

PIX/ASA : PPPoE クライアント設定の例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[CLI 設定](#)

[ASDM の設定](#)

[確認](#)

[設定の解除](#)

[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](#)

[サブネットマスクは /32 として現われます](#)

[関連情報](#)

概要

このドキュメントでは、バージョン 7.2.(1) 以降で Point-to-Point Protocol over Ethernet (PPPoE) のクライアントとして ASA/PIX セキュリティ アプライアンスを設定する例を説明します。

PPPoE では、一般的に使用されている標準技術であるイーサネットと PPP の 2 つを組み合わせ、クライアントシステムに IP アドレスを割り当てる認証方式を提供します。一般的な PPPoE クライアントは、DSL やケーブル サービスなどのリモート ブロードバンド接続によって ISP に接続されているパーソナル コンピュータです。既存のリモート アクセス インフラストラクチャを使用する高速ブロードバンド アクセスをサポートするために、またユーザにとって使いやすいことから、ISP では PPPoE を導入しています。

PPPoE は、PPPoE ネットワークの認証方式を使用するための標準方式です。ISP が PPPoE を使用すると、IP アドレスの認証割り当てを実行できます。このタイプの実装では、PPPoE クライアントとサーバは、DSL または他のブロードバンド接続上で実行されているレイヤ 2 ブリッジング プロトコルによって相互に接続されます。

PPPoE は、次の 2 つの主要フェーズで構成されています。

- アクティブなディスカバリはこのフェーズを、PPPoE クライアント取付けますセッションID が割り当てられる PPPoE 層が確立されるアクセスコンセントレータと呼ばれる PPPoE サーバをフェーズインし、

- PPP セッションはこのフェーズをフェーズインします、ポイントツーポイントプロトコル (PPP) オプションはネゴシエートされ、認証は実行された。リンクのセットアップが完了すると、PPPoE がレイヤ 2 カプセル化方式としての機能を開始し、PPP リンク経由で PPPoE ヘッダーにデータを転送できるようになります。

PPPoE クライアントは、システムの初期化時に一連のパケットを交換して、アクセス コンセントレータとのセッションを確立します。セッションが確立されると、PPP リンクがセットアップされます。このとき、認証には Password Authentication Protocol (PAP; パスワード認証プロトコル) が使用されます。PPP セッションが確立されると、各パケットは PPPoE ヘッダーと PPP ヘッダーでカプセル化されます。

注: 適応型セキュリティ アプライアンスでフェールオーバーが設定されている場合、またはマルチ コンテキストや透過モードの場合、PPPoE はサポートされません。PPPoE は、フェールオーバーを実行しない、シングル ルーテッド モードでのみサポートされます。

[前提条件](#)

[要件](#)

このドキュメントに関しては個別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、Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) バージョン 8.x 以降に基づいています。

本書の情報は、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、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

[関連製品](#)

この設定は、バージョン 7.2(1) 以降で稼働する Cisco PIX 500 シリーズ セキュリティ アプライアンスでも使用できます。PIX OS バージョン 6.2 では、Cisco Secure PIX Firewall で PPPoE クライアントを設定するためにこの機能が導入され、ローエンド PIX (501/506) に対応します。詳細については、『[Cisco Secure PIX Firewall 上での PPPoE クライアントの設定](#)』を参照してください。

[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の情報を提供しています。

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。

[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。

[CLI 設定](#)

このドキュメントでは、次の設定を使用します。

デバイス名 1

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif dmz
 security-level 50
 ip address 10.77.241.111 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
!--- Specify a VPDN group for the PPPoE client pppoe
client vpdn group CHN
!--- "ip address pppoe [setroute]" !--- The setroute
option sets the default routes when the PPPoE client has
!--- not yet established a connection. When you use the
setroute option, you !--- cannot use a statically
defined route in the configuration. !--- PPPoE is not
supported in conjunction with DHCP because with PPPoE !-
-- the IP address is assigned by PPP. The setroute
option causes a default !--- route to be created if no
default route exists. !--- Enter the ip address pppoe
command in order to enable the !--- PPPoE client from
interface configuration mode.

 ip address pppoe
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
```

```
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
access-list 100 extended permit ip any any
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 10.
20.10.0 255.255.255.0 inactive
pager lines 24
mtu dmz 1500
!--- The maximum transmission unit (MTU) size is
automatically set to 1492 bytes, !--- which is the
correct value to allow PPPoE transmission within an
Ethernet frame. mtu outside 1492
mtu inside 1500

!--- Output suppressed. global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
!--- The NAT statements above are for ASA version 8.2
and earlier. !--- For ASA versions 8.3 and later the NAT
statements are modified as follows. object network
obj_any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface

!--- Output suppressed. telnet timeout 5 ssh timeout 5
console timeout 0 !--- Define the VPDN group to be used
for PPPoE. vpdn group CHN request dialout pppoe
!--- Associate the user name assigned by your ISP to the
VPDN group. vpdn group CHN localname cisco
!--- If your ISP requires authentication, select an
authentication protocol. vpdn group CHN ppp
authentication pap
!--- Create a user name and password for the PPPoE
connection. vpdn username cisco password *****

threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
  match default-inspection-traffic
!
!
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
```

```
!  
service-policy global_policy global  
username cisco123 password ffIRPGpDS0Jh9YLq encrypted  
privilege 15  
prompt hostname context  
Cryptochecksum:3cf813b751fe78474dfb1d61bb88a133  
: end  
ciscoasa#
```

ASDM の設定

適応型セキュリティ アプライアンスに付属する PPPoE クライアントを設定するには、次の手順を実行します。

注: ASA を ASDM で設定できるようにするには、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

1. ASA の ASDM にアクセスします。ブラウザを開き、https://<ASDM_ASA_IP_ADDRESS> と入力します。ここで、ASDM_ASA_IP_ADDRESS は ASDM アクセスに設定されている ASA インターフェイスの IP アドレスです。注: SSL 証明書の信頼性に関連してブラウザから出力されるすべての警告を承認します。デフォルトのユーザ名とパスワードは、両方も空白です。ASA がこのウィンドウを表示するのは、ASDM アプリケーションのダウンロードを許可するためです。次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。
2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連の手順を実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
4. **http** - コマンドで設定したインターフェイスの IP アドレス、およびユーザ名とパスワード (指定した場合) を入力します。次の例では、ユーザ名として **cisco123**、パスワードとして **cisco123** を使用しています。
5. [Configuration] > [Device Setup] > [Interfaces] の順に選択し、outside インターフェイスを強調表示して、[Edit] をクリックします。
6. [Interface Name] フィールドに **outside** と入力し、[Enable Interface] チェックボックスをオンにします。
7. IP アドレス エリアの [Use PPPoE] オプション ボタンをクリックします。
8. グループ名、PPPoE ユーザ名、パスワードを入力し、適切な PPP 認証のタイプ (PAP、CHAP、MSCHAP) オプション ボタンをクリックします。
9. [Advanced] タブをクリックし、MTU サイズが **1492** に設定されていることを確認します。
注: Maximum Transmission Unit (MTU; 最大伝送ユニット) のサイズは自動的に 1492 バイトに設定されます。これは、イーサネット フレームで PPPoE 伝送を実行する正しい値です。
10. [OK] をクリックして、次に進みます。
11. 入力した情報が正しいことを確認し、[Apply] をクリックします。

確認

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。

- **show ip address outside pppoe** : このコマンドを使用して、現在の PPPoE クライアント設定情報を表示します。
- **show vpdn session [l2tp | pppoe] [id sess_id | パケット | 状態 | window]** : このコマンドを使用して、PPPoE セッションのステータスを表示します。

このコマンドで表示される情報の例を次に示します。

```
hostname#show vpdn
Tunnel id 0, 1 active sessions
  time since change 65862 secs
  Remote Internet Address 10.0.0.1
  Local Internet Address 199.99.99.3
  6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
Session state is SESSION_UP
  Time since event change 65865 secs, interface outside
  PPP interface id is 1
  6 packets sent, 6 received, 84 bytes sent, 0 received
```

```
hostname#show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
Session state is SESSION_UP
  Time since event change 65887 secs, interface outside
  PPP interface id is 1
  6 packets sent, 6 received, 84 bytes sent, 0 received
```

```
hostname#show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
  time since change 65901 secs
  Remote Internet Address 10.0.0.1
  Local Internet Address 199.99.99.3
  6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#
```

設定の解除

すべての vpdn group コマンドを設定から削除するには、グローバル コンフィギュレーション モードで clear configure vpdn group コマンドを使用します。

```
hostname(config)#clear configure vpdn group
```

すべての vpdn username コマンドを削除するには、clear configure vpdn username コマンドを使用します。

```
hostname(config)#clear configure vpdn username
```

注: これらのコマンドによる、アクティブな PPPoE 接続への影響はありません。

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。

- `hostname# [no] debug pppoe {event | error | packet}` : このコマンドを使用して、PPPoE クライアントのデバッグをイネーブルまたはディセーブルにします。

サブネットマスクは /32 として現われます

問題

IP アドレス `x.x.x.x 255.255.255.240 pppoe setroute` コマンドを使用するとき、IP アドレスは正しく割り当てられますが、/28 としてコマンドで規定されるがサブネットマスクは /32 として現われます。なぜ、このような現象が発生するのでしょうか。

解決策

これは正常な動作です。サブネットマスクは PPPoe インターフェイスの場合には関係がないです; ASA は /32 にそれを常に変更します。

関連情報

- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス](#)
- [シスコ以外の DSL CPE に接続するための Cisco 2600 での PPPoE クライアントの設定](#)
- [Cisco Adaptive Security Device Manager](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)