# ASA 8.3 en later: NTP met en zonder een IPsectunnelconfiguratievoorbeeld

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configuratie Netwerkdiagram VPN-tunnelconfiguratie ASDM NTP ASDM-configuratie ASA1 CLI-configuratie ASA2 CLI-configuratie Verifiëren Problemen oplossen Opdrachten voor probleemoplossing Gerelateerde informatie

# **Inleiding**

Dit document biedt een voorbeeldconfiguratie voor het synchroniseren van de adaptieve security applicatie (ASA) kloktijd met een netwerktijdserver via Network Time Protocol (NTP). ASA1 communiceert direct met de netwerktijdserver. ASA2 geeft NTP-verkeer door een IPsec-tunnel door aan ASA1, die op zijn beurt de pakketten naar de netwerktijdserver doorgeeft.

Raadpleeg <u>ASA/PIX: NTP met en zonder een IPsec Tunnel Configuration Voorbeeld</u> voor een identieke configuratie op Cisco ASA met versies 8.2 en eerder.

**Opmerking:** Een router kan ook als NTP-server worden gebruikt voor het synchroniseren van de ASA Security Appliance-kloktijd.

# Voorwaarden

#### **Vereisten**

Er zijn geen specifieke vereisten van toepassing op dit document.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA met versie 8.3 en hoger
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.x en hoger

**Opmerking:** Raadpleeg <u>HTTPS-toegang voor ASDM</u> om de ASA te kunnen configureren door de ASDM.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

#### **Conventies**

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

# **Configuratie**

#### **Netwerkdiagram**

Het netwerk in dit document is als volgt opgebouwd:



**Opmerking:** de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn <u>RFC 1918</u> adressen, die in een labomgeving gebruikt zijn.

- VPN-tunnelconfiguratie ASDM
- <u>NTP ASDM-configuratie</u>
- ASA1 CLI-configuratie
- ASA2 CLI-configuratie

#### VPN-tunnelconfiguratie ASDM

Voltooi deze stappen om de VPN-tunnel te maken:

 Open uw browser en type https://<Inside\_IP\_Address\_of\_ASA>om toegang te krijgen tot de ASDM in de ASA.Vergeet niet alle waarschuwingen goed te keuren die uw browser u geeft met betrekking tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De ASA presenteert dit venster om het downloaden van de ASDM-toepassing mogelijk te

maken.



Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-applet.

- 2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDMtoepassing te downloaden.
- 3. Voltooi na het downloaden van de ASDM Launcher de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
- 4. Voer het IP-adres in voor de interface die u met de http opdracht en een gebruikersnaam en wachtwoord hebt ingesteld als u er een hebt opgegeven.Dit voorbeeld gebruikt de standaard lege gebruikersnaam en het wachtwoord:

🚰 Cisco ASDM-IDM Launcher v1.5(50)	
🐴 Cisco ASDM-IDM	Launcher 'lindu
Device IP Address / Name: 172.22.1.163	<b>•</b>
Username:	
Password:	
🜅 Run in Demo Mode	
	lose
	💼 🖕 🔒

5. Start de VPN-wizard zodra de ASDM-toepassing op de ASA-band is aangesloten.

🚰 Cisco ASDM 6.	3 for a	ASA						
File View Tools	Wizar	ds Windov	v Hel	P				
Home 🖧 Cor		Startup Wiza	rtup Wizard		n 🔇 Back 🌔	🔪 Forward 🛛 🦻 Help		
Device List		IPsec VPN W	'izard					~ °
Add 🗊 Delete		SSL VPN Wiz	ard	51			Firewall Dashh	oard
172.22.1.163		High Avaiab	ility and	d Scalability	Wizar	d		
localhost:55		Unified Com	ified Communication Wizard					
		Packet Capti	ket Capture Wizard					
				Host Nan ASA Vers ASDM Ve Firewall N Total Fla:	ne: ion: rsion: 1ode: sh:	myFirewa 8.3(1) 6.3(5) Routed 64 MB	al Device Uptime: Device Type: Context Mode: Total Memory:	0d 0h 30m 6s ASA 5520 Single 2048 MB

6. Kies Site-to-Site voor het tunneltype IPsec VPN en klik op Volgende.

ổ VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Prametr Prametr Prametr Prametr Prametr	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	VPN Tunnel Type: Site to Site VPN
THE REAL	⊙ <u>Site-to-Site</u>
	Remote Access     Remote Access     Remote Access
	VPN Tunnel Interhace: Outside 🗸
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and behauser automization access ists still apply to the traffic.
	Back Next > Finish Cancel Help

7. Specificeer het externe IP-adres van de externe peer. Voer de te gebruiken authenticatieinformatie in, de vooraf gedeelde toets in dit voorbeeld:

🗯 VPN Wizard		$\times$
VPN Wizard	Remote Site Peer (Step 2 of 6)	
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: 10.20.21.	
	Authentication Met rod     O Pro shared key	
Corporate Network	Pre-Shared Key: Distol 23	
	🔘 Certificate	
J. J.	Lertificate Signing Agorithm: Irsa-sig	
	Certificate Name:	
	Tunnel Group For site-to-site connections with pre-shared key authentication, the tunnel group name must	
TTTT	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. Specificeer de eigenschappen die voor IKE moeten worden gebruikt, ook bekend als fase 1. Deze eigenschappen moeten aan beide zijden van de tunnel gelijk zijn.

🖆 VPN Wizard				
VPN Wizard	IKE Policy	(Step 3 of 6)		
Prandt Prandt Fist Fist Fist Corporat8	Soloc: ti Usviuss them 11	he eneryption algorithm, author Loluse to negotiate B i I nerr et onfigurations on both sides of t	ntication algorithm, and Diffiel He Likey Exchange (IKE) Security as the connection must match exac	Ilman group for the sociation between tly.
Nation		Encryptions	AES 256 😽	
		Authenticet on : Diffie-Helman Group	SHA 🗸	
			< Back Next > Fin	ish Cancel Help

 Specificeer de eigenschappen die voor IPsec moeten worden gebruikt, ook bekend als fase
 Deze eigenschappen moeten aan beide kanten overeenkomen.

🖆 VPN Wizard		×
VPN Wizard	IFsec Rule (Step 4 of 6)	
Prandt Prandt ISP Frandt Frandt	Select the eneryption and authentication algorithms and configure Ferfect Forwarding Secrecy (PFS) for this (PSec YPN to mell. Configurations on both sides of the connection must match exactly.	
Notwork	Encryption: 🛛 🗛 🕹	
	Authenticet cn: SHA 🐱	
-T-HU	Enable Perfect Forwarding Secrety (PES)	
TIT	Diffie-Helman Group; 1	
	Back Next > Finish Cancel Help     Ca	

10. Specificeer de hosts waarvan het verkeer door de VPN-tunnel moet kunnen passeren. In deze stap moet u de lokale netwerken en Remote-netwerken voor de VPN-tunnelleiding bieden. Klik op de knop naast **Local Networks** (zoals hier getoond) om het lokale netwerkadres in het vervolgkeuzemenu te kiezen:

🞼 VPN Wizard	<u> </u>
VPN Wizard	Hasts and Networks (Step 5 of 6)
Prandt 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 🔿 IFvG
aunorate )	ocal Networks
Network	Remote Networks:
	Exempt ASA side rust/hetwork from address translator :
	Back Next > Finish Cancel Help

11. Kies het lokale netwerkadres en klik op OK.

🖆 Browse Local Netwo	orks			
🗣 Add 🔹 🕼 Edit 🗊	Delete O			
Filter:	00000			Filter Clear
Name ^	<sup>1</sup> 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			
				K Cancel

12. Klik op de knop naast **Remote Networks** om het externe netwerkadres in het vervolgkeuzemenu te kiezen.

🎼 VPN Wizard	
VPN Wizard	Hosts and Networks (Step 5 of 6)
Prands	An IPsee tunnel protects data exchanged by speeted hosts and networks at the local and remote sites. Flease, dentify hosts and networks to be used in the IPseu tunnel
	Network type: 💿 IPv4 🔿 IFv6
(avrigorata)	oral Networks Inside-networku24
Network	Remote Networks:
	ج Exempt ASA side usi/network "run address rais at un"
	Back Naxt > Finish Cancel Help

13. Kies het Remote Network-adres en klik op OK.N.B.: Als u het Remote Network niet in de lijst hebt staan, moet het netwerk aan de lijst worden toegevoegd. Klik op Toevoegen om dit te

doen.

🖆 Browse Remote Net	works			
🗣 Add 👻 📝 Edit 🏛	Delete Q			
Filter:	C C			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		
通 172.16.1.0	172.16.1.0	255.255.255.0		
Selected Local Networks -				
Local Networks ->	any			
			OK	

14. Controleer de **vrijstellingsASA side host/network van adresomzetting** selectieteken om te voorkomen dat het tunnelverkeer doorgaat met netwerkadresomzetting. Klik op **Volgende**.

📧 VPN Wizard		
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Brandt Brandt	An IPsec tunnel protects data exchanged by spected hosts and not verks at the local and remote sites. Flease, dentify hosts and networks to be used in the (Psec tunnel)	
	Network type; 💿 IPv4 🔹 🔿 IFv6	
THE	ocal Networks Inside-networku2+	
Network	Remote Networks: 172.18.1.0/24	
	ج Example ASA side iust/retwork from address trace at or 3 inde	~
		Lolo
		Feip

15. De eigenschappen die door de VPN Wizard worden gedefinieerd, worden in deze samenvatting weergegeven. Controleer de configuratie en klik op **Voltooien** wanneer u ervan overtuigd bent dat de instellingen juist

VPN Wizard	Summary (Step 6 of 6)
	You have created a Site-to-Site VPN tunnel with the following attributes: VPN Tunnel Interface: outside Peer IP Address: 10.20.20.1 Tunnel Group Name: 10.20.20.1 IPSec authentication uses pre-shared key: clsco123 IRE Policy Encryption / Authentication / DHGroup: AES-256 / SHA / Group 5 IPSec ESP Encryption / ESP Authentication: AES-256 / SHA / Group 5 IPSec ESP Encryption / ESP Authentication: AES-256 / SHA / Group 5 IPSec ESP Encryption / ESP Authentication: AES-256 / SHA / Group 5 IPSec (ocal) 172.22.1.0/24 (remote) 172.16.1.0/24
	≪ Back Next > Finish Cancel Help

### NTP ASDM-configuratie

Voltooi deze stappen om NTP op Cisco security applicatie te configureren:

1. Kies Configuration in de ASDM-

Ş	startp	bagina.					
	📬 C	isco ASDM 6.3 for ASA - Demo mod	e				
	File	View Tools Wizards Window Hel	)				
	Ó	Hone 🖧 Configuration 🔯 Monitorin	1   (	릚 Save 🔇 R	efresh 🔇 🔾 E	ack 🕐 Forwa	rd 🧖 Help
	e List	Device Setup 고 무 ×		Configuration > D	<b>Device Setup</b> : vers and define :	> System Time	E > NTP ws and values.
	Device						
		Device Name/Password		TP Address	Interface	Preferred?	Key Number
		Clock					
			ľ		L V L'		
				Enable MTP aut	nentication		
		👫 Firewall					

2. Kies Apparaatinstelling > Systeemtijd > NTP om de NTP-configuratiepagina van ASDM te openen.

onfigure NTP se	ervers and define	authentication ke	ys and values.		
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add
					Edit
					Delete
					]
Enable NTP a	uthentication				

3. Klik op Add om een NTP-server toe te voegen en de vereiste eigenschappen te geven zoals IP-adres, interfacenaam (binnen of buiten), sleutelnummer en trefwaarde voor verificatie in het nieuwe venster dat verschijnt. Klik op

🚰 Add NTP Server	Configuration 🛛 🛛 🔀
IP Address:	172.22.1.161 Preferred
Interface:	inside 💌
Authentication Key —	
Key Number:	1 V Trusted
Key Value:	••••
Re-enter Key Value:	••••
ОК	Cancel Help

Opmerking: De

interfacenaam dient voor ASA1 en daarbuiten voor ASA2 te worden gekozen.**Opmerking:** de **NTP-verificatiesleutel** dient dezelfde te zijn in ASA en de NTP-server.De configuratie van de verificatieeigenschap in de CLI voor ASA1 en ASA2 wordt hier weergegeven: 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 cis	SCO
ntp	trust	ed-key 1				
ntp	serve	r 172.22.1.161	key	1	source	outside

4. Klik op het selectieknop **NTP-verificatie inschakelen** en klik op **Toepassen**, waarmee de NTP-configuratietaak wordt

oltooid.	Device Colum	. Custom Tim				
onfiguration :	» Device Setup	<u>&gt; System Tim</u>	e > <u>NIP</u>			
Configure NTP servers and define authentication keys and values.						
	7.1	De Caralin		Tauta Irano		
IP Address	Interface	Preferred?	Key Number	Trusted Key?	Add	
172.22.1.161	inside	No	1	Yes	Edit	
					Delete	
🔽 Enable NTP a	authentication					
			F			

### ASA1 CLI-configuratie

ASA 1
ASA# <b>show run</b>
: 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
```

Deze video die in de <u>Cisco Support Community</u> is gepost legt met een demo uit de procedure om ASA als NTP-client te configureren:

Hoe u een Cisco adaptieve security applicatie (ASA) kunt configureren om de klok te synchroniseren met een Network Time Protocol (NTP) server.



#### ASA2 CLI-configuratie

```
ASA 2
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#
```

## **Verifiëren**

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** <u>Output Interpreter (alleen voor</u> <u>geregistreerde klanten)</u>. Hiermee kunt u een analyse van de output van opdrachten met **show genereren**.

• <u>NTP-status tonen</u> - Hier wordt de NTP-klokinformatie weergegeven. 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

    toon ntp associaties [detail] - Hier worden de geconfigureerde netwerktijdserverassociaties

 weergegeven.
 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
 filtoffset = 9.76 7.09 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
```

### Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

#### Opdrachten voor probleemoplossing

Bepaalde opdrachten met **show worden ondersteund door de tool** <u>Output Interpreter (alleen voor</u> <u>geregistreerde klanten)</u>. <u>Hiermee kunt u een analyse van de output van opdrachten met</u> **show genereren**.

**Opmerking:** Voordat u **debug-**opdrachten afgeeft, raadpleegt u <u>Belangrijke informatie over Debug</u> <u>Commands</u>.

 debug ntp validatie - Hiermee geeft u de geldigheid van NTP-peer klokwaarden weer.Dit is een debug van uitvoer uit een belangrijk verschil:

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

• debug ntp pakket - Hiermee geeft u NTP-pakketinformatie weer.Wanneer er geen respons is van de server, wordt alleen het NTP-uitgiftepakket gezien op de ASA zonder NTP rcv-pakket. 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.f1211384 (13:18:14.941 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)
```

### **Gerelateerde informatie**

- <u>Cisco adaptieve security apparaatbeheer</u>
- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie Cisco Systems