PIX/ASA: Пример конфигурации PPPoE-клиента

Содержание

Введение

В этом документе приведен пример конфигурации для использования устройства защиты ASA/PIX в качестве клиента протокола PPP по Ethernet (PPPoE) для версий 7.2.(1) и выше.

Протокол PPPoE объединяет два широко распространенных стандарта — Ethernet и PPP, обеспечивая механизм назначения IP-адресов клиентским системам с прохождением аутентификации. Обычно PPPoE-клиентами являются персональные компьютеры, подключенные к поставщику услуг Интернета через удаленное широкополосное соединение, например, через DSL-канал или кабельную сеть. Поставщики услуг Интернета используют протокол PPPoE, поскольку он сравнительно прост для пользователей и использует существующую инфраструктуру удаленного доступа поставщика услуг.

Протокол PPPoE реализует стандартный метод применения методов аутентификации в сети PPPoE. С точки зрения поставщика услуг Интернета протокол PPPoE позволяет назначать IP-адреса с прохождением аутентификации. Для этого вида применения PPPoE-клиент и сервер устанавливают соединение с помощью протоколов моста второго уровня, действующих через DSL-канал или другое широкополосное соединение.

PPPoE-протокол работает в два основных этапа:

- Этап активного обнаружения — на этом этапе PPPoE-клиент обнаруживает PPPoE-сервер, вызываемый концентратором доступа. Последний назначает идентификатор сеанса и устанавливает уровень PPPoE
- Этап сеанса PPP — на этом этапе оговариваются параметры протокола PPP и выполняется аутентификация. После завершения установки канала связи, PPPoE функционирует в качестве метода инкапсуляции второго уровня, делая возможной передачу данных через PPP-канал под PPPoE-заголовками.

При инициализации системы PPPoE-клиент открывает сеанс с концентратором доступа путем обмена сериями пакетов данных. После открытия сеанса устанавливается PPP-соединение, использующее протокол парольной аутентификации (PAP). Кроме того, после открытия PPP-сеанса каждый пакет инкапсулируется в PPPoE- и PPP-пакет.

Примечание: Когда аварийное переключение настроено на устройстве адаптивной безопасности, или в составном контексте или прозрачном режиме, PPPoE не поддерживается. PPPoE поддерживается только в одиночном режиме с маршрутизацией и без переключения при отказе.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Информация в этом документе касается устройств адаптивной защиты Cisco ASA серии 5500, работающих под управлением ПО версии 8.x или более поздней версии.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Эту конфигурацию также можно использовать для устройств защиты Cisco PIX серии 500, работающих под управлением ПО версии 7.2(1) и более поздних версий. Для настройки клиента PPPoE в межсетевом экране Cisco Secure PIX операционная система PIX версии 6.2 снабжена этой функцией, ориентированной на устройства PIX (501/506) младшего сегмента. Дополнительные сведения см. в документе Настройка клиента PPPoE на межсетевом экране Cisco Secure PIX

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе представлены сведения по настройке функций, описанных в данном документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурация интерфейса командой строки CLI

Эти конфигурации используются в данном документе:

Имя устройства 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
```

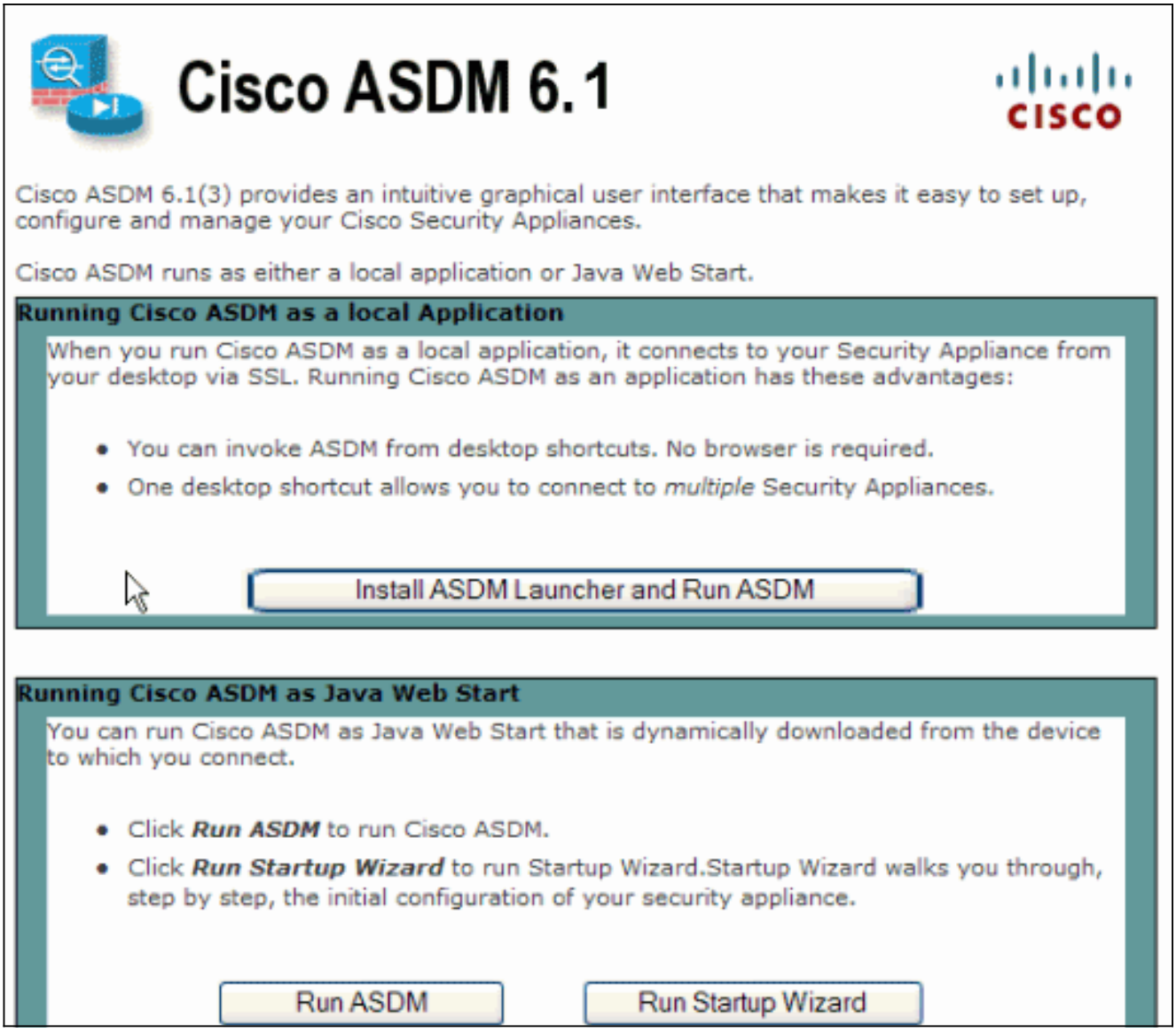
```
1500 !--- Output suppressed. global (outside) 1
interface nat (inside) 1 0.0.0.0 0.0.0.0 !--- The NAT
statements above are for ASA version 8.2 and earlier. !-
-- For ASA versions 8.3 and later the NAT statements are
modified as follows. object network obj_any subnet
0.0.0.0 0.0.0.0 nat (inside,outside) 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#
```

Настройка посредством ASDM

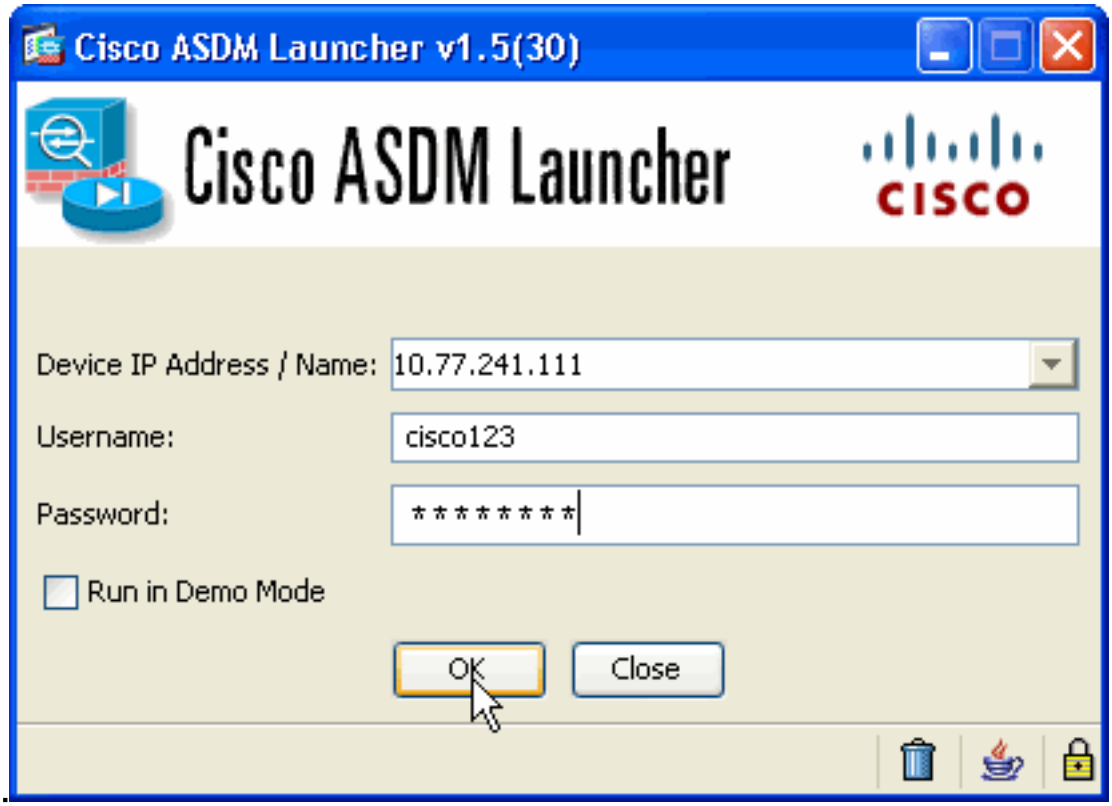
Для настройки клиента PPPoE, поставляемого вместе с устройством адаптивной защиты, выполните следующие шаги:

Примечание: Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

1. Войдите в ASDM на устройстве ASA:***Откройте браузер и введите https://<IP-АДРЕС_ASDM_ASA>.****Где IP-АДРЕС_ASDM_ASA— IP-адрес интерфейса ASA, настроенного для доступа к ASDM.***Примечание:** Отвечайте на все предупреждения, связанные с проверкой SSL-сертификата, выдаваемые браузером. По умолчанию имя пользователя и пароль являются пустыми.ASA отобразит следующее окно для загрузки приложения ASDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение
Java.

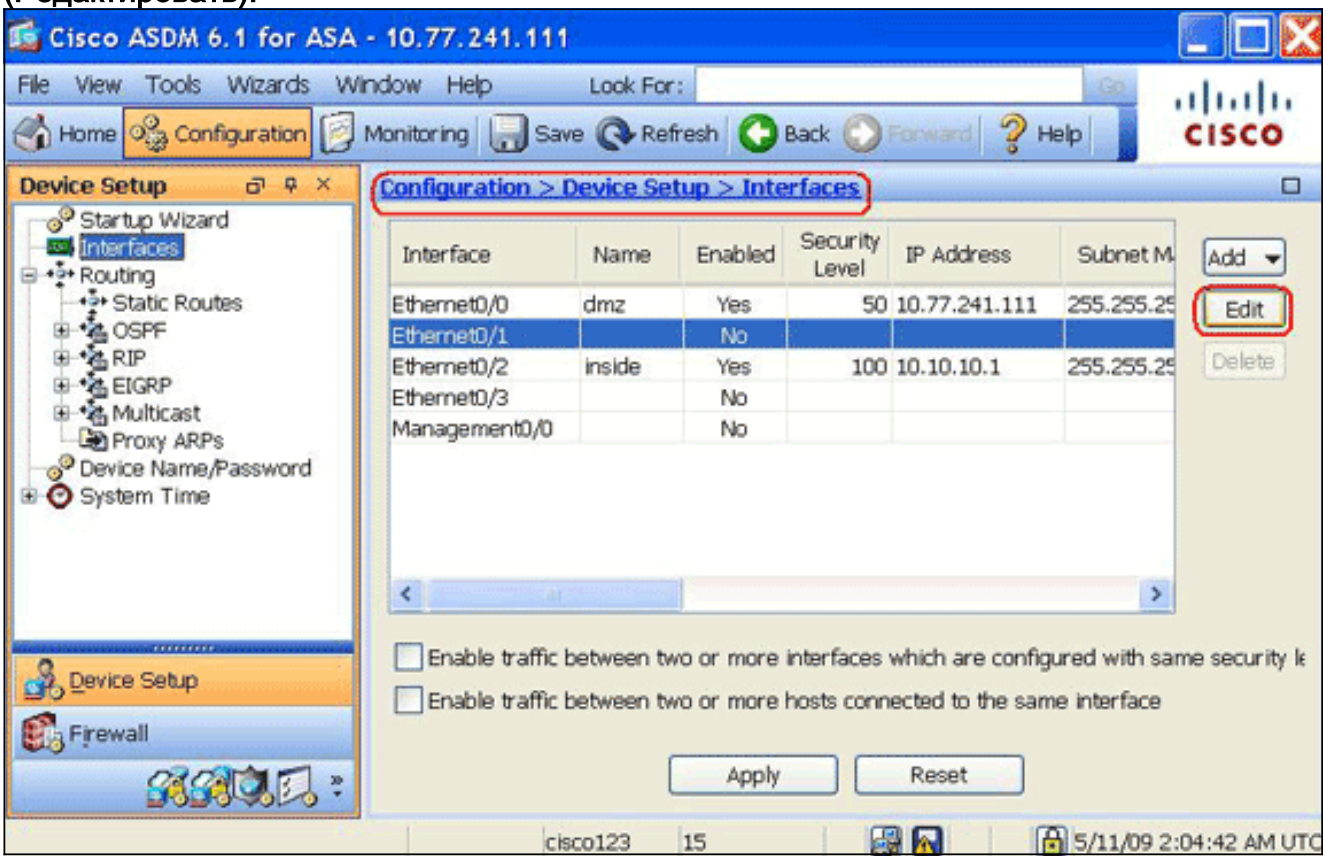


2. **Нажмите кнопку Download ASDM Launcher and Start ASDM, чтобы загрузить файл установки приложения ASDM.**
3. После загрузки ASDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco ASDM Launcher.
4. **Введите в поле Device IP Address IP-адрес настроенного интерфейса с помощью команды http -, а также имя пользователя (в поле Username) и пароль (в поле Password), если они были заданы.В этом примере используется имя пользователя cisco123 и пароль**



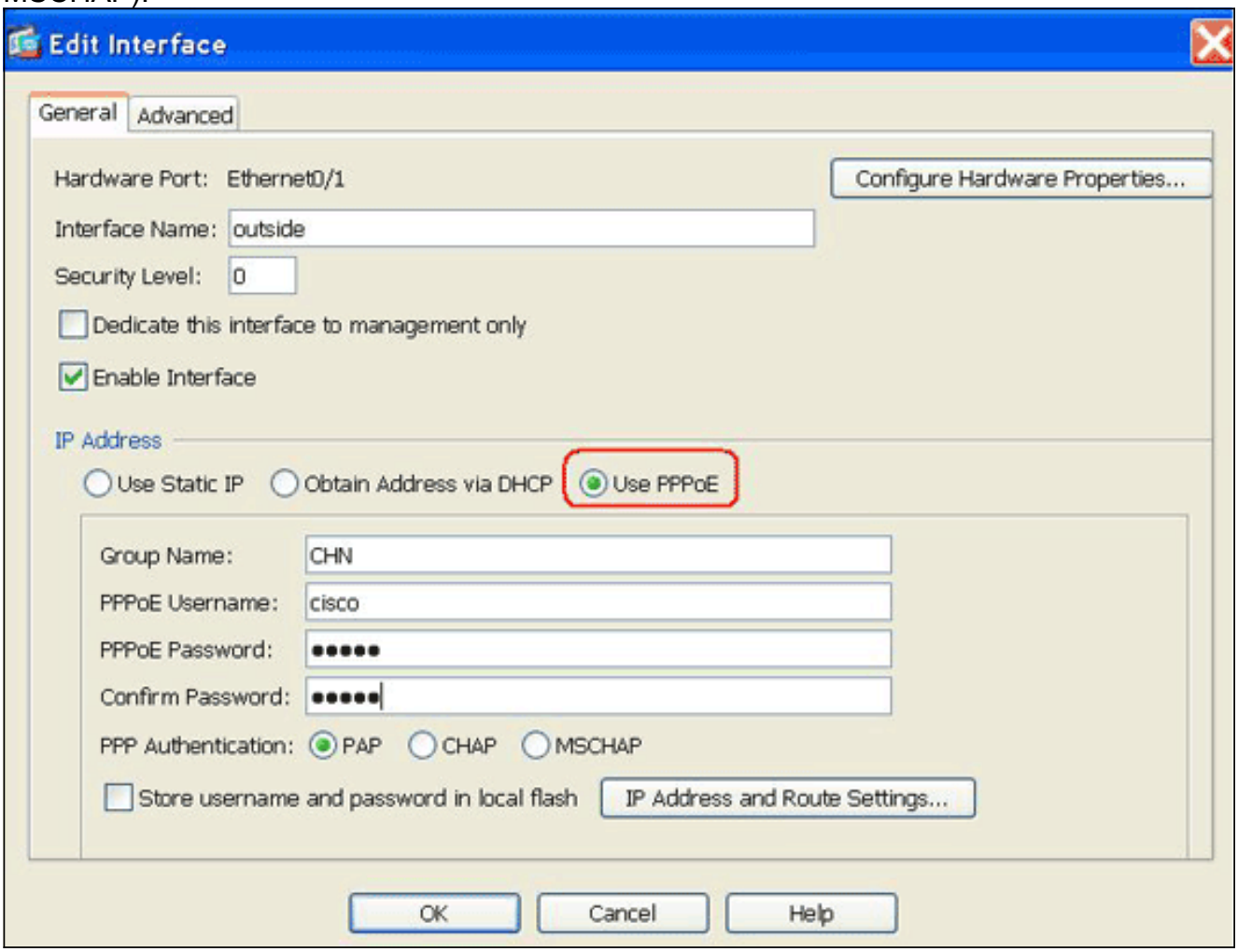
cisco123.

5. **Выберите Configuration > Device Setup > Interfaces (Конфигурация > Настройка устройств > Интерфейсы), выделите внешний интерфейс и нажмите кнопку Edit (Редактировать).**

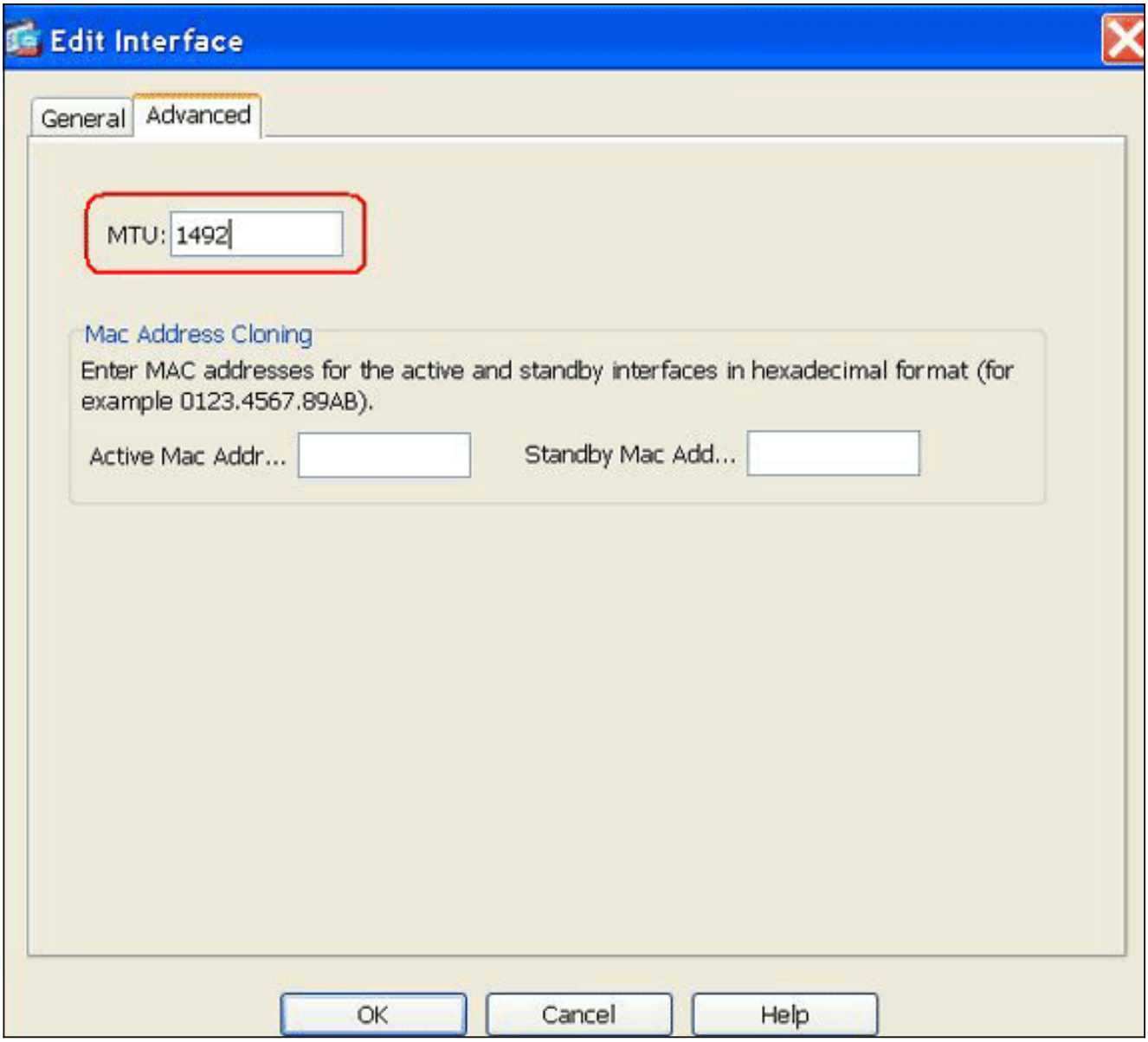


6. **В поле Interface Name (Название интерфейса) введите outside и отметьте флажок Enable Interface (Включить интерфейс).**
7. **Выберите переключатель Use PPPoE (Использовать PPPoE) в области IP Address (IP-адрес).**
8. Введите имя группы, имя пользователя PPPoE и пароль и выберите переключателем соответствующий тип аутентификации PPP (PAP, CHAP или

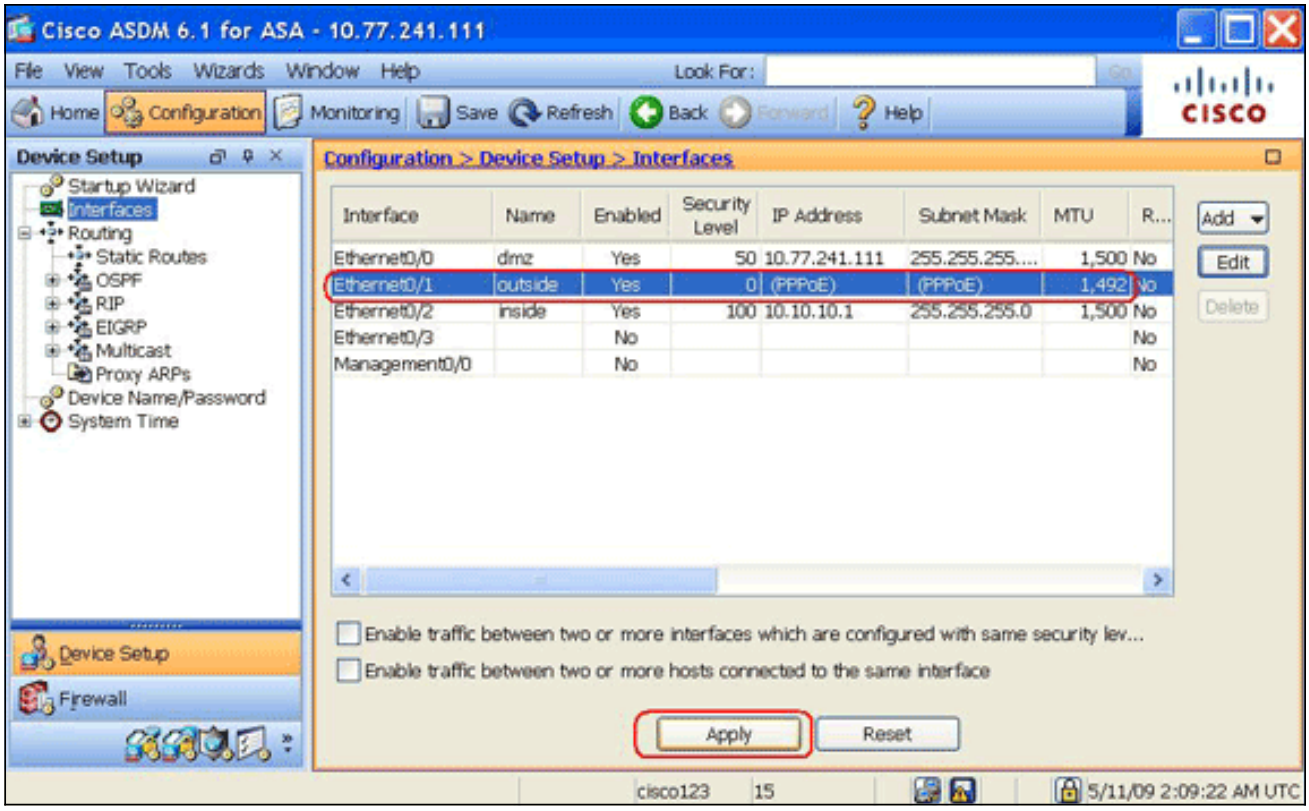
MSCHAP).



9. **Щелкните вкладку Advanced (Дополнительно) и убедитесь, что установлен размер MTU 1492 байта.Примечание:** Максимальный размер передаваемого блока данных (MTU) автоматически установлен в 1492 байта, который является правильным значением для разрешения передачи PPPoE во Фрейме
Ethernet.



10. Для продолжения нажмите кнопку OK.
11. Проверьте правильность сведений и нажмите кнопку Apply (Применить).



Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show ip address outside pppoe— показывает текущую информацию о конфигурации клиента PPPoE.**
- **show vpdn session [l2tp | pppoe] [id sess_id | packets | state | window]— показывает состояние сеансов PPPoE.**

Образец сведений, предоставляемых этой командой, показан в следующем примере:

```
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#
```

Очистка конфигурации

Для удаления из конфигурации всех команд vpdn group выполните команду clear configure vpdn group в режиме глобальной конфигурации:

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

Для удаления всех команд vpdn username используйте команду clear configure vpdn username:

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

Примечание: Эти команды не имеют никакого влияния на активных соединениях PPPoE.

Устранение неполадок

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **hostname# [no] debug pppoe {event | error | packet}— включает или отключает отладку для клиента PPPoE.**

Маска подсети появляется как/32

Проблема

Когда вы используете **IP-адрес x. x. x. x 255.255.255.240 pppoe setroute** команда, IP-адрес назначен правильно, но маска подсети появляется как/32 невзирая на то, что это задано в команде как/28. Почему это происходит?

Решение

Это - правильное поведение. Маска подсети не важна в случае интерфейса PPPoe; ASA будет всегда изменять его на/32.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Настройка клиента PPPoE на Cisco 2600 для подключения к Non-Cisco DSL CPE
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Cisco Systems – техническая поддержка и документация