ASA 8. x Вручную Сертификаты Поставщика третьей стороны Установки для использования с Примером конфигурации WebVPN

Содержание

Введение

В этом примере конфигурации описывается метод установки цифрового сертификата стороннего поставщика в ASA для использования вместе с WebVPN. В данном примере используется пробный сертификат Verisign. Каждый шаг состоит из процедуры приложения ASDM и примера интерфейса командной строки.

Предварительные условия

Требования

Для выполнения действий, описанных в этом документе, необходимо иметь доступ к центру сертификации (CA) для регистрации сертификатов. Список примеров сторонних поставщиков CA включает, помимо прочего, следующие компании: Baltimore, Cisco, Entrust, Geotrust, Godaddy, iPlanet/Netscape, Microsoft, RSA, Thawte и VeriSign.

Используемые компоненты

Этот документ относится к ASA 5510, где запущена версия ПО 8.0(2) и версия ASDM 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.

Настройка

Чтобы установить цифровой сертификат стороннего поставщика в ASA, выполните следующие действия:

1. Проверьте, что Дата, Время и Значения Часового пояса Точна
2. Генерируйте запрос подписи сертификата
3. Аутентифицируйте точку доверия
4. Установите сертификат
5. Настройте WebVPN для Использования нового установленного сертификата

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

Шаг 1. Проверьте, что Дата, Время и Значения Часового пояса Точна

Порядок действий в диспетчере ASDM

1. **Нажмите кнопку Configuration, после чего нажмите Device Setup.**
2. **Разверните раздел System Time и выберите Clock.**
3. Проверьте правильность отображаемой информации.Значения параметров Date, Time и Time Zone должны быть правильными, чтобы проверка сертификата прошла успешно.

Пример командной строки

cisco ASA
ciscoasa#**show clock** 11:02:20.244 UTC Thu Jul 19 2007 ciscoasa#

Шаг 2. Генерируйте запрос подписи сертификата

Запрос на подписывание сертификата (CSR) требуется для того, чтобы сторонний центр сертификации выпустил идентификационный сертификат. В запросе CSR содержится строка с отличительным именем (DN) ASA вместе со сгенерированным открытым ключом ASA. Устройство ASA использует сгенерированный закрытый ключ для цифрового

подписания запроса CSR.

Порядок действий в диспетчере ASDM

1. **Нажмите кнопку Configuration, после чего нажмите Device Management.**
2. **Разверните Certificate Management и выберите Identity Certificates.**
3. **Нажмите Add.**
4. **Установите переключатель в положение Add a new identity certificate.**
5. **Для параметра «Key Pair» нажмите кнопку New.Примечание:** При использовании сертификат на 2048 битов, генерируете ключ на 2048 битов также.
6. **Установите переключатель в положение Enter new key pair name.** Необходимо четко указать название пары ключей, чтобы их можно было распознать.
7. **Нажмите кнопку Generate Now.**Теперь нужно создать пару ключей.
8. **Чтобы определить DN субъекта сертификата, щелкните Select и настройте атрибуты, перечисленные в этой таблице:Таблица 4.1: Атрибуты DNЧтобы настроить эти значения, выберите значение в раскрывающемся списке "Атрибут", введите его и щелкните Add.Примечание:** Некоторые сторонние поставщики требуют включения определенных атрибутов перед выдачей идентификационного сертификата. Если вы не уверены в том, какие атрибуты необходимы, обратитесь за подробными сведениями к своему поставщику.
9. **После добавления соответствующих значений нажмите кнопку OK.**Откроется диалоговое окно «Add Identity Certificate» с заполненным полем «Certificate Subject DN».
10. **Нажмите кнопку Advanced.**
11. В поле FQDN введите полное имя домена, которое будет использоваться для подключения к устройству из Интернета.Это значение должно совпадать со значением FQDN, используемым для общего имени (CN).
12. **Щелкните OK, а затем выберите Add Certificate.**Будет предложено сохранить запрос CSR в файл на локальном компьютере.
13. **Щелкните Browse, выберите местоположение для сохранения CSR и сохраните файл с расширением .txt.Примечание:** При сохранении файла с расширением .txt с помощью текстового редактора (например, блокнота) этот файл можно открыть и просмотреть запрос PKCS#10.
14. Отправьте сохраненный CSR своему стороннему поставщику. После отправки CSR своему стороннему поставщику он предоставит вам идентификационный сертификат, который должен быть установлен в ASA.

Пример командной строки

В ASDM 6.x автоматически создается точка доверия при создании CSR или установке сертификата CA. В интерфейсе командной строки точку доверия необходимо создать вручную.

cisco ASA
ciscoasa#**conf t** ciscoasa(config)#**crypto key generate rsa label my.verisign.key modulus 1024 ! Generates 1024 bit RSA key pair. "label" defines ! the name of the Key Pair.** INFO: The name for the keys will be: my.verisign.key Keypair generation process begin. Please wait... ciscoasa(config)#**crypto ca trustpoint my.verisign.trustpoint** ciscoasa(config-ca-

```
trustpoint)#subject-name CN=webvpn.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh ! 
Defines x.500 distinguished name. Use the attributes ! 
defined in table 4.1 in Step 2 as a guide.
ciscoasa(config-ca-trustpoint)#keypair my.verisign.key ! 
Specifies key pair generated in Step 3. ciscoasa(config-
ca-trustpoint)#fqdn webvpn.cisco.com ! Specifies the 
FQDN (DNS:) to be used as the subject ! alternative 
name. ciscoasa(config-ca-trustpoint)#enrollment terminal 
! Specifies manual enrollment. ciscoasa(config-ca-
trustpoint)#exit ciscoasa(config)#crypto ca enroll 
my.verisign.trustpoint ! Initiates certificate signing 
request. This is the request ! to be submitted via Web 
or Email to the 3rd party vendor. % Start certificate 
enrollment .. % The subject name in the certificate will 
be: CN=webvpn.cisco.com,OU=TSWEB, O=Cisco 
Systems,C=US,St=North Carolina,L=Raleigh % The fully-
qualified domain name in the certificate will be: 
webvpn.cisco.com % Include the device serial number in 
the subject name? [yes/no]: no ! Do not include the 
device's serial number in the subject. Display 
Certificate Request to terminal? [yes/no]: yes ! 
Displays the PKCS#10 enrollment request to the terminal. 
! You will need to copy this from the terminal to a text 
! file or web text field to submit to the 3rd party CA. 
Certificate Request follows: 
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not 
part of the certificate request--- Redisplay enrollment 
request? [yes/no]: no ciscoasa(config)#
```

Шаг 3. Аутентифицируйте точку доверия

После получения идентификационного сертификата от стороннего поставщика можно перейти к этому шагу.

Порядок действий в диспетчере ASDM

1. Сохраните идентификационный сертификат на локальном компьютере.
2. Если вы получили сертификат в кодировке base64 не в виде файла, то необходимо

скопировать текст этого сертификата и вставить в текстовый файл.

3. Переименуйте файл, изменив его расширение на .cer. Примечание: После переименования файла с присвоением ему расширения .cer значок файла должен отображаться в виде сертификата.
4. Дважды щелкните файл сертификата.Появится диалоговое окно Certificate.**Примечание:** *Если на вкладке General появляется сообщение "Windows does not have enough information to verify this certificate", то для продолжения процедуры необходимо получить корневой сертификат стороннего поставщика или промежуточный сертификат CA.* Свяжитесь со своим сторонним поставщиком или администратором CA, чтобы получить корневой сертификат выпустившего его CA или промежуточный сертификат CA.
5. **Щелкните вкладку Путь к сертификату.**
6. **Выберите сертификат CA, расположенный над вашим выпущенным идентификационным сертификатом, и нажмите View Certificate.**Подробные сведения о промежуточном сертификате CA появляются.**% Warning:** Не устанавливайте идентификационный сертификат (сертификат устройства) на этом шаге. На данном этапе добавляется только корневой сертификат, подчиненный корневой сертификат или сертификат CA. Идентификационные сертификаты (сертификаты устройства) устанавливаются на шаге 4.
7. **Нажмите кнопку Details.**
8. **Щелкните Copy to File.**
9. **В Certificate Export Wizard щелкните Next.**
10. **В диалоговом окне Export File Format щелкните переключатель Base-64 encoded X.509 (.CER), а затем выберите Next.**
11. Введите имя файла и папки, в которую требуется сохранить сертификат CA.
12. **Щелкните Next, а затем — Finish.**
13. **Щелкните OK в диалоговом окне Export Successful.**
14. Перейдите к месту размещения сохраненного сертификата CA.
15. Откройте файл в текстовом редакторе, например, в "Блокнот". **Щелкните его правой кнопкой, а затем выберите Отправить > Блокнот.**)Должно появиться сообщение в кодировке base64, которое похоже на сертификат на следующем рисунке:
16. **В диспетчере ASDM нажмите кнопку Configuration, после чего нажмите Device Management.**
17. **Разверните Certificate Management и выберите CA Certificates.**
18. **Нажмите Add.**
19. **Щелкните переключатель Paste certificate in PEM Format и вставьте в текстовое поле сертификат центра сертификации, предоставленный сторонним поставщиком.**
20. **Нажмите кнопку Install Certificate (Установить сертификат).**Диалоговое окно появляется, который подтверждает, что установка была успешна.

Пример командной строки

cisco ASA
ciscoasa(config)#**crypto ca authenticate my.verisign.trustpoint** *! Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provided by the 3rd party vendor.* Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself **-----BEGIN CERTIFICATE----- MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B**

```
AQUFADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk1OVowgcsxCzAJBgNVBAYT
AlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEzlUZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD
QTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6
1BBD6Zqk
d85lPl/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAwEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZlcmlzaWdu
LmNvbS9j
cHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
AgEGMB0G
A1UdDgQWBBRmIo6B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4x
MDAuBgNV
BAsTJ0ZvciBUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
LjEyMDAG
A1UEAxMpVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IFJv
b3QgQ0GC
ECCol67bggLewTagTia9h3MwDQYJKoZIhvcNAQEFBQADgYEASz5v8s3/
SjzRvY2l
Kqf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5q0mB+nyK9fB2aBzOiaiHSiIWzAJeQjuqA+Q93jNew+peu
j4AhdvGN n/KK/+1Yv61w3+7g6ukFMARVBNg= -----END
CERTIFICATE----- quit ! Manually pasted certificate into
CLI. INFO: Certificate has the following attributes:
Fingerprint: 8de989db 7fcc5e3b fdde2c42 0813ef43 Do you
accept this certificate? [yes/no]: yes Trustpoint
'my.verisign.trustpoint' is a subordinate CA and holds a
non self-signed certificate. Trustpoint CA certificate
accepted. % Certificate successfully imported
ciscoasa(config)# ciscoasa(config-ca-trustpoint)# exit
```

Шаг 4. . Установите сертификат

Порядок действий в диспетчере ASDM

Для выполнения этих шагов используйте идентификационный сертификат, предоставленный сторонним поставщиком:

1. **Нажмите кнопку Configuration, после чего нажмите Device Management.**
2. **Разверните раздел Certificate Management и выберите Identity Certificates.**
3. Выберите идентификационный сертификат, созданный на шаге 2 (в поле Expiry Date должно быть указано значение Pending).)
4. **Нажмите кнопку Install (Установить).**
5. Нажмите **Paste данные сертификата в** кнопке с зависимой фиксацией **формата base64** и вставьте сертификат идентификации, предоставленный поставщиком третьей стороны в текстовое поле.
6. **Нажмите кнопку Install Certificate (Установить сертификат).**Появится диалоговое окно, подтверждающее успешное выполнение импорта.

Пример командной строки

cisco ASA

```
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate ! Initiates prompt to paste the base64
identity ! certificate provided by the 3rd party vendor.
% The fully-qualified domain name in the certificate
will be: webvpn.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself ! Paste the base 64 certificate provided by the
3rd party vendor. -----BEGIN CERTIFICATE-----
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
QjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5j
b20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
dXJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4G
A1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQF
VFNXRUIx
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2ln
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHQYD
```

```
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYi
joHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYY
aHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZS
U2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N
7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/
54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE----- quit INFO: Certificate
successfully imported ciscoasa(config)#
```

Шаг 5. . Настройте WebVPN для Использования нового установленного сертификата

Порядок действий в диспетчере ASDM

1. **Нажмите кнопку Configuration, после чего нажмите Device Management.**
2. **Раскройте раздел Advanced, а затем раскройте раздел SSL Settings.**
3. Под Сертификатами выберите интерфейс, который используется для завершения сеансов WebVPN.В этом примере применяется внешний интерфейс.
4. **Нажмите Edit.**
5. В раскрывающемся списке Certificate выберите сертификат, установленный на шаге 4.
6. **Нажмите кнопку OK.**
7. **Щелкните "Применить".**Ваш новый сертификат должен теперь применяться во всех сеансах WebVPN, которые завершаются в указанном интерфейсе.
8. Чтобы подтвердить успешную установку, см. раздел Проверка.

Пример командной строки

cisco ASA

```
ciscoasa(config)#ssl trust-point my.verisign.trustpoint
outside ! Specifies the trustpoint that will supply the
! SSL certificate for the defined interface.
ciscoasa(config)# wr mem Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08 8808
bytes copied in 3.630 secs (2936 bytes/sec) [OK]
ciscoasa(config)# ! Save configuration.
```

Проверка

Используйте следующие шаги для проверки успешной установки Сертификата Поставщика

третьей стороны и использования для подключений WebVPN.

Просмотрите установленные сертификаты

Порядок действий в диспетчере ASDM

1. Щелкните Configuration, а затем выберите Device Management.
2. Разверните Certificate Management и выберите Identity Certificates.На экране должен появиться идентификационный сертификат, выпущенный сторонним поставщиком.

Пример командной строки

cisco ASA

```
ciscoasa(config)#show crypto ca certificates ! Displays
all certificates installed on the ASA. Certificate
Status: Available Certificate Serial Number:
32cfe85eebbd2b5e1e30649fd266237d Certificate Usage:
General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test CA ou=Terms
of use at https://www.verisign.com/cps/testca ©)05
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=webvpn.cisco.com ou=Terms of
use at www.verisign.com/cps/testca ©)05 ou=TSWEB o=Cisco
Systems l=Raleigh st=North Carolina c=US OCSP AIA: URL:
http://ocsp.verisign.com CRL Distribution Points: [1]
http://SVRSecure-crl.verisign.com/SVRTrial2005.crl
Validity Date: start date: 00:00:00 UTC Jul 19 2007 end
date: 23:59:59 UTC Aug 2 2007 Associated Trustpoints:
my.verisign.trustpoint ! Identity certificate received
from 3rd party vendor displayed above. CA Certificate
Status: Available Certificate Serial Number:
63b1a5cdc59f78801da0636cf975467b Certificate Usage:
General Purpose Public Key Type: RSA (2048 bits) Issuer
Name: cn=VeriSign Trial Secure Server Test Root CA
ou=For Test Purposes Only. No assurances. o=VeriSign\,
Inc. c=US Subject Name: cn=VeriSign Trial Secure Server
Test CA ou=Terms of use at
https://www.verisign.com/cps/testca ©)05 ou=For Test
Purposes Only. No assurances. o=VeriSign\, Inc. c=US
Validity Date: start date: 00:00:00 UTC Feb 9 2005 end
date: 23:59:59 UTC Feb 8 2015 Associated Trustpoints:
my.verisign.trustpoint ! CA intermediate certificate
displayed above.
```

Проверка установленного сертификата для WebVPN с помощью браузера

Чтобы удостовериться в том, что в WebVPN используется новый сертификат, выполните следующие действия:

1. Подключитесь к своему интерфейсу WebVPN с помощью браузера. Включите в адрес префикс https://, а также полное доменное имя, использованное при запросе сертификата (например, https://webvpn.cisco.com).При получении одного из следующих оповещений безопасности выполните процедуру, соответствующую этому оповещению:**Название сертификата безопасности недопустимо или не совпадает с названием узла**Проверьте использование корректного FQDN/CN для соединения с интерфейсом WebVPN ASA. Необходимо использовать полное доменное имя или

общее имя, определенное при запрашивании идентификационного сертификата. *Можно применить команду show crypto ca certificates имя точки доверия, чтобы проверить полное доменное имя или общее имя сертификатов.***Сертификат безопасности был выпущен компанией, для которой вы не выбрали параметр доверия...**Выполните указанные ниже шаги, чтобы установить корневой сертификат стороннего производителя в свой браузер:**В диалоговом окне Security Alert щелкните View Certificate.В диалоговом окне Certificate щелкните вкладку Certificate Path.Выберите сертификат CA, расположенный над выпущенным вами идентификационным сертификатом, и нажмите View Certificate.Нажмите кнопку Install Certificate (Установить сертификат).В диалоговом окне Certificate Install Wizard щелкните Next.**Нажмите **Automatically выбирают хранилище сертификата на основе типа** кнопки с зависимой фиксацией **сертификата**, **нажимают Next**, и затем нажимают **Finish**.**Щелкните Yes при появлении окна для подтверждения установки сертификата.В окне Import operation was successful щелкните OK, а затем нажмите Yes.Примечание:** Поскольку в этом примере используется пробный сертификат Verisign, должен быть установлен пробный корневой сертификат Verisign CA во избежание появления ошибок во время проверки при подключении пользователей.
2. Дважды щелкните значок замка, который расположен в правом нижнем углу страницы входа в WebVPN.На экране должна появиться информация об установленном сертификате.
3. Просмотрите содержимое, чтобы подтвердить, что оно совпадает с вашим сертификатом стороннего поставщика.

Команды

В ASA можно воспользоваться несколькими командами группы show в командной строке для проверки статуса сертификата.

- **show crypto ca trustpoint Отображает настроенные точки доверия.**
- **show crypto ca certificate Отображает все сертификаты, установленные в системе.**
- **show crypto ca crls Отображает списки отзыва кэшированных сертификатов (CRL).**
- **show crypto key mypubkey rsa Отображает все сгенерированные пары криптоключей.**

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

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Здесь приведен ряд сообщений об ошибках, с которыми можно столкнуться:

- **% Warning: CA cert is not found. The imported certs might not be usable.INFO: Сертификат успешно импортирован**Сертификат CA не аутентифицировался правильно. *Воспользуйтесь командой show crypto ca certificate имя доверенного CA, чтобы проверить, установлен ли сертификат CA*. Если сертификат центра сертификации существует, убедитесь в том, что он ссылается на правильную точку доверия.
- **Ошибка: Failed to parse or verify imported certificate (Не удалось обработать или**

проверить импортированный сертификат)Эта ошибка может возникнуть тогда, когда был установлен идентификационный сертификат, но не было правильного сертификата промежуточного или корневого CA, удостоверенного связанной точкой доверия. Необходимо удалить и произвести повторную аутентификацию с помощью правильного сертификата промежуточного или корневого CA . Свяжитесь со своим сторонним поставщиком, чтобы убедиться в получении правильного сертификата CA.

- **Certificate does not contain general purpose public key (Сертификат не содержит открытых ключей общего назначения)**Эта ошибка может возникнуть при попытке установить идентификационный сертификат на неверную точку доверия. Вы пытаетесь установить неверный идентификационный сертификат или пара ключей, связанная с точкой доверия, не подходит открытому ключу, содержащемуся в идентификационном сертификате. *Воспользуйтесь командой show crypto ca certificates имя точки доверия, чтобы удостовериться, что ваш идентификационный сертификат установлен в правильную точку доверия. Обратите внимание на строку Associated Trustpoints:* Если указана неверная точка доверия, используйте процедуры, описанные в этом документе, чтобы удалить и установить подходящую точку доверия. Также проверьте, не изменилась ли пара ключей с момента создания запроса CSR.
- **: %PIX|ASA-3-717023 SSL не удалось установить сертификат устройства для доверенного CA [имя доверенного CA]**Это сообщение отображается при появлении сбоя, когда сертификат устройства задается для заданной точки доверия, чтобы проверить подлинность подключения SSL. При установке подключения SSL предпринимается попытка задать используемый сертификат устройства. При возникновении сбоя создается сообщение об ошибке, включающее настроенную точку доверия, которая должна использоваться для загрузки сертификата устройства, и причину сбоя.*имя точки доверия — имя точки доверия, для которой SSL не удалось задать сертификат устройства*.**Рекомендуемое действие:** Решите проблему, которая определяется причиной, сообщенной для сбоя.Убедитесь в том, что указанная точка доверия зарегистрирована и обладает сертификатом устройства.Убедитесь, что используется действительный сертификат устройства.При необходимости повторно зарегистрируйте точку доверия.

Дополнительные сведения

- Получение цифрового сертификата в Microsoft Windows CA с помощью ASDM на ASA
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация