ASA/PIX：ASA 経由の BGP の設定例

内容

概要

この設定例では、セキュリティ アプライアンス（PIX/ASA）を経由して、Border Gateway Protocol（BGP）を実行する方法と、マルチホームの BGP および PIX 環境で冗長性を実現する方法を示します。このドキュメントでは、例としてネットワーク図を使用して、AS 64496 が ISP-A（または逆）に対する接続が失われたときに、AS 64496 のすべてのルータ間で実行されるダイナミック ルーティング プロトコルを使用して、インターネット サービス プロバイダー B（ISP-B）にトラフィックを自動的にルーティングする方法を説明します。

BGPはポート179でユニキャストTCPパケットを使用してピアと通信するため、PIX1とPIX2を設定して、TCPポート179でユニキャストトラフィックを許可できます。この方法では、ファイアウォールを介して接続されているルータ間でBGPピアリングをを確立します。冗長性と望ましいルーティング ポリシーは、BGP 属性を操作して実現できます。

前提条件

要件

このドキュメントの読者は、BGP の設定と基本的なファイアウォールの設定に精通している必要があります。

使用するコンポーネント

このドキュメントのシナリオの例は、次のソフトウェアのバージョンに基づくものです。

- Cisco IOSが稼働する Cisco 2600 ルータソフトウェア リリース 12.2(27) が稼働中の Cisco 3640 ルータ
- Cisco PIX Firewall バージョン 6.3(3) 以降が稼働する PIX 515

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- バージョン 7.x 以降が稼働する Cisco 適応型セキュリティ アプライアンス（ASA）5500 シリーズ
- バージョン 3.2 以降のソフトウェアが稼働する Cisco ファイアウォール サービス モジュール（FWSM）

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

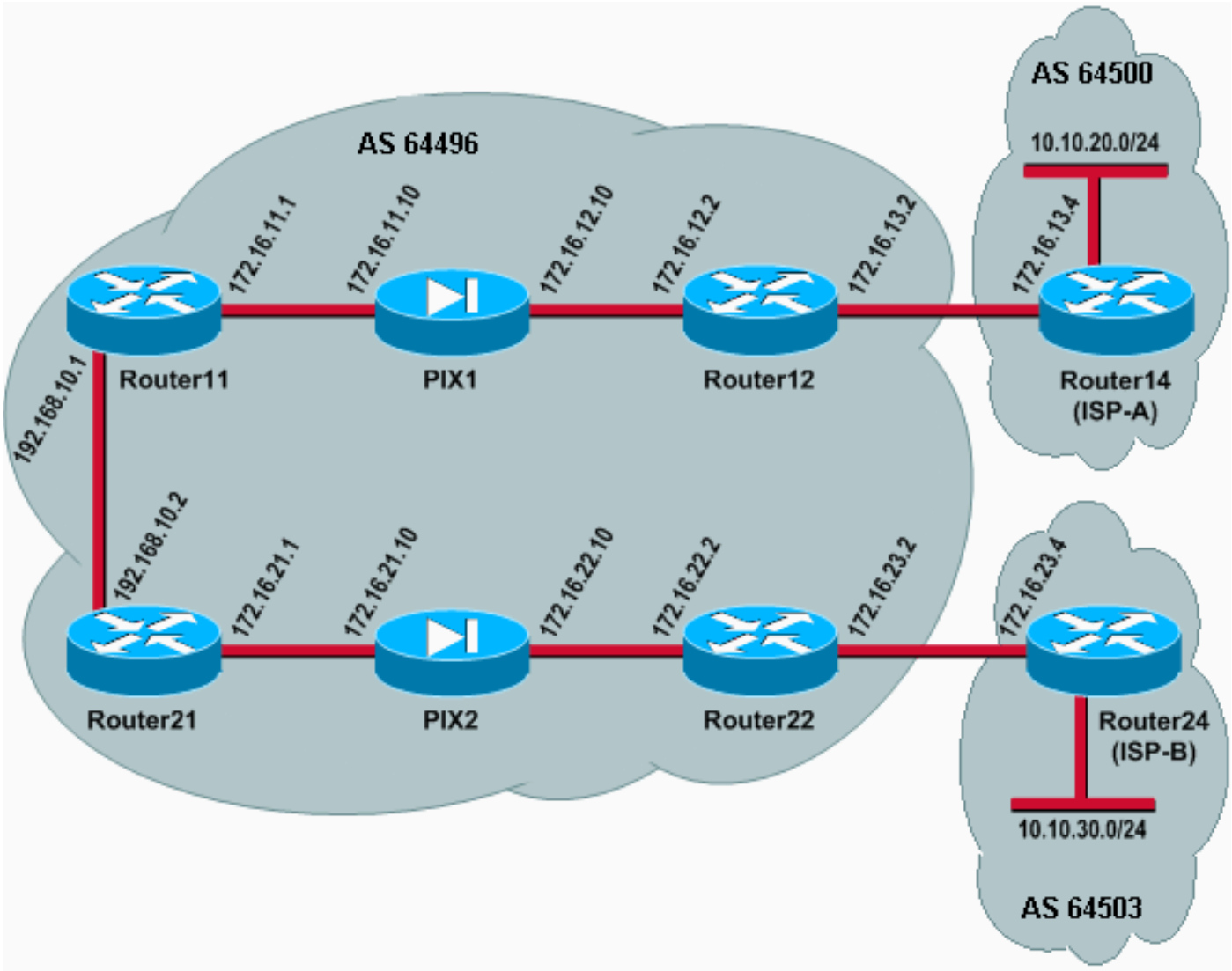
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供します。

注：このドキュメントのコマンドに関する詳細については、Command Lookup Tool(登録ユーザ専用)を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



このネットワーク構成では、Router12 および Router22（AS 64496 に属する）は、冗長性を実現するため、それぞれ Router14（ISP-A）および Router24（ISP-B）にマルチホームされています。内部ネットワーク 192.168.10.0/24 は、ファイアウォールの内部にあります。Router11 および Router21 は、ファイアウォールを経由して、Router12 および Router22 に接続されています。PIX1 と PIX2 は、ネットワーク アドレス変換（NAT）を実行するように設定されていません。

シナリオ 1

このシナリオでは、AS 64496のRouter12はAS 64500のRouter14(ISP-A)との外部BGP(eBGP)ピアリングを行います。Router12はPIX1を介した内部BGPピアリングも行を行いますISP-AからeBGPで学習したルートが存在する場合、Router12はiBGPでデフォルトルート0.0.0.0/0をRouter11にアナウンスします。ISP-Aへのリンクに障害が発生すると、Router12はデフォルトルートのアナウンスを停止します。

同様に、AS 64496 内の Router22 では、AS 64503 内の Router24（ISP-B）との eBGP ピアリングが行われ、ルーティング テーブルに ISP-B ルートが存在することを条件に、iBGP での Router21 へのデフォルト ルートがアナウンスされます。

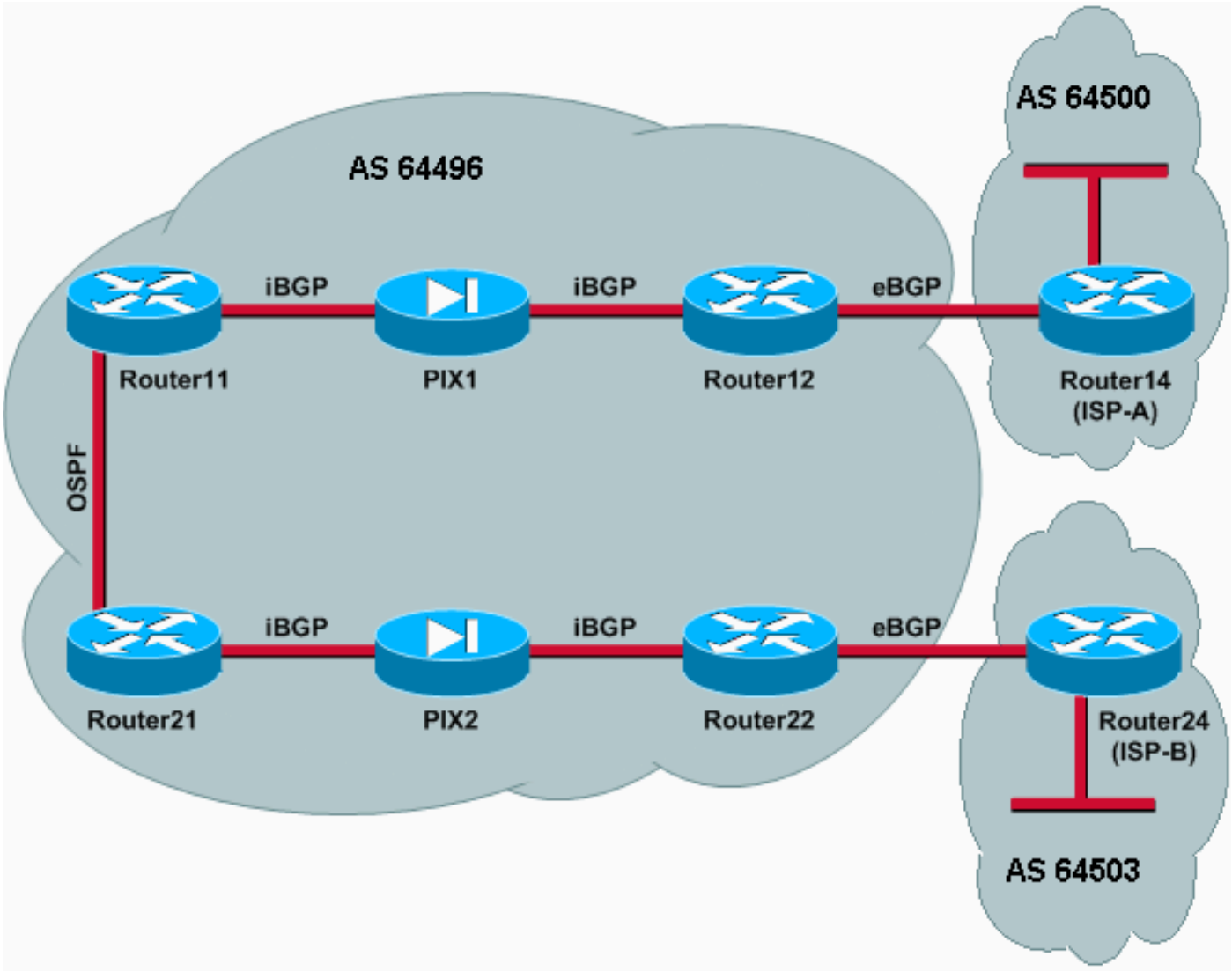
PIX1 と PIX2 は、アクセス リストを使用して、iBGP ピア間の BGP トラフィック（TCP、ポート 179）を許可するように設定されています。これは、PIX インターフェイスには、関連付けられたセキュリティ レベルがあるためです。デフォルトでは、内部インターフェイス（ethernet1）のセキュリティ レベルは 100 で、外部インターフェイス（ethernet0）のセキュリティ レベルは 0 です。接続およびトラフィックは、通常、高いセキュリティ レベルのインター

フェイスから低いレベルのセキュリティ インターフェイスへと許可されます。ただし、セキュリティ レベルの低いインターフェイスからセキュリティ レベルの高いインターフェイスへのトラフィックを許可するには、PIX でアクセス リストを明示的に定義する必要があります。また、外部のルータに PIX 内部のルータとの BGP セッションを開始するように許可するには、PIX1 と PIX2 のスタティックな NAT 変換を設定する必要があります。

Router11 と Router21 はともに、iBGP を通じて学習されたデフォルト ルートに基づいて、Open Shortest Path First（OSPF）ドメインへのデフォルト ルートが条件付きでアナウンスされます。Router11 では OSPF ドメインへのデフォルト ルートがメトリック 5 でアナウンスされ、Router21 ではデフォルト ルートがメトリック 30 でアナウンスされます。したがって、Router11 からのデフォルト ルートが優先されます。この設定は、Router11 と Router21 にデフォルト ルート 0.0.0.0/0 のみを伝搬するのに役立ちます。これにより、内部ルータでのメモリ消費が節約され、最適なパフォーマンスが実現されます。

このように、これらの条件をまとめるには、AS 64496 のルーティング ポリシーを次のようにします。

- AS 64496 では、すべての発信トラフィック（192.168.10.0/24 からインターネット）について、Router12 から ISP-A へのリンクが優先されます。
- ISP-A への接続に障害が発生した場合は、すべてのトラフィックは Router22 から ISP-B へのリンクを経由してルーティングされます。
- インターネットから 192.168.10.0/24 に到達するすべてのトラフィックでは、ISP-A から Router12 へのリンクが使用されます。
- ISP-A から Router12 へのリンクで障害が発生した場合は、すべての着信トラフィックは ISP-B から Router22 へのリンクを経由するようにルーティングされます。



設定

このシナリオでは、次の設定を使用します。

- 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.
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

両方の BGP セッションがアップしている場合は、すべてのパケットが ISP-A 経由でルーティングされることを予測できます。Router11のBGPテーブルを検討します。ネクストホップが172.16.12.2のRouter12からデフォルトルート0.0.0.0/0を学習します。

```
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
```

BGP を通じて学習された 0.0.0.0/0 デフォルト ルートは、Router11 の **show ip route の出力に示されるように、ルーティング テーブルにインストールされます。**

```
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
```

次に、Router21のBGPテーブルを検討します。Router22経由のデフォルトルートも学習します。

```
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
```

次に、BGP を通じて学習されたこのデフォルト ルートが、Router21 のルーティング テーブルにインストールされているかどうかを確認します。

```
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
```

Router21 のデフォルト ルートは OSPF を通じて学習されています (0.0.0.0/0 ルートの。 BGP を通じて Router22 から学習されたデフォルト ルートは存在しますが、**show ip route の出力には、OSPF を通じて学習されたデフォルト ルートが示されるのは興味深い点です。**

OSPF のデフォルト ルートは、Router21 で次の 2 つのソース、Router22 (iBGP 経由) と Router11 (OSPF 経由) からデフォルト ルートが学習されるため、Router21 にインストールされています。ルート選択プロセスでは、ルーティング テーブルへのより適切なアドミニストレーティブ ディスタンスによってルートがインストールされます。OSPFのアドミニストレーティブディスタンスは110で、iBGPのアドミニストレーティブディスタンスは200です。したがって、110は200未満であるため、OSPFで学習したデフォルトルートがルーティングテーブルにインストールされます。ルート選択の詳細

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

Router12 と ISP-A 間の BGP セッションをダウンにします。

```
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 には、BGP を通じて Router12 から学習されたデフォルト ルートがありません。

```
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
```

Router11のルーティングテーブルをチェックします。デフォルトルートは、ネクストホップがRouter21のOSPF (アドミニストレーティブディスタンス110) を介して学習されます。

```
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
```

この出力は、事前に定義したポリシーのように予測されます。ただし、この段階で、Router11 の **distance bgp 20 105 200 コンフィギュレーション コマンドについて理解し、このコマンドが Router11 でのルート選択にどのように影響するのかを理解することが重要です。**

このコマンドのデフォルト値は、**distance bgp 20 200 200** で、eBGP を通じて学習されたルート

のアドミニストレーティブ ディスタンスは 20、iBGP を通じて学習されたルートのアドミニストレーティブ ディスタンスは 200、ローカル BGP ルートのアドミニストレーティブ ディスタンスは 200 です。

Router12とISP-A間のリンクが再びアップすると、Router11はiBGP経由のデフォルトルートをRouter12から学習します。ただし、iBGPで学習したルートのデフォルトのアドミニストレーティブディスタンスは202020200であるため、OSPF00未満0に000です。 これにより、Router12 から ISP-A へのリンクが再びアップしても、Router21 から Router22 へのリンクに対するすべての発信トラフィックは、ISP-B へ強制されます。この問題を解決するには、iBGP を通じて学習されたルートの管理距離を、使用される Interior Gateway Protocol（IGP）よりも小さい値に変更します。この例では、IGP は OSPF であり、105 の距離が選択されました（105 は 110 より小さいため）。

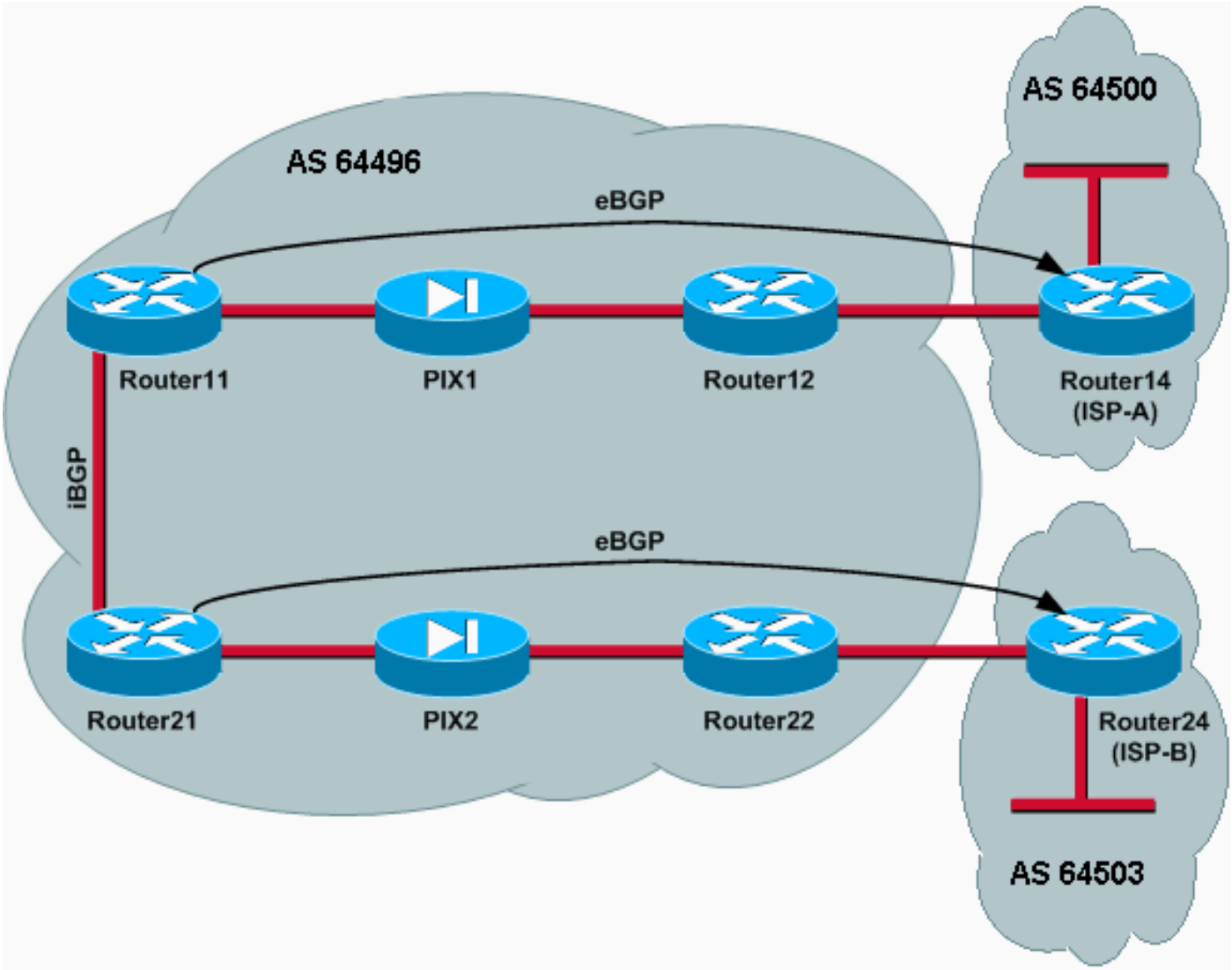
distance bgp コマンドの詳細については、「BGP コマンド」を参照してください。BGP を使用したマルチホーミングの詳細については、「シングルホームおよびマルチホーム環境における、BGP を使用したロード シェアリング：設定例」を参照してください。

シナリオ 2

このシナリオでは、Router11 によって Router14（ISP-A）との eBGP ピアリングが直接行われ、Router21 によって Router24（ISP-B）との eBGP ピアリングが直接行われています。Router12 と Router22 は BGP ピアリングには参加しませんが、それらによって ISP への IP 接続が提供されます。eBGP ピアはネイバーに直接接続されていないため、**neighbor ebgp-multihop コマンドはルータの参加で使用されます。neighbor ebgp-multihop**コマンドを使用すると、eBGPパケットの存続可能時間(TTL)がデフォルト値1から変更されるため、BGPはデフォルトの1ホップeBGP制限を上書きできます。このシナリオでは、eBGPネイバーは3ホップです値は3に変更されます。また、スタティックルートは、Router11がRouter14(ISP-A)アドレス172.16.13.4をpingでき、Router21がRouter24(ISP-B)アドレス172.16.23.4をpingできるように、ルータとPIXで設定されます。

デフォルトでは、PIX で、（**ping コマンドの発行時に送信される）Internet Control Message Protocol（ICMP）パケットのパス スルーは許可されていません。**ICMP パケットを許可するには、次の PIX 設定で示すように、**access-list コマンドを使用します。access-list コマンドの詳細については、「PIX Firewall の A から B のコマンド」を参照してください。**

ルーティング ポリシーは、シナリオ 1 と同じです。シナリオ 1 では、Router12 と ISP-A 間のリンクは、Router22 と ISP-B 間のリンクより優先されます。ISP-A のリンクがダウンすると、ISP-B のリンクはすべての着信および発信トラフィックに使用されます。



設定

このシナリオでは、次の設定を使用します。

- 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
```

確認

ISP-A および ISP-B へのリンクがアップしている状況から開始します。Router11 と Router21 での **show ip bgp summary コマンドの出力では、ISP-A と ISP-B にそれぞれ確立されている BGP セッションを確認します。**

```
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
```

Router11 の BGP テーブルには、ネクスト ホップ ISP-A 172.16.13.4 に向かうデフォルト ルート（0.0.0.0/0）が示されます。

```
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
```

次に、Router21のBGPテーブルを確認します。0.0.0.0/0ルートが2つあります。1つはeBGPで172.16.23.4のネクストホップを持つISP-Bから、もう1つはiBGPを通じてローカルプリファレンス200で学習されたルートです。Router21はlocal-preference属性が高いため、iBGPで学習ルート

します。BGP のパスの選択については、「BGP でベスト パスを選択するアルゴリズム」を参照してください。

```
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
```

トラブルシュート

Router11 と ISP-A BGP セッションをダウンにします。

```
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
```

ISP-A への eBGP セッションは、ホールドダウン タイマー (180 秒) が時間切れになると、ダウンします。

```
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
```

ISP-A へのリンクがダウンすると、Router11 では 192.168.10.2 (Router21) のネクスト ホップで 0.0.0.0/0 がインストールされます。これは、ルーティング テーブルで iBGP を通じて学習されます。これにより、次の出力に示されるように、すべての発信トラフィックが Router21 を介して ISP-B へプッシュされます。

```
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
```

PIX/ASA による BGP ネイバーの MD5 認証

PIX 6.x の設定

他のルーティング プロトコルと同様、BGP は認証用に設定できます。MD5 認証は 2 つの BGP ピアの間で設定できます。これは、ピア間の TCP 接続で送信された各セグメントが検証されるという意味です。MD5 認証は、両方の BGP ピアで同じパスワードを使って設定する必要があります。そうしないと、ピア間の接続が確立されません。MD5 認証を設定すると、Cisco IOS ソフトウェアによって TCP 接続で送信される各セグメントの MD5 ダイジェストが生成およびチェックされます。認証が呼び出され、セグメントが認証に失敗すると、エラー メッセージが生成されます。

PIX Firewall をパス スルーする MD5 認証で BGP ピアを設定する際は、BGP ネイバー間の TCP フローのシーケンス番号がランダムにならないように、BGP ネイバー間で PIX を設定することが重要です。これは PIX Firewall 上の TCP のランダムなシーケンス番号の機能がデフォルトで有効になっているためで、着信パケットの TCP シーケンス番号は転送前に変更されます。

MD5認証は、TCP psuedo-IPヘッダー、TCPヘッダー、およびデータに適用されます(RFC 2385を参照)。TCP はこのデータを使用します：TCP シーケンスと ACK 番号が含まれています：128 ビットのハッシュ番号を作成するため BGP ネイバー パスワードを付けます。ハッシュ番号は、TCP ヘッダー オプション フィールドのパケットに含まれています。PIX では、TCP フローごとにランダムな番号によってシーケンス番号がデフォルトで相殺されます。送信 BGP ピアでは、TCP によって元のシーケンス番号を使用されて 128 ビットの MD5 ハッシュ番号が作成され、このハッシュ番号がパケットに含められます。受信 BGP ピアがパケットを受け取ると、TCP では PIX で変更されたシーケンス番号が使用されて 128 ビットの MD5 ハッシュ番号が作成され、パケットに含まれるハッシュ番号と比較されます。

ハッシュ番号は、TCP シーケンス値が PIX によって変更されたため異なり、BGP ネイバーの TCP によってパケットがドロップされて、次のような MD5 の失敗メッセージが記録されます。

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

この問題を解決し、PIX によって TCP シーケンス番号が相殺されるのを停止するには、**norandomseq キーワードを static (inside,outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq コマンドとともに使用します。**次の例では、**norandomseq キーワードの使用について示します。**

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 !---
```

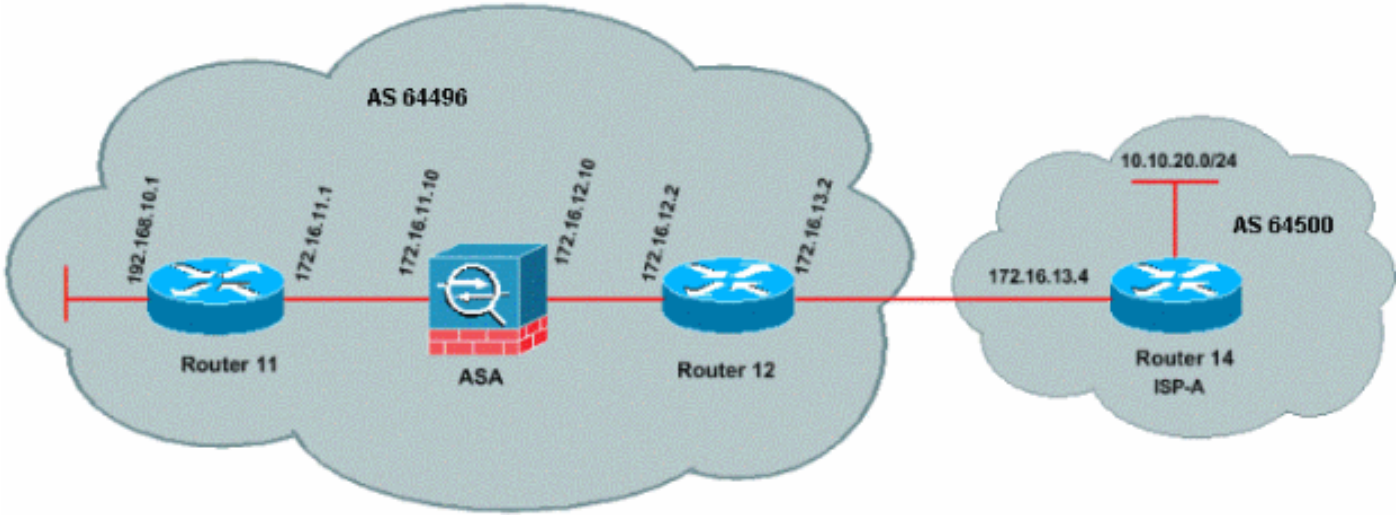
```
Allows ping to pass through for testing purposes only.

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 以降

このセクションでは、次のネットワーク構成を使用します。



PIX/ASA バージョン 7.x 以降では、MD5 認証を使用して BGP ピアリング セッションを確立しようとする場合の新たな課題を取り込んでいます。デフォルトでは、PIX/ASA バージョン 7.x 以降では、デバイスを通過する TCP データグラムに含まれる TCP MD5 オプションが書き換えられ、オプションの種類、サイズ、および値は NOP オプションのバイトに置き換えられます。これによって、BGP MD5 認証が壊され、それぞれのピアリング ルータで次のようなエラー メッセージが生成されることになります。

```
000296:Apr 7 2010 15:13:22.221 EDT:%TCP-6-BADAUTH:No MD5 digest from 172.16.11.1(28894) to
172.16.12.2(179)
```

MD5 認証を使用して BGP セッションが正常に確立されるためには、次の 3 つの問題を解決する必要があります。

- TCP シーケンス番号のランダム化の無効化
- TCP MD5 オプションの書き換えの無効化
- ピア間の NAT の無効化

クラス マップとアクセスリストは、ともに TCP のシーケンス番号のランダム化機能から除外される必要がある、ピア間のトラフィックを選択するために使用され、書き換えなしで MD5 オプションを伝送するように許可されます。tcp マップは、許可されるオプションの種類、この場合、オプションの種類 19 (TCP MD5 オプション) を指定するために使用されます。 クラス マップおよび tcp マップはともに、モジュラ ポリシー フレームワーク インフラストラクチャの一部であるポリシー マップを介してリンクされます。設定は、**service-policy コマンドを使用してアクティブ化されます。**

注： ピア間の NAT を無効にする必要性は、**no nat-control コマンドによって処理されます。**

バージョン 7.0 以降では、ASA のデフォルトの特性は **no nat-control** であり、ASA を介したすべての接続は、デフォルトでは、NAT テストにパスする必要がないことを示しています。ASA には **no nat-control** のデフォルト設定があると想定しています。詳細については、「nat-control」を参照してください。**nat-control が強制されている場合は、BGP ピアに対して NAT を明示的に無効にする必要があります。**これは、内部および外部インターフェイス間で、**static コマンドを使用して行うことができます。**

```
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
```

確認

show ip bgp summary コマンドからの出力は、認証が成功し、BGP セッションが Router11 で確

立されていることを示しています。

```
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#
```

関連情報

- BGP に関するサポート ページ
- BGP でベスト パスを選択するアルゴリズム
- シングルホームおよびマルチホーム環境における、BGP を使用したロード シェアリング：サンプル設定
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- PIX Firewall の設定とテスト
- テクニカル サポートとドキュメント – Cisco Systems