Exemple de configuration de l'installation manuelle de certificats de fournisseurs tiers dans ASA 8.x pour une utilisation avec WebVPN

Contenu

Introduction

Cet exemple de configuration décrit comment installer manuellement un certificat numérique de constructeur de tiers sur l'ASA pour l'usage avec le webvpn. Un certificat d'essai de Verisign est utilisé dans cet exemple. Chaque étape contient la procédure d'application ASDM et un exemple CLI.

Conditions préalables

Conditions requises

Ce document exige que vous avez accès à un Autorité de certification (CA) pour l'inscription de certificat. Les exemples des constructeurs du tiers CA incluent, mais ne sont pas limités à, Baltimore, Cisco, confient, Geotrust, Godaddy, iPlanet/Netscape, Microsoft, RSA, Thawte, et Verisign.

Composants utilisés

Ce document utilise une ASA 5510 qui exécute la version de logiciel 8.0(2) et la version 6.0(2) ASDM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Afin d'installer un certificat numérique de constructeur de tiers sur l'ASA, terminez-vous ces étapes :

1. Vérifiez que les valeurs de date, de temps, et de fuseau horaire sont précises
2. Générez une demande de signature de certificat
3. Authentifiez le point de confiance
4. Installez le certificat
5. Configurez le webvpn pour utiliser le certificat nouvellement installé

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Étape 1. Vérifiez que les valeurs Date, Heure et Fuseau Horaire soient exactes

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Device Setup**.
2. Développez **System Time** et choisissez **Clock**.
3. Vérifiez que les informations répertoriées sont correctes.Les valeurs pour la date, le temps, et le fuseau horaire doivent être précises pour que la validation appropriée de certificat se produise.

Exemple de ligne de commande

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

Étape 2. Générez une demande de signature de certificat

Une demande de signature de certificat (CSR) est exigée afin du tiers CA pour délivrer un certificat d'identité. La CSR contient la chaîne du nom distinctif (DN) de votre ASA et la clé publique générée de l'ASA. L'ASA utilise la clé privée générée pour signer numériquement la CSR.

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Device Management**.
2. Développez **Certificate Management**, puis choisissez **Identity Certificates**.
3. Cliquez sur **Add**.
4. Cliquez sur la case d'option **Add a new identity certificate**.
5. Pour la paire de clés, cliquez sur **New**.**Remarque:** Si vous utilisez un certificat de 2048 bits, générez un bit 2048 principal aussi bien.
6. Cliquez sur la case d'option **Enter new key pair name**. Vous devriez distinctement identifier le nom de paire de clés pour la reconnaissance.
7. Cliquez sur **Generate Now**.La paire de clés devrait maintenant être créée.
8. Pour définir le DN de sujet de certificat, le clic **choisi**, et configurer les attributs l'a répertorié dans cette table :**Tableau 4.1 : Attributs de DN**Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribute, entrez la valeur, puis cliquez sur **Add**.**Remarque:** Quelques constructeurs de tiers exigent des attributs particuliers pour être inclus avant qu'un certificat d'identité soit délivré. Si vous avez des doutes concernant les attributs requis, contactez votre fournisseur afin d'obtenir plus de détails.
9. Une fois que les valeurs appropriées ont été ajoutées, cliquez sur **OK**.La boîte de dialogue Add Identity Certificate, apparaît avec le champ Certificate Subject DN rempli.
10. Cliquez sur **Advanced**.
11. Dans le domaine FQDN, écrivez le FQDN qui sera utilisé pour accéder au périphérique de l'Internet.Cette valeur devrait être le même FQDN que vous avez utilisé pour le nom commun (NC).
12. Cliquez sur **OK**, puis sur **Add Certificate**.Vous êtes invité à enregistrer la CSR dans un fichier sur votre ordinateur local.
13. Cliquez sur **Browse**, choisissez un emplacement dans lequel enregistrer la CSR, puis enregistrez le fichier avec l'extension .txt.**Remarque:** quand vous enregistrez le fichier avec une extension .txt, vous pouvez ouvrir le fichier avec un éditeur de texte (tel que le Bloc-notes) et afficher la requête PKCS#10.
14. Soumettez le CSR enregistré à votre constructeur de tiers. Une fois que vous soumettez le CSR à votre constructeur de tiers, ils te fourniront le certificat d'identité à installer sur l'ASA.

Exemple de ligne de commande

Dans ASDM 6.x, le point de confiance est automatiquement créé quand un CSR est généré ou quand le certificat de CA est installé. Dans le CLI, le point de confiance doit être créé manuellement.

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)#
```

Étape 3. Authentifiez le point de confiance

Une fois que vous recevez le certificat d'identité du constructeur de tiers, vous pouvez poursuivre cette étape.

Procédure ASDM

1. Enregistrez le certificat d'identité sur votre ordinateur local.
2. Si votre étaient fournis un certificat base64-encoded qui n'a pas été livré comme fichier, vous devez copier le message base64, et le collez dans un fichier texte.
3. Renommez le fichier avec une extension de .cer. Remarque: Une fois le fichier est renommé avec l'extension de .cer, l'icône de fichier devrait afficher comme certificat.
4. Double-cliquez sur le fichier de certificat.La boîte de dialogue de certificat apparaît.**Remarque:** Si « *Windows n'a pas assez d'informations pour vérifier ce certificat* » le message apparaît dans l'onglet Général, vous devez obtenir la racine CA de constructeur de

tiers ou le certificat de CA intermédiaire avant que vous continuiez cette procédure. Contactez votre constructeur de tiers ou administrateur CA afin d'obtenir la racine émettante CA ou le certificat de CA intermédiaire.

5. Cliquez sur l'onglet de **Certificate Path**.
6. Cliquez sur le certificat de CA situé au-dessus de votre certificat d'identité délivré, et cliquez sur le **certificat de vue**.Les informations détaillées au sujet du certificat de CA intermédiaire apparaissent.**Avertissement :** N'installez pas le certificat d'identité (périphérique) dans cette étape. Seulement la racine, la racine subalterne, ou le certificat de CA sont ajoutés dans cette étape. Les Certificats d'identité (périphérique) sont installés dans l'étape 4.
7. Cliquez sur **Details** (Détails).
8. **Copie de** clic **à classer**.
9. Chez l'assistant d'exportation de certificat, cliquez sur Next.
10. Dans la boîte de dialogue de format de fichier d'exportation, cliquez sur le **Base-64 la** case d'option **X.509 (.CER) encodée**, et cliquez sur Next.
11. Entrez le nom du fichier et l'emplacement auxquels vous voulez sauvegarder le certificat de CA.
12. Cliquez sur Next, et puis cliquez sur Finish.
13. Cliquez sur OK dans la boîte de dialogue réussie d'exportation.
14. Naviguez jusqu'à l'emplacement où vous avez enregistré le certificat d'autorité de certification.
15. Ouvrez le fichier avec un éditeur de texte, tel que le Bloc-notes. (Cliquez avec le bouton droit le fichier, et choisissez **envoient à > Notepad**.)Le message base64-encoded devrait ressembler au certificat dans cette image :
16. Dans ASDM, cliquez sur **Configuration**, puis sur **Device Management**.
17. Développez **Certificate Management**, puis choisissez **CA Certificates**.
18. Cliquez sur **Add**.
19. Cliquez sur le **certificat de pâte dans la** case d'option de **format PEM**, et collez le certificat de CA base64 fourni par le constructeur de tiers dans le champ texte.
20. Cliquez sur **Install Certificate**.Une boîte de dialogue apparaît qui confirme l'installation était réussie.

Exemple de ligne de commande

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
```

Étape 4. Installez le certificat

Procédure ASDM

Utilisez le certificat d'identité fourni par le constructeur de tiers pour exécuter ces étapes :

1. Cliquez sur **Configuration**, puis sur **Device Management**.
2. Développez **Certificate Management**, et choisissez alors **Identity Certificates**.
3. Sélectionnez le certificat d'identité que vous avez créé dans l'étape 2. (l'expiration date devrait afficher *en suspens*.)
4. Cliquez sur **Install**.
5. Cliquez sur la **pâte les données de certificat dans la** case d'option du **format base-64**, et collez le certificat d'identité fourni par le constructeur de tiers dans le champ texte.

6. Cliquez sur **Install Certificate**.Une boîte de dialogue apparaît qui confirme l'importation était réussie.

Exemple de ligne de commande

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)#
```

Étape 5. Configurez le webvpn pour utiliser le certificat nouvellement installé

Procédure ASDM

1. Cliquez sur **Configuration**, puis sur **Device Management**.
2. Développez **avancé**, et puis développez les **configurations SSL**.
3. Sous des Certificats, sélectionnez l'interface qui est utilisée pour terminer des sessions de webvpn.Dans cet exemple, l'interface extérieure est utilisée.
4. Cliquez sur **Edit**.
5. Dans la liste déroulante de certificat, choisissez le certificat installé dans l'étape 4.
6. Cliquez sur **OK**.
7. Cliquez sur **Apply**.Votre nouveau certificat devrait maintenant être utilisé pour toutes les sessions de webvpn qui se terminent sur l'interface spécifiée.
8. Voyez la section de vérifier afin de confirmer que le processus d'installation était réussi.

Exemple de ligne de commande

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.
```

Vérifiez

Employez les étapes suivantes pour vérifier l'installation réussie du certificat et de l'utilisation de constructeur de tiers pour des connexions de webvpn.

Certificats installés par vue

Procédure ASDM

1. Configuration de clic, et Gestion de périphériques de clic.
2. Développez **Certificate Management**, puis choisissez **Identity Certificates**.Le certificat d'identité délivré par votre constructeur de tiers devrait apparaître.

Exemple de ligne de commande

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.
```

Vérifiez le certificat installé pour le webvpn avec un navigateur Web

Afin de vérifier que le webvpn utilise le nouveau certificat, terminez-vous ces étapes :

1. Connectez à votre interface de webvpn par un navigateur Web. Utilisez https:// avec le FQDN que vous demandiez le certificat (par exemple, https://webvpn.cisco.com).Si vous recevez une des alertes sécurité suivantes, exécutez la procédure qui correspond à celle alerte :**Le nom du Security Certificate est non valide ou n'apparie pas le nom du site**Vérifiez que vous avez utilisé le FQDN/CN correct afin de se connecter à l'interface de webvpn de l'ASA. Vous devez utiliser le FQDN/CN que vous avez défini quand vous avez demandé le certificat d'identité. Vous pouvez employer la commande de *trustpointname de* **show crypto ca certificat** afin de vérifier les Certificats FQDN/CN.**Le Security Certificate a été émis par une société que vous n'avez pas choisi de faire confiance…**Terminez-vous ces étapes afin d'installer le certificat racine de constructeur de tiers sur votre navigateur Web :Dans la boîte de dialogue d'alerte sécurité, **certificat de vue de** clic.Dans la boîte de dialogue de certificat, cliquez sur l'onglet de **chemin de certificat**.Sélectionnez le certificat de CA situé au-dessus de votre certificat d'identité délivré, et cliquez sur le **certificat de vue**.Cliquez sur **Install Certificate**.Dans la zone de dialogue d'Assistant d'installation de certificat, cliquez sur Next.Cliquez sur **automatiquement le choisi la mémoire de certificat basée sur le type de** case d'option de **certificat**, cliquez sur Next, et puis cliquez sur Finish.Cliquez sur **oui** quand vous recevez l'installer la demande de confirmation de certificat.Àl'importation l'exécution était demande réussie, clique sur OK, et puis clique sur **oui.Remarque:** Puisque cet exemple utilise le certificat d'essai de Verisign Verisign le certificat racine CA d'essai doit être installé afin d'éviter des erreurs de vérification quand les utilisateurs se connectent.

2. Double-cliquer l'icône de verrouillage qui apparaît dans l'angle inférieur droit de la page de connexion de webvpn.Les informations installées de certificat devraient apparaître.
3. Passez en revue le contenu pour vérifier qu'il apparie votre certificat de constructeurs de tiers.

Commandes

Sur l'ASA vous pouvez utiliser plusieurs commandes show à la ligne de commande de vérifier l'état d'un certificat.

- **crypto ca trustpoint d'exposition** — Les affichages ont configuré des points de confiance.
- **affichez le crypto certificat Ca** — Affiche tous les Certificats installés sur le système.
- **show crypto ca crl** — Les affichages ont caché les listes des révocations de certificat (CRL).
- **show crypto key mypubkey rsa** — Affiche toutes les cryptos paires de clés générées.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Voici quelques erreurs possibles que vous pourriez rencontrer :

- **% d'avertissement : Le CERT CA n'est pas trouvé. Les CERT importés ne pourraient pas être usable.INFORMATION : Certificat avec succès importé**Le certificat de CA n'a pas été authentifié correctement. Employez la **crypto** commande de *trustpointname de* **certificat Ca d'exposition** afin de vérifier que le certificat de CA a été installé. Si le certificat de CA existe, vérifiez-le met en référence le point de confiance correct.
- **ERREUR : Failed to parse or verify imported certificate**Cette erreur peut se produire quand vous installez le certificat d'identité et que vous n'avez pas le certificat d'autorité de certification racine ou intermédiaire correct authentifié avec le point de confiance associé. Vous devez supprimer et réauthentifier avec le certificat d'autorité de certification racine ou intermédiaire correct. Contactez votre constructeur de tiers afin de vérifier que vous avez reçu le certificat de CA correct.
- **Certificate does not contain general purpose public key**Cette erreur peut se produire quand vous essayez d'installer votre certificat d'identité sur le point de confiance incorrect. Vous essayez d'installer un certificat d'identité non valide ou la paire de clés associée au point de confiance ne correspond pas à la clé publique contenue dans le certificat d'identité. Employez la commande de *trustpointname de* **show crypto ca certificat** afin de vous vérifier a installé votre certificat d'identité sur le point de confiance correct. Recherchez la ligne qui indique **Associated Trustpoints** : si le point de confiance incorrect est répertorié, utilisez les procédures décrites dans ce document afin de supprimer et de réinstaller le point de confiance approprié. Vérifiez également que la paire de clés n'a pas changé depuis que la CSR a été générée.
- **Message d'erreur : SSL %PIX|ASA-3-717023 n'a pas placé le certificat de périphérique pour le point de confiance [le nom de point de confiance]**Affichages de ce message quand une panne se produit quand vous placez un certificat de périphérique pour le point de confiance donné afin d'authentifier la connexion SSL. Quand la connexion SSL est soulevée, une

tentative est faite pour placer le certificat de périphérique qui sera utilisé. Si une panne se produit, un message d'erreur est enregistré qui inclut le point de confiance configuré qui devrait être utilisé pour charger le certificat de périphérique et la raison pour la panne.*nom de point de confiance — Nom du point de confiance pour lequel le SSL n'a pas placé un certificat de périphérique.***Action recommandée :** Résolvez le problème indiqué par la raison signalée pour la panne.Assurez-vous que le point de confiance spécifié est inscrit et a un certificat de périphérique.Assurez-vous que le certificat de périphérique est valide.Reenroll le point de confiance, s'il y a lieu.

Informations connexes

- Comment obtenir un certificat numérique d'une autorité de certification Microsoft Windows à l'aide d'ASDM sur un dispositif ASA
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems