ASA pakketvastlegging met CLI en ASDM configureren

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram Configuraties Packet Capture configureren met de ASDM Packet Capture configureren met de CLI Beschikbare opnametypen op de ASA Standaard Bekijk de opgenomen pakketten Op de ASA Downloaden van de ASA voor offline analyse **Opname wissen** Een opname stoppen Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u de Cisco ASA firewall moet configureren om de gewenste pakketten met de ASDM of de CLI op te nemen.

Voorwaarden

Vereisten

Bij deze procedure wordt ervan uitgegaan dat de ASA volledig operationeel is en zodanig is geconfigureerd dat Cisco ASDM of de CLI configuratiewijzigingen kunnen doorvoeren.

Gebruikte componenten

Dit document is niet beperkt tot specifieke hardware- of softwareversies.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Deze configuratie wordt ook gebruikt met deze Cisco-producten:

- Cisco ASA versies 9.1(5) en hoger
- Cisco ASDM versie 7.2.1

Achtergrondinformatie

Dit document beschrijft hoe de Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall OM de gewenste pakketten op te nemen met Cisco Adaptive Security Device Manager (ASDM) of de Command Line Interface (CLI) (ASDM).

Het pakketopnameproces is handig om connectiviteitsproblemen op te lossen of verdachte activiteit te bewaken. Daarnaast is het mogelijk om meerdere opnamen te maken om verschillende soorten verkeer op meerdere interfaces te analyseren.

Configureren

Deze sectie verschaft informatie die wordt gebruikt om de pakketopnamefuncties te configureren die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

De IP-adresschema's die in deze configuratie worden gebruikt, zijn juridisch niet routeerbaar op internet. Het zijn RFC 1918-adressen die in een laboratoriumomgeving worden gebruikt.

Packet Capture configureren met de ASDM

Deze voorbeeldconfiguratie wordt gebruikt om de pakketten op te nemen die tijdens een ping worden verzonden van Gebruiker1 (binnen netwerk) naar Router1 (buiten netwerk).

Voltooi deze stappen om de pakketopnamefunctie op de ASA te configureren met de ASDM:

1. Navigeer naar Wizards > Packet Capture Wizard om de configuratie voor pakketopname te starten,

zoals wordt getoond:

Cisco ASUM 7/2 for ASA = 10.106.44.185									
File	File View Tools Wizards Window Help								
🝙 Device List	Home Conf Home Device Infor General Lic	Startup Wizard VPN Wizards High Availability and Scalability Wizard. Unified Communication Wizard Packet Capture Wizard ense	Back Forward ? Help						
	Host Name: ASA.cisco.com								
	ASA Version: 9.1(5)2		Device Uptime: 61d 14h 36m 54s						
	ASOM Version	an: 7.2(1)	Device Type: ASA 5520, SSH-CSC-20-K9						
	Freval Mode: Routed Total Flash: 256 HB		Context Mode: Single						
			Total Memory: 2048 MB						

2. De Capture Wizard wordt geopend. Klik Next.

Capture Wizard							
Packet Capture Wizard	Overview of Packet Capture (Step 1 of 6)						
Q. Pla	Use this wizard to configure and run capture. The wizard will run one capture on each of the ingress and egress interfaces. After capturing you can save the captures to your PC for examination or replay in a packet analyzer. The wizard will guide you through the following tasks:						
	Select an ingress interface. Select an egress interface. Set the buffer parameters. Run the captures. Save the captures to your PC (optional).						
	<back next=""> Finish Cancel Help</back>						

3.0 Geef in het nieuwe venster de parameters op die worden gebruikt om het toegangsverkeer op te nemen.

3.1 Selecteer inside voor de Ingress Interface en de bron en de IP-doeladressen van de pakketten die moeten worden opgenomen, samen met hun subnetmasker, in de respectieve ruimte te verstrekken.

3.2 Kies het pakkettype dat door de ASA moet worden opgenomen (IP is het hier gekozen pakkettype), zoals getoond:

Capture Wizard				-X-
Packet Capture Wizard	Ingress Traffic Selector	r (Step 2 of 6)		
· · · · · · · · · · · · · · · · · · ·	Point of Ingress			
and the second	Select interface:	inside 👻		
	Use backplane cha	nnel		
A.		Ingress		
all a star		(
1 ton		inside		
	Packet Match Criteria -			
54	 Select access list: 	botnet-exclude +	Manage	
THE TAK	Specify packet particular	rameters		
	Source Host:	192.168.10.10	Source Network:	255.255.255.255 •
	Destination Host:	203.0.113.3	Destination Network:	255.255.255.255 •
TTHE	Protocol:	je .	•	
- The				
19.91 MT				
			<back next=""> Fini</back>	sh Cancel Help
	AND ADDRESS TO ADDRESS			

3.3 Klik op Next.

4.1 Selecteer outside voor de Egress Interface en de bron en de bestemmingsIP adressen, samen met hun subnetmasker, in de respectieve verstrekte ruimten verstrekken.

If Network Address Translation (NAT) wordt uitgevoerd op de firewall, neem dit ook in overweging.

Capture Wizard				×
Packet Capture Wizard	Egress Traffic Selector	(Step 3 of 6)		
A CONTRACTOR OF THE OWNER	Point of Egress			
and the second	Select interface:	outside -		
	Use backplane cha	annel		
			Egress	
and the second	-+		<u> </u>	
			outside	•• '
	Packet Match Criteria -			
100 m	 Select access list: 	[botnet-exclude +]	Manage	
11 A. 1 4 1	Specify packet pa	rameters		
	Source Host:	192.168.10.10	Source Network:	255.255.255.255 +
	Destination Host:	203.0.113.3	Destination Network:	255.255.255.255 👻
THUN	Protocol:	ip ~]	
The state				
1 21 M				
· ·				
		[< Back. Next > Finit	sh Cancel Help

4.2 Klik op Next.

5.1 Voer de juiste Packet Size en de Buffer Size in de daartoe bestemde ruimte. Deze gegevens zijn nodig om de opname te kunnen uitvoeren.

5.2 Controleer de Use circular buffer om de cirkelbufferoptie te gebruiken. Circulaire buffers vullen nooit op.

Aangezien de buffer zijn maximumgrootte bereikt, worden de oudere gegevens verworpen en gaat de opname verder.

In dit voorbeeld, cirkelbuffer wordt niet gebruikt, zodat wordt de controledoos niet gecontroleerd.



5.3 Klik op Next.

6.0 Dit venster toont de Access-lists die op de ASA moeten worden geconfigureerd (zodat de gewenste pakketten worden opgenomen) en het type pakketten dat moet worden opgenomen (IP-pakketten worden in dit voorbeeld opgenomen).

6.1 Klik op Next.



7. Klik op start zo start u de pakketopname zoals aangegeven:

Capture Wizard	-			x
Packet Capture Wizard	Run Captures (Step 6 of 6) Click the Start button to begin o Start Ingress: inside	apturing. Stop	Get Capture Buffer	
	Egress: management	ve captures	Launch Network Sniffer Application	
			<back next=""> Finish Cancel I</back>	Help

Aangezien het pakketvastlegging is gestart, probeert u het buitennetwerk vanaf het binnennetwerk te pingen zodat de pakketten die tussen de bron en de IP-adressen van de bestemming stromen, door de ASA-opnamebuffer worden opgenomen.

8. Klik op Get Capture Buffer om de pakketten te bekijken die door de ASA worden gevangen vangt buffer.



De opgenomen pakketten worden in dit venster weergegeven voor zowel het in- als uitgaand verkeer.

9. Klik op Save captures om de opnameinformatie op te slaan.

Capture Wizard		_	_			×
Packet Capture Wizard	Run Captures (Step 6	of 6)				
A PROPERTY AND A PROP	Click the Start button to b	egin capturing.				
T AL ANDRESS		Start 5	top 🔽	Get Capture Buffer	-	
	Ingress	i inside		Launch Network Sniffer	Application	
Jela /	1: 03:58:37.845262	192, 168, 10, 10 > 203	3.0.113.3: icm	p: echo request		
and the second second	2:03:58:37.845903	203.0.113.3 > 192.1	68.10.10: icm	p: echo reply		(B)
	3: 03:58:37.846941	192.168.10.10 > 203	1.0.113.3: ion	p: echo request		
	+ 03:58:37.847520	203.0.113.3 > 192.1	68.10.10: icm	p: echo reply		1.1
	5: 03:58:37.848299	192.168.10.10 > 203	3.0.113.3: icm	p: echo request		
Contraction of the second	6: 03:58:37.848665	203.0.113.3 > 192.1	68.10.10: km	p: echo reply		
	7: 03:58:37.849443	192, 168, 10, 10 > 203	3.0.113.3: icm	p: echo request		
A MARKET A MARKET	8: 03:58:37.849824	203.0.113.3 > 192.1	68.10.10: icm	p: echo reply		
St. St. St.	9: 03:58:37.850618	192, 168, 10, 10 > 200	3.0.113.3: icm	p: echo request		
	10: 03:58:37.850984	203.0.113.3 > 192.	168, 10, 10; icm	np: echo reply		
HULL IIIIIII	11: 03:58:38.868302	192.168.10.10 > 20	3.0.113.3: KM	rp: echo request		
	12:03:58:38.868897	203.0.113.3 > 192.	168, 10, 10; km	ip: echo reply		
The	Egress:	outside		Launch Network Sniffer	Application	
	1:03:58:37.845491	192, 168, 10, 10 > 200	3.0.113.3: icm	o: echo request		
	2: 03:58:37.845873	203.0.113.3 > 192.1	68.10.10: icm	p: etho reply		
	3: 03:58:37.847139	192.168.10.10 > 203	3.0.113.3: icm	p: etho request		
	4: 03:58:37.847490	203.0.113.3 > 192.1	68. 10. 101 icm	p: echo reply		
	5: 03:58:37.848314	192.168.10.10 > 203	3.0.113.3: icm	p: etho request		1
	6: 03:58:37.848634	203.0.113.3 > 192.1	68.10.10: icm	p: echo reply		
	7: 03:58:37.849458	192, 168, 10, 10 > 200	3.0.113.3: icm	p: echo request		
	8: 03:58:37.849794	203.0.113.3 > 192.1	68.10.10: icm	p: echo reply		
	9:03:58:37.850648	192, 168, 10, 10 > 200	1.0.113.3: km	p: echo request		
	10: 03:58:37.850953	203.0.113.3 > 192.	168. 10. 10: km	rpt echo reply		
	11: 03:58:38.868500	192.168.10.10 > 20	3.0.113.3: ion	rp: echo request		
	12:03:58:38.868866	203.0.113.3 > 192.	168, 10, 10; ice	no: echo reply		*
		Save captu	nes	Clear Buffer on Device]	
				<back next=""></back>	Finish Cano	N Help

10.1 Van de **Save captures** Kies het gewenste formaat waarin de opnamebuffer moet worden opgeslagen.

10.2 Dit is ofwel **ASCII** of **PCAP**. Klik op het keuzerondje naast de bestandsnamen.

10.3 Klik vervolgens op Save ingress capture of Save egress capture zoals vereist.

De PCAP-bestanden kunnen worden geopend met opnameanalysatoren, zoals **Wireshark**, en het is de voorkeursmethode.

📧 Save Captures 🛛 🔀
ASCII PCAP Save the buffer in the specified format to the localhost.
Save egress capture
Close Help

11.1 Van de **Save capture file** Typ in het venster de bestandsnaam en de locatie waar het opnamebestand moet worden opgeslagen.

11.2 Klik op Save.

Save capture f	ile				? 🛛
Save in:	Capture data		•	🗢 🗈 💣 📰•	
My Recent Documents					
My Documents					
My Computer					
My Network Places	File name: Save as type:	ingress All Files (".")		• •	Save Cancel

12. Klik op Finish.



Hiermee is de GUI-pakketopnameprocedure voltooid.

Packet Capture configureren met de CLI

Voltooi deze stappen om de pakketopnamefunctie op de ASA te configureren met de CLI:

- 1. Configureer de binnen- en buiteninterfaces zoals aangegeven in het netwerkdiagram met het juiste IP-adres en de juiste beveiligingsniveaus.
- 2. Start het pakketopnameproces met de opnameopdracht in geprivilegieerde EXEC-modus. In dit configuratievoorbeeld wordt de opname met de naam capin gedefinieerd. Bind het aan de binneninterface, en specificeer met het overeenkomende sleutelwoord dat slechts de pakketten die het verkeer van belang aanpassen worden gevangen:

ASA# capture capin interface inside match ip 192.168.10.10 255.255.255.255 203.0.113.3 255.255.255.255

3. Op dezelfde manier wordt de opname met de naam **capout** gedefinieerd. Bind het aan de **buiteninterface**, en specificeer met het **matchsleutelwoord** dat slechts de pakketten die het verkeer van belang aanpassen worden gevangen:

```
ASA# capture capout interface outside match ip 192.168.10.10 255.255.255.255
203.0.113.3 255.255.255.255
```

ASA begint nu de verkeersstroom tussen de interfaces op te nemen. Om de opname op elk moment te stoppen, voert u de opdracht no Capture in gevolgd door de opnamenaam.

Hierna volgt een voorbeeld:

```
no capture capin interface inside
no capture capout interface outside
```

Beschikbare opnametypen op de ASA

In deze sectie worden de verschillende soorten opnamen beschreven die op de ASA beschikbaar zijn.

 asa_dataplane - Leg pakketten op de ASA backplane vast die tussen de ASA en een module die de backplane gebruikt, zoals de ASA CX of IPS module.

```
ASA# cap asa_dataplace interface asa_dataplane
ASA# show capture
capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]
```

 asp-drop drop-code - legt pakketten op die door het versnelde beveiligingspad worden gedropt. De vervolgcode specificeert het type verkeer dat door het versnelde beveiligingspad wordt verbroken.

```
ASA# capture asp-drop type asp-drop acl-drop
ASA# show cap
ASA# show capture asp-drop
```

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S
2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
Flow is denied by configured rule
2 packets shown

ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2 packets shown

 ethernet-type type - Selecteert een Ethernet-type voor opname. Ondersteunde Ethernet-typen zijn 8021Q, ARP, IP, IP6, LACP, PPPOES, PPPOES, RARP en VLAN.

Dit voorbeeld toont hoe ARP verkeer te vangen:

```
ASA# cap arp ethernet-type ?
 exec mode commands/options:
  802.10
  <0-65535> Ethernet type
  arp
  ip
  iрб
  pppoed
  pppoes
  rarp
  vlan
 cap arp ethernet-type arp interface inside
 ASA# show cap arp
 22 packets captured
 1: 05:32:52.119485 arp who-has 10.10.3.13 tell 10.10.3.12
 2: 05:32:52.481862
                          arp who-has 192.168.10.123 tell 192.168.100.100
 3: 05:32:52.481878 arp who-has 192.168.10.50 tell 192.168.100.10
 4: 05:32:53.409723 arp who-has 10.106.44.135 tell 10.106.44.244
 5: 05:32:53.772085 arp who-has 10.106.44.108 tell 10.106.44.248
 6: 05:32:54.782429 arp who-has 10.106.44.135 tell 10.106.44.244
 7: 05:32:54.784695 arp who-has 10.106.44.1 tell xx.xx.xx.xx:

    real-time - Geeft de opgenomen pakketten continu in realtime weer. Om een pakketopname in
```

- real time te beëindigen, drukt u op Ctrl-C. om de opname permanent te verwijderen, gebruikt u de nrvorm van dit bevel.
- Deze optie wordt niet ondersteund wanneer u de cluster exec capture uit.

```
Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.
```

ASA#cap in interface Webserver trace match tcp any any eq 80

Use ctrl-c to terminate real-time capture

 Trace - Traceert de opgenomen pakketten op een manier die vergelijkbaar is met de functie ASA pakkettracer.

// Initiate Traffic 1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S 2322784363:2322784363(0) win 8192 <mss 1460, nop, wscale 2, nop, nop, sackOK> Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 0.0.0.0 0.0.0.0 outside Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group any in interface inside access-list any extended permit ip any4 any4 log Additional Information: Phase: 5 Type: NAT Subtype: Result: ALLOW Config: object network obj-10.0.0.0 nat (inside, outside) dynamic interface Additional Information: Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498

Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: Subtype: Result: ALLOW Config: Additional Information: Phase: 9 Type: ESTABLISHED Subtype: Result: ALLOW Config: Additional Information: Phase: 10 Type: Subtype: Result: ALLOW Config: Additional Information: Phase: 11 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 12 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 13 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 41134, packet dispatched to next module Phase: 14 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 203.0.113.1 using egress ifc outside adjacency Active

```
Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Opmerking: Op ASA 9.10+ neemt het willekeurige trefwoord alleen pakketten met ipv4adressen op. Het Any6-trefwoord neemt al het ipv6-geadresseerde verkeer op.

Dit zijn geavanceerde instellingen die met Packet Captures kunnen worden geconfigureerd.

Raadpleeg de opdrachtreferentiehandleiding voor de manier waarop u deze kunt instellen.

- ikev1/ikev2 Capture only Internet Key Exchange versie 1 (IKEv1) of IKEv2 protocolinformatie.
- isakmp Capture Internet Security Association en Key Management Protocol (ISAKMP) verkeer voor VPN-verbindingen. Het ISAKMP-subsysteem heeft geen toegang tot de bovenlaagprotocollen. De opname is een pseudo-opname, waarbij de fysieke, IP- en UDPlagen met elkaar worden gecombineerd om aan een PCAP-parser te voldoen. De peeradressen worden verkregen uit de SA-uitwisseling en worden opgeslagen in de IP-laag.
- Iacp Leg LACP-verkeer (Captures Link Aggregation Control Protocol) vast. Indien geconfigureerd is de interfacenaam de fysieke interfacenaam. Dit is nuttig wanneer u met Etherchannel werkt om het huidige gedrag van LACP te identificeren.
- tls-proxy Leg gedecrypteerde inkomende en uitgaande gegevens vast uit de TLS-proxy (Transport Layer Security) op een of meer interfaces.
- webvpn Leg WebVPN-gegevens vast voor een specifieke WebVPN-verbinding.

Voorzichtig: Wanneer u WebVPN Capture inschakelt, beïnvloedt dit de prestaties van het security apparaat. Zorg ervoor dat u de opname uitschakelt nadat u de opnamebestanden hebt gegenereerd die nodig zijn om problemen op te lossen.

Standaard

Dit zijn de standaardwaarden voor het ASA-systeem:

- Het standaardtype is raw-data.
- De standaardbuffergrootte is 512 KB.
- Het standaard Ethernet-type is IP-pakketten.
- De standaardpakketlengte is 1.518 bytes.

Bekijk de opgenomen pakketten

Op de ASA

Om de opgenomen pakketten te bekijken, voert u de opdracht show-opname in gevolgd door de

opnamenaam. Deze sectie verschaft de output van de **showopdracht** van de inhoud van de opnamebuffer. Het show capture capin de opdracht toont de inhoud van de genoemde opnamebuffer capin:

ASA# show cap capin

8 packets captured

```
1: 03:24:35.526812 192.168.10.10 > 203.0.113.3: icmp: echo request
2: 03:24:35.527224 203.0.113.3 > 192.168.10.10: icmp: echo reply
3: 03:24:35.528247 192.168.10.10 > 203.0.113.3: icmp: echo request
4: 03:24:35.528582 203.0.113.3 > 192.168.10.10: icmp: echo reply
5: 03:24:35.529345 192.168.10.10 > 203.0.113.3: icmp: echo request
6: 03:24:35.529681 203.0.113.3 > 192.168.10.10: icmp: echo reply
7: 03:24:57.440162 192.168.10.10 > 203.0.113.3: icmp: echo request
8: 03:24:57.440757 203.0.113.3 > 192.168.10.10: icmp: echo reply
```

Het show capture capout de opdracht toont de inhoud van de genoemde opnamebuffer capout:

ASA# show cap capout

8 packets captured

```
1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request

2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply

3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request

4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply

5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request

6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply

7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request

8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply
```

Downloaden van de ASA voor offline analyse

Er zijn een paar manieren om het pakket te downloaden vangt voor analyse offline:

1. Navigeer naar /admin/capture/scapture_name>/pcap">https://sip_of_asa>/admin/capture/scapture_name>/pcap op elke browser.

Tip: Als u de pcap trefwoord, dan alleen het equivalent van het show capture er is opdrachtoutput beschikbaar.

 Voer de opdracht voor kopiëren en uw voorkeursprotocol voor bestandsoverdracht in om de opname te downloaden:

copy /pcap capture:<capture-name> tftp://<server-ip-address>

Tip: Wanneer u een probleem met het gebruik van pakketopnamen oplost, raadt Cisco u aan de opnamen voor offline analyse te downloaden.

Opname wissen

Om de opnamebuffer te wissen, voert u de clear capture opdracht:

ASA# show capture capture capin type raw-data interface inside [Capturing - 8190 bytes] match icmp any any capture capout type raw-data interface outside [Capturing - 11440 bytes] match icmp any any ASA# clear cap capin ASA# clear cap capin ASA# clear cap capout ASA# show capture capture capin type raw-data interface inside [Capturing - 0 bytes] match icmp any any capture capout type raw-data interface outside [Capturing - 0 bytes] match icmp any any Capture capout type raw-data interface outside [Capturing - 0 bytes] match icmp any any VOer het clear capture /all opdracht om de buffer voor alle opnamen te verwijderen:

ASA# clear capture /all

Een opname stoppen

De enige manier om een opname op de ASA te stoppen, is door deze opdracht volledig uit te schakelen:

no capture <capture-name>

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke informatie over probleemoplossing beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.