PIX/ASA： PPPoE クライアント設定の例

目次

はじめに

このドキュメントでは、ASA/PIX セキュリティ アプライアンスをバージョン 7.2(1) 以降の Point-to-Point Protocol over Ethernet（PPPoE）クライアントとして設定する例について説明します。

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに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。 ISP が PPPoE を採用するのは、顧客が簡単に利用できる点と、既存のリモートアクセス インフラストラクチャを活用して高速ブロードバンドアクセスをサポートできる点によります。

PPPoE は PPPoE ネットワーク向けの標準的な認証方式を提供します。 ISP が使用する場合は、PPPoE で IP アドレスを割り当ててから認証できます。 このタイプの実装では、PPPoE クライアントとサーバが、DSL または他のブロードバンド接続上で実行されるレイヤ 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。

- アクティブディスカバリフェーズ：このフェーズでは、PPPoE クライアントはアクセス コンセントレータと呼ばれる PPPoE サーバを探し、そこでセッション ID が割り当てられ、PPPoE レイヤが確立します。
- PPP セッション フェーズ：このフェーズでは、Point-to-Point Protocol（PPP）オプションが

ネゴシエートされ、認証処理が実行されます。 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、PPPoE ヘッダーにデータを入れて PPP リンク経由で転送できるようになります。

システム初期化時に PPPoE クライアントはセッションを確立するため、アクセス コンセントレータと一連のパケットを交換します。 セッションが確立されると Password Authentication Protocol（PAP）による認証を使用する PPP リンクがセットアップされます。 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: PPPoE は、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を設定している場合、またはマルチ コンテキスト モードやトランスペアレント モードではサポートされません。 PPPoE がサポートされるのは、フェールオーバーを設定していない、シングル モード、ルーテッド モードの場合だけです。

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 適応型セキュリティ アプライアンス（ASA）バージョン 8.x 以降に基づくものです。

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。 PPPoE クライアントを Cisco Secure PIX Firewall に設定するため、PIX OS バージョン 6.2 はこの機能を導入しており、ローエンドの PIX (501/506) をターゲットとしています。 詳細については、「Cisco Secure PIX Firewall 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

この項では、この文書で説明する機能を設定するために必要な情報を示します。

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。

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
```

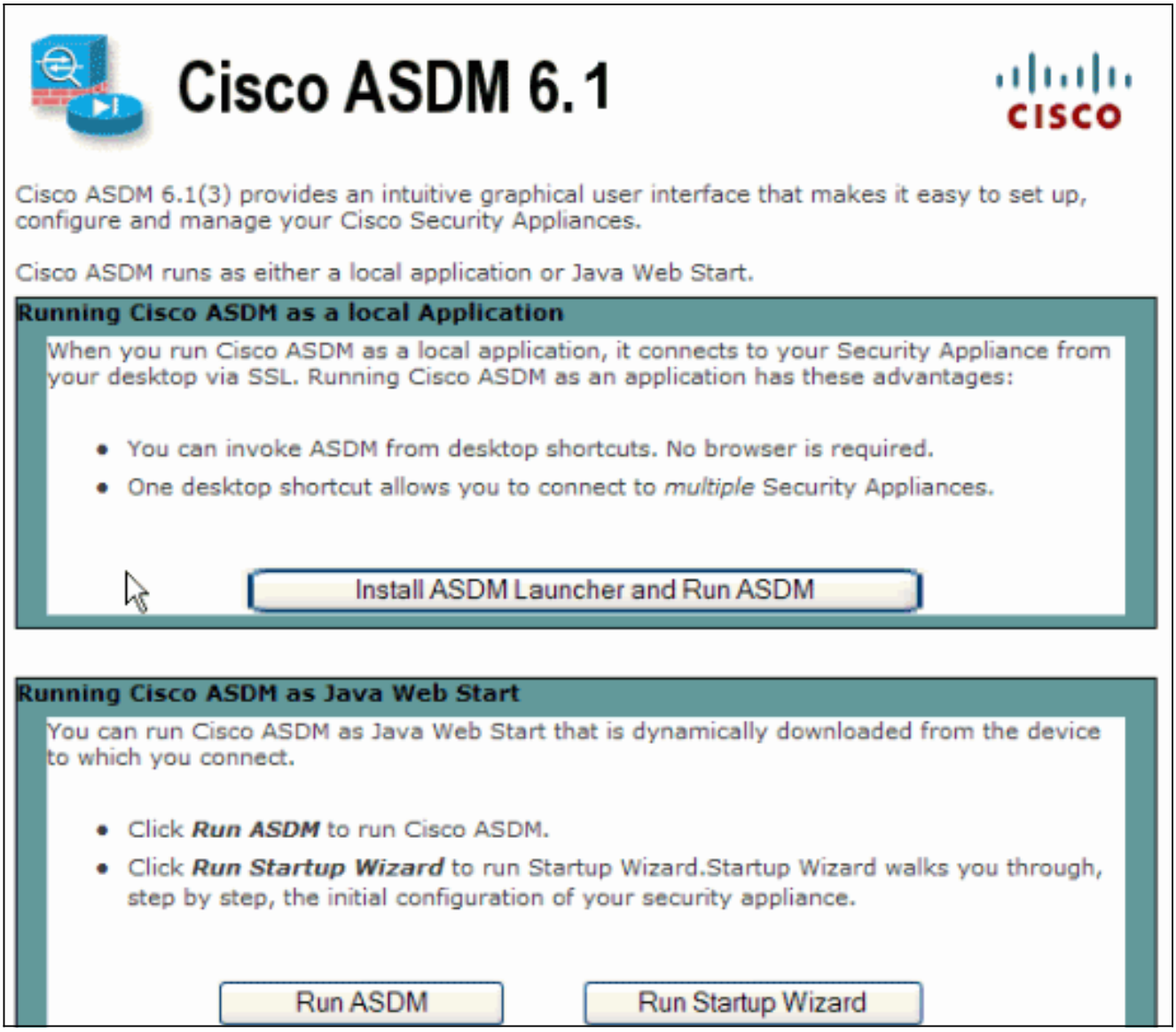
```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
username cisco123 password ffIRPGpDSOJh9YLq encrypted
privilege 15
prompt hostname context
Cryptochecksum:3cf813b751fe78474dfb1d61bb88a133
: end
ciscoasa#
```

ASDM の設定

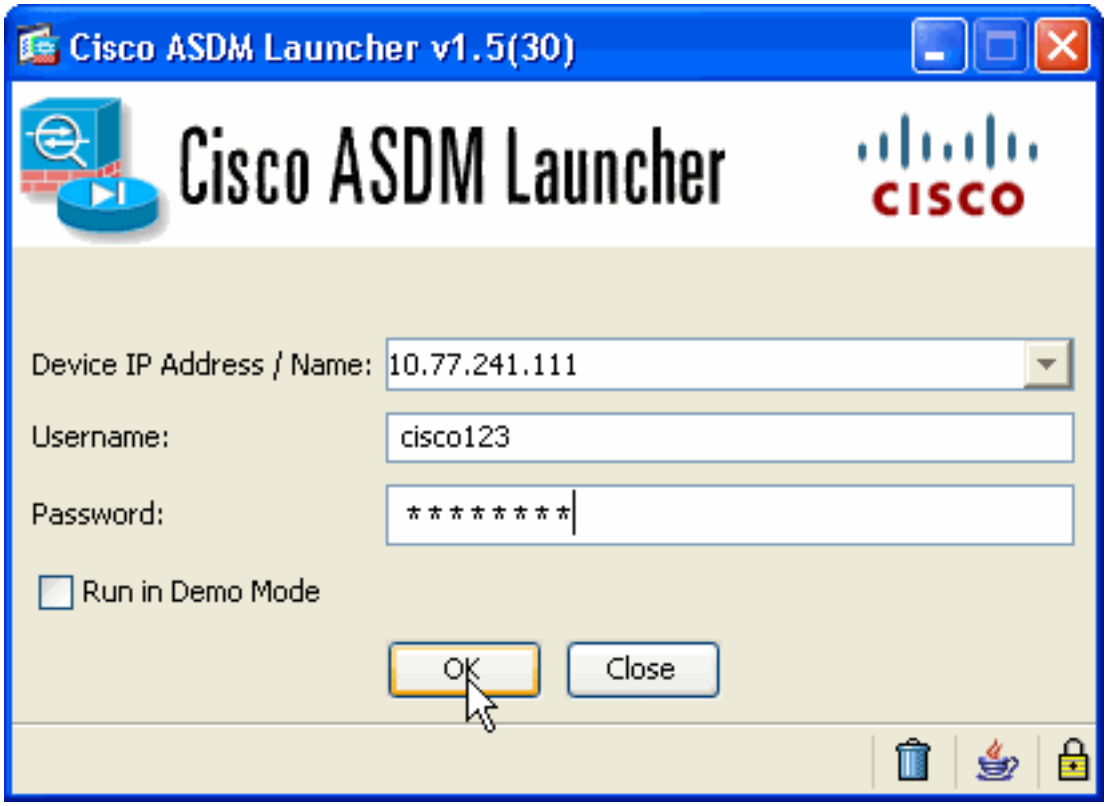
適応型セキュリティ アプライアンスの PPPoE クライアントを設定するには、次の手順を実行します。

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 で 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。*ASDM_ASA_IP_ADRESS* は ASDM アクセス用に設定された ASA インターフェイスの IP アドレスとします。**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、両方とも空白です。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。

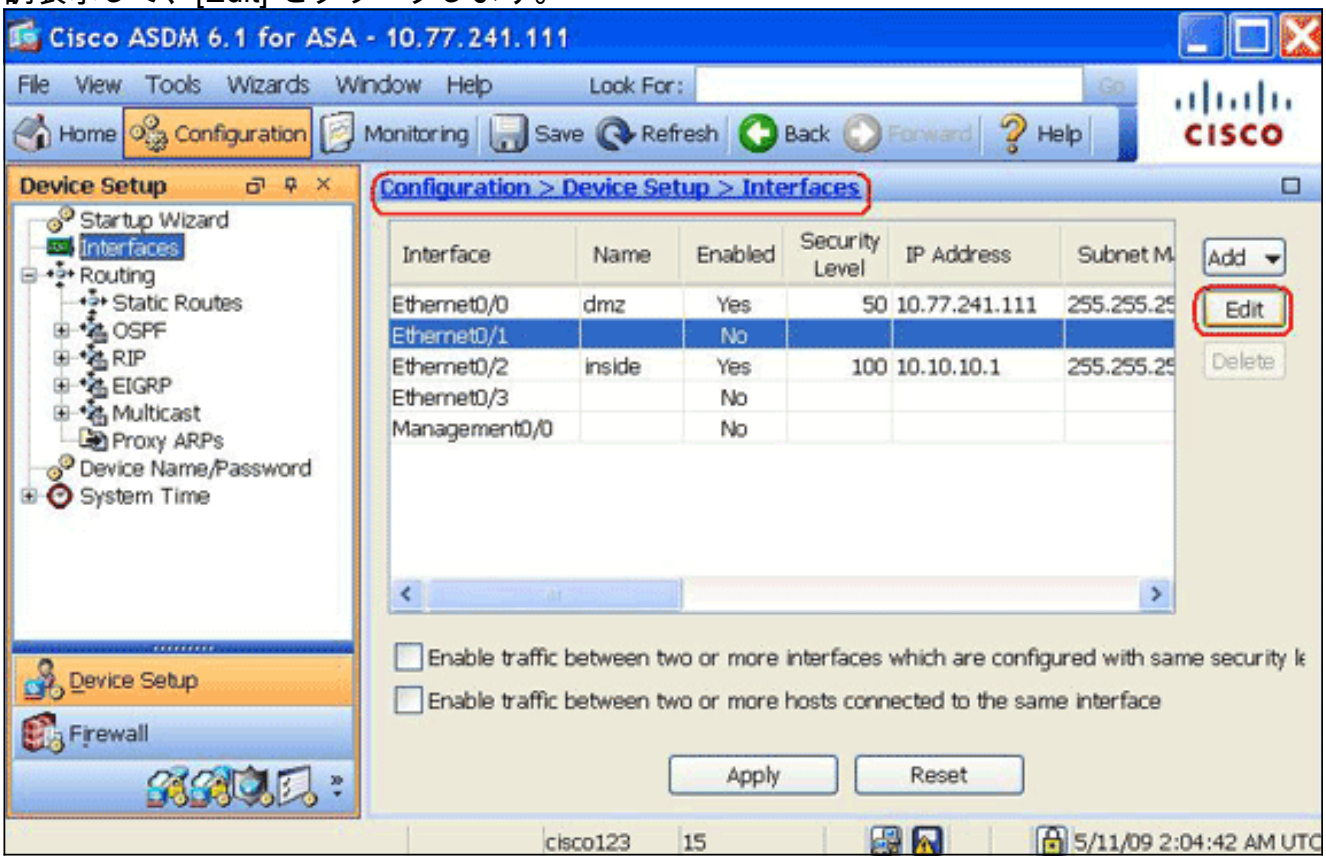


2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
4. **http -** コマンドで設定したインターフェイスの IP アドレスとユーザ名とパスワード（指定した場合）を入力します。この例では、ユーザ名を **cisco123**、パスワードを **cisco123** として

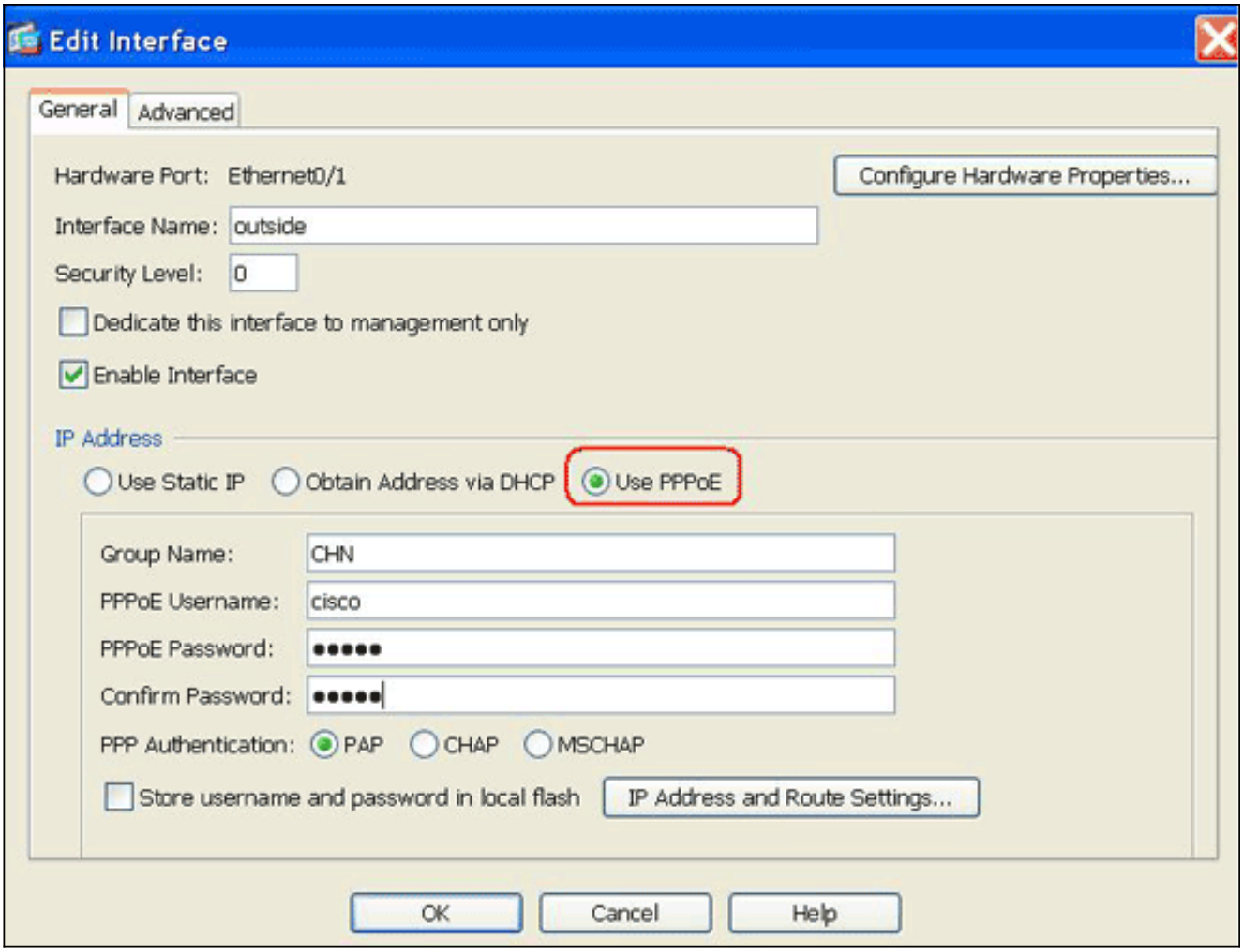


います。

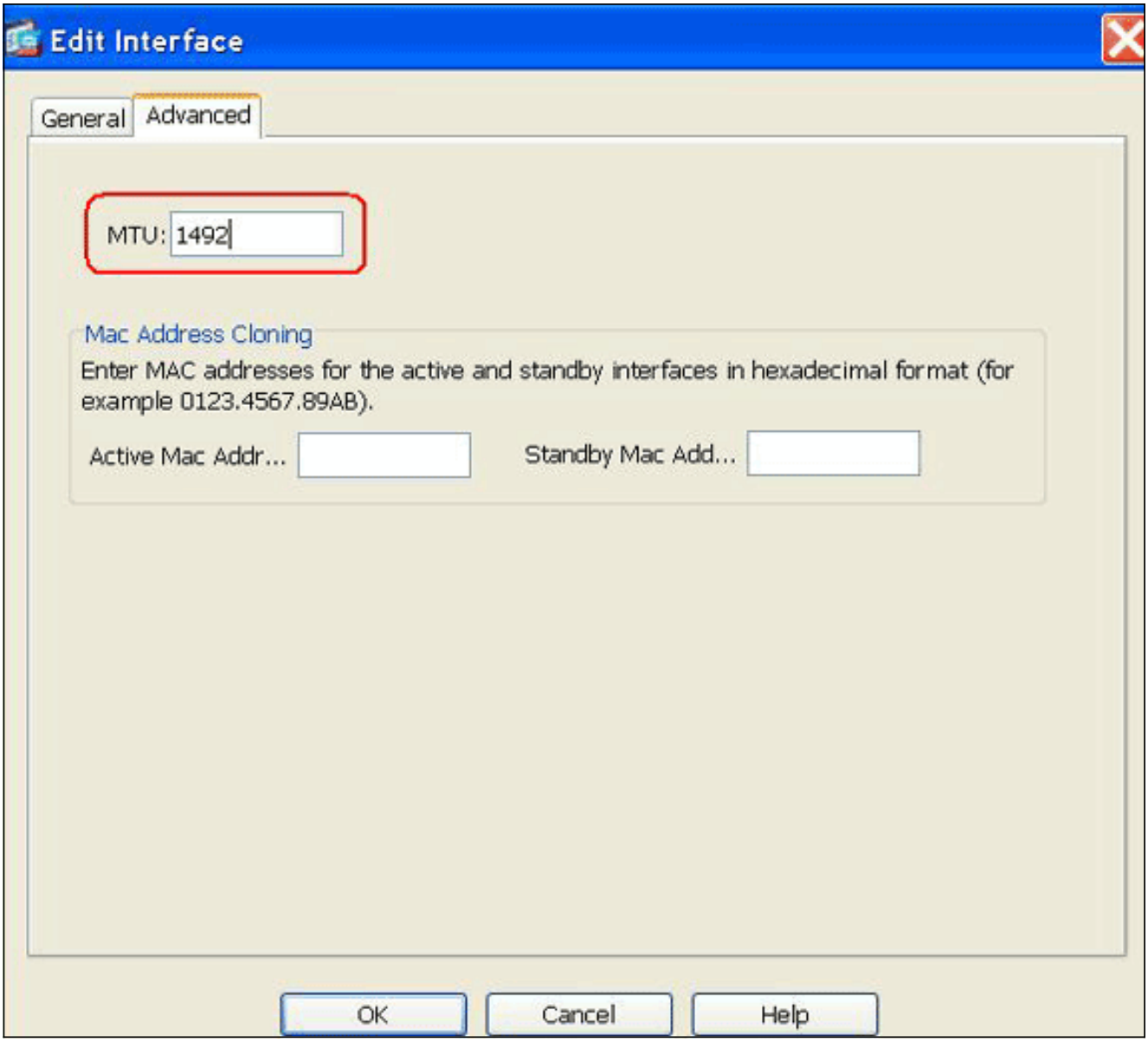
5. [Configuration] > [Device Setup] > [Interfaces] の順に選択し、outside インターフェイスを強調表示して、[Edit] をクリックします。



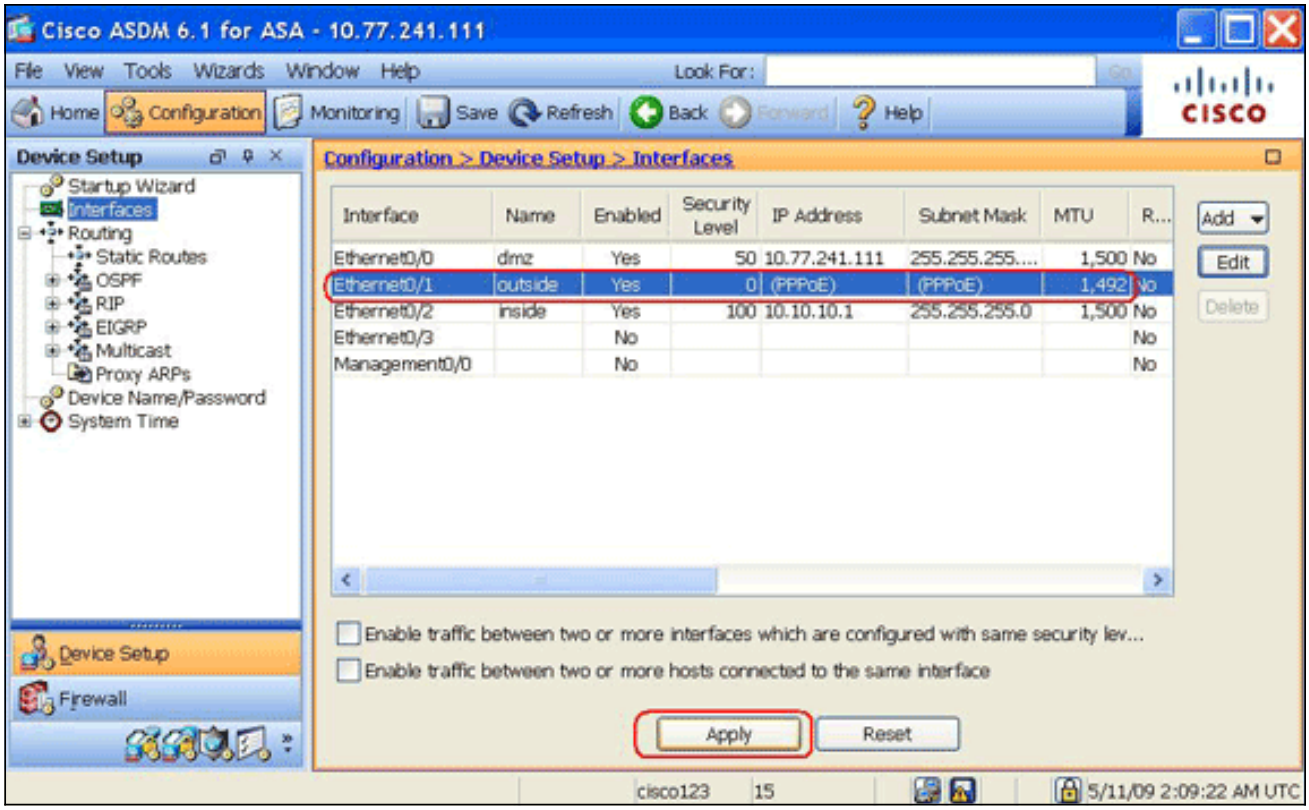
6. [Interface Name] フィールドに **outside** と入力し、[Enable Interface] チェックボックスをオンにします。
7. IP アドレスエリアの [Use PPPoE] オプション ボタンをクリックします。
8. グループ名、PPPoE ユーザ名とパスワードを入力し、適切な PPP 認証タイプ（PAP、CHAP、MSCHAP）のオプション ボタンをクリックします。



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**：最大伝送単位（MTU）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 フレーム内で PPPoE 伝送を許可する正しい値です。



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 | state | window]**：PPPoE セッションの状態を表示するには、このコマンドを使用します。

次の例は、このコマンドで提供される情報のサンプルです。

```
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#
```

設定の消去

コンフィギュレーションからすべての **vpdn group** コマンドを削除するには、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: これらのコマンドは有効になっている PPPoE 接続に影響しません。

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}**：PPPoE クライアントのデバッグを有効または無効にするには、このコマンドを使用します。

サブネットマスクが /32 と表示される

問題

IP address x.x.x.x 255.255.255.240 pppoe setroute コマンドを使用したとき、IP アドレスは正しく割り当てられますが、コマンドで /28 に指定したにもかかわらず、サブネットマスクが /32 と表示されます。 なぜ、このような現象が発生するのでしょうか。

解決策

これは正しい動作です。 PPPoE インターフェイスでは、サブネットマスクは無関係です。 ASA は常にサブネットマスクを /32 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