ASA 8.3 y posterior: NTP con y sin un ejemplo de configuración del túnel IPsec

Contenido

Introducción prerrequisitos Requisitos Componentes Utilizados Convenciones Configuración Diagrama de la red Configuración de ASDM del túnel VPN Configuración de ASDM NTP Configuración CLI ASA1 Configuración CLI ASA2 Verificación Troubleshooting Comandos para resolución de problemas Información Relacionada

Introducción

Este documento proporciona una configuración de muestra para sincronizar el reloj adaptante del dispositivo de seguridad (ASA) con un servidor de tiempo de la red usando el Network Time Protocol (NTP). ASA1 comunica directamente con el servidor de tiempo de la red. ASA2 pasa el tráfico NTP a través de un túnel IPsec a ASA1, que a su vez adelante los paquetes al servidor de tiempo de la red.

Refiérase <u>ASA/PIX: NTP con y sin un ejemplo de configuración del túnel IPsec</u> para una configuración idéntica en Cisco ASA con las versiones 8.2 y anterior.

Nota: Un router puede también ser utilizado como servidor NTP para sincronizar el reloj del dispositivo de seguridad ASA.

prerrequisitos

Requisitos

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 ASA con la versión 8.3 y posterior
- Versión 6.x y posterior del Cisco Adaptive Security Device Manager (ASDM)

Nota: Consulte <u>Cómo Permitir el Acceso HTTPS para el ASDM</u> para que el ASA sea configurado por el ASDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

Configuración

Diagrama de la red



En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del <u>RFC 1918</u>, que se han utilizado en un ambiente de laboratorio.

- Configuración de ASDM del túnel VPN
- Configuración de ASDM NTP
- <u>Configuración CLI ASA1</u>
- <u>Configuración CLI ASA2</u>

Configuración de ASDM del túnel VPN

Complete estos pasos para crear el túnel VPN:

1. Abra su <Inside_IP_Address_of_ASA> de https:// del navegador y del tipo para acceder el ASDM en el ASA.Esté seguro de autorizar cualquier advertencia que su navegador le dé relacionado con la autenticidad de certificados SSL. Nombre de usuario predeterminado y la contraseña son ambos espacio en blanco.El ASA presenta esta ventana para permitir la descarga de la aplicación

ASDM.



Este ejemplo carga la aplicación sobre la computadora local y no se ejecuta en los subprogramas java.

- 2. Haga clic el **activador de ASDM de la descarga y comience el ASDM** para descargar el instalador para la aplicación ASDM.
- 3. Una vez que el activador de ASDM descarga, complete los pasos ordenados por los prompts para instalar el software y funcionar con el Cisco ASDM launcher.
- 4. Ingrese el IP Address para la interfaz que usted configuró con el HTTP ordene, y un nombre de usuario y contraseña si usted especificó uno.Este ejemplo utiliza el nombre de usuario y contraseña en blanco predeterminado:

🖆 Cisco ASDM-IDM La	uncher v1.5(50)	
🐴 Cisco A	cisco	
Device IP Address / Name:	172.22.1.163	_
Username:		
Password:		
🔄 Run in Demo Mode		
	OK Close	
	· v	1 🗊 불 🔂

5. Funcione con al Asistente VPN una vez que la aplicación ASDM conecta con el ASA.

🚰 Cisco ASDM 6.	3 for AS	A				
File View Tools	Wizards	Window Hel	p		_	
Home 🖧 Cor	Sta	artup Wizard			n 🕜 Back 🌔	🔪 Forward 🛛 🧿 Help
Device List	IPs	ec VPN Wizard	·			~ °
Add Delete	55	. VPN Wizard	5		Eirowall Dachb	voard
	Hiç	h Avai ability and	l Scalability Wiz	ard		
localhost:55	Un	ified Communicat	ion Wizard			
_	Pa	tket Capture Wiz	ard			
			Host Name: ASA Version: ASDM Version Firewall Mode Total Flash:	myFirew 8.3(1) n: 6.3(5) e: Routed 64 MB	al Device Uptime: Device Type: Context Mode: Total Memory:	0d 0h 30m 6s ASA 5520 Single 2048 MB

6. Elija el **sitio a localizar** para el tipo de túnel del IPSec VPN, y haga clic **después**.

ổ VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Promoti Promoti SP SP SP SP SP SP SP SP SP SP SP SP SP	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A cunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunne established by calls from remote users such as telecommitters is called remote access trippel. This wizard creates basic cunnel configurations that you can editrate using the ADDM.
Corporate Network	VPN Turmel Type: Site to Site VPN
THE END	
THUN IN	VEN Remote Access
	Remote Access
	VPN Tunnel Interhace: Outside 🗸
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and behaver a subscription access lists still apply to the traffic.
	< Back N∋xt ≻ Finish Cancel Help

7. Especifique el IP Address externo del peer remoto. Ingrese la información de autenticación para utilizar, que es la clave previamente compartida en este ejemplo:

🗯 VPN Wizard		\times
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Prametr Prametr Prametr Prametr Prametr	Configure the JH address of the peer device, authentication method and the cunnel group for this site to site tunnel. Feer TP Address: 10.20.20.	
	Authentication Metrod	
Corporate Network	Pre-Shared Key: Distol 23	
	🔿 Certificate	
-14	Certificate Signing Agorithm: Irsa-sig	
	Certificate Name:	
	Tunnel Group -or site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IF address or the peer hostname, whichever is used as the beer's identity.	
A	Tunnel Group Name: 10.20.20.1	
	Back Next > Finish Cancel Help]

8. Especifique los atributos para utilizar para el IKE, también conocido como fase 1. Estos atributos deben ser lo mismo a ambos lados del túnel.

🎼 VPN Wizard				8	K
VPN Wizard	IKE Policy	(5tep 3 of 6)			
Prand Prand ST ST Fish Fish Fish Fish Fish	Soloc: th Usvius them 10	he eneryption algorithm, auther to use to negotiate en I den et onfigurations on both sides of t	itication algorithm, and i . Key Exchange (IKE) se he connection must mat	Diffic Hollman group for the curity association between tohiexactly.	
Nerm		Encryptions	AES 256	*	
Corporate Network		Authenticet crit	SHA	*	
			< Back Next :	Finish Cancel Help	

9. Especifique los atributos para utilizar para el IPSec, también conocido como fase 2. Estos atributos deben hacer juego en los ambos lados.

🞼 VPN Wizard		×
VPN Wizard	IFsec Rule (Step 4 of 5)	
Pramdr Pramdr SP SP SP SP SP SP SP SP SP SP SP SP SP	Solect the eneryption and authentication algorithms and configure Ferfect Forwarding Socreey (PFS) for this IPSec VPN to met. Configurations on both sides of the connection must natch exactly.	
Notwork	Encryption: 🗛 ƏƏƏ	
	Authentication: SHA	
- Therefull	Enable Perfect Forwarding Secrety (PES)	
TT TT	Diffie-Helman Group; 1	

10. Especifique a los host cuyo tráfico se debe permitir pasar a través del túnel VPN. En este paso, usted tiene que proporcionar las redes locales y las redes remotas para el VPN hacen un túnel. Haga clic el botón al lado de las **redes locales** (como se muestra aquí) para elegir el direccionamiento de red local del menú desplegable:

🎼 VPN Wizard	
VPN Wizard	Hosts and Networks (Step 5 of 6)
Prametr	An IPsed tunnel protects data exchanged by solicated hosts and networks at the local and remote sites. Flease the Mifvill usus and networks to be used in the IPsed tunnel
	Network type: 💿 IPv4 🔿 JFv6
(armersta)	oral Networks
Network	Remote Networks:
	▼ Exempt ASA side rust/hetwork from address translator :
	< Back Next > Finish Cancel Help

11. Elija el direccionamiento de **red local**, y haga clic la **AUTORIZACIÓN**.

🖆 Browse Local Netwo	irks			X
🗣 Add 🔹 🕼 Edit 🕅	Delete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
-Network Objects				
- 🏈 any	0.0.0.0	0.0.0.0		
📲 dmz-network	10.77.241.64	255.255.255.192		
inside-network	172.22.1.0	255.255.255.0		
	172.16.1.0	255.255.255.0		
Selected Local Networks -				
Local Networks ->	any			
			С	Cancel

12. Haga clic el botón al lado de las **redes remotas** para elegir el direccionamiento de red remota del menú desplegable.

🎼 VPN Wizard	
VPN Wizard	Hosts and Networks (Step 5 of 6)
Prandt Brandt	An IPsee tunnel protects data exchanged by solected heats and networks at the local and remote sites. Flease the Mifvill usts and networks to be used in the (Pseultunnel
	Network type: 💿 IPv4 🔿 JFv6
(Corporate)	oral Networks Inside-networku2+
Network	Remote Networks:
	~5
	Exampl ASA side Tust/Letwork from address translations in the Very Very Very Very Very Very Very Ver
	< Back Next > Finish Cancel Help

13. Elija el direccionamiento de **red remota**, y haga clic la **AUTORIZACIÓN.Nota:** Si usted no tiene la red remota en la lista, después la red tiene que ser agregada a la lista. El tecleo **agrega** para hacer tan.

🖆 Browse Remote Net	works			X
🗣 Add 🝷 📝 Edit 🎁	Delete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	_
 Network Objects 				
any 🧼	0.0.0.0	0.0.0.0		
dmz-network	10.77.241.64	255.255.255.192		_
inside-network	172.22.1.0	255.255.255.0		
····· @ 1/2.16.1.0	172.16.1.0	233,235,235,0		
Selected Local Networks -				
Local Networks ->	any			
			OK.	Cancel

14. Marque el **host/la red exentos del lado ASA del** checkbox de la **traducción de la dirección** para evitar que el tráfico de túnel experimente la traducción de dirección de red. Haga clic en Next

(Siguiente).

🞼 VPN Wizard		×
VPN Wizard	Hasts and Networks (Step 5 of 6)	
Pramdt Brandt	An IPsed tunnel protects data exchanged by solected heats and networks at the local and remote sites. Flease, dentify hosts and networks to be used in the IPsed tunnel	
	Network type: 💿 IPv4 🔿 IFv6	
(armersta)	oral Networks Inside-networku24 -	
Network	Remote Networks: 172.18.1.0/24	
	5	
	Exampl ASA side instituet work from address translations; inside	1
	Reck Next > Finish Cancel Help	

15. Los atributos definidos por el Asistente VPN se visualizan en este resumen. Compruebe la configuración y el clic en Finalizar con minuciosidad cuando le satisfacen que las configuraciones están correctas.



Configuración de ASDM NTP

Complete estos pasos para configurar el NTP en el dispositivo del Cisco Security:

1. Elija la **configuración** en el Home Page del ASDM.

1	🚰 Cisco ASDM 6.3 for ASA - Demo mode				
File	View Tools Wizards Window Hel				
6	Hone 🥵 Configuration 🔯 Monitorin	🔚 Save 🔇 Refresh 🔇 Eack 🚫 Forward 🧖 H	elp		
Ъ	Device Setup □ ₽ ×	Configuration > Device Setup > System Time > NTP			
)evice Lis	Startup Wizard	Configure NTP servers and define authentication keys and valu	es.		
	Pevice Name/Password	IP Address Interface Preferred? Key Num	her		
	🖻 🮯 System Time				
		Enable NTP authentication			
	Device Setup				
	🗊 Firewall				

 Elija la configuración > el Tiempo del sistema > el NTP de dispositivo para abrir la página de la configuración del NTP del ASDM.

Configuration >	Device Setup	> System Time	> NTP		
Configure NTP ser	vers and define	authentication ke	ys and values.		
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add
					Edit
					Delete
]
🗌 Enable NTP au	thentication				

3. El tecleo **agrega** para agregar a un servidor NTP y proporcionar los atributos requeridos tales como nombre de la dirección IP, de la interfaz (interno o externo), número dominante, y valor de la clave para la autenticación en la nueva ventana que sube. Haga clic en

🚰 Add NTP Server	Configuration	×
IP Address:	172.22.1.161	Preferred
Interface:	inside 💌	
Authentication Key —		
Key Number:	1 🖌	🗸 Trusted
Key Value:	••••	
Re-enter Key Value:	•••••	
ОК	Cancel Hel	p

Nota: El nombre de la

interfaz se debe elegir como dentro para ASA1 y el exterior para ASA2.**Nota: Autenticación NTP el dominante** debe ser lo mismo en el ASA y el servidor NTP.La configuración del atributo de la autenticación en el CLI para ASA1 y ASA2 se muestran aquí: ASA1#ntp authentication-key 1 md5 cisco ntp trusted-key 1

ntp server 172.22.1.161 key 1 source inside

```
ASA2#ntp authentication-key 1 md5 cisco
ntp trusted-key 1
ntp server 172.22.1.161 key 1 source outside
```

4. Haga clic el **permiso del** checkbox **autenticación NTP** y el tecleo **se aplica**, que completa la tarea de la configuración del

	Incentace	Preferred?	Key Number	Trusted Key?	Add
72.22.1.161	inside	No	1	Yes	Edit
					Delot
					Delec
					1

Configuración CLI ASA1

ASA1
ASA#show run
: Saved
ASA Version 8.3(1)
!
hostname ASA1
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.10.10.1 255.255.255.0

- Configure the outside interface. ! interface Ethernet1 nameif inside security-level 100 ip address 172.22.1.163 255.255.255.0 !--- Configure the inside interface. ! !-- Output suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns servergroup DefaultDNS domain-name default.domain.invalid access-list inside_nat0_outbound extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---This access list (inside_nat0_outbound) is used !--with the **nat zero** command. This prevents traffic which !--- matches the access list from undergoing network address translation (NAT). !--- The traffic specified by this ACL is traffic that is to be encrypted and !--sent across the VPN tunnel. This ACL is intentionally !--- the same as (outside_cryptomap_20). !--- Two separate access lists should always be used in this configuration. access-list outside_cryptomap_20 extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !--- This access list (outside_cryptomap_20) is used !--- with the crypto map **outside_map** !--- to determine which traffic should be encrypted and sent !--- across the tunnel. !--- This ACL is intentionally the same as (inside_nat0_outbound). !--- Two separate access lists should always be used in this configuration. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image flash:/asdm-631.bin !--- Enter this command to specify the location of the ASDM image. asdm history enable arp timeout 14400 object network obj-local subnet 172.22.1.0 255.255.255.0 object network obj-remote subnet 172.16.1.0 255.255.255.0 nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote obj-remote !--- NAT 0 prevents NAT for networks specified in !--- the ACL inside_nat0_outbound. route outside 0.0.0.0 0.0.0.0 10.10.10.2 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable !--- Enter this command in order to enable the HTTPS server !--- for ASDM. http 172.22.1.1 255.255.255.255 inside !--- Identify the IP addresses from which the security appliance !--- accepts HTTPS connections. no snmp-server location no snmp-server contact !--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac !--- Define the transform set for Phase 2. crypto map outside_map 20

```
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
121 !--- In order to create and manage the database of
connection-specific !--- records for ipsec-121-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections,
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.
tunnel-group 10.20.20.1 ipsec-attributes
pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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
!--- Define the NTP server authentication-key, Trusted-
key !--- and the NTP server address for configuring NTP.
ntp authentication-key 1 md5 *
ntp trusted-key 1
!--- The NTP server source is to be mentioned as inside
for ASA1 ntp server 172.22.1.161 key 1 source inside
Cryptochecksum:ce7210254f4a0bd263a9072a4ccb7cf7
: end
```

Este vídeo fijado a la <u>comunidad del soporte de Cisco</u> explica con una versión parcial de programa, el procedimiento para configurar el ASA como cliente NTP:

<u>Cómo configurar un dispositivo de seguridad adaptante de Cisco (ASA) para sincronizar su reloj</u> <u>con un servidor del Network Time Protocol (NTP).</u>



Configuración CLI ASA2

```
ASA2
ASA Version 8.3(1)
1
hostname ASA2
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
1
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name default.domain.invalid
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on ASA1.
access-list outside_cryptomap_20 extended permit ip
172.16.1.0 255.255.255.0 172
```

.22.1.0 255.255.255.0 !--- Note that this ACL is a mirror of the outside_cryptomap_20 !--- ACL on ASA1. pager lines 24 mtu inside 1500 mtu outside 1500 no failover asdm image flash:/asdm-631.bin no asdm history enable arp timeout 14400 object network obj-local subnet 172.22.1.0 255.255.255.0 object network obj-remote subnet 172.16.1.0 255.255.255.0 nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote obj-remote 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 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac crypto map outside_map 20 match address outside_cryptomap_20 crypto map outside_map 20 set peer 10.10.10.1 crypto map outside_map 20 set transform-set ESP-AES-256-SHA crypto map outside_map interface outside isakmp enable outside isakmp policy 10 authentication pre-share isakmp policy 10 encryption aes-256 isakmp policy 10 hash sha isakmp policy 10 group 5 isakmp policy 10 lifetime 86400 tunnel-group 10.10.10.1 type ipsec-121 tunnel-group 10.10.10.1 ipsec-attributes pre-shared-key * telnet timeout 5 ssh timeout 5 console timeout 0 1 class-map inspection_default match default-inspection-traffic 1 policy-map global_policy class inspection_default inspect dns maximum-length 512 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
!--- Define the NTP server authentication-key, Trusted-
key !--- and the NTP server address for configuring NTP.
ntp authentication-key 1 md5 *
ntp trusted-key 1
!--- The NTP server source is to be mentioned as outside
for ASA2. ntp server 172.22.1.161 key 1 source outside
Cryptochecksum:d5e2ee898f5e8bd28e6f027aeed7f41b
: end
ASA#
```

Verificación

Esta sección proporciona la información que usted puede utilizar para confirmar que su configuración trabaja correctamente.

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

```
• <u>muestre a se muestra el estados NTP la</u> información del reloj NTP.
ASA1#show ntp status
```

Clock is synchronized, stratum 2, reference is 172.22.1.161 nominal freq is 99.9984 Hz, actual freq is 99.9983 Hz, precision is 2**6 reference time is ccf22b77.f7a6e7b6 (13:28:23.967 UTC Tue Dec 16 2008) clock offset is 34.8049 msec, root delay is 4.78 msec root dispersion is 60.23 msec, peer dispersion is 25.41 msec

```
    <u>show ntp associations detail</u> - Visualiza las asociaciones del Servidor de tiempo de la red
configurada.
```

```
ASA1#show ntp associations detail
```

```
172.22.1.161 configured, authenticated, our_master, sane, valid, stratum 1
ref ID .LOCL., time ccf2287d.3668b946 (13:15:41.212 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 7, sync dist 23.087
delay 4.52 msec, offset 9.7649 msec, dispersion 20.80
precision 2**19, version 3
org time ccf22896.fla4fca3 (13:16:06.943 UTC Tue Dec 16 2008)
rcv time ccf22896.efb94b28 (13:16:06.936 UTC Tue Dec 16 2008)
xmt time ccf22896.ee5691dc (13:16:06.931 UTC Tue Dec 16 2008)
filtdelay = 4.52 4.68 4.61 0.00 0.00 0.00 0.00 0.00
filtoffset = 9.76 7.09 3.85 0.00 0.00 0.00 0.00
filterror = 15.63 16.60 17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

Comandos para resolución de problemas

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

Nota: <u>Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.</u>

 haga el debug de la validez NTP - Validez del reloj del par de las visualizaciones NTP.Ésta es salida de los debugs de la discrepancia de clave:

```
NTP: packet from 172.22.1.161 failed validity tests 10
Authentication failed
```

• paquete NTP del debug - Información del paquete NTP de las visualizaciones.Cuando no hay respuesta del servidor, sólo paquete xmit NTP se ve en el ASA sin el paquete rov NTP.

```
ASA1# NTP: xmit packet to 172.22.1.161:

leap 0, mode 3, version 3, stratum 2, ppoll 64

rtdel 012b (4.562), rtdsp 0cb6 (49.652), refid ac1601a1 (172.22.1.161)

ref ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)

org ccf22916.f426232d (13:18:14.953 UTC Tue Dec 16 2008)

rec ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008)

xmt ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)

NTP: rcv packet from 172.22.1.161 to 172.22.1.163 on inside:

leap 0, mode 4, version 3, stratum 1, ppoll 64

rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 4c4f434c (76.79.67.76)

ref ccf2293d.366a4808 (13:18:53.212 UTC Tue Dec 16 2008)

org ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008)

rec ccf22956.f52e480e (13:19:18.957 UTC Tue Dec 16 2008)

xmt ccf22956.f5688c29 (13:19:18.958 UTC Tue Dec 16 2008)

inp ccf22956.f982bcd9 (13:19:18.974 UTC Tue Dec 16 2008)
```

Información Relacionada

- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Solicitudes de Comentarios (RFC)</u>
- Soporte Técnico y Documentación Cisco Systems