PIX/ASA：PPPoE客户端配置示例

Contents

Introduction

本文档针对版本 7.2.(1) 及更高版本为作为以太网上的点对点协议 (PPPoE) 客户端的 ASA/PIX 安全设备提供一个示例配置。

PPPoE 将两个广泛接受的标准（以太网和 PPP）结合，从而提供一种用于将 IP 地址分配给客户端系统的经过身份验证的方法。PPPoE 客户端通常是通过远程宽带连接（例如 DSL 或电缆服务）连接到 ISP 的个人计算机。ISP 会部署 PPPoE，因为 PPPoE 更便于客户使用且 PPPoE 使用其现有的远程访问基础架构以支持高速宽带访问。

PPPoE 提供一种采用 PPPoE 网络的身份验证方法的标准方法。ISP 使用该方法时，PPPoE 允许对 IP 地址进行经过身份验证的分配。在这种类型的实现中，PPPoE 客户端和服务器由通过 DSL 或其他宽带连接运行的第 2 层桥接协议互联。

PPPoE 由以下两个主要阶段组成：

- 活动发现阶段 — 在该阶段中，PPPoE 客户端会找到 PPPoE 服务器（称为访问集中器），在其中已分配会话 ID 且已建立 PPPoE 层
- PPP 会话阶段 — 在该阶段中，将协商点对点协议 (PPP) 选项并执行身份验证。完成链路设置后，PPPoE 会用作第 2 层封装方法，该方法允许在 PPPoE 报头中通过 PPP 链路传输数据。

在系统初始化时，PPPoE 客户端会交换一系列的数据包，从而与访问集中器建立会话。建立会话后，会设置 PPP 链路，该 PPP 链路使用口令身份验证协议 (PAP) 进行身份验证。建立 PPP 会话后，每个数据包会封装在 PPPoE 和 PPP 报头中。

Note: 在自适应安全设备上或在多上下文模式或透明模式下配置故障切换时不支持 PPPoE。仅在单一路由模式下无故障切换时支持 PPPoE。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于 Cisco 自适应安全设备 (ASA) 版本 8.x 及更高版本。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

相关产品

此配置还可用于运行版本 7.2(1) 及更高版本的 Cisco PIX 500 系列安全设备。为了在 Cisco Secure PIX 防火墙上配置 PPPoE 客户端，PIX 操作系统版本 6.2 引入此功能且目标是低端 PIX (501/506)。有关详细信息，请参阅在 Cisco Secure PIX 防火墙上配置 PPPoE 客户端

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Configure

本部分提供配置此文档中介绍的功能所需的信息。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Network Diagram

本文档使用以下网络设置：

CLI 配置

本文档使用以下配置：

设备名称 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
```

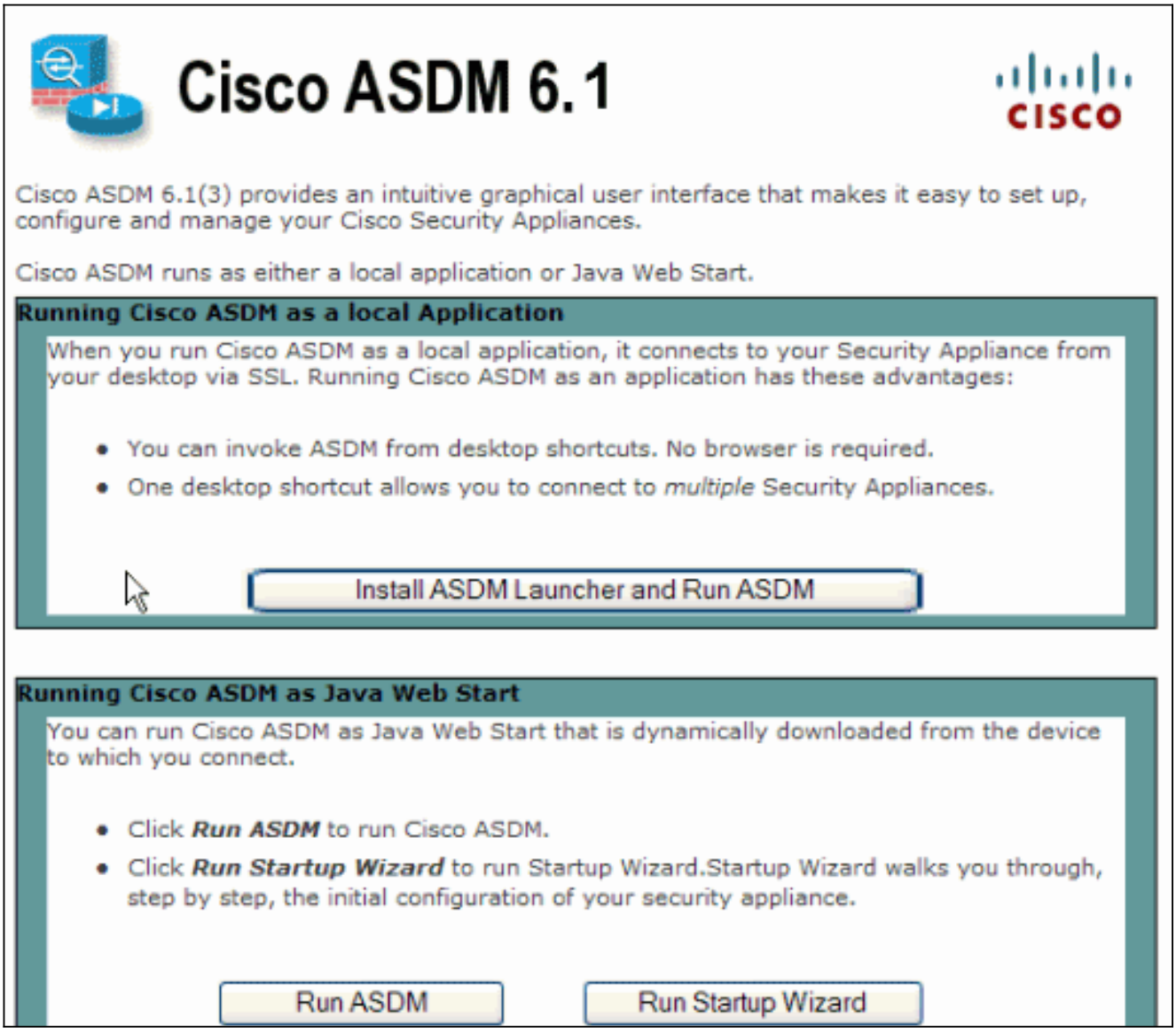
```
mtu dmz 1500
!--- The maximum transmission unit (MTU) size is
automatically set to 1492 bytes, !--- which is the
correct value to allow PPPoE transmission within an
Ethernet frame. mtu outside 1492
mtu inside 1500

!--- 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 配置

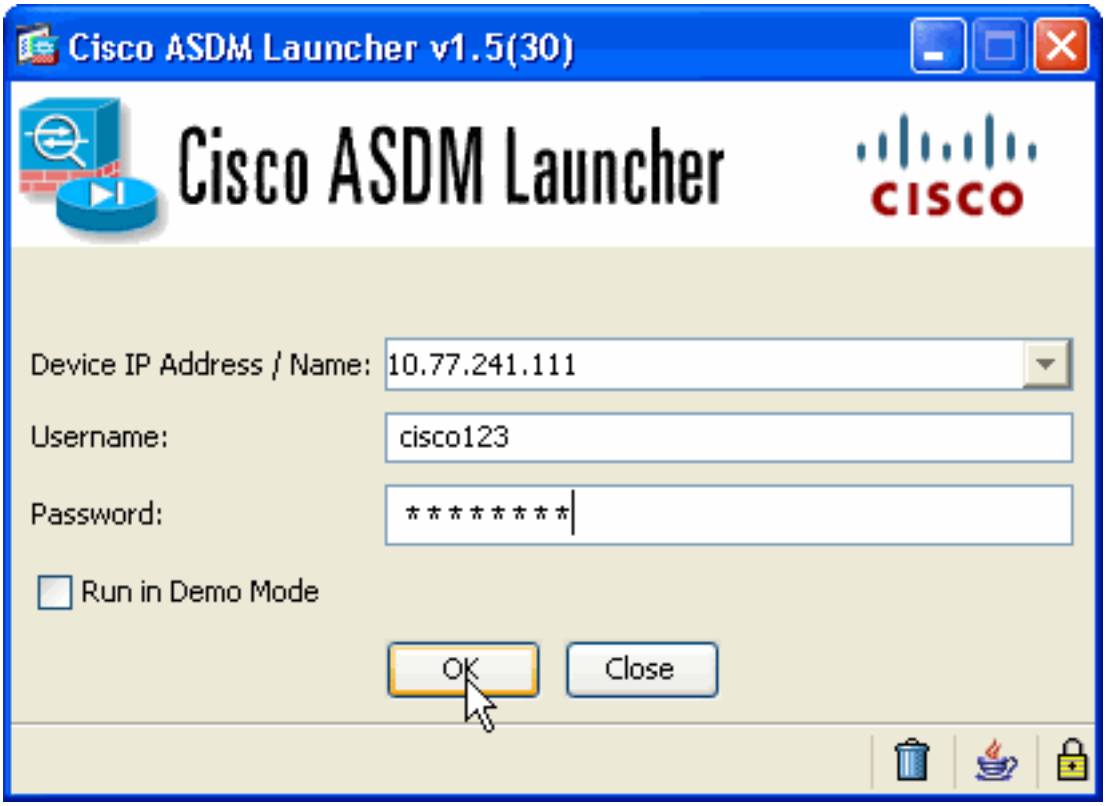
完成下列步骤以配置与自适应安全设备一起提供的 PPPoE 客户端：

Note: 要使 ASDM 可配置 ASA，请参阅允许 ASDM 进行 HTTPS 访问。

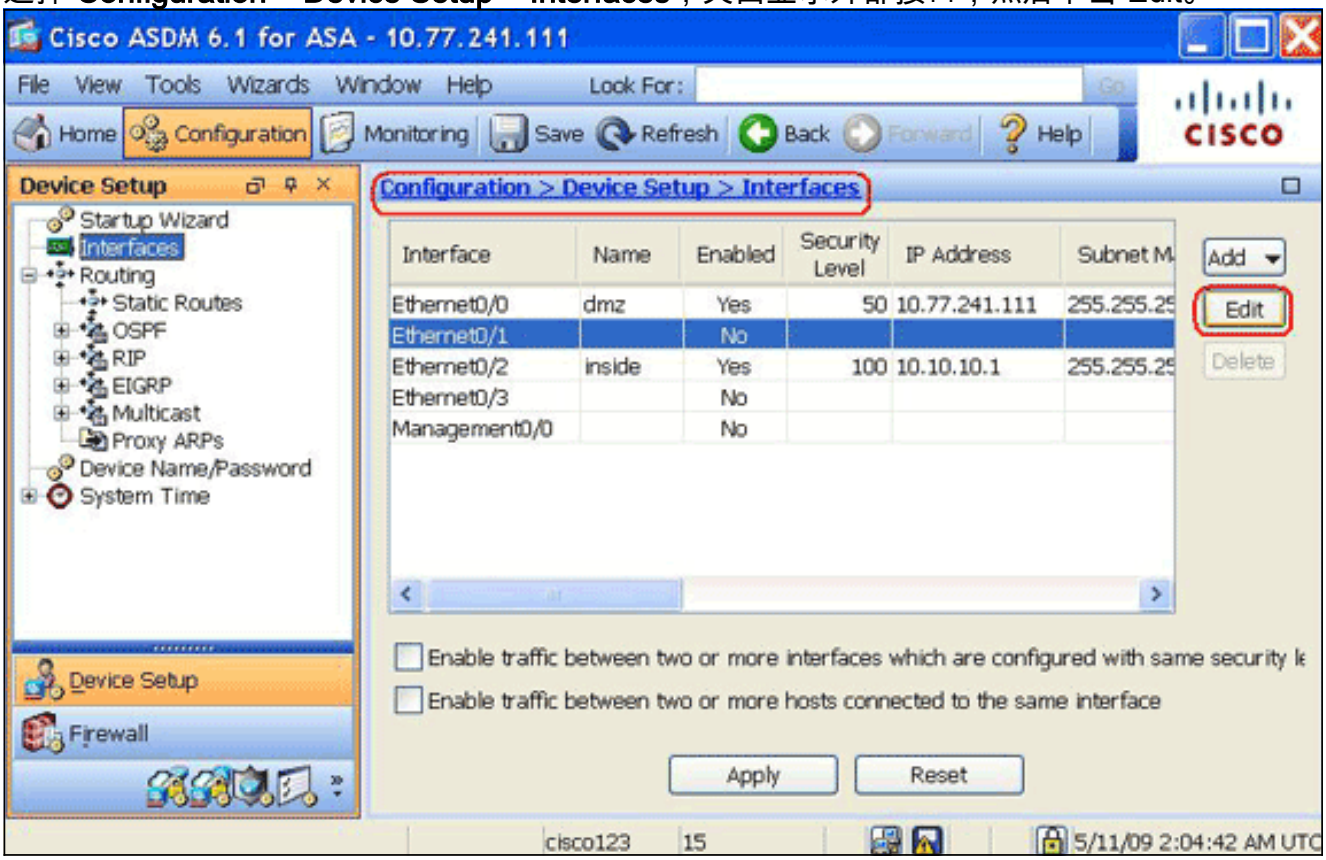
1. 访问 ASA 上的 ASDM：打开浏览器，然后输入 **https://<ASDM_ASA_IP_ADDRESS>**。其中 *ASDM_ASA_IP_ADRESS* 为配置进行 ASDM 访问的 ASA 接口的 IP 地址。**Note:** 确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空白。ASA 显示此窗口以允许下载 ASDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。



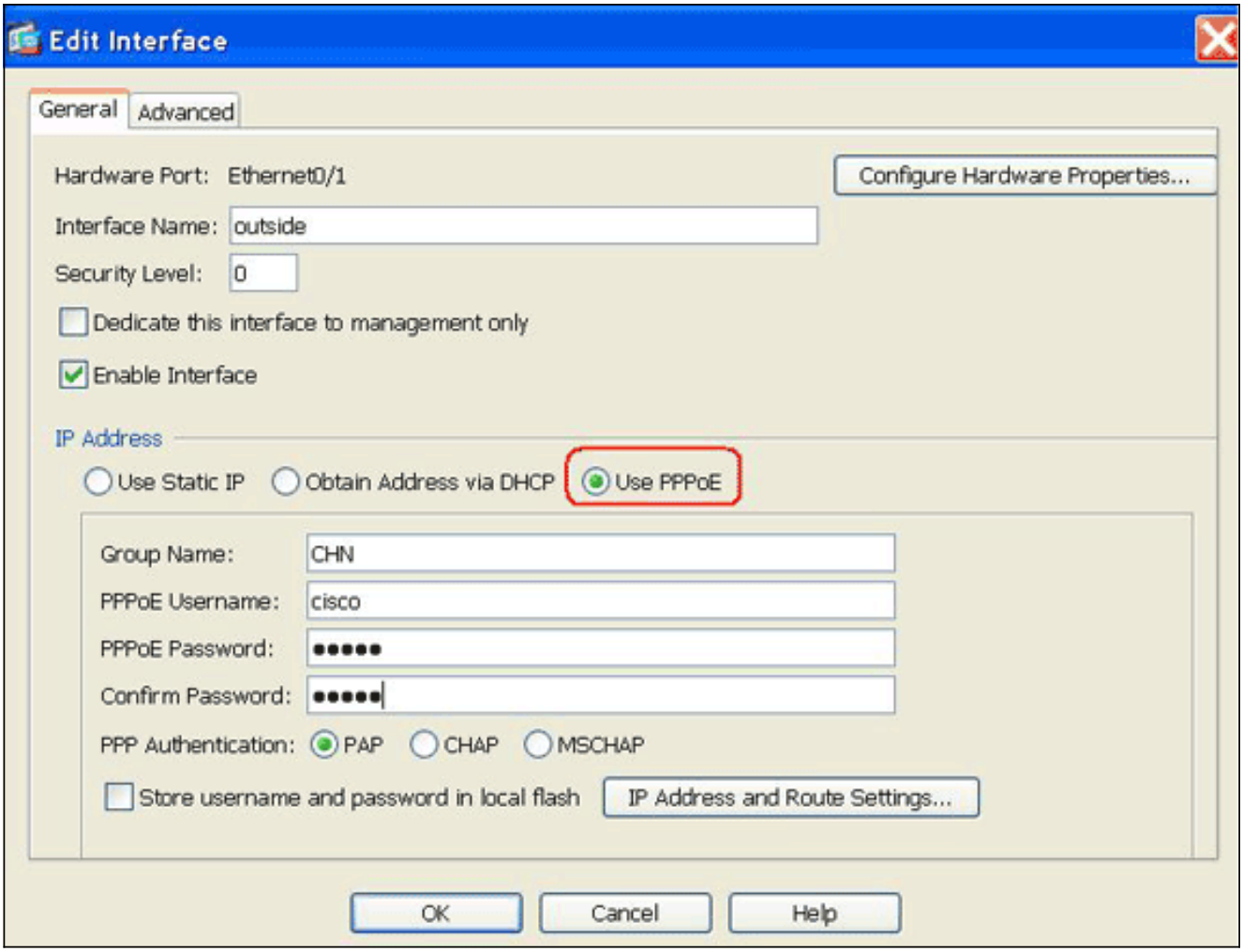
2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序后，完成提示所指示的步骤，以便安装该软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http -** 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。此示例将 **cisco123** 用于用户名并使用 cisco123 作为口令。



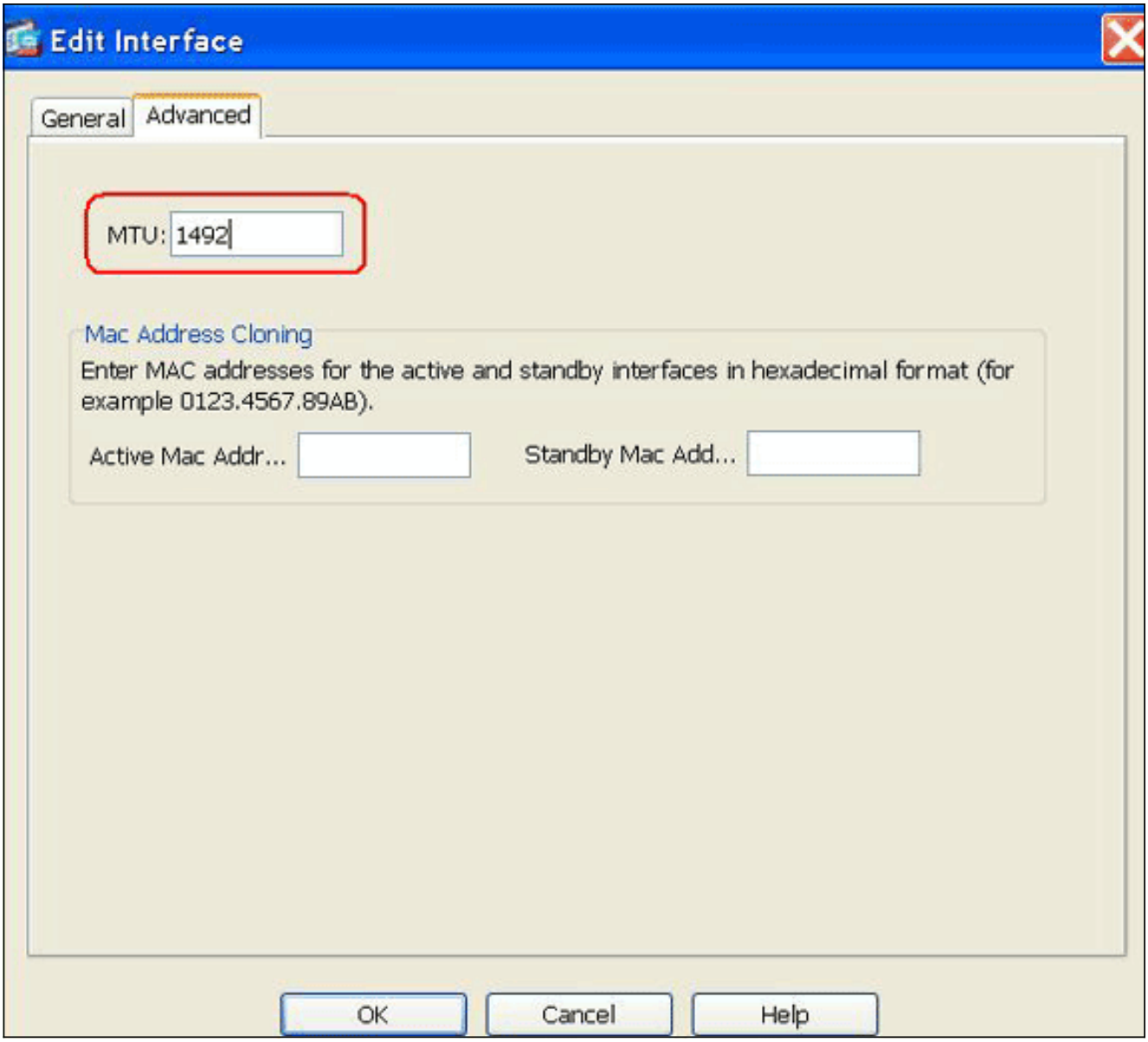
5. 选择 **Configuration > Device Setup > Interfaces**，突出显示外部接口，然后单击 Edit。



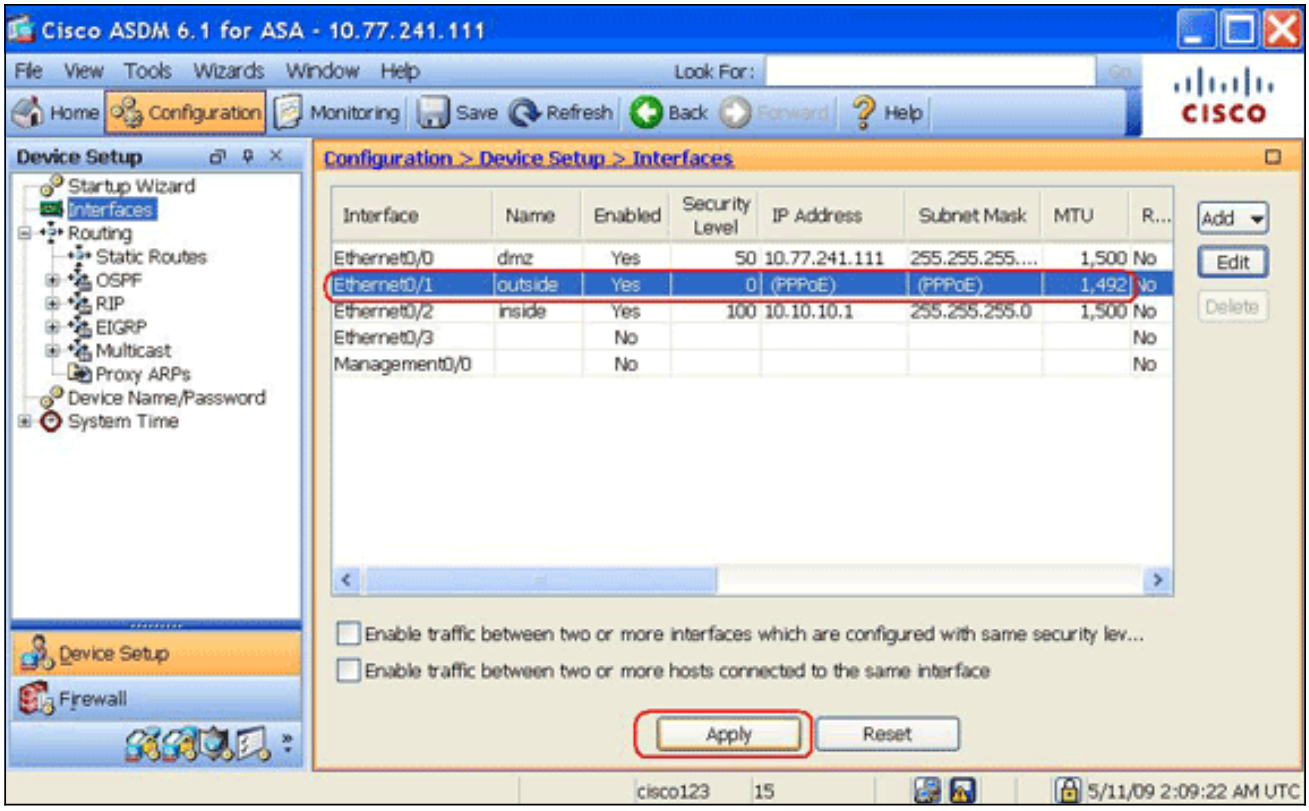
6. 在 Interface Name 字段中，输入 **outside**，然后选中 Enable Interface 复选框。
7. 在 IP Address 区域中单击 **Use PPPoE** 单选按钮。
8. 输入组名称、PPPoE 用户名和口令，然后单击相应的 PPP 身份验证类型（PAP、 CHAP 或 MSCHAP）单选按钮。



9. 单击 **Advanced** 选项卡，并验证 MTU 大小是否设置为 1492。**Note:** 最大传输单元 (MTU) 大小会自动设置为 1492 字节，这是正确值，以允许在以太网帧内进行 PPPoE 传输。



10. 点击OK键继续。
11. 验证输入的信息是否正确，然后单击 **Apply**。



Verify

Use this section to confirm that your configuration works properly.

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ip address outside pppoe** — 使用此命令以显示当前 PPPoE 客户端配置信息。
- **show vpdn session [l2tp|pppoe] [id sess_id|信息包|状态|window]** — 使用此命令以查看 PPPoE 会话的状态。

下面的示例显示此命令提供的信息示例：

```
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#
```

清除配置

为了从配置中删除所有 **vpdn group** 命令，请在全局配置模式下使用 clear configure vpdn group 命令：

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

为了删除所有 **vpdn username** 命令，请使用 clear configure vpdn username 命令：

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

Note: 这些命令对活动 PPPoE 连接没有任何影响。

Troubleshoot

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

Note: 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **hostname# [no] debug pppoe {event|错误|packet}** — 使用此命令以对 PPPoE 客户端启用或禁用调试。

子网掩码出现作为/32

问题

当您使用**IP地址x.x.x.x 255.255.255.240 pppoe setroute命令时**， IP地址正确地分配，但是子网掩码出现作为/32，虽然在命令指定作为/28。为什么会发生这种情况？

解决方案

这是正确行为。子网掩码是毫不相关的一旦PPPoe接口;ASA永远将更改它到/32。

Related Information

- Cisco ASA 5500 系列自适应安全设备
- 在 Cisco 2600 上配置 PPPoE 客户端以连接到非 Cisco DSL CPE
- Cisco 自适应安全设备管理器
- Technical Support & Documentation - Cisco Systems