ASA 8. x: Доступ к VPN с помощью VPN-клиента AnyConnect, для которого используется пример конфигурации с недоверительным сертификатом

Содержание

Введение

В этом документе описывается способ применения самостоятельно подписанных сертификатов, разрешающих удаленный доступ подключений SSL VPN к ASA из клиента Cisco AnyConnect 2.0.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем

попробовать эту конфигурацию:

- Базовая конфигурация ASA, где запущено ПО версии 8.0
- ASDM 6.0(2)

Используемые компоненты

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

- Cisco ASA 8.0(2), ASDM 6.0 (2)
- Cisco AnyConnect 2.0

Условные обозначения

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

Общие сведения

Клиент Cisco AnyConnect 2.0 — это клиент VPN, работающий на базе SSL. Клиент AnyConnect можно использовать и устанавливать в самых разных операционных системах (таких как Windows 2000, XP, Vista, Linux (разные дистрибутивы) и MAC OS X). Системный администратор может установить клиент AnyConnect вручную на удаленный компьютер. Его также можно загрузить в устройство обеспечения безопасности и подготовить для загрузки удаленными пользователями. После загрузки приложение можно автоматически удалить вслед за разрывом подключения либо оставить на удаленном компьютере для будущих подключений SSL VPN. В этом примере клиент AnyConnect подготавливается к загрузке после успешной аутентификации SSL на основе браузера.

Дополнительные сведения о клиенте AnyConnect 2.0 см. в документе Заметки о выпуске AnyConnect 2.0.

Примечание: Сервисы терминалов MS не поддерживаются в сочетании с клиентом AnyConnect. Невозможно подключиться по протоколу удаленного рабочего стола (RDP) к компьютеру, а затем запустить сеанс AnyConnect. К клиенту, подключенному с помощью AnyConnect, невозможно подключиться с помощью RDP.

Примечание: Для первой установки AnyConnect требуется, чтобы пользователь имел права администратора (независимо от того, используете ли вы автономный msi-пакет AnyConnect или получаете файл pkg от ASA). Если у пользователя нет прав администратора, появляется диалоговое окно с соответствующим требованием. Последующие обновления не потребуют наличия прав администратора у пользователя, ранее установившего AnyConnect.

Настройка

Чтобы настроить ASA для доступа через VPN с помощью любого клиента AnyConnect, выполните следующие действия:

1. Настройка самостоятельно выпущенного сертификата.
2. Загрузка на сервер и идентификация образа клиента SSL VPN.
3. Включение доступа к Anyconnect.
4. Создание новой групповой политики.
5. Настройка обхода списка доступа для подключений VPN.
6. Создание профиля подключения и туннельной группы для подключений клиента AnyConnect.
7. Настройка исключения NAT для клиентов AnyConnect.
8. Добавление пользователей в локальную базу данных.

Шаг 1. Настройка самостоятельно выпускаемого сертификата

По умолчанию устройство обеспечения безопасности обладает самостоятельно подписанным сертификатом, который создается заново каждый раз, когда устройство перезагружается. Приобрести свой собственный сертификат можно у поставщиков (например, у Verisign или EnTrust), либо настроить ASA так, чтобы идентификационный сертификат выпускался самим устройством. Этот сертификат остается одинаковым даже в случае перезагрузки устройства. Завершите этот шаг, чтобы создать самостоятельно выпускаемый сертификат, который сохраняется при перезагрузке.

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Разверните раздел Certificate Management и выберите Identity Certificates.**
3. **Щелкните Add, а затем щелкните переключатель Add a new identity certificate.**
4. **Щелкните New.**
5. **В окне Add Key Pair щелкните переключатель Enter new key pair name.**
6. Введите название, которое идентифицирует пару ключей.*В этом примере используется название sslvpnkeypair.*
7. **Нажмите кнопку Generate Now.**
8. Убедитесь, что в окне Add Identity Certificate выбрана только что созданная пара ключей.
9. В поле Certificate Subject DN введите полное доменное имя (FQDN), которое будет использоваться для подключения к конечному интерфейсу VPN.**CN=sslvpn.cisco.com**
10. **Щелкните Advanced и введите FQDN, использованный для поля Certificate Subject DN.Например, FQDN:** sslvpn.cisco.com
11. **Нажмите кнопку OK.**
12. **Установите флажок Generate Self Signed Certificate и щелкните Add Certificate.**
13. **Нажмите кнопку OK.**
14. **Щелкните Configuration, а затем выберите Remote Access VPN.**
15. **Раскройте раздел Advanced, а затем раскройте раздел SSL Settings.**
16. **В области Certificates выберите интерфейс, который будет использоваться в качестве конечного для SSL VPN (внешний), а затем нажмите Edit.**
17. В раскрывающемся списке Certificate выберите самостоятельно подписанный сертификат, который был ранее сгенерирован.
18. **Нажмите кнопку OK, а затем нажмите Apply.**

Пример командной строки

cisco ASA
ciscoasa(config)#**crypto key generate rsa label sslvpnkeypair** INFO: The name for the keys will be: sslvpnkeypair Keypair generation process begin. Please wait... *!--- Generate an RSA key for the certificate. (The name should be unique. !--- For example, sslvpnkeypair.)* ciscoasa(config)#**crypto ca trustpoint localtrust** *!--- Create a trustpoint for the self-issued certificate.* ciscoasa(config-ca-trustpoint)#**enrollment self** ciscoasa(config-ca-trustpoint)#**fqdn sslvpn.cisco.com** ciscoasa(config-ca-trustpoint)#**subject-name CN=sslvpn.cisco.com** *!--- The fully qualified domain name is used for both fqdn and CN. !--- The name should resolve to the ASA outside interface IP address.* ciscoasa(config-ca-trustpoint)#**keypair sslvpnkeypair** *!--- The RSA key is assigned to the trustpoint for certificate creation.* ciscoasa(config-ca-trustpoint)#**crypto ca enroll localtrust noconfirm** % The fully-qualified domain name in the certificate will be: sslvpn.cisco.com ciscoasa(config)# **ssl trust-point localtrust outside** *!--- Assign the trustpoint to be used for SSL connections on the outside interface.*

Шаг 2. Загрузка на сервер и идентификация образа клиента SSL VPN

В этом документе используется клиент AnyConnect SSL 2.0. Этот клиент можно загрузить с сайта загрузки программного обеспечения Cisco. Для каждой операционной системы, которую планируют применять удаленные пользователи, требуется отдельный образ Anyconnect. Дополнительные сведения см. в документе Заметки о выпуске Cisco AnyConnect 2.0.

Загрузив клиент AnyConnect, выполните следующие действия:

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Разверните раздел Network (Client) Access, а затем разверните раздел Advanced.**
3. **Разверните раздел SSL VPN и выберите Client Settings.**
4. **В области SSL VPN Client Images щелкните Add, а затем — Upload.**
5. Перейдите к папке, в которую был загружен клиент AnyConnect.
6. **Выберите файл и щелкните Upload File.**После загрузки клиента появляется сообщение о том, что файл успешно загружен во флэш-память.
7. **Нажмите кнопку OK.**Появится окно, подтверждающее намерение использовать только что загруженный образ в качестве текущего образа клиента SSL VPN.
8. **Нажмите кнопку OK.**
9. **Нажмите кнопку OK, а затем нажмите Apply.**
10. Повторите действия из этого раздела для каждого пакета Anyconnect для операционной системы, который требуется использовать.

Пример командной строки

cisco ASA
ciscoasa(config)#**copy tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg flash** Address or name of remote host [192.168.50.5]? Source filename [anyconnect-win-

```
2.0.0343-k9.pkg]? Destination filename [anyconnect-win-
2.0.0343-k9.pkg]? Accessing
tftp://192.168.50.5/anyconnect-win-2.0.0343-
k9.pkg...!!!!!!!!!!!!! Writing file disk0:/anyconnect-
win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!! 2635734 bytes copied in 4.480 secs
(658933 bytes/sec) !--- AnyConnect image is downloaded
to ASA via TFTP. ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1 !--- Specify the AnyConnect image to
be downloaded by users. The image that is !---
downloaded the most should have the lowest number. This
image uses 1 for the !--- AnyConnect Windows image.
```

Шаг 3. Включение доступа к Anyconnect

Чтобы разрешить клиенту AnyConnect подключаться к ASA, необходимо включить доступ в оконечном интерфейсе подключений SSL VPN. В этом примере в качестве оконечного интерфейса для подключений Anyconnect используется внешний интерфейс.

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Разверните раздел Network (Client) Access, а затем выберите SSL VPN Connection Profiles.**
3. **Установите флажок Enable Cisco AnyConnect VPN Client.**
4. **Установите флажок Allow Access для внешнего интерфейса и щелкните Apply.**

Пример командной строки

cisco ASA

```
ciscoasa(config)#webvpn ciscoasa(config-webvpn)#enable
outside ciscoasa(config-webvpn)#svc enable !--- Enable
AnyConnect to be downloaded to remote computers.
```

Шаг 4. Создание новой групповой политики

Групповая политика служит для указания параметров конфигурации, которые должны применяться к клиентам при подключении. *В этом примере создается групповая политика, которая называется SSLClientPolicy.*

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Разверните раздел Network (Client) Access, а затем разверните раздел Group Policies.**
3. **Нажмите Add.**
4. **Выберите General, а затем введите SSLClientPolicy в поле Name.**
5. **В разделе Address Pools снимите флажок Inherit.**
6. **Щелкните Select, а затем выберите Add.**Появится окно Add IP Pool.
7. Настройте пул адресов из диапазона IP-адресов, который в данный момент не используется в вашей сети.В этом примере используются следующие значения:**Name:** SSLClientPool**Starting IP Address:** 192.168.25.1**Ending IP Address:** 192.168.25.50**Маска**

подсети: 255.255.255.0

8. Нажмите кнопку OK.
9. Выберите только что созданный пул и щелкните Assign.
10. Нажмите кнопку OK, а затем щелкните More Options.
11. В разделе Tunneling Protocols снимите флажок Inherit.
12. Установите флажок SSL VPN Client.
13. На левой панели выберите Servers.
14. В разделе DNS Servers снимите флажок Inherit и введите IP-адрес внутреннего сервера DNS, который будет использоваться клиентами AnyConnect.*В этом примере используется адрес 192.168.50.5.*
15. Щелкните More Options.
16. В разделе Default Domain снимите флажок Inherit.
17. Введите домен, используемый вашей внутренней сетью. *Например, tsweb.local.*
18. Нажмите кнопку OK, а затем нажмите Apply.

Пример командной строки

cisco ASA
ciscoasa(config)#**ip local pool SSLClientPool 192.168.25.1-192.168.25.50 mask 255.255.255.0** *!--- Define the IP pool. The IP pool should be a range of IP addresses !--- not already in use on the internal network.* ciscoasa(config)#**group-policy SSLClientPolicy internal** ciscoasa(config)#**group-policy SSLClientPolicy attributes** ciscoasa(config-group-policy)#**dns-server value 192.168.50.5** *!--- Specify the internal DNS server to be used.* ciscoasa(config-group-policy)#**vpn-tunnel-protocol svc** *!--- Specify VPN tunnel protocol to be used by the Group Policy.* ciscoasa(config-group-policy)#**default-domain value tsweb.local** *!--- Define the default domain assigned to VPN users.* ciscoasa(config-group-policy)#**address-pools value SSLClientPool** *!--- Assign the IP pool created to the SSLClientPolicy group policy.*

Настройка обхода списка доступа для подключений VPN

При включении этого параметра клиентам SSL/IPsec разрешается обходить список доступа интерфейса.

Порядок действий в диспетчере ASDM

1. Щелкните Configuration, а затем выберите Remote Access VPN.
2. Разверните раздел Network (Client) Access, а затем разверните раздел Advanced.
3. Разверните раздел SSL VPN и выберите Bypass Interface Access List.
4. Убедитесь в том, что установлен флажок Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists и нажмите Apply.

Пример командной строки

cisco ASA
ciscoasa(config)#**sysopt connection permit-vpn** *!--- Enable interface access-list bypass for VPN connections. !--- This example uses the* ***vpn-filter*** *command for access control.* ciscoasa(config-group-policy)#

Шаг 6. Создание профиля подключения и туннельной группы для подключений клиента AnyConnect

Когда клиенты VPN подключаются к ASA, они подключаются к профилю подключения или туннельной группе. Туннельная группа используется для определения параметров подключения для определенных типов подключений VPN (таких как IPsec L2L, удаленный доступ с помощью IPsec, SSL без клиентов и SSL с клиентами).

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Разверните раздел Network (Client) Access, а затем разверните раздел SSL VPN.**
3. **Выберите Connection Profiles и щелкните Add.**
4. **Выберите Basic и введите следующие значения:Name:** SSLClientProfile**Authentication:** ЛОКАЛЬНЫЙ**Default Group Policy:** SSLClientPolicy
5. **Убедитесь в том, что установлен флажок SSL VPN Client Protocol.**
6. **Разверните на левой панели раздел Advanced и выберите SSL VPN.**
7. **В разделе Connection Aliases щелкните Add и введите имя, которое пользователи могут связать со своими подключениями VPN.** *Например, SSLVPNClient.*
8. **Нажмите кнопку OK, а затем нажмите кнопку OK еще раз.**
9. **В нижней части окна ASDM установите флажок Allow user to select connection, identified by alias in the table above at login page и щелкните Apply.**

Пример командной строки

cisco ASA
ciscoasa(config)#**tunnel-group SSLClientProfile type remote-access** *!--- Define tunnel group to be used for VPN remote access connections.* ciscoasa(config)#**tunnel-group SSLClientProfile general-attributes** ciscoasa(config-tunnel-general)#**default-group-policy SSLCLientPolicy** ciscoasa(config-tunnel-general)#**tunnel-group SSLClientProfile webvpn-attributes** ciscoasa(config-tunnel-webvpn)#**group-alias SSLVPNClient enable** *!--- Assign alias for tunnel group.* ciscoasa(config-tunnel-webvpn)#**webvpn** ciscoasa(config-webvpn)#**tunnel-group-list enable** *!--- Enable alias/tunnel group selection for SSL VPN connections.*

Шаг 7. Настройка исключения NAT для клиентов AnyConnect

Исключение NAT должно настраиваться для любых IP-адресов или диапазонов IP-адресов, к которым требуется разрешить доступ клиентов SSL VPN. В данном примере клиентам SSL VPN нужен доступ только к внутреннему IP-адресу 192.168.50.5.

Примечание: Если управление NAT не включено, это действие не требуется. **Воспользуйтесь для проверки командой show run nat-control. Чтобы выполнить проверку с помощью ASDM, щелкните Configuration, затем — Firewall, а затем выберите Nat Rules. Если установлен флажок Enable traffic through the firewall without address translation это действие можно пропустить.**

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Firewall.**
2. **Выберите Nat Profiles и щелкните Add.**
3. **Выберите Add NAT Exempt Rule и введите следующие значения:Действие:** СвободноInterface: внутриИсточник: 192.168.50.5Destination: 192.168.25.0/24**NAT Exempt Direction:** Исходящий трафик исключения NAT, поступающий из интерфейса "inside" в менее безопасные интерфейсы (по умолчанию)
4. **Нажмите кнопку OK, а затем нажмите Apply.**

Пример командной строки

cisco ASA
ciscoasa(config)#**access-list no_nat extended permit ip host 192.168.50.5 192.168.25.0 255.255.255.0** *!--- Define access list to be used for NAT exemption.* ciscoasa(config)#**nat (inside) 0 access-list no_nat** *!--- Allow external connections to untranslated internal !--- addresses defined by access lisy no_nat.* ciscoasa(config)#

Шаг 8. Добавление пользователей в локальную базу данных

При использовании локальной аутентификации (по умолчанию) необходимо определить имена пользователей и пароли в локальной базе данных для аутентификации пользователей.

Порядок действий в диспетчере ASDM

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. **Раскройте раздел AAA Setup, а затем раскройте раздел Local Users.**
3. **Выберите Add и введите следующие значения:Username:** matthewp**Password:** p@ssw0rd**Confirm Password:** p@ssw0rd
4. **Выберите переключатель No ASDM, SSH, Telnet or Console Access.**
5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Повторите это действие для других пользователей, а затем щелкните Save.**

Пример командной строки

cisco ASA
ciscoasa(config)#**username matthewp password p@ssw0rd** ciscoasa(config)#**username matthewp attributes** ciscoasa(config-username)#**service-type remote-access** *!--- Assign user remote access only. No SSH, Telnet, ASDM access allowed.* ciscoasa(config-username)#**write memory** *!--- Save the configuration.*

Проверка

С помощью сведений в этом разделе можно убедиться в успешности конфигурации SSL VPN

Подключитесь к ASA с помощью клиента AnyConnect

Установите клиент прямо на компьютер и подключите внешний интерфейс ASA. Кроме того,

можно ввести https и полное доменное имя (или IP-адрес) ASA в браузере. При использовании браузера клиент устанавливается после успешного входа в систему.

Проверка подключений клиента SSL VPN

Воспользуйтесь командой show vpn-sessiondb svc, чтобы проверить подключенные клиенты SSL VPN.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc Session Type: SVC Username : matthewp Index
: 6 Assigned IP : 192.168.25.1 Public IP : 172.18.12.111 Protocol : Clientless SSL-Tunnel DTLS-
Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 35466 Bytes Rx : 27543 Group Policy :
SSLClientPolicy Tunnel Group : SSLClientProfile Login Time : 20:06:59 UTC Tue Oct 16 2007
Duration : 0h:00m:12s NAC Result : Unknown VLAN Mapping : N/A VLAN : none ciscoasa(config-group-
policy)#
```

Команда vpn-sessiondb logoff name username дает пользователям возможность выполнять вход по имени пользователя. После отключения пользователю отправляется сообщение Administrator Reset.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp Do you want to logoff the VPN session(s)?
[confirm] INFO: Number of sessions with name "matthewp" logged off : 1 ciscoasa(config)#
```

Дополнительные сведения о клиенте AnyConnect 2.0 см. в документе Руководство администратора Cisco AnyConnect VPN.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды устранения неисправностей (необязательные)

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 webvpn svc 255 — отображение сообщений отладки о подключениях к клиентам SSL VPN с помощью WebVPN.Успешный вход в AnyConnect**

```
ciscoasa(config)#debug webvpn svc 255 INFO: debug webvpn svc enabled at level 255. ciscoasa(config)#ATTR_FILTER_ID: Name:
SSLVPNClientAccess , Id: 1, refcnt: 1 webvpn_rx_data_tunnel_connect CSTP state =
HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field() ...input: 'Host: 10.10.1.5' - !--- Outside IP of ASA
Processing CSTP header line: 'Host: 10.10.1.5' webvpn_cstp_parse_request_field() ...input:
'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version Processing
CSTP 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=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
Processing CSTP header line: 'Cookie: webvpn=3338474156@28672@119
2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN cookie:
'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE' WebVPN
Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02 164F790435897AC72EE70AE'
IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782' webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1' Processing CSTP header line: 'X-CSTP-Version: 1' Setting
version to '1' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: wkstation1' -
!--- Client desktop hostname Processing CSTP header line: 'X-CSTP-Hostname: wkstation1'
```

Setting hostname to: '**wkstation1**' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0' Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1206' Processing CSTP header line: 'X-CSTP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4' webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51' Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51' 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: **192.168.25.1/255.255.255.0** - *!--- IP assigned from IP Pool* CSTP state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, 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 sessmgmt 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 **Неудачный вход в AnyConnect (неправильный пароль)**webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT) webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0 ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0 ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180] WebVPN: user: (**matthewp**) **rejected**.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749] webvpn_portal.c:http_webvpn_kill_cookie[627]

Дополнительные сведения

- Руководства администратора Cisco AnyConnect VPN Client, версия 2.0
- Комментарии к выпуску для AnyConnect VPN Client (выпуск 2.0)
- Cisco Systems – техническая поддержка и документация