PIX/ASA:PPPoE 클라이언트 컨피그레이션 예

목차

소개

이 문서에서는 버전 7.2.(1) 이상의 PPPoE(Point-to-Point Protocol over Ethernet) 클라이언트로 ASA/PIX 보안 어플라이언스의 샘플 컨피그레이션을 제공합니다.

PPPoE는 클라이언트 시스템에 IP 주소를 할당하는 인증된 방법을 제공하기 위해 널리 사용되는 두 가지 표준인 이더넷과 PPP를 결합합니다.PPPoE 클라이언트는 일반적으로 DSL 또는 케이블 서비스와 같은 원격 광대역 연결을 통해 ISP에 연결된 개인용 컴퓨터입니다.ISP는 PPPoE를 구축하는데, 이는 고객이 더 쉽게 사용하고 고속 광대역 액세스를 지원하기 위해 기존 원격 액세스 인프라를 사용하기 때문입니다.

PPPoE는 PPPoE 네트워크의 인증 방법을 사용하는 표준 방법을 제공합니다.ISP에서 사용할 경우 PPPoE는 인증된 IP 주소 할당을 허용합니다.이러한 유형의 구현에서 PPPoE 클라이언트와 서버는 DSL 또는 기타 광대역 연결을 통해 실행되는 레이어 2 브리징 프로토콜로 상호 연결됩니다.

PPPoE는 두 가지 주요 단계로 구성됩니다.

- Active Discovery Phase(활성 검색 단계) - 이 단계에서는 PPPoE 클라이언트가 액세스 집중기라는 PPPoE 서버를 찾습니다. 여기서 세션 ID가 할당되고 PPPoE 레이어가 설정됩니다
- PPP Session Phase(PPP 세션 단계) - 이 단계에서는 PPP(Point-to-Point Protocol) 옵션이 협상되고 인증이 수행됩니다.링크 설정이 완료되면 PPPoE는 PPPoE 헤더 내의 PPP 링크를 통해 데이터를 전송할 수 있는 레이어 2 캡슐화 방법으로 작동합니다.

시스템 초기화 시 PPPoE 클라이언트는 액세스 집중기와의 세션을 설정하기 위해 일련의 패킷을 교

환합니다.세션이 설정되면 PPP 링크가 설정되며, 이 링크는 인증에 PAP(Password Authentication Protocol)를 사용합니다.PPP 세션이 설정되면 각 패킷은 PPPoE 및 PPP 헤더에 캡슐화됩니다.

참고: Adaptive Security Appliance에서 장애 조치가 구성되거나 다중 컨텍스트 또는 투명 모드에서 장애 조치가 구성된 경우에는 PPPoE가 지원되지 않습니다.PPPoE는 장애 조치 없이 단일 라우팅 모드에서만 지원됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA(Adaptive Security Appliance) 버전 8.x 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 버전 7.2(1) 이상을 실행하는 Cisco PIX 500 Series Security Appliance에서도 사용할 수 있습니다.Cisco Secure PIX Firewall에서 PPPoE 클라이언트를 구성하기 위해 PIX OS 버전 6.2는 이 기능을 도입하며 로우엔드 PIX(501/506)를 대상으로 합니다. 자세한 내용은 Cisco Secure PIX Firewall에서 PPPoE 클라이언트 구성 을 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 필요한 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.

CLI 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

장치 이름 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
```

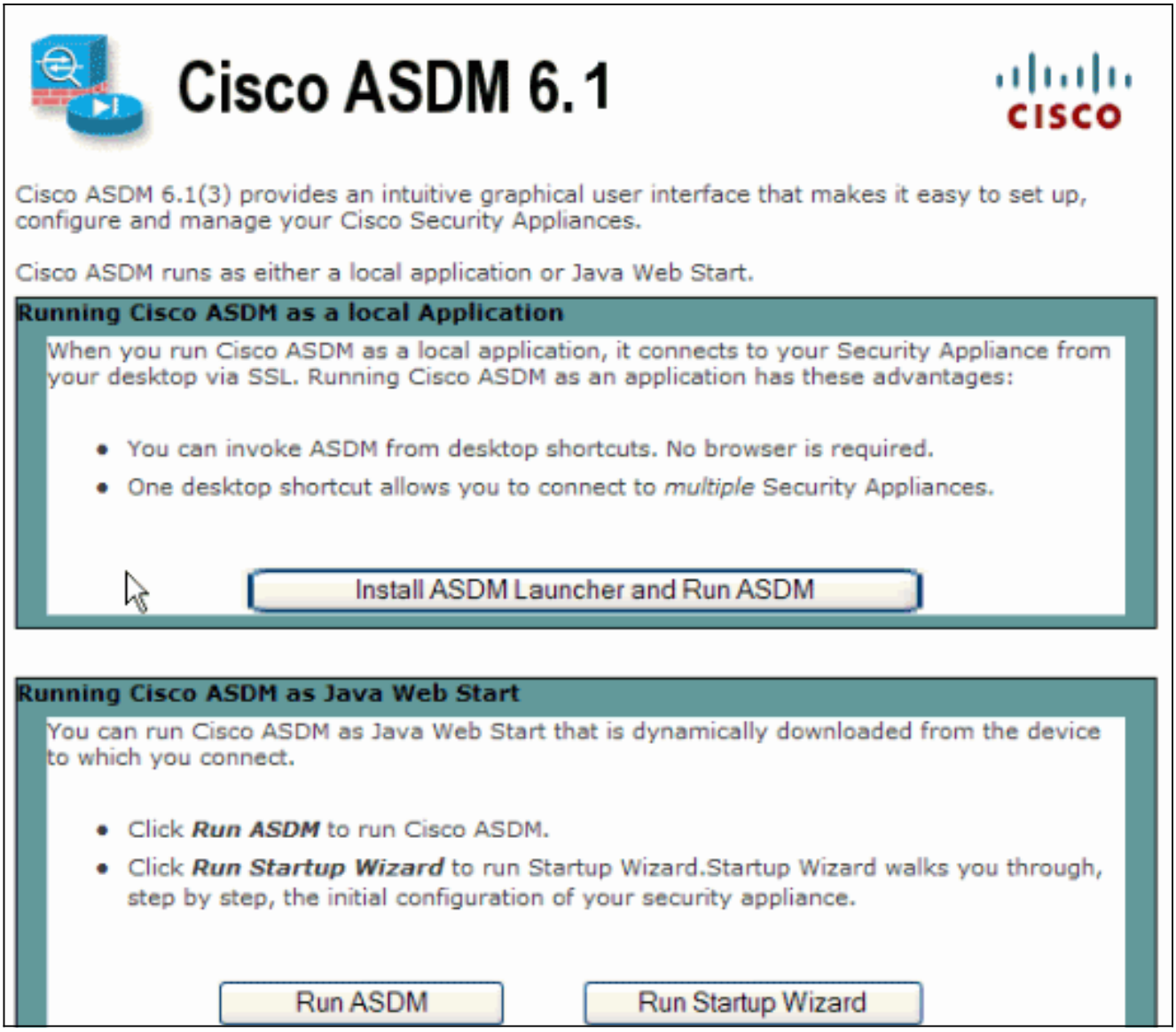
```
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
username cisco123 password ffIRPGpDSOJh9YLq encrypted
privilege 15
prompt hostname context
Cryptochecksum:3cf813b751fe78474dfb1d61bb88a133
: end
ciscoasa#
```

ASDM 컨피그레이션

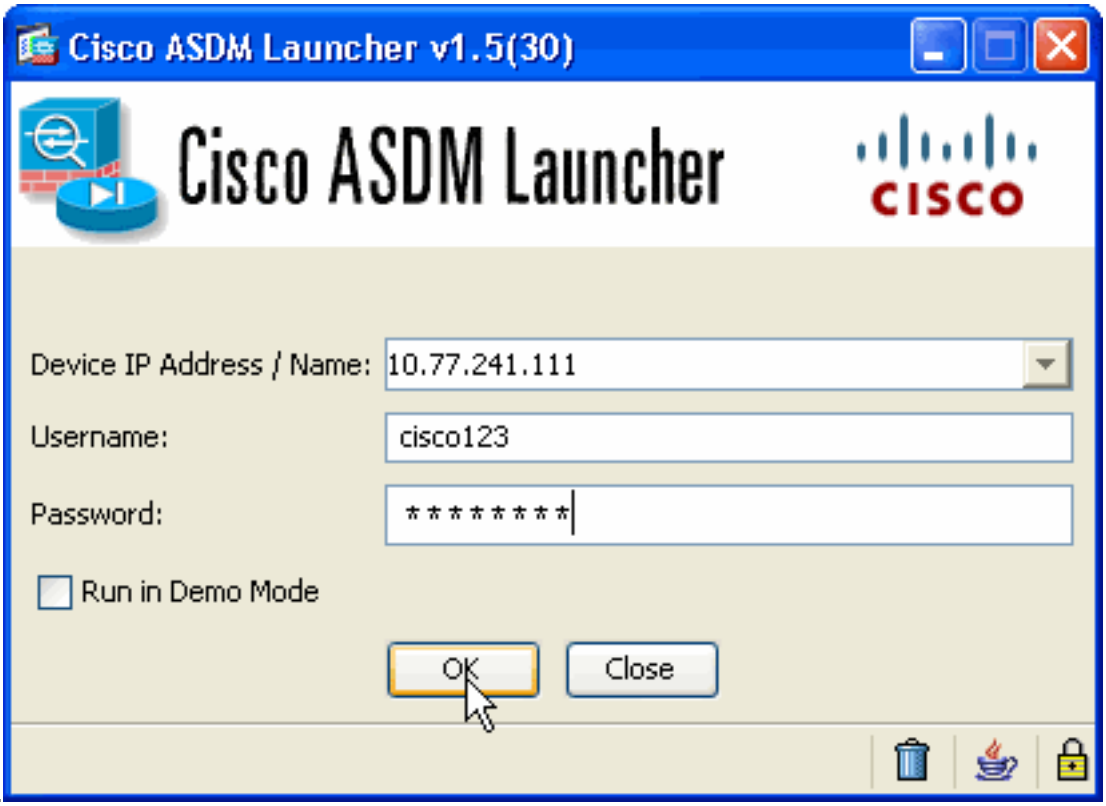
Adaptive Security Appliance와 함께 제공된 PPPoE 클라이언트를 구성하려면 다음 단계를 완료합니다.

참고: ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

1. ASA에서 ASDM에 액세스합니다.브라우저를 열고 https:// **<ASDM_*ASA_IP_ADDRESS*>를 입력합니다**.여기서 *ASDM_ASA_IP_ADDRESS*는 ASDM 액세스를 위해 구성된 ASA 인터페이스의 IP 주소입니다.**참고:** 브라우저에서 SSL 인증서 신뢰성과 관련된 경고를 승인해야 합니다.기본 사용자 이름과 비밀번호는 모두 비어 있습니다.ASDM 애플리케이션의 다운로드를 허용하기 위해 ASA에 이 창이 표시됩니다.이 예에서는 응용 프로그램을 로컬 컴퓨터에 로드하며 Java 애플릿에서 실행되지 않습니다
   .



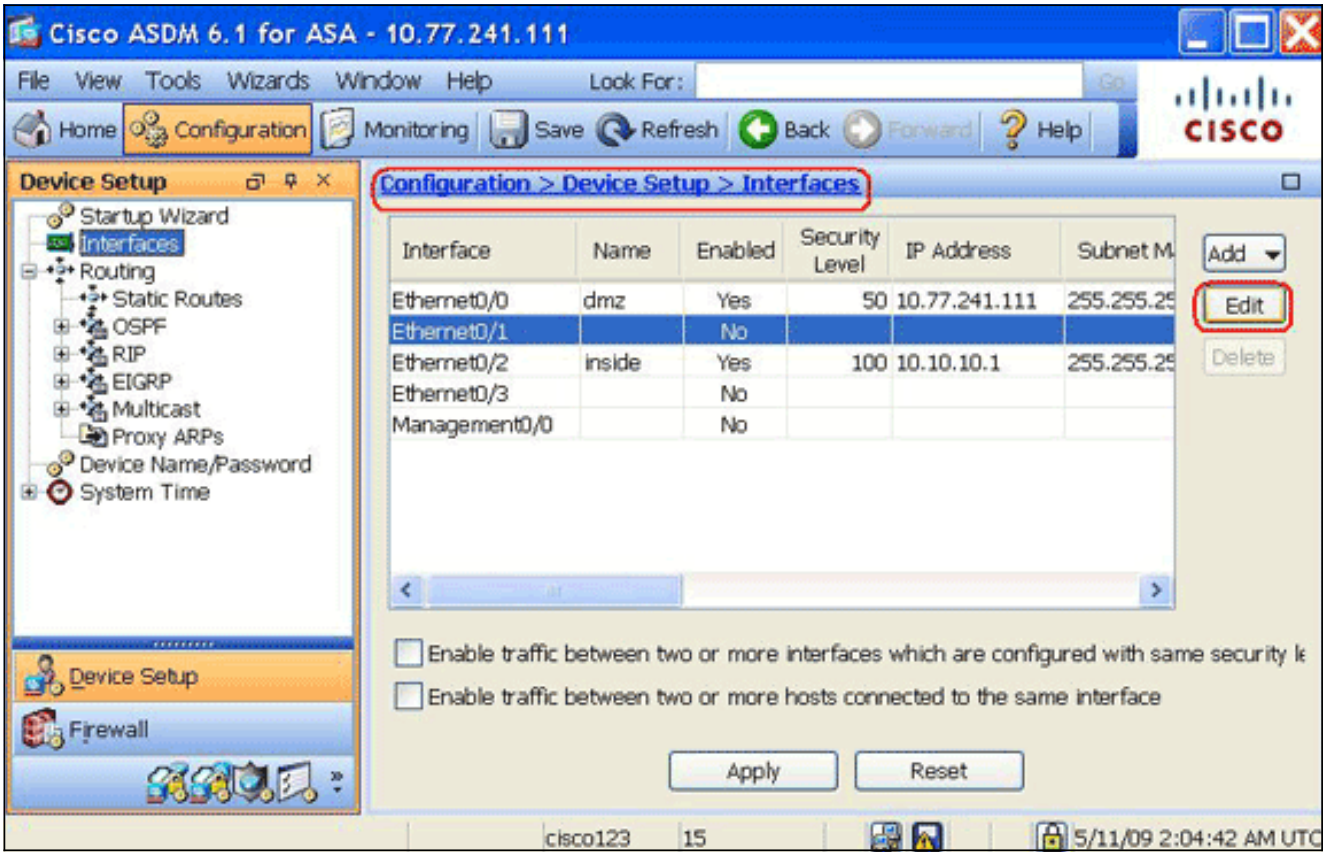
2. ASDM 애플리케이션 **설치** 프로그램을 다운로드하려면 **Download ASDM Launcher and Start ASDM(ASDM 시작** 시작 **시작**)을 클릭합니다.
3. ASDM Launcher가 다운로드되면 소프트웨어를 설치하기 위해 프롬프트에 의해 지시된 단계를 완료하고 Cisco ASDM Launcher를 실행합니다.
4. **http -** 명령으로 구성한 인터페이스의 IP 주소를 입력하고 사용자 이름과 비밀번호를 지정한 경우 입력합니다.이 예에서는 **cisco123**을 사용자 이름으로 사용하고 **cisco123**을 비밀번호로



사용합니다.

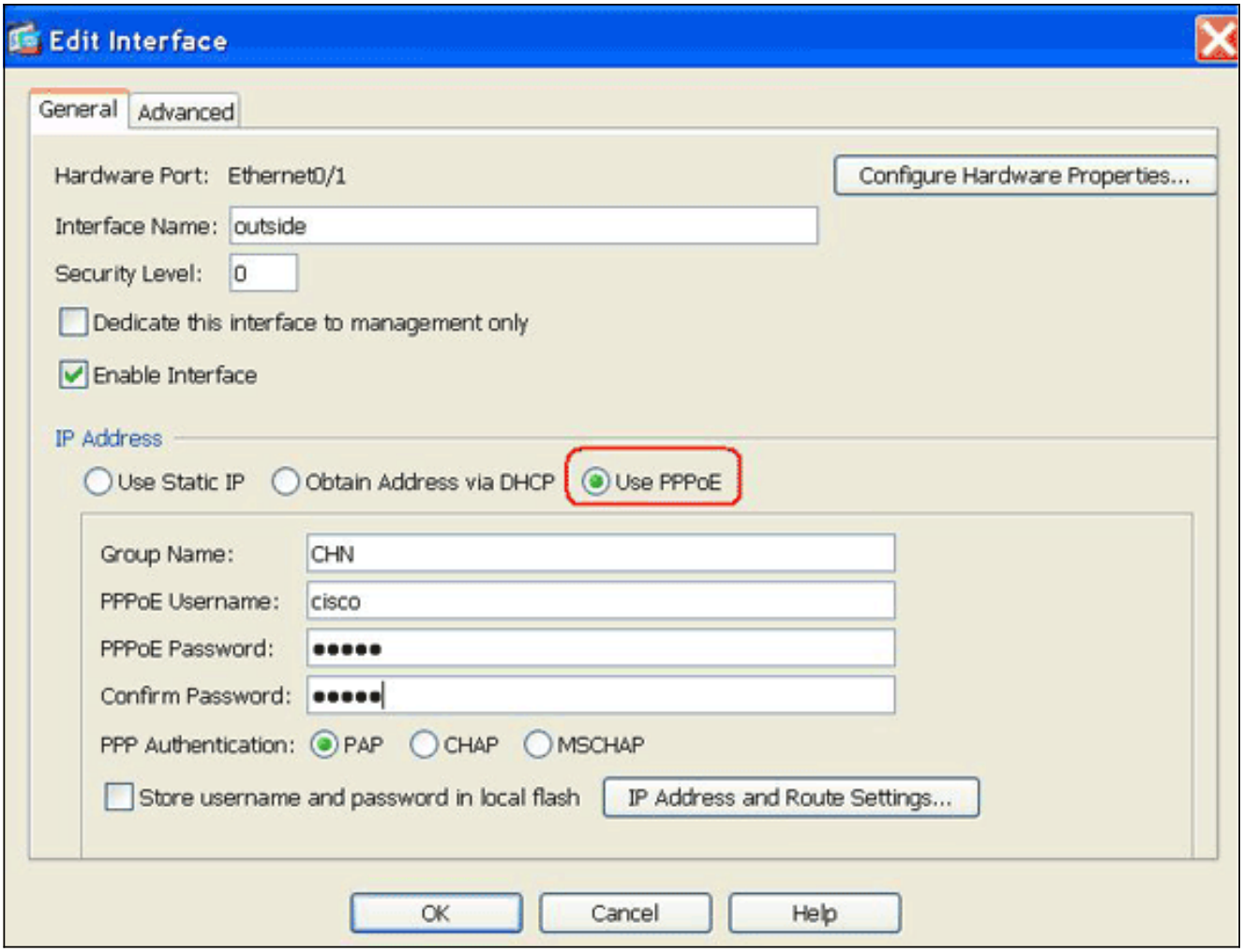
5. Configuration **> Device Setup > Interfaces**를 선택하고 외부 인터페이스를 강조 표시한 다음 Edit를 **클릭합니다**

.



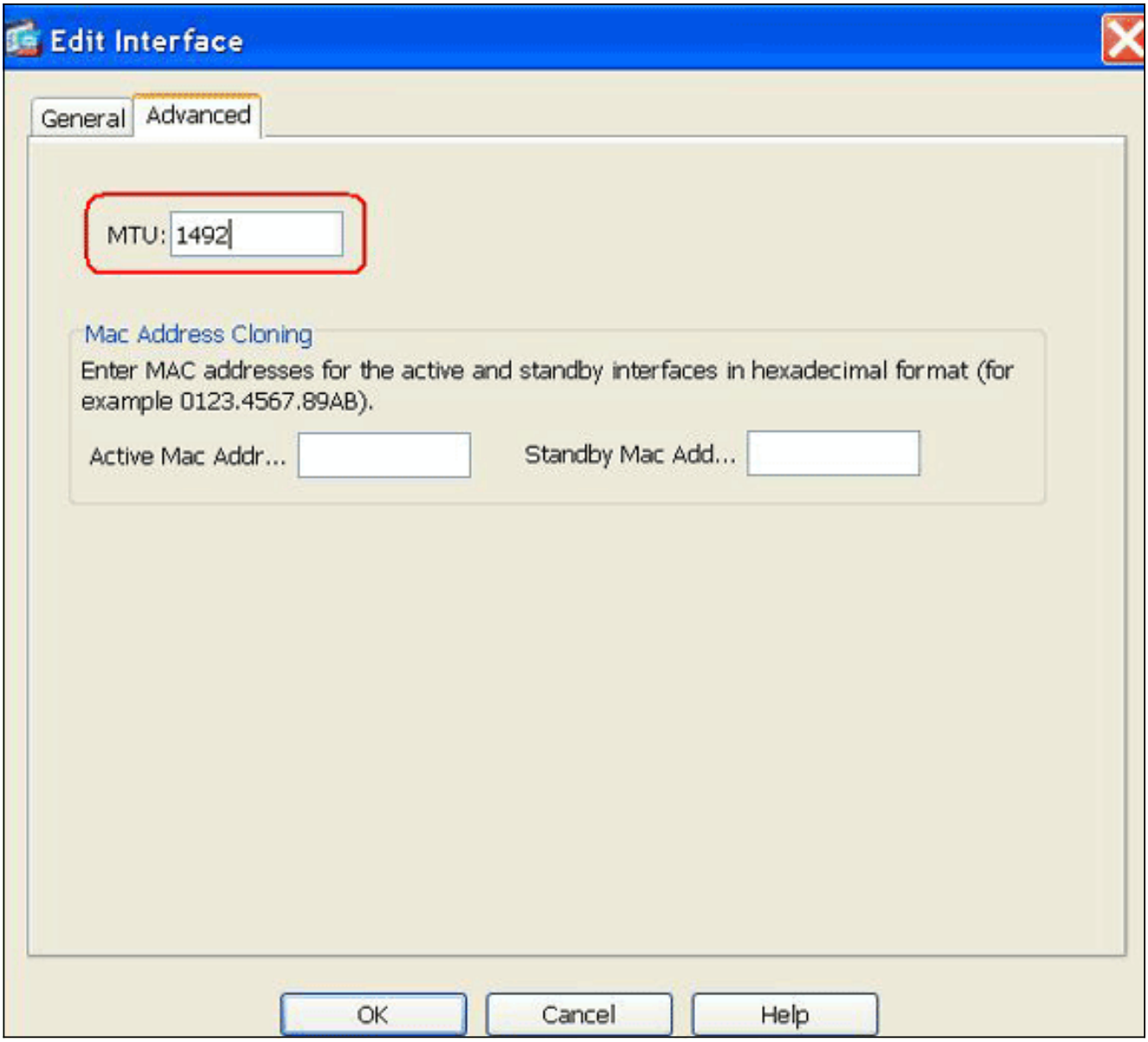
6. Interface Name 필드에 **outside**를 입력하고 Enable **Interface** 확인란**을** 선택합니다.
7. IP Address 영역**에서 Use PPPoE** 라디오 버튼을 클릭합니다.
8. 그룹 이름, PPPoE 사용자 이름 및 비밀번호를 입력하고 적절한 PPP 인증 유형(PAP, CHAP 또는 MSCHAP) 라디오 버튼을 클릭합니다

.



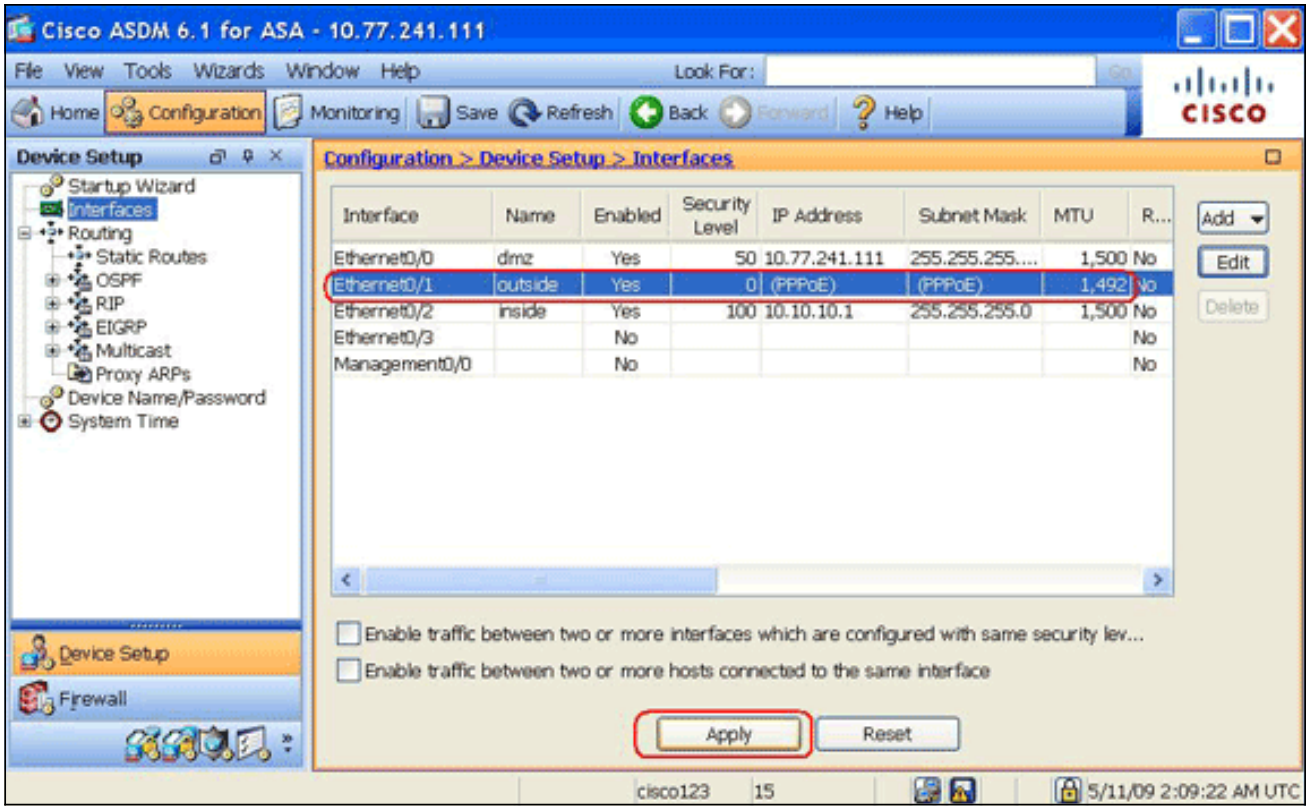
9. Advanced(**고급**) 탭을 클릭하고 MTU 크기가 **1492**로 설정되어 있는지 확인합니다.**참고:** MTU(Maximum Transmission Unit) 크기는 자동으로 1492바이트로 설정되며, 이는 이더넷 프레임 내에서 PPPoE 전송을 허용하는 올바른 값입니다

.



10. OK(**확인**)를 클릭하여 계속합니다.
11. 입력한 정보가 올바른지 확인하고 Apply(적용)를 **클릭합니다**

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show ip address outside pppoe** - 현재 PPPoE 클라이언트 컨피그레이션 정보를 표시하려면 이 명령을 사용합니다.
- **show vpdn 세션 [l2tp | pppoe] [id sess_id | 패킷 | 상태 | window]**—PPPoE 세션의 상태를 보려면 이 명령을 사용합니다.

다음 예는 이 명령에서 제공하는 정보의 샘플을 보여줍니다.

```
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#
```

구성 지우기

컨피그레이션에서 모든 vpdn **group** 명령을 제거하려면 글로벌 컨피그레이션 모드에서 clear configure vpdn group 명령을 사용합니다.

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

모든 vpdn **username** 명령을 제거하려면 clear configure vpdn username 명령을 사용합니다.

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

참고: 이 명령은 활성 PPPoE 연결에는 영향을 미치지 않습니다.

문제 해결

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **호스트 이름 번호 [no] 디버그 pppoe {event | 오류 | packet}** - PPPoE 클라이언트에 대한 디버깅을 활성화하거나 비활성화하려면 이 명령을 사용합니다.

서브넷 마스크가 /32로 나타납니다.

문제

IP 주소 x.x.x.x 255.255.255.240 pppoe setroute 명령을 사용할 경우 IP 주소가 올바르게 할당되지만 서브넷 마스크는 /28로 명령에 지정되었지만 /32로 나타납니다. 왜 이런 일이 발생합니까?

솔루션

이는 올바른 동작입니다.서브넷 마스크는 PPPoe 인터페이스의 경우 관련이 없습니다.ASA는 항상 /32로 변경합니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco 2600에서 비 Cisco DSL CPE에 연결하도록 PPPoE 클라이언트 구성
- Cisco Adaptive Security Device Manager
- 기술 지원 및 문서 – Cisco Systems