn nicht zufällig gewählt werden. Der Grund hierfür ist, dass die Funktion der zufälligen TCP-Sequenznummern auf der PIX-Firewall standardmäßig aktiviert ist und die TCP-Sequenznummer der eingehenden Pakete ändert, bevor sie weitergeleitet werden.

MD5-Authentifizierung wird auf den TCP-Psuedo-IP-Header, den TCP-Header und die Daten angewendet (siehe RFC 2385). TCP verwendet diese Daten (einschließlich der TCP-Sequenz und der ACK-Nummern) zusammen mit dem BGP-Nachbarkennwort, um eine 128-Bit-Hash-Nummer zu erstellen. Die Hash-Nummer ist im Feld "TCP-Header-Option" im Paket enthalten. Standardmäßig gleicht das PIX die Sequenznummer pro TCP-Fluss durch eine zufällige Nummer aus. Auf dem sendenden BGP-Peer verwendet TCP die ursprüngliche Sequenznummer, um die 128-Bit-MD5-Hash-Nummer zu erstellen. Diese Hash-Nummer ist im Paket enthalten. Wenn der empfangende BGP-Peer das Paket abruft, verwendet TCP die PIX-geänderte Sequenznummer, um eine MD5-Hashnummer mit 128 Bit zu erstellen und mit der Hash-Nummer im Paket zu vergleichen.

Die Hash-Nummer ist anders, da der TCP-Sequenzwert von PIX geändert wurde, und TCP auf dem BGP-Nachbarn verwirft das Paket und protokolliert eine MD5-Fehlermeldung, die dieser ähnlichen Meldung ähnelt:

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

Verwenden Sie das **norandomseq-**Schlüsselwort mit dem **statischen (inside,outside) 172.16.11.1 172.16.11.1-Netzmaske 255.255.255.0 norandomseq**-Befehl, um dieses Problem zu beheben und das Auslagern, die TCP-Sequenznummer ... Dieses Beispiel veranschaulicht die Verwendung des **norandomseq-**Schlüsselworts:

Router11

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

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

Router12

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

 neighbor 172.16.11.1 distribute-list 1 out
 neighbor 172.16.13.4 remote-as 64500
 neighbor 172.16.13.4 route-map adv-to-ispa out
 no auto-summary
!
ip route 172.16.11.0 255.255.255.0 172.16.12.10
!--- Static route to iBGP peer, because it is not
directly connected. ! access-list 1 permit 0.0.0.0
access-list 10 permit 192.168.10.0 access-list 20 permit
10.10.20.0 0.0.0.255 access-list 21 permit 172.16.13.4 !
route-map check-ispa-route permit 10 match ip address 20
match ip next-hop 21 ! route-map adv-to-ispa permit 10
match ip address 10
```

PIX1

```
nameif ethernet0 outside security0
```

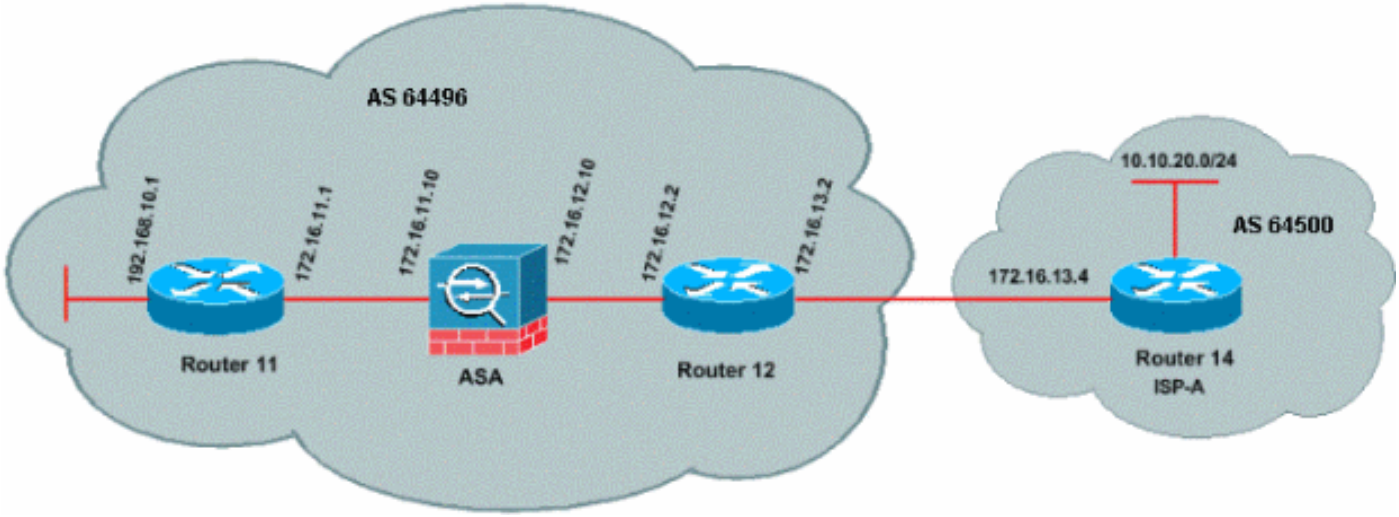
```
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any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

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

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

PIX/ASA 7.x und höher

In diesem Abschnitt wird diese Netzwerkeinrichtung verwendet.



PIX/ASA Version 7.x und höher stellt eine zusätzliche Herausforderung dar, wenn Sie versuchen, eine BGP-Peering-Sitzung mit MD5-Authentifizierung einzurichten. Standardmäßig schreibt PIX/ASA Version 7.x und höher jede TCP-MD5-Option, die in einem TCP-Datagramm enthalten ist, das das Gerät durchläuft, um die Art, Größe und den Wert der Option durch Bytes der NOP-Option zu ersetzen. Dadurch wird die BGP MD5-Authentifizierung effektiv unterbrochen, und es werden Fehlermeldungen wie diese auf jedem Peering-Router ausgegeben:

```
000296: 7. April 2010, 15:13:22.221 EDT: %TCP-6-BADAUTH: Kein MD5-Digest von 172.16.11.1(28894)
bis 172.16.12.2(179)
```

Damit eine BGP-Sitzung mit MD5-Authentifizierung erfolgreich eingerichtet werden kann, müssen die folgenden drei Probleme gelöst werden:

- TCP-Sequenznummern-Randomisierung deaktivieren
- Umschreiben der TCP-MD5-Option deaktivieren
- NAT zwischen Peers deaktivieren

Mit einer Klassenzuordnung und einer Zugriffsliste wird der Datenverkehr zwischen den Peers ausgewählt, der von der Randomisierungsfunktion der TCP-Sequenznummer befreit und die Übertragung einer MD5-Option ohne Umschreiben gestattet werden muss. Eine tcp-map wird

verwendet, um den zulässigen Optionstyp anzugeben, in diesem Fall die Option 19 (TCP MD5-Option). Die Klassenzuordnung und die tcp-map sind beide über eine Richtlinienzuordnung verbunden, die Teil der Infrastruktur des modularen Richtlinien-Frameworks ist. Die Konfiguration wird dann mit dem Befehl **service-policy** aktiviert.

Hinweis: Die Notwendigkeit, NAT zwischen den Peers zu deaktivieren, wird mit dem Befehl **no nat control** behandelt.

In Version 7.0 und höher ist der Standard, dass ASA **keine NAT-Kontrolle** besitzt, was bedeutet, dass jede Verbindung über ASA standardmäßig nicht den NAT-Test bestehen muss. Es wird davon ausgegangen, dass ASA eine Standardeinstellung **ohne NAT-Kontrolle** hat. Weitere Informationen finden Sie unter NAT-Control. Wenn **NAT-Kontrolle** erzwungen wird, müssen Sie NAT für die BGP-Peers explizit deaktivieren. Dies kann mithilfe des **statischen** Befehls zwischen internen und externen Schnittstellen erfolgen.

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

PIX/ASA 7.x/8.x

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

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


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


!
!--- TCP-MAP to allow MD5 Authentication. tcp-map BGP-
MD5-OPTION-ALLOW
  tcp-options range 19 19 allow
!
!--- Apply the ACL that allows traffic !--- from the
outside peer to the inside peer access-group OUTSIDE-
ACL-IN in interface outside
```

```
!
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400

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

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

!
service-policy global_policy global
prompt hostname context
Cryptochecksum:64ea55d7271e19eea87c8603ab3768a2
: end
```

Router11

```
Router11#sh run
hostname Router11
!
```

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

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

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

Router12

```
Router12#sh run
hostname Router12
!
aaa new-model
!
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.13.2 255.255.255.0
!
interface Ethernet1
 ip address 172.16.12.2 255.255.255.0
!
```

```
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router bgp 64496
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.11.1 remote-as 64496

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

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

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

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

Router14 (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
```

Überprüfen

Die Ausgabe des Befehls **show ip bgp summary** gibt an, dass die Authentifizierung erfolgreich ist und dass die BGP-Sitzung auf Router11 eingerichtet wurde.

```
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#
```

Zugehörige Informationen

- BGP-Support-Seite
- BGP-Algorithmus für die beste Pfadauswahl
- Lastverteilung mit BGP in Single- und Multihomed-Umgebungen: Beispielkonfigurationen
- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Konfigurieren und Testen der PIX-Firewall
- Technischer Support und Dokumentation - Cisco Systems