ASA/PIX: Пример конфигурации обращения к VPN Client IPsec, посредством сервера DHCP с ASDM

Содержание

Введение

Этот документ описывает способ настройки устройства адаптивной защиты (ASA) Cisco серии 5500 для того, чтобы сервер DHCP назначал клиентские IP-адреса всем клиентам VPN. Настройка выполняется с использованием диспетчера устройств адаптивной защиты (ASDM) или командной строки. Программа ASDM предоставляет возможность качественного управления и контроля за безопасностью с помощью интуитивно понятного и простого в использовании web-интерфейса управления. Готовую конфигурацию Cisco ASA можно проверить, используя VPN-клиент Cisco.

См. PIX/ASA 7.x и Cisco VPN Client 4.x с Windows 2003 IAS RADIUS (Против Active Directory) Пример Конфигурации аутентификации для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7. x. Пользователь удаленного клиента VPN аутентифицируется против Active Directory с помощью сервера RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года.

См. PIX/ASA 7.x и Cisco VPN Client 4.x для Примера Конфигурации аутентификации Cisco Secure ACS для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7.x использование сервера Cisco Secure Access Control Server (Версия ACS 3.2) для расширенной проверки подлинности (XAUTH).

Предварительные условия

Требования

В этом документе предполагается, что устройство адаптивной защиты полностью исправно и в нем разрешено изменение конфигурации с помощью Cisco ASDM или интерфейса командной строки.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM или PIX/ASA 7. x: Пример настройки SSH на внутреннем и внешнем интерфейсах для удаленной настройки устройства по протоколам ASDM или Secure Shell (SSH).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ПО устройств адаптивной защиты Cisco версии 7.x и более поздних версий
- Менеджер устройств адаптивной безопасности (ASDM) Версайон 5.x и позже
- Cisco VPN Client версии 4.x или выше

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

Эти настройки также могут быть использованы в устройствах защиты Cisco PIX, начиная с версий 7.x.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

VPN адреса удалённого доступа требуются для мобильных сотрудников для безопасного соединения с сетью организации. Мобильные пользователи могут настроить безопасное соединение с помощью программного обеспечения VPN Client, установленного на их ПК. VPN Client инициирует подключение к устройству центрального узла, настроенному для приема таких запросов. В данном примере устройством центрального узла является Устройство адаптивной безопасности серии 5500 ASA, которое использует динамические

криптокарты.

В управлении адресами устройства безопасности мы должны настроить IP-адреса, которые подключают клиента с ресурсом на частной сети, через туннель, и позволяют клиентской функции, как будто это напрямую подключилось к частной сети. Кроме того, мы имеем дело только с закрытыми IP - адресами, которые назначены на клиентов. IP-адреса, назначенные на другие ресурсы на вашей частной сети, являются частью ваших обязанностей по администрированию сети, не частью управления VPN. Поэтому, когда IP-адреса обсуждены здесь, мы имеем в виду те IP-адреса, доступные в вашей схеме адресации частной сети, которые позволяют клиентской функции как оконечной точке туннеля.

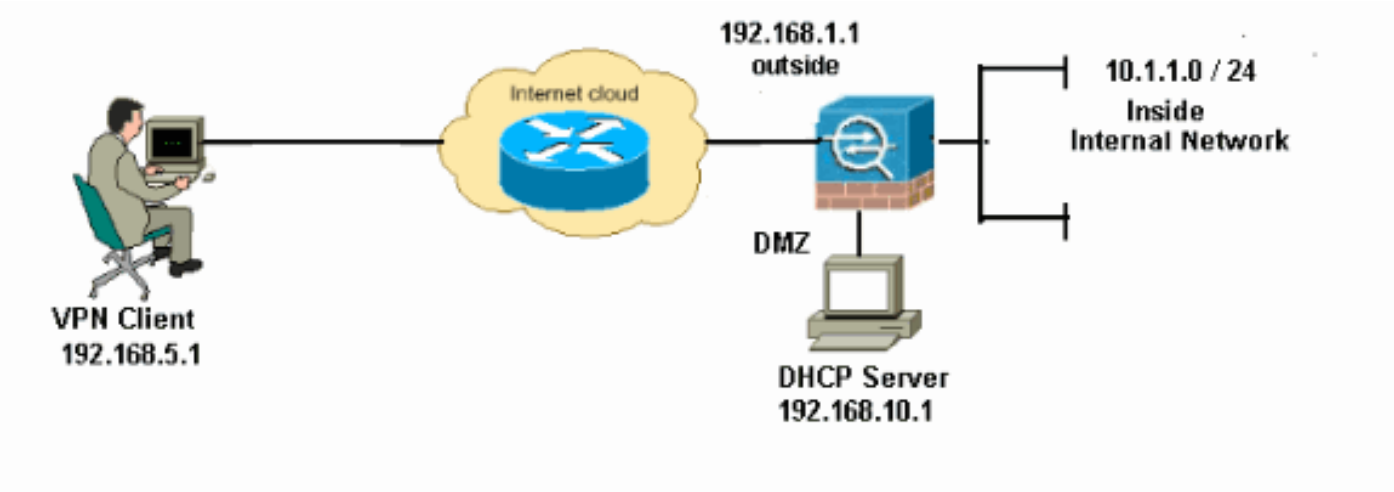
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



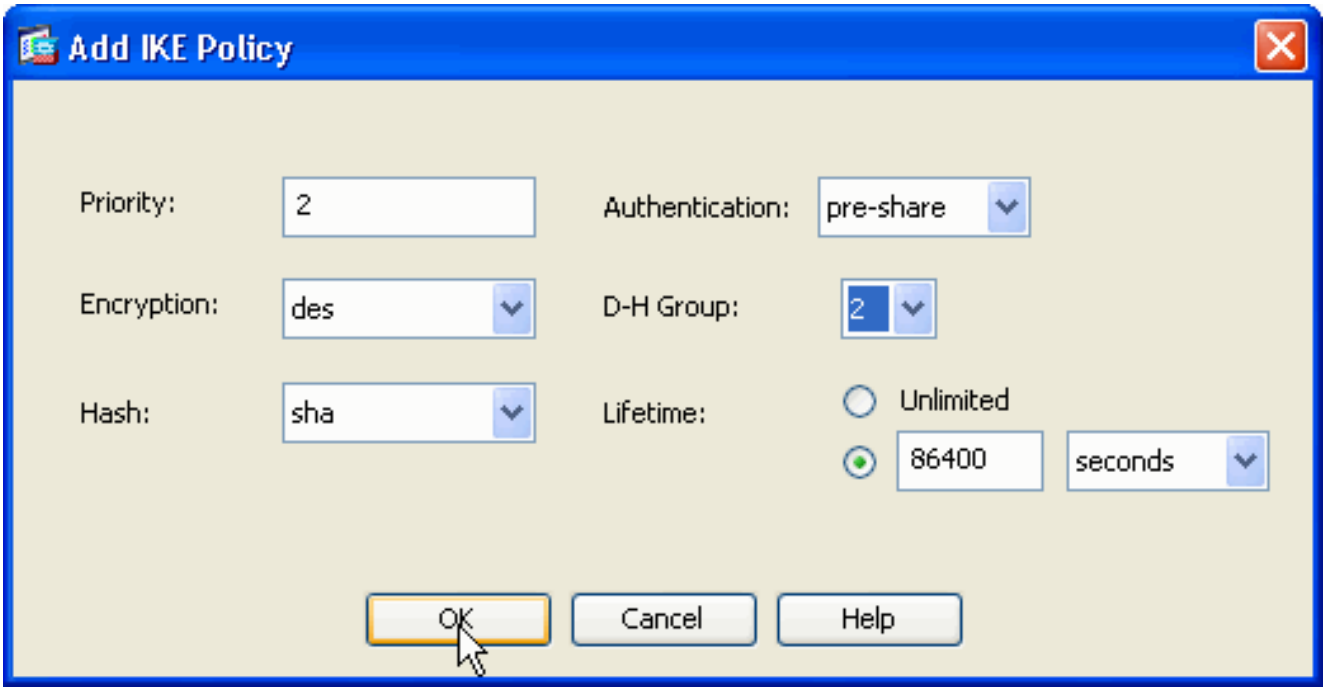
Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Настройка VPN для удаленного доступа (IPSec)

Порядок действий в диспетчере ASDM

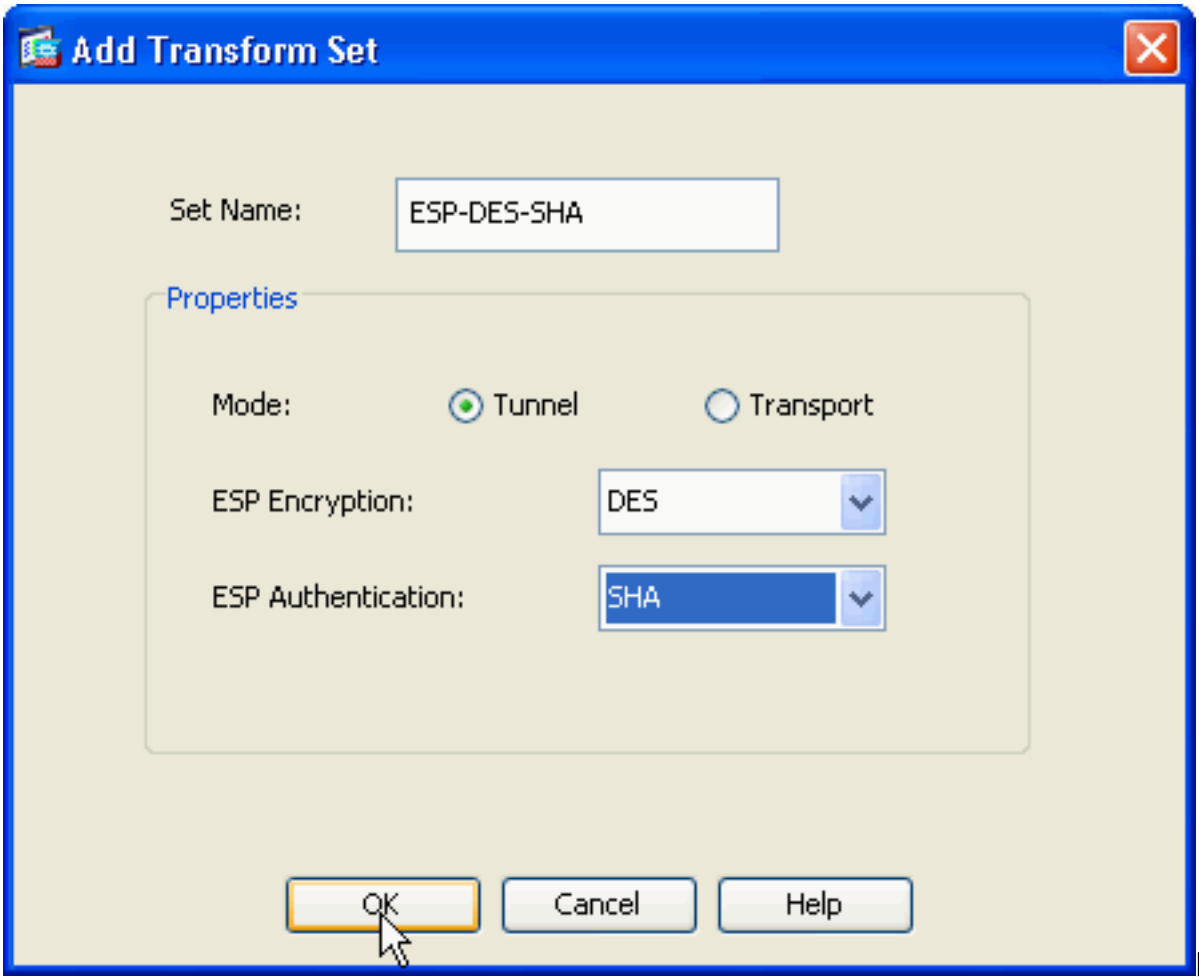
Выполните эти шаги, чтобы настроить удаленный доступ через сеть VPN:

1. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> IPSec> IKE Policies> Add** для создания Политики ISAKMP 2, как показано.



Нажмите кнопку OK и Apply.

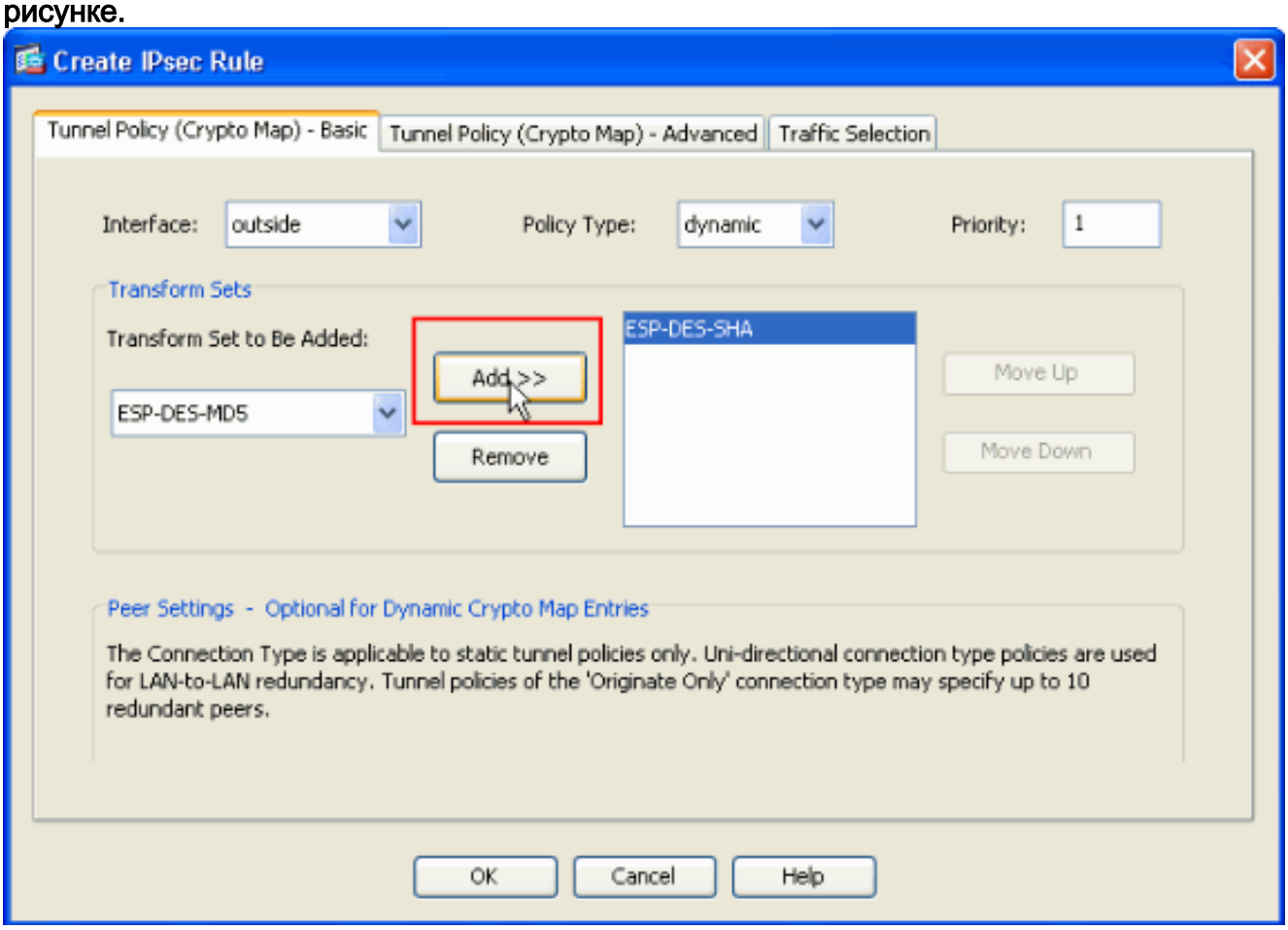
2. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> IPSec> IPSec Transform Sets> Add** для создания набора преобразований **SHA ESP-DES**, как показано.



Нажмите кнопку OK и Apply.

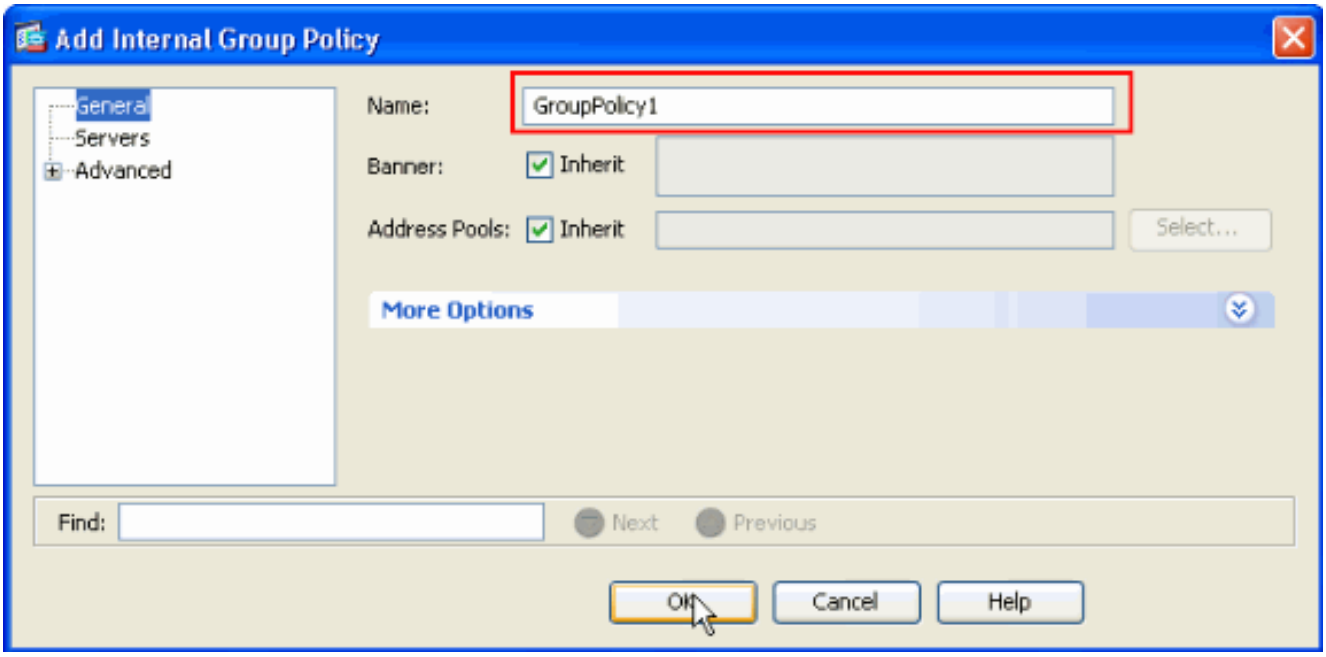
3. **Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add (Конфигурация > VPN для удаленного доступа > Сетевой (клиентский) доступ > Дополнительно > IPSec > Криптографические**

карты > Добавить), чтобы создать криптографическую карту с приоритетом динамической политики равным 1, как показано на рисунке.



Нажмите кнопку OK и Apply.

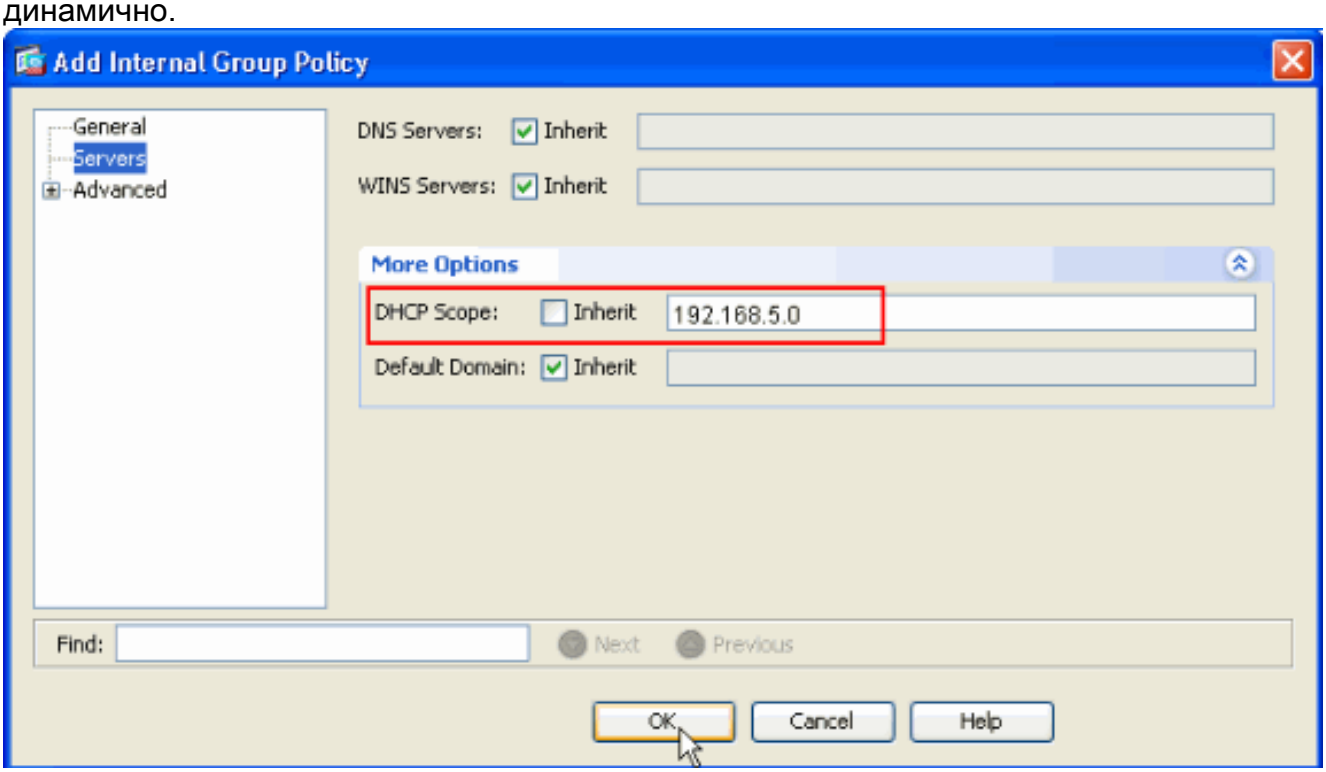
4. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> Group Policies> Add> Internal Group Policies** для создания групповой политики (Например, **GroupPloicy1**), как показано.



Нажмите кнопку OK и Apply.

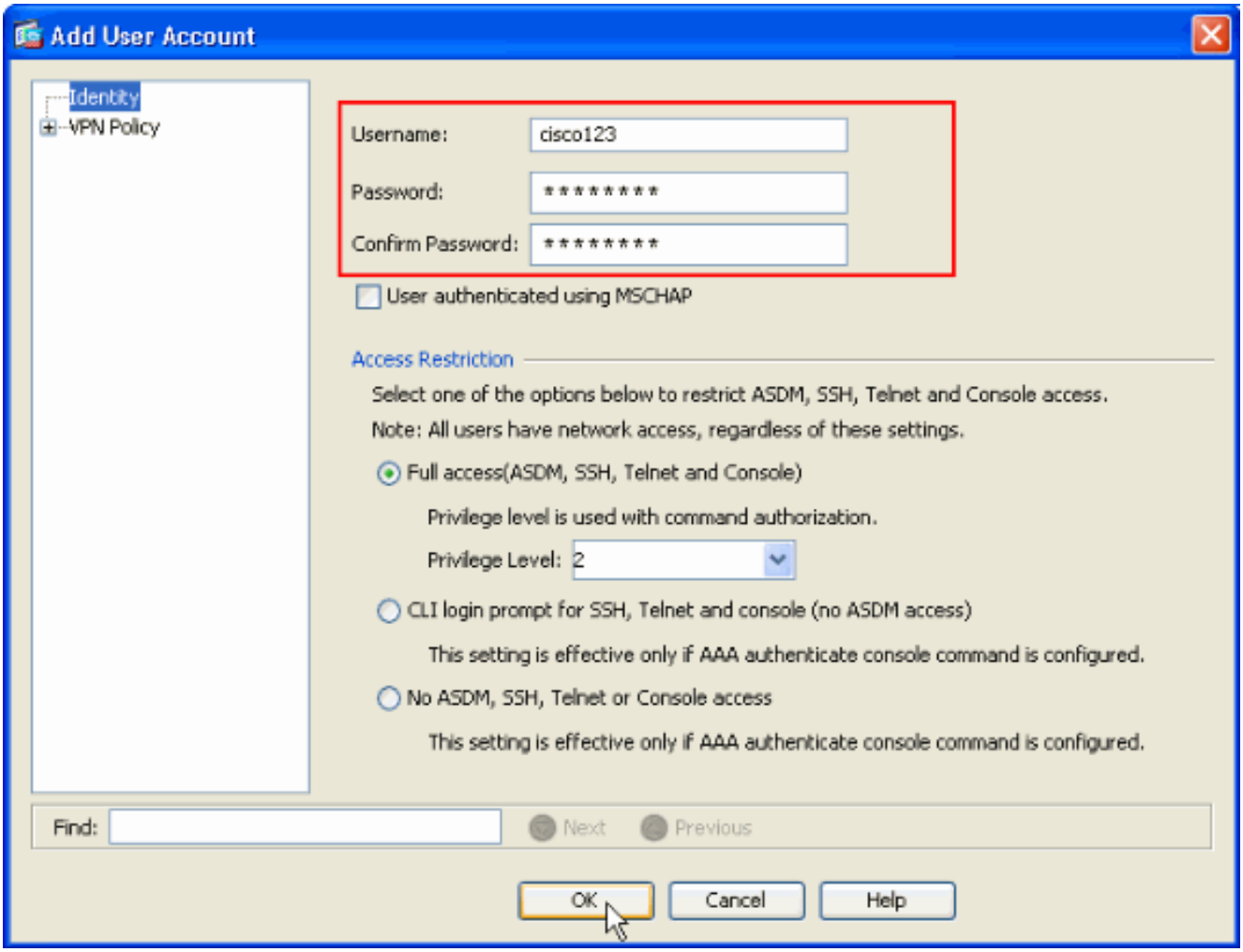
5. Выберите **Configuration> Remote Access VPN> Network (Client) Access> Advanced> Group Policies> Add> Internal Group Policies> Servers>>** для настройки **Области DHCP**

для Пользователей VPN-клиента, которые будут назначены динамично.

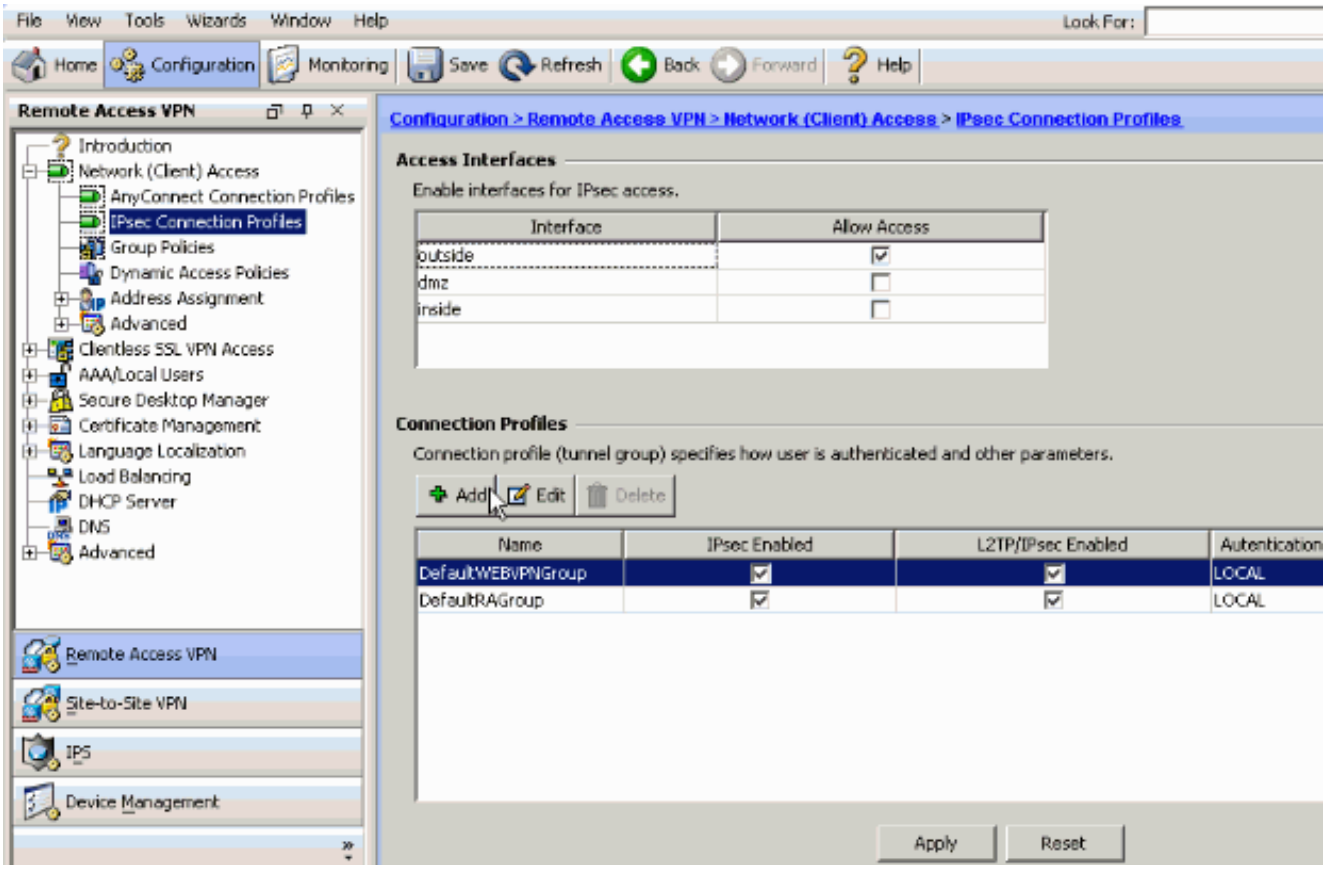


Нажмите кнопку OK и Apply.Примечание: Конфигурация Области DHCP является дополнительной. См. Адресацию DHCP Настройки для получения дополнительной информации.

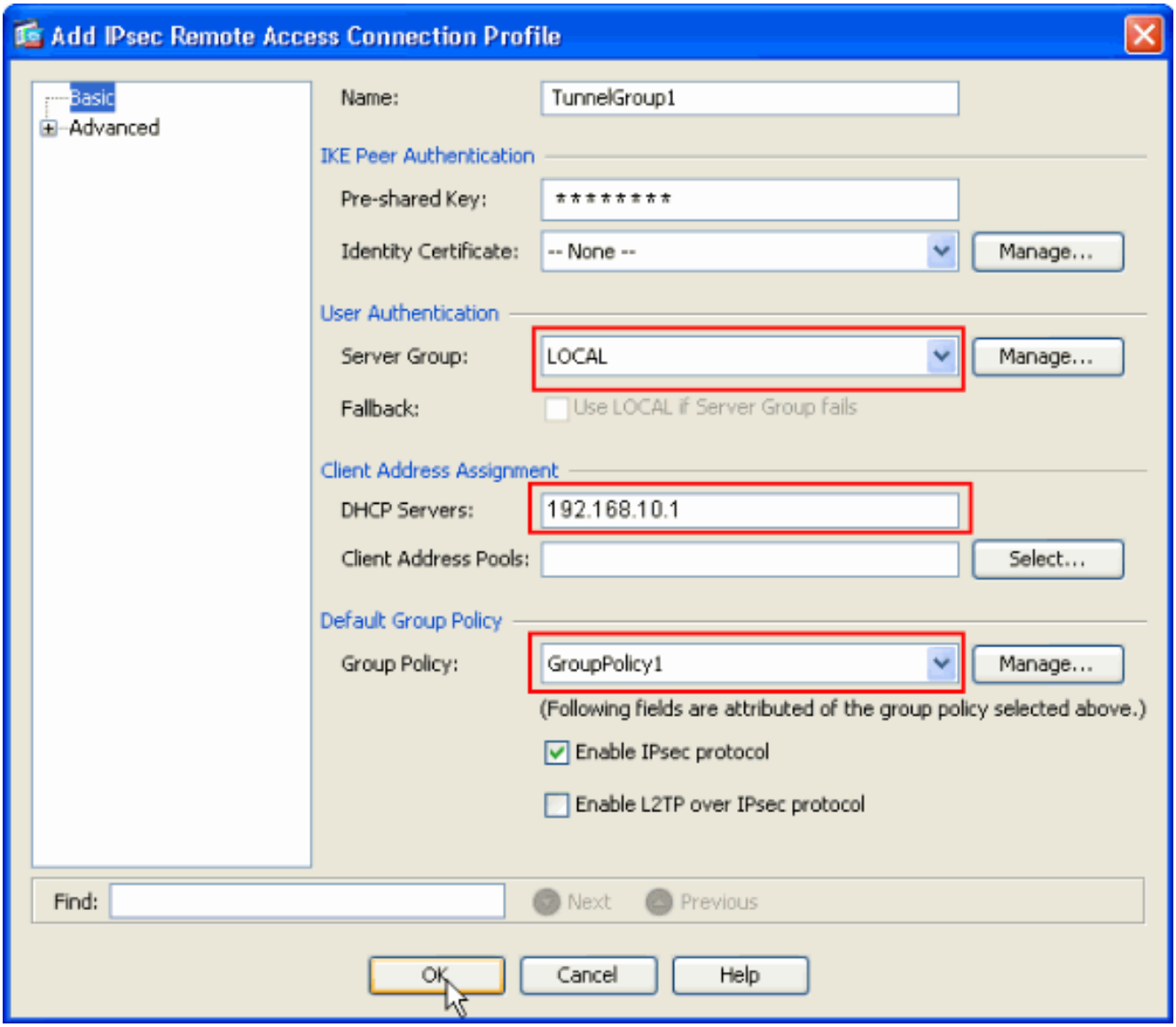
6. Выберите **Configuration> Remote Access VPN> AAA Setup> Local Users> Add** для создания учетной записи пользователя (например, имя пользователя - cisco123 и Пароль - cisco123) для доступа клиента VPN.



7. Выберите **Configuration> Remote Access VPN> Network (Client) Access> IPSec Connection Profiles> Add>** для добавления туннельной группы (например, **TunnelGroup1** и Общий ключ как cisco123), как показано.

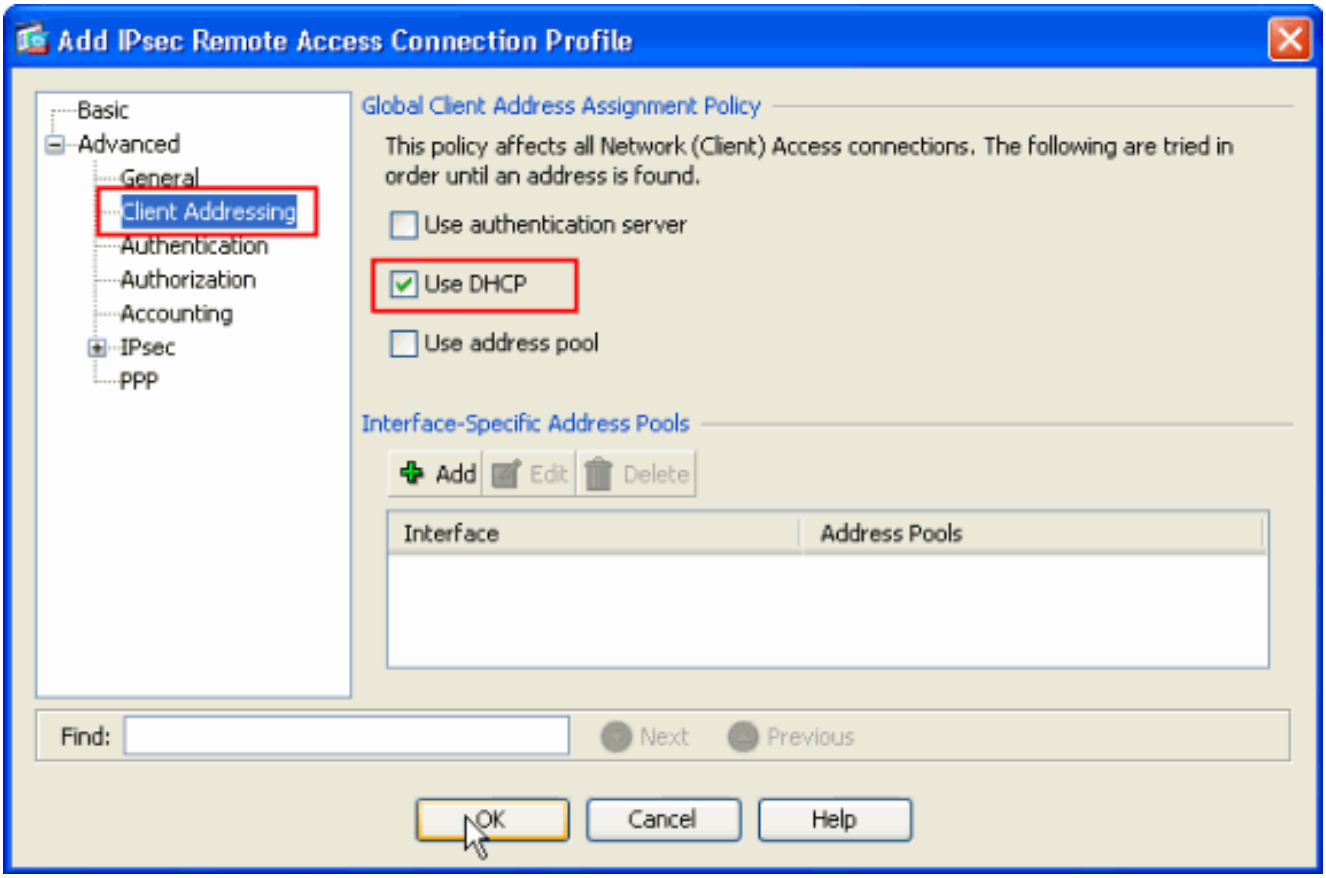


Под **Basic** вкладка выбирают группу серверов в качестве **ЛОКАЛЬНОЙ** для поля User Authentication.Выберите **Grouppolicy1** в качестве Групповой политики для поля Policy Группы по умолчанию.Предоставьте IP - адрес сервера DHCP в пространстве, обеспечил **Серверы**
DHCP.



Нажмите кнопку ОК.

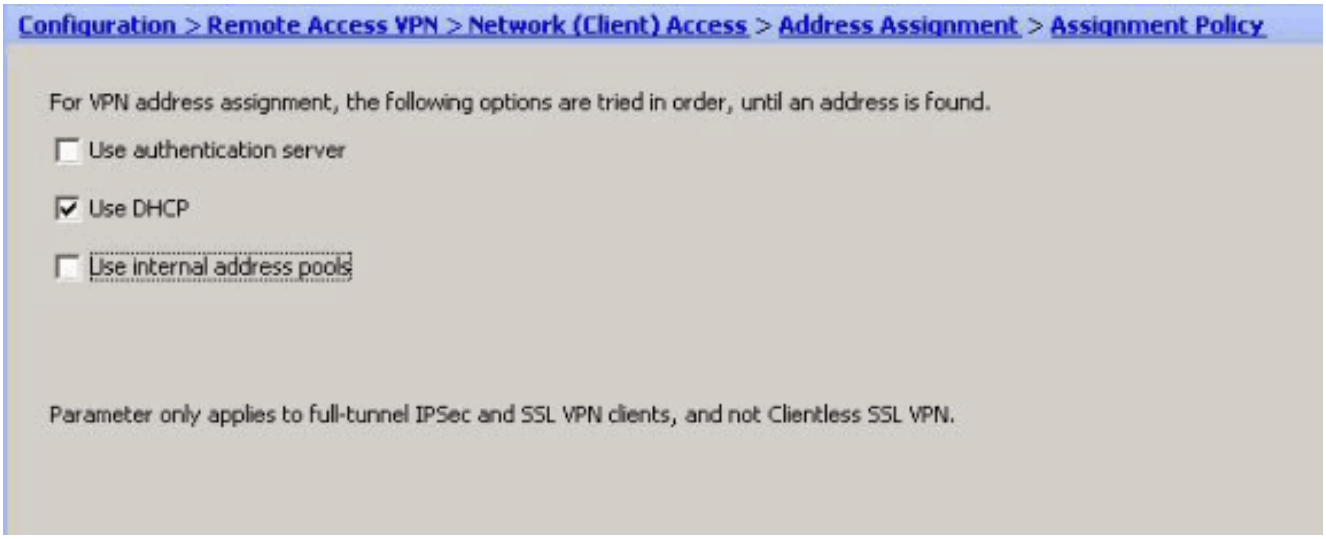
8. Выберите **Advanced> Client Addressing>** и проверьте флажок **Use DHCP** для сервера DHCP для присвоения IP-адреса на клиенты VPN.**Примечание:** Удостоверьтесь, что сняли флажок с флажками для **сервера проверки подлинности Использования** и **пула адресов**
Использования.



Конфигурация для ASDM 6. x

Та же конфигурация ASDM хорошо работает с версией 6.x ASDM, за исключением некоторых незначительных модификаций с точки зрения путей ASDM. Пути ASDM к определенным полям имели различие от версии 6.2 ASDM и позже. Модификации наряду с существующими путями упомянуты ниже. Здесь графические изображения не подключены в случаях, где они остаются тем же для всех главных версий ASDM.

1. Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)> Усовершенствованный> IPSec> Наборы правил IKE> Добавляет
2. Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)> Усовершенствованный> IPSec> Команды IPsec transform set> Добавляет
3. Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)> Усовершенствованный> IPSec> Криптокарты> Добавляет
4. Выберите Configuration> Remote Access VPN> Network (Client) Access> Group Policies> Add> Internal Group Policies
5. Выберите Configuration> Remote Access VPN> Network (Client) Access> Group Policies> Add> Internal Group Policies> Servers
6. Выберите Configuration> Remote Access VPN> AAA Setup/Local Users> Local Users> Add
7. Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)> Профили IP - безопасного соединения> Добавляет
8. Выберите Configuration> Remote Access VPN> Network (Client) Access> Address Assignment> Assignment
   Policy



Все эти три опции включены по умолчанию. Cisco ASA придерживается того же заказа назначить адреса на клиенты VPN. При снятии выделения с другими двумя опциями Cisco ASA не проверяет опции сервер и local pool aaa. Включенные опции по умолчанию могут быть проверены **командой show run all | in vpn-add**. Это - пример выходных данных для вашей ссылки:`vpn-addr-assign aaa`
`vpn-addr-assign dhcp`
`vpn-addr-assign local reuse-delay 0`Для получения дополнительной информации об этой команде, обратитесь к [vpn-addr-assign](#).

Настройте ASA/PIX с помощью CLI

Выполните эти шаги для настройки сервера DHCP для обеспечения IP-адреса клиентам VPN из командной строки. Дополнительные сведения о каждой из используемых команд см. в документах Настройка сетей VPN для удаленного доступа и Справочник по командам устройств адаптивной защиты Cisco ASA серии 5500.

Выполнение Config на устройстве ASA

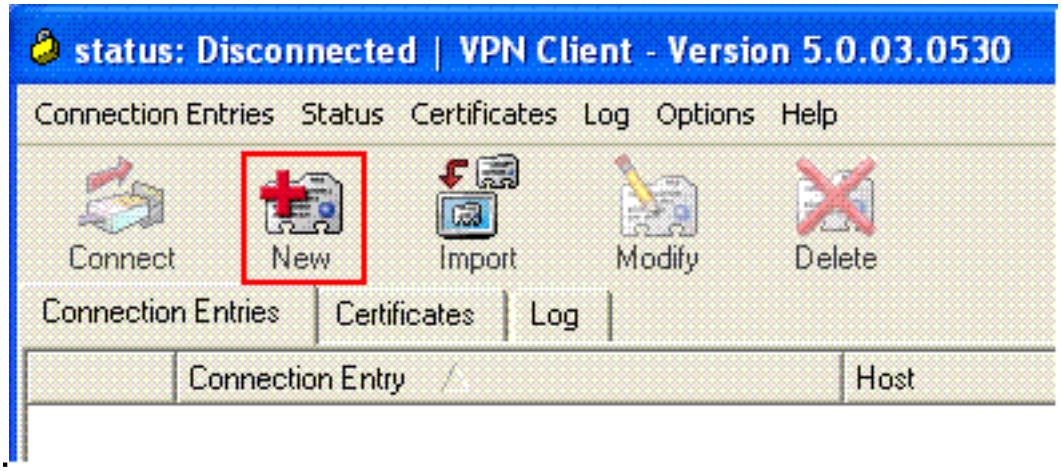
```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 !--- Specify the location of the ASDM image for
ASA to fetch the image for ASDM access. asdm image
disk0:/asdm-613.bin no asdm history enable arp timeout
14400 global (outside) 1 192.168.1.5 nat (inside) 0
access-list 101 nat (inside) 1 0.0.0.0 0.0.0.0 route
outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate
```

```
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command. no vpn-addr-assign aaa no
vpn-addr-assign local telnet timeout 5 ssh timeout 5
console timeout 0 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
! group-policy GroupPolicy1 internal group-policy
GroupPolicy1 attributes !--- define the DHCP network
scope in the group policy.This configuration is Optional
dhcp-network-scope 192.168.5.0 !--- In order to identify
remote access users to the Security Appliance, !--- you
can also configure usernames and passwords on the
device. username cisco123 password ffIRPGpDSOJh9YLq
encrypted !--- Create a new tunnel group and set the
connection !--- type to remote-access. tunnel-group
TunnelGroup1 type remote-access !--- Define the DHCP
server address to the tunnel group. tunnel-group
TunnelGroup1 general-attributes default-group-policy
GroupPolicy1 dhcp-server 192.168.10.1 !--- Enter the
pre-shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

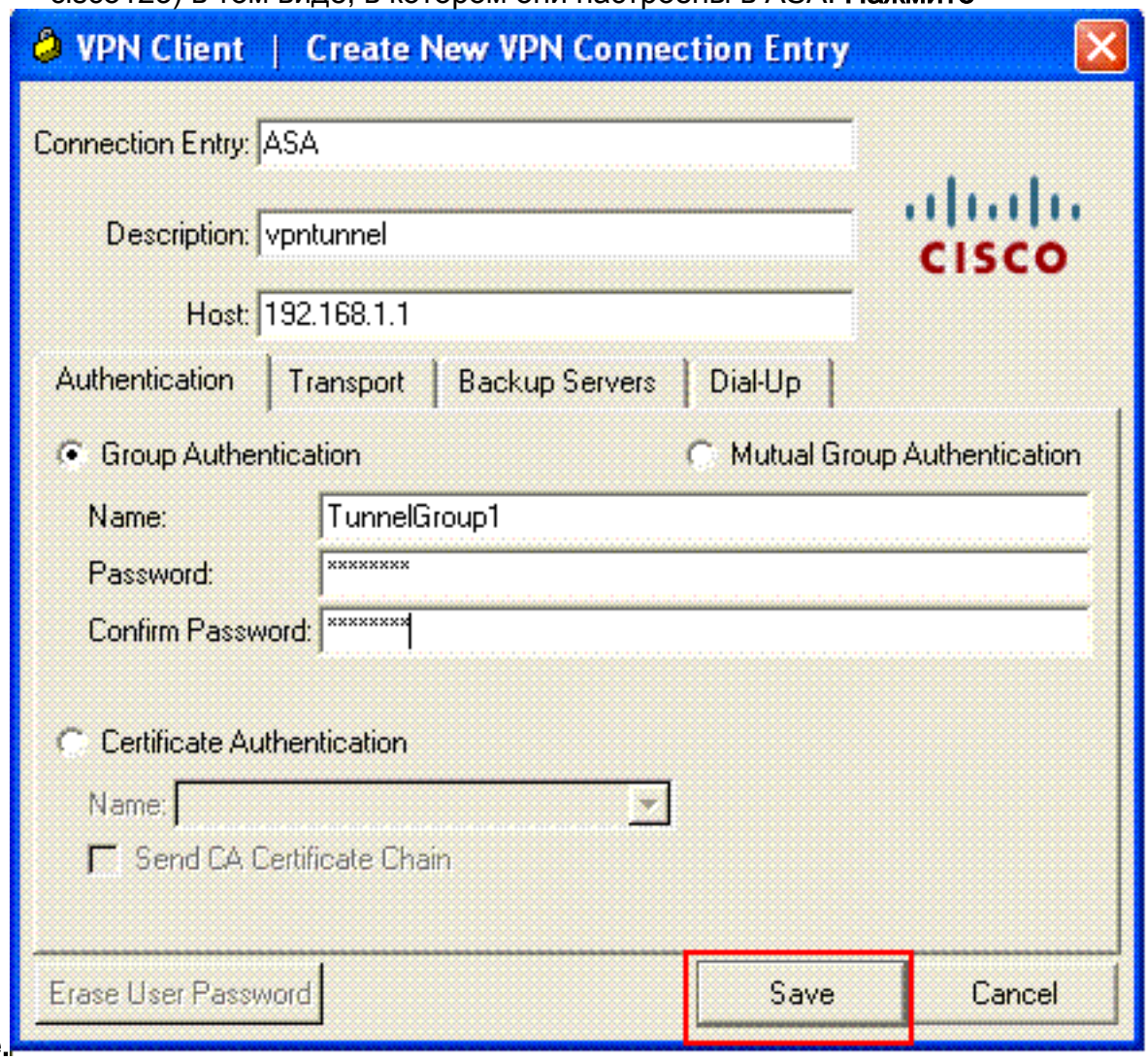
Настройка VPN-клиента Cisco VPN Client

Попытайтесь соединиться с Cisco ASA с помощью Cisco VPN Client, чтобы проверить, что успешно настроен ASA.

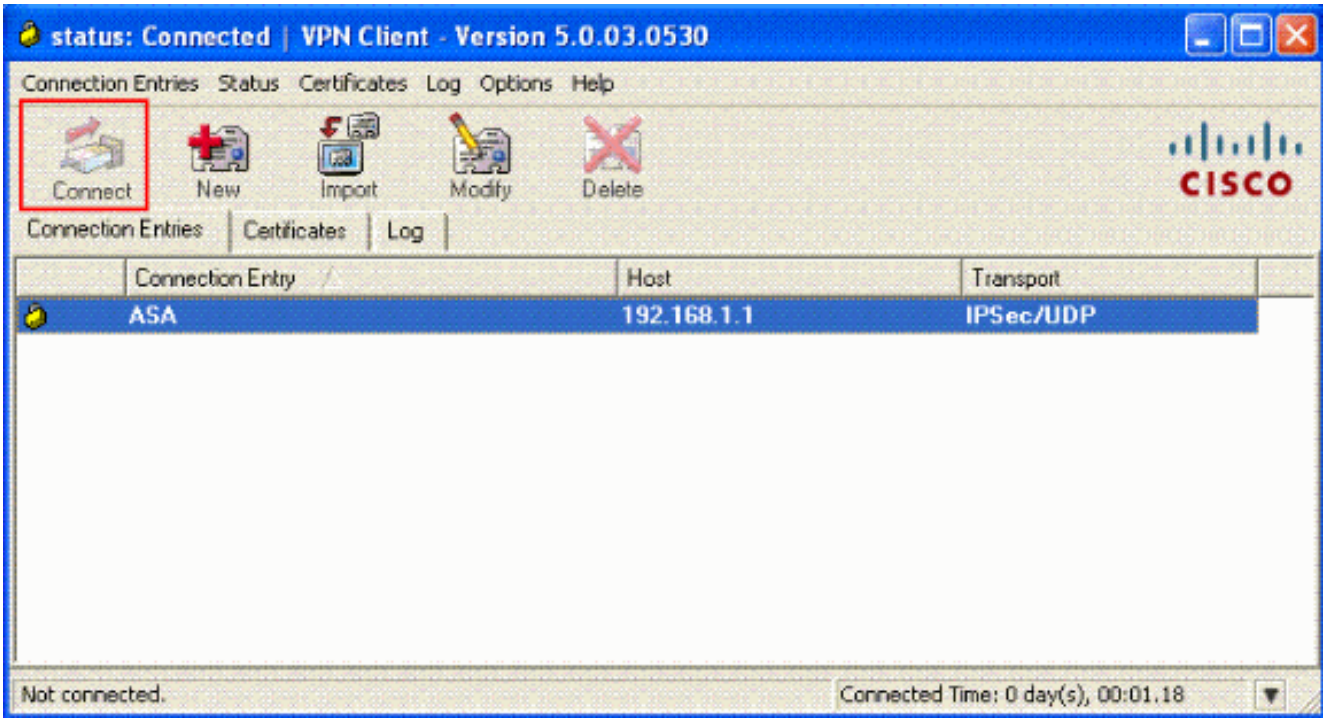
1. Выберите **Start> Programs> Cisco Systems VPN Client> VPN Client**.
2. **Нажмите кнопку New (Создать), чтобы открыть окно Create New VPN Connection Entry (Создание записи нового VPN-**



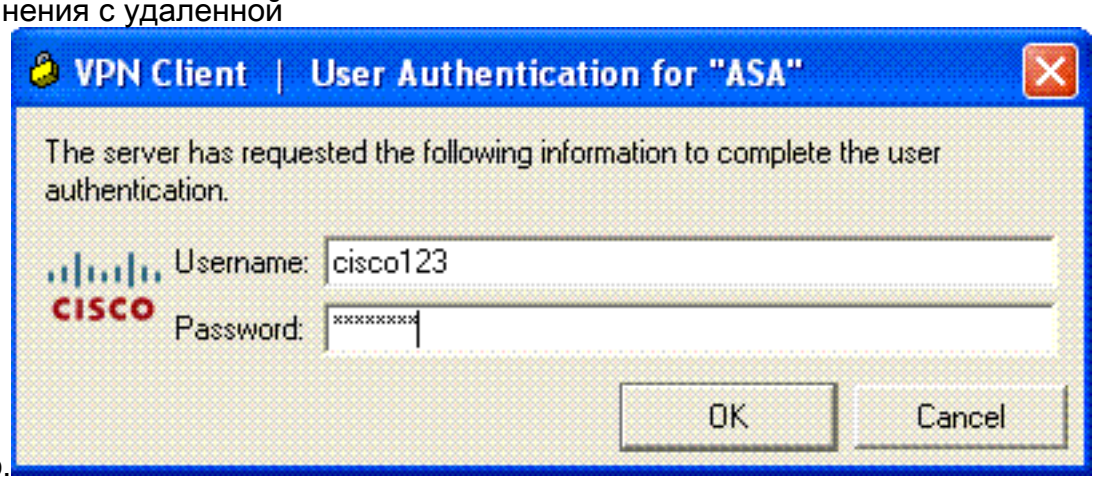
подключения).
3. Введите данные нового подключения.Введите имя записи и описание подключения. **Введите внешний IP-адрес устройства ASA в поле Host (Хост).** Затем введите имя (TunnelGroup1) группы туннеля сети VPN и пароль (предварительно согласованный ключ — cisco123) в том виде, в котором они настроены в ASA. **Нажмите**



Save.
4. Щелкните по соединению, вы хотите использовать и нажать **Connect** от главного окна VPN
Client.

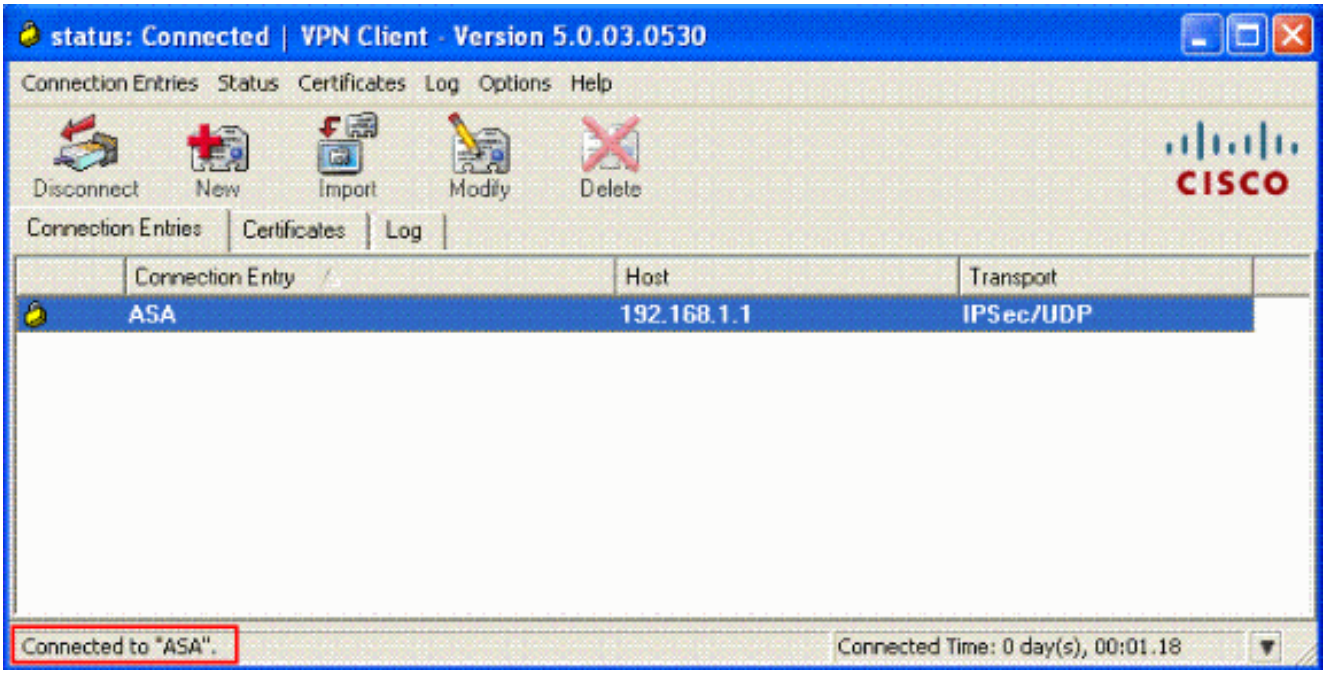


5. **При появлении приглашения введите имя пользователя Username : cisco123** и **Пароль: cisco123** согласно конфигурации в ASA выше для xauth, и нажимает **OK** для соединения с удаленной

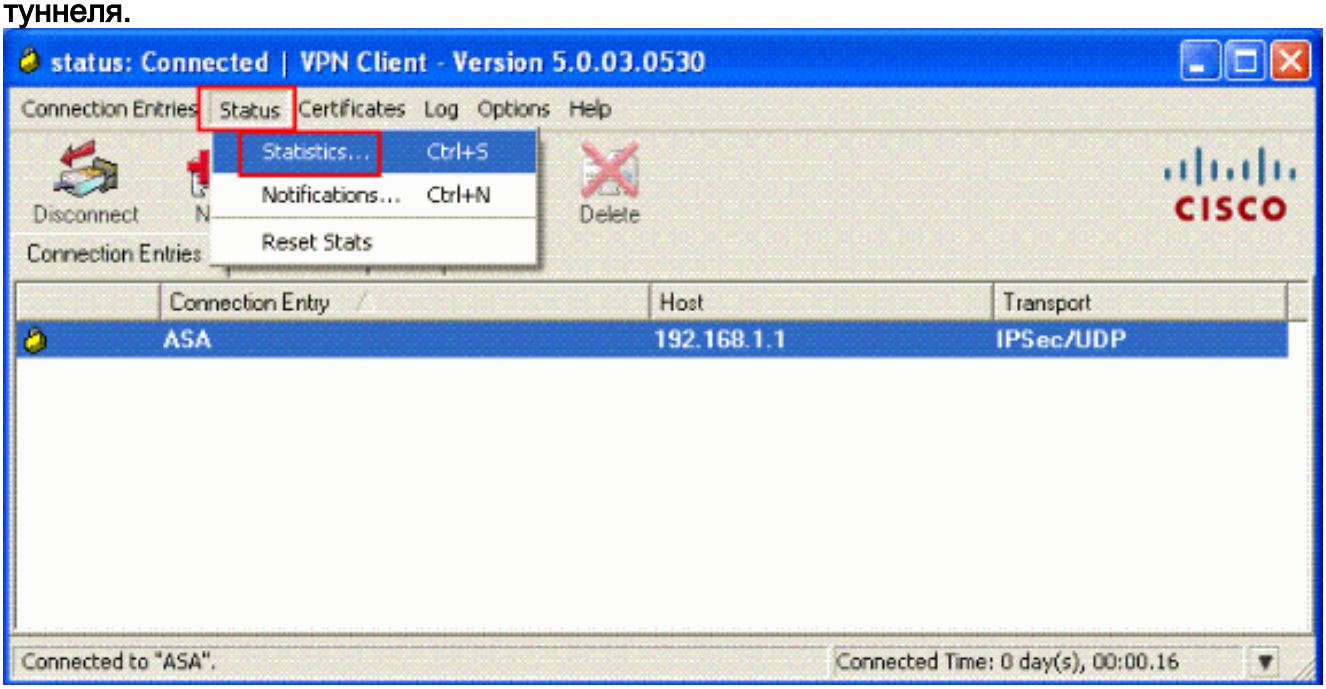


сетью.

6. ПО VPN Client соединится с устройством ASA на центральном узле.



7. После успешного установления соединения выберите пункт Статистика в меню Status ("Состояние"), чтобы проверить данные туннеля.



Проверка

команды "show"

Используйте этот раздел, чтобы подтвердить, что ваша конфигурация работает должным образом.

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

- show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.

- **show crypto ipsec sa—отображает параметры, используемые текущими SA.**

```
ASA #show crypto ipsec sa interface: outside Crypto map tag: dynmap, seq num: 10, local addr:
192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0) current_peer: 192.168.1.2, username:
cisco123 dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 55, #pkts encrypt: 55, #pkts
digest: 55 #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag
successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0,
#decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.:
192.168.1.1, remote crypto endpt.: 192.168.1.2 path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: C2C25E2B inbound esp sas: spi: 0x69F8C639 (1777911353) transform: esp-des
esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa
timing: remaining key lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y
outbound esp sas: spi: 0xC2C25E2B (3267517995) transform: esp-des esp-md5-hmac none in use
settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa timing: remaining key
lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y ASA #show crypto isakmp sa
Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE
SA: 1 1 IKE Peer: 192.168.1.2 Type : user Role : responder Rekey : no State : AM_ACTIVE
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации. Также показан пример выходных данных команды debug.

Примечание: Для получения дополнительной информации об устранении проблем IPSec VPN Удаленного доступа обращаются Решения для Устранения проблем IPSEC VPN Наиболее распространенного соединения L2L и Удаленного доступа

Очистка ассоциаций безопасности

Когда вы устраняете неполадки, удостоверьтесь, что очистили существующие Сопоставления безопасности после внесения изменения. В привилегированном режиме PIX используйте следующие команды:

- **clear [crypto] ipsec sa— удаляет все активные ассоциации безопасности IPSec.** Ключевое слово crypto является необязательным.
- **clear crypto isakmp sa— удаляет активные ассоциации безопасности IKE.** Ключевое слово crypto является необязательным.

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".

- **debug crypto ipsec 7 – отображает связь IPsec этапа 2.**
- **debug crypto isakmp 7 — отображает процесс установления связи по протоколу ISAKMP на этапе 1.**

Пример результата отладки

- ASA 8. 0
- Клиент VPN 5.0 для Windows

ASA 8. 0

ASA#**debug crypto isakmp 7** Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le ngth : 856 Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ISA_KE payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received xauth V6 VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Fragmentation VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included IKE fragmenta tion capability flags: Main Mode: True Aggressive Mode: False Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received NAT-Traversal ver 02 V ID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun nelGroup1 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g IKE SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr oposal # 1, Transform # 13 acceptable Matches global IKE entry # 2 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ISAKMP SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing nonce payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin g keys for Responder... Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Cisco Unity VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing xauth V6 VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing dpd vid payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Fragmentation VID + extended capabilities payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti ga/Cisco VPN3000/Cisco ASA GW VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le ngth : 368 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 116 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g notify payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing blank hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing qm hash payload Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a 1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8 a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a ttr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP =

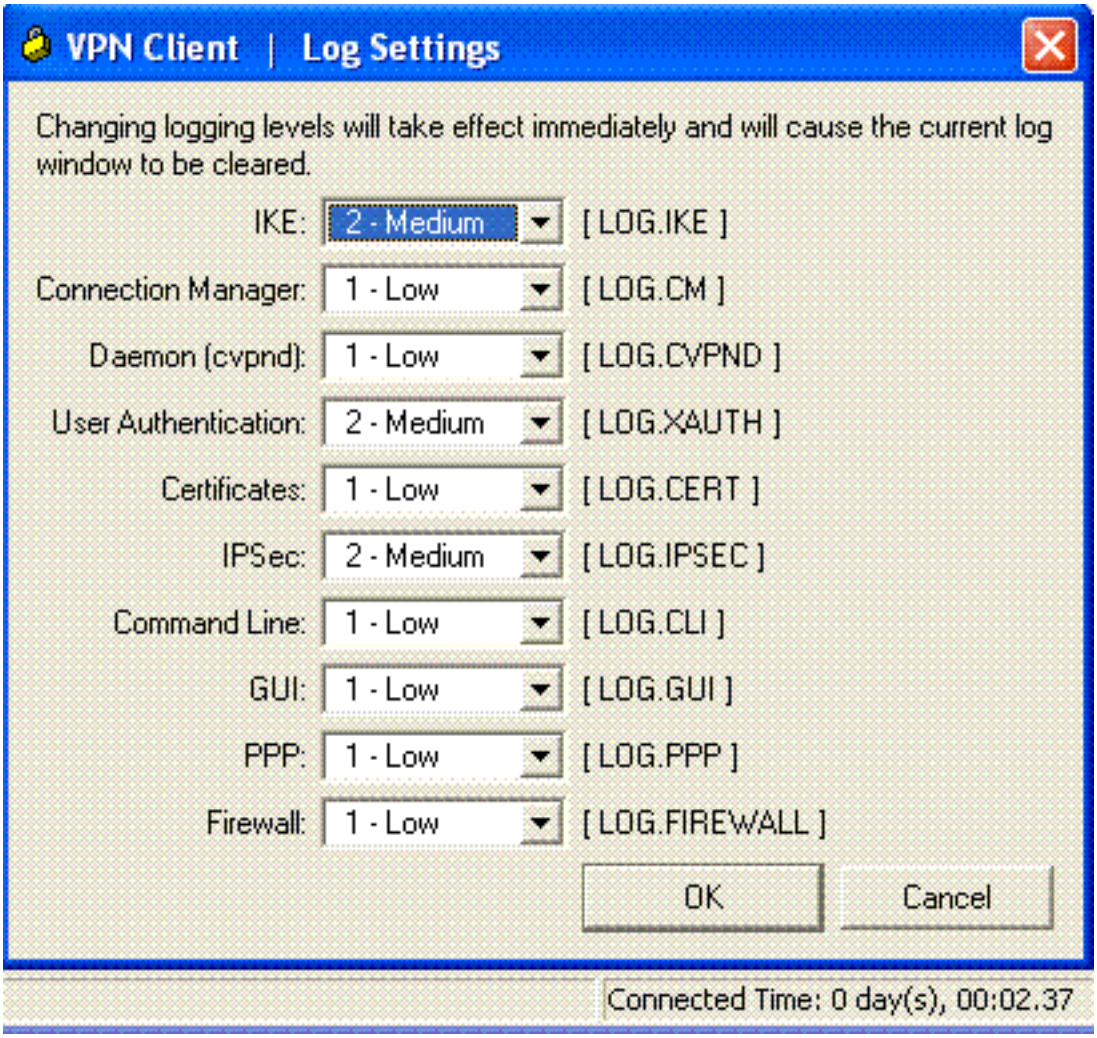
192.168.1.2, Processin g MODE_CFG Reply attributes. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: IP Compression = disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, User (cisco123) authenticated. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143 60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14 360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg ACK attributes Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26 63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg Request attributes Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 net mask! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DNS server address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for WINS server address! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received unsupported transaction mode attribute: 5 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Banner! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Save PW setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Default Domain Name! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Split Tunnel List! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Split DNS! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for PFS setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received unknown transaction mode attribute: 28684 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Application Version! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Client Type: WinNT Client Application Version: 5.0.03.0530 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for FWTYPE! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12 3! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for UDP Port! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e nabled) Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Assigned private IP address 192.168.5.1 to remote user Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Send Client Browser Proxy Attributes! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu ded in the mode-cfg reply Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username =

cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266 3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, **PHASE 1 COMPLETED** Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Starting P1 rekey timer: 950 seconds. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, sending notify message Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44 35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received remote Proxy Host data in ID Payload: Address 192.168.5.1, Proto col 0, Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, QM IsRekeyed old sa not found by addr Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, IKE Remote Peer configured for crypto map: dynmap Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing IPSec SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IPSec SA Proposal # 14, Transform # 1 acceptable Matches global IPS ec SA entry # 10 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, IKE: requesting SPI! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, oakley constucting quick mode Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec SA payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon ds Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing proxy ID Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Transmitting Proxy Id: Remote host: 192.168.5.1 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541 f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, loading all IPSEC SAs Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Security negotiation complete for User (cisco123) Responder, Inbound SPI = 0x31de01d8, Outbound SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username =

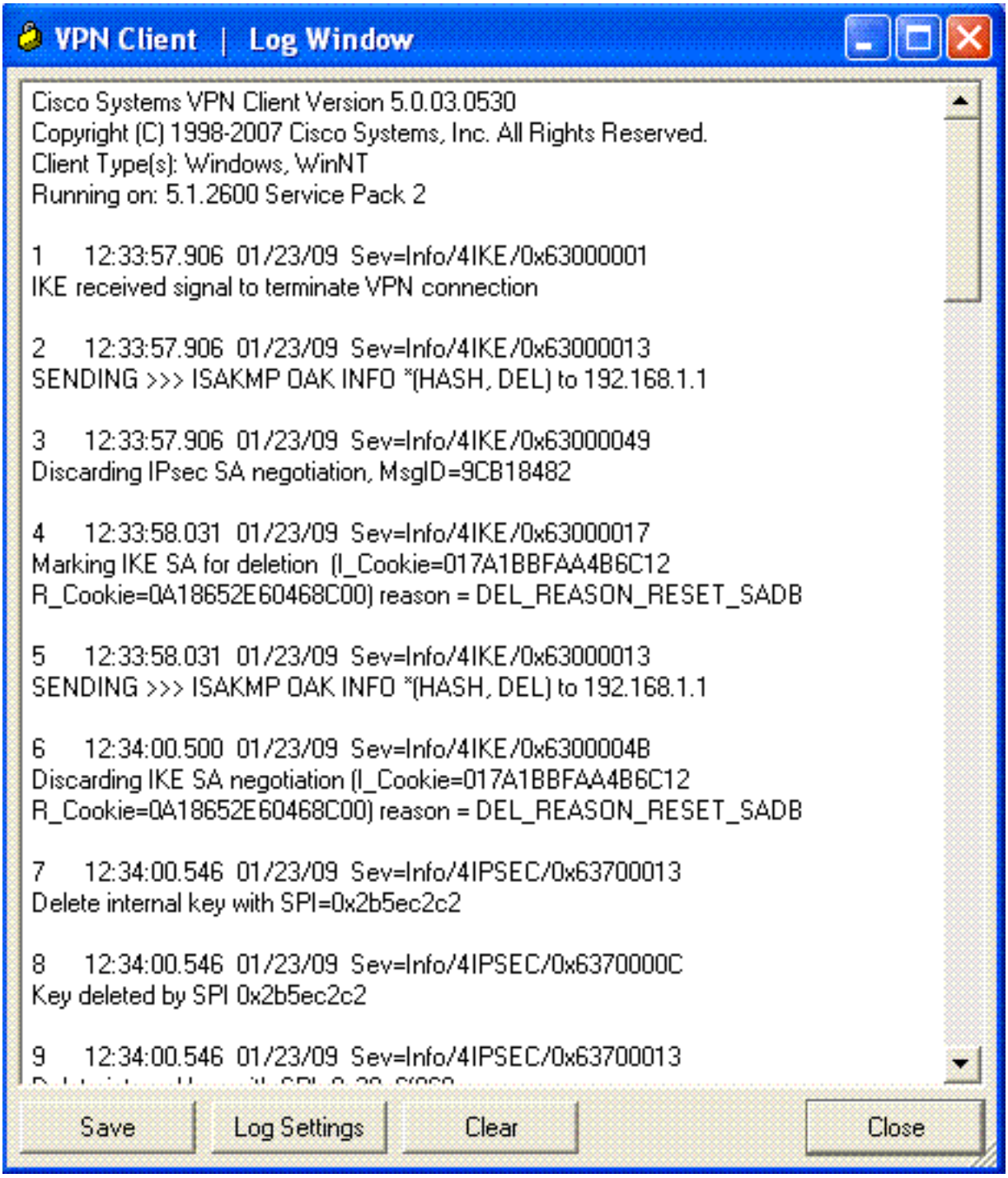
```
cisco123, IP = 1 92.168.1.2, Starting P2 rekey timer: 27360 seconds. Jan 22 22:21:31 [IKEv1]:
Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Adding static route for client
address: 192.168.5.1 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP =
192.168 .1.2, PHASE 2 COMPLETED (msgid=541f8e43) Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2,
IKE_DECODE RECEIVED Message (msgid=78 f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) +
NONE (0) total length : 8 0 ASA#debug crypto ipsec 7 !--- Deletes the old SAs. ASA# IPSEC:
Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: Deleted inbound permit
rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A
Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C
IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Deleted outbound
permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Deleted outbound VPN context, SPI
0xC921E280 VPN handle: 0x00040AB4 !--- Creates new SAs. ASA# IPSEC: New embryonic SA created @
0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI : 0x7F3C985A Session ID: 0x0000F000 VPIF num
: 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA
created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound SPI : 0xC921E280 Session ID:
0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC:
Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating outbound VPN context, SPI 0xC921E280
Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer :
0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI
0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound encrypt rule, SPI 0xC921E280 Src addr:
0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask: 255.255.255.255 Src ports Upper: 0
Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false
SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0xC921E280 Rule ID:
0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src addr: 192.168.1.1 Src mask:
255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op :
ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0xC921E280
Use SPI: true IPSEC: Completed outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC:
Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating inbound VPN context, SPI 0x7F3C985A
Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0 bytes VCID : 0x00000000 Peer :
0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed inbound VPN context, SPI
0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context 0x00040AB4, SPI
0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000
Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context,
SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner rule, SPI 0xC921E280 Rule
ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280 Rule ID: 0xD5123250
IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr: 192.168.5.1 Src mask:
255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst
ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI:
false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: New
inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr:
192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0
Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: New inbound permit
rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst
mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op :
ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound
permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0
```

Клиент VPN 5.0 для Windows

Выберите **Log> Настройки журнала** для включения регистрационных уровней в Клиенте VPN.



Выберите **Log> Log Window** для просмотра записей журнала в Клиенте VPN.



Дополнительные сведения

- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- Справочники по командам устройств адаптивной защиты Cisco ASA серии 5500
- Страница поддержки устройств защиты Cisco PIX серии 500
- Справочник по командам устройств защиты Cisco PIX серии 500
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Страница технической поддержки протоколов согласования IPSec и IKE
- Страница поддержки Cisco VPN Client
- Cisco Systems – техническая поддержка и документация