

ASA 8. x: Разрешить отдельное туннелирование для VPN Client AnyConnect на примере конфигурации ASA

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Настройка ASA при помощи ASDM 6.0\(2\)](#)

[Конфигурация ASA в интерфейсе командной строки](#)

[Установка соединения SSL VPN с SVC](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

[Введение](#)

В этом документе приведены пошаговые инструкции, как разрешить VPN-клиентам Cisco AnyConnect доступ в Интернет в то время, как их трафик туннелируется в модуль Cisco Adaptive Security Appliance (ASA) 5500. Эта конфигурация обеспечивает VPN-клиентам безопасный доступ к корпоративным ресурсам по протоколу SSL и небезопасный доступ в Интернет с помощью отдельного туннелирования.

[Предварительные условия](#)

[Требования](#)

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Устройство адаптивной защиты ASA с ПО версии 8.x
- Cisco AnyConnect VPN Client версии 2.x **Примечание:** Загрузите пакет Клиента AnyConnect VPN Client (anyconnect-win*.pkg) от [Загрузки Программного обеспечения Cisco \(только зарегистрированные клиенты\)](#). Скопируйте VPN-клиент AnyConnect во флэш-память ASA, из которой он должен загружаться на удаленные компьютеры

пользователей для установления VPN-соединения по протоколу SSL с устройством ASA. [Для получения дополнительных сведений о настройке обратитесь к разделу Установка клиента AnyConnect руководства по настройке ASA.](#)

Используемые компоненты

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

- Устройство адаптивной защиты Cisco серии ASA 5500, на котором установлено ПО версии 8.0(2)
- Cisco AnyConnect SSL VPN Client версии 2.0.0343 для Windows
- На ПК должна быть установлена ОС Microsoft Vista, Windows XP SP2 или Windows 2000 Professional SP4 с установщиком Microsoft версии 3.1
- Cisco Adaptive Security Device Manager (ASDM) версии 6.0(2)

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.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

Общие сведения

Cisco AnyConnect VPN Client предоставляет удаленным пользователям безопасный доступ к устройству защиты с помощью SSL-подключений. Без ранее установленного клиента удаленные пользователи в своем браузере вводят IP-адрес интерфейса, настроенного на прием VPN-соединений по протоколу SSL. Если устройство защиты не настроено перенаправлять запрос с адреса http:// на https://, пользователям необходимо будет вводить URL-адрес в виде https://<адрес>.

После ввода URL-адреса, браузер подключается к интерфейсу и отображает окно входа в систему. Если пользователь выполнит вход в систему и пройдет аутентификацию, то устройство защиты определит, что ему необходим клиент, после чего загрузит на удаленный компьютер ту версию клиента, которая соответствует его ОС. После загрузки выполняется установка клиента и его автоматическая настройка, после чего устанавливается безопасное SSL-соединение. После завершения соединения либо клиент остается, либо выполняется его автоматическое удаление (в зависимости от конфигурации устройства защиты).

При наличии ранее установленного клиента после прохождения пользователем аутентификации устройство защиты проверяет версию клиента и при необходимости обновляет его.

Когда клиент устанавливает VPN-соединение с устройством защиты по протоколу SSL, он подключается с помощью протокола TLS либо DTLS. Использование протокола DTLS позволяет избежать проблем, вызванных задержками и полосой пропускания, связанными с

некоторыми SSL-соединениями, а также позволяет улучшить производительность приложений, работающих в режиме реального времени, чувствительных к задержкам пакетов.

Клиент AnyConnect можно загрузить с устройства защиты, или он может быть установлен на удаленном ПК вручную системным администратором. См. [руководство для администратора клиента VPN Cisco AnyConnect](#) для получения дополнительной информации о том, как установить клиента вручную.

Устройство защиты производит загрузку клиента на основе групповой политики или атрибутов пользователя, устанавливающего соединение. Можно настроить устройство защиты на автоматическую загрузку клиента или можно его настроить выдавать удаленному пользователю запрос, устанавливать клиент или нет. Можно настроить устройство защиты загружать клиент после завершения времени ожидания ответа пользователя или при отображении страницы входа в систему.

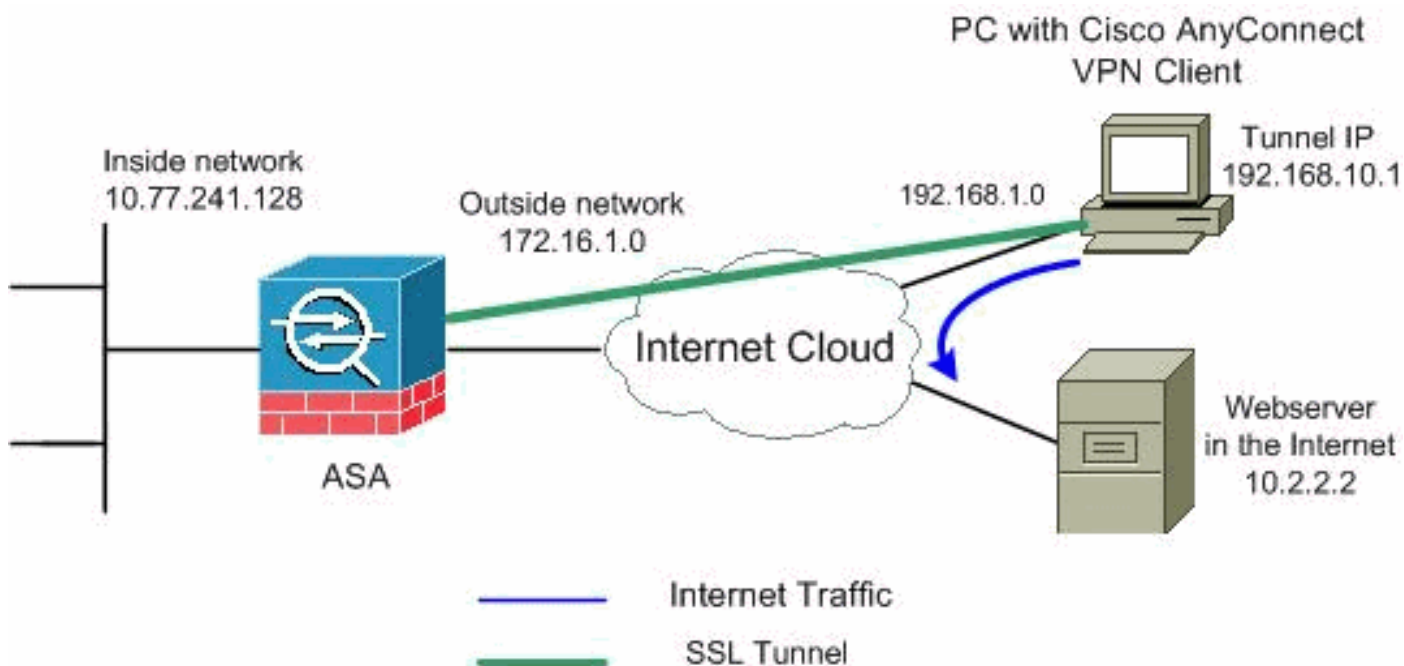
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом 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:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. [Это адреса RFC 1918, используемые в лабораторной среде.](#)

Настройка ASA при помощи ASDM 6.0(2)

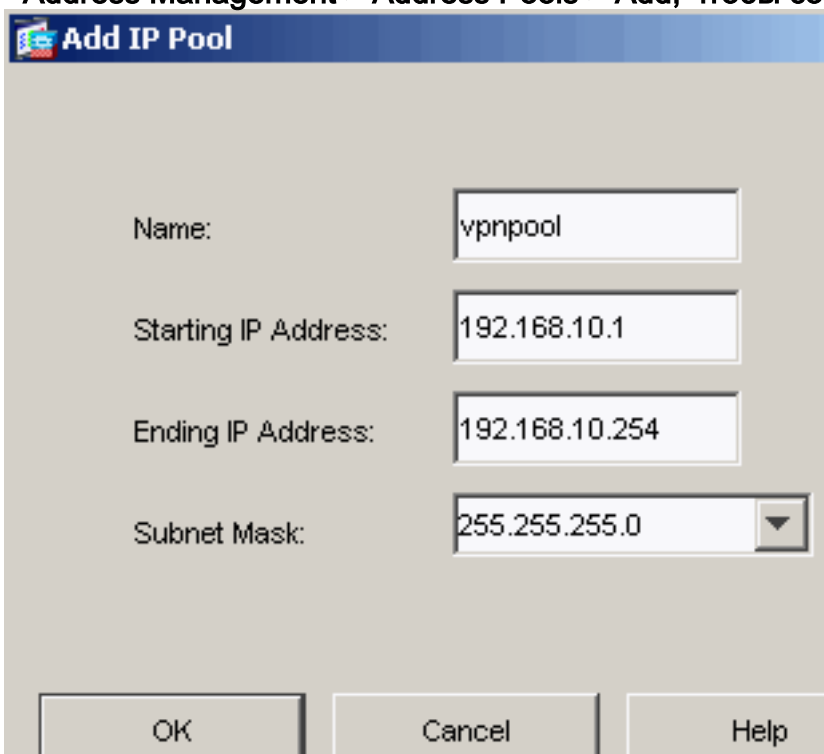
В данном документе предполагается, что вся базовая настройка, например, настройка интерфейса, уже выполнена и работает правильно.

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

Примечание: Нельзя включать WebVPN и ASDM на одном и том же интерфейсе ASA, если не изменены номера портов. [Для получения дополнительных сведений обратитесь к документу Включение ASDM и WebVPN на одном и том же интерфейсе ASA.](#)

Выполните эти шаги, чтобы настроить VPN-соединение с ASA по SSL-протоколу с раздельным туннелированием:

1. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add, чтобы создать пул IP-адресов



The screenshot shows a dialog box titled "Add IP Pool" with the following fields and values:

Field	Value
Name	vpnpool
Starting IP Address	192.168.10.1
Ending IP Address	192.168.10.254
Subnet Mask	255.255.255.0

Buttons: OK, Cancel, Help

vpnpool.

2. Щелкните "Применить". Эквивалентная конфигурация в интерфейсе командной строки:
3. Включенный WebVPN. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles и в разделе Access Interfaces установите флажки Allow Access и Enable DTLS для внешнего интерфейса. Также поставьте флажок Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below, чтобы разрешить SSL VPN на внешнем интерфейсе.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

Access Interfaces

Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

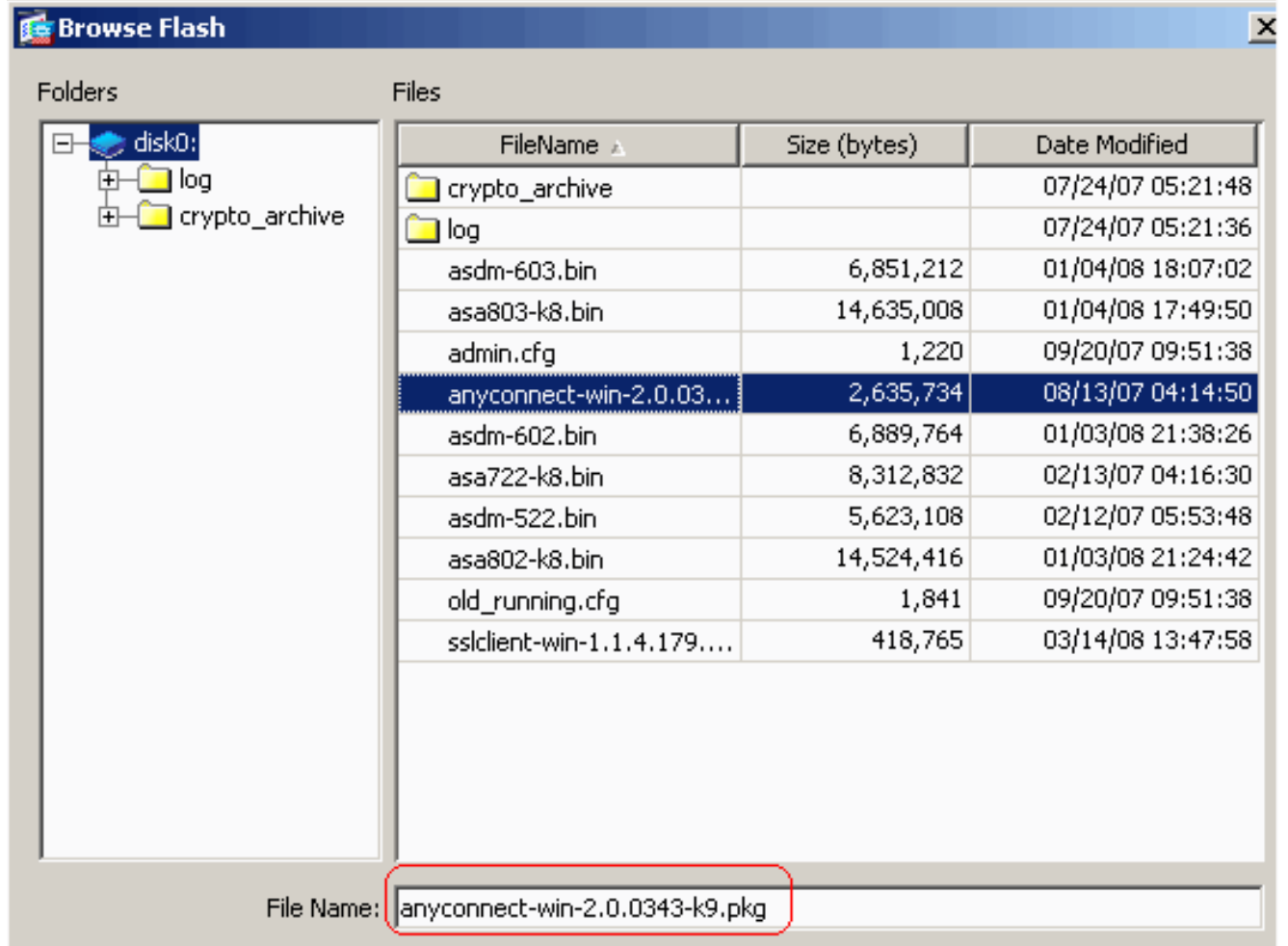
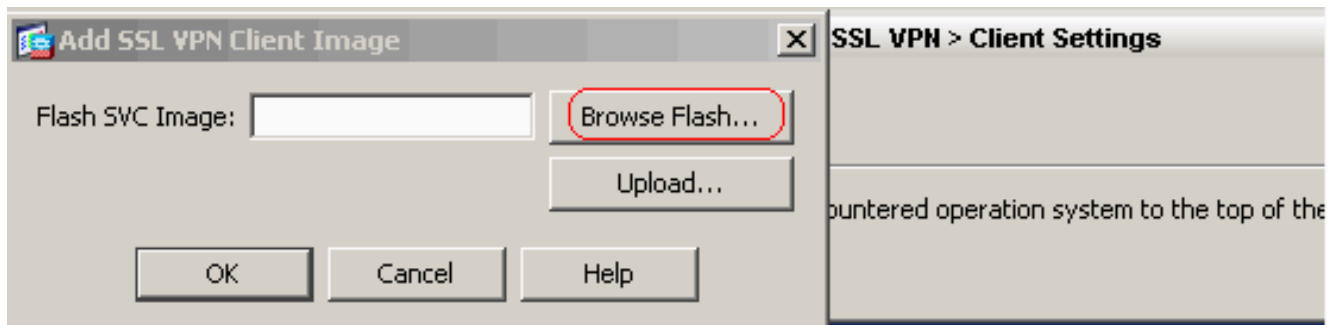
Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

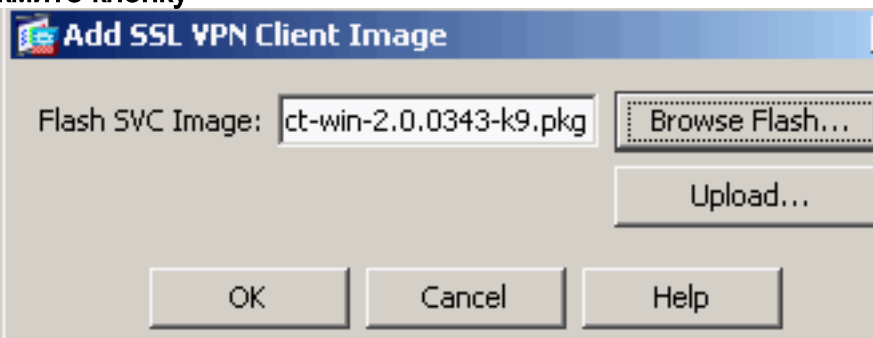
DTLS Port:

Click here to [Assign Certificate to Interface](#).

Щелкните "Применить". Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add, чтобы добавить образ VPN-клиента Cisco AnyConnect из флэш-память ASA, как показано ниже.



Нажмите кнопку



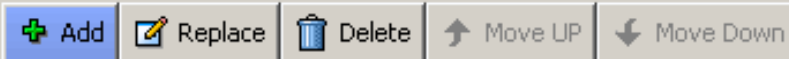
OK.
Add.

Нажмите

Identify SSL VPN Client (SVC) related files.

SSL VPN Client Images

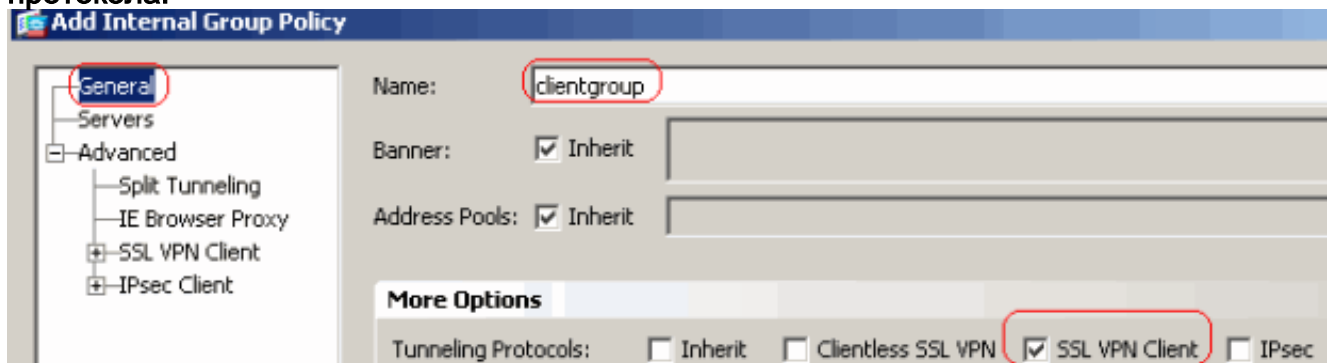
Minimize connection setup time by moving the image used by the most commonly encountered operation system to t



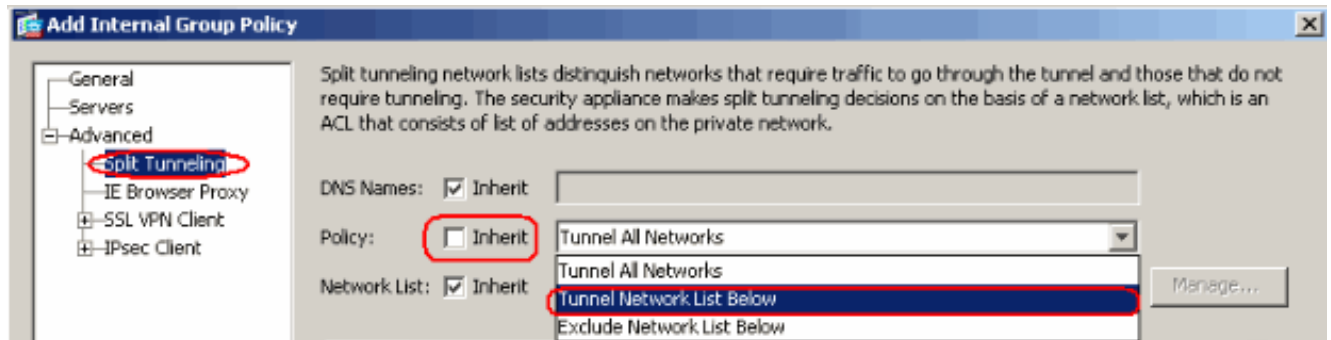
disk0:/anyconnect-win-2.0.0343-k9.pkg

Эквивалентная конфигурация в интерфейсе командной строки:

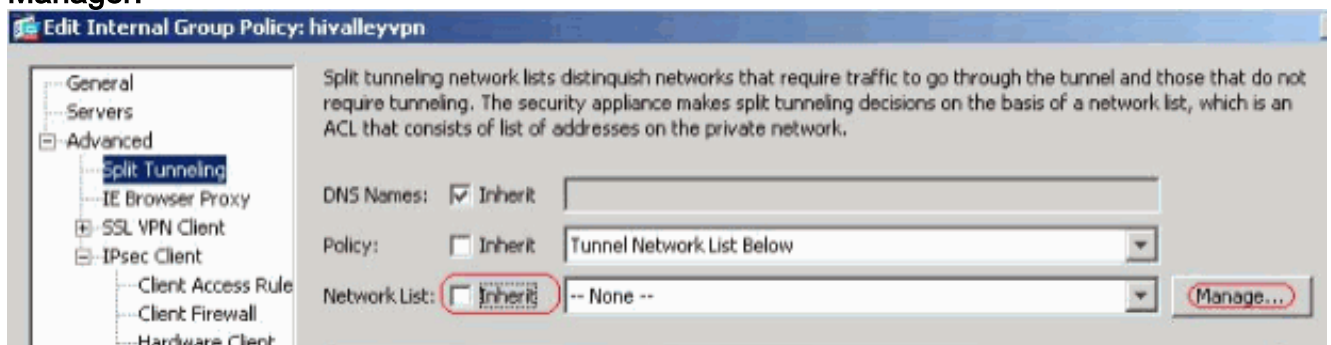
4. Настройка групповой политики. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > Group Policies, чтобы создать внутреннюю групповую политику clientgroup. На вкладке General установите флажок SSL VPN Client, чтобы разрешить использование WebVPN в качестве туннельного протокола.



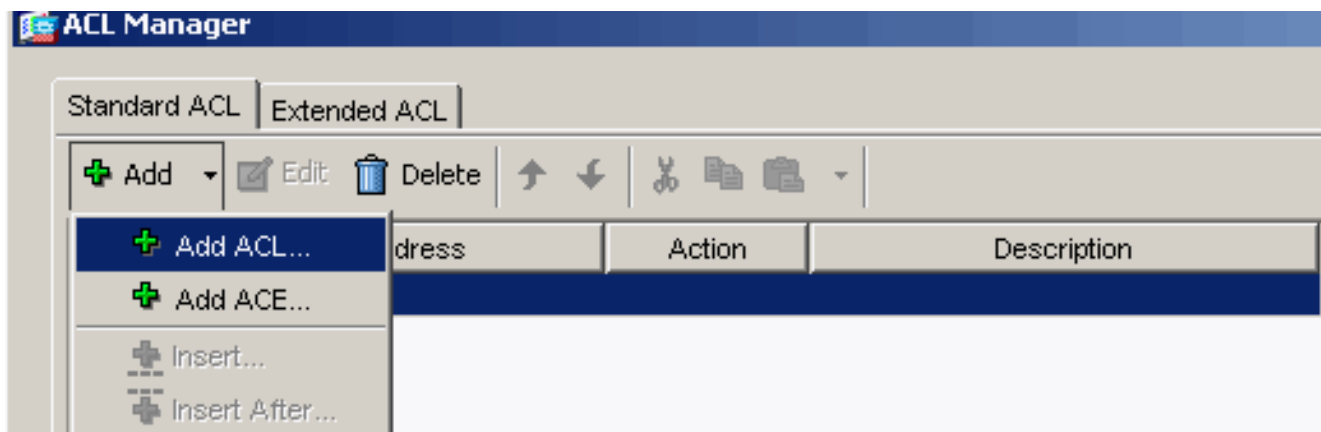
На вкладке Advanced > Split Tunneling снимите флажок Inherit для политики Split Tunnel и выберите Tunnel Network List Below из раскрывающегося списка.



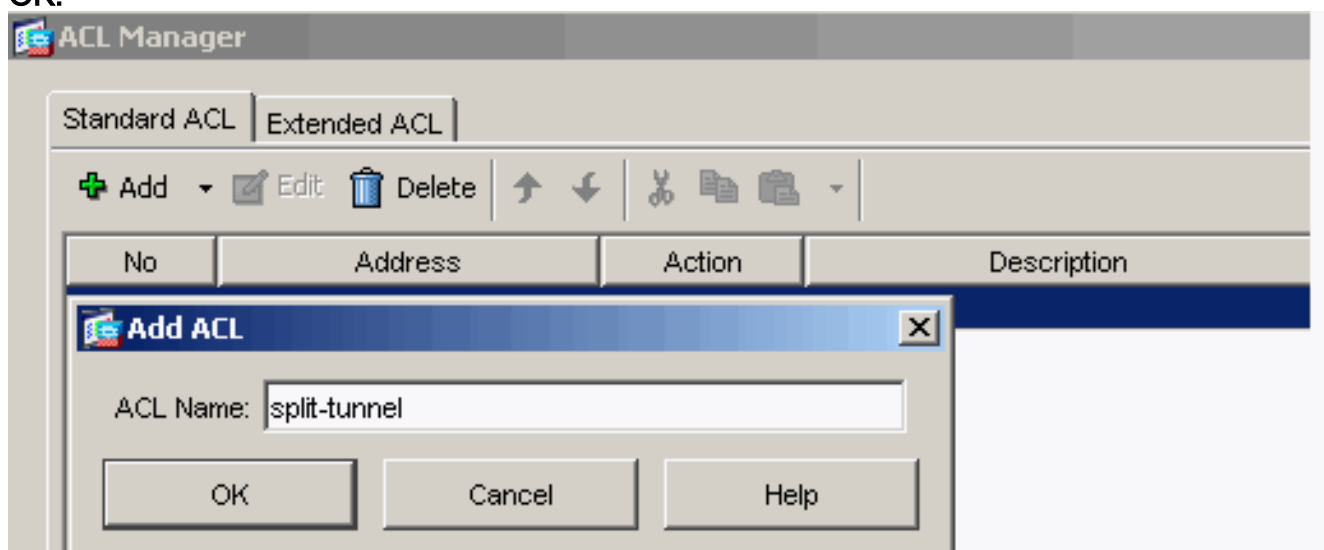
Снимите флажок Inherit для Split Tunnel Network List и нажмите кнопку Manage, чтобы запустить приложение ACL Manager.



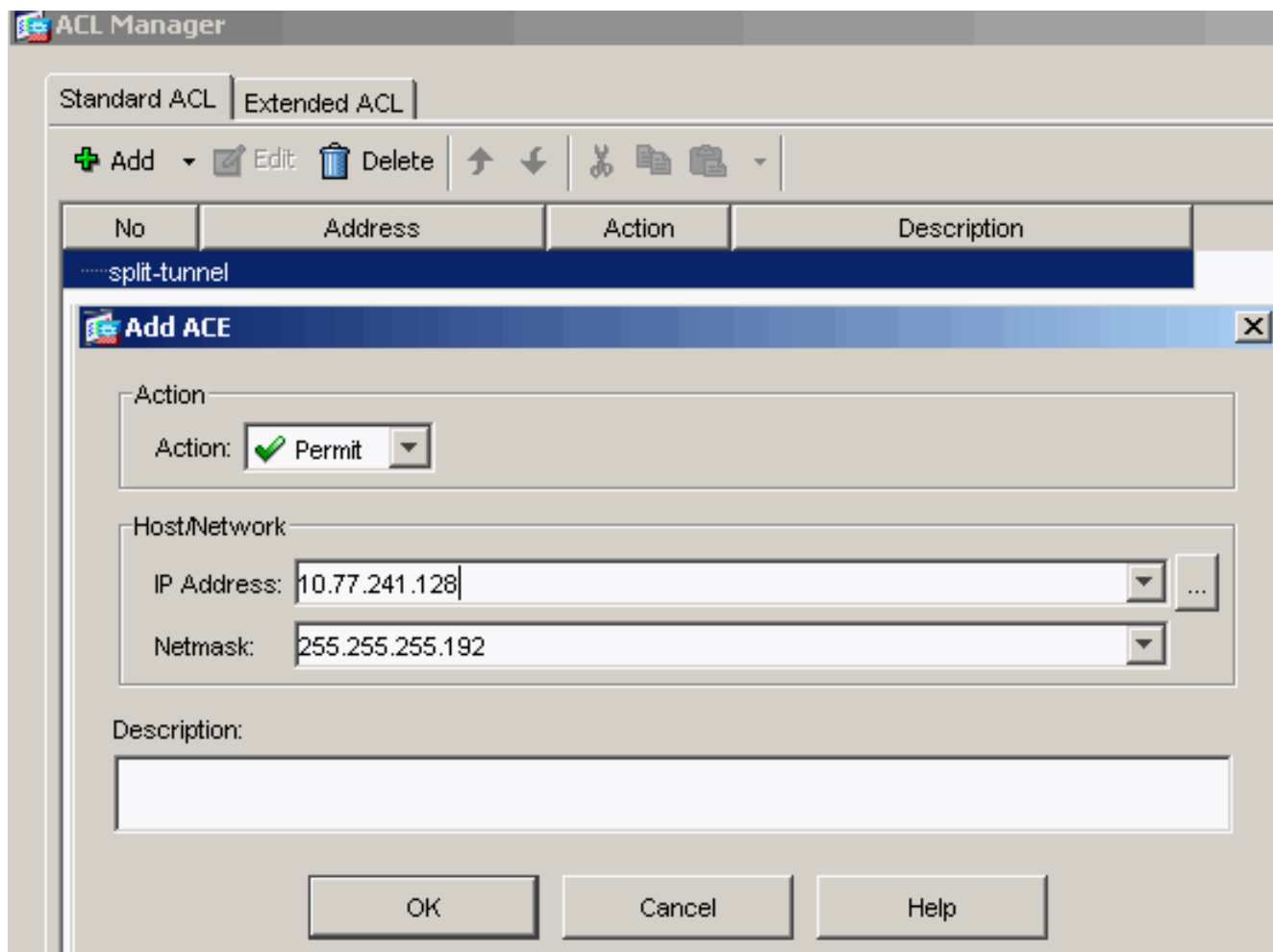
В данном диспетчере выберите Добавить > Добавить список ACL..., чтобы создать новый список контроля доступа.



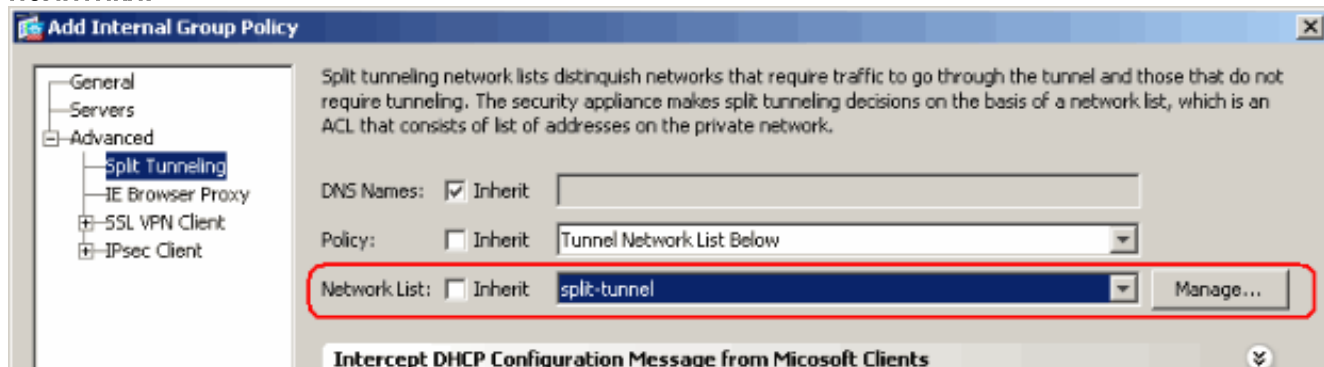
Укажите имя ACL и нажмите кнопку ОК.



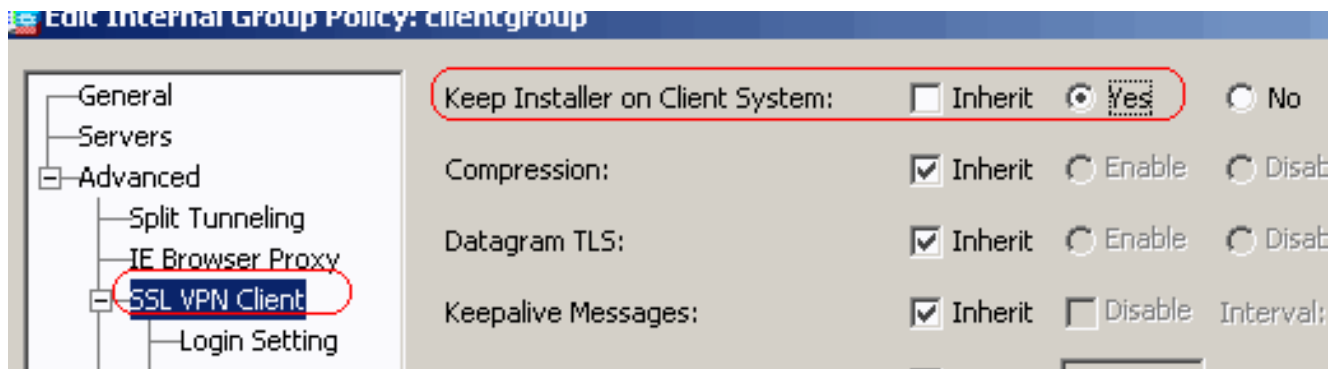
После создания списка ACL выберите Add > Add ACE, чтобы добавить элемент контроля доступа (ACE). Задайте запись ACE, соответствующую локальной сети, расположенной за модулем ASA. Укажите адрес сети (в нашем случае - 10.77.241.128/26) и выберите Permit из списка Action. Нажмите кнопку ОК, чтобы завершить работу с приложением ACL Manager.



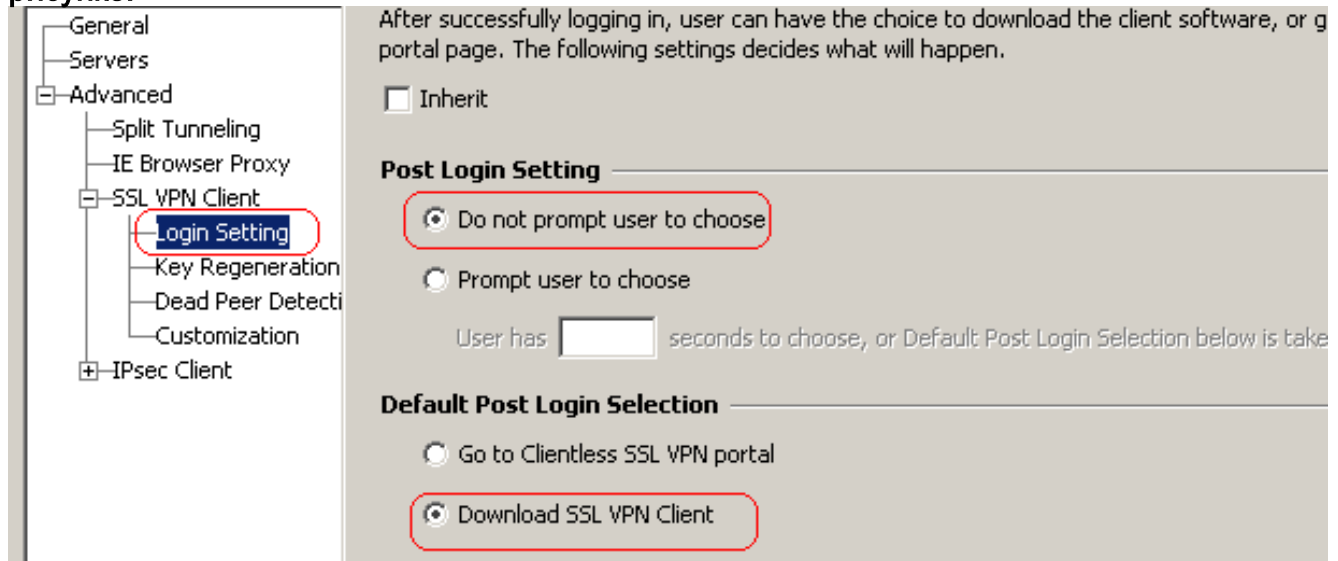
Убедитесь, что только что созданный ACL выбран для списка сетей с разделенными туннелями (Network List). **Нажмите кнопку ОК, чтобы вернуться к настройке групповой политики.**



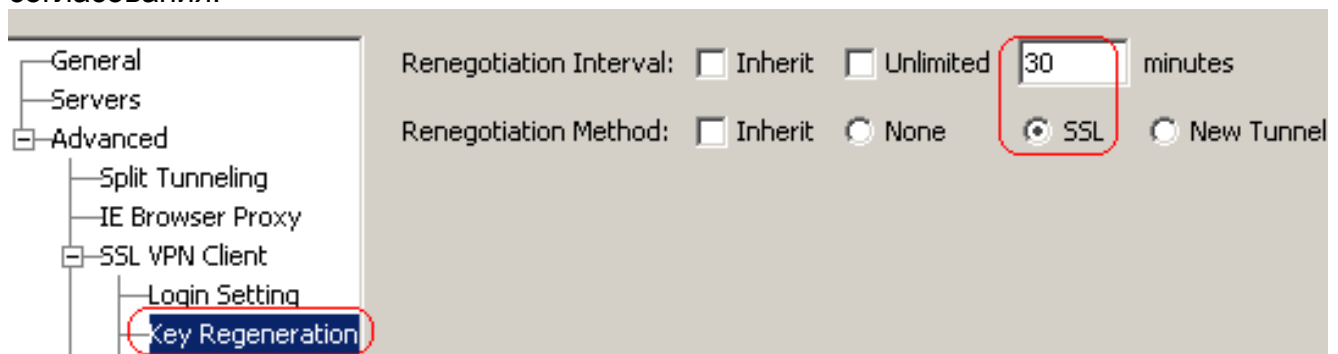
Нажмите кнопку Apply, а затем (если потребуется) Send, чтобы отправить эти команды в модуль ASA. Настройте параметры SSL VPN в режиме групповой политики. В разделе "Keep Installer on Client System" снимите флажок Inherit и установите переключатель в положение Yes. Это позволит ПО SVC оставаться на клиентской машине. Таким образом, модулю ASA не потребуется загружать ПО SVC на клиент во время каждого установления соединения. Такой выбор оптимален для удаленных пользователей, которые часто обращаются к корпоративной сети.



Выберите в дереве раздел Login Setting, чтобы установить переключатели в разделах Post Login Setting и Default Post Login Selection, как показано на рисунке.






В разделе "Renegotiation Interval" снимите флажки Inherit и Unlimited, после чего укажите время до смены ключа в минутах. Задание лимита времени, в течение которого действителен ключ, повышает безопасность. В разделе "Renegotiation Method" снимите флажок Inherit и установите переключатель в положение SSL. При повторном согласовании может использоваться имеющийся туннель SSL или новый туннель, созданный специально для повторного согласования.



Нажмите кнопку ОК, а затем Apply.

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

 Add  Edit  Delete

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A --
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A --

Эквивалентная конфигурация в интерфейсе командной строки:

5. Последовательно выберите Configuration > Remote Access VPN > AAA Setup > Local Users > Add, чтобы создать учетную запись нового пользователя ssluser1. Нажмите кнопку ОК, а затем

Apply.

Add User Account

Identity

- VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

Эквивалентная конфигурация в интерфейсе командной строки:

6. Последовательно выберите Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit, чтобы изменить группу серверов по умолчанию LOCAL, установив флажок Enable Local User Lockout и указав максимальное количество попыток равное 16.

Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts:

OK

Cancel

Help

7. Нажмите кнопку ОК, а затем Apply. Эквивалентная конфигурация в интерфейсе командной строки:

8. Настройка группы туннелирования. Последовательно выберите Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add, чтобы создать новую группу туннелирования sslgroup. На вкладке Basic можно заполнить список конфигурации так, как показано на рисунке: Назовите группу туннелирования sslgroup. В разделе "Client Address Assignment" выберите пул адресов vpnpool из раскрывающегося списка. В разделе "Default Group Policy" выберите групповую политику clientgroup из раскрывающегося списка.

Add SSL VPN Connection Profile

Basic
Advanced

Name:

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group:

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Default Group Policy

Group Policy:

SSL VPN Client Protocol: Enabled

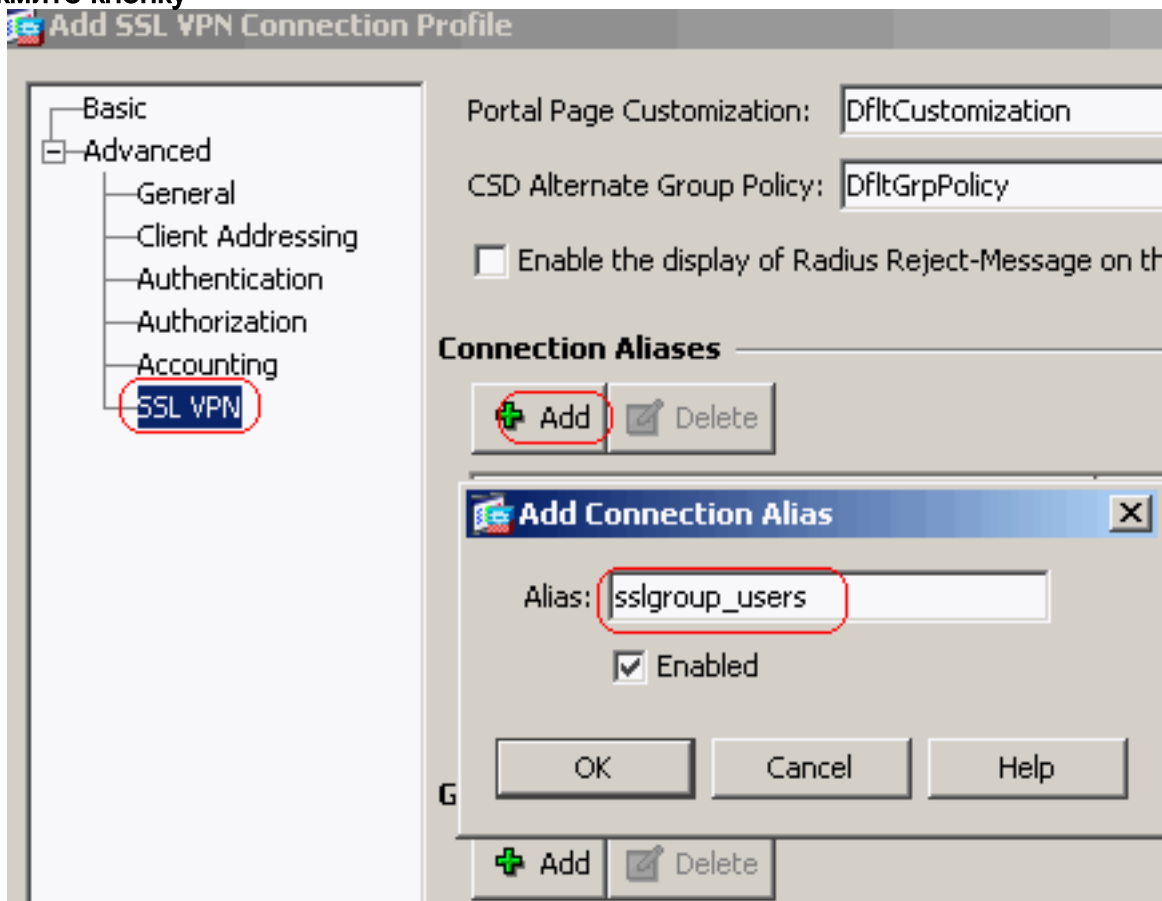
OK

Cancel

Help

На вкладке SSL VPN > Connection Aliases укажите псевдоним группы sslgroup_users и

нажмите кнопку

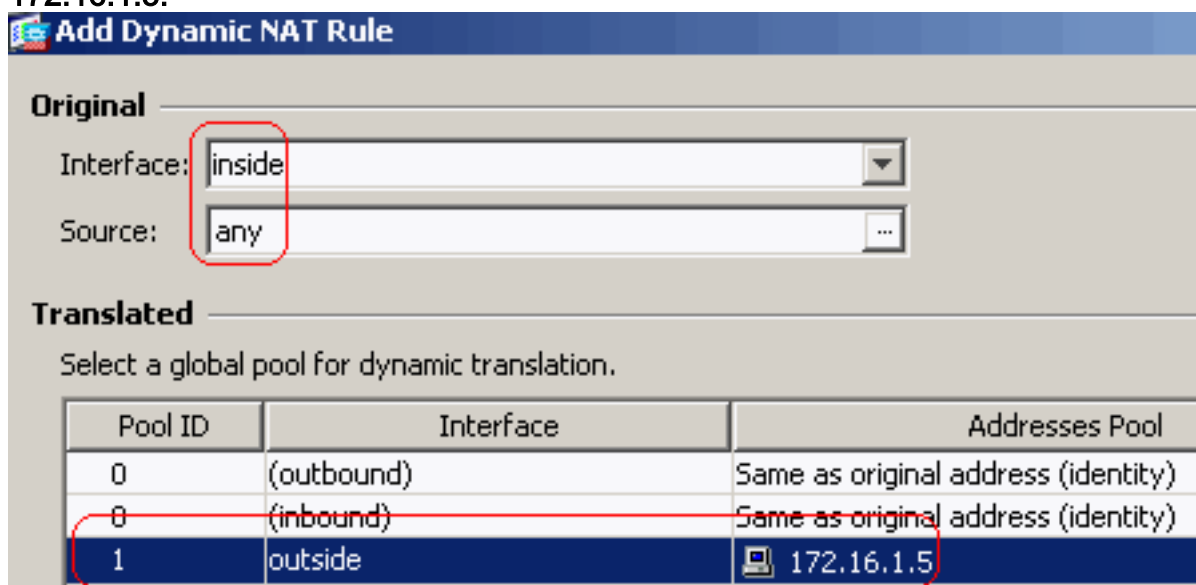


OK.

Нажм

ите кнопку OK, а затем Apply.Эквивалентная конфигурация в интерфейсе командной строки:

9. Настройка NAT.Последовательно выберите Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule, чтобы трафик, входящий из внутренней сети, мог транслироваться с внешним IP-адресом 172.16.1.5.



Нажми

те кнопку OK.Нажмите кнопку OK.

Configuration > Firewall > NAT Rules						
#	Type	Original			Interface	
		Source	Destination	Service		
[-] inside (1 Dynamic rules)						
1	Dynamic	any			outside	

Щелкните "Применить". Эквивалентная конфигурация в интерфейсе командной строки:

10. Настройте туземное освобождение для ответного трафика из сети клиенту

```
VPN.ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat
(inside) 0 access-list nonat
```

Конфигурация ASA в интерфейсе командной строки

Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config : Saved : ASA
Version 8.0(2) ! hostname ciscoasa domain-name
default.domain.invalid enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.77.241.142
255.255.255.192 ! interface Ethernet0/1 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
interface Ethernet0/2 shutdown no nameif no security-
level no ip address ! 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 clock timezone IST
5 30 dns server-group DefaultDNS domain-name
default.domain.invalid access-list split-tunnel standard
permit 10.77.241.128 255.255.255.192 !--- ACL for Split
Tunnel network list for encryption. access-list nonat
permit ip 10.77.241.0 192.168.10.0 access-list nonat
permit ip 192.168.10.0 10.77.241.0 !--- ACL to define
the traffic to be exempted from NAT. pager lines 24
logging enable logging asdm informational mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The
address pool for the Cisco AnyConnect SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-602.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5 !--- The
global address for Internet access used by VPN Clients.
!--- Note: Uses an RFC 1918 range for lab setup. !---
Apply an address from your public range provided by your
ISP. nat (inside) 0 access-list nonat !--- The traffic
permitted in "nonat" ACL is exempted from NAT. nat
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 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 no crypto isakmp nat-traversal telnet
```

```

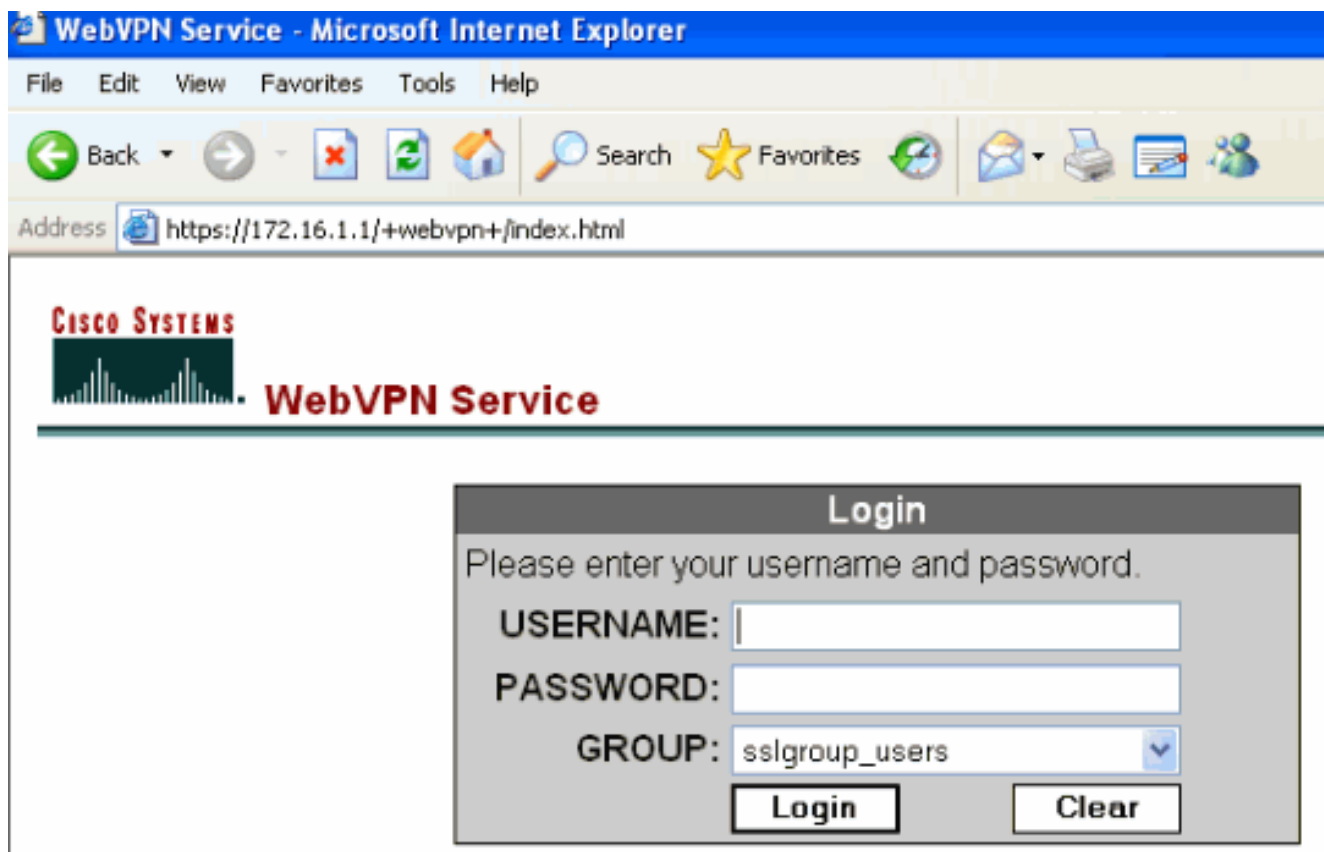
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
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 webvpn enable outside !---
Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 !--- Assign an
order to the AnyConnect SSL VPN Client image svc enable
!--- Enable the security appliance to download SVC
images to remote computers tunnel-group-list enable !---
Enable the display of the tunnel-group list on the
WebVPN Login page group-policy clientgroup internal !---
Create an internal group policy "clientgroup" group-
policy clientgroup attributes vpn-tunnel-protocol svc !-
-- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified split-tunnel-
network-list value split-tunnel !--- Encrypt the traffic
specified in the split tunnel ACL only webvpn svc keep-
installer installed !--- When the security appliance and
the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the
security of the connection. svc rekey time 30 !---
Command that specifies the number of minutes from the
start of the !--- session until the rekey takes place,
from 1 to 10080 (1 week). svc rekey method ssl !---
Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc
username ssluser1 password ZRhW85jZqEaVd5P. encrypted !-
-- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access !--- Create a tunnel group
"sslgroup" with type as remote access tunnel-group
sslgroup general-attributes address-pool vpnpool !---
Associate the address pool vpnpool created default-
group-policy clientgroup !--- Associate the group policy
"clientgroup" created tunnel-group sslgroup webvpn-
attributes group-alias sslgroup_users enable !---
Configure the group alias as sslgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#

```

Установка соединения SSL VPN с SVC

Выполните эти шаги, чтобы установить VPN-подключение к ASA по протоколу SSL:

1. Введите URL-адрес или IP-адрес интерфейса ASA WebVPN в своем браузере в формате, который показан ниже. `https://url` Или `https://<IP address of the ASA WebVPN interface>`



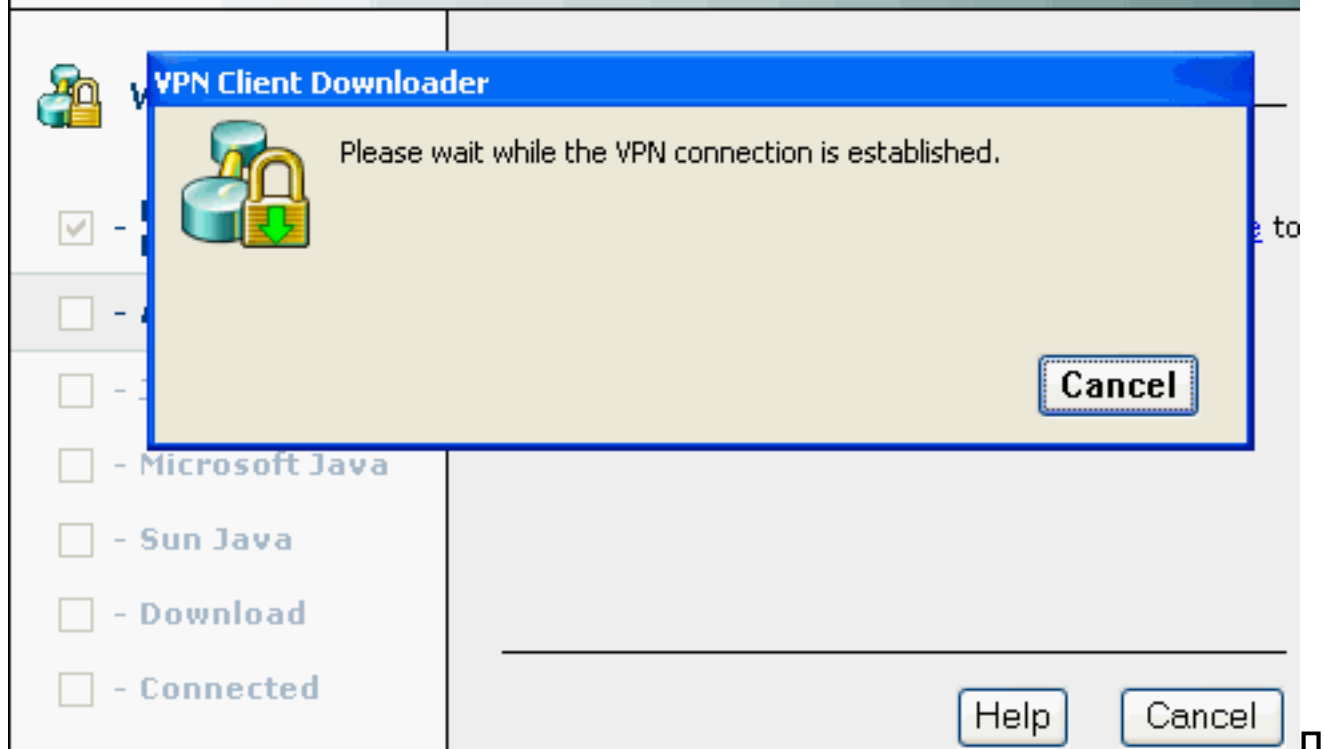
2. Введите имя пользователя и пароль. Также выберите соответствующую группу из раскрывающегося списка, как показано

ниже.

Это окно будет отображаться перед тем, как VPN-соединения по протоколу SSL будет установлено.



Cisco AnyConnect VPN Client



римечание: Программное обеспечение ActiveX должно быть установлено в вашем компьютере перед загрузкой SVC. После установления соединения будет отображено следующее окно.



Cisco AnyConnect VPN Client



WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Microsoft Java
- Sun Java
- Download
- Connected

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:



Help

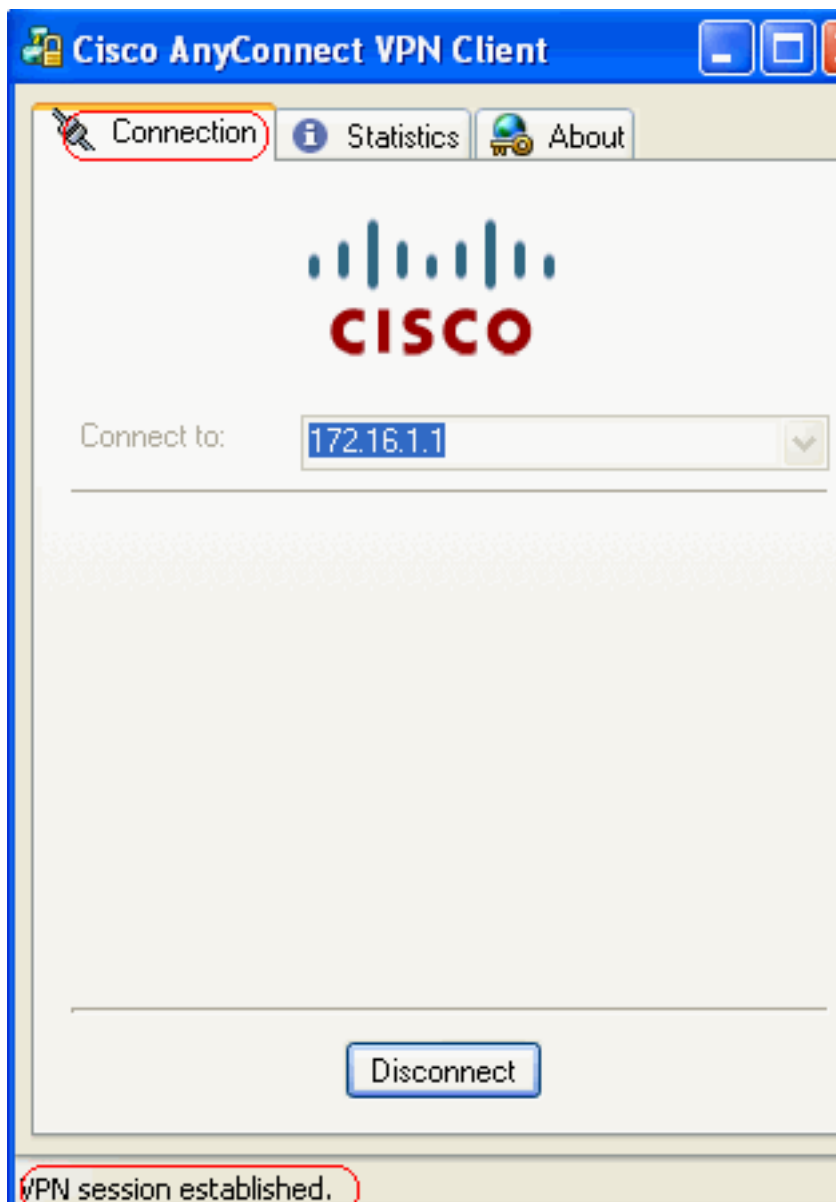
Cancel

system...

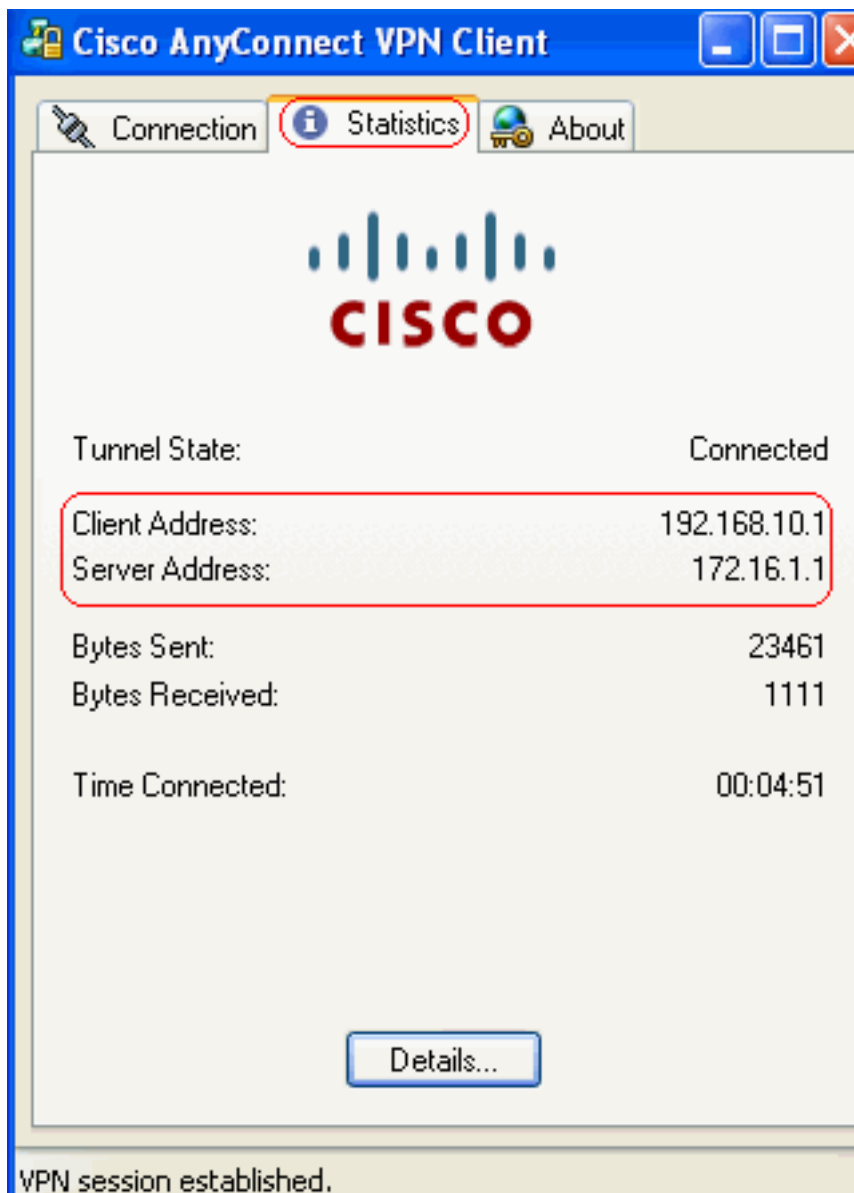
anyconnect - Paint

Cisco AnyConnect
Connected

3. Щелкните по значку с замком, который появился на панели



задач. **VPN session established.** Появится следующее окно с информацией о SSL-соединении. Например, 192.168.10.1 — это IP-адрес, назначенный многофункциональным устройством защиты, и



т.д. VPN session established.
отображается информация о версии VPN-клиента Cisco

В следующем окне



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 webvpn svc** — отображает образы SVC, записанные во флэш-памяти
ASA.ciscoasa#show webvpn svc 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1 CISCO STC win2k+ 2,0,0343 Mon 04/23/2007 4:16:34.63 1 SSL VPN Client(s) installed
- **show vpn-sessiondb svc** — отображает информацию о текущих SSL-подключениях.
ciscoasa#show vpn-sessiondb svc Session Type: SVC Username : **ssluser1** Index : 12 Assigned IP : **192.168.10.1** Public IP : **192.168.1.1** Protocol : **Clientless SSL-Tunnel DTLS-Tunnel** Encryption : **RC4 AES128** Hashing : **SHA1** Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : **clientgroup** Tunnel Group : **sslgroup** Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none
- **show webvpn group-alias** — отображает псевдонимы, назначенные разным группам.
ciscoasa#show webvpn group-alias Tunnel Group: **sslgroup** Group Alias: **sslgroup_users** enabled

- В ASDM последовательно выберите **Monitoring > VPN > VPN Statistics > Sessions**, чтобы узнать текущие сеансы WebVPN в ASA.

Monitoring > VPN > VPN Statistics > Sessions

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
		Clientless	With Client	Total		
0	0	0	0	0	0	0

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

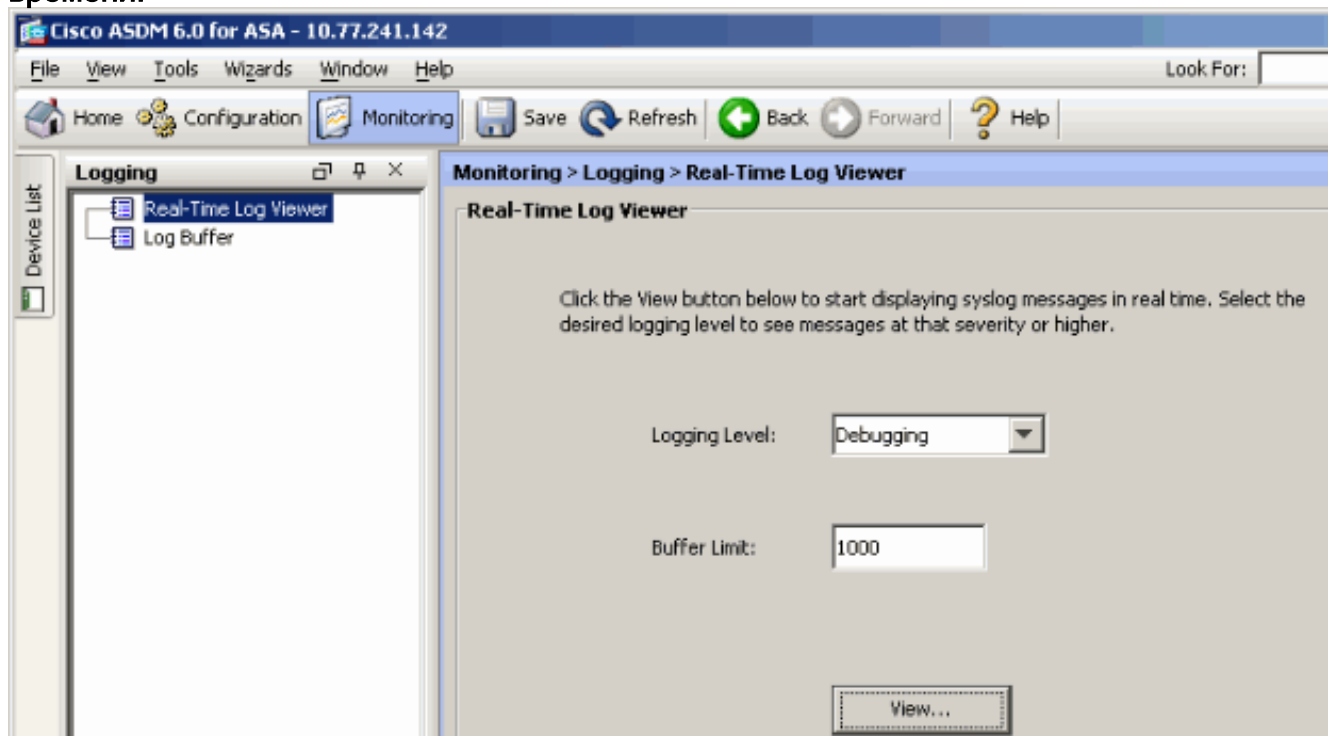
Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

1. команда `vpn-sessiondb logoff name<username>` используется для прекращения сеанса SSL VPN для определенного пользователя. `ciscoasa#vpn-sessiondb logoff name ssluser1` Do you want to logoff the VPN session(s)? [confirm] Y INFO: Number of sessions with name "ssluser1" logged off : 1 `ciscoasa#Called vpn_remove_uauth: success!`
`webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL`
`np_svc_destroy_session(0xB000)` Также можно использовать команду `vpn-sessiondb logoff svc`, чтобы прекратить все SVC-сеансы.
2. **Примечание:** Если ПК переходит к резерву, или будьте в спящем режиме режим, то VPN-подключение на базе SSL может быть завершено.
`webvpn_rx_data_cstp webvpn_rx_data_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e tc) Called vpn_remove_uauth: success!`
`webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL`
`np_svc_destroy_session(0xA000) ciscoasa#show vpn-sessiondb svc` INFO: There are presently no active sessions
3. команда `debug webvpn svc <1-255>` предоставляет все события webvpn в реальном времени для установления сеанса. `Ciscoasa#debug webvpn svc 7`
`webvpn_rx_data_tunnel_connect CSTEP state = HEADER_PROCESSING http_parse_cstp_method()`
`...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1' Processing CSTEP header line: 'Host: 172.16.1.1'`
`webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Processing CSTEP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'`
`Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'`
`webvpn_cstp_parse_request_field() ...input: 'Cookie:`
`webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B 7D75F4EDEF26' Processing CSTEP`
`header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8`
`625B92C1338D631B08B7D75F4EDEF26' Found WebVPN cookie:`
`'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B 08B7D75F4EDEF26' WebVPN Cookie:`
`'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7 5F4EDEF26'`
`webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-Version: 1' Processing CSTEP header`
`line: 'X-CSTEP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field()`
`...input: 'X-CSTEP-Hostname: tacweb' Processing CSTEP header line: 'X-CSTEP-Hostname: tacweb'`
`Setting hostname to: 'tacweb' webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-Accept-`
`Encoding: deflate;q=1.0' Processing CSTEP header line: 'X-CSTEP-Accept-Encoding:`
`deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-MTU: 1206' Processing`
`CSTEP header line: 'X-CSTEP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTEP-`

```
Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret:
CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693' Processing CSTP header line: 'X-DTLS-
Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-
CBC3-SHA:DES-CBC-SHA' Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-
SHA:DES-CBC3 -SHA:DES-CBC-SHA' Validating address: 0.0.0.0 CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0 CSTP state = HAVE_ADDRESS No subnetmask...
must calculate it SVC: NP setup np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

4. В ASDM последовательно выберите **Monitoring > Logging > Real-time Log Viewer > View**, чтобы увидеть все события в реальном времени.



В этом примере показан SSL-сеанс, установленный с головным устройством.

The screenshot shows the 'Real-Time Log Viewer' application window. The title bar indicates the host IP is 10.77.241.142. The interface includes a menu bar (File, Tools, Window, Help) and a toolbar with icons for Pause, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, Show Details, and Help. Below the toolbar is a filter section with 'Filter By:', 'Filter', 'Show All', and 'Find:' fields. The main area contains a table of log entries with columns for Severity, Date, Time, Syslog ID, Source IP, Destination IP, and a description. The entry with Syslog ID 725002 is highlighted in blue. Below the table, a detailed view of this entry is shown, with a red circle around the text: '%ASA-6-725002 Device completed SSL handshake with remote_device_interface_name:IP_address/port' and 'The SSL handshake has completed successfully with the remote device.'

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Description
6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.
6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44:
6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identit
6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl
6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026
6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.
6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TL5v1 se
6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23

```
%ASA-6-725002 Device completed SSL handshake with remote_device_interface_name:IP_address/port
The SSL handshake has completed successfully with the remote device.
```

Дополнительные сведения

- [Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500](#)
- [Комментарии к выпуску для AnyConnect VPN Client \(выпуск 2.0\)](#)
- [ASA/PIX: Пример конфигурации устройства ASA, разрешающей раздельное туннелирование для VPN-клиентов](#)
- [Пример конфигурации маршрутизатора, разрешающего VPN-клиентам подключаться к узлам по протоколу IPsec и к сети Интернет, с использованием раздельного туннелирования](#)
- [Пример настройки PIX/ASA 7.x и VPN-клиента для сети VPN, организованной в общедоступной части Интернета и имеющей один внешний интерфейс](#)
- [Пример настройки SSL клиента VPN \(SVC\) на ASA с ASDM](#)
- [Cisco Systems – техническая поддержка и документация](#)