O ASA 7.x instala manualmente certificados de terceiros para uso com o exemplo de configuração da WebVPN

Contents

Introduction **Prerequisites Requirements Componentes Utilizados Conventions** Configurar Etapa 1. Verifique se os valores de data, hora e fuso horário estão corretos Etapa 2. Gerar o par de chaves RSA Etapa 3. Criar o ponto de confiança Etapa 4. Gerar a inscrição de certificado Etapa 5. Autenticar o ponto confiável Etapa 6. Instalar o certificado Passo 7. Configurar o WebVPN para usar o certificado recém-instalado Verificar Substituir certificado autoassinado do ASA Exibir certificados instalados Verificar o certificado instalado para WebVPN com um navegador da Web Etapas para renovar o certificado SSL Comandos Troubleshoot Informações Relacionadas

Introduction

Este exemplo de configuração descreve como instalar manualmente um certificado digital de terceiros no ASA para uso com WebVPN. Um certificado de avaliação de versão é usado neste exemplo. Cada etapa contém o procedimento de aplicação ASDM e um exemplo de CLI.

Prerequisites

Requirements

Este documento exige que você tenha acesso a uma autoridade de certificação (AC) para a inscrição de certificado. Os fornecedores de CA de terceiros suportados são Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA e VeriSign.

Componentes Utilizados

Este documento usa um ASA 5510 que executa a versão de software 7.2(1) e a versão 5.2(1) do ASDM. No entanto, os procedimentos neste documento funcionam em qualquer dispositivo ASA executado 7.x com qualquer versão ASDM compatível.

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.

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Configurar

Para instalar um certificado digital de terceiros no PIX/ASA, faça o seguinte:

- 1. <u>Verifique se os valores de data, hora e fuso horário estão corretos</u>.
- 2. Gere o par de chaves RSA.
- 3. <u>Crie o ponto de confiança</u>.
- 4. Gerar a inscrição de certificado.
- 5. Autentique o ponto de confiança.
- 6. Instale o certificado.
- 7. Configure o WebVPN para usar o certificado recém-instalado.

Etapa 1. Verifique se os valores de data, hora e fuso horário estão corretos

- 1. Clique em Configuração e, em seguida, clique em Propriedades.
- 2. Expanda Administração de dispositivos e escolha Relógio.
- Verifique se as informações listadas estão corretas.Os valores de Data, Hora e Fuso Horário devem ser precisos para que ocorra a validação adequada do certificado.



Exemplo de linha de comando

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

Etapa 2. Gerar o par de chaves RSA

A chave pública RSA gerada é combinada com as informações de identidade do ASA para formar uma solicitação de certificado PKCS#10. Você deve identificar distintamente o nome da chave com o ponto de confiança para o qual você cria o par de chaves.

- 1. Clique em Configuração e, em seguida, clique em Propriedades.
- 2. Expanda Certificate e escolha Key Pair.
- 3. Clique em Add.

as.	El-101 Certificate	1				
66	Authentication					
NAT	Enrolment	Key P	air Nama	Lisage	Modulus Size	A dat
	- El Import Certificate	10097		osage	modulus dize	700
<u>21</u>	- Key Pair					
UDAL VIDAL	- An Manage Certificates					Show Details
VPN	E- A Trustpoint					
a	- R Configuration					Delete
	- Export	💼 Add Key Pair			×	BOH949
CSD Manager	- Import					
	E-G Device Access					Refresh
1 128	E-S Device Administration	Nome: C	Use default key nam	e		
Routing	P- C DHONServices			-		
	R-B DNS		my.verisign.key			
8	High Availability and Scal	_				
Clobal Objects	Fairwar	Size: 10	24 💌			
Giobal Objects	Fragment					
	- Wistony Metrice	Linear G	Ceneral Dumona	C Service		
20	MILLION Y MELLOS	Usage. (*	General Purpose	 Special 		
Properties	E D Ave					
	E Cogging	Canarata Nava	Cancel	blain		
	Phoney Queue	Generale Now	Caricel	map		
	SSL SSL					
	SUNPC Server					
	TCP Options					
	Timeouts					

- 4. Insira o nome da chave, escolha o tamanho do módulo e selecione o tipo de uso. Note: O tamanho recomendado do par de chaves é 1024.
- 5. Clique em **Gerar**.O par de chaves que você criou deve estar listado na coluna Nome do par de chaves.

Exemplo de linha de comando

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)#

Etapa 3. Criar o ponto de confiança

Os pontos de confiança são necessários para declarar a autoridade de certificação (CA) que o ASA usará.

- 1. Clique em Configuração e, em seguida, clique em Propriedades.
- 2. Expanda Certificate e expanda Trustpoint.
- 3. Escolha **Configuração** e clique em **Adicionar**.

Configuration > Properties > Ce	rtificate >	Trustpoint > Confi	guration		
Startup Wizard	Configura	ation			
🕀 🚮 AAA Setup	Confi	oure a Certificate Aut	hority (CA) as a trustnoint		
	Com	gui e a certinicate Mu	nonty (GA) as a nasquent.		
🔁 🖳 🖓 ARP					
Client Update	ſ				
E-M Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add
Authentication					
Enrolment					Edit
Import Certificate					
- Sig Key Pair					
Manage Certificates					Delete
E-Ba Trustpoint		N			
- 30 Contiguration		45			Request CRL
Export					
- import					
Device Access					

- Configure estes valores: Nome do ponto de confiança: O nome do ponto confiável deve ser relevante para o uso pretendido. (Este exemplo usa *my.verisign.trustpoint.*)Par chave: Selecione o par de chaves gerado na <u>Etapa 2</u>. (*my.verisign.key*)
- 5. Verifique se a opção Inscrição manual está selecionada.
- 6. Clique em **Parâmetros de certificado**. A caixa de diálogo Parâmetros do certificado é exibida.
- 7. Clique em **Editar** e configure os atributos listados nesta tabela:Para configurar esses valores, escolha um valor na lista suspensa **Attribute (Atributo), insira o valor e clique em Add** (Adicionar).

	WEDVDIT.CISCU.C	Common Name (CN)					
	TSWEB	Department (OU)			ed	to be Adde	tribute
stems	Cisco Systems	Company Name (O)					
rolina	North Carolina	State (St)	Add	•	Attribute	Select A	te:
	US	State (St)					
	Raleigh	Location (L)	Del				
						<i>.</i>	
	Raleigh	Location (L)	Del				ue:

- 8. Quando os valores adequados forem adicionados, clique em OK.
- 9. Na caixa de diálogo Parâmetros do certificado, insira o FQDN no campo Especificar FQDN.Esse valor deve ser o mesmo FQDN usado para o nome comum (CN).

🚰 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. Click **OK**.
- 11. Verifique se o par de chaves correto está selecionado e clique no botão de opção Usar inscrição manual.
- 12. Clique em OK e em Aplicar.

Add Trustpoint Co	nfiguration	
Trustpoint Name:	my.verisign.truspoint	
Generate a self	-signed certificate on enrollment	
If this option is e	enabled, only Key Pair and Certificate Parameters can be specified.	
Enrollment Settings	Revocation Check CRL Retrieval Policy CRL Retrieval Method OCSP Rules Adv	anced
Key Pair:	my.verisign.key Show Details New Key Pair	
Challenge Password:	Confirm Challenge Password:	
Eproliment Mode	can only be energified if there are no partificates associated with this trustment	
Enrolment Mode	can only be specified in there are no certificates associated with this trustpoint.	
(Lise m	anual enrolment	
C		
Use au	tomatic enrollment	
Enrollmer	nt URL: http://	
Retry Per	riod: 1 minutes	
Retry Co	unt: 0 (Use 0 to indicate unlimited retries)	
	Certificate Parameters	
	OK Cancel Help	

Exemplo de linha de comando

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>
<i>! Defines x.500 distinguished name.</i> ciscoasa(config-ca- trustpoint)# keypair my.verisign.key
<i>! Specifies key pair generated in <u>Step 3</u>.</i> ciscoasa(config-ca-trustpoint)# fqdn webvpn.cisco.com
! Specifies subject alternative name (DNS:).

Etapa 4. Gerar a inscrição de certificado

Procedimento ASDM

- 1. Clique em Configuração e, em seguida, clique em Propriedades.
- 2. Expanda Certificate e escolha Enrollment.
- Verifique se o ponto de confiança criado na <u>Etapa 3</u> está selecionado e clique em Inscrever. Aparece uma caixa de diálogo que lista a solicitação de inscrição de certificado (também chamada de solicitação de assinatura de certificado).

X

🚰 Enrollment Request



 Copie a solicitação de inscrição PKCS#10 em um arquivo de texto e envie o CSR ao fornecedor de terceiros apropriado.Depois que o fornecedor terceirizado receber o CSR, ele deverá emitir um certificado de identidade para instalação.

Exemplo de linha de comando

Nome do dispositivo 1

```
ciscoasa(config)#crypto ca enroll my.verisign.trustpoint

! 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,
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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3vEJq
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]:
ciscoasa(config)#
```

Etapa 5. Autenticar o ponto confiável

Depois de receber o certificado de identidade do fornecedor terceirizado, você pode prosseguir com esta etapa.

- 1. Salve o certificado de identidade no computador local.
- 2. Se você recebeu um certificado codificado em base64 que não veio como um arquivo, você deve copiar a mensagem base64 e colá-la em um arquivo de texto.
- 3. Renomeie o arquivo com uma extensão .cer.**Observação:** quando o arquivo for renomeado com a extensão .cer, o ícone do arquivo deverá ser exibido como um certificado.
- 4. Clique duas vezes no arquivo do certificado. A caixa de diálogo Certificado é

Certificate	? ×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s):	
•Ensures the identity of a remote computer •Proves your identity to a remote computer •2.16.840.1.113733.1.7.21	

ção: se a *mensagem* "*O Windows não tem informações suficientes para verificar esse certificado*" for exibida na guia Geral, você deverá obter a CA raiz de terceiros ou o certificado CA intermediário antes de continuar com este procedimento. Entre em contato com o fornecedor de terceiros ou o administrador de CA para obter a AC raiz ou o certificado de CA intermediário emissor.

- 5. Clique na guia Caminho do certificado.
- 6. Clique no certificado CA localizado acima do certificado de identidade emitido e clique em **Exibir**

Certificate	? ×	
General Details Certification Path		
Certification path Image: VeriSign Trial Secure Server Test Root CA Image: VeriSign Trial Secure Server Test CA Image: VeriSign Trial Secure Server Test CA Image: VeriSign Trial Secure Server Test CA		
	View Certificate	
Certificate status:		
This certificate is OK.		
	ОК	Infor

certificado.

mações detalhadas sobre o certificado CA intermediário são exibidas. **Aviso:** não instale o certificado de identidade (dispositivo) nesta etapa. Somente a raiz, raiz subordinada ou certificado CA são adicionados nesta etapa. Os certificados de identidade (dispositivo) estão instalados na Etapa 6.

7. Clique em

Certificate	? ×
General Details Certification Path	1
	1
Show: <all></all>	-
,	
Field	Value 🔺
E 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:
Subject	VeriSign Trial Secure Server Te
	RSA (2048 Bits)
E	dit Properties Copy to File
	ОК

Details.

- 8. Clique em Copiar para arquivo.
- 9. No Assistente para exportação de certificado, clique em Avançar.
- Na caixa de diálogo Export File Format (Exportar formato de arquivo), clique no botão de opção X.509 (.CER) codificado em Base-64 e clique em Next (Avançar).

(port Fi Certif	le Format icates 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)
0	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 > Car

- 11. Insira o nome do arquivo e o local no qual deseja salvar o certificado CA.
- 12. Clique em Avançar e, em seguida, clique em Concluir.

ertificate Expo	rt Wizard				
File to Expor Specify th	t le name of the file you wa	ant to export			
File name:	:			_	
c:\introo	tca			Browse	e
		< B	ack Net	xt >	Cancel
					Cancor

- 13. Clique em **OK** na caixa de diálogo Exportar com êxito.
- 14. Navegue até o local onde você salvou o certificado CA.
- 15. Abra o arquivo com um editor de texto, como o Bloco de Notas. (Clique com o botão direito do mouse no arquivo e escolha Enviar para > Bloco de Notas.)A mensagem codificada em base64 deve ser semelhante ao certificado nesta imagem:

File Edit Format View Help

----BEGIN CERTIFICATE---MIIFSjçCBDKqAwIBAqIQCECQ47aTdj6BtrI60/Vt6zANBqkqhkiG9w0BAQUFADCB yzelMA&GA1UEBhMCVVMxFzAVBqNVBAoTD]Z]cm]TaWduLCBJbmMuMTAwLqYDVQQL ÉydGb3IqVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV BĀsTOVRĪcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz L3R]c3RjYSAOYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwqU2VidXJ1IFN] cnZlciBUZXNOIENBMB4XDTA3MDcyNzAwMDAwMFoXDTA3MDgxMDIzNTkloVowgZ4x CZAJBGNVBAYTA]VTMRCwFQYDVQQIEw50b3J0aCBDYXJVbG]uYTEWMBQGA1UEČhQN Q21zY28qU31zdGVtczEOMAwGA1UECXQFVFNXRUIX0jA4BqNVBAsUMVR1cm1zIG9m IHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxEjAQBgNV BAMUCWNsaWVudHZwbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1V9Ahzsm SZiUwosov+yL/SMZUĹWKigVgwズlaVJ4UwqpUg9TqaIEn9wFvrZmJdOT/ucJW6k1A TjajzxxSocuVAKuJ7cnOxSj+KlHIBNUjz8Ey3r26nLa9fBCOK9YSZ6fA7zJimMQp RŴMāzEvoFaiiY+5oG7XAiWCPY4677K3INFECAWEAAaOCAdcwqqHTMAkGA1UdEwQC MAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TV]JTZWN1 cmUtY3JsLnZlcmlzaŴdūLmNvbS9TVlJUcmlhbDIwMDUuY3JsMEoGALUdIARDMEEw PWYKYIZIAYb4RQEHFTAXMC8GCCsGAQUFBWIBFiNodHRwczovL3d3dy52ZXJpc2ln bi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw HwYDVR0jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBq MCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUH MAKGNmh0dHA6Ly9Tv]JTZWN1cmUtyW]hLnZ]cm]zaWduLmNvbS9Tv[JUcm]hbDIw MDUtywlhLmNlcjBuBqqrBqEFBQcBDARiMGChXqBcMFowWDBWFqlpbWFnZS9naWYw ITAFMACGBSsOAwIaBBRLa7ko]gYMu9BSOJspresHiyEFGDAmFiRodHRw0i8vbG9n by52zxJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKozIhvcNAQEFBQADggEBAC4k abSwqooGaNtm4lrJhv8TSGsjdPpOspLSeBFxuLEzJlTHGprCf0sALrqb1FEL4b9q 1/EajjdteeYTqIorIC1aWwWx+RHCcTqIrlzf0vfUD0DNZ6949sM2aGaMzrRsBy63 Lb1/3+jz8skIAkiZP79pmqMEECZ+cUm10rk631c46yBCsJMZVbG6sZlNSI80RRwK hAKDsfufvsirHc8c9nJdoEC0905izUTrE854jvlXzŽjiOJ51FbcmCOx/uB7zv3zC Ftm412+TgfyZ3z7wCEnUlvhMa7bc2T3mmdqB5kCeHEZ2kAL6u6N0pXy5l7TLKy1a idT1FmBvf02qaZS6S40= ----END CERTIFICATE----

- 16. No ASDM, clique em **Configuration** e em **Properties.**
- 17. Expanda Certificate e escolha Authentication.
- 18. Clique no botão de opção Enter the certificate text in hexadecimal or base64 format.
- 19. Cole o certificado CA formatado com base64 do editor de texto na área de texto.
- 20. Clique em
 - Autenticar.

Configuration > Properties > Certificate > Authentication					
Startup Wizard	Authentication				
AAA Setup	Authenticate a CA certificate. As the result of authentication, the CA certificate will be associated with a trustpoint and installed on the device.				
Auto Update	Trustpoint Name: my.verisign.truspo Edit New				
Authentication	Fingerprint (optional):				
-83 Key Pair	The certificate text can be specified if the selected trustpoint is configured for manual enrolment.				
Manage Certificates Manage Certificates Manage Certificates Configuration Export Monort Device Access Device Administration DHCP Services High Availability and Scal Failover Fragment History Metrics HITPALTIPS	Certificate Text				
P Audit Logging Priority Queue SSL SUNRPC Server TCP Options Timeouts URL Filtering WCCP	Authentication Successful Authentication Successful The trustpoint my.verisign.truspoint has been authenticated. OK				

21. Click **OK**.

Exemplo de linha de comando

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
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAw
LGYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4x
MjAwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290
IENBMB4X
DTA1MDIwOTAwMDAwMFoXDTE1MDIwODIzNTk10VowgcsxCzAJBgNVBAYT
Alvimcw
FQYDVQQKEw5WZXJpU21nbiwgSW5jLjEwMC4GA1UECxMnRm9yIFR1c3Qg
UHVycG9z
ZXMgT25seS4gIE5vIGFzc3VyYW5jZXMuMUIwQAYDVQQLEz1UZXJtcyBv
ZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMp
MDUxLTAr
BgNVBAMTJFZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBD

DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALsXGt1M4HyjXwA+/NAu
wElv6IJ/
${\tt DV8zgpvxuwdaMv6fNQBHSF4eKkFDcJLJVnP53ZiGcLAAwTC5ivGpGqE6}$
1BBD6Zqk
d851P1/6XxK0EdmrN7qVMmvBMGRsmOjje1op5f0nKPqVoNK2qNUB6n45
1P4qoyqS
E0bdru16quZ+II2cGFAG1oSyRy4wvY/dpVHuZOZqYcIkK08yGotR2xA1
D/OCCmZO
5RmNqLLKSVwYHhJ25EskFhgR2qCxX2EQJdnDXuTw0+4tlqj97ydk5iDo
xjKfV6sb
tnp3TIY6S07bTb9gxJCk4pGbcf8DOPvOfGRu1wpfUUZC8v+WKC20+sK6
QMECAWEA
AaOCAVwwggFYMBIGA1UdEwEB/wQIMAYBAf8CAQAwSwYDVR0gBEQwQjBA
BgpghkgB
hvhFAQcVMDIwMAYIKwYBBQUHAgEWJGh0dHBzOi8vd3d3LnZ1cmlzaWdu
CHMvdGVzdGNhLzAOBgNVHQ8BAf8EBAMCAQYwEQYJYIZIAYb4QgEBBAQD
A1UdDgQWBBRmIo6B4DFZ3Sp/qUbFNgIGcCeHWjCBsgYDVR0jBIGqMIGn
oYGSpIGP
MIGMMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIE1uYy4x
MDAuBgNV
BASTJUZVC1BUZXN0IFB1cnBvc2VzIE9ubHkuICBObyBhc3N1cmFuY2Vz
AIUEAXMPVmvyavNpz24gvHJpYWWgU2vJdXJIIFNICHZICIBUZXNUIFJV
DSQQQUGC
CCCCI6/DggLewTagTIa9H3MwDQ10KOZIHVCNAQEFDQADg1EAS25V6S5/
Kaf234YROiL51ZS111oUZ2MANp2H4biw4itfsG5spDDlwSRmiH3BW/SU
6EEzD90i
Ai9TXvRIcD5g0mB+nvK9fB2aBzOiaiHSiIWzAJeOiugA+O93iNew+peu
i4AhdvGN
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)#

Etapa 6. Instalar o certificado

Procedimento ASDM

Use o certificado de identidade fornecido pelo fornecedor terceirizado para executar estas etapas:

- 1. Clique em Configuração e, em seguida, clique em Propriedades.
- 2. Expanda Certificate e escolha Import Certificate.
- Clique no botão de opção Enter the certificate text in hexadecimal or base64 format e cole o certificado de identidade base64 no campo de texto.

Configuration > Properties > C	ertificate > Import Certificate			
Startup Wizard	Import Certificate			
🖲 🚮 AAA Setup	loatell as identity antidicate that uses yearing from a Cartificate Authority (CA) is years as to a manual			
- B Anti-Spoofing	enrolment request			
🟵 🐻 ARP	Construction of Construction			
	Trusteeint Name			
Certificate	Indisport Name. my verisign truspo Edit New			
- Authentication				
	Certificate Text			
Import Certificate	C based from a film			
Key Pair	Composition a rise.			
Manage Certificates				
Trustpoint	(*) Enter the certificate text in hexadecimal or base64 format:			
Configuration				
	USBSOJSpreshtyer GDAminikodhkwolavbGenby522XJpc2hbojb20vanis			
import	MSSHBYYTWD013K02ImcNA0EFD0ADggEDAAhTVWSKFOgkWYXY0pF1			
Device Access	FEVERSENIACK/MINEMAMMA4075K/EtzoVI Initial Doi 138001 JAmetro Da TAVIATAVE			
B B Device Administration	0YVwM3kDQAO6EbArtUoAxovDbJucdx86ZVTtyevMcgzCkX0HEVxa5P)			
P B DNS	ssX9YJtvhNjaKCHzSHstd69N20SmluEOR4utcGgGZD8tVGx26b5OWTz8K			
High Availability and Scal	8EvHm3grdbDZP+ISMotWYE+CgfKpZb+CPAqH2Cdpz2aJljJhl6CS6NM=			
Falover	END CERTIFICATE			
- Fragment				
- Mistory Metrics				
HTTP/HTTPS	🚺 Information 🛛 🕺			
🕀 📲 🔁 IP Audit				
🟵 🛅 Logging				
- mail Priority Queue	Certificate import succeeded.			
SUNRPC Server				
TCP Options				
Timeouts	OK			
URL Fitering				
CCP WCCP				
1				

4. Clique em Importar e, em seguida, clique em OK.

Exemplo de linha de comando

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
EydGD31gVGvZdCBQdXJwD3N1CyBPDmx5L1AgTm8gYXNZdXJhDmN1Cy4x
Q]BABGNV
bASTOVRICHIZIGJHIRVZZSBNACBOARKWCZOVLJAJAJQJZZZAJDCZINDIJ
dx.TITENI
cnZlciBUZXN0IENBMB4XDTA3MDcvNjAwMDAwMFoXDTA3MDgwOTIzNTk1
OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBDYXJvbGluYTEQMA4G
AluebxQH
UmFsZWlnaDEWMBQGA1UEChQNQ21zY28gU31zdGVtczEOMAwGA1UECxQF
VFNXRUIX

OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29t
L2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20w
gZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ
/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1Ec
rO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxS1Egry
osBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF
oDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJ1LWNybC52ZXJpc21n
bi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUw
MTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0
Y2EwHOYD
~ VR01BBYwFAYIKwYBBOUHAwEGCCsGAOUFBwMCMB8GA1UdIwOYMBaAFGYi
ioHgMVnd
Kn+rRsU2AgZwJ4daMHgGCCsGAOUFBwEBBGwwaiAkBggrBgEFBOcwAYYY
aHR0cDov
L29ic3AudmVvaXNpZ24uY29tMEIGCCsGAOUFBzAChiZodHRwOi8vU1ZS
u2vidxJ1
LWFpYS52ZXJpc21nbi5ib20vU1ZSVHJpYWwvMDA1LWFpYS5iZXIwbgYI
KwybBouh
AOWEY jBgoV6gXDBaMFgwVhYJaW1hZ2UvZ21mMCEwHzAHBgUrDgMCGgOU
S2u5KJYG
DLyOUiibKaxLB4shBRgwJbYkaHR0cDoyL2xyZ28udmVyaXNpZ24uY29t
L3ZzbG9n
bzEuZ21mMA0GCSgGSIb3D0EBB0UAA4IBA0Anvm4GVThPIvL/9v1DBd8N
7/vW30v3
blirHfHJvfPJ1znZOXvXdObpZkuA6Jvu03V2CYNnDomn4xRXOTUDD8g8
6ZiKvMIj
XM2VCmcHSajmMMRvjpvdxfk6CIdDMtMGotCavRHD9T12tvwgrBock/v/
540021kB
SmlzVV7crlV.TEuhaau3Pz7aNRd8N0Un6c9sbw01BuM990xzTzdAo89FS
rtab5F+oiTc5xGv8w7NARAfNgFXihgnLgWTtA35/oWuv86bie1TWbevg
i8ePM9Td
01.daw6kIII11PNimPt+MDhcF7cuevn+R0ks0c0PBPy5F.TCcMiII7Cryiu50
END CERTIFICATE
mit
INFO. Certificate successfully imported
ciscoasa (config) #
CISCOASA (CONTINUE) #

Passo 7. Configurar o WebVPN para usar o certificado recém-instalado

- 1. Clique em Configuração, clique em Propriedades e escolha SSL.
- 2. Na área Pontos confiáveis, selecione a interface que será usada para encerrar sessões WebVPN. (Este exemplo usa a interface externa.)
- 3. Clique em **Editar**. A caixa de diálogo Editar ponto de confiança SSL é exibida.

Configuration > Properties > S	SL .			
Startup Wizard	SSL			
🕀 🖬 AAA Setup	Configure SSI according. These according offent both ASDM and Michigh Childrenes.			
	Configure SSL parameters. These parameters affect outh ASUM and WebYPM access.			
12-103 ARP	Server SSL Version: Any Client SSL Version: Any			
	Encryption			
	End Boost			
E-Certificate	Available Algorithms Add >> Active Algorithms Move Up			
E Device Access	30ES-SHA1			
1 Device Administration	The Edit SSI Trustoniot			
E BHCP Services				
🕀 👼 DNS	Specify an enrolled trustpoint to be used for SSL authentication on the outside interface. To enroll a trustpoint			
High Availability and Scal	ao to Configuration > Properties > Certificate > Enrolment.			
- Failover				
Fragment				
-24 History Metrics				
HTTP/HTTPS	Interface: outside			
P Audit				
Logging	Enroled Trustpoint: my.verisign.trustp			
Priority Queue				
SUNKPC Server				
The options	City Cancel nep			
UNL LIEL Electron				
	Trustpoints			
the state of the s	Specify which enrolled trustpoints, if any, should be used for SSL authentication on each interface. The fallback			
	trustpoint will be used on interfaces not associated with a trustpoint of their own.			
	Fallback Trustroint			
	Interface Trustpoint Edit			
	management			
	o telde mu varision truetoaixt			
	per presidente a constructione e			
I I				

- 4. Na lista suspensa Ponto confiável inscrito, escolha o ponto confiável criado na Etapa 3.
- 5. Clique em OK e em Aplicar.

Seu novo certificado deve agora ser utilizado para todas as sessões WebVPN terminadas na interface especificada. Consulte a seção Verificar neste documento para obter informações sobre como verificar uma instalação bem-sucedida.

Exemplo de linha de comando

ciscoasa
ciscoasa(config)# ssl trust-point my.verisign.trustpoint outside
! Specifies the trustpoint that will supply the SSL ! certificate for the defined interface. ciscoasa(config)#write memory
Building configuration Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08
8808 bytes copied in 3.630 secs (2936 bytes/sec) [OK] ciscoasa(config)#
! Save configuration.

Verificar

Esta seção descreve como confirmar se a instalação do certificado de fornecedor terceirizado foi bem-sucedida.

Substituir certificado autoassinado do ASA

Esta seção descreve como substituir o certificado autoassinado instalado do ASA.

- 1. Emita uma solicitação de assinatura de certificado para Verisign.Depois de receber o certificado solicitado da Verisign, você poderá instalá-lo diretamente no mesmo ponto de confiança.
- 2. Digite este comando: crypto ca enroll VerisignVocê é solicitado a responder às perguntas.
- 3. Para Exibir solicitação de certificado para terminal, insira yes e envie a saída para Verisign.
- 4. Depois de fornecer o novo certificado, digite este comando: crypto ca import Verisign certificate

Exibir certificados instalados

Procedimento ASDM

- 1. Clique em **Configuração** e clique em **Propriedades**.
- 2. Expanda **Certificado** e escolha **Gerenciar Certificados**.O certificado CA usado para autenticação de ponto confiável e o certificado de identidade emitido pelo fornecedor terceirizado devem aparecer na área Gerenciar



Exemplo de linha de comando





Verificar o certificado instalado para WebVPN com um navegador da Web

Para verificar se o WebVPN usa o novo certificado, siga estas etapas:

- 1. Conecte-se à interface WebVPN por meio de um navegador da Web. Use https:// junto com o FQDN usado para solicitar o certificado (por exemplo, https://webvpn.cisco.com).Se você receber um desses alertas de segurança, execute o procedimento correspondente a esse alerta: O nome do certificado de segurança é inválido ou não corresponde ao nome do siteVerifique se você usou o FQDN/CN correto para se conectar à interface WebVPN do ASA. Você deve usar o FQDN/CN que definiu guando solicitou o certificado de identidade. Você pode usar o comando show crypto ca certificate trustpoint name para verificar os certificados FQDN/CN.O certificado de segurança foi emitido por uma empresa em que você não optou por confiar...Conclua estes passos para instalar o certificado raiz de fornecedor terceirizado em seu navegador da Web:Na caixa de diálogo Alerta de segurança, clique em Exibir certificado. Na caixa de diálogo Certificado, clique na guia Caminho do certificado. Selecione o certificado CA localizado acima do certificado de identidade emitido e clique em Exibir certificado. Clique em Install certificate (Instalar certificado). Na caixa de diálogo Assistente de instalação de certificado, clique em Avançar. Selecione a opção Selecionar automaticamente o arquivo de certificados com base no botão de opção tipo de certificado, clique em Avançar e, em seguida, clique em Concluir. Clique em Sim quando receber o prompt de confirmação Install the certificate.No prompt A operação de importação foi bem-sucedida, clique em OK e, em seguida, clique em Sim. Observação: como este exemplo usa o certificado de avaliação de versão, o certificado raiz de CA de avaliação de versão deve ser instalado para evitar erros de verificação quando os usuários se conectam.
- 2. Clique duas vezes no ícone de cadeado exibido no canto inferior direito da página de login do WebVPN.As informações do certificado instalado devem ser exibidas.
- 3. Revise o conteúdo para verificar se ele corresponde ao certificado de

	Certificate	? ×	
	General 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	
terceiros	Ok	:	

Etapas para renovar o certificado SSL

Conclua estes passos para renovar o certificado SSL:

- 1. Selecione o ponto de confiança que precisa renovar.
- 2. Escolha **Inscrever-se**.Esta mensagem é exibida: *Se ele for inscrito com êxito novamente, o certificado atual será substituído pelos novos. Deseja continuar*?
- 3. Escolha sim.lsso gerará um novo CSR.
- 4. Envie o CSR para sua CA e importe o novo certificado de ID quando o receber de volta.
- 5. Remova e reaplique o ponto de confiança à interface externa.

Comandos

No ASA, você pode usar vários comandos show na linha de comando para verificar o status de um certificado.

• show crypto ca trustpoint — Exibe pontos confiáveis configurados.

- show crypto ca certificate Exibe todos os certificados instalados no sistema.
- show crypto ca cris Exibe listas de revogação de certificados em cache (CRL).
- show crypto key mypubkey rsa —Exibe todos os pares de chaves de criptografia gerados.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Aqui estão alguns possíveis erros que você pode encontrar:

- % Aviso: Certificado CA não encontrado. Os certificados importados podem não ser utilizáveis.INFORMAÇÕES: Certificado importado com êxitoO certificado da AC não foi autenticado corretamente. Use o comando show crypto ca certificate trustpoint name para verificar se o certificado CA foi instalado. Procure a linha que começa com Certificado CA. Se o certificado CA estiver instalado, verifique se ele faz referência ao ponto de confiança correto.
- ERRO: Falha ao analisar ou verificar certificado importadoEsse erro pode ocorrer quando você instala o certificado de identidade e não tem o certificado CA raiz ou intermediário correto autenticado com o ponto de confiança associado. Você deve remover e reautenticar com o certificado CA intermediário ou raiz correto. Entre em contato com o fornecedor de terceiros para verificar se você recebeu o certificado de CA correto.
- O certificado não contém uma chave pública de finalidade geralEste erro pode ocorrer quando você tenta instalar seu certificado de identidade no ponto de confiança errado. Você tenta instalar um certificado de identidade inválido ou o par de chaves associado ao ponto de confiança não corresponde à chave pública contida no certificado de identidade. Use o comando show crypto ca certificate trustpoint name para verificar se você instalou seu certificado de identidade no ponto de confiança correto. Procure a linha que indica *Pontos de Confiança Associados:* Se o ponto de confiança errado estiver listado, use os procedimentos descritos neste documento para remover e reinstalar no ponto de confiança apropriado. Verifique também se o par de chaves não foi alterado desde que o CSR foi gerado.
- Mensagem de Erro: %PIX|ASA-3-717023 SSL falhou ao definir o certificado do dispositivo para o ponto de confiança [nome do ponto de confiança] Esta mensagem é exibida quando ocorre uma falha quando você define um certificado de dispositivo para o ponto confiável especificado para autenticar a conexão SSL. Quando a conexão SSL é ativada, é feita uma tentativa de definir o certificado do dispositivo que será usado. Se ocorrer uma falha, uma mensagem de erro será registrada que inclui o ponto confiável configurado que deve ser usado para carregar o certificado do dispositivo e o motivo da falha.nome do ponto de confiança — nome do ponto de confiança para o qual o SSL falhou ao definir um certificado de dispositivo.Ação recomendada: Resolva o problema indicado pelo motivo reportado para a falha.Certifique-se de que o ponto confiável especificado esteja inscrito e tenha um certificado de dispositivo.Verifique se o certificado do dispositivo é válido.Registre novamente o ponto confiável, se necessário.

Informações Relacionadas

<u>Como obter um certificado digital de uma CA do Microsoft Windows usando o ASDM em um</u>

<u>ASA</u>

- Avisos de campo do produto de segurança
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação Cisco Systems