El ASA 8.x instala manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN

Contenido

Introducción

Este ejemplo de configuración describe cómo instalar manualmente un certificado digital del vendedor de las de otras compañías en el ASA para el uso con el WebVPN. Un certificado de ensayo de Verisign se utiliza en este ejemplo. Cada paso contiene el procedimiento de la aplicación ASDM y un ejemplo CLI.

prerrequisitos

Requisitos

Este documento requiere que usted tenga acceso a un Certificate Authority (CA) para la inscripción del certificado. Los ejemplos de los vendedores de CA de las de otras compañías incluyen, pero no se limitan a, Baltimore, Cisco, confían, Geotrust, Godaddy, iPlanet/Netscape, Microsoft, RSA, Thawte, y Verisign.

Componentes Utilizados

Este documento utiliza un ASA 5510 que funcione con la versión de software 8.0(2) y la versión 6.0(2) del ASDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Para instalar un certificado digital del vendedor de las de otras compañías en el ASA, complete estos pasos:

1. Verifique que la fecha, el tiempo, y los valores del huso horario sean exactos
2. Genere un pedido de firma de certificado
3. Autentique el trustpoint
4. Instale el certificado
5. Configure el WebVPN para utilizar el certificado nuevamente instalado

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Paso 1. Verifique que la fecha, el tiempo, y los valores del huso horario sean exactos

Procedimiento del ASDM

1. Haga clic la **configuración**, y después haga clic la **configuración de dispositivo**.
2. Amplíe el **Tiempo del sistema**, y elija el **reloj**.
3. Verifique que la información enumerada sea exacta.Los valores por la fecha, el tiempo, y el huso horario deben ser exactos para que la validación de certificado apropiada ocurra.

Ejemplo de la línea de comando

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

Paso 2. Genere un pedido de firma de certificado

Un pedido de firma de certificado (CSR) se requiere para que las de otras compañías CA para publicar un certificado de identidad. El CSR contiene la cadena del Nombre distintivo (DN) su ASA junto con la clave pública generada ASA. El ASA utiliza la clave privada generada para firmar

digitalmente el CSR.

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic la **Administración de dispositivos**.
2. Amplíe la **administración de certificados**, y elija los **certificados de identidad**.
3. Haga clic en Add (Agregar).
4. Haga clic el **agregar un nuevo** botón de radio del **certificado de identidad**.
5. Para el par clave, haga clic **nuevo**.**Nota:** Si usted utiliza un certificado de 2048 bits, genere un bit 2048 dominante también.
6. Haga clic el **nuevo** botón de radio del **nombre del par clave del ingresar**. Usted debe identificar distintamente el nombre del par clave para los propósitos del reconocimiento.
7. El tecleo **ahora genera**.El par clave debe ahora ser creado.
8. Para definir el tema DN del certificado, el tecleo **selecto**, y configurar los atributos enumerados en esta tabla:**Cuadro 4.1: Atributos DN**Para configurar estos valores, elija un valor de la lista desplegable del atributo, ingrese el valor, y el haga click en Add**Nota:** Algunos vendedores de las de otras compañías requieren los atributos determinados ser incluidos antes de que se publique un certificado de identidad. Si usted es inseguro de los atributos requeridos, marque con su vendedor para los detalles.
9. Una vez que se agregan los valores apropiados, haga clic la **AUTORIZACIÓN**.El cuadro de diálogo del certificado de identidad del agregar aparece con el campo del tema DN del certificado poblado.
10. Haga clic en **Advanced**.
11. En el campo FQDN, ingrese el FQDN que será utilizado para acceder el dispositivo del Internet.Este valor debe ser el mismo FQDN que usted utilizó para el Common Name (CN).
12. El Haga Click en OK, y entonces hace clic **agrega el certificado**.A le indican que salve el CSR a un archivo en su máquina local.
13. Haga clic **hojean**, eligen una ubicación en la cual salvar el CSR, y salvar el archivo con la extensión de .txt.**Nota:** Cuando usted salva el archivo con una extensión de .txt, usted puede abrir el archivo con un editor de textos (tal como libreta) y ver PKCS-10 la petición.
14. Someta el CSR guardado a su vendedor de las de otras compañías. Una vez que usted somete el CSR a su vendedor de las de otras compañías, le proporcionarán el certificado de identidad que se instalará en el ASA.

Ejemplo de la línea de comando

En el ASDM 6.x, el trustpoint se crea automáticamente cuando se genera un CSR o cuando el certificado de CA está instalado. En el CLI, el trustpoint se debe crear manualmente.

ciscoasa

```
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)#
```

Paso 3. Autentique el trustpoint

Una vez que usted recibe el certificado de identidad del vendedor de las de otras compañías, usted puede proceder con este paso.

Procedimiento del ASDM

1. Salve el certificado de identidad a su computadora local.
2. Si su fueron proporcionados un certificado codificado en base64 que no vino como un archivo, usted debe copiar el mensaje del base64, y lo pega en un archivo de texto.
3. Retitule el archivo con una extensión de .cer. Nota: El archivo se retitula una vez con la extensión de .cer, el icono del archivo debe visualizar como certificado.
4. Haga doble clic el archivo de certificado.El cuadro de diálogo del certificado aparece.**Nota:** Si

"*Windows no tiene bastante información para verificar el* mensaje de *este certificado*" aparece en la ficha general, usted debe obtener al vendedor de las de otras compañías raíz CA o certificado de CA intermedio antes de que usted continúe con este procedimiento. Entre en contacto su vendedor de las de otras compañías o administrador de CA para obtener la publicación raíz CA o el certificado de CA intermedio.

5. Haga clic la lengueta de la **trayectoria del certificado**.
6. Haga clic el certificado de CA situado sobre su certificado de identidad publicado, y haga clic el **certificado de la visión**.La información detallada sobre el certificado de CA intermedio aparece.**Advertencia:** No instale el certificado de la identidad (dispositivo) en este paso. Solamente la raíz, la raíz subordinada, o el certificado de CA se agregan en este paso. Los Certificados de la identidad (dispositivo) están instalados en el paso 4.
7. Haga clic en **Details**.
8. **Copia del** tecleo **a clasifiar**.
9. Dentro del Asisitente de la exportación del certificado, haga clic **después**.
10. En el cuadro de diálogo del formato de archivo de la exportación, haga clic el botón de radio **codificado base 64 X.509 (.CER)**, y haga clic **después**.
11. Ingrese el nombre del archivo y la ubicación a los cuales usted quiere salvar el certificado de CA.
12. Haga clic en Next (Siguiente) y luego en Finish (Finalizar).
13. Haga Click en OK en el cuadro de diálogo acertado de la exportación.
14. Hojee a la ubicación en donde usted guardó el certificado de CA.
15. Abra el archivo con un editor de textos, tal como libreta. (Haga clic con el botón derecho del ratón el archivo, y elija **envían a > libreta**.)El mensaje codificado en base64 debe aparecer similar al certificado en esta imagen:
16. Dentro del ASDM, la **configuración del** tecleo, y entonces hace clic la **Administración de dispositivos**.
17. Amplíe la **administración de certificados**, y elija los **Certificados de CA**.
18. Haga clic en Add (Agregar).
19. Haga clic el **certificado de la goma en el** botón de radio del **formato PEM**, y pegue el certificado de CA del base64 proporcionado por el vendedor de las de otras compañías en el campo de texto.
20. El tecleo **instala el certificado**.Un cuadro de diálogo aparece que confirma la instalación era acertado.

Ejemplo de la línea de comando

ciscoasa

```
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
```

Paso 4. Instale el certificado

Procedimiento del ASDM

Utilice el certificado de identidad proporcionado por el vendedor de las de otras compañías para realizar estos pasos:

1. Haga clic la **configuración**, y después haga clic la **Administración de dispositivos**.
2. Amplíe la **administración de certificados**, y después elija los **certificados de identidad**.
3. Seleccione el certificado de identidad que usted creó en el paso 2. (la fecha de vencimiento

debe visualizar *pendiente*.)

4. El tecleo **instala**.
5. Haga clic la **goma los datos del certificado en el** botón de radio del **formato del base 64**, y pegue el certificado de identidad proporcionado por el vendedor de las de otras compañías en el campo de texto.
6. El tecleo **instala el certificado**.Un cuadro de diálogo aparece que confirma la importación era acertado.

Ejemplo de la línea de comando

ciscoasa

```
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)#
```

Paso 5. WebVPN de la configuración para utilizar el certificado nuevamente instalado

Procedimiento del ASDM

1. **La configuración del** tecleo, y entonces hace clic la **Administración de dispositivos**.
2. Amplíe **avanzado**, y después amplíe las **configuraciones SSL**.
3. Bajo los Certificados, seleccione la interfaz que se utiliza para terminar a las sesiones WebVPN.En este ejemplo, se utiliza la interfaz exterior.
4. Haga clic en **Editar**.
5. En la lista desplegable del certificado, elija el certificado instalado en el paso 4.
6. Haga clic en OK.
7. Haga clic en Apply (Aplicar).Su nuevo certificado se debe ahora utilizar para todas las sesiones WebVPN que terminen en la interfaz especificada.
8. Vea la sección del verificar para confirmar que el proceso de instalación era acertado.

Ejemplo de la línea de comando

ciscoasa

```
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.
```

Verificación

Utilice los pasos siguientes para verificar la instalación exitosa del certificado del vendedor de las de otras compañías y el uso para las conexiones WebVPN.

Vea los Certificados instalados

Procedimiento del ASDM

1. Configuración del tecleo, y Administración de dispositivos del tecleo.
2. Amplíe la administración de certificados, y elija los certificados de identidad.El certificado de identidad publicado por su vendedor de las de otras compañías debe aparecer.

Ejemplo de la línea de comando

ciscoasa
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.*

Verifique el certificado instalado para el WebVPN con un buscador Web

Para verificar que el WebVPN utilice el nuevo certificado, complete estos pasos:

1. Conecte con su WebVPN la interfaz a través de un buscador Web. Utilice https:// junto con el FQDN que usted pedía el certificado (por ejemplo, https://webvpn.cisco.com).Si usted recibe una de las alertas de seguridad siguientes, realice el procedimiento que corresponde a esa alerta:**El nombre del Security Certificate es inválido o no hace juego el nombre del sitio**Verifique que usted utilizara el FQDN/CN correcto para conectar con el WebVPN la interfaz del ASA. Usted debe utilizar el FQDN/CN que usted definió cuando usted pidió el certificado de identidad. Usted puede utilizar el comando **crypto del** *trustpointname de los* **Certificados Ca de la demostración** para verificar los Certificados FQDN/CN.**El Security Certificate fue publicado por una compañía que usted no ha elegido confiar en…**Complete estos pasos para instalar el certificado raíz del vendedor de las de otras compañías a su buscador Web:En el cuadro de diálogo de la alerta de seguridad, haga clic el **certificado de la visión**.En el cuadro de diálogo del certificado, haga clic la lengueta de la **trayectoria del certificado**.Seleccione el certificado de CA situado sobre su certificado de identidad publicado, y haga clic el **certificado de la visión**.El tecleo **instala el certificado**.En el

certificado instale el cuadro de diálogo del Asisitente, tecleo **después.**Haga clic el **automáticamente selecto el almacén de certificados basado en el tipo de** botón de radio, de tecleo **después**, y entonces de clic en Finalizar del **certificado**.Haga clic **sí** cuando usted recibe el instalar el prompt de la confirmación del certificado.En la operación de la importación era el prompt acertado, hace clic la **AUTORIZACIÓN**, y después hace clic **sí.Nota:** Puesto que este ejemplo utiliza el certificado de ensayo de Verisign Verisign el certificado raíz de CA de ensayo se debe instalar para evitar los errores de la verificación cuando los usuarios conectan.
2. Haga doble clic el icono del bloqueo que aparece en la esquina inferior derecha de la página de registro del WebVPN.La información instalada del certificado debe aparecer.
3. Revise el contenido para verificar que hace juego su certificado de los vendedores de las de otras compañías.

Comandos

En el ASA usted puede utilizar varios comandos show en la línea de comando de verificar el estatus de un certificado.

- **muestre el trustpoint crypto Ca** — Las visualizaciones configuraron el trustpoints.
- **muestre el certificado Ca crypto** — Visualiza todos los Certificados instalados en el sistema.
- **muestre los crls crypto Ca** — Las visualizaciones ocultaron las listas de revocación de certificados (CRL).
- **mypubkey rsa del show crypto key** — Visualiza todos los pares de crypto key generados.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Aquí están algunos errores posibles que usted puede ser que encuentre:

- **%Warning: El CERT de CA no se encuentra. Los certs importados no pudieron ser usable.INFORMATION: Certificado importado con éxito**El certificado de CA no fue autenticado correctamente. Utilice el comando **crypto del** *trustpointname del* **certificado Ca de la demostración** para verificar que el certificado de CA fue instalado. Si existe el certificado de CA, verifiquelo se refiere al trustpoint correcto.
- **ERROR: No podido analizar o verificar el certificado importado**Este error puede ocurrir cuando usted instala el certificado de identidad y no tiene el intermedio correcto o certificado raíz CA autenticado con el trustpoint asociado. Usted debe quitar y reauthenticate con el intermedio correcto o certificado raíz CA. Entre en contacto a su vendedor de las de otras compañías para verificar que usted recibió el certificado de CA correcto.
- **El certificado no contiene la clave pública de fines generales**Este error puede ocurrir cuando usted intenta instalar su certificado de identidad al trustpoint incorrecto. Usted intenta instalar un certificado de identidad inválido, o el par clave asociado al trustpoint no hace juego la clave pública contenida en el certificado de identidad. Utilice el comando **crypto del** *trustpointname de los* **Certificados Ca de la demostración** para verificarle instaló su certificado

de identidad al trustpoint correcto. Busque la línea que expone el *trustpoints asociado:* Si el trustpoint incorrecto es mencionado, utilice los procedimientos descritos en este documento para quitar y reinstalar el trustpoint apropiado. También, verifique el par clave no ha cambiado puesto que el CSR fue generado.

- **Mensaje de error: %PIX|ASA-3-717023 SSL no pudo fijar el certificado del dispositivo para el [trustpoint name] del trustpoint**Este presentaciones del mensaje cuando ocurre un error cuando usted fija un certificado del dispositivo para el trustpoint dado para autenticar la conexión SSL. Cuando sube la conexión SSL, una tentativa se hace para fijar el certificado del dispositivo que será utilizado. Si ocurre un error, se registra un mensaje de error que incluye el trustpoint configurado que se debe utilizar para cargar el certificado del dispositivo y la razón del error.*nombre del trustpoint — Nombre del trustpoint para las cuales el SSL no pudo fijar un certificado del dispositivo.***Acción Recomendada:** Resuelva el problema indicado por la razón señalada para el error.Asegúrese de que el trustpoint especificado esté alistado y tenga un certificado del dispositivo.Aseegurese el certificado del dispositivo es válido.Reenroll el trustpoint, si procede.

Información Relacionada

- Cómo obtener un certificado digital de Microsoft Windows CA usando el ASDM en un ASA
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems