

Exemple de configuration d'authentification IPSec sur ASA/PIX 8.x et clients VPN à l'aide de certificats numériques avec une autorité de certification Microsoft

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration ASA](#)

[Résumé de configuration ASA](#)

[Configuration du client VPN](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment installer manuellement un certificat numérique de fournisseur tiers sur le dispositif de sécurité Cisco (ASA/PIX) 8.x et des clients VPN afin d'authentifier les homologues IPSec auprès du serveur d'autorité de certification Microsoft.

Conditions préalables

Exigences

Ce document requiert que vous ayez accès à une autorité de certification pour l'inscription de certificat. Les fournisseurs d'autorité de certification tiers pris en charge sont Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA et Verisign.

Ce document suppose qu'il n'y a aucune configuration VPN préexistante dans l'ASA/PIX.

Remarque : ce document utilise un serveur Microsoft Windows 2003 comme serveur AC pour le

scénario.

Remarque : reportez-vous à [Configuration d'une autorité de certification sur un serveur Windows](#) pour obtenir des informations complètes sur la configuration d'un serveur Windows 2003 en tant qu'autorité de certification.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5510 qui exécute la version logicielle 8.0(2) et ASDM version 6.0(2)
- Client VPN qui exécute la version logicielle 4.x et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

La configuration ASA peut également être utilisée avec le PIX Cisco de la gamme 500 qui exécute la version logicielle 8.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- [Configuration ASA](#)
- [Résumé de configuration ASA](#)
- [Configuration du client VPN](#)

Configuration ASA

Afin d'installer un certificat numérique de fournisseur tiers sur l'ASA, procédez comme suit :

- [Étape 1. Vérifiez que les valeurs Date, Time et Time Zone sont exactes](#)
- [Étape 2. Générer une demande de signature de certificat](#)
- [Étape 3. Authentification du point de confiance](#)
- [Étape 4. Installer le certificat](#)
- [Étape 5. Configurer un VPN d'accès à distance \(IPSec\) pour utiliser le certificat nouvellement installé](#)

Étape 1. Vérifiez que les valeurs Date, Time et Time Zone sont 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 de date, heure et fuseau horaire doivent être correctes pour que la validation de certificat appropriée se produise.

Exemple de ligne de commande

CiscoASA
CiscoASA#show clock 05:37:37.904 UTC Fri Dec 21 2007

Étape 2. Générer une demande de signature de certificat

Une demande de signature de certificat (CSR) est requise afin que l'autorité de certification tierce délivre 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.
6. Cliquez sur la case d'option Enter new key pair name. Vous devez identifier distinctement le nom de la paire de clés afin de faciliter sa reconnaissance.
7. Cliquez sur Generate Now.

La paire de clés doit maintenant être créée.

8. Pour définir le DN d'objet de certificat, cliquez sur Select et configurez les attributs répertoriés dans le tableau suivant :

Attribut	Description
CN	Nom de domaine complet (FQDN) à utiliser pour les connexions à votre pare-feu. PAR EXEMPLE : CiscoASA.cisco.com
OU	Nom de service
O	Nom de la société (évitez d'utiliser des caractères spéciaux)
C	Code du pays (code de 2 lettres sans ponctuation)
St	État (Doit être épelé complètement EX : Caroline du Nord)
L	Ville

Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribute, entrez la valeur, puis cliquez sur Add.

Remarque : certains fournisseurs tiers exigent l'inclusion d'attributs particuliers avant l'émission d'un certificat d'identité. 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 champ FQDN, entrez le nom de domaine complet à utiliser pour accéder au périphérique à partir d'Internet.

Cette valeur doit être identique à celle que vous avez utilisée 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 : lorsque vous enregistrez le fichier avec une extension .txt, vous pouvez ouvrir le fichier à l'aide d'un éditeur de texte (tel que le Bloc-notes) et afficher la demande PKCS#10.

14. Soumettez la CSR enregistrée à votre fournisseur tiers, tel que Microsoft CA, comme indiqué.

a. Effectuez la connexion Web au serveur d'autorité de certification 172.16.5.1 à l'aide des informations d'identification utilisateur fournies pour le vpnserver.

Remarque : vérifiez que vous disposez d'un compte d'utilisateur pour l'ASA (serveur VPN) avec le serveur AC.

b. Cliquez sur Demander un certificat > demande de certificat avancée afin de sélectionner Soumettez une demande de certificat en utilisant un fichier CMC ou PKCS #10 codé en base 64, ou soumettez une demande en utilisant un fichier PKCS #7 codé en base 64.

c. Copiez et collez les informations encodées dans la zone Demande enregistrée, puis cliquez sur OK.

d. Cliquez sur la case d'option Codé en base 64, puis sur Télécharger le certificat.

e. La fenêtre File Download apparaît. Sauvegardez le certificat sous le nom cert_client_id.cer, qui est le certificat d'identité à installer sur l'ASA.

Exemple de ligne de commande

```
CiscoASA
<#root>
CiscoASA# configure terminal
CiscoASA(config)#
crypto key generate rsa label my.ca.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.CA.key
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

```
crypto ca trustpoint CA1
```

```
ciscoasa(config-ca-trustpoint)# subject-name CN=CiscoASA.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](#) as a guide.

```
CiscoASA(config-ca-trustpoint)#
```

```
keypair my.CA.key
```

!--- Specifies key pair generated in [Step 3](#)

```
CiscoASA(config-ca-trustpoint)#
```

```
fqdn CiscoASA.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 CA1
```

!--- Initiates certificate signing request. This is the request to be !--- submitted via Web or Email

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will be: cn=CiscoASA.cisco.com OU=TSWEB,
O=Cisco Systems, C=US,St=North Carolina,L=Raleigh
```

```
% The fully-qualified domain name in the certificate will be: CiscoASA.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]:

y

!--- Displays the PKCS#10 enrollment request to the terminal. You will need to !--- copy this from the

Certificate Request follows:

```
MIICKzCCA ZQCAQAwga0xEDA0BgNVBAcTB1JhbGVpZ2gxZzAVBgNVBAgTDk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31zdGVtczEk
MCIGA1UEAxMbQ21zY29BU0EuY21zY28uY29tIE9VPVRTV0VCMUwEgYDVQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNvbTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAu0IKqDMjVrdbZgBzUAjTc10jxS1bkkcr
XgKoH2Pce1cGZ9dUXn+Y09Qjm0Krj68L6KXT1PgNAaFMwB2YsTIO+hJBVq5Sxjv
MI6xLyKrGo7b0PAsLPe0Bx1/LVLTy30Rqcy2QP3Ir1BSwoyBaoFPsReJGSAYG+0
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJJDjEuMCwwCwYDVROPAQDAgWgMBOG
A1UdEQQwMBSCEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd2OLCbXAoP5L1KbPaEeaCkfn/Pp5mATAsG832TBm
bsxSv1jSSXQsQ1Sb842D6MEG6cu7Bxj/K1Z6MxafUvCHR0PYWVU1wgRjGh+ndCZK
j89/Y4S8XhQ79fvBwBR8Ux9emhFHpGHnQ/MpSfU0dQ==
```

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:

n

CiscoASA(config)#

Étape 3. Authentification du point de confiance

Une fois que vous avez reçu le certificat d'identité du fournisseur tiers, vous pouvez continuer avec cette étape.

Procédure ASDM

1. Enregistrez le certificat d'identité sur votre ordinateur local.
2. Si votre certificat base64 ne vous a pas été fourni sous la forme d'un fichier, vous devez copier le message base64 et le coller dans un fichier texte.
3. Renommez le fichier avec une extension .cer

Remarque : une fois le fichier renommé avec l'extension .cer, l'icône du fichier s'affiche sous la forme d'un certificat, comme illustré.

4. Double-cliquez sur le fichier de certificat.

Remarque : si Windows ne dispose pas d'informations suffisantes pour vérifier que ce message de certificat apparaît dans l'onglet Général, vous devez obtenir le certificat CA racine ou le certificat CA intermédiaire du fournisseur tiers avant de poursuivre cette

procédure. Contactez votre fournisseur tiers ou administrateur d'autorité de certification afin d'obtenir le certificat d'autorité de certification racine ou intermédiaire émettrice.

5. Cliquez sur l'onglet de Certificate Path.
6. Cliquez sur le certificat d'autorité de certification associé à votre certificat d'identité délivré, puis cliquez sur View Certificate.

Les informations détaillées au sujet du certificat d'authentification apparaissent.

7. Cliquez sur Details afin d'en savoir plus sur le certificat d'identité.
8. Avant d'installer le certificat d'identité, vous devez télécharger le certificat d'autorité de certification à partir du serveur d'autorité de certification et l'installer dans l'ASA, comme indiqué.

Effectuez les étapes suivantes pour télécharger le certificat d'autorité de certification à partir du serveur d'autorité de certification nommé CA1.

- a. Effectuez la connexion Web au serveur d'autorité de certification 172.16.5.1 à l'aide des informations d'identification fournies au serveur VPN.
- b. Cliquez sur Download a CA certificate, certificate chain or CRL pour ouvrir la fenêtre, comme indiqué. Cliquez sur la case d'option Base 64 comme méthode de codage, puis cliquez sur Download CA certificate.
- c. Enregistrez le certificat d'autorité de certification avec le nom certnew.cer sur votre ordinateur.

9. Naviguez jusqu'à l'emplacement où vous avez enregistré le certificat d'autorité de certification.
10. Ouvrez le fichier avec un éditeur de texte, tel que le Bloc-notes. Cliquez avec le bouton droit sur le fichier et choisissez Envoyer vers > Bloc-notes.
11. Le message codé en base 64 semblable au certificat dans cette image apparaît :
12. Dans ASDM, cliquez sur Configuration, puis sur Device Management.
13. Développez Certificate Management, puis choisissez CA Certificates.
14. Cliquez sur Add.
15. Cliquez sur la case d'option Paste certificate in PEM Format et collez le certificat d'autorité de certification base64 délivré par le fournisseur tiers dans le champ de texte.
16. Cliquez sur Install Certificate.

Une boîte de dialogue apparaît pour confirmer que l'installation a réussi.

Exemple de ligne de commande


```
<#root>
```

```
CiscoASA(config)#
```

```
crypto ca authenticate CA1
```

!--- Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provided

```
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBBRMRMwEQYKCZImiZPyLQBGRYDY29tMRUwEwYKCZImiZPyLQBGRYFY2lZY28xFTATBgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGAlUEAxMDQ0ExMB4XDTA3MTIxNDA2MDE0MlOxDTYyMTIxNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCSgmsJomT8ixkARKWBWNpc2NvMRUwEwYKCZImiZPyLQBGRYFVFNXZWIxDDAKBgNVBAMTA0NBMTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuVvyiLmA9BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjXbt6czaHpBuyIsoz00U1PmwaMuiMAD+mL9IqTbdosJfy7Yhh2vWeMijcQnwdOq+Kx+sWaeNCjslrxeuaHpIBTuaNOckueBUBjxgppJuNPAk1G8YwBfaTV4M7kZf4dbQIy3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uCO4xxQmr//Sct1tdWQcvk2VuBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Qlo+fQeSSz+TldhXxwPXRO18CAwEAAaOCaw8wggFrMBMGCSsGAQQBgjcUAQGHGQAQwBBMASGAlUdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GAlUdDgQWBbTzrb8I8jqI8RRDL3mYfnQJpAPLWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLvcySzMtQUNTLENOPUNEUCxDTj1QdWJsawMlMjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWdlcmF0aw9uLERDPVRTV2ViLERDPWNpc2NvLERDPWNvbtT9jZXJ0awZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9Y1JMRGlzdHJpYnV0aw9uUG9pbnsGNWWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKrL6Z86JGW1Rbf5VYnlTrqRy6HEolrdu6cHGhUCD9/BZWAgfmGum++HMLjnW8liyIFDcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyyVrSGKOLE+OC5L+ytJvw19Gzh1zEloVUFPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNcNItcuFu0x1b1XXc68DKoZY09pPq877uTaou8cLtuipPomeOyZgJON+xaZx2EwGpn149zpXv5tqt9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dxlVD+p85at
```

```
-----END CERTIFICATE-----
```

```
quit
```

!--- Manually pasted certificate into CLI.

```
INFO: Certificate has the following attributes:
Fingerprint:      98d66001 f65d98a2 b455fbce d672c24a
Do you accept this certificate? [yes/no]:
```

```
yes
```

```
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
CiscoASA(config)#
```

Étape 4. Installer le certificat

Procédure ASDM

Utilisez le certificat d'identité délivré par le fournisseur tiers afin d'effectuer 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 à l'[Étape 2](#).

Note : La date d'expiration affiche En attente.

4. Cliquez sur Install.

Cliquez sur la case d'option Paste the certificate data in base-64 format et collez le certificat d'identité délivré par le fournisseur tiers dans le champ de texte.

5. Cliquez sur Install Certificate.

Une boîte de dialogue apparaît afin de confirmer que l'importation a réussi.

Exemple de ligne de commande

```
CiscoASA

<#root>
CiscoASA(config)#
crypto ca import CA1 certificate

!--- Initiates prompt to paste the base64 identity !--- certificate provided by the third party vendor

%The fully-qualified domain name in the certificate will be: CiscoASA.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 third party vendor.

-----BEGIN CERTIFICATE-----
MIIFPzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBMRMwEQYK
CZImiZPyLQBGGRYDY29tMRUwEwYKZCZImiZPyLQBGGRYFY2lzY28xFTATBgoJkiaJ
k/IsZAEZFgVUU1d1YjEMMAoGAlUEAxMDQ0ExMB4XDTA3MTIxNTA4MzUzOVoXDTA5
MTIxNDA4MzUzOVowdjELMAkGAlUEBhMCVVMxZAVBgNVBAGTDk5vcnRoIENhcm9s
aw5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjaXNjbyBTeXN0ZWlzMScw
IgdVdVQDEExtDaXNjb0FTQs5jaXNjby5jb20gT1U9VFNXRUlwgZ8wDQYJKoZIhvcN
```

```
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14CqB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/osQVauUsY7zCOsS8iqxqO
2zjwLcz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/CaeqnGRN
AgMBAAGjggLeMIIC2jALBgnVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21zY29BU0Eu
Y21zY28uY29tMB0GAlUdDgQWBbQsJC3bsQzeGv4tY+MeH7KMl0xCFjAfBgNVHSME
GDAWgBTZrb8I8jqI8RRDL3myfNqJpAPLWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB
74aBtwXkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJs
aWMLMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnsSGNWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3Js
MIIBHQYIKwYBBQUHAQEegEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFwOi8vL0NO
PUNBMSxDTj1BSUESQ049UHViBGljJTIwS2V5JTIwU2Vydm1jZXMsQ049U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1jb20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5j
b20vQ2VydeVucm9sbC9UUY1XMksZLUFDUy5UU1dlYi5jaXNjby5jb21fQ0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFCAZQBiAFMAZQByAHYAZQByMAwGAlUdEwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAWEdQYJKoZIhvcNAQEFBQADggEBAIqCaA9G
+8h+3IS8rfVAGzCWAEVRXCyBlx0NPr/jlocGJ7QbQxkjkEswXq/O2xDB7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZLGEpuBnENTohdhtz5vBjGlCROXIs8+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP5151YB0y
NSLsYWqjkCBg+aUO+WPfk4jICr2XUOK74oWTFPNpfv2x4VFI/Mpcs87ychngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnFlzCnqfcyHcETieZtSt1nwLpsc
lL5nuPsd8MaexBc=
```

-----END CERTIFICATE-----

quit

INFO: Certificate successfully imported
CiscoASA(config)#

Étape 5. Configurer un VPN d'accès à distance (IPSec) pour utiliser le certificat nouvellement installé

Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

1. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add afin de créer une stratégie ISAKMP 65535, comme indiqué.

Cliquez sur OK et sur Apply.

2. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add afin de créer l'ensemble de transformations myset , comme indiqué.

Cliquez sur OK et sur Apply.

3. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add afin de créer une carte de chiffrement avec une stratégie dynamique de priorité 10, comme indiqué.

Cliquez sur OK et sur Apply.

Remarque : ASA 8.0 ne prend pas en charge SHA 2. Les clients IPSec qui utilisent des certificats avec un hachage 256 ne sont pas non plus pris en charge.

4. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add afin de créer une stratégie de groupe Defaultgroup , comme indiqué.

Cliquez sur OK et sur Apply.

5. Choisissez Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add afin de configurer le pool d'adresses vpnpool pour que les utilisateurs de clients VPN soient attribués de manière dynamique.

Cliquez sur OK et sur Apply.

6. Choisissez Configuration > Remote Access VPN > AAA Setup > Local Users > Add afin de créer le compte d'utilisateur vpnuser pour l'accès des clients VPN. Faites également en sorte que cet utilisateur soit membre de DefaultRAGroup.

7. Choisissez Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Edit afin de modifier DefaultRAGroup, comme indiqué.

- Choisissez le certificat d'identité approprié dans la liste déroulante pour le champ IKE Peer Authentication.
- Choisissez le groupe de serveurs LOCAL pour le champ User Authentication.
- Choisissez vpnpool comme pool d'adresses clientes pour le champ Client Address Assignment.
- Choisissez defaultgroup comme stratégie de groupe pour le champ Default Group Policy.

Cliquez sur OK et sur Apply.

Exemple de ligne de commande

```
CiscoASA
<#root>
CiscoASA(config)#
crypto isakmp enable outside
CiscoASA(config)#
crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#
authentication rsa-sig
```

```
CiscoASA(config-isakmp-policy)#
```

```
encryption 3des
```

```
CiscoASA(config-isakmp-policy)#
```

```
hash md5
```

```
CiscoASA(config-isakmp-policy)#
```

```
group 2
```

```
CiscoASA(config-isakmp-policy)#
```

```
lifetime 86400
```

```
CiscoASA(config-isakmp-policy)#exit
```

```
CiscoASA(config)#
```

```
crypto isakmp identity auto
```

!--- Phase 1 Configurations

```
CiscoASA(config)#
```

```
crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

```
CiscoASA(config)#
```

```
crypto dynamic-map dynmap 10 set transform-set myset
```

```
CiscoASA(config)#
```

```
crypto map mymap 10 ipsec-isakmp dynamic dynmap
```

```
CiscoASA(config)#
```

```
crypto map mymap interface outside
```

!--- Phase 2 Configurations

```
CiscoASA(config)#
```

```
group-policy defaultgroup internal
```

```
CiscoASA(config)#
```

```
group-policy defaultgroup attributes
```

```
CiscoASA(config-group-policy)#
```

```
default-domain value cisco.com
```

```
CiscoASA(config-group-policy)# exit
```

!--- Create a group policy "defaultgroup" with domain name !--- cisco.com

```
CiscoASA(config)#
```

```
username vpnuser password Cisco123
```

```
CiscoASA(config)#
username vpnuser attributes
CiscoASA(config-username)#
memberof DefaultRAGroup
CiscoASA(config-username)#exit

!--- Create a user account "vpnuser" and added to !--- "DefaultGroup"

CiscoASA(config)#
tunnel-group DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel groups !--- for remote access (DefaultRAGroup)

CiscoASA(config-tunnel-general)#
address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the address pool.

CiscoASA(config-tunnel-general)#
default-group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the tunnel group.

CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#
tunnel-group DefaultRAGroup ipsec-attributes
CiscoASA(config-tunnel-ipsec)#
trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer !--- authentication
```

Résumé de configuration ASA

CiscoASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/1
 shutdown
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 90
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
 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
dns server-group DefaultDNS
 domain-name cisco.com
access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0
 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu DMZ 1500
ip local pool vpnpool 10.5.5.10-10.5.5.20
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
route outside 172.16.5.0 255.255.255.0 192.168.1.1 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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
crypto ca trustpoint CA1
  enrollment terminal
  subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems, C=US,
  St=North Carolina,L=Rale
  serial-number
  keypair my.CA.key
  crl configure
crypto ca certificate chain CA1
certificate 611ee59b000000000007
  308205a7 3082048f a0030201 02020a61 1ee59b00 00000000 07300d06 092a8648
  86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31
  15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689
  93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 1e170d30
  37313231 35303833 3533395a 170d3039 31323134 30383335 33395a30 76310b30
  09060355 04061302 55533117 30150603 55040813 0e4e6f72 74682043 61726f6c
  696e6131 10300e06 03550407 13075261 6c656967 68311630 14060355 040a130d
  43697363 6f205379 7374656d 73312430 22060355 0403131b 43697363 6f415341
  2e636973 636f2e63 6f6d204f 553d5453 57454230 819f300d 06092a86 4886f70d
  01010105 0003818d 00308189 02818100 b8e20aa8 332356b7 5b660073 5008d373
  5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754 5e7f98d3 d4239b42 ab8faf0b
  e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a b94b18ef 308eb12f 22ab1a8e
  db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9 03f722bd 414b0a32 05aa053e
  c45e2464 80606f8e 417f09a7 aa9c644d 02030100 01a38202 de308202 da300b06
  03551d0f 04040302 05a0301d 0603551d 11041630 14821243 6973636f 4153412e
  63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cde1a fe2d63e3
  1e1fb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f
  79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081
  ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143
  532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 25323053 65727669
  6365732c 434e3d53 65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e
  2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966
  69636174 65526576 6f636174 696f6e4c 6973743f 62617365 3f6f626a 65637443
  6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 74863568 7474703a
  2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365
  7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 01050507 01010482
  010f3082 010b3081 a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e
  3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365
  72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174
  696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143
  65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274
  69666963 6174696f 6e417574 686f7269 7479305d 06082b06 01050507 30028651
  68747470 3a2f2f74 732d7732 6b332d61 63732e74 73776562 2e636973 636f2e63
  6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e
  63697363 6f2e636f 6d5f4341 312e6372 74302106 092b0601 04018237 14020414
  1e120057 00650062 00530065 00720076 00650072 300c0603 551d1301 01ff0402
  30003013 0603551d 25040c30 0a06082b 06010505 07030130 0d06092a 864886f7
  0d010105 05000382 0101008a 82680f46 fbc87edc 84bc45f5 401b3716 0045515c
  2c81971d 0da51fe3 96870627 b41b4319 23284b30 5eafcedb 10c1ef05 d0686a61
```



```
cd1ab877 100b965d 499088e1 7de418fb b5529199 46129b81 9c4353a2 1761b61c
f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433 bddef040 b4b0431e 7456fe29
8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74 97997a23 340fe65e 75601d32
3522ec61 6aa39020 60f9a50e f963c593 88c80abd 9750e2bb e285933c 53697efd
b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285 2b19b30f 6ea733c4 1f62ff3b
7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87 7044e279 9b52b759 f02e9b1c
94be67b8 fb1df0c6 9ec417
```

quit

```
certificate ca 7099f1994764e09c4651da80a16b749c
```

```
3082049d 30820385 a0030201 02021070 99f19947 64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011 060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401 19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231 0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d 31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916 03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306 0a099226 8993f22c 64011916
05545357 6562310c 300a0603 55040313 03434131 30820122 300d0609 2a864886
f70d0101 01050003 82010f00 3082010a 02820101 00ea8fee c7ae56fc a22e603d
0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d 28ece906 02902f9a d1eb2b8d
f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd a1e906ec 88b32a19 38e5353e
6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621 876bd678 c8a37109 f074eabe
2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4 9b8d3c09
351bc630 05f69357 833b9197 f875b408 cb71a814 69a1f331 b1eb2b35 0c469443
1455c210 db308bf0 a9805758 a878b82d 38c71426 afffd272 dd6d7564 1cbe4d95
b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67 94b97ac7 63249009 fa05ca4d
6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b 5f020301 0001a382 016f3082
016b3013 06092b06 01040182 37140204 061e0400 43004130 0b060355 1d0f0404
03020186 300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414
d9adbf08 f23a88f1 14432f79 987cd409 a403e558 30820103 0603551d 1f0481fb
3081f830 81f5a081 f2a081ef 8681b56c 6461703a 2f2f2f43 4e3d4341 312c434e
3d54532d 57324b33 2d414353 2c434e3d 4344502c 434e3d50 75626c69 63253230
4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f
6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443
3d636f6d 3f636572 74696669 63617465 5265766f 63617469 6f6e4c69 73743f62
6173653f 6f626a65 6374436c 6173733d 63524c44 69737472 69627574 696f6e50
6f696e74 86356874 74703a2f 2f74732d 77326b33 2d616373 2e747377 65622e63
6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f 4341312e 63726c30 1006092b
06010401 82371501 04030201 00300d06 092a8648 86f70d01 01050500 03820101
001abc5a 40b32112 22da80fb bb228bfe 4bf8a515 df8fc3a0 4e0c89c6 d725e2ab
2fa67ce8 9196d516 dfe55627 953aea47 2e871289 6b754e9c 1e01d408 3f7f0595
8081f986 526fbe1c c9639d6f 258b2205 0dc370c6 5431b034 fe9fd60e 93a6e71b
ab8e7f84 a011336b 37c13261 5ad218a3 a513e382 e4bfb2b4 9bf0d7d1 99865cc4
94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92 860152d4 f06b2b15 df306433
c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196 34f693ea f3beee4d
aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76 13018f9f 5e3dce95 efe6da93
f4cb3b00 102efa94 48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad
```

quit

```
crypto isakmp enable outside
crypto isakmp policy 65535
 authentication rsa-sig
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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
group-policy defaultgroup internal
group-policy defaultgroup attributes
  default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
  memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
  address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
  trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
: end
CiscoASA#
```

Configuration du client VPN

Exécutez les étapes suivantes afin de configurer le client VPN.

1. Choisissez Démarrer > Programmes > Cisco Systems VPN Client > VPN Client afin de lancer le logiciel client VPN.
2. Effectuez les étapes suivantes pour télécharger le certificat d'autorité de certification à partir du serveur nommé CA1 et installez-le dans le client VPN Cisco.
 - a. Effectuez la connexion Web au serveur d'autorité de certification 172.16.5.1 à l'aide des informations d'identification fournies au vpnuser.

Remarque : vérifiez que vous disposez d'un compte utilisateur pour l'utilisateur client VPN avec le serveur AC.

- b. Cliquez sur Download a CA certificate, certificate chain or CRL pour ouvrir la fenêtre, comme indiqué. Cliquez sur la case d'option Base 64 comme méthode de codage, puis cliquez sur Download CA certificate.
- c. Enregistrez le certificat d'autorité de certification avec le nom certnew.cer sur votre ordinateur. Par défaut, il est stocké dans C:\Program Files\Cisco Systems\VPN Client.
- d. Sur le client VPN, choisissez l'onglet Certificates > Import et cliquez sur le bouton Import from Fileradio. Cliquez sur Browse afin d'importer le certificat d'autorité de certification à partir de l'emplacement de stockage C:\Program Files\Cisco Systems\VPN Client, comme indiqué.

Cliquez sur Import. Une fenêtre de réussite apparaît, comme indiqué.

Sous l'onglet Certificates, les certificats d'autorité de certification CA1 apparaissent, comme indiqué.

Remarque : assurez-vous que l'option Show CA/RA Certificates est sélectionnée, comme indiqué, sinon les certificats CA ne doivent pas apparaître dans la fenêtre de certificat.

3. Effectuez les étapes suivantes pour télécharger le certificat d'identité et l'installer sur le client VPN.

- a. Dans le serveur d'autorité de certification CA1, choisissez Demander un certificat > demande de certificat avancée > Créer et soumettre une demande de requête auprès de cette Autorité de certification afin de s'inscrire pour le certificat d'identité.

Cliquez sur Submit.

- b. Cliquez sur Yes pour poursuivre.
- c. Cliquez sur Installer ce certificat.
- d. Cliquez sur Yes pour poursuivre.
- e. Vous devez recevoir le message de certificat installé, comme indiqué.
- f. Quittez le client VPN et relancez-le afin de démarrer le certificat d'identité installé et de l'afficher sous l'onglet de certificat du client VPN, comme indiqué.

4. Sous l'onglet Connection entries, cliquez sur New afin de créer l'entrée de connexion vpnuser, comme indiqué.

- Entrez l'adresse IP du partenaire distant (routable) dans le champ Host.
- Cliquez sur la case d'option Certificate Authentication et choisissez le certificat d'identité dans la liste déroulante, comme indiqué.
- Cliquez sur Save.

5. Cliquez sur Connect.
6. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe pour Xauth et cliquez sur OK pour vous connecter au réseau distant.
7. Le client VPN se connecte à l'ASA, comme indiqué.

Vérifier

Sur l'ASA, vous pouvez exécuter plusieurs commandes show sur la ligne de commande afin de vérifier l'état d'un certificat.

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- La commande `show crypto ca trustpoint` affiche les points de confiance configurés.

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- La commande `show crypto ca certificate` affiche tous les certificats installés sur le système.

```
CiscoASA# show crypto ca certificate
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
```

```
CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
```

```
DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
```

```
[2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.cr1
Validity Date:
  start date: 14:00:36 UTC Dec 27 2007
  end   date: 14:00:36 UTC Dec 26 2008
Associated Trustpoints: CA1
```

CA Certificate

```
Status: Available
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Issuer Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
Subject Name:
  cn=CA1
  dc=TSWeb
  dc=cisco
  dc=com
CRL Distribution Points:
  [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
      CN=Services,CN=Configuration,DC=TSWeb,DC=cisco,
      DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  [2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.cr1
Validity Date:
  start date: 06:01:43 UTC Dec 14 2007
  end   date: 06:10:15 UTC Dec 14 2012
Associated Trustpoints: CA1
```

Certificate

```
Subject Name:
  Name: CiscoASA.cisco.com
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
Associated Trustpoint: CA1
```

- La commande `show crypto ca crls` affiche les listes des révocations de certificat (CRL) mises en cache.
- La commande `show crypto key mypubkey rsa` affiche toutes les paires de clés de chiffrement générées.

```
CiscoASA# show crypto key mypubkey rsa
Key pair was generated at: 01:43:45 UTC Dec 11 2007
Key name: <Default-RSA-Key>
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:
```

```
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
```

```

4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
Key pair was generated at: 06:36:00 UTC Dec 15 2007
Key name: my.CA.key
Usage: General Purpose Key
Modulus Size (bits): 1024
Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
CiscoASA#

```

- La commande `show crypto isakmp sa` affiche les informations de tunnel IKE 1.

```
CiscoASA#show crypto isakmp sa
```

```

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.1.1.5
  Type      : user           Role      : responder
  Rekey     : no            State     : MM_ACTIVE

```

- La commande `show crypto ipsec sa` affiche les informations de tunnel IPsec.

```
CiscoASA#show crypto ipsec sa
```

```

interface: outside
  Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
  current_peer: 10.1.1.5, username: vpnuser
  dynamic allocated peer ip: 10.5.5.10

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #rcv errors: 0

  local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: FF3EEE7D

inbound esp sas:

```

```
spi: 0xEFDF8BA9 (4024404905)
  transform: esp-3des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
outbound esp sas:
  spi: 0xFF3EEE7D (4282314365)
  transform: esp-3des esp-md5-hmac none
  in use settings ={RA, Tunnel, }
  slot: 0, conn_id: 4096, crypto-map: dynmap
  sa timing: remaining key lifetime (sec): 28314
  IV size: 8 bytes
  replay detection support: Y
```

[L'Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show.](#) Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Dépannage

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

Voici quelques erreurs possibles que vous pouvez rencontrer :

- ERREUR : Impossible d'analyser ou de vérifier le certificat importé

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 fournisseur tiers afin de vérifier que vous avez reçu le certificat d'autorité de certification 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. Exécutez la commande `show crypto ca certificates trustpointname` afin de vérifier que vous avez installé votre certificat d'identité au point de confiance correct. Recherchez la ligne indiquant Associated Trustpoints : Si le mauvais point de confiance est répertorié, utilisez les procédures décrites dans ce document afin de supprimer et réinstaller le point de confiance approprié. Vérifiez également que la paire de clés n'a pas changé depuis que la CSR a été générée.

- ERREUR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:

Si vous avez des problèmes d'authentification avec des certificats, ce message d'erreur peut apparaître sur le client VPN. Utilisez la commande `crypto isakmp identity auto` dans la configuration ASA/PIX afin de résoudre le problème.

Informations connexes

- [Page d'assistance pour Serveur de sécurité adaptatif Cisco](#)
- [Cisco VPN Client Support Page](#)
- [Configuration de Microsoft Server comme Autorité de certification](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.