Ejemplo de Configuración de IPSec entre PIX y Cisco VPN Client Usando Certificados Smartcard

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Inscripción y configuración de PIX Configuraciones Inscriba certificados de Cisco VPN Client Configure Cisco VPN Client para Utilizar el Certificado para la Conexión con el PIX Instalación de controladores de tarjeta inteligente eToken Verificación Troubleshoot Información Relacionada

Introducción

Este documento muestra cómo configurar un túnel IPSec VPN entre un Firewall PIX y un Cisco VPN Client 4.0.x. El ejemplo de configuración de este documento también resalta el procedimiento de inscripción de la entidad de certificación (CA) tanto para el router Cisco IOS® como para Cisco VPN Client, así como el uso de una Smartcard como almacenamiento de certificados.

Consulte <u>Configuración de IPSec entre Cisco IOS Routers y Cisco VPN Client Usando</u> <u>Certificados Entrust</u> para obtener más información sobre la Configuración de IPSec entre Cisco IOS Routers y Cisco VPN Client usando Certificados Entrust.

Consulte <u>Configuración de Autoridades de Certificados de Identidad Múltiple en Cisco IOS</u> <u>Routers</u> para obtener más información sobre la Configuración de Autoridades de Certificados de Identidad Múltiple en Cisco IOS Routers.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco PIX Firewall que ejecuta la versión de software 6.3(3)
- Cisco VPN Client 4.0.3 en un PC con Windows XP
- En este documento se utiliza un servidor de CA de Microsoft Windows 2000 como servidor de CA.
- Los certificados en Cisco VPN Client se almacenan usando Aladdin e-Token Smartcard.

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.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Inscripción y configuración de PIX

En esta sección se ofrece información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la <u>Command Lookup Tool</u> (sólo clientes registrados).

Configuraciones

Este documento usa estas configuraciones.

- Inscripción de certificados en PIX Firewall
- Configuración de Firewall de PIX

Inscripción de certificados en PIX Firewall			
<i>!</i> Define a hostname and domain name for the router.			
! The fully qualified domain name (FQDN) is used !			
as the identity of the router during certificate			
enrollment. pix(config)#hostname sv2-11			
sv2-11(config)#domain-name cisco.com			
<i>! Confirm that you have the correct time set on the</i>			
PIX. show clock			
clock set			
! This command clears the PIX RSA keys. ca zeroize			
rsa			
! Generate RSA (encryption and authentication) keys.			
ca gen rsa key			

- Select the modulus size (512 or 1024). !--- Confirm the keys generated. show ca mypub rsa - Define the CA identity. ca ident kobe 10.1.1.2:/certsrv/mscep/mscep.dll ca conf kobe ra 1 20 crlopt ca auth kobe ca enroll kobe [ipaddress] !--- Confirm the certificate and validity. show ca cert Configuración de Firewall de PIX PIX Version 6.3(3) interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown interface ethernet3 auto shutdown interface ethernet4 auto shutdown interface ethernet5 auto shutdown nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security4 nameif ethernet3 intf3 security6 nameif ethernet4 intf4 security8 nameif ethernet5 intf5 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname sv2-11 domain-name cisco.com fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol tftp 69 names access-list 101 permit tcp any host 209.165.201.21 eq www access-list 120 permit ip 10.1.1.0 255.255.255.0 10.0.0.0 255.255.255.0 pager lines 24 mtu outside 1500 mtu inside 1500 mtu intf2 1500 mtu intf3 1500 mtu intf4 1500 mtu intf5 1500 ip address outside 209.165.201.20 255.255.255.224 ip address inside 10.1.1.10 255.255.255.0 ip address intf2 127.0.0.1 255.255.255.255 no ip address intf3 no ip address intf4 no ip address intf5 ip audit info action alarm ip audit attack action alarm ip local pool vpnpool 10.0.0.10-10.0.0.100

```
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 120
static (inside, outside) 209.165.201.21 10.1.1.2 netmask
255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodquard enable
sysopt connection permit-ipsec
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
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpncert address-pool vpnpool
vpngroup vpncert idle-time 1800
vpngroup vpncert password *******
ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca configure kobe ra 1 20 crloptional
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum: 2ae252ac69e5218d13d35acdf1f30e55
: end
[OK]
sv2-11(config)#
```

Inscriba certificados de Cisco VPN Client

Recuerde instalar todos los controladores y utilidades necesarios que vienen con el dispositivo Smartcard en el PC para ser usados con Cisco VPN Client.

Estos pasos demuestran los procedimientos utilizados para inscribir Cisco VPN Client para

certificados MS. El certificado se almacena en la tienda Aladdin e-Token Smartcard.

- 1. Inicie un explorador y vaya a la página servidor de certificados (http://CAServeraddress/certsrv/, en este ejemplo).
- 2. Seleccione Request a certificate y haga clic en

lext.	
ddress 🕘 http://209.165.201.21/certsrv/	💙 🄁 Go 🛛 L
Microsoft Certificate Services kobe	<u>Hom</u>
Welcome	
You use this web site to request a certificate for your web brow other secure program. Once you acquire a certificate, you will identify yourself to other people over the web, sign your e-mail your e-mail messages, and more depending upon the type of	vser, e-mail client, or be able to securely messages, encrypt certificate you request
Select a task:	
O Retrieve the CA certificate or certificate revocation list	
 Request a certificate 	
Check on a pending certificate	
	Nexts

3. En la ventana Elegir tipo de solicitud, seleccione **Solicitud avanzada** y haga clic en **Siguiente**.

	1101
Choose Request Type	
Please select the type of request you would like to make:	
 User certificate request: 	
Web Browser Certificate	
E-Mail Protection Certificate	
Advanced request	
	Next >

4. Seleccione Submit a certificate request to this CA using a form y haga clic en Next.

Microsoff Certificate Services Kobe	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a following methods. Note that the policy of the certification a the certificates that you can obtain.	a computer using one of the authority (CA) will determine
 Submit a certificate request to this CA using a form. 	
 Submit a certificate request using a base64 encoded l renewal request using a base64 encoded PKCS #7 fil 	PKCS #10 file or a le.
 Request a certificate for a smart card on behalf of anot Card Enrollment Station. 	ther user using the Smart
You must have an enrollment agent certificate to submit a reque	est for another user.

5. Rellene todos los elementos del formulario de solicitud de certificado avanzado. Asegúrese de que el Departamento o la unidad organizativa (OU) corresponda al nombre del grupo de Cisco VPN Client, tal como se configuró en el nombre del vpngroup PIX. Seleccione el proveedor de servicios de certificados (CSP) adecuado para la configuración.

rtificate Request	
mation:	
ericetoken	
cisco	
vpncert	
ctd	
nsw	
AU	
e:	
Client Authentication Certificate 🔽	
eToken Base Cryptographic Provider	<u> </u>
© Exchange © Signature 💿 Both	
512 Max:1024 (common key sizes: <u>512</u> <u>1024</u>)	
Oreate new key set	
Set the container name	
OUse existing key set	
Enable strong private key protection	
Mark keys as exportable	
Use local machine store You must he an administrator to generate	
ns:	
SHA-1 💙	
Only used to sign request.	
Save request to a PKCS #10 file	
~ ~	
S 2	
	Submit >
	rtificate Request mation: ericetoken cisco vpncert ctd nsw AU AU e: Client Authentication Certificate EToken Base Cryptographic Provider Client Authentication Certificate Exchange Signature Etoken Base Cryptographic Provider Exchange Signature Set the container name Set the container name Use existing key set Set the container name Use existing key set Set the container name Use local machine store You must be an administrator to generate ns: SHA-1 Chy used to sign request. Save request to a PKCS #10 file

6. Seleccione **Yes** para continuar con la instalación cuando reciba la advertencia Validación de scripts

potencial.

Potentia	al Scripting Violation 🔣
⚠	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Yes No

7. La inscripción de certificados invoca el almacén de eToken. Introduzca la contraseña y haga

eTo	ken	
Input eTok	en password	
eToken:	eToken [AKS ifdh 0]	<u>.</u>
Password:	*****	
Login to yo your private	ur eToken to enable using key.	/creating/removing
Less <<	7 ок	Cancel

8. Haga clic en Install this certificate (Instalar este certificado).

<u>Home</u>

 Seleccione Yes para continuar con la instalación cuando reciba la advertencia Validación de scripts

potencial.

Potential Scripting Violation

This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

Yes	No
res	NO

10. Seleccione Yes para agregar el certificado raíz al almacén



11. Aparece la ventana Certificado instalado y confirma la instalación correcta.

Microsoft Certificate Services kobe	<u>Home</u>
Certificate Installed	
Your new certificate has been successfully installed.	

12. Utilice eToken Application Viewer para ver el certificado almacenado en la Smartcard.

📑 eToken Prope	erties	
eToken		
	Advanced 🕢 Refresh 🛛 👔 Help	
1000	eToken [PRO]	
Contraction of the second	Details Settings Certificates & keys	
Local Machine		
	* Evchange key /beb2b14a.e925.4476.bfb3.8e22d95	Delete
	The second	
eTokeo [AKS if		
eToken [AKS if		
eToken [AKS if	Version V3	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 5d 41 81 23	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Jacuar All new old antworp were kohe	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a-e935-4476-bfb3-8e22d95a3d19	
eToken [AKS if	Version V3 Serial number 11 00 00 00 00 00 5d 41 81 23 Signature algorithm RSA_SHA1RSA Issuer AU, nsw, ctd, apt-vpn, vpn, kobe Valid from Tuesday, 14 October 2003 2:24:58 AM Valid to Thursday, 14 October 2004 2:34:58 AM Subject AU, nsw, ctd, cisco, vpncert, ericetoken Keu container beb2b14a-e935-4476-bfb3-8e22d95a3d19	Refresh

<u>Configure Cisco VPN Client para Utilizar el Certificado para la</u> <u>Conexión con el PIX</u>

Estos pasos demuestran los procedimientos utilizados para configurar Cisco VPN Client para utilizar el certificado para las conexiones PIX.

1. Inicie Cisco VPN Client. En Connection Entries (Entradas de conexión), haga clic en **New** para crear una nueva conexión.

Ø VPN Client - Version	n 4.0.3 (Rel)			
Connection Entries Status	Certificates Log	Options	Help	
<u>Connect to to_pix</u>	Ctrl+O	-	×4	CISCO SYSTEMS
Disconnect	Ctrl+D		Delete	مالة مالة
Create Shortcut Modify				
D <u>e</u> lete Dyplicate			Host	I rans
Set as Default Connecti	on Entry	-		
<u>N</u> ew				
Import				
E <u>x</u> it VPN Client	Ctrl+Q			¥
•				•
Not connected.				

2. Complete el detalle de conexión, especifique la autenticación de certificado y seleccione el certificado obtenido de la inscripción. Click

Connection Entry:	to_pix		-
Description:	connection to pix	5	
<u>H</u> ost:	209.165.201.20		
Authentication	Transport Backup Servers	Dial-Up	
C Group Authe	ntication		
<u>N</u> ame:			
Password:			
C <u>o</u> nfirm Passv	vord:		
 Certificate Au 	Ithentication		
Name: erice	token (Microsoft)		•
□ S <u>e</u> nd CA (Certificate Chain		
			1
			-

3. Para iniciar la conexión de Cisco VPN Client con el PIX, seleccione la entrada de conexión

deseada y haga clic en Conectar

VPN Cuent - Version	4.0.5 (Ret)			1	
Connection Entries Status	C <u>e</u> rtificates <u>L</u> og	Options	<u>H</u> elp		
Connect to to_pix	Ctrl+O		1	Cisc	O SYSTEMS
Disconnect	Ctrl+D		Delete		e ále
Create Shortcut		pairy	Delete		linsan titina.
<u>M</u> odify		<u></u>	Host		Tran
D <u>e</u> lete			209,165,201	.20	IPSe
Dyplicate					
<u>S</u> et as Default Connection	on Entry				
Import					
Exit VPN Client	Ctrl+Q				
•		- U			•
Not connected.					

Instalación de controladores de tarjeta inteligente eToken

Estos pasos demuestran la instalación de los controladores <u>Aladdin</u> eToken Smartcard.

1. Abra el asistente de configuración de eToken Run time Environment 3.51.



2. Acepte los términos del acuerdo de licencia y haga clic en **Next**.

🖁 eToken Run Time Environment 3.51 Setup		
End-User License Agreement Please read the following license agreement carefully	eToken Your Key to eSecurity	RTE
ALADDIN KNOWLEDGE SYSTE	MS LTD.	^
ETOKEN ENTERPRISE END USER LIG	CENSE AGREEMENT	
IMPORTANT INFORMATION - PLEASE I CAREFULLY BEFORE OPENING THE PA THE CONTENTS THEREOF AND/OR BEFO INSTALLING THE SOFTWARE PROGRAM. USE OF THE ETOKEN ENETERPRISE PRO limitation, libraries, utilities, diskettes, CD_ROM, Guide) (hereinafter "Product") SUPPLIED BY	READ THIS AGREEME CKAGE AND/OR USI ORE DOWNLOADING ALL ORDERS FOR A ODUCTS (including with eToken® keys and the U ALADDIN KNOWLAD	NT NG OR ND Iout Ser GE
 I accept the license agree I do not accept the license 	ment e agreement	
Reset < Bac	k Next> Can	cel

3. Haga clic en **Install**.

🙀 eToken Run Time Environment 3	1.51 Setup 📃 🗖 🔀
Ready to Install the Application	T-
Click Next to begin installation.	Your Key to eSecurity RTE
	Please click Next to begin installation.
	<pre>< Back Next > Cancel</pre>

4. Los controladores eToken Smartcard están instalados. Haga clic en **Finalizar** para salir del asistente de configuración.



Verificación

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

• show crypto isakmp sa: muestra todas las asociaciones de seguridad (SA) de Internet Key Exchange (IKE) actuales en un par.

```
SV2-11(config)#show crypto isa sa
Total : 1
Embryonic : 0
dst src state pending created
209.165.201.20 209.165.201.19 QM_IDLE 0 1
```

 show crypto ipsec sa: muestra la configuración utilizada por las asociaciones de seguridad actuales.

```
SV1-11(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, local addr. 209.165.201.20
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0)
current_peer: 209.165.201.19:500
dynamic allocated peer ip: 10.0.0.10
PERMIT, flags={}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
```

#pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.19 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: c9a9220e inbound esp sas: spi: 0xa9857984(2844096900) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 1, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607996/28746) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xc9a9220e(3383304718) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4608000/28748) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

Troubleshoot

Refiérase a <u>Troubleshooting de PIX para Pasar el Tráfico de Datos en un Túnel IPSec</u> <u>Establecido</u> para obtener más información sobre la solución de problemas de esta configuración.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Solicitudes de Comentarios (RFC)
- Página de Soporte de IPSec (IP Security Protocol)
- Página de soporte para cliente Cisco VPN
- Página de soporte técnico de Firewalls PIX serie 500
- <u>Soporte Técnico Cisco Systems</u>