PIX/ASA 7.x 以降： 3 つの内部ネットワークでの PIX/ASA 7.x の設定例

目次

概要

このドキュメントでは、コマンド ライン インターフェイス (CLI) または Adaptive Security Device Manager (ASDM) 5.x 以降を使用して、複数の内部ネットワークをインターネットに接続するための PIX/ASA セキュリティ アプライアンス バージョン 7.x 以降の設定例について説明します。

PIX/ASA 経由による接続の確立方法とトラブルシューティングの詳細は、『Cisco セキュリティ アプライアンス経由の接続の確立とトラブルシューティング』を参照してください。

PIX コマンド一般についての詳細は、『PIX での nat、global、static、conduit、および access-list の各コマンドとポート リダイレクション (フォワーディング) の使用方法』 を参照してください。

注: 他のバージョンの ASDM では、一部のオプションが ASDM 5.1 とは異なって表記されている可能性があります。 詳細は、『ASDM ドキュメント』を参照してください。

前提条件

要件

PIX ファイアウォールの背後に複数の内部ネットワークを追加する際には、次のポイントに留意してください。

- PIX ではセカンダリ アドレッシングがサポートされない。
- 既存のネットワークと新しく追加されるネットワークとの間のルーティングを達成するために、ルータは PIX の背後で使用される必要がある。
- すべてのホストのデフォルト ゲートウェイは、内部ルータをポイントする必要がある。
- PIX をポイントする内部ルータにデフォルト ルートを追加する。
- 内部ルータの Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュをクリアする。

ASDM でデバイスを設定できるようにする方法については、『ASDM 用の HTTPS アクセスの許可』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.1 が稼働する PIX セキュリティ アプライアンス 515E
- ASDM 5.1
- Cisco IOS(R) ソフトウェア リリース 12.3(7)T が稼働するシスコ製ルータ

注: このドキュメントの内容は、PIX/ASA ソフトウェア バージョン 8.x と Cisco IOS ソフトウェア リリース 12.4 で再検証されています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco ASA セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

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

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

この設定で使用している IP アドレス スキームは、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。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

背景説明

このシナリオでは、PIX 経由でインターネット（または、外部ネットワーク）に接続される 3 つの内部ネットワーク（10.1.1.0/24、 10.2.1.0/24、および 10.3.1.0/24）が使用されます。 内部ネットワークは、PIX の Inside インターフェイスに接続されます。 インターネットには、PIX の Outside インターフェイスに接続されたルータを経由して接続されます。 PIX の IP アドレスは、172.16.1.1/24 です。

内部ネットワークからインターネットへ、およびその逆方向へのパケットのルーティングには、スタティック ルートが使用されます。 スタティック ルートではなく、Routing Information Protocol（RIP）や Open Shortest Path First（OSPF）などのダイナミック ルーティング プロトコルを使用することもできます。

内部ホストでは、ダイナミック NAT プール（IP アドレス 172.16.1.5 ~ 172.16.1.10）を使用して、PIX 上の内部ネットワークを変換することによって、インターネットとの通信が行われます。 IP アドレスのプールが使い果たされた場合には、PIX は内部ホストを（IP アドレス 172.16.1.4 を使用して）ポート アドレス変換（PAT）することによって、インターネットに到達できるようにします。

NAT/PAT の詳細は、『PIX/ASA 7.x および FWSM：NAT と PAT の設定例』を参照してください。

注: スタティック NAT で変換に Outside IP（global_IP）アドレスを使用すると、これにより変換が行われる可能性があります。 そのため、スタティック変換では IP アドレスではなくキーワード interface を使用します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

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 をポイントしています。 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、PIX の内側のインターフェイスをポイントするデフォルト ルートが設定されています。

設定

このドキュメントでは、次の設定を使用します。

- ルータ A の設定
- ルータ B の設定
- PIX セキュリティ アプライアンス 7.1 の設定ASDM を使用した PIX の設定CLI を使用した PIX セキュリティ アプライアンスの設定

ルータ A の設定

```
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service config service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterA ! interface Ethernet2/0 ip address
10.2.1.1 255.255.255.0 half-duplex ! interface
Ethernet2/1 ip address 10.1.1.2 255.255.255.0 half-
duplex ! 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 ! ! line con 0
line aux 0 line vty 0 4 ! end RouterA#
```

ルータ B の設定

```
RouterB#show running-config Building configuration...
Current configuration : 1132 bytes ! version 12.4
service config service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname RouterB ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed
auto ! interface Ethernet1/0 ip address 10.3.1.1
255.255.255.0 half-duplex ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! end RouterB#
```

PIX セキュリティ アプライアンスの設定に ASDM を使用したい場合に、デバイスのブートストラップが済んでいないときには、次の手順を実行します。

1. PIX にコンソール接続します。
2. デフォルト設定の状態から、インタラクティブなプロンプトを使用して、Workstation 10.1.1.5 から ASDM で PIX を管理できるようにします。

PIX セキュリティ アプライアンス 7.1 の設定

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
```

```
commands
        INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
        INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
        INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
        INFO: converting 'fixup protocol rsh 514' to
MPF commands
        INFO: converting 'fixup protocol rtsp 554' to
MPF commands
        INFO: converting 'fixup protocol sip 5060' to
MPF commands
        INFO: converting 'fixup protocol skinny 2000'
to MPF commands
        INFO: converting 'fixup protocol smtp 25' to
MPF commands
        INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
        INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
        INFO: converting 'fixup protocol tftp 69' to
MPF commands
        INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
        INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
        OZ-PIX>
```

ASDM を使用した PIX の設定

ASDM の GUI から設定を行うには、次の手順を実行します。

1. Workstation 10.1.1.5 で、ADSM を使用するために Web ブラウザを開きます（この例では、https://10.1.1.1）。
2. 認証のプロンプトで [**yes**] をクリックします。
3. あらかじめ設定されたとおりに、イネーブル パスワードでログインします。
4. PC 上で初めて ASDM を実行する場合は、Java App として ASDM Launcher または ASDM を使用するように指示されます。 この例では、ASDM Launcher が選択され、インストールされます。
5. [ASDM Home] ウィンドウに移動して、[Configuration] をクリックします。
6. [Interface] >[Edit] を選択して、Outside インターフェイスを設定します。
7. インターフェイスの詳細を入力し、完了したら [OK] をクリックします。
8. Security Level Change ダイアログ ボックスで OK をクリックします。
9. [Apply] をクリックして、インターフェイスの設定を承認します。 設定内容は PIX にもプッシュされます。
10. [Features] タブの [Security Policy] を選択して、使用するセキュリティ ポリシー ルールを確認します。 この例では、デフォルトの 内部ルールが使用されます。
11. この例では、NAT を使用します。 [Enable traffic through the firewall without address translation] チェック ボックスをオフにし、[Add] をクリックして、NAT ルールを設定します。
12. Source Network を設定します。 この例では、IP アドレスに 10.0.0.0 が使用され、マスクに 255.0.0.0 が使用されています。[**Manage Pools**] をクリックして、NAT プール アドレス

を定義します。
13. outside インターフェイスを選択し、[Add] をクリックします。
14. この例では、Range と PAT アドレス プールが設定されています。 NAT プール アドレスの範囲を設定し、[OK] をクリックします。
15. ステップ 13 で指定した outside インターフェイスを選択し、PAT アドレスを設定します。[OK] をクリックします。[OK] をクリックして続行します。
16. [Edit Address Translation Rule] ウィンドウで、ソース ネットワークで使用する Pool ID を選択します。 [OK] をクリックします。
17. [Apply] をクリックして、設定した NAT ルールを PIX にプッシュします。
18. この例では、スタティック ルートが使用されています。 [Routing] をクリックし、[Static Route] を選択して、[Add] をクリックします。
19. デフォルト ゲートウェイを設定し、[OK] をクリックします。
20. [Add] をクリックして、inside ネットワークにルートを追加します。
21. 正しいルートが設定されていることを確認して、[Apply] をクリックします。

CLI を使用した PIX の設定

ASDM GUI による設定は、これで完了しました。

この設定を CLI を使用して確認できます。

PIX セキュリティ アプライアンスの CLI

```
pixfirewall(config)#write terminal PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 172.16.1.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- Assign name and IP address
to the interfaces enable password 2KFQnbNIdI.2KYOU
encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image
flash:/asdmfile.50073 no asdm history enable arp timeout
14400 nat-control !--- Enforce a strict NAT for all the
traffic through the Security appliance global (outside)
1 172.16.1.5-172.16.1.10 netmask 255.255.255.0 !---
Define a pool of global addresses 172.16.1.5 to
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
(outside) 1 172.16.1.4 netmask 255.255.255.0 !--- Define
a single IP address 172.16.1.4 with NAT ID 1 to be used
for PAT nat (inside) 1 10.0.0.0 255.0.0.0 !--- Define
the inside networks with same NAT ID 1 used in the
global command for NAT route inside 10.3.1.0
255.255.255.0 10.1.1.3 1 route inside 10.2.1.0
255.255.255.0 10.1.1.2 1 !--- Configure static routes
for routing the packets towards the internal network
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1 !---
Configure static route for routing the packets towards
the Internet (or External network) timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 timeout uauth 0:05:00 absolute http server
enable !--- Enable the HTTP server on PIX for ASDM
access http 10.1.1.5 255.255.255.255 inside !--- Enable
HTTP access from host 10.1.1.5 to configure PIX using
ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

[File] > [Show Running Configuration in New Windows] を選択して、ASDM の CLI 設定を表示します。

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

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

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できるようにするには、構成内に **access-list** コマンドを追加して、ICMP を許可するようにする必要があります。
- **logging buffer debugging**：PIX を通過するホストに対して確立された接続と拒否された接続を示します。 情報は PIX ログ バッファに保存され、**show log** コマンドで出力を表示できます。

トラブルシューティング手順

ASDM を使用してロギングを有効にし、ログを表示できます。

1. [Configuration] > [Properties] > [Logging] > [Logging Setup] を選択し、[Enable Logging] をオンにします。そして、[Apply] をクリックします。
2. [Monitoring] > [Logging] > [Log Buffer] > [Logging Level] を選択し、ドロップダウン リストから [Logging Buffer] を選択します。 [View] をクリックします。
3. Log Buffer の例を次に示します。

ドメイン名を使用して Web サイトにアクセスできない

シナリオによっては、Web ブラウザで（IP アドレスと連動する）名前を使用した場合に、内部ネットワークがインターネットの Web サイトにアクセスできない場合があります。 この問題は、通常は DNS サーバが定義されていないとき、特に PIX/ASA が DHCP サーバであるという状況でよく発生します。 また、PIX/ASA が DNS サーバにプッシュできない場合、または DNS サーバに到達できない場合にも発生する可能性があります。

関連情報

- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- Cisco Adaptive Security Device Manager

- Cisco Adaptive Security Device Manager (ASDM) Troubleshoot and Alerts
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems