# PIX/ASA: PPPoE-Client-Konfigurationsbeispiel

## Inhalt



## Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die ASA/PIX Security Appliance als Point-to-Point Protocol over Ethernet (PPPoE)-Client für Version 7.2.(1) und höher.

PPPoE kombiniert zwei weit verbreitete Standards, Ethernet und PPP, um eine authentifizierte Methode bereitzustellen, die Client-Systemen IP-Adressen zuweist. PPPoE-Clients sind in der Regel PCs, die über eine Remote-Breitbandverbindung, z. B. DSL oder Kabeldienst, mit einem ISP verbunden sind. ISPs stellen PPPoE bereit, da die Nutzung für Kunden einfacher ist und die vorhandene Infrastruktur für den Remote-Zugriff zur Unterstützung des Hochgeschwindigkeits-Breitbandzugangs genutzt wird.

PPPoE bietet eine Standardmethode zur Verwendung der Authentifizierungsmethoden des PPPoE-Netzwerks. Bei Verwendung durch ISPs ermöglicht PPPoE die authentifizierte Zuweisung von IP-Adressen. Bei dieser Art der Implementierung sind der PPPoE-Client und der Server über Layer 2-Bridging-Protokolle verbunden, die über eine DSL- oder andere Breitbandverbindung ausgeführt werden.

PPPoE besteht aus zwei Hauptphasen:

- Aktive Erkennungsphase - In dieser Phase sucht der PPPoE-Client einen PPPoE-Server, den so genannten Zugriffskonzentrator, auf dem eine Session-ID zugewiesen wird und die PPPoE-Ebene eingerichtet ist.

- PPP-Sitzungsphase - In dieser Phase werden Point-to-Point Protocol (PPP)-Optionen ausgehandelt und eine Authentifizierung durchgeführt. Nach Abschluss der Verbindungseinrichtung fungiert PPPoE als Layer-2-Kapselungsmethode, mit der Daten über die PPP-Verbindung in PPPoE-Headern übertragen werden können.

Bei der Systeminitialisierung tauscht der PPPoE-Client eine Reihe von Paketen aus, um eine Sitzung mit dem Zugriffskonzentrator einzurichten. Nach Einrichtung der Sitzung wird eine PPP-Verbindung eingerichtet, die das Password Authentication Protocol (PAP) für die Authentifizierung verwendet. Nach Einrichtung der PPP-Sitzung wird jedes Paket in die PPPoE- und PPP-Header gekapselt.

**Hinweis:** PPPoE wird nicht unterstützt, wenn Failover auf der Adaptive Security Appliance oder im Multiple Context- oder Transparent-Modus konfiguriert wird. PPPoE wird nur im gerouteten Einzelmodus ohne Failover unterstützt.

# Voraussetzungen

## Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA) Version 8.x und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Security Appliance der Serie PIX 500 verwendet werden, die Version 7.2(1) und höher ausführt. Um den PPPoE-Client auf der Cisco Secure PIX Firewall zu konfigurieren, führt PIX OS 6.2 diese Funktion ein und ist für den Low-End-PIX (501/506) ausgelegt. Weitere Informationen finden Sie unter Konfigurieren des PPPoE-Clients auf einer Cisco Secure PIX Firewall.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Konfigurieren

Dieser Abschnitt enthält die erforderlichen Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:


## CLI-Konfiguration

In diesem Dokument werden folgende Konfigurationen verwendet:

**Gerätename 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
```

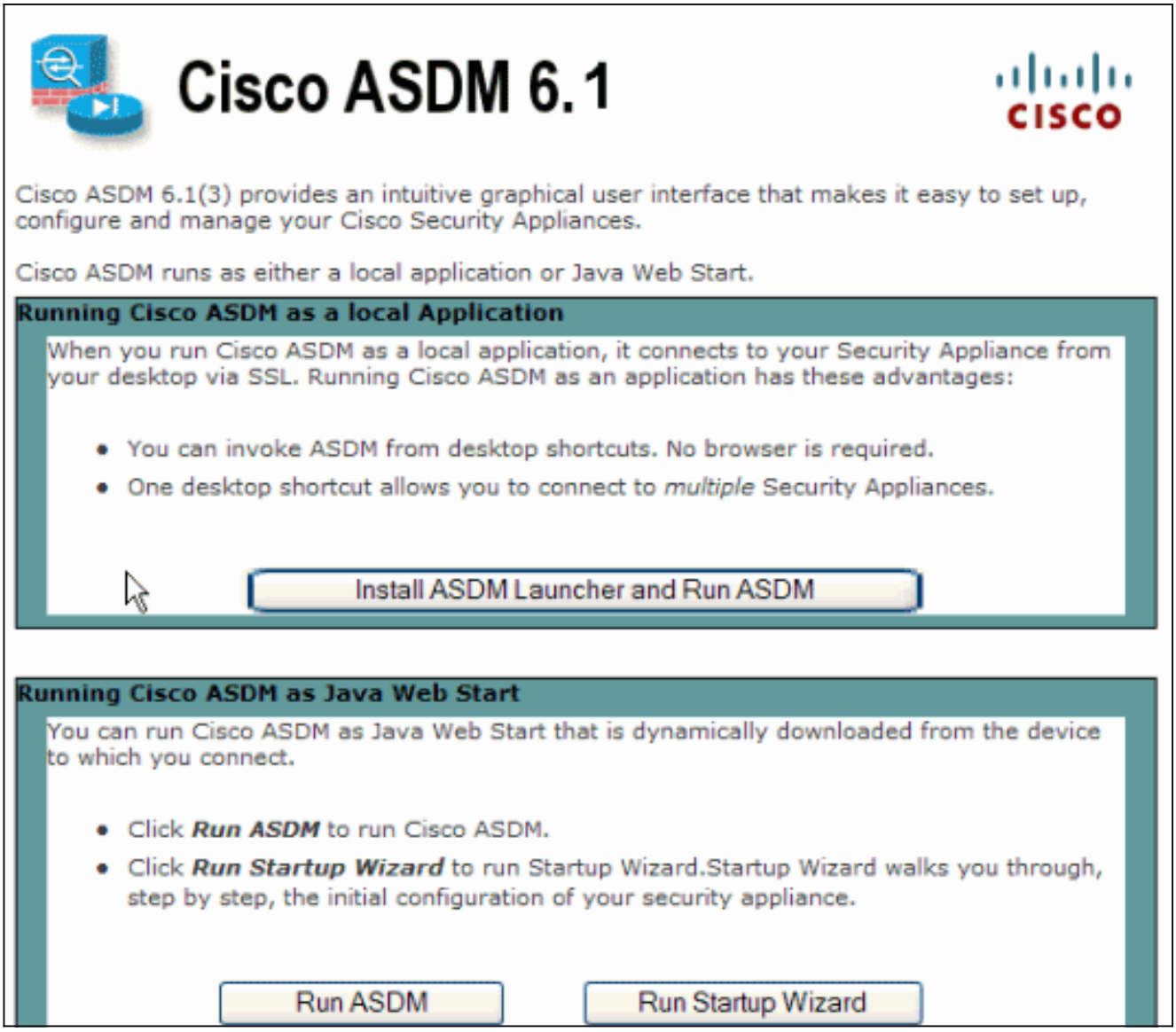
```
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
username cisco123 password ffIRPGpDSOJh9YLq encrypted
privilege 15
prompt hostname context
Cryptochecksum:3cf813b751fe78474dfb1d61bb88a133
: end
ciscoasa#
```

## ASDM-Konfiguration

Gehen Sie wie folgt vor, um den mit der Adaptive Security Appliance gelieferten PPPoE-Client zu konfigurieren:

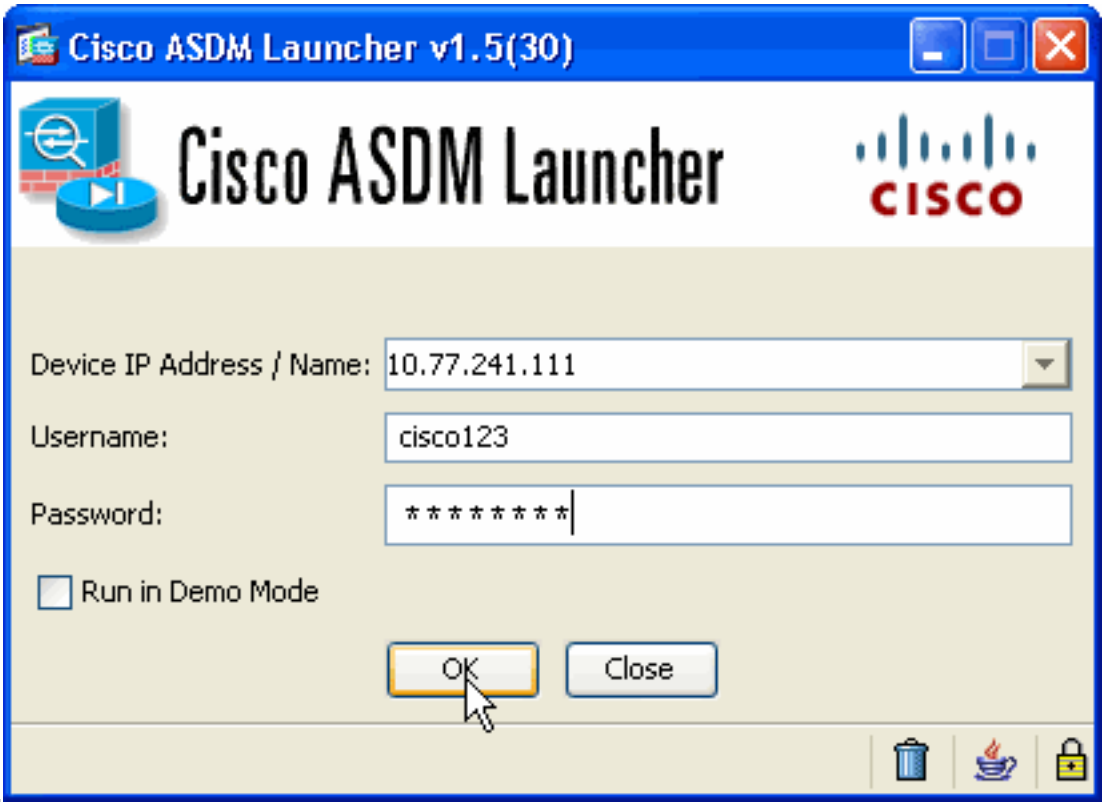
**Hinweis:** Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

1. Zugriff auf das ASDM auf der ASA:Öffnen Sie Ihren Browser, und geben Sie **https://<*ASDM_ASA_IP_ADDRESS*>** ein.Dabei ist *ASDM_ASA_IP_ADRESSE* die IP-Adresse der ASA-Schnittstelle, die für den ASDM-Zugriff konfiguriert ist.**Hinweis:** Achten Sie darauf, alle Warnungen zu autorisieren, die Ihr Browser bezüglich der Authentizität von SSL-Zertifikaten ausgibt. Standardmäßig sind Benutzername und Kennwort leer.Die ASA zeigt dieses Fenster an, um den Download der ASDM-Anwendung zu ermöglichen. In diesem Beispiel wird die Anwendung auf den lokalen Computer geladen und nicht in einem Java-Applet
   ausgeführt.

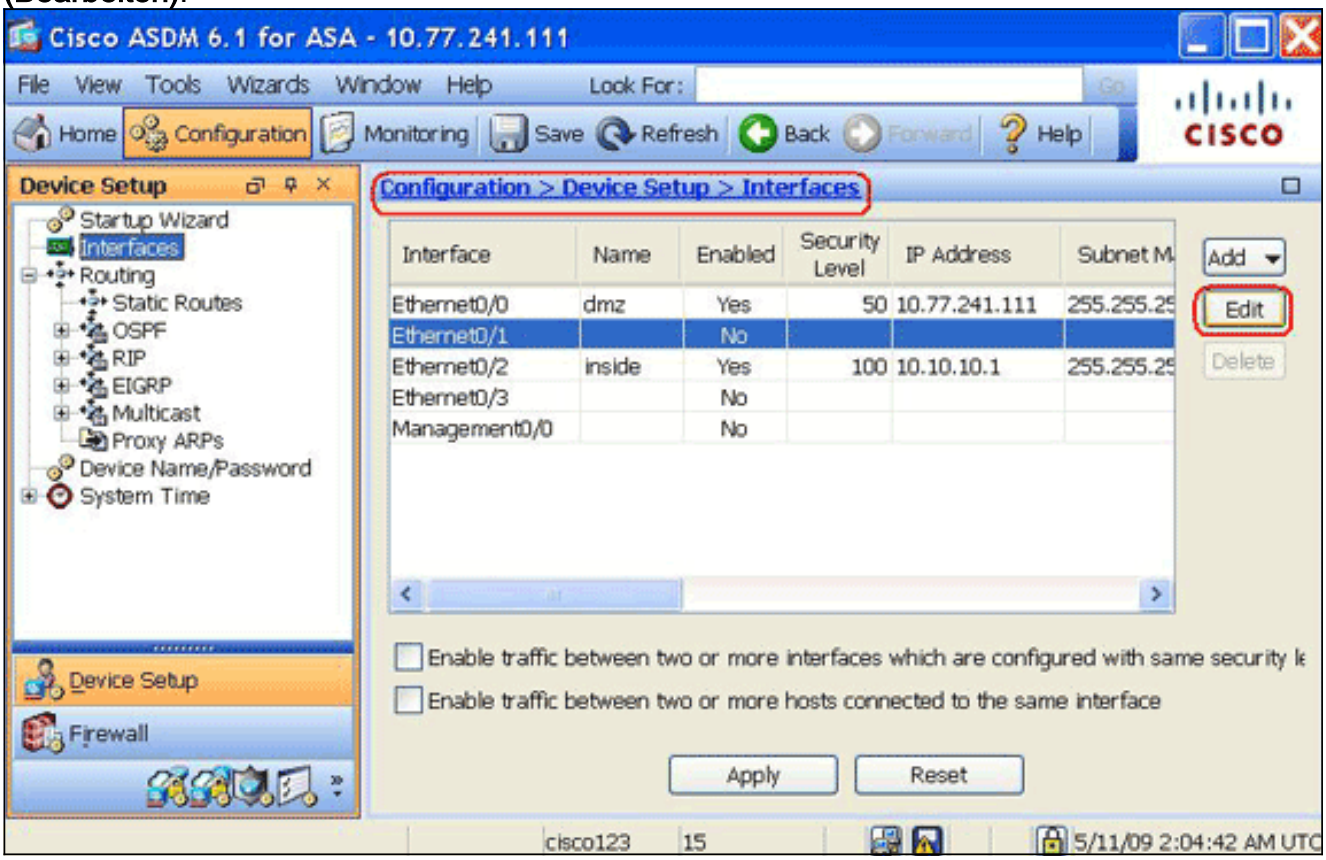



2. Klicken Sie auf **ASDM Launcher herunterladen und ASDM starten**, um das Installationsprogramm für die ASDM-Anwendung herunterzuladen.
3. Wenn der ASDM Launcher heruntergeladen wurde, führen Sie die Schritte aus, die von den Aufforderungen zur Installation der Software geleitet werden, und führen Sie den Cisco ASDM Launcher aus.
4. Geben Sie die IP-Adresse für die Schnittstelle ein, die Sie mit dem Befehl **http** konfiguriert haben, sowie einen Benutzernamen und ein Kennwort, wenn Sie einen Befehl angegeben haben.In diesem Beispiel wird **cisco123** als Benutzername und **cisco123** als Kennwort

verwendet.

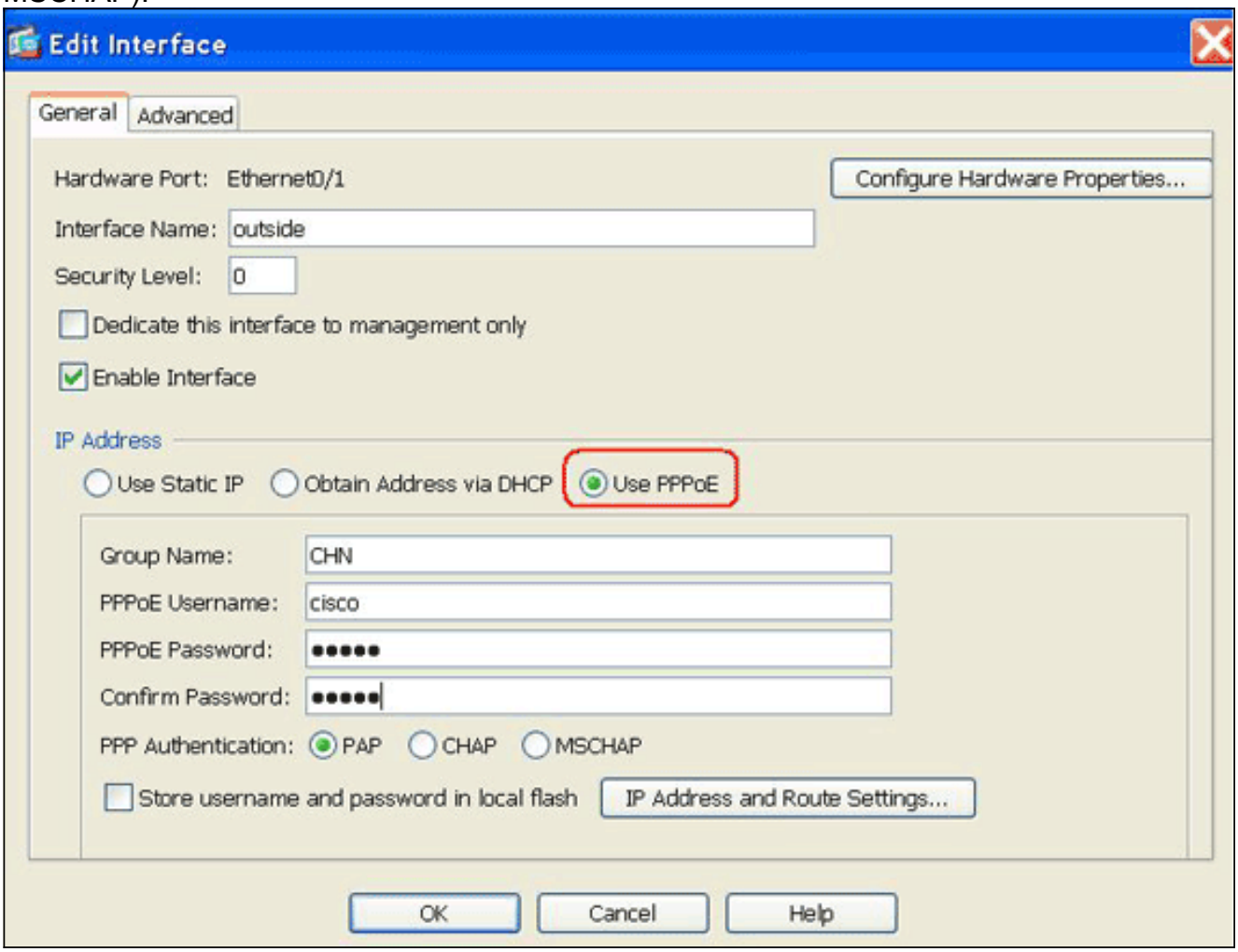



5. Wählen Sie **Configuration > Device Setup > Interfaces (Konfiguration > Geräteeinrichtung > Schnittstellen) aus**, markieren Sie die externe Schnittstelle, und klicken Sie auf **Edit (Bearbeiten)**.

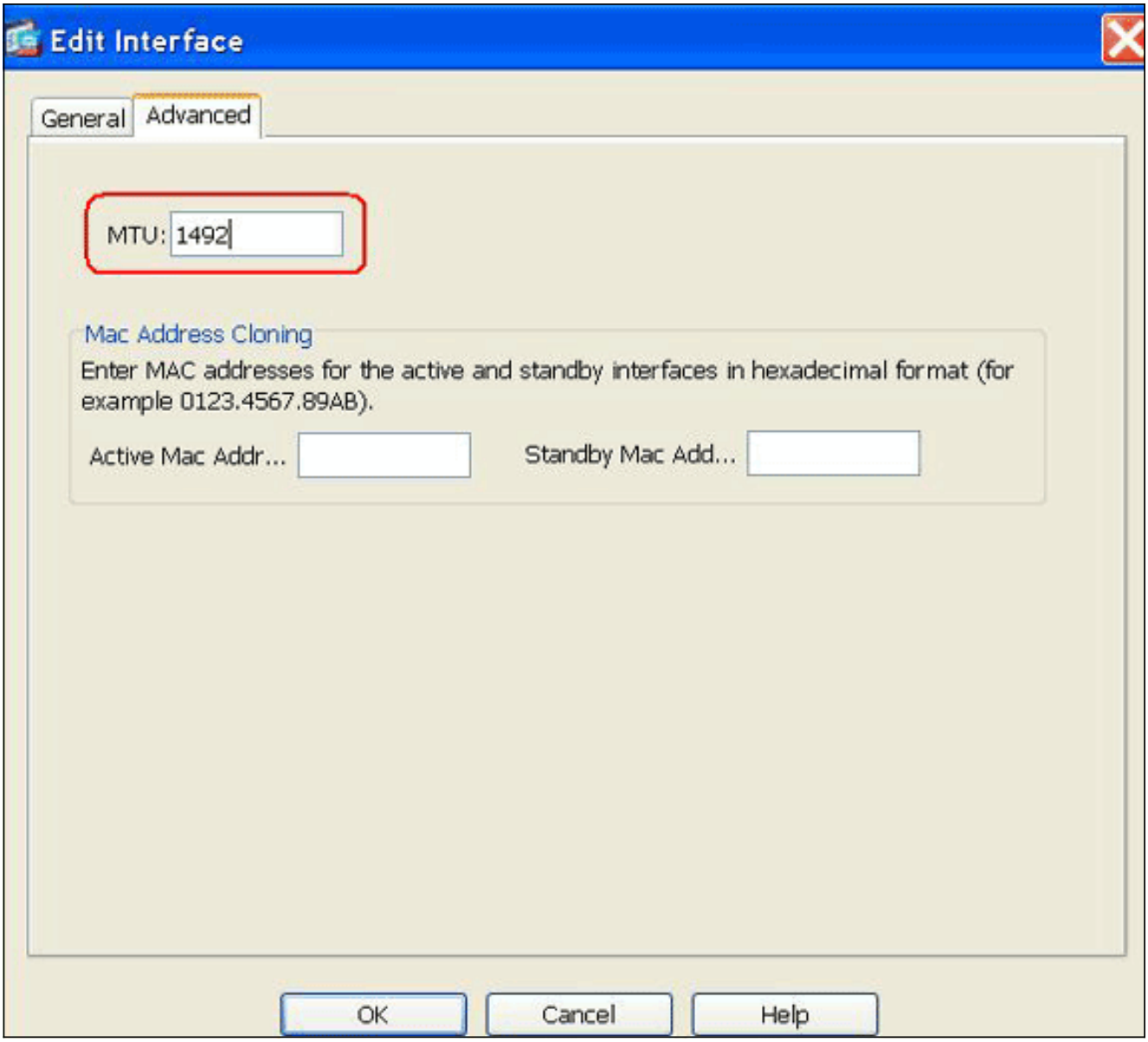



6. Geben Sie im Feld Interface Name (Schnittstellenname) **einen externen Namen ein**, und aktivieren Sie das Kontrollkästchen **Enable Interface (Schnittstelle aktivieren)**.
7. Klicken Sie im Bereich IP-Adresse auf das Optionsfeld **PPPoE verwenden**.
8. Geben Sie einen Gruppennamen, einen PPPoE-Benutzernamen und ein Kennwort ein, und klicken Sie auf das Optionsfeld für den entsprechenden PPP-Authentifizierungstyp (PAP, CHAP oder

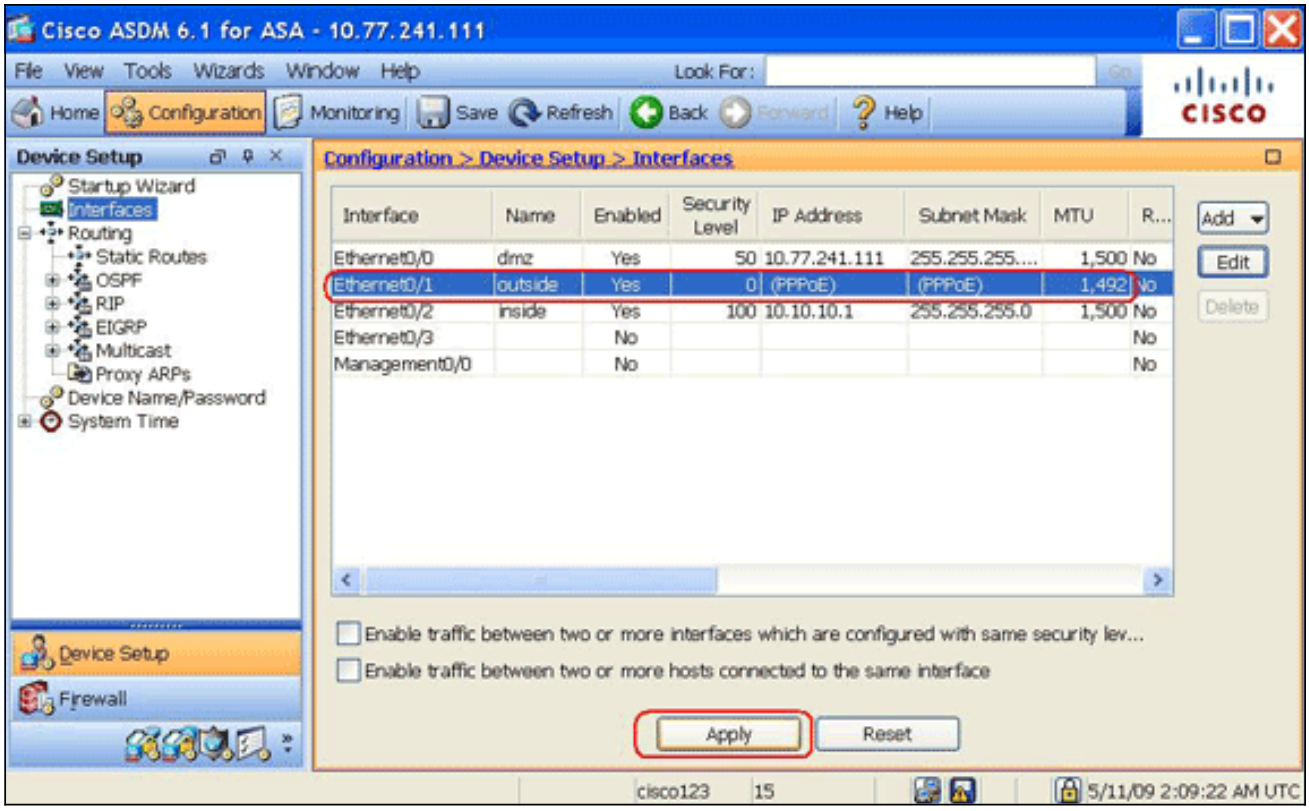
MSCHAP).




9. Klicken Sie auf die Registerkarte **Erweitert**, und überprüfen Sie, ob die MTU-Größe auf **1492** festgelegt ist.**Hinweis:** Die MTU-Größe (Maximum Transmission Unit) wird automatisch auf 1492 Byte festgelegt. Dies ist der richtige Wert für die PPPoE-Übertragung innerhalb eines Ethernet-
Frames.




10. Klicken Sie auf **OK**, um fortzufahren.
11. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Übernehmen**.




# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show ip address outside pppoe** - Verwenden Sie diesen Befehl, um die aktuellen PPPoE-Client-Konfigurationsinformationen anzuzeigen.
- **show vpdn session [l2tp | pppoe [id sess_id] | Pakete | Status | window]** - Verwenden Sie diesen Befehl, um den Status von PPPoE-Sitzungen anzuzeigen.

Das folgende Beispiel zeigt ein Beispiel für Informationen, die durch diesen Befehl bereitgestellt werden:

```
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#
```

# Löschen der Konfiguration

Um alle Befehle der **vpdn-Gruppe** aus der Konfiguration zu entfernen, verwenden Sie den Befehl clear configure vpdn group im globalen Konfigurationsmodus:

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

Um alle Befehle für **vpdn-Benutzernamen** zu entfernen, verwenden Sie den Befehl clear configure vpdn username:

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

**Hinweis:** Diese Befehle wirken sich nicht auf aktive PPPoE-Verbindungen aus.

# Fehlerbehebung

## Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

**Hinweis:** Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **hostname# [no] debug pppoe {event | Fehler | Packet}** - Verwenden Sie diesen Befehl, um das Debuggen für den PPPoE-Client zu aktivieren oder zu deaktivieren.

## Subnetzmaske wird als /32 angezeigt

### Problem

Wenn Sie den Befehl **IP address x.x.x.x 255.255.255.240 pppoe setroute** verwenden, wird die IP-Adresse korrekt zugewiesen, aber die Subnetzmaske wird als /32 angezeigt, obwohl sie im Befehl als /28 angegeben ist. Warum geschieht das?

### Lösung

Das ist das richtige Verhalten. Die Subnetzmaske ist für die PPPone-Schnittstelle irrelevant. die ASA ändert sie immer auf /32.

## Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Konfigurieren des PPPoE-Clients auf dem Cisco 2600 für eine Verbindung zu einem nicht von Cisco stammenden DSL CPE
- Cisco Adaptive Security Device Manager
- Technischer Support und Dokumentation - Cisco Systems