PIX/ASA Esempio di configurazione del client PPPoE

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per l'appliance di sicurezza ASA/PIX come client PPPoE (Point-to-Point Protocol over Ethernet) per le versioni 7.2.2(1) e successive.

PPPoE combina due standard ampiamente accettati, Ethernet e PPP, per fornire un metodo autenticato che assegna indirizzi IP ai sistemi client. I client PPPoE sono in genere personal computer connessi a un ISP tramite una connessione a banda larga remota, ad esempio DSL o un servizio via cavo. Gli ISP implementano il protocollo PPPoE perché è più facile da utilizzare per i clienti e utilizza l'infrastruttura di accesso remoto esistente per supportare l'accesso a banda larga ad alta velocità.

PPPoE fornisce un metodo standard per utilizzare i metodi di autenticazione della rete PPPoE. Se utilizzato dagli ISP, il protocollo PPPoE consente l'assegnazione autenticata di indirizzi IP. In questo tipo di implementazione, il client e il server PPPoE sono interconnessi da protocolli di bridging di layer 2 eseguiti su una connessione DSL o altra connessione a banda larga.

Il PPPoE è costituito da due fasi principali:

- Fase di rilevamento attivo: in questa fase, il client PPPoE individua un server PPPoE,

denominato concentratore di accesso, in cui viene assegnato un ID sessione e viene stabilito il livello PPPoE
- Fase di sessione PPP: in questa fase, le opzioni PPP (Point-to-Point Protocol) vengono negoziate e viene eseguita l'autenticazione. Al termine dell'impostazione del collegamento, il protocollo PPPoE funziona come metodo di incapsulamento di layer 2, che consente il trasferimento dei dati sul collegamento PPP all'interno delle intestazioni PPPoE.

Al momento dell'inizializzazione del sistema, il client PPPoE scambia una serie di pacchetti per stabilire una sessione con il concentratore di accesso. Una volta stabilita la sessione, viene impostato un collegamento PPP che utilizza il protocollo PAP (Password Authentication Protocol) per l'autenticazione. Una volta stabilita la sessione PPP, ogni pacchetto viene incapsulato nelle intestazioni PPPoE e PPP.

Nota: il protocollo PPPoE non è supportato quando il failover è configurato sull'appliance Adaptive Security o in modalità contesto multiplo o trasparente. Il protocollo PPPoE è supportato solo in modalità di routing singolo, senza failover.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata la versione 8.x di Cisco Adaptive Security Appliance (ASA) e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance, con versione 7.2(1) e successive. Per configurare il client PPPoE su Cisco Secure PIX Firewall, PIX OS versione 6.2 introduce questa funzione ed è destinato ai PIX di fascia bassa (501/506). Per ulteriori informazioni, consultare il documento sulla configurazione del client PPPoE su un firewall Cisco Secure PIX

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità

descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Configurazione CLI

Nel documento vengono usate queste configurazioni:

Nome dispositivo 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
```

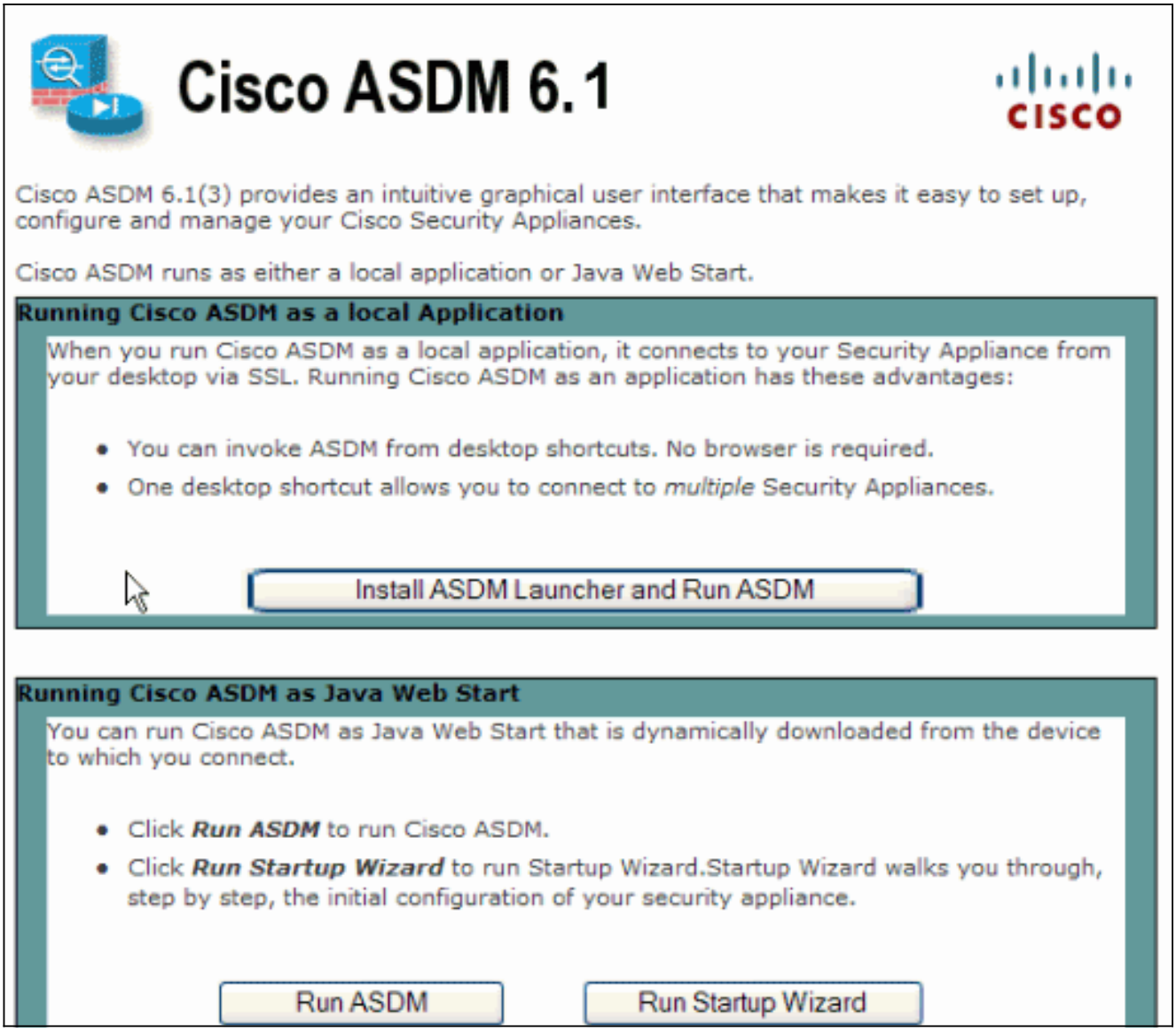
```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy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

Configurazione ASDM

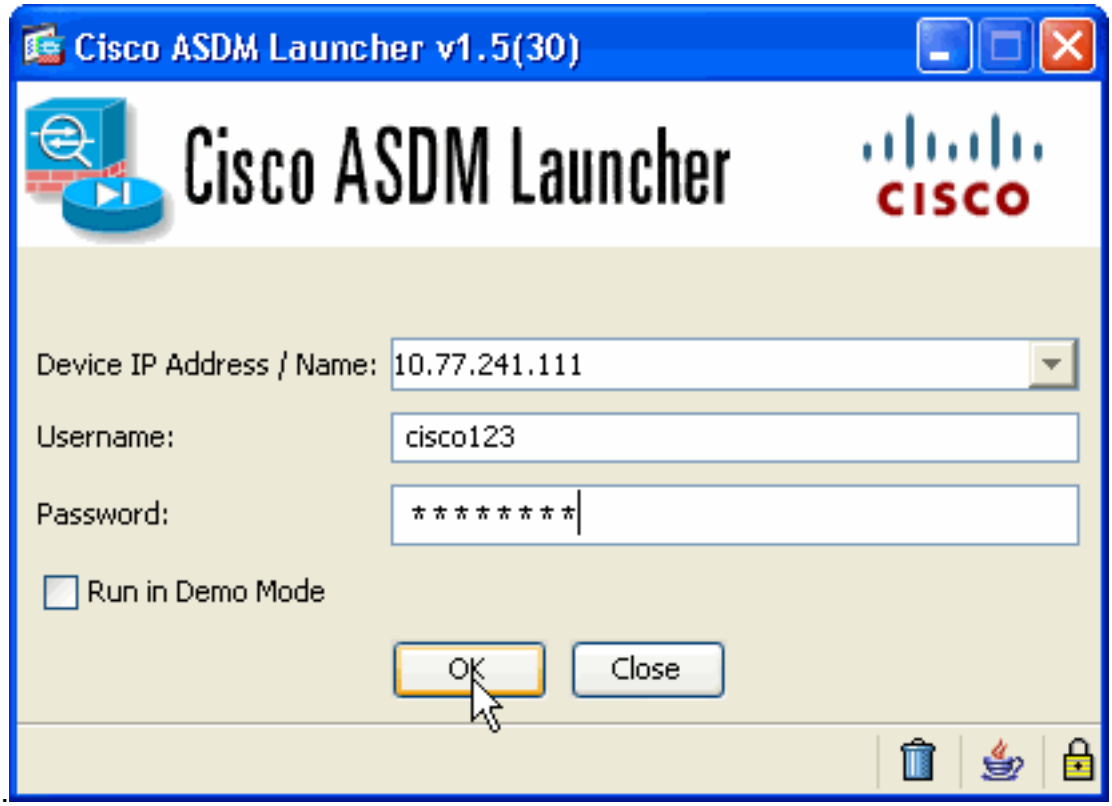
Per configurare il client PPPoE fornito con l'appliance di sicurezza adattiva, completare la procedura seguente:

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

1. Accedere all'ASDM sull'appliance ASA:Aprire il browser e immettere **https://<*ASDM_ASA_IP_ADDRESS*>**.Dove *ASDM_ASA_IP_ADDRESS* è l'indirizzo IP dell'interfaccia ASA configurata per l'accesso ASDM.**Nota:** assicurati di autorizzare gli avvisi che il browser ti invierà relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione ASDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet
   Java.

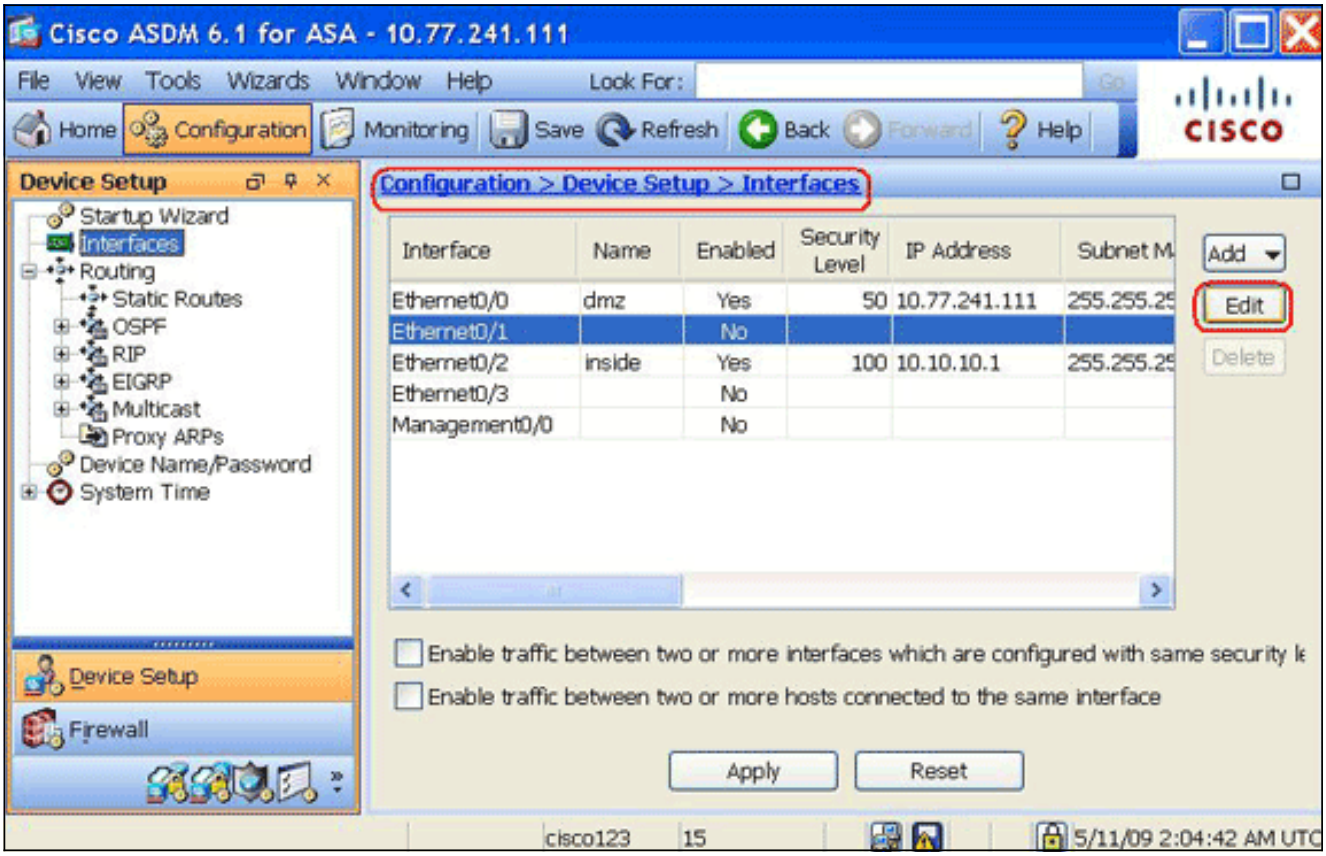


2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
4. Immettere l'indirizzo IP per l'interfaccia configurata con il comando **http -**, nonché un nome utente e una password, se specificati.In questo esempio viene utilizzato **cisco123** come nome utente e **cisco123** come

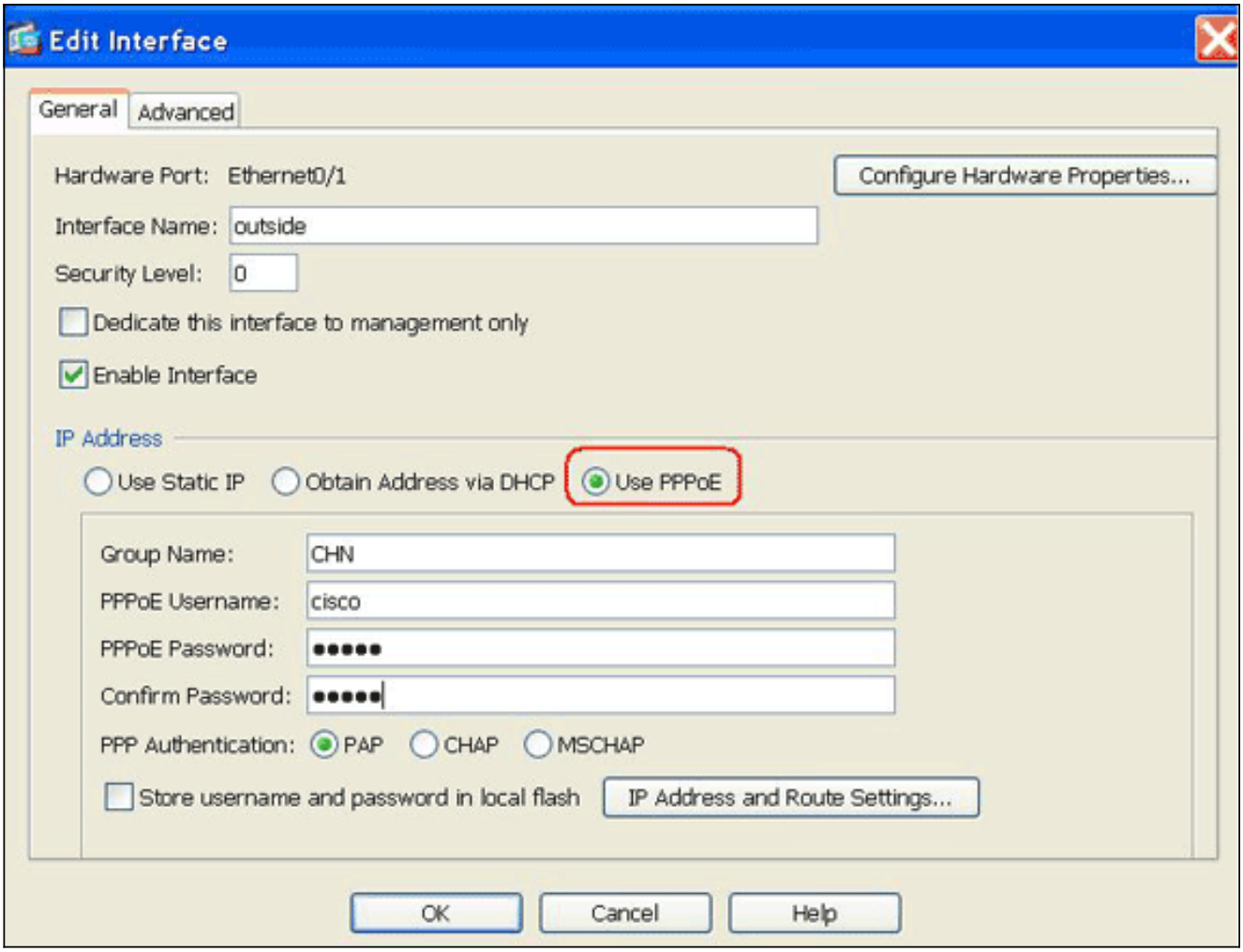


password.

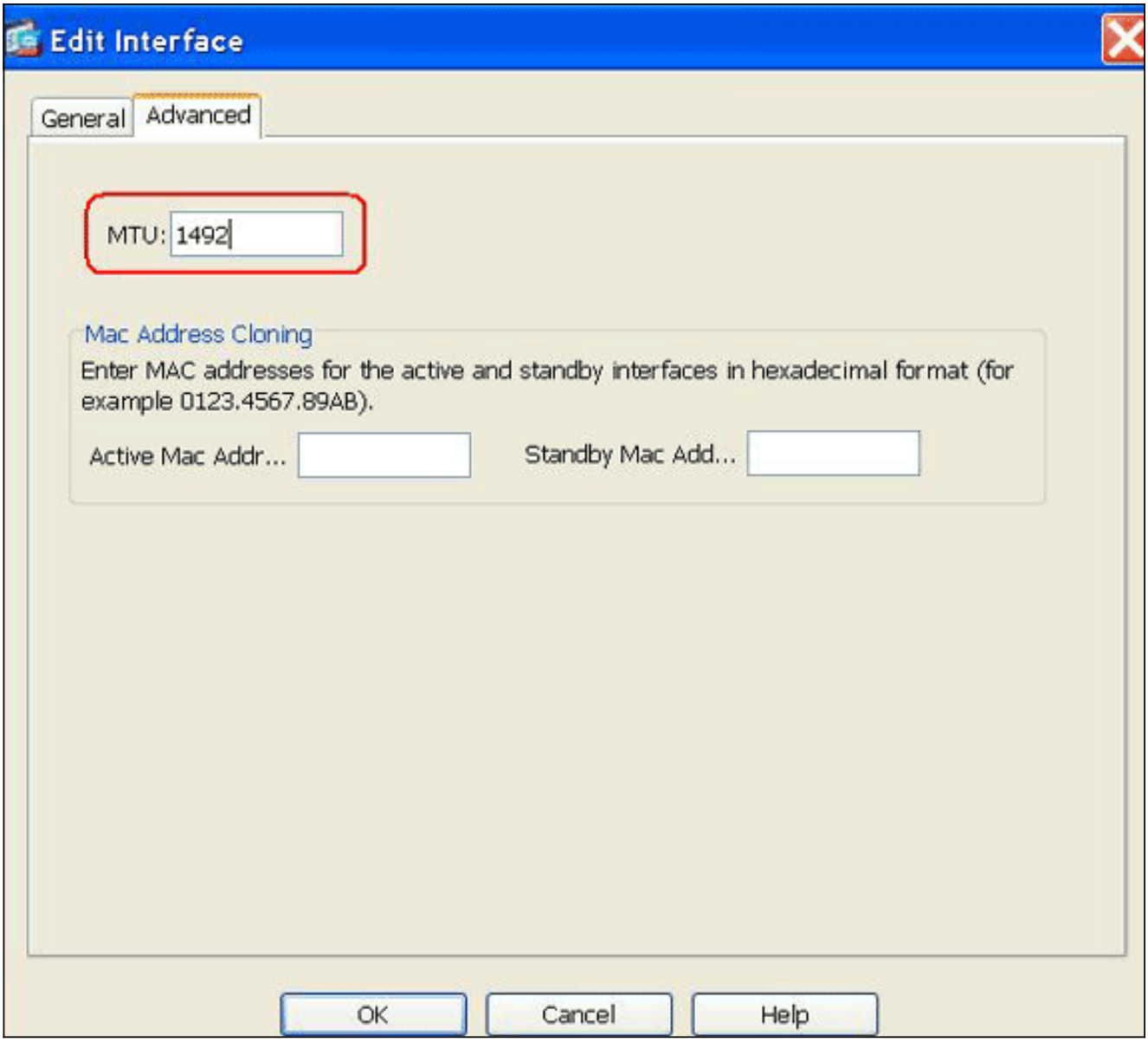
5. Scegliete **Configurazione > Impostazione periferica > Interfacce**, evidenziate l'interfaccia esterna e fate clic su **Modifica**.



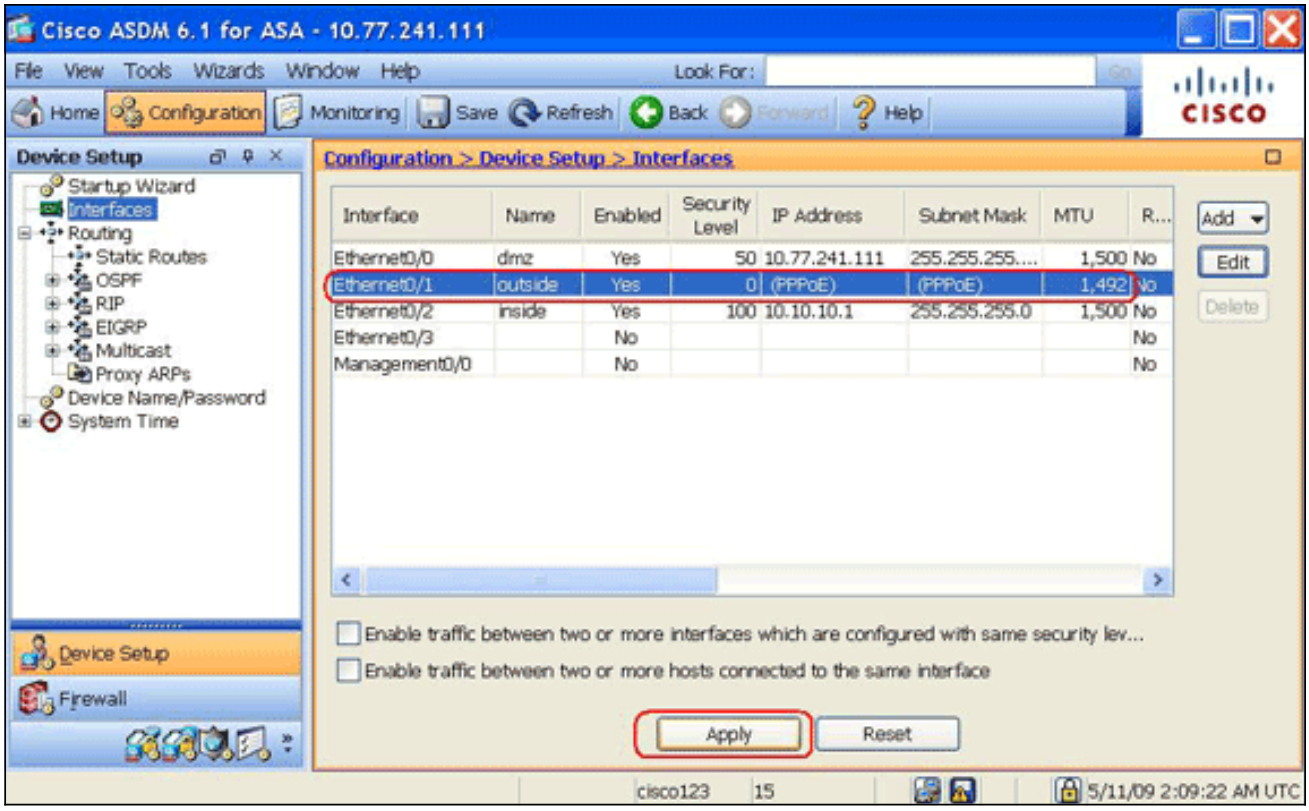
6. Nel campo Nome interfaccia immettere **outside**, quindi selezionare la casella di controllo **Enable Interface**.
7. Fare clic sul pulsante di scelta **Usa PPPoE** nell'area Indirizzo IP.
8. Immettere un nome di gruppo, un nome utente e una password PPPoE, quindi fare clic sul pulsante di opzione relativo al tipo di autenticazione PPP (PAP, CHAP o MSCHAP).



9. Fare clic sulla scheda **Advanced** (Avanzate) e verificare che la dimensione MTU sia impostata su **1492.Nota:** le dimensioni della MTU (Maximum Transmission Unit) vengono impostate automaticamente su 1492 byte, il valore corretto per consentire la trasmissione PPPoE in un frame
Ethernet.



10. Fare clic su **OK** per continuare.
11. Verificare che le informazioni immesse siano corrette, quindi fare clic su **Applica**.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip address outside pppoe**: utilizzare questo comando per visualizzare le informazioni di configurazione correnti del client PPPoE.
- **show vpdn session [l2tp] | pppoe] [id id_sess | pacchetti | stato | window]**: utilizzare questo comando per visualizzare lo stato delle sessioni PPPoE.

Nell'esempio seguente viene illustrato un esempio di informazioni fornite da questo comando:

```
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#
```

Cancellazione della configurazione

Per rimuovere tutti i comandi **vpdn group** dalla configurazione, utilizzare il comando clear configure vpdn group in modalità di configurazione globale:

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

Per rimuovere tutti i comandi **vpdn username**, usare il comando clear configure vpdn username:

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

Nota: questi comandi non influiscono sulle connessioni PPPoE attive.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **hostname# [no] debug pppoe {event Errore | | packet}**: utilizzare questo comando per abilitare o disabilitare il debug per il client PPPoE.

La subnet mask viene visualizzata come /32

Problema

Quando si utilizza il comando **indirizzo IP x.x.x.x 255.255.255.240 pppoe setroute**, l'indirizzo IP viene assegnato correttamente, ma la subnet mask viene visualizzata come /32 sebbene sia specificata nel comando come /28. Perché ciò accade?

Soluzione

Questo è il comportamento corretto. La subnet mask non è pertinente nel caso dell'interfaccia PPPoe; l'ASA la cambia sempre in /32.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Configurazione del client PPPoE su Cisco 2600 per la connessione a un CPE DSL non Cisco
- Cisco Adaptive Security Device Manager
- Documentazione e supporto tecnico – Cisco Systems