DHCP サーバおよびクライアントとしての PIX/ASA の設定例

目次

概要

PIX 500 シリーズのセキュリティ アプライアンスと Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）は、Dynamic Host Configuration Protocol（DHCP）サーバと DHCP クライアントのいずれとしても動作できます。 DHCP とは、サブネット マスク付きの IP アドレス、デフォルト ゲートウェイ、DNS サーバ、WINS サーバの IP アドレスなどの設定パラメータを自動的にホストに付与するためのプロトコルです。

セキュリティ アプライアンスは DHCP サーバまたは DHCP クライアントとして動作できます。セキュリティ アプライアンスがサーバとして動作する場合には、ネットワークの設定パラメータはセキュリティ アプライアンスにより直接 DHCP クライアントに付与されます。 セキュリティ アプライアンスが DHCP クライアントとして動作する場合には、これらのパラメータはセキュリティ アプライアンスから DHCP サーバに要求されます。

このドキュメントでは、セキュリティ アプライアンスの Cisco Adaptive Security Device Manager（ASDM）を使用して、DHCP サーバと DHCP クライアントを設定する方法に重点を置いて説明しています。

前提条件

要件

このドキュメントでは、PIX セキュリティ アプライアンスまたは ASA が完全に動作していて、Cisco ASDM で設定を変更できるように設定されていることを想定しています。

注: デバイスを ASDM で設定できるようにする方法については、『ASDM 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。

- PIX 500 シリーズ セキュリティ アプライアンス 7.x**注:** バージョン 7.x で使用する PIX CLI の設定は、PIX 6.x にも適用できます。 唯一の違いは、PIX 6.3 より前のバージョンでは DHCP サーバを内側のインターフェイスでしかイネーブルにできないことです。 PIX 6.3 以降では、DHCP サーバは使用可能なすべてのインタフェイスでイネーブルにできます。 この設定では、DHCP サーバの機能を外部インターフェイスで使用します。
- ASDM 5.x**注:** ASDM では、PIX 7.0 以降だけをサポートしています。 PIX Device Manager（PDM）は PIXバージョン 6.x を設定して利用できます。詳細については、『Cisco ASA 5500 シリーズおよび PIX 500 シリーズ セキュリティ アプライアンスのハードウェアとソフトウェアの互換性』を参照してください。

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 7.x にも使用できます。

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

この設定では、バージョン 7.x が稼働している 2 台の PIX セキュリティ アプライアンスを使用しています。 片方が DHCP サーバとして動作して、もう一方の DHCP クライアントとして動作する PIX セキュリティ アプライアンス 7.x に設定パラメータを与えます。 DHCP サーバとして機能する場合、PIX は指定されている IP アドレスのプールから IP アドレスを DHCP クライアントに動的に割り当てます。

セキュリティ アプライアンスの各インターフェイスで DHCP サーバを設定できます。 各インターフェイスにはアドレスを引き出すための独自のアドレス プールを置くことができます。 ただし、DNS サーバ、ドメイン名、オプション、ping タイムアウト、WINS サーバなどの他の DHCP 設定は、すべてのインターフェイスについて DHCP サーバでグローバルに設定して使用します。

サーバがイネーブルになっているインターフェイスでは、DHCP クライアントや DHCP リレー サービスを設定できません。 さらに、DHCP クライアントはサーバがイネーブルになっているイ

ンターフェイスに、直接に接続されている必要があります。

そして、あるインターフェイスで DHCP サーバがイネーブルになっているときには、そのインターフェイスの IP アドレスは変更できません。

注: 基本的には、DHCPサーバ（PIX/ASA）から送信 される DHCP応答のデフォルトゲートウェイアドレスを設定 する 設定 オプションがありません。 DHCPサーバは DHCP クライアントのためのゲートウェイとして自身のアドレスを常に送信 します。 ただしインターネットルータへのポイントがユーザがインターネットに達することを可能にすること、デフォルト ルートを定義します。

注: 割り当てることができる DHCPプール アドレスの数はセキュリティ アプライアンス モデル（PIX/ASA）で使用されるライセンスに左右されます。 ライセンスと基礎/セキュリティを使用すればこれらの制限は DHCPプールに適用します。 ホスト制限が 10 のホストである場合、32 アドレスに DHCPプールを制限します。 ホスト制限が 50 のホストである場合、128 アドレスに DHCPプールを制限します。 ホスト制限が無制限である場合、256 アドレスに DHCPプールを制限します。 従ってホストの数に基づくアドレス プールは限られています。

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。

このドキュメントでは、次の設定を使用します。

- ASDM を使用した DHCP サーバの設定
- ASDM を使用した DHCP クライアントの設定
- DHCP サーバの設定
- DHCP クライアントの設定

ASDM を使用した DHCP サーバの設定

ASDM を使用して PIX セキュリティ アプライアンスまたは ASA を DHCP サーバとして設定するには、次の手順を実行します。

1. **> Properties > DHCP 保守します** Home ウィンドウから **> DHCPサーバ** 『Configuration』を選択 して下さい。 インターフェイスを選択し、Edit をクリックして、DHCP サーバをイネーブルにし、DHCP アドレス プールを作成します。アドレス プールはセキュリティ アプライアンスのインターフェイスと同じサブネット上にある必要があります。 この例では、DHCP サーバは PIX セキュリティ アプライアンスの外部インターフェイスに設定されています。
2. DHCP クライアントの要求を受信する外部インターフェイスに対して、Enable DHCP server にチェック マークを入れます。 DHCP クライアントに割り当てるアドレスのプールを指定して、OK をクリックし、メイン ウィンドウに戻ります。
3. Enable auto-configuration on the interface にチェック マーク入れ、DHCP サーバで DHCP クライアントに対して DNS、WINS、デフォルトのドメイン名を自動的に設定するようにします。 Apply をクリックして、セキュリティ アプライアンスの実行コンフィギュレーションをアップデートします。

ASDM を使用した DHCP クライアントの設定

ASDM を使用して PIX セキュリティ アプライアンスを DHCP クライアントとして設定するには

、次の手順を実行します。

1. Configuration > Interfaces の順に選択 し、Ethernet0 インターフェイスを DHCPサーバからのサブネット マスク、デフォルト ゲートウェイ、DNSサーバおよび WINS サーバのIPアドレスの IP アドレスのようなコンフィギュレーションパラメータを受け取るためにイネーブルに設定するために『Edit』 をクリック して下さい。
2. Enable Interface にチェック マークを入れ、インターフェイスの名前とセキュリティ レベルを入力します。 IP アドレスについては Obtain address via DHCP を、デフォルト ゲートウェイについては Obtain default route using DHCP を選択し、OK をクリックしてメイン ウィンドウに戻ります。
3. Apply をクリックし、DHCP サーバから取得した Ethernet0 の IP アドレスを確認します。

DHCP サーバの設定

この設定は ASDM で作成されたものです。

DHCP サーバ

```
pixfirewall#show running-config PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.0.0.1
255.0.0.0 ! !--- Output is suppressed. logging enable
logging asdm informational mtu inside 1500 mtu outside
1500 no failover asdm image flash:/asdm-511.bin http
server enable http 10.0.0.0 255.0.0.0 inside no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 !--- Specifies a DHCP address pool and the interface
for the client to connect. dhcpd address 192.168.1.5-
192.168.1.7 outside !--- Specifies the IP address(es) of
the DNS and WINS server !--- that the client uses. dhcpd
dns 192.168.0.1 dhcpd wins 172.0.0.1 !--- Specifies the
lease length to be granted to the client. !--- This
lease equals the amount of time (in seconds) the client
!--- can use its allocated IP address before the lease
expires. !--- Enter a value between 0 to 1,048,575. The
default value is 3600 seconds. dhcpd lease 3600 dhcpd
ping_timeout 50 dhcpd auto_config outside !--- Enables
the DHCP daemon within the Security Appliance to listen
for !--- DHCP client requests on the enabled interface.
dhcpd enable outside dhcprelay timeout 60 ! !--- Output
is suppressed. service-policy global_policy global
Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab : end
```

DHCP クライアントの設定

この設定は ASDM で作成されたものです。

DHCP Client

```
pixfirewall#show running-config PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 !---
```

```
Configures the Security Appliance interface as a DHCP
client. !--- The setroute keyword causes the Security
Appliance to set the default !--- route using the
default gateway the DHCP server returns. ip address dhcp
setroute ! interface Ethernet1 nameif inside security-
level 100 ip address 10.0.0.14 255.0.0.0 !--- Output is
suppressed. ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging console debugging logging asdm informational mtu
outside 1500 mtu inside 1500 no failover asdm image
flash:/asdm-511.bin no asdm history enable arp timeout
14400 timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
uauth 0:05:00 absolute http server enable http 10.0.0.0
255.0.0.0 inside !--- Output is suppressed. ! service-
policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989 : end
```

確認

次の手順に従って、ASDM を使用して DHCP 統計情報と DHCP サーバと DHCP クライアントのバインディング情報を確認します。

1. **>** DHCPDISCOVER、DHCPREQUEST、DHCPOFFER および DHCPACK のような DHCP 統計情報を、確認する DHCPサーバからの **DHCP > DHCP 統計情報** 『Monitoring』 を選択して下さい **> インターフェイスします**。CLI で show dhcpd statistics コマンドを入力して、DHCP の統計情報を表示します。
2. **> DHCP >** DHCP バインディング情報を表示する DHCP クライアントからの **DHCP クライアント リース情報** 『Monitoring』 を選択 して下さい **> インターフェイスします**。CLI で show dhcpd binding コマンドを入力して、DHCP のバインディング情報を表示します。
3. **> ロギング >** リアルタイム ログメッセージを表示するためにログ レベルおよびバッファの制限を選択する**リアルタイム ログ ビューア** 『Monitoring』 を選択 して下さい。
4. DHCP クライアントからリアルタイムのログ イベントを表示します。 DHCP クライアントの外部インターフェイスに IP アドレスが割り当てられています。

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

ここでは、設定が正常に動作していることを確認します。

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。

- **dhcpd を event** — 表示する DHCPサーバと関連付けられる催物の表示部分を**デバッグして下さい。**
- **デバッグして下さい dhcpd パケット**— DHCPサーバと関連付けられるパケット情報を表示す

る。

エラー メッセージ

```
CiscoASA(config)#dhcpd address 10.1.1.10-10.3.1.150 inside Warning, DHCP pool range is limited
to 256 addresses, set address range as: 10.1.1.10-10.3.1.150
```

説明： アドレス プールのサイズはセキュリティ アプライアンス モデルのプール毎に 256 アドレスに制限されます。 これは変更することができないし、ソフトウェア 制限です。 合計は 256 であるただ場合もあります。 アドレス プール 範囲が大きければより 253 アドレス（ たとえば 254 は、255、256 ）、セキュリティ アプライアンス モデル インターフェイスのネットマスク アドレス クラス C である場合もありません（ たとえば、255.255.255.0 ）。 それは、たとえばより大きい、何か 255.255.254.0 である必要があります。

セキュリティ アプライアンス モデルに DHCPサーバ 機能を設定する方法の情報に関しては Ciscoセキュリティ アプライアンス コマンド・ライン コンフィギュレーション ガイドを参照して下さい。

FAQ： アドレス 指定

質問— DHCPサーバとして ASA を使用するコンピュータに静的な/常置 IP アドレスを割り当てることは可能性のあるですか。

返事—それは PIX/ASA を使用して可能性のあるではないです。

質問— ASA の特定の MAC アドレスに DHCP アドレスを結ぶことは可能性のあるですか。

返事—いいえ、それは可能性のあるではないです。

関連情報

- PIX セキュリティ アプライアンスに関するサポート ページ
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- テクニカルサポートとドキュメント - Cisco Systems