

ASA 8.3(x) : 3つの内部ネットワークとインターネットの接続の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[ASA 8.3 の設定](#)

[ASA 8.3 以降の設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、3つの内部ネットワークで使用するCisco適応型セキュリティアプライアンス(ASA)バージョン8.3を設定する方法について説明します。話を簡単にするため、ルータでスタティックルートを使用します。

セキュリティアプライアンスで適用されている変換を確認するには、『[PIX/ASA : 3つの内部ネットワークとインターネットの接続の設定例](#)』を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、バージョン8.3のCisco適応型セキュリティアプライアンス(ASA)に基づくものです。

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在

的な影響について理解しておく必要があります。

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

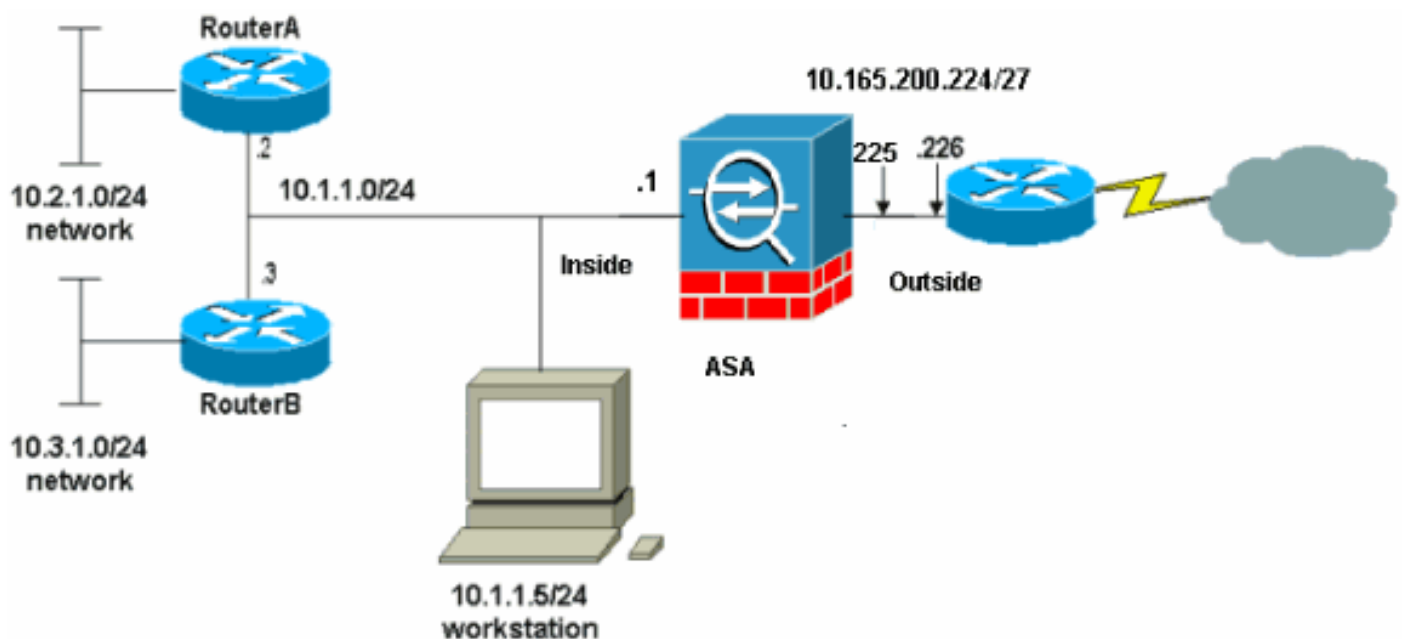
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。

注：10.1.1.0ネットワーク上のホストのデフォルトゲートウェイはRouterAを指しています。RouterBには、RouterAをポイントするデフォルトルートが追加されています。ルータAには、ASA内部インターフェイスをポイントするデフォルトルートがあります。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは [RFC 1918](#) で使用されているアドレスであり、ラボ環境で使用されたものです。

ASA 8.3 の設定

このドキュメントでは次の設定を使用します。

ご使用のシスコ デバイスの `write terminal` コマンドの出力データがある場合は、[アウトプット インタープリタ](#)（登録ユーザ専用）を使用して、今後予想される障害や修正を表示できます。

- [ルータ A の設定](#)
- [ルータ B の設定](#)
- [ASA 8.3 以降の設定](#)

ルータ A の設定

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
```

```
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.1.1  
ip route 10.3.1.0 255.255.255.0 10.1.1.3  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line 33  
no activation-character  
no exec  
transport preferred none  
transport input all  
transport output all  
line aux 0  
line vty 0 4  
password ww  
login  
!  
!  
end  
  
RouterA#
```

ルータBの設定

```
RouterB#show running-config  
Building configuration...  
  
Current configuration : 1132 bytes  
!  
version 12.4  
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname RouterB  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no network-clock-participate slot 1  
no network-clock-participate wic 0  
no network-clock-participate wic 1  
no network-clock-participate wic 2  
no network-clock-participate aim 0  
no network-clock-participate aim 1  
no aaa new-model  
ip subnet-zero  
ip cef  
!  
!  
!
```

```
!  
ip audit po max-events 100  
no ip domain lookup  
no ftp-server write-enable  
!  
!  
!  
!  
!  
no crypto isakmp enable  
!  
!  
!  
interface FastEthernet0/0  
ip address 10.1.1.3 255.255.255.0  
duplex auto  
speed auto  
no cdp enable  
!  
interface FastEthernet0/1  
ip address 10.3.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface IDS-Sensor1/0  
no ip address  
shutdown  
hold-queue 60 out  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.1.1.2  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
stopbits 1  
line 33  
no activation-character  
no exec  
transport preferred none  
transport input all  
transport output all  
line aux 0  
line vty 0 4  
password cisco  
login  
!  
!  
end  
  
RouterB#
```

[ASA 8.3 以降の設定](#)

注：デフォルト以外のコマンドは太字で表示されます。

ASA 8.3(1) の実行コンフィギュレーション

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.165.200.225 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa831-k8.bin

ftp mode passive

!--- Output Suppressed !--- Creates an object called
OBJ_GENERIC_ALL. !--- Any host IP not already matching
another configured !--- object will get PAT to the
outside interface IP !--- on the ASA (or 10.165.200.226)
for internet bound traffic. object network
OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL
interface

!--- Output Suppressed !--- Define a default route to
the ISP router. route outside 0.0.0.0 0.0.0.0
10.165.200.226 1

!--- Define a route to the INTERNAL router with network
10.2.1.0. route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network
10.3.1.0. route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

注：ASA 8.3でのNATおよびPATの設定の詳細については、『[NATに関する情報](#)』を参照してください。

PIX/ASA のアクセス リストの設定方法の詳細については、『[PIX/ASA 7.x : nat、global、static および access-list の各コマンドを使用したポート リダイレクション \(フォワーディング\)](#)』を参照してください。

確認

現在、この設定に使用できる確認手順はありません。

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに使用できる情報を示します。

注：PIX/ASAのトラブルシューティング方法の詳細は、『[PIXおよびASAを経由した接続のトラブルシューティング](#)』を参照してください。

[トラブルシューティングのためのコマンド](#)

[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。

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **debug icmp trace** : ホストからのICMP要求がPIXに到達するかどうかを示します。このデバッグを実行するには、**access-list** コマンドを設定に追加して、ICMP を許可する必要があります。
- **logging buffer debuggggging**:PIXを通過するホストへの接続が確立および拒否されていることを示します。この情報は PIX ログ バッファに保存されており、**show log** コマンドを使用して表示できます。

ロギングの設定方法については、『[PIX Syslog のセットアップ](#)』を参照してください。

[関連情報](#)

- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)