ASA 8.3 e versioni successive: Esempio di configurazione di NTP con e senza tunnel IPsec

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazione ASDM tunnel VPN Configurazione ASDM NTP Configurazione CLI di ASA1 Configurazione ASA2 CLI Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per sincronizzare l'orologio di Adaptive Security Appliance (ASA) con un Network Time Server che utilizza il protocollo NTP (Network Time Protocol). ASA1 comunica direttamente con il network time server. ASA2 passa il traffico NTP attraverso un tunnel IPsec a ASA1, che a sua volta inoltra i pacchetti al server di riferimento orario della rete.

Per ulteriori informazioni, fare riferimento al documento <u>ASA/PIX: NTP con e senza tunnel IPsec</u> <u>Esempio</u> di configurazione identica su Cisco ASA con versioni 8.2 e precedenti.

Nota: un router può essere usato anche come server NTP per sincronizzare l'orologio dell'appliance di sicurezza ASA.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA con versione 8.3 e successive
- Cisco Adaptive Security Device Manager (ASDM) versione 6.x e successive

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Configurazione

Esempio di rete



Nel documento viene usata questa impostazione di rete:

Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi <u>RFC 1918</u> utilizzati in un ambiente lab.

- <u>Configurazione ASDM tunnel VPN</u>
- <u>Configurazione ASDM NTP</u>
- <u>Configurazione CLI di ASA1</u>
- <u>Configurazione ASA2 CLI</u>

Configurazione ASDM tunnel VPN

Per creare il tunnel VPN, completare i seguenti passaggi:

 Aprire il browser e digitare https://<Inside_IP_Address_of_ASA> per accedere alle funzionalità ASDM sull'appliance ASA.Assicurarsi di autorizzare tutti gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione

ASDM.



In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet Java.

- 2. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
- 3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
- 4. Immettere l'indirizzo IP dell'interfaccia configurata con il comando **http -**, nonché un nome utente e una password, se specificati.In questo esempio vengono utilizzati il nome utente e la password vuoti

🕵 Cisco ASDM-IDM La	uncher v1.5(50)	
🖺 Cisco A	SDM-IDM Launcher	cisco
Device IP Address / Name:	172.22.1.163	*
Username:		
Password:		
🔲 Run in Demo Mode		
	OK Close	
	· v	📋 불

predefiniti:

5. Eseguire la VPN Wizard una volta che l'applicazione ASDM si connette all'appliance ASA.

🚰 Cisco ASDM 6.	3 for AS	A				
File View Tools	Wizards	Window Hel	p		_	
Home 🖧 Cor	Sta	rtup Wizard			n 🔇 Back 🕥	Forward 🦻 🍘 Help
Device List	IPs	ec VPN Wizard				
Add Delete	SSL Higi Unil Pac	. VPN Wizard h Avaiability and fied Communicat ket Capture Wiz	N Scalability Wizar ion Wizard ard	d	Firewall Dashboar	d
			Host Name: ASA Version: ASDM Version: Firewall Mode: Total Flash:	myFirew 8.3(1) 6.3(5) Routed 64 MB	all Device Uptime: Od Device Type: A9 Context Mode: Sir Total Memory: 20	l 0h 30m 6s 5A 5520 ngle 148 MB

6. Scegliere **Da sito a sito** per il tipo di tunnel VPN IPsec e fare clic su **Avanti**.

ổ VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Prameter Prameter Promoter Promoter	Use this woard to configure new site-to-site VPN tunnels or new remote access VPN tunnes. A sunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunne established by calls from remote users such as teleforminitiers is called remote access trinnel. This wizerd creates basic sunnel configurations that you can editrate rusho the ACOM.
Corporate	VPN Tunnel Type: Site to Site VPN
2 Julion	VEN Remote Access
TH	O Remote Access
	VPN Tunnel Interhace: Outside 🗸
	Enable inbound (Psec sessions to bypass interface access lists, Group policy and per-user at the rization access lists still apply to the traffic.
	Back Next > Finish Cancel Felp

7. Specificare l'indirizzo IP esterno del peer remoto. Immettere le informazioni di autenticazione da utilizzare, ovvero la chiave già condivisa in questo esempio:

🗯 VPN Wizard		×
VPN Wizard	Remote Site Peer (Step 2 of 6)	
Prametr Prametr Prametr Prametr Prametr Prametr	Configure the JF address of the peer device, authentication method and the cunnel group for this site to site tunnel. Feer TP Address: 10.20.20.	
Home	Pro shared key	
CorporatB Network	Pre-Shared Key: Discol 23	
artita In	🔿 Certificate	
the second	Certificate Signing Algorithm: Irsa-sig	
	Oertificate Name:	J
111	Funnel 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, which ever is used as the open's identity.	
A	Tunnel Group Varre: 10.20.20.1	
	< Back Next > Finish Cancel Help	2

8. Specificare gli attributi da utilizzare per IKE, noti anche come Fase 1. Questi attributi devono essere gli stessi su entrambi i lati del tunnel.

🖆 VPN Wizard					\times
VPN Wizard	IKE Policy	(Step 3 of 6)			
Pramdr Pramdr Fist Formorata Corporata	Soloc: the Usvilues to them "Lon	chervption algorithm, auther use to negotiate en I nen et figurations on both sides of t	tication algorithm, and Key Exchange (IKE) se he connection must ma	Diffic Hollman group for the curity association between tohiexactly.	
Nati		Encryption:	AES 256	₩	
1 Alter		Authenticet on:	SHA	~	
51444		D F ^a is-Helman Group	5		
			< Back Next	> Finish Cancel Help	

9. Specificare gli attributi da utilizzare per IPSec, noti anche come Fase 2. Questi attributi devono corrispondere su entrambi i lati.

🞼 VPN Wizard		×
VPN Wizard	IFsec Rule (Step 4 of 6)	
Prand Prand First First Home	Select the eneryption and authentication algorithms and cenfigure Ferfect Forwarding Secrecy (PFS) for this (PSec VPN to mell. Configurations on both sides of the connection must match exactly.	
Notwork	Encryption: 😽 🗛 🐼	
	Authenticetion: SHA 🐱	
- THE	Enable Perfect Forwarding Secrety (PES)	
TT TT	Diffie-Helman Group; 1	
	Back Next > Finish Cancel Help Ca	

10. Specificare gli host il cui traffico deve poter passare attraverso il tunnel VPN. In questo passaggio, sarà necessario fornire le reti locali e remote per il tunnel VPN. Fare clic sul pulsante accanto a **Reti locali** (come mostrato di seguito) per scegliere l'indirizzo di rete locale dal menu a discesa:

🎼 VPN Wizard	
VPN Wizard	Hasts and Networks (Step 5 of 6)
Prametr Provide	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
(Corporate)	oral Networks
Notwork	Remote Networks:
	Evenue ASà side un là element in un elèbres, ce s el uni
	Reck Next > Finish Cancel Help

11. Scegliere l'indirizzo di **rete locale** e fare clic su **OK**.

🖆 Browse Local Netw	orks			
🗣 Add 👻 🖪 Edit 🇊	Delete Q			
Filter:				Filter Clear
Name	1 IP Address	Netmask	Description	
-Network Objects				
- 🏈 any	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			
Local Notifolds ->	Jany			
			0	Cancel
				NE

12. Fare clic sul pulsante accanto a **Reti remote** per scegliere l'indirizzo di rete remoto dal menu a

discesa.

🎼 VPN Wizard		<
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Prandt	An IPsed tunnel protects data exchanged by solicated hosts and not verks at the local and remote sites. Flease, dentify hosts and networks to be used in the (Pseu tunnel	
	Network type: 💿 IPv4 🔿 IFv6	
(arroutata)	oral Networks Inside-network/24	
Network	Remote Networks:	
	ج Exempt ASA side ust/ietwork "rum address trans dur ;) آنه de	
	Rack Next > Finish Cancel Help	

13. Scegliere l'indirizzo di **rete remota** e fare clic su **OK.Nota:** se la rete remota non è presente nell'elenco, è necessario aggiungerla all'elenco. A tale scopo, fare clic su **Add** (Aggiungi).

🖆 Browse Remote Netv	works			X
🗣 Add 👻 🎯 Edit 👔 I	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		
nside-network	172.22.1.0	255.255.255.0		
172.16.1.0	172.16.1.0	255.255.255.0		
Selected Local Networks —				
Local Networks ->	any			
				Cancel

 Per evitare che il traffico del tunnel venga convertito tramite Network Address Translation, selezionare la casella di controllo Esenzione host/rete lato ASA dalla conversione degli indirizzi. Fare clic su Next (Avanti).

📧 VPN Wizard			
VPN Wizard	Hosts and Networks (Step 5 of 6)		
erametr Electronic SP	An IPsec tunnel protects data exchanged by remote sites. Flease dentify hosts and netw	y spected hosts and networks at the local and forks to be used in the (Pseu tunnel	
	Metwork type: 💿 IPv4 🛛 🔿 IPv6		
T mm	oral Networks Inside-networku24	-	
Network	Remote Networks: 172.16.1.0/24		
	▼ Exampl ASA side ust/retwork "rom ad	utess ratectu ; iede	v
		<pre>< Back Next > Frish Cancel</pre>	⊢elp

 In questo riepilogo vengono visualizzati gli attributi definiti dalla Creazione guidata VPN. Verificare la configurazione e fare clic su **Finish** (Fine) dopo aver verificato la correttezza delle

impostazioni.



Configurazione ASDM NTP

Per configurare l'NTP su Cisco Security Appliance, completare i seguenti passaggi:

1. Scegliere **Configurazione** nella home page di 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				

2. Scegliere **Device Setup > System Time > NTP** per aprire la pagina di configurazione **NTP** di ASDM.

Configuration >	• Device Setup ervers and define	> System Time authentication ke	e > <u>NTP</u> eys and values.		
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add
					Edit
					Delete
🔄 Enable NTP a	uthentication				

3. Fare clic su **Add** (Aggiungi) per aggiungere un server NTP e fornire gli attributi richiesti, ad esempio indirizzo IP, nome interfaccia (interna o esterna), numero chiave e valore chiave per Authentication (Autenticazione), nella nuova finestra che viene visualizzata. Fare clic su

🖆 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 H	lelp			

dell'interfaccia deve essere scelto tra ASA1 e ASA2.**Nota:** la **chiave di autenticazione ntp** deve essere la stessa nell'ASA e nel server NTP.Di seguito è riportata la configurazione degli attributi di autenticazione nella CLI per ASA1 e ASA2: 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. Fare clic sulla casella di controllo **Abilita autenticazione NTP** e fare clic su **Applica** per completare il task di configurazione

TP.	Desite Cale				
Configuration >	Device Setup	<u>> System Tim</u>	<u>ie > NTP</u>		
Configure NTP se	ervers and define	authentication k	eys and values.		
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add
172.22.1.161	inside	No	1	Yes	Edit
					Delete
]
Enable NTP a	uthentication				
			-		
			0	Apply	Reset
			L		

Configurazione CLI di 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
```

Questo video pubblicato nella <u>Cisco Support Community</u> spiega, con una demo, la procedura per configurare l'ASA come client NTP:

<u>Come configurare un'appliance Cisco Adaptive Security (ASA) in modo che sincronizzi il proprio orologio con un server NTP (Network Time Protocol).</u>



Configurazione ASA2 CLI

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#
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi show sono supportati dallo strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

• <u>show ntp status</u>: visualizza le informazioni sull'orologio 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 association [detail]</u> - Visualizza le associazioni del server di riferimento orario di rete configurate.

```
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.f1a4fca3 (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
              9.76 7.09
filtoffset =
                             3.85 0.00 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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla

configurazione.

rcv.

Comandi per la risoluzione dei problemi

Alcuni comandi show sono supportati dallo <u>strumento Output Interpreter (solo utenti</u> <u>registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> show.

Nota: prima di usare i comandi di **debug**, consultare le <u>informazioni importanti sui comandi di</u> <u>debug</u>.

 debug ntp valid: visualizza la validità dell'orologio peer NTP.Questo è l'output del comando debug per la mancata corrispondenza della chiave:

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

 debug ntp packet: visualizza le informazioni sul pacchetto NTP. In assenza di risposta dal server, solo il pacchetto NTP xmit viene visualizzato sull'appliance ASA senza pacchetto 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 ccf22936.f08ee8b4 (13:19:18.939 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)
```

Informazioni correlate

- <u>Cisco Adaptive Security Device Manager</u>
- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems