Получение цифрового сертификата в Microsoft Windows CA с помощью ASDM на ASA

Содержание

Введение

Цифровые сертификаты могут использоваться для аутентификации сетевых устройств и пользователей в сети. Они могут использоваться для согласования сеансов IPsec между узлами сети.

Устройства Cisco определяют себя надежно в сети тремя основными способами:

1. **Предварительные ключи.** Два или больше устройства могут иметь тот же общий секретный ключ. Узлы аутентифицируют друг друга путем вычислений и передачи хэширования по ключу данных, которые включают общий ключ. Если принимающий пиринговый узел в состоянии создать тот же хэш независимо с помощью его общего ключа, это знает, что оба узла должны совместно использовать ту же тайну, таким образом аутентифицируя другой узел. Этот метод является ручным и не очень масштабируемым.
2. **Подписанные сертификаты**. Устройство генерирует свой собственный сертификат и подписывает его как являющийся допустимым. Этот тип сертификата должен был ограничить использование. Использование этого сертификата с SSH и доступом

HTTPS для целей настройки является хорошими примерами. Отдельная пара из имени пользователя/пароля необходима для завершения соединения.**Примечание:** Персистентные Подписанные сертификаты переживают перезагрузки маршрутизатора, потому что они сохранены в Nonvolatile Random Access Memory (NVRAM) устройства. См. Персистентные Подписанные сертификаты для получения дополнительной информации. Один хороший пример использования является с VPN SSL (WebVPN) соединениями.

3. **Сертификат Центра сертификации**. Третья сторона проверяет и аутентифицирует два или больше узла та попытка связаться. Каждый узел имеет открытый и закрытый ключ. Открытый ключ шифрует данные, и секретный ключ дешифрует данные. Поскольку они получили свои сертификаты из того же источника, они могут быть уверены в своих соответствующих личностях. Устройство ASA может получить цифровой сертификат из независимого поставщика с методом ручной регистрации или автоматическим методом регистрации.**Примечание:** Метод регистрации и тип цифрового сертификата, который вы выбираете, зависят от функций и функций каждого стороннего продукта. Свяжитесь с поставщиком сервиса сертификации для получения дополнительной информации.

Устройство адаптивной защиты Cisco (ASA) может использовать предварительные общие ключи или цифровые сертификаты, предоставленные сторонним Центром сертификации (CA) для аутентификации IP - безопасных соединений. Кроме того, ASA может произвести свой собственный самоподписанный цифровой сертификат. Это должно использоваться для SSH, HTTPS и Cisco Adaptive Security Device Manager (ASDM) соединения с устройством.

Этот документ демонстрирует процедуры, необходимые для автоматического получения цифрового сертификата из Microsoft Certificate Authority (CA) для ASA. Это не включает ручной способ регистрации. Этот документ использует ASDM для действий настройки, а также представляет заключительную конфигурацию интерфейса командной строки (CLI).

См. Хранилище сертификатов Cisco IOS Использование Примера конфигурации Расширенных команд регистрации для узнавания больше о том же сценарии с платформами Cisco IOS®.

См. Настройку Cisco VPN 3000 Concentrator 4.7.x для Получения Цифрового сертификата и сертификата SSL для узнавания больше о том же сценарии с концентратором Cisco VPN серии 3000.

Предварительные условия

Требования

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

Требования к устройству ASA

- Настройте Microsoft® Windows 2003 Server как CA.См. вашу документацию microsoft или к Инфраструктуре открытых ключей для Windows Server 2003
- Чтобы позволить Cisco ASA или Версии PIX 7.x быть настроенным Менеджером устройств адаптивной безопасности (ASDM) (ASDM), обратитесь к документу

Разрешение HTTPS-доступа для ASDM.
- Установите дополнение для сервисов сертификации (mscep.dll).
- Получите исполняемый файл (cepsetup.exe) для Дополнения от Дополнения Протокола SCEP (SCEP) для Сервисов сертификации или mscep.dll файла от Программных средств Пакета ресурсов Windows Server 2003.**Примечание:** Настройте корректную дату, время и часовой пояс на машине Microsoft Windows. Использование Протокола NTP настоятельно рекомендовано, но не необходимое.

Используемые компоненты

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

- Многофункциональное устройство защиты Cisco ASA серии 5500, Версия программного обеспечения 7.x и позже
- Диспетчер многофункциональных устройств защиты Adaptive Security Device Manager (ASDM) версии 5.x и более поздних версий
- Центр сертификации Microsoft Windows 2003 Server

Родственные продукты

Эта конфигурация может также использоваться с Версией 7 устройства защиты Cisco PIX серии 500. x.

Условные обозначения

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

Настройте ASA к сертификатам Exchange с Microsoft CA

Задача

В этом разделе вас показывают, как настроить ASA для получения сертификата от Microsoft Certificate Authority.

Инструкции для Настройки ASA

Цифровые сертификаты используют компонент даты/времени/часового пояса в качестве одной из проверок для Достоверности сертификата. Обязательно настроить Microsoft CA и все ваши устройства с корректной датой и времей. Microsoft CA использует дополнение (mscep.dll) для его Сервисов сертификации чтобы к акционерным сертификатам с устройствами Cisco.

Выполните эти шаги для настройки ASA:

1. Откройте приложение ASDM и нажмите кнопку **Configuration**.Из левого меню нажмите **Кнопку свойства**.От панели переходов нажмите **Device Administration> Device**.Введите

имя хоста и доменное имя для ASA. **Щелкните "Применить".**Когда предложено, нажмите **Save> Yes**.

2. Настройте ASA с корректной датой, время и часовой пояс. Это важно для генерации сертификата устройства. Используйте сервер NTP, если это возможно.От панели переходов нажмите **Device Administration> Clock**.В окне Clock используйте поля и стрелки выпадающего списка для назначения корректной даты, время и часовой пояс.
3. ASA должен иметь свою собственную пару ключей (секретные и открытые ключи). Открытый ключ будет передаваться Microsoft CA.От панели переходов нажмите **Certificate> Key Pair**.Нажмите **кнопку Add** и показы диалогового окна Add Key Pair.Проверьте кнопку с зависимой фиксацией около пустого поля области **Name** и введите на название для ключа.Нажмите **Размер:** стрелка раскрывающимся окном, чтобы выбрать размер для ключа или принять по умолчанию.Проверьте кнопку с зависимой фиксацией **General Purpose** при Использовании.Нажмите кнопку **Generate Now**, чтобы восстановить ключи и возвратиться к окну Key Pair, где можно просмотреть информацию для пары ключей.
4. Настройте Microsoft CA, которую будут считать защищенными. От панели переходов нажмите **Trustpoint> Configuration**.От Окна конфигурации нажмите **кнопку Add**.Показы Окна конфигурации Точки доверия Редактирования.Заполните название для Точки доверия с названием CA.Нажмите **Пару ключей:** стрелка раскрывающимся окном, и выбирает название пары ключей, которую вы создали.Проверьте **Использование автоматическая кнопка с зависимой фиксацией enrollment** и введите URL для Microsoft CA: **http://CA_IP_Address/certsrv/mscep/mscep.dll**.
5. Нажмите вкладку **Crl Retrieval Method**.Анчек Разрешать HTTP и Включите флажки Протокола LDAP.Проверьте флажок Enable Simple Certificate Enrollment Protocol (SCEP). Оставьте все другие установки позиций табуляции при их настройках по умолчанию.**Нажмите кнопку «ОК».**
6. Аутентифицируйте и зарегистрируйте с Microsoft CA. From панель переходов, нажмите **Certificate> Authentication**. Удостоверьтесь, недавно созданная точка доверия показывает на **Название Точки доверия:** поле. Нажмите кнопку **Authenticate**.
7. Диалоговое окно отображается, чтобы сообщить вам, что аутентифицировалась точка доверия. **Нажмите кнопку «ОК».**
8. От панели переходов нажмите **Enrollment**. Удостоверьтесь показы названия точки доверия в Поле имени Точки доверия и нажмите кнопку **Enroll**.
9. Диалоговое окно отображается, чтобы сообщить вам, что запрос был отправлен к CA. **Нажмите кнопку «ОК».Примечание: На Автономном устройстве Microsoft Windows необходимо выполнить сертификаты для любых запросов, которые были отправлены к CA., которым сертификат будет в состоянии ожидания, пока вы не щелкнете правой кнопкой по сертификату и проблеме щелчка на сервере Microsoft.**

Результаты

Это - конфигурация интерфейса командой строки, которая следует из шагов ASDM:

cisco ASA
ciscoasa# sh run ASA Version 7.2(1) ! hostname ciscoasa

```
domain-name cisco.com
enable password t/G/EqWCJSp/Q6R4 encrypted
names
name 172.22.1.172 AUSNMLAAA01
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.4.4.1 255.255.255.0
!
interface Ethernet0/2
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
ftp mode passive
!--- Set your correct date/time/time zone ! clock
timezone CST -6 clock summer-time CDT recurring dns
server-group DefaultDNS domain-name cisco.com pager
lines 20 logging enable logging asdm informational mtu
inside 1500 mtu outside 1500 asdm image
disk0:/asdm521.bin no asdm history enable arp timeout
14400 nat (inside) 0 0.0.0.0 0.0.0.0 route outside
0.0.0.0 0.0.0.0 172.22.1.1 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
username cisco password VjcVTJy0i9Ys9P45 encrypted
privilege 15 http server enable http AUSNMLAAA01
255.255.255.255 outside http 172.22.1.0 255.255.255.0
outside http 64.101.0.0 255.255.0.0 outside no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart ! !--- identify the trustpoint ! crypto ca
trustpoint ausnmlaaa01 enrollment url
http://172.22.1.172:80/certsrv/mscep/mscep.dll keypair
key1 crl configure no protocol http no protocol ldap !--
- the certificate chain generated automatically crypto
ca certificate chain ausnmlaaa01 certificate
61c79bea000100000008 30820438 30820320 a0030201 02020a61
c79bea00 01000000 08300d06 092a8648 86f70d01 01050500
30423113 3011060a 09922689 93f22c64 01191603 636f6d31
15301306 0a099226 8993f22c 64011916 05636973 636f3114
30120603 55040313 0b617573 6e6d6c61 61613031 301e170d
30363038 31363231 34393230 5a170d30 37303831 36323135
3932305a 30233121 301f0609 2a864886 f70d0109 02131263
6973636f 6173612e 63697363 6f2e636f 6d30819f 300d0609
2a864886 f70d0101 01050003 818d0030 81890281 8100c2c7
fefc4b18 74e7972e daee53a2 b0de432c 4d34ec76 48ba37e6
```

e7294f9b 1f969088 d3b2aaef d6c44cfa bdbe740b f5a89131
b177fd52 e2bfb91c d665f54e 7eee0916 badc4601 79b4f7b3
8102645a 01fedb62 e8db2a60 188d13fc 296803a5 68739bb6
940cd33a d746516f 01d52935 8b6302b6 3c3e1087 6c5e91a9
c5e2f92b d3cb0203 010001a3 8201d130 8201cd30 0b060355
1d0f0404 030205a0 301d0603 551d1104 16301482 12636973
636f6173 612e6369 73636f2e 636f6d30 1d060355 1d0e0416
0414080d fe9b7756 51b5e63b fa6dcfa5 076030db 08c5301f
0603551d 23041830 16801458 026754ae 32e081b7 8522027e
33bffe79 c6abb730 75060355 1d1f046e 306c306a a068a066
86306874 74703a2f 2f617573 6e6d6c61 61613031 2f436572
74456e72 6f6c6c2f 6175736e 6d6c6161 61303128 31292e63
726c8632 66696c65 3a2f2f5c 5c415553 4e4d4c41 41413031
5c436572 74456e72 6f6c6c5c 6175736e 6d6c6161 61303128
31292e63 726c3081 a606082b 06010505 07010104 81993081
96304806 082b0601 05050730 02863c68 7474703a 2f2f6175
736e6d6c 61616130 312f4365 7274456e 726f6c6c 2f415553
4e4d4c41 41413031 5f617573 6e6d6c61 61613031 2831292e
63727430 4a06082b 06010505 07300286 3e66696c 653a2f2f
5c5c4155 534e4d4c 41414130 315c4365 7274456e 726f6c6c
5c415553 4e4d4c41 41413031 5f617573 6e6d6c61 61613031
2831292e 63727430 3f06092b 06010401 82371402 04321e30
00490050 00530045 00430049 006e0074 00650072 006d0065
00640069 00610074 0065004f 00660066 006c0069 006e0065
300d0609 2a864886 f70d0101 05050003 82010100 0247af67
30ae031c cbd9a2fb 63f96d50 a49ddff6 16dd377d d6760968
8ad6c9a8 c0371d65 b5cd6a62 7a0746ed 184b9845 84a42512
67af6284 e64a078b 9e9d1b7a 028ffdd7 d262f6ba f28af7cf
57a48ad4 761dcfda 3420c506 e8c4854c e4178304 a1ae6e38
a1310b5b 2928012b 40aaad56 1a22d4ce 7d62a0e5 931f74f5
5510574f 27a6ea21 3f3d2118 2a087aad 0177cc56 1f8c024c
42f9fb9a ef180bc1 4fca1504 59c3b850 acad01a9 c2fbb46b
2be53a9f 10ad50a4 1f557b8d 1f25f7ae b2e2eeca 7800053c
3afd436 73863d76 53bd58c9 803fe5e9 708f00fd 85e84220
0c713c3f 4ccb0c0b 84bb265d fd40c9d0 a68efb3e d6faeef0
b9958ca7 d1eb25f8 51f38a50 quit certificate ca
62829194409db5b94487d34f44c9387b 308203ff 308202e7
a0030201 02021062 82919440 9db5b944 87d34f44 c9387b30
0d06092a 864886f7 0d010105 05003042 31133011 060a0992
268993f2 2c640119 1603636f 6d311530 13060a09 92268993
f22c6401 19160563 6973636f 31143012 06035504 03130b61
75736e6d 6c616161 3031301e 170d3036 30383136 31383135
31325a17 0d313130 38313631 38323430 325a3042 31133011
060a0992 268993f2 2c640119 1603636f 6d311530 13060a09
92268993 f22c6401 19160563 6973636f 31143012 06035504
03130b61 75736e6d 6c616161 30313082 0122300d 06092a86
4886f70d 01010105 00038201 0f003082 010a0282 01010096
1abddec6 ce3768e6 4e04b42f ec28d6f9 330cd9a2 9ec3eb9e
8a091cf8 b4969158 3dc6d6ba 332bc3b4 32fc1495 9ac85322
1c842df1 7a110be2 7f2fc5e2 3a475da8 711e4ff7 0dd06c21
6f6e3517 621c89f9 a01779b8 3a5fce63 3ed66c58 2982dbf2
21f9c139 5cd6cf17 7bde4c0a 22033312 d1b98435 e3a05003
888da568 6223243f 834316f0 4874168d c291f098 24177ade
a71d5128 120e1848 6f8a5a33 6f4efa1c 27bb7c4d f49fb0f7
57736f7d 320cf834 1ef28649 b719ae7c e58de17f 1259f121
df90668d aee59f71 dd1110a2 de8a2a8b db6de0c7 b5540e21
4ff1a0c5 7cb0290e bfd5a7bb 21bd7ad3 bce7b986 e0f77b30
c8b719d9 37c355f6 ec103188 7d5d3702 03010001 a381f030
81ed300b 0603551d 0f040403 02018630 0f060355 1d130101
ff040530 030101ff 301d0603 551d0e04 16041458 026754ae
32e081b7 8522027e 33bffe79 c6abb730 75060355 1d1f046e
306c306a a068a066 86306874 74703a2f 2f617573 6e6d6c61
61613031 2f436572 74456e72 6f6c6c2f 6175736e 6d6c6161
61303128 31292e63 726c8632 66696c65 3a2f2f5c 5c415553

```
4e4d4c41 41413031 5c436572 74456e72 6f6c6c5c 6175736e
6d6c6161 61303128 31292e63 726c3012 06092b06 01040182
37150104 05020301 00013023 06092b06 01040182 37150204
16041490 48bcef49 d228efee 7ba90b35 879a5a61 6a276230
0d06092a 864886f7 0d010105 05000382 01010042 f59e2675
0defc49d abe504b8 eb2b2161 b76842d3 ab102d7c 37c021d4
a18b62d7 d5f1337e 22b560ae acbd9fc5 4b230da4 01f99495
09fb930d 5ff0d869 e4c0bf07 004b1deb e3d75bb6 ef859b13
6b6e0697 403a4a58 4f6dd1bc 3452f329 a73b572a b41327f7
5af61809 c9fb86a4 b8d4aca6 f5ebc97f 2c3e306b ea58ed49
c245be2a 03f40878 273ae747 02b22219 5e3450a9 6fd72f1d
40e0931a 7b5cc3b0 d6558ec7 514ef928 b1dfa9ab 732ecea0
40a458c3 e824fd6f b7c6b306 122da64d b3ab23b1 adacf609
1d1132fb 15aa6786 06fbf713 b25a4a5c 07de565f 6364289c
324aacff abd6842e b24d4116 5c0934b3 794545df 47da8f8d
2b0e8461 b2405ce4 6528 99 quit telnet 64.101.0.0
255.255.0.0 outside telnet timeout 5 ssh timeout 5
console timeout 0 ! 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 prompt hostname context
Cryptochecksum:fa0c88a5c687743ab26554d54f6cb40d : end
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Проверьте и управляйте своим сертификатом

Рассмотрите и управляйте своим сертификатом.

1. Откройте приложение ASDM и нажмите кнопку **Configuration**.
2. Из левого меню нажмите **Кнопку свойства**.Нажмите **Certificate**.Нажмите **Manage Certificate**.

Команды

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

- **Команда show crypto ca certificates** используется для просмотра информации о сертификате, сертификате CA и любых сертификатах центра регистрации (RA).
- **Команда show crypto ca trustpoints** используется для проверки конфигурации точки доверия.
- **Команда show crypto key mypubkey rsa** используется для отображения открытых ключей RSA ASA.
- **Команда show crypto ca crls** используется для отображения всех кэшируемых CRL.

Примечание: Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать**

выходные данные команд show.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

См. Инфраструктуру открытых ключей для Windows Server 2003 для получения дополнительной информации о том, как устранить неполадки CA. Microsoft Windows 2003 года

Команды

Примечание: Использование команд debug может неблагоприятно сказаться на производительности модуля Cisco. Перед использованием команд debug ознакомьтесь с документом Важные сведения о командах debug.

Дополнительные сведения

- Настройка Microsoft Certificate services
- Настройка Cisco VPN 3000 Concentrator 4.0.x для получения цифрового сертификата
- Версия программного обеспечения 7.1¡ Cisco PIX Security Appliance
- Cisco Systems – техническая поддержка и документация