ASA 7.x WebVPN で使用するサードパーティ ベ ンダーの証明書を手動でインストールする設定 例

内容

概要 前提条件 要件 使用するコンポーネント 表記法 設定 手順1:日付、時刻、およびタイム ゾーンが正しいことを確認する 手順 2: RSA キー ペアを生成する 手順3:トラストポイントを作成する 手順4:証明書の登録を生成する 手順5:トラストポイントを認証する 手順6:証明書をインストールする 手順7:新規インストールされた証明書を使用するための WebVPN を設定する 確認 ASA からの自己署名証明書の置き換え インストールされた証明書の表示 Web ブラウザによる WebVPN 用にインストールされた証明書の確認 SSL 証明書の更新手順 コマンド トラブルシュート 関連情報

概要

この設定例では、WebVPN で使用するサードパーティ ベンダーのデジタル証明書を、ASA 上で 手動でインストールする方法について説明しています。この例では、Verisign Trial Certificate を 使用しています。各ステップには、ASDM アプリケーションの手順と CLI の例が記載されていま す。

前提条件

要件

このドキュメントでは、証明書を登録するために Certificate Authority(CA; 認証局)にアクセス する必要があります。サポートされるサード パーティ CA ベンダーは、Baltimore、Cisco、 Entrust、iPlanet/Netscape、Microsoft、RSA、および VeriSign です。

使用するコンポーネント

このドキュメントでは、ソフトウェア バージョン 7.2(1) および ASDM バージョン 5.2(1) が稼働 する ASA 5510 を使用しています。 ただし、このドキュメントの手順は、互換性のある ASDM バージョンと共に 7.x を実行する ASA アプライアンス上で動作します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

設定

PIX/ASA 上にサード パーティ ベンダーのデジタル証明書をインストールするには、次の手順を 実行します。

- 1. 日付、時刻、およびタイム ゾーンが正しいことを確認する。
- 2. <u>RSA キー ペアを生成する。</u>
- 3. <u>トラストポイントを作成する。</u>
- 4. 証明書の登録を生成する。
- 5. <u>トラストポイントを認証する。</u>
- 6. 証明書をインストールする。
- 7. <u>新規インストールされた証明書を使用するための WebVPN を設定する。</u>

手順1:日付、時刻、およびタイム ゾーンが正しいことを確認する

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Device Administration] を展開し、[Clock] を選択します。
- 3. 表示されている情報が正しいことを確認します。証明書の検証が適切に行われるために、 Date、Time、および Time Zone の値は正確である必要があります。



コマンドラインの例

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

手順 2: RSA キー ペアを生成する

生成された RSA 公開キーは、ASA の ID 情報と結合され、PKCS#10 証明書要求が形成されます。キー ペアを作成するトラストポイントでキー名を明確に特定する必要があります。

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Key Pair] を選択します。
- 3. [Add] をクリックします。

U.	E- Certificate		
65	- Authentication		
NAT	Enrolment	Key Pair Name Usage Moduli	is Size Add
S	- Key Pair		1
VPN	Manage Certificates		Show Details
	E- A Trustpoint		
l A	- 3 Configuration		Delete
CCC Manager	- Seport	Add Key Pair	
CSU Manager	Import		Refresh
430	E B Device Access	Name: C Lise default key name	Refresh
120	Device Administration		
Routing	E-ff DHC Services	(my verision key	
\$ 2	E-P DNS	(, , , , , , , , , , , , , , , , , , ,	
678	High Availability and Scal		
Global Objects	Failover	Size: 1024	
	Fragment		
3	History Metrics	Usage: 💽 General Purpose 🔿 Special	
Properties	HTTP.HTTPS		
	E-10 IP Audit		
	E-1 Logging		
	Priority Queue	Generate Now Cancel Help	
	SSL SSL		
	SUNRPC Server		
	TCP Options		
	Timeouts		

- 4. キー名を入力し、モジュール サイズを選択し、使用タイプを選択します。注:推奨される キー ペアのサイズは 1024 です。
- 5. [Generate] をクリックします。作成したキー ペアが [Key Pair Name] 列に表示されます。 コマンドラインの例

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)#

手順3:トラストポイントを作成する

トラストポイントは、ASA が使用する認証局(CA)を宣言する必要があります。

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Trustpoint] を展開します。
- 3. [Configuration] を選択し、[Add] をクリックします。

Configuration > Properties > Ce	ertificate > Trustpoint > Configuration	
Startup Wizard	Configuration	
🗈 🖬 AAA Setup	Configure a Certificate Authority (CA) as a trustroint	
	Configure a Certificate Autority (CA) as a trusport.	
🕀 🐻 ARP		
-B Client Update		-1
E E Certificate	Trustpoint Name Device Certificate Subject CA Certificate Subject Add	
Authentication		
Enrolment	Edit	
Import Certificate		
	Defet	1
Manage Certificates	Dete	
E-122 Trustpoint		Ξ.
- Contiguration	No Request CRL	
Export		-
- import		
Device Access		

- 4. 以下の値を設定します。**トラストポイント名**:トラストポイント名は目的の用途に関連する 名前にしますこの例では *my.verisign.trustpoint を使用しています。***キー ペア**:<u>手順 2 で生</u> <u>成したキー ペア(</u>*my.verisign.key)を選択します。*
- 5. [Manual Enrollment] を選択していることを確認します。
- 6. [Certificate Parameters] をクリックします。[Certificate Parameters] ダイアログ ボックスが 表示されます。
- 7. [Edit] をクリックし、次の表に示す属性を設定します。[Attribute] ドロップダウン リストか ら値を選択し、値を入力して、[Add] をクリックし、これらの値を設定します。

			Common Name (CN)	webvpn.cisco.com
Attribute to be	Added		Department (OU)	TSWEB
		0.44	Company Name (O)	Cisco Systems
Attribute: Select Attribute	Add >>	State (St)	North Carolina	
_			State (St)	US
alue:		Delete	Location (L)	Raleigh

- 8. 適切な値を追加したら、OK をクリックします。
- 9. [Certificate Parameters] ダイアログボックスで、[Specify FQDN] フィールドに FQDN を入 力します。この値は、Common Name(CN)に使用したものと同じ FQDN である必要があ ります。

🚰 Certificate Parameters	×
Enter the values for the parameters that are to be included in the certificate.	
Subject DN: ystems,St=North Carolina,St=US,L=Raleigh	
FQDN	
C Use FQDN of the device	
Specify FQDN webvpn.cisco.com	
O Use none	
E-mail:	
IP Address:	
Include device serial number	
OK Cancel Help	

- 10. [OK] をクリックします。
- 11. 正しいキー ペアが選択されていることを確認し、[Use manual enrollment] オプション ボタ ンをクリックします。
- 12. [OK] をクリックして、[Apply] をクリックします。

Trustpoint Name: my.ve	erisign.truspoint
Generate a self-signed of	certificate on enrollment
If this option is enabled, o	only Key Pair and Certificate Parameters can be specified.
Enrollment Settings Revoc	cation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Advanced
Key Pair: my.verisi	ign.key 💌 Show Details New Key Pair
Challenge	Confirm Challenge
Password.	Passwora.
Enrollment Mode can only	be specified if there are no certificates associated with this trustpoint.
Enrollment Mode	
Itse manual enro	olment
C Use automatic e	nrollment
C Use automatic en	http://
C Use automatic en Enrollment URL: Retry Period:	http://
C Use automatic en Enrollment URL: Retry Period: Retry Count:	http://
C Use automatic en Enrollment URL: Retry Period: Retry Count:	http://

コマンドラインの例

CiscoASA
ciscoasa(config)#crypto ca trustpoint my.verisign.trustpoint
! Creates the trustpoint.
ciscoasa(config-ca-trustpoint)# enrollment terminal
<pre>! Specifies cut and paste enrollment with this trustpoint. ciscoasa(config-ca-trustpoint)#subject-name CN=wepvpn.cisco.com,OU=TSWEB,</pre>
Systems,C=US,St=North Carolina,L=Raleigh
<pre>! Defines x.500 distinguished name. ciscoasa(config-ca- trustpoint)#keypair my.verisign.key</pre>
! Specifies key pair generated in <u>Step 3</u> . ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

手順4:証明書の登録を生成する

ASDM の手順

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Enrollment] を選択します。
- 3. <u>手順3で作成したトラストポイントが選択されていることを確認して、[Enroll] をクリック</u> します。 ダイアログ ボックスに証明書登録要求(証明書署名要求とも呼ばれる)が一覧表 示されます。

o complete the enrollment process, please paste the following PKCS10 enrollment request into anagement interface of the CA. ou will need to install the certificate after receiving it. o to Configuration > Properties > Certificate > Import Certificate to do so. artificate Request:
ou will need to install the certificate after receiving it. o to Configuration > Properties > Certificate > Import Certificate to do so. ertificate Request:
o to Configuration > Properties > Certificate > Import Certificate to do so. artificate Request:
ertificate Request:
wcNAQkCFhtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN
QEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm
SMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY
AAH4UWUXB118BHZSSGxPX6BGe1C9BJJZVdqCgq+xR4U4/IYPUOeKKfq/apCHVVHF
AGNEAAGGRJEEEGRQNRIGSWOECQ4XNZAIMASGAIOODWQEAWIFODAMEGNVHREEHZAO
moBmSBWnL0gwDtnSlbweKew0AdG5/fxnJBYU2UunllW6sG0KaJYCiFH//eaewF3
F ΤΕ ή VABVhB7Ni6N29710mDAbnPsOR3IγMwbr3eChIFwkZjBTwoe9LuR0gefWfγAH0
jonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=
End - This line not part of the certificate request
ОК

4. PKCS#10 登録要求をテキスト ファイルにコピーして、適切なサード パーティ ベンダーに CSR を送信します。サード パーティ ベンダーは CSR を受信した後、インストール用の ID 証明書を発行します。

コマンドラインの例

デバイス名 1
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint
<pre>! Initiates CSR. 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,</pre>

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/2VteHnhihS1u0j0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACrEnd - This line not
part of the certificate request Redisplay enrollment
request? [yes/no]:
ciscoasa(config)#

手順5:トラストポイントを認証する

サードパーティ ベンダーから ID 証明書を受信したら、引き続きこのステップを実行します。

- 1. ID 証明書をローカル コンピュータに保存します。
- 2. ファイル形式ではない Base64 で符号化された証明書が提供された場合、Base64 メッセージをコピーし、テキスト ファイルに貼り付ける必要があります。
- 3. .cer 拡張子を使用してファイルの名前を変更します。注:ファイルの名前を.cer拡張子で変更すると、ファイルアイコンが証明書として表示されます。
- 4. 証明書ファイルをダブルクリックします。Certificate ダイアログボックスが表示されます。



フに「Windows does not have enough information to verify this certificate」というメッセー ジが表示された場合は、この手順を続行する前に、サードパーティベンダーのルートCAま たは中間CA証明書を取得する必要があります。ルート CA または中間 CA 証明書を入手す るには、サードパーティ ベンダーまたは CA 管理者に問い合せてください。

5. Certificate Path タブをクリックします。

6. 発行された ID 証明書の上にある CA 証明書をクリックし、View Certificate をクリックしま

ertificate	<u>? ×</u>
General Details Certification Path	
Certification path VeriSign Trial Secure Server Test Root C/ VeriSign Trial Secure Server Test CA Webvpn.cisco.com	
	View Certificate
Cortificato status	
This certificate is OK.	
,	

明書に関する詳細情報が表示されます。警告:この手順ではID (デバイス)証明書をイン ストールしないでください。このステップでは、ルート、下位ルート、または CA 証明書の みを追加します。ID(デバイス)証明書は<u>手順6でインストールします。</u>

7. [Details] をクリックします。

Certificate	<u>? ×</u>
General Details Certification Pat	
Show: <a>	▼
Field	Value
Version	V3
Serial number	63 b1 a5 cd c5 9f 78 80 1d a0
Signature algorithm	sha1RSA
Issuer	VeriSign Trial Secure Server Te
Valid from	Tuesday, February 08, 2005 8
Valid to	Sunday, February 08, 2015 7:
E Public key	PSA (2048 Bits)
E	dit Properties Copy to File
	ОК

- 8. Copy to File をクリックします。
- 9. Certificate Export Wizard 内で Next をクリックします。
- 10. Export File Format ダイアログ ボックスで **Base-64 encoded X.509 (.CER)** オプション ボタ ンをクリックし、**Next** をクリックします。

rtificate Export Wizard	[
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
C DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
\square Include all certificates in the certification path if possible	
C Personal Information Exchange - PKCS #12 (.PFX)	
\square Include all certificates in the certification path if possible	
Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
Delete the private key if the export is successful	
< Back Next > Ca	ancel

11. ファイル名と、CA 証明書を保存する場所を入力します。 12. [**Next]** をクリックし、次に [**Finish**] をクリックします。

ertificate Export Wizard]
File to Export Specify the name of the file you want to	export	
File name:		
c:\introotca	Browse	
	< Back Next > Can	cel

- 13. Export Successful ダイアログ ボックスで OK をクリックします。
- 14. CA 証明書を保存した場所を表示します。
- 15. メモ帳などのテキスト エディタでファイルを開きます(ファイルを右クリックし、Send To > Notepad の順に選択します。)Base64 で符号化されたメッセージは、次の画像の証 明書のようになります。

File Edit Format View Help ----BEGIN CERTIFICATE--MIIFSj&CBDKgAwIBAgIQCECQ47aTdj6BtrI60/Vt6zANBgkghkiG9w0BAQUFADCB |yzELMÁᢤGA1UÉBhMCVVMxFzAVBqNVBÅoTD]Z]cm]TaWduLČBĴbmMuMTAwLqYDVQQL ÉydGb3IqVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3R]c3RjYSAOYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwqU2VidXJ1IFN] cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTk1OVowgZ4x CZAJB9NVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q2lzY28qU3lzdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BgNVBAsUMVRlcm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWvudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRw0i8vb2NzcC52zXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9Tv]JTZWN1cmUtyW]hLnZ]cm]zaWduLmNvbS9Tv[JUcm]hbDIw MDUtywlhLmnlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zxJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKozIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTgIorIClawwwx+RHCcTqIrlzf0VfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvlXzŽjiOJ51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6NQpXy5l7TLKyja |idT1FmBvf02qaZS6S40= ----END CERTIFICATE----

- 16. ASDM で [Configuration] をクリックし、[Properties] をクリックします。
- 17. [Certificate] を展開し、[Authentication] を選択します。
- 18. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックします。
- 19. Base64 形式で作成された CA 証明書をテキスト エディタからテキスト領域に貼り付けます。
- 20. [Authenticate] をクリックします。

Configuration > Properties > C	ertificate > Authentication					
Startup Wizard	Authentication					
🗄 💼 🖬 AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a					
Anti-Spoofing	trustpoint and installed on the device.					
E-BARP						
Auto Update	Trustpoint Name: my verision truspo. V Edit New					
Client Update						
Certificate	Einserwint (ortionel):					
Authentication	r ingerprink (optional).					
S Import Cartificate						
- Rev Pair	The certificate text can be specified if the selected trustpoint is configured for manual enrollment.					
Manage Certificates	Certificate Text					
Configuration	C Import from a file: Browse					
- Export						
- Minport	Enter the certificate text in hexadecimal or base64 format:					
E-12 Device Access	A11 EA xMaX/axX/AxX/Ma724a3/dd IsX/AAaaa122/ddX IIENice 7/c811770/0E hds2					
E-20 Device Administration	ECcol67bgdl.ewTagTia9b3MwDQY.Ko7bvcNAQEEBQADgYEAS75v8s35					
E DHCP Services	Kgf234YROIL51ZS111oUZ2MANp2H4biw4tfsG5snDDIwSRmiH3BW/SU6E					
DNS	A/9TXvRicD5q0mB+nyK91B2aBzOiaiHSiM/zAJeQjuqA+Q93jNew+peuj4Ahc					
High Availability and Scal	n/KK/+1Yv61w3+7g6ukFMARVBNg=					
Fallover	END CERTIFICATE					
Vietery Metrice						
H-10 IP Audt	🔂 Authentication Successful					
E-E Logging						
- Priority Queue						
- B SSL	The trustpoint my.verisign.truspoint has been authenticated.					
SUNRPC Server						
- 🔂 TCP Options						
Timeouts						
URL Filtering						
E-B, MCCb						

21. [OK] をクリックします。 **コマンドラインの例**

CiscoASA			
ciscoasa(config)# crypto ca authenticate			
my.verisign.trustpoint			
! Initiates the prompt to paste in the base64 CA root !			
or intermediate certificate. Enter the base 64 encoded			
CA certificate. End with the word "quit" on a line by			
itselfBEGIN CERTIFICATE			
MIIEwDCCBCmgAwIBAgIQY7GlzcWfeIAdoGNs+XVGezANBgkqhkiG9w0B			
AQUFADCB			
${\tt jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw}$			
LgYDVQQL			
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x			
MjAwBgNV			
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290			
IENBMB4X			
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT			
AlvTMRcw			
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjEwMC4GA1UECxMnRm9yIFRlc3Qg			
UHVycG9z			
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv			
ZiB1c2Ug			
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp			
MDUxLTAr			
${\tt BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD}$			

QTCCASIW
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
${\tt DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6}$
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4t1qj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu
LmNvbS9j
CHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
A1UdDgQWBBRmI06B4DFZ3Sp/q0bFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
MIGMMQswCQYDVQQGEwJVUZEXMBUGA1UEChMOVmVyaVNpZ24sIEIUYy4x
BASTJUZVCIBUZXNUIFBICHBVCZVZIEJUDHKUICBODYBHCJNICMFUIZVZ
1 JEYMDAG
hiorangemeyaenpzzagenopiewgozejakoiifnichzicibozknoifoe
$F(C_0) = 67$ have T_0 and T_0
SizRvY21
Kaf234YROiL517S1110UZ2MAND2H4biw4itfsG5snDDlwSRmiH3BW/SU
6EEzD9oi
Ai9TXvRIcD5g0mB+nvK9fB2aBzOiaiHSiIWzAJeOiugA+O93iNew+peu
14AhdvGN
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)#

手順6:証明書をインストールする

ASDM の手順

次の手順を実行するには、サードパーティ ベンダーにより提供された ID 証明書を使用します。

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Import Certificate] を選択します。
- 3. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックし 、テキスト フィールドに Base64 ID 証明書を貼り付けます。

Configuration > Properties > C	ertificate > Import Certificate
	Import Certificate
E 🚅 AAA Setup	Install an identity certificate that was received from a Certificate Authority (CA) in response to a manual
Anti-spooting	enrolment request.
C-CO ARP	
Auto Update	
Client Update	Trustpoint Name: my verision truspo V Edit New
Certificate	
Authentication	
2 Enroiment	Certificate Text
88 Key Pair	C Import from a file: Browse
- Manage Certificates	
- A Trustpoint	Enter the certificate text in hexadecimal or base64 format:
- 20 Configuration	
- Export	u9BSOJsprEsHiyEFGDAmFiRodHRwOi8vbG9nbyS2ZXJpc2hbi5jb20vdnNs
	MSSnaWYWDQYJRo2IIWENAQEFBQADgBBARhTWISKFCgkWWVQjAY
Device Access	PURSIDE/CLACQB//SCACASS/SCASS/SCASS/SCASS/SCASS/SCASS/SCASS/SC
Device Administration	DYVwM3kD0A06EbArti InAyovDb.lucdyb67VTtvevMccr7CkXMHEVya5P)
DHCP Services	ssX9Y.itvhNaKCHzSHstd69N20SmluEOR4utcGqGZD8tVGx28b5OWTz8K
tel−and DNS	8EvHm3ardbDZP+ISMotWYE+CgfKpZb+CPAgH2Cdpz2aJAJN6CS6NM=
High Availability and Scal	END CERTIFICATE
Fallover	
Fragment	
History Metrics	for Information
P Audt	
- Priority Queue	Certificate import succeeded.
	\checkmark
SUNRPC Server	
TCP Options	
	OK
URL Filtering	
E- G WCCP	
-	
I	

4. [Import] をクリックし、[OK] をクリックします。 コマンドラインの例

CiscoASA
ciscoasa(config)#crypto ca import my.verisign.trustpoint
certificate
<pre>! 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 itselfBEGIN</pre>
CERTIFICATE
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0B
AQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LgYDVQQL
EydGb3IgVGVzdCBQdXJwb3N1cyBPbmx5LiAgTm8gYXNzdXJhbmN1cy4x
QjBABgNV
BAsTOVR1cm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5j
b20vY3Bz
L3R1c3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2Vj
Cnzicibuzxnuienbmb4xDTA3mDcynjawmDawmFoxDTA3mDgwOTiznTki
CZAJBGNVBAITAIVTMKCWFQIDVQQIEW5OD3JUACBDIXJVDGIUITEQMA4G
ALUEBXUH I = E = E = E = E = E = E = E = E = E =
UNIFSZWINADEWNEQGAIUECNQNQZIZIZ8GU5IZ0GVCCZEOMAWGAIUECXQF
VENARUIX

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxS1Egry
osBMMazg
5 5 IcLhqSpAqMBAAGiqqHXMIIB0 zAJBqNVHRMEA iAAMAsGA1UdDwOEAwIF
oDBDBgNV
HR8EPDA6MDigNgA0hiJodHRwOi8vU1ZSU2VidXJ1LWNvbC52ZXJpc21n
bi5ib20v
U1ZSVHJpYWwyMDA1LmNybDBKBqNVHSAEOzBBMD8GCmCGSAGG+EUBBxUw
MTAvBagr
BgEFBOcCARYjaHR0cHM6Lv93d3cudmVvaXNpZ24uY29tL2Nwcv90ZXN0
Y2EwHOYD
~ VR01BBYwFAYIKwYBBOUHAwEGCCsGAOUFBwMCMB8GA1UdIwOYMBaAFGYi
ioHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAOUFBwEBBGwwaiAkBggrBgEFBOcwAYYY
aHR0cDov
L29ic3AudmVvaXNpZ24uY29tMEIGCCsGAOUFBzAChiZodHRwOi8vU1ZS
U2VjdXJ1
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYI
KwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgQU
S2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ21mMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9y1DBd8N
7/yW30v3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q8
6ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9T12tvwgrBock/v/
540021kB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FS
ewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyq
j8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntR0ks0gQPBPx5FJSqMiUZGrvju50
END CERTIFICATE
quit
INFO: Certificate successfully imported
ciscoasa(config)#

手順7:新規インストールされた証明書を使用するための WebVPN を設定する

- 1. [Configuration] をクリックし、[Properties] をクリックし、次に SSL を選択します。
- 2. [Trustpoints] エリアで、WebVPN セッションを終端するために使用するインターフェイスを 選択します。(この例では、外部インターフェイスを使用します)。
- 3. [Edit] をクリックします。[Edit SSL Trustpoint] ダイアログボックスが表示されます。

Configuration > Properties > S	<u>ŞL</u>
Startup Wizard	SSL
🕀 🖬 AAA Setup	Continues SCI assessments. These assessments of fact hath ASDM and Mahabatha This assess
	Configure SSL parameters. These parameters affect both ASDM and WebVPN access.
19-100 ARP	Server SSL Version: Any Client SSL Version: Any
	- Formation
	Children (
🔁 🐼 Certificate	Available Algorithms Add >> Active Algorithms Move Up
E-F Device Access	30ES-SHA1
1 Device Administration	Set Edit SSI Transformint
E-P DHCP Services	
🔄 🚑 DNS	Specify an enrolled trustopict to be used for SSI authentication on the outside interface. To enroll a trustopict
High Availability and Scal	appendix and a resolution of the second and the sec
- Failover	go to configuration - reportion - continued - Encontration
- Fragment	
-2 History Metrics	
- HTTP/HTTPS	Interface: outside
E-10 IP Audit	
E Logging	Enroled Trustpoint: my.verisign.trustp
Priority Queue	
- SSL	
SUNRPC Server	
TCP Options	OK Cancel Help
Timeouts	
URL Fitering	Trustocints
E-m WCCP	Construction and the should be identicable of any should be used for CCI as the tribution on each interface. The following
	Specify which enroled trusports, if any, should be used to SSL authentication on each interface. The failback Interfacts will be used on interfaces not associated with a function of their own.
	Education while deal of the ended of the ended and a solution of the ended of the ended
	raiback irustpont:
	hterfees Toutsid 5.0
	interlace industrial Eat
	management
	outside my.verisign.trustpoint
-	

- 4. [Enrolled Trustpoint] ドロップダウン リストから、<u>手順 3 で作成したトラストポイントを選</u> <u>択します。</u>
- 5. [OK] をクリックして、[Apply] をクリックします。

新しい証明書が、指定のインターフェイス上で終端するすべての WebVPN セッションに使用されます。適切なインストールを確認する方法については、このドキュメントの「確認」セクションを参照してください。

コマンドラインの例

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)#write memory
Building configuration Cryptochecksum: 694687al f75042af ccc6addf 34d2cb08
8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)#
! Save configuration.



このセクションでは、サード パーティ ベンダーの証明書のインストールが成功したことを確認す る方法を説明します。

ASA からの自己署名証明書の置き換え

このセクションでは、ASA からインストールされた自己署名証明書を置き換える方法を説明しま す。

- 1. 証明書署名要求を Verisign に発行します。要求した証明書を Verisign から受信した後、そ れを同じトラストポイントに直接インストールします。
- 2. 次のコマンドを入力します。crypto ca enroll Verisign質問に回答するよう求められます。
- 3. [Display Certificate Request to terminal] に [yes] と入力し、その出力を Verisign に送信します。
- 4. Verisign から新しい証明書を受け取ったら、次のコマンドを入力します。crypto ca import Verisign certificate

インストールされた証明書の表示

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Manage Certificates] を選択します。トラストポイントの認証に使用 する CA 証明書およびサード パーティ ベンダーから発行された ID 証明書が [Manage Certificates] エリアに表示されます。

Configuration > Properties > Ce	rtificate > Manage Cer	tificates				
Startup Wizard	Manage Certificates					
🕀 🚮 AAA Setup	Manage the Certificat	es associate	atoicoteunt difue b			
	manage the certificat	00 00000000	u wara u ustporns.			
E-B ARP						
— 🛃 Auto Update	Subject	Туре	Trustpoint	Status	Usage	Add
	VeriSign Trial	CA	my.verisign.tru	Available	General Purpo	
E-Certificate	webypn.cisco	Identity	my.verisign.tru	Available	General Purpo	Show Details
Authentication						
						Petrech
Import Certificate						Neirean
Key Pair						1
Manage Certificates						Delete
E-62 Trustpoint						
Configuration						
ンドフインの例						

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 (c)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 (c)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:			
63bla5cdc59f78801da0636cf975467b 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 (c)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.			

Web ブラウザによる WebVPN 用にインストールされた証明書の確認

WebVPN が新しい証明書を使用していることを確認するには、次の手順を実行します。

- 1. Web ブラウザを介して WebVPN インターフェイスに接続します。証明書を要求するために 使用した FQDN とともに https:// を使用します(たとえば、https://webvpn.cisco.com のよ うにします)。次のいずれかのセキュリティ アラートが表示された場合、そのアラートに 対応する手順を実行します。The Name of the Security Certificate Is Invalid or Does Not Match the Name of the SiteASA の WebVPN インターフェイスに接続するために正しい FQDN/CN を使用したことを確認します。ID 証明書を要求したときに定義した FQDN/CN を 使用する必要があります。show crypto ca certificates trustpointname コマンドを使用すると 、証明書の FQDN/CN を確認できます。The security certificate was issued by a company you have not chosen to trust...Web ブラウザにサードパーティ ベンダーのルート証明書をイ ンストールするには、次の手順を実行します。Security Alert ダイアログ ボックスで、View Certificate をクリックします。Certificate ダイアログ ボックスで、Certificate Path タブをク リックします。発行された ID 証明書の上にある CA 証明書を選択し、View Certificate をク リックします。[Install Certificate] をクリックします。Certificate Install Wizard ダイアログ ボックスで Next をクリックします。Automatically select the certificate store based on the type of certificate オプション ボタンを選択し、Next をクリックし、次に Finish をクリック します。証明書のインストールを確認するプロンプトが表示されたら、Yes をクリックしま す。Import operation was successful プロンプトで、OK をクリックし、次に Yes をクリッ クします。**注:この例では**Verisignトライアル証明書を使用しているため、ユーザが接続す る際の検証エラーを回避するために、VerisignトライアルCAルート証明書をインストールす る必要があります。
- WebVPN login ページの右下隅に表示されているロック アイコンをダブルクリックします。
 インストールされている証明書の情報が表示されます。
- 3. 内容を確認し、サードパーティベンダーの証明書に合致することを確認します。

Certificate ?		
Ge	eneral Details Certification Path	_ 1
	Certificate Information	
	This certificate is intended for the following purpose(s):	-
	 Ensures the identity of a remote computer 	
	* Refer to the certification authority's statement for details.	_
	Issued to: webvpn.cisco.com	
	Issued by: VeriSign Trial Secure Server Test CA	
	Valid from 8/14/2007 to 8/29/2007	
		_
	Install Certificate Issuer Statemer	nt
	0	

SSL 証明書の更新手順

SSL 証明書を更新するには、次の手順を実行します。

- 1. 更新するトラストポイントを選択します。
- 2. [enroll] を選択します。次のメッセージが表示されます。*If it is successfully enrolled again, the current cert will be replaced with the new ones.Do you want to continue?*
- 3. [Yes] を選択します。これにより、新しい CSR が生成されます。
- 4. CSR を CA に送信し、返信された新しい ID 証明書をインポートします。
- 5. 外部インターフェイスへのトラストポイントを削除し、再度適用します。

コマンド

ASA では、コマンド ラインで各種の show コマンドを使用し、証明書の状況を確認できます。

- show crypto ca trustpoint 設定されているトラストポイントを表示します。
- show crypto ca certificate システムにインストールされているすべての証明書を表示しま

す。

- show crypto ca crls キャッシュされている Certificate Revocation List (CRL; 証明書失効リ スト)を表示します。
- show crypto key mypubkey rsa 生成されたすべての暗号鍵ペアを表示します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

発生する可能性のあるエラーを次に示します。

- %Warning:CA cert is not found.The imported certs might not be usable.INFO:Certificate successfully importedCA 証明書が正しく認証されていません。CA 証明書がインストールさ れていることを確認するには、show crypto ca certificate trustpointname コマンドを使用しま す。CA 証明書で始まる行を探します。CA 証明書がインストールされている場合は、正しい トラストポイントを参照していることを確認します。
- ERROR:Failed to parse or verify imported certificateこのエラーが発生する可能性があるのは、ID 証明書をインストールしたけれども、関連付けられたトラストポイントで認証された正しい中間証明書またはルート CA 証明書がない場合です。正しい中間証明書またはルート CA 証明書を使用して削除と再認証を行う必要があります。正しい CA 証明書を受け取っていることを確認するには、サードパーティ ベンダーに問い合せてください。
- Certificate does not contain general purpose public keyこのエラーが発生する可能性があるの は、正しくないトラストポイントに ID 証明書をインストールしようとした場合です。無効な ID 証明書をインストールしようとしているか、トラストポイントと関連付けられた鍵ペアが ID 証明書に含まれている公開鍵と合致しません。正しいトラストポイントに ID 証明書をイ ンストールしたことを確認するには、show crypto ca certificates trustpointname コマンドを 使用します。Associated Trustpoints がある行を探します。正しくないトラストポイントが表 示されている場合は、このドキュメントで説明されている手順に従って、トラストポイント を削除して適切なトラストポイントを再インストールします。また、CSR が生成されてから キーペアが変更されていないことも確認します。
- エラーメッセージ:%PIX|ASA-3-717023 SSL failed to set device certificate for trustpoint [trustpoint name]このメッセージが表示されるのは、SSL 接続を認証するために、指定のトラ ストポイント用のデバイス証明書を設定したときにエラーが発生した場合です。SSL 接続が アップ状態になると、使用されるデバイス証明書が設定されます。エラーが発生すると、デ バイス証明書のロードに使用される必要がある設定済みのトラストポイントと、エラーの理 由が含まれるエラーメッセージがログに記録されます。trustpoint name—Name of the trustpoint for which SSL failed to set a device certificate.推奨処置:障害に対して報告された 理由で示された問題を解決します。指定のトラストポイントは登録済みであり、デバイス証 明書があることを確認します。デバイス証明書が有効であることを確認します。必要に応じ てトラストポイントを再度登録します。

関連情報

- ASA で ASDM を使用して Microsoft Windows CA からデジタル証明書を取得する方法
- ・<u>セキュリティ製品に関するField Notice</u>
- <u>Requests for Comments (RFCs)</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>