

ASA prestatiekwesities bewaken en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Problemen met prestaties oplossen](#)

[Snelheids- en duplexinstellingen](#)

[CPU-gebruik](#)

[Hoog geheugengebruik](#)

[PortFast, Channel en Trunking](#)

[Netwerkadresomzetting \(NAT\)](#)

[Syslogs](#)

[SNMP](#)

[Omgekeerde DNS-raadplegingen](#)

[Opdrachten weergeven](#)

[CPU-gebruik tonen](#)

[Verkeer tonen](#)

[Perfmon tonen](#)

[Blokken weergeven](#)

[Geheugen weergeven](#)

[Xlate tonen](#)

[Conn Count tonen](#)

[show interface](#)

[Processen weergeven](#)

[Overzicht van opdrachten](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de opdrachten die moeten worden gebruikt om de prestaties van een Cisco adaptieve security applicatie (ASA) te bewaken en probleemoplossing te bieden.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco adaptieve security applicatie (ASA) die versie 8.3 en hoger uitvoert.


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.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

Problemen met prestaties oplossen

Controleer de basisgebieden die in deze sectie worden beschreven om problemen met de prestaties op te lossen.

 **Opmerking:** als u de uitvoer van de `show` opdracht vanaf uw Cisco-apparaat hebt, kunt u de [Cisco CLI Analyzer](#) gebruiken om potentiële problemen en oplossingen weer te geven. De Cisco CLI Analyzer ondersteunt bepaalde `show` opdrachten. Als u de Cisco CLI Analyzer gebruikt, moet u een geregistreerde Cisco-gebruiker zijn, moet u zijn aangemeld bij uw Cisco-account en moet



JavaScript zijn ingeschakeld binnen uw browser.

Snelheids- en duplexinstellingen

Het security apparaat is vooraf geconfigureerd om de snelheid en duplexinstellingen op een interface automatisch te detecteren. Er bestaan echter verschillende situaties waarin het automatische onderhandelingsproces kan mislukken, wat leidt tot fouten op het gebied van snelheid of duplex (en prestatieproblemen). Voor mission-critical netwerkinfrastructuur codeert Cisco handmatig de snelheid en de duplex op elke interface, zodat er geen kans op fouten is. Deze apparaten bewegen zich over het algemeen niet rond, zodat als u hen behoorlijk vormt, hoeft u hen niet te veranderen.

Voor om het even welk netwerkapparaat, kan de verbindingssnelheid worden ontdekt, maar duplex moet worden besproken. Als twee netwerkapparaten zijn geconfigureerd om automatisch te onderhandelen over snelheid en duplex, ruilen ze frames (Fast Link Pulsen, of FLP's) uit die hun snelheid en duplexmogelijkheden adverteren. Deze pulsen zijn vergelijkbaar met reguliere 10 Mbps-frames, zodat een koppelingspartner zich niet bewust is van deze pulsen. Om een koppelingspartner die de pulsen kan decoderen, bevatten de FLP's alle snelheid en duplexinstellingen die de koppelingspartner kan bieden. Het station dat de FLP's ontvangt, erkent de frames, en de apparaten stemmen onderling in over de hoogste snelheid en duplexinstellingen die elk kan bereiken. Als het ene apparaat geen automatische onderhandeling ondersteunt, ontvangt het andere apparaat de FLP's en overgangen naar de parallele detectiemodus. Om de snelheid van de partner te voelen, luistert het apparaat naar de lengte van de pulsen en stelt vervolgens de snelheid in op basis van de lengte. Het probleem ontstaat bij de duplexinstelling. Omdat duplex moet worden onderhandeld, kan het apparaat dat is ingesteld op automatisch onderhandelen niet de instellingen voor het andere apparaat bepalen, dus blijft het standaard op half-duplex, zoals vermeld in de IEEE 802.3u standaard.

Als u bijvoorbeeld de ASA-interface configureert voor automatische onderhandeling en deze aansluit op een switch die is gehard voor 100 Mbps en full-duplex, stuurt de ASA FLP's. De switch reageert echter niet omdat hij hard is gecodeerd voor snelheid en duplex en niet deelneemt aan automatische onderhandeling. Omdat de ASA geen respons van de switch ontvangt, gaat de ASA over naar de parallele detectiemodus en detecteert de lengte van de pulsen in de frames die de switch uitzendt. Dat wil zeggen dat de ASA inziet dat de switch is ingesteld op 100 Mbps. Op basis hiervan stelt de ASA de interfacesnelheid in. Omdat de switch echter geen FLP's uitwisselt, kan de ASA niet detecteren of de switch full-duplex kan uitvoeren. ASA stelt de duplex dus in op half-duplex, zoals vermeld in de IEEE 803.2u-standaard. Omdat de switch gehard is tot 100 Mbps en full-duplex en de ASA automatisch tot 100 Mbps en half-duplex (zoals de ASA dat doet) heeft onderhandeld, is het resultaat een duplexmismatch die ernstige prestatieproblemen kan veroorzaken.

Een snelheid of duplexwanverhouding wordt het vaakst geopenbaard wanneer de foutentellers op de interfaces in kwestie stijgen. De meest voorkomende fouten zijn frame, cyclische redundantiecontroles (CRC's) en runs. Als deze waarden op uw interface toenemen, of komt een snelheid/duplex wanverhouding of een aanleg van kabelnettenkwestie voor. U moet dit probleem oplossen voordat u doorgaat.

Voorbeeld

<#root>

Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A

157 runts

, 0 giants

379 input errors, 107 CRC, 273 frame

, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output, 774

CPU-gebruik

Als u merkt dat het CPU-gebruik hoog is, moet u deze stappen voltooien om problemen op te lossen:

- Controleer of het aantal verbindingen in show xlate count laag is.
- Controleer of het geheugenblok normaal is.
- Controleer of het aantal ACL's hoger is.
- Geef de opdrachtshow memory detail uit en controleer of het geheugen dat door de ASA wordt gebruikt normaal gebruik is.
- Controleer of de tellingen in show processes cpu-hog en normaal zijnshow processes memory.
- Elke host die aanwezig is binnen of buiten het security apparaat kan het kwaadaardige of massaverkeer genereren dat een broadcast/multicast-verkeer kan zijn en het hoge CPU-gebruik kan veroorzaken. Om dit probleem op te lossen moet u een toegangslijst configureren om het verkeer tussen de hosts (end-to-end) te weigeren en het gebruik te controleren.
- Controleer de instellingen voor duplex en snelheid in ASA-interfaces. De foutieve instelling met de externe interfaces kan het CPU-gebruik verhogen.

In dit voorbeeld wordt het hogere aantal *invoerfouten* en *overschrijdingen* ten gevolge van snelheidsfouten weergegeven. Gebruik de opdrachtshow interface om de fouten te verifiëren:

<#root>

Ciscoasa#

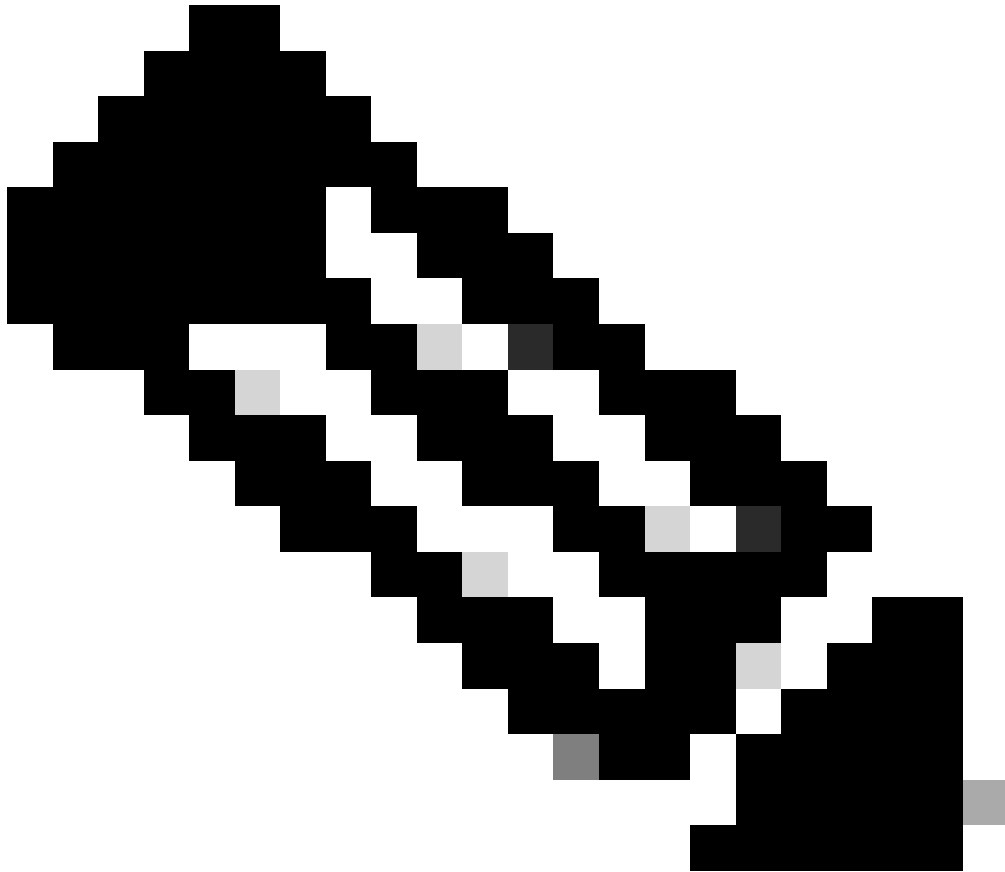
```
sh int GigabitEthernet0/1
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0013.c480.b2b8, MTU 1500
  IP address 192.168.17.4, subnet mask 255.255.255.0
  311981 packets input, 20497296 bytes, 0 no buffer
  Received 311981 broadcasts, 157 runts, 0 giants
```

```
7186 input errors, 0 CRC, 0 frame, 7186 overrun
```

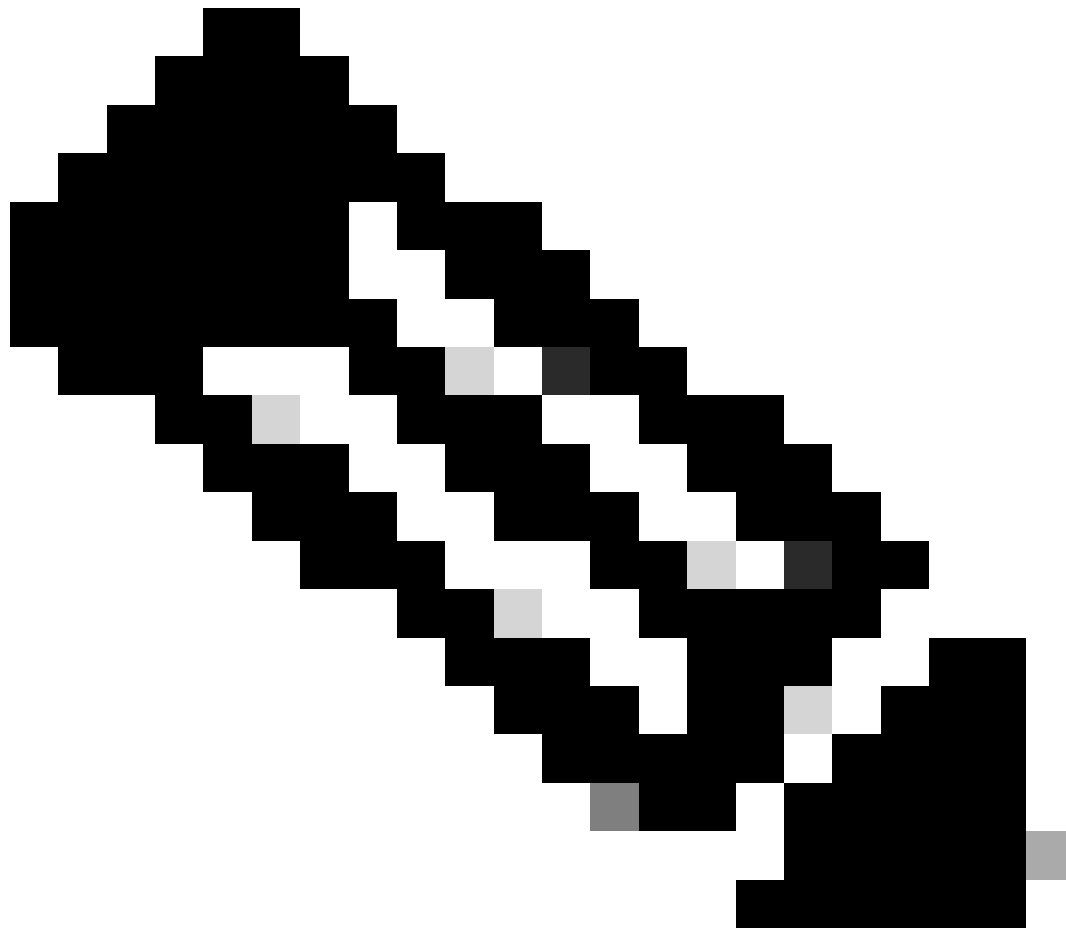
```
, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  121 packets output, 7744 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 1 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops, 0 tx hangs
  input queue (blocks free curr/low): hardware (255/249)
  output queue (blocks free curr/low): hardware (255/254)
```

Om dit probleem op te lossen, stelt u de snelheid in als *automatisch* in de corresponderende interface.




Opmerking: Cisco raadt u aan de opdracht op alle interfaces in te schakelen `verify reverse-path interface`. Dit zorgt ervoor dat pakketten zonder geldig bronadres worden gedropt en resulteert in minder CPU-gebruik. Dit is van toepassing op FWSM wanneer het wordt geconfronteerd met hoge CPU-problemen.

-
- Een andere reden voor het hoge CPU gebruik kan te wijten zijn aan te veel multicast routes. `show mroute` Geef de opdracht uit om te controleren of ASA te veel multicastroUTES ontvangt.
 - Gebruik het `show local-host` commando om te zien of het netwerk een denial-of-service aanval ervaart, die kan wijzen op een virusaanval in het netwerk.
 - Hoge CPU's kunnen voorkomen door Cisco bug-id [CSC48636](#) . Raadpleeg Cisco bug-id [CSC48636](#) voor meer informatie.



Opmerking: alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en buginformatie.

 **Opmerking:** als de eerder geleverde oplossing het probleem niet oplost, upgrade dan het ASA-platform op basis van de vereisten. Raadpleeg [Cisco Security Modules voor security applicaties](#) voor meer informatie over de mogelijkheden en capaciteiten van het adaptieve security applicatie platform. Neem contact op met TAC ([Cisco Technical Support](#)) voor meer informatie.

Hoog geheugengebruik

Hier zijn enkele mogelijke oorzaken en resoluties voor een hoog geheugengebruik:

- **Event logging:** Event logging kan veel geheugen in beslag nemen. Om dit probleem op te lossen, installeert en registreert u alle gebeurtenissen op een externe server, zoals een syslogserver.
- **Geheugenlekkage:** een bekend probleem in de software van het veiligheidstoestel kan tot hoog geheugenverbruik leiden. Upgrade de software van het security apparaat om dit probleem op te lossen.
- **Debugging ingeschakeld:** debuggen kan veel geheugen in beslag nemen. Om deze kwestie op te lossen, maak het zuiveren met `undebug all` bevel onbruikbaar.
- **Blokkerende poorten:** het blokkeren van poorten op de buiteninterface van een security applicatie zorgt ervoor dat het security apparaat grote hoeveelheden geheugen verbruikt om de pakketten te blokkeren via de opgegeven poorten. Om deze kwestie op te lossen, blokkeer je het beledigende verkeer aan de ISP-kant.
- **Threat-Detection:** De optie voor het detecteren van bedreigingen bestaat uit verschillende statistische niveaus die worden verzameld voor verschillende bedreigingen en gescande detectie van bedreigingen, die bepaalt wanneer een host een scan uitvoert. **Schakel** deze functie uit om minder geheugen te verbruiken.

PortFast, Channel en Trunking

Standaard zijn veel switches, zoals Cisco-switches waarop het Catalyst-besturingssysteem (OS) wordt uitgevoerd, ontworpen als plug-and-play apparaten. Als zodanig zijn veel van de standaardpoortparameters niet gewenst wanneer een ASA op de switch is aangesloten. Op een switch waarop Catalyst OS wordt uitgevoerd, is standaardkanalisatie bijvoorbeeld ingesteld op Auto, is trunking ingesteld op Auto en is PortFast uitgeschakeld. Als u een ASA aansluit op een switch die het Catalyst OS draait, schakelt u het kanaliseren uit, schakelt u trunking uit en schakelt u PortFast in.

Gekanaliseerde verbindingen, ook bekend als Fast EtherChannel of Giga EtherChannel, worden gebruikt om twee of meer fysieke poorten in een logische groep te verbinden om de doorvoersnelheid over de link te verhogen. Wanneer een poort is geconfigureerd voor automatisch kanaliseren, stuurt het poortaggregatieprotocol (PAgP) frames uit als de link actief wordt om te bepalen of deze deel uitmaakt van een kanaal. Deze frames kunnen problemen veroorzaken als het andere apparaat automatisch probeert te onderhandelen over de snelheid en duplex van de link. Als het kanaliseren op de poort is ingesteld op Auto, resulteert het ook in een extra vertraging van ongeveer 3 seconden voordat de poort begint met het doorsturen van verkeer nadat de link is omhoog.

 **Opmerking:** op de Switches van Catalyst XL Series is de kanalisatie standaard niet ingesteld op Auto. Om deze reden moet u het



kanaliseren op elke switch poort die verbinding maakt met een ASA uitschakelen.

Trunking, ook bekend onder de gemeenschappelijke trunkingprotocollen Inter-Switch Link (ISL) of Dot1q, combineert meerdere virtuele LAN's (VLAN's) op één poort (of link). Trunking wordt meestal gebruikt tussen twee switches wanneer beide switches meer dan één VLAN op hen gedefinieerd hebben. Wanneer een poort is geconfigureerd voor automatische trunking, stuurt het DTP-frames (Dynamic Trunking Protocol) als de link omhoog komt om te bepalen of de poort die is aangesloten op wil trunken. Deze DTP-frames kunnen problemen veroorzaken met automatische onderhandeling van de link. Als trunking is ingesteld op Auto op een switch poort, voegt het een extra vertraging van ongeveer 15 seconden toe voordat de poort begint met het doorsturen van verkeer nadat de link is omhoog.

PortFast, ook bekend als Fast Start, is een optie die de switch informeert dat een Layer 3-apparaat is verbonden via een switch-poort. De poort wacht niet op de standaardtijd van 30 seconden (15 seconden om te luisteren en 15 seconden om te leren); in plaats daarvan zorgt deze actie ervoor dat de switch de poort onmiddellijk na het verschijnen van de link in de verzendstaat zet. Het is belangrijk om te begrijpen dat wanneer u PortFast inschakelt, overspannen - boom is niet uitgeschakeld. Spanning Tree is nog steeds actief op die poort. Wanneer u PortFast inschakelt, wordt de switch alleen meegedeeld dat er geen andere switch of hub (Layer 2-only device) is aangesloten aan de andere kant van de link. De switch omzeilt de normale 30-seconde vertraging terwijl het probeert te bepalen of een Layer 2-loop resulteert als het die poort omhoog brengt. Nadat de link is opgevoed, neemt het nog steeds deel aan het overspannen - boom. De poort stuurt BPDU's (Bridge Packet Data Units) uit en de switch luistert nog steeds naar BPDU's op die poort. Om deze redenen wordt aanbevolen om PortFast in te schakelen op elke switch-poort die verbinding maakt met een ASA.



set port host <mod>/<port> **Opmerking:** Catalyst OS release 5.4 en hoger bevatten de opdracht waarmee u één opdracht kunt gebruiken om het kanaliseren uit te schakelen, trunking uit te schakelen en PortFast in te schakelen.

Netwerkadresomzetting (NAT)

Elke NAT of NAT Overload (PAT) sessie wordt een vertaalsleuf toegewezen die als een *xlate* bekend staat. Deze verklaringen kunnen voortduren zelfs nadat u veranderingen in de NAT regels aanbrengt die hen beïnvloeden. Dit kan leiden tot een uitputting van vertaalslots of onverwacht gedrag of beide door verkeer dat wordt vertaald. In dit gedeelte wordt uitgelegd hoe u het beveiligingsapparaat kunt bekijken en uitschakelen.



Waarschuwing: een tijdelijke onderbreking van de doorstroming van al het verkeer door het apparaat kan optreden wanneer u de informatie over het beveiligingsapparaat globaal opheldert.

ASA-voorbeeldconfiguratie voor PAT die het IP-adres van de buiteninterface gebruikt:

```
object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
```

Het verkeer dat door het veiligheidstoestel stroomt ondergaat zeer waarschijnlijk NAT. Om de vertalingen te bekijken die op het security apparaat in gebruik zijn, moet u de opdrachtshow xlate uitvoeren:

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NAT
```

Vertaalsleuven kunnen blijven bestaan nadat belangrijke wijzigingen zijn aangebracht. Om de huidige vertaalslots op het security apparaat te wissen, geeft u de opdrachtclear xlate:

```
<#root>
```

```
Ciscoasa#
```

```
clear xlate
```

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
0 in use, 1 most used
```

Met `clear xlate` deze opdracht wordt alle huidige dynamische vertaling uit de uitklaptabel gewist. Om een bepaalde IP-vertaling te wissen, kunt u de opdracht `clear xlate` met het global [ip address] trefwoord gebruiken.

Hier is een voorbeeld van een ASA-configuratie voor NAT:

```
object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside
```

`show xlate` Neem de output voor de vertaling voor binnen 10.2.2.2 aan buiten globaal 10.10.10.10 waar:

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
2 in use, 2 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle 62:33:57 timeout 0:00:30
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

Schakel de vertaling voor 10.10.10.10 wereldwijd IP-adres uit:

```
<#root>
```

```
Ciscoasa# clear xlate global 10.10.10.10
```

In dit voorbeeld is de vertaling voor in 10.2.2.2 naar buiten wereldwijd 10.10.10.10 verdwenen:

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

Syslogs

Syslogs maken het mogelijk problemen op te lossen met de ASA. Cisco biedt een gratis syslog server voor Windows NT, ASA Firewall Syslog Server (PFSS) genoemd. U kunt PDF-bestanden downloaden van [Cisco Technical Support & Downloads](#).


Verschillende andere leveranciers bieden syslog servers aan voor verschillende Windows-platforms, zoals Windows 2000 en Windows XP. De meeste UNIX en Linux machines hebben syslog servers standaard geïnstalleerd.

Wanneer u de syslog server instelt, configureer dan de ASA om logbestanden naar de server te verzenden.

Voorbeeld:

<#root>

logging on logging host <ip_address_of_syslog_server> logging trap debugging

 **Opmerking:** in dit voorbeeld wordt ASA geconfigureerd om debugging (niveau 7) en meer kritische syslogs naar de syslogserver te sturen. Omdat deze ASA-logbestanden de meest breedsprakige zijn, kunt u ze alleen gebruiken bij het oplossen van problemen. Voor normaal gebruik moet u het registratieniveau instellen op Waarschuwing (niveau 4) of Fout (niveau 3).

Als u een probleem met langzame prestaties ervaart, opent u de syslog in een tekstbestand en zoekt u naar het IP-bronadres dat aan het prestatiekwestie is gekoppeld. (Als u UNIX gebruikt, kunt u via de syslog **grijpen** voor het IP-bronadres.) Controleer op berichten die aangeven dat de externe server geprobeerd heeft toegang te krijgen tot het interne IP-adres op TCP-poort 113 (voor Identification Protocol, of Ident), maar de ASA heeft het pakket geweigerd. Het bericht moet aan dit voorbeeld gelijkaardig zijn:

```
%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN
```

Als u dit bericht ontvangt, geef het service resetinboundbevel aan ASA uit. ASA laat geen stille pakketten vallen; in plaats daarvan zorgt deze opdracht ervoor dat de ASA alle inkomende verbindingen die door het beveiligingsbeleid worden ontkend, onmiddellijk opnieuw instelt. De server wacht niet op het Ident-pakket om de TCP-verbinding uit te schakelen; in plaats daarvan ontvangt de server onmiddellijk een reset-pakket.

SNMP

Een aanbevolen methode voor de Enterprise-implementaties is om de prestaties van Cisco ASA met SNMP te bewaken. Cisco ASA ondersteunt dit met SNMP-versies 1, 2c en 3.

U kunt het security applicatie configureren om traps naar een Network Management Server (NMS) te verzenden, of u kunt de NMS gebruiken om door de MIB's op het security applicatie te bladeren. MIB's zijn een verzameling definities en het security apparaat houdt een database van waarden bij voor elke definitie. Raadpleeg voor meer informatie hierover [Cisco ASA 5500 Series configuratiehandleidingen met de CLI, 8.4 en](#)

[8.6.](#)

Alle ondersteunde MIB's voor Cisco ASA zijn te vinden op ASA MIB Support List. Van deze lijst, zijn deze MIBs nuttig wanneer u prestaties controleert:

- Cisco-FIREWALL-MIB ---- bevat objecten die nuttig zijn voor failover.
- Cisco-PROCES-MIB ---- bevat objecten die nuttig zijn voor CPU-gebruik.
- Cisco-MEMORY-POOL-MIB ---- bevat objecten die nuttig zijn voor Memory Objects.

Omgekeerde DNS-raadplegingen

Als u traag presteert met de ASA, moet u controleren of u records voor Domain Name System Pointer (DNS PTR), ook bekend als Reverse DNS Lookup-records, hebt in de gezaghebbende DNS-server voor de externe adressen die de ASA gebruikt. Dit omvat elk adres in uw wereldwijde netwerkadresomzetting (NAT)-pool (of de ASA externe interface als u de interface overbelast), elk statisch adres en intern adres (als u geen NAT met deze poorten gebruikt). Sommige toepassingen, zoals File Transfer Protocol (FTP) en Telnet servers, kunnen omgekeerde DNS-lookups gebruiken om te bepalen waar de gebruiker vandaan komt en of het een geldige host is. Als de omgekeerde DNS raadpleging niet oplost, dan worden de prestaties als verzoektijden uit gedegradeerd.

nslookup Om ervoor te zorgen dat er een PTR-record voor deze hosts bestaat, geeft u de opdracht uit vanaf uw pc of UNIX-machine; neem het globale IP-adres op dat u gebruikt om verbinding te maken met internet.

Voorbeeld

```
<#root>
```

```
% nslookup 192.168.219.25
```

```
10.219.133.198.in-addr.arpa name = www.cisco.com.
```

U moet een antwoord terug met de DNS naam van het apparaat ontvangen dat aan dat IP adres wordt toegewezen. Als u geen antwoord ontvangt, neemt u contact op met de persoon die uw DNS controleert om de toevoeging van PTR-records voor elk van uw globale IP-adressen te vragen.

Overschrijdingen op de interface

Als u een verkeersbreuk hebt, kunnen de gelaten vallen pakketten voorkomen als de burst de als buffer optredende capaciteit van de FIFO buffer op NIC en ontvangt ringsbuffers overschrijdt. Als u pauze frames inschakelt voor flowcontrole, kan dit probleem worden opgelost. Pauze (XOFF) en XON-frames worden automatisch gegenereerd door de NIC-hardware op basis van het FIFO-buffergebruik. Er wordt een pauzestand verstuurd wanneer de bufferhoeveelheid de hoogwatermarkering overschrijdt. Gebruik deze opdracht om Pauze (XOFF)-frames in te schakelen voor stroomregeling:

```
<#root>
```

```
hostname(config)#
```

```
interface tengigabitethernet 1/0
```

```
hostname(config-if)#
```

```
flowcontrol send on
```

Opdrachten weergeven

CPU-gebruik tonen

Dit show cpu usage commando wordt gebruikt om de verkeersbelasting op de ASA CPU te bepalen. Tijdens piekuren van het verkeer, netwerkpieken of aanvallen kan het CPU-gebruik pieken.

ASA heeft één enkele CPU om een verscheidenheid van taken te verwerken; bijvoorbeeld, verwerkt het pakketten en drukt debug berichten aan de console. Elk proces heeft zijn eigen doel, en sommige processen vereisen meer CPU-tijd dan andere processen. Encryptie is waarschijnlijk het meest CPU-intensieve proces, dus als uw ASA veel verkeer doorlaat via versleutelde tunnels, moet u een snellere ASA overwegen, een speciale VPN Concentrator, zoals de VPN 3000. De VAC offload de encryptie en decryptie van de ASA CPU en voert het uit in hardware op de

kaart. Hiermee kan de ASA 100 Mbps verkeer versleutelen en ontsleutelen met 3DES (168-bits codering).

Vastlegging is een ander proces dat grote hoeveelheden systeembronnen kan verbruiken. Wegens dit, adviseert men dat u console, monitor, en bufferlogboekregistratie op ASA onbruikbaar maakt. U kunt deze processen inschakelen wanneer u een probleem oplost, maar u kunt ze uitschakelen voor de dagelijkse werking, met name als u geen CPU-capaciteit hebt. Er wordt ook voorgesteld om syslog of Simple Network Management Protocol (SNMP)-vastlegging (loggeschiedenis) in te stellen op niveau 5 (melding) of lager. Daarnaast kunt u specifieke syslog bericht ID's uitschakelen met de opdracht `logging message <syslog_id>`.

Cisco Adaptive Security Device Manager (ASDM) biedt ook een grafiek op het Monitoring tabblad die u in staat stelt het CPU-gebruik van de ASA in de loop der tijd te bekijken. U kunt deze grafiek gebruiken om de lading op uw ASA te bepalen.

De `show cpu usage` opdracht kan worden gebruikt om CPU-gebruiksstatistieken weer te geven.

Voorbeeld

```
<#root>
```

```
Ciscoasa#
```

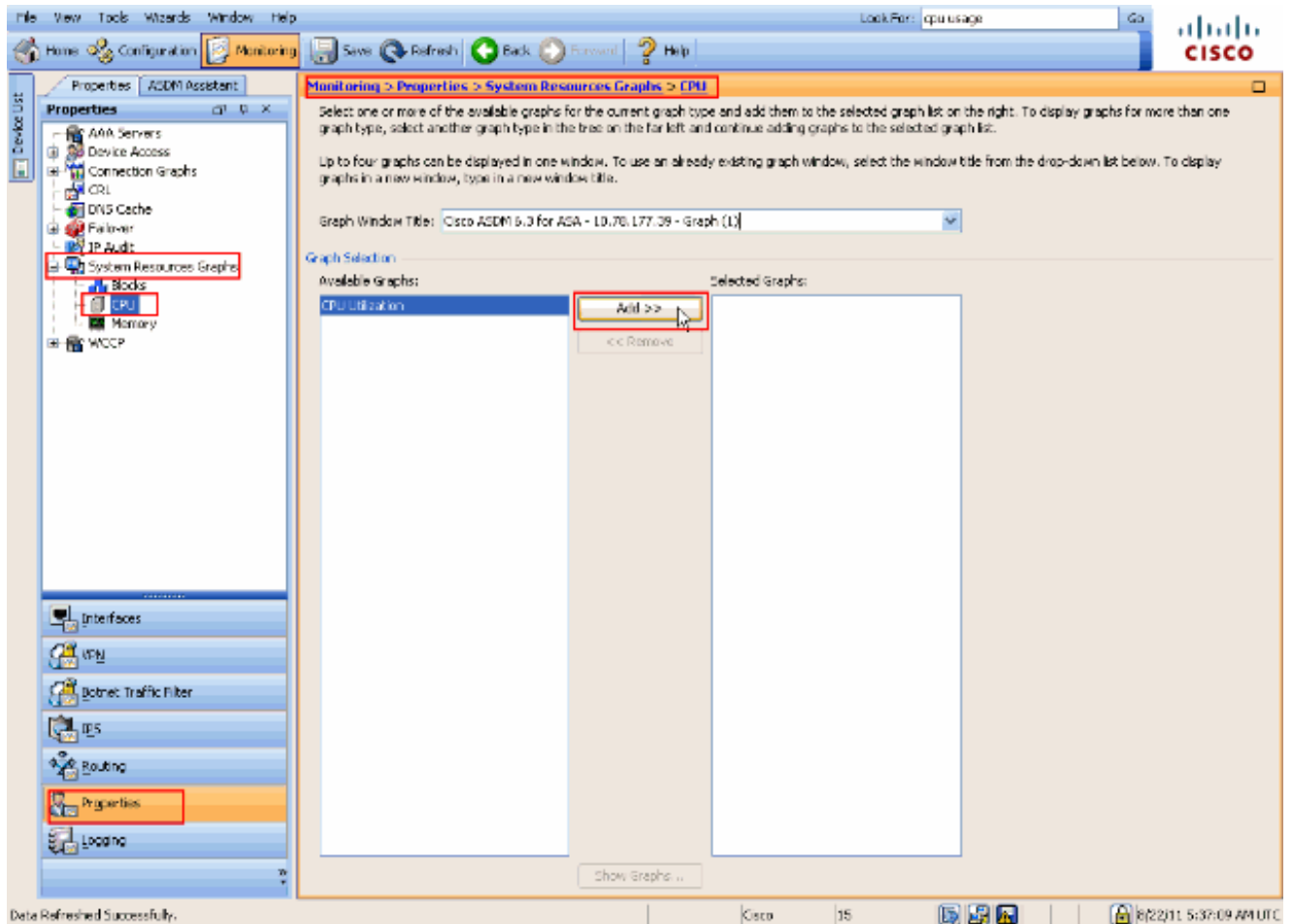
```
show cpu usage
```

```
CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

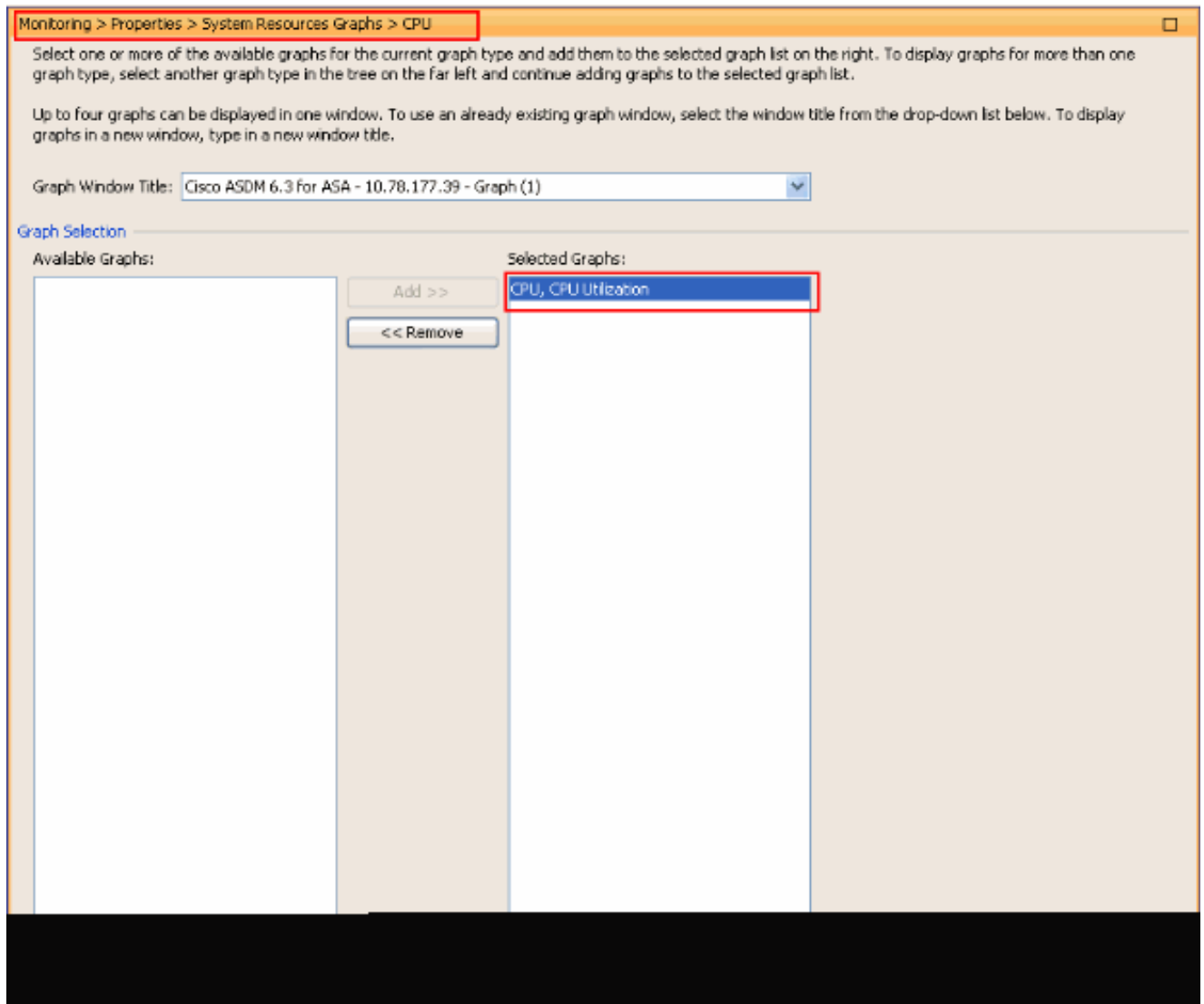
Bekijk het CPU-gebruik op ASDM

Voltooi de volgende stappen om het CPU-gebruik op de ASDM te bekijken:

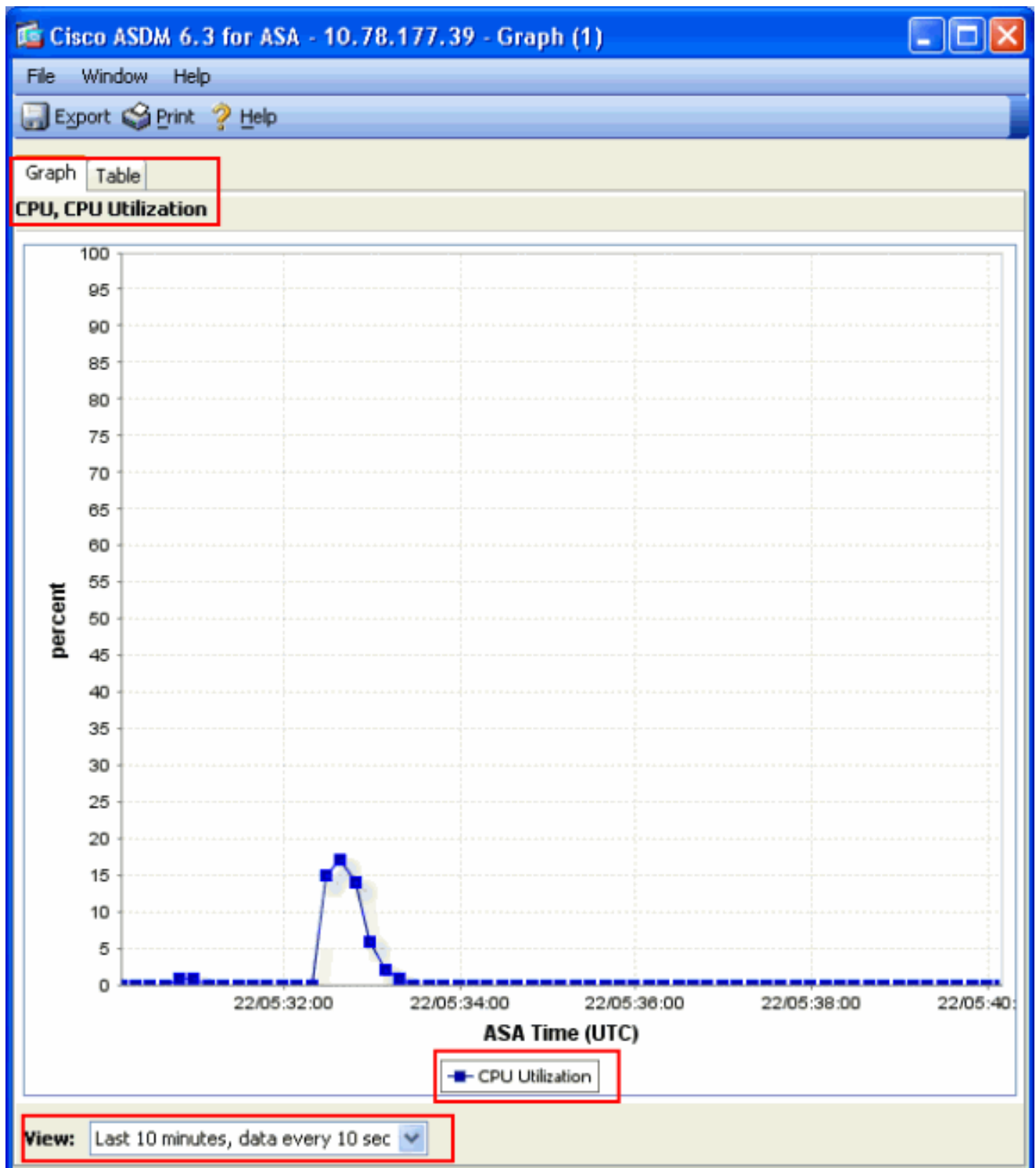
- Ga naar Monitoring > Properties > System Resources Graphics > CPU ASDM en kies de **titel** van het **grafiekvenster**. Kies vervolgens de gewenste grafieken in de lijst met **beschikbare grafieken** en klik op **Toevoegen** zoals aangegeven op de afbeelding.



- Klik op **Grafieken tonen** als de gewenste grafieknaam is toegevoegd onder het gedeelte **Geselecteerde grafieken**.



Het volgende beeld toont de **CPU**-gebruiksgrafiek op de ASDM. Er zijn verschillende weergaven van deze grafiek beschikbaar. Deze kunnen worden gewijzigd wanneer de weergave in de vervolgkeuzelijst Weergave is geselecteerd. Deze uitvoer kan naar wens worden afgedrukt of opgeslagen op de computer.



Beschrijving van de output

Deze tabel beschrijft de velden in de **show cpu usage** uitvoer.

Veld	Beschrijving
CPU-gebruik gedurende 5 seconden	CPU-gebruik voor de afgelopen vijf seconden
1 minuut	Gemiddeld 5 seconden durende voorbeelden van CPU-gebruik in de laatste minuut
5 minuten	Gemiddelde van 5 seconden CPU-gebruik in de afgelopen vijf minuten

Verkeer tonen

Het `show traffic` bevel toont hoeveel verkeer dat door ASA over een bepaalde periode overgaat. De resultaten zijn gebaseerd op het tijdsinterval sinds het bevel het laatst werd uitgegeven. Voor nauwkeurige resultaten, geef eerst het **clear traffic** bevel uit en wacht dan 1-10 minuten alvorens u het `show traffic` bevel uitgeeft. U kunt ook de opdracht `show traffic` geven en 1-10 minuten wachten voordat u de opdracht opnieuw uitgeeft, maar alleen de uitvoer van de tweede instantie is geldig.

U kunt de opdracht `show traffic` gebruiken om te bepalen hoeveel verkeer door uw ASA wordt doorgegeven. Als u meerdere interfaces hebt, kan de opdracht u helpen bepalen welke interfaces de meeste gegevens verzenden en ontvangen. Voor ASA-toestellen met twee interfaces moet de som van het inkomende en het uitgaande verkeer op de buiteninterface gelijk zijn aan de som van het inkomende en het uitgaande verkeer op de binneninterface.

Voorbeeld

```
<#root>
```

```
Ciscoasa#
```

```
show traffic
```

```
outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tr
```

Als u dicht bij de opgegeven doorvoersnelheid op een van uw interfaces komt of deze bereikt, moet u upgraden naar een snellere interface of de hoeveelheid verkeer beperken die naar of uit die interface gaat. Wanneer u dit niet doet, kan dit leiden tot verloren pakketten. Zoals in het **show interface** gedeelte uitgelegd, kunt u de interfacetellers onderzoeken om meer te weten te komen over de doorvoersnelheid.

Perfmon tonen

show perfmon De opdracht wordt gebruikt om de hoeveelheid en de soorten verkeer te bewaken die de ASA inspecteert. Deze opdracht is de enige manier om het aantal vertalingen (xlates) en verbindingen (conn) per seconde te bepalen. De verbindingen worden verder opgesplitst in TCP- en User Datagram Protocol (UDP)-verbindingen. Zie **Beschrijving van uitvoer** voor beschrijvingen van de uitvoer die met deze opdracht wordt gegenereerd.

Voorbeeld

```
PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve
```

Beschrijving van de output

Deze tabel beschrijft de velden in de uitvoershow perfmon .

Veld	Beschrijving
Xlaten	Vertalingen per seconde opgebouwd
Aansluitingen	Aansluitingen per seconde vastgesteld
TCP-verbindingen	TCP-verbindingen per seconde
UDP Conns	UDP-verbindingen per seconde

URL-toegang	URL's (websites) per seconde benaderd
URL-serverantwoord	Verzoeken verzonden naar Websense en N2H2 per seconde (vereist filter opdracht)
TCP-instelling	Aantal TCP-pakketten die de ASA per seconde doorstuurt
TCP-onderschepping	Aantal SYN-pakketten per seconde dat de op een statische dosis
HTTP-correctie	Aantal pakketten die bestemd zijn voor poort 80 per seconde (vereist fixup protocol http opdracht)
FTP-correctie	FTP-opdrachten per seconde geïnspecteerd
AAA Authen	Verificatieverzoeken per seconde
AAA-auteur	Vergunningsaanvragen per seconde
AAA-account	Boekhoudkundige verzoeken per seconde

Blokken weergeven

Samen met de opdrachtshow cpu usage kunt u de show blocksopdracht gebruiken om te bepalen of de ASA is overbelast.

Packet blokkeringen (1550 en 16384 bytes)

Wanneer het in de ASA interface komt, wordt een pakket geplaatst op de wachtrij van de inputinterface, doorgegeven aan OS, en in een blok geplaatst. Voor Ethernet-pakketten worden de blokken van 1550 bytes gebruikt; als het pakket op een 66 MHz Gigabit Ethernet-kaart wordt geleverd, worden de blokken van 16384 bytes gebruikt. ASA bepaalt of het pakket is toegestaan of geweigerd op basis van het Adaptieve security algoritme (ASA) en verwerkt het pakket door naar de uitvoerwachtrij op de uitgaande interface. Als de ASA de verkeerslading niet kan ondersteunen, ligt het aantal beschikbare blokken van 1550 bytes (of blokken van 16384 bytes voor 66 MHz GE) dicht bij 0 (zoals wordt

getoond in de CNT-kolom van de opdrachtoutput). Wanneer de CNT kolom nul bereikt, probeert de ASA meer blokken toe te wijzen, tot een maximum van 8192. Als er geen blokken meer beschikbaar zijn, laat de ASA het pakket vallen.

failover- en syslog-blokkeringen (256 bytes)

De 256-byte blokken worden voornamelijk gebruikt voor stateful failover-berichten. De actieve ASA genereert en verstuurt pakketten naar de stand-by ASA om de vertaal- en verbindingstabel bij te werken. Tijdens periodes van bursty verkeer waarbij hoge tarieven van verbindingen worden gecreëerd of afgebroken, kan het aantal beschikbare 256-byte blokken dalen naar 0. Deze druppel geeft aan dat een of meer verbindingen niet worden bijgewerkt naar de stand-by ASA. Dit is over het algemeen aanvaardbaar omdat de volgende tijd rond het stateful failover protocol de xlate of verbinding vangt die wordt verloren. Als de CNT-kolom voor 256-byte-blokken echter gedurende langere perioden op of nabij 0 blijft, kan ASA de vertaling- en verbindingstabellen die gesynchroniseerd zijn vanwege het aantal verbindingen per seconde dat de ASA verwerkt, niet bijhouden. Als dit consequent gebeurt, upgrade dan de ASA naar een sneller model.

Syslog-berichten die vanuit de ASA worden verstuurd, maken ook gebruik van de blokken van 256 bytes, maar worden over het algemeen niet vrijgegeven in een zodanige hoeveelheid dat de pool van 256 bytes wordt uitgeput. Als de CNT-kolom aangeeft dat het aantal blokken van 256 bytes bijna 0 bedraagt, moet u ervoor zorgen dat u niet logt bij debuggen (niveau 7) op de syslogserver. Dit wordt aangegeven door de logboekvanglijn in de ASA-configuratie. Aanbevolen wordt om de logboekregistratie in te stellen op Melding (niveau 5) of lager, tenzij u aanvullende informatie nodig hebt voor debugging.

Voorbeeld

```
<#root>
```

```
Ciscoasa#
```

```
show blocks
```

```
SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444 1170 1188 16384 2048 1532 1
```

Beschrijving van de output

Deze tabel beschrijft de kolommen in de uitvoershow blocks.

Kolom	Beschrijving
GROOTTE	E Grootte, in bytes, van de blokpool. Elke grootte vertegenwoordigt een bepaald type
MAX	Maximum aantal blokken beschikbaar voor de opgegeven blokpool voor bytes. Het maximum aantal blokken wordt uitgesneden uit geheugen bij bootup. Doorgaans verandert het maximale aantal blokken niet. De uitzondering is voor de blokken van 256 en 1550 bytes, waar het adaptieve security apparaat dynamisch meer kan creëren wanneer nodig, tot een maximum van 8192.
LAAG	Laagwatermarkering. Dit getal geeft het laagste aantal blokken van dit formaat aan dat beschikbaar is sinds het adaptieve security apparaat is ingeschakeld of sinds de laatste opheldering van de blokken (met de opdracht Ontruimen blokken). Een nul in de kolom LAAG geeft een eerdere gebeurtenis aan waarbij het geheugen vol was.
CNT	Huidig aantal blokken beschikbaar voor die specifieke blokpool van de grootte. Een nul in de kolom CNT betekent dat het geheugen nu vol is.

Deze tabel beschrijft de WAARDEN van de SIZE-rij in de uitvoershow blocks.

SIZE Value	Beschrijving
0	Gebruikt door dupb blokken.
4	Dupliceert bestaande blokken in toepassingen zoals DNS, ISAKMP, URL-filtering, audio, TFTP en TCP-modules. Ook kan dit formaat blok normaal gebruikt worden door code om pakketten te versturen naar chauffeurs, enzovoort.
80	Gebruikt in TCP-onderschepping om herkenningpakketten en voor failover hello-berichten te genereren.
256	Wordt gebruikt voor stateful failover-updates, syslog-vastlegging en andere TCP-functies. Deze blokken worden voornamelijk gebruikt voor stateful failover-berichten. Het actieve adaptieve security apparaat genereert en verzendt pakketten naar het stand-by adaptieve security apparaat om de vertaling en verbindingstabel bij te werken. In bursty verkeer,

	<p>waar hoge tarieven van verbindingen worden tot stand gebracht of afgebroken, kan het aantal beschikbare blokken tot 0 dalen. Deze situatie geeft aan dat een of meer verbindingen niet zijn bijgewerkt naar het stand-by adaptieve security apparaat. Het Stateful failover-protocol vangt de volgende keer de verloren vertaling of verbinding. Als de CNT-kolom voor 256-byte blokken gedurende langere perioden op of nabij 0 blijft, heeft het adaptieve security apparaat moeite om de vertaling- en verbindingstabellen gesynchroniseerd te houden vanwege het aantal verbindingen per seconde dat het adaptieve security apparaat verwerkt. Syslog-berichten die vanuit het adaptieve security apparaat worden verzonden, gebruiken ook de blokken van 256 bytes, maar ze worden meestal niet in een dergelijke hoeveelheid vrijgegeven om een uitputting van de pool van 256 bytes te veroorzaken. Als de CNT-kolom aangeeft dat het aantal blokken van 256 bytes bijna 0 bedraagt, moet u ervoor zorgen dat u niet registreert bij Foutopsporing (niveau 7) op de syslogserver. Dit wordt aangegeven door de afsluitlijn in de configuratie van het adaptieve security apparaat. We raden aan om de logboekregistratie in te stellen op Notification (niveau 5) of lager, tenzij u aanvullende informatie nodig hebt voor debugging.</p>
1550	<p>Wordt gebruikt om Ethernet-pakketten op te slaan die moeten worden verwerkt via het adaptieve security apparaat. Wanneer een pakket een adaptieve security applicatie interface invoert, wordt het in de invoerinterface wachtrij geplaatst, doorgegeven aan het besturingssysteem en in een blok geplaatst. Het adaptieve security applicatie bepaalt of het pakket moet worden toegestaan of geweigerd op basis van het beveiligingsbeleid en verwerkt het pakket door naar de uitvoerwachtrij op de uitgaande interface. Als het adaptieve security apparaat moeite heeft om gelijke tred te houden met de verkeersbelasting, kan het aantal beschikbare blokken in de buurt van 0 zweven (zoals weergegeven in de CNT-kolom van de opdrachtoutput). Als de kolom CNT nul is, probeert het adaptieve security apparaat meer blokken toe te wijzen, tot een maximum van 8192. Als er geen blokken meer beschikbaar zijn, laat het adaptieve security apparaat het pakket vallen.</p>
16384	<p>Alleen gebruikt voor de 64-bits, 66 MHz Gigabit Ethernet-kaarten (i82543). Zie de beschrijving voor 1550 voor meer informatie over Ethernet-pakketten.</p>
2048	<p>Beheer of begeleide frames gebruikt voor controle updates.</p>

Geheugen weergeven

show memory De opdracht geeft het totale fysieke geheugen (of RAM) voor de ASA weer, samen met het aantal bytes dat momenteel beschikbaar is. Om deze informatie te gebruiken, moet u eerst begrijpen hoe ASA geheugen gebruikt. Wanneer de ASA opstart, kopieert het OS van Flash naar RAM en voert het OS vanaf RAM (net als routers). Vervolgens kopieert de ASA de opstartconfiguratie van Flash en plaatst deze

in het RAM-geheugen. Tot slot wijst de ASA RAM toe om de in de sectie besproken blokpools te makenshow blocks. Zodra deze toewijzing is voltooid, heeft de ASA alleen extra RAM nodig als de configuratie groter wordt. Daarnaast slaat de ASA de vertaal- en verbidingsgegevens op in RAM.

Tijdens normaal gebruik moet het vrije geheugen op de ASA zeer weinig of helemaal niet veranderen. Typisch, moet u laag op geheugen in werking stellen is als u onder aanval bent en honderdduizenden verbindingen door ASA gaan. Om de verbindingen te controleren, geef het show conn count bevel uit, dat het huidige en maximaantal verbindingen door ASA toont. Als de ASA geen geheugen meer heeft, crasht hij uiteindelijk. Voorafgaand aan de crash kunt u meldingen van storingen in de geheugentoewijzing in de syslog opmerken (%ASA-3-211001).

Als u geen geheugen meer hebt omdat u onder vuur ligt, neemt u contact op met het [Cisco Technical Support](#)-team.

Voorbeeld

```
<#root>
```


```
Ciscoasa#
```


```
show memory
```

```
Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) -----
```

Xlate tonen

show xlate count De opdracht geeft het huidige en maximale aantal vertalingen via de ASA weer. Een vertaling is een afbeelding van een intern adres naar een extern adres en kan een één-op-één afbeelding zijn, zoals Netwerkadresomzetting (NAT), of een veel-op-één omzetting, zoals PAT (Port Address Translation). Deze opdracht is een subset van de opdrachtshow xlate, die elke vertaling via de ASA uitvoert. De opdrachtoutput toont "in gebruik" vertalingen, die verwijzen naar het aantal actieve vertalingen in de ASA wanneer de opdracht wordt uitgegeven; "meest gebruikte" verwijst naar de maximale vertalingen die ooit op de ASA zijn gezien sinds deze werd ingeschakeld.

 **Opmerking:** één host kan meerdere verbindingen hebben naar verschillende bestemmingen, maar slechts één vertaling. Als de teller veel groter is dan het aantal hosts op uw interne netwerk, is het mogelijk dat een van uw interne hosts is gecompromitteerd. Als uw interne host is gecompromitteerd, spooft het het bronadres en verstuurt pakketten de ASA.

 **show xlate** **Opmerking:** Wanneer de vpnclient configuratie is ingeschakeld en de binnenhost DNS-verzoeken verstuurt, kan de opdracht meerdere versies van een statische vertaling weergeven.

Voorbeeld

<#root>

Ciscoasa#

show xlate count

84 in use, 218 most used

<#root>

Ciscoasa(config)#

show xlate

3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,
TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30

ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30

De eerste ingang is een TCP-poortadresomzetting voor host-poort (10.1.1.15, 1026) op het interne netwerk naar host-poort (192.168.49.1, 1024) op het externe netwerk. De "r"-vlag geeft aan dat de vertaling een poortadresomzetting is. De "i" vlaggen geven aan dat de vertaling van toepassing is op de binnenkant van de adreshaven.

De tweede ingang is een UDP-poortadresomzetting voor host-poort (10.1.1.15, 1028) op het interne netwerk naar host-poort (192.168.49.1, 1024) op het externe netwerk. De "r"-vlag geeft aan dat de vertaling een poortadresomzetting is. De "i" vlaggen geven aan dat de vertaling van toepassing is op de binnenkant van de adreshaven.

Het derde item is een ICMP-poortadresomzetting voor host-ICMP-id (10.1.1.15, 21505) op het interne netwerk naar host-ICMP-id (192.168.49.1, 0) op het externe netwerk. De "r"-vlag geeft aan dat de vertaling een poortadresomzetting is. De 'i'-vlaggen geven aan dat de vertaling van toepassing is op het interne adres-ICMP-id.

De binnenste adresvelden verschijnen als bronadressen op pakketten die van de veiligere interface naar de minder veilige interface lopen. Omgekeerd, verschijnen zij als bestemmingsadressen op pakketten die van de minder veilige interface naar de veiligere interface oversteken.

Conn Count tonen

Het show conn count bevel toont het huidige en maximumaantal verbindingen door ASA. Een verbinding is een afbeelding van Layer 4-informatie van een intern adres naar een extern adres. De verbindingen worden opgebouwd wanneer de ASA een SYN-pakket voor TCP-sessies ontvangt of wanneer het eerste pakket in een UDP-sessie aankomt. De verbindingen worden afgebroken wanneer ASA het laatste ACK-pakket ontvangt, dat optreedt wanneer de TCP-sessiehanddruk wordt gesloten of wanneer de time-out verloopt in de UDP-sessie.

Extreem hoge verbindingsgetallen (50-100 keer normaal) kunnen aangeven dat u onder vuur ligt. Geef het show memory commando uit om er zeker van te zijn dat het hoge aantal verbindingen niet tot gevolg heeft dat de ASA geen geheugen meer heeft. Als u onder vuur ligt, kunt u het maximum aantal verbindingen per statische ingang beperken en ook het maximum aantal embryonale verbindingen beperken. Deze actie beschermt uw interne servers, zodat ze niet overweldigd raken. Raadpleeg de [configuratiehandleiding voor Cisco ASA 5500 Series met de CLI, 8.4 en 8.6](#) voor meer informatie.

Voorbeeld

```
<#root>
```

```
Ciscoasa#
```

```
show conn count
```

```
2289 in use, 44729 most used
```

```
show interface
```

Het bevel van de [showinterface](#) kan helpen duplexwanverhouding problemen en kabelkwesties bepalen. Het kan ook meer inzicht bieden in het al dan niet overschrijden van de interface. Als de ASA geen CPU-capaciteit heeft, zweeft het aantal 1550-byte-blokken in de buurt van 0 (kijk naar de 16384-byte-blokken op de 66 MHz Gig-kaarten). Een andere indicator is de verhoging van "geen buffers" op de interface. Het bericht no buffers geeft aan dat de interface niet in staat is het pakket naar het ASA OS te verzenden omdat er geen beschikbaar blok is voor het pakket en het pakket wordt gedropt. show proc cpu Als er regelmatig een toename van het aantal bufferniveaus optreedt, geeft u de opdracht uit om het CPU-gebruik op de ASA te controleren. Als het CPU-gebruik hoog is vanwege een zware verkeerslading, upgrade dan naar een krachtigere ASA die deze lading kan verwerken.

Wanneer een pakket voor het eerst een interface invoert, wordt het in de wachtrij van de inpuhardware geplaatst. Als de wachtrij voor de invoerhardware vol is, wordt het pakket in de wachtrij voor de invoersoftware geplaatst. Het pakket wordt doorgegeven van de invoerwachtrij en geplaatst in een blok van 1550 bytes (of in een blok van 16384 bytes op 66 MHz Gigabit Ethernet-interfaces). ASA bepaalt vervolgens de uitvoerinterface voor het pakket en plaatst het pakket in de juiste hardwarevrij. Als de hardware wachtrij vol is, wordt het pakket geplaatst in de wachtrij van de uitvoersoftware. Als de maximale blokken in een van de softwarewachtrijen groot zijn, wordt de interface overbelast. Bijvoorbeeld, als 200 Mbps in ASA komen en allen uit één enkele 100 Mbps interface gaan, wijst de rij van de outputsoftware op hoge aantallen op de uitgaande interface, die erop wijst dat de interface niet het verkeersvolume kan behandelen. Als u deze situatie ervaart, upgrade dan naar een snellere interface.

Voorbeeld

```
<#root>
```

```
Ciscoasa#
```

```
show interface
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

U moet ook de interface op fouten controleren. Als u runs, invoerfouten, CRCs, of kaderfouten ontvangt, is het waarschijnlijk dat u een duplexwanverhouding hebt. De kabel kan ook defect zijn. Zie [Snelheids- en duplexinstellingen](#) voor meer informatie over duplexkwesties. Vergeet niet dat elke foutenteller het aantal pakketten vertegenwoordigt dat vanwege die specifieke fout is kwijtgeraakt. Als u een specifieke teller ziet die regelmatig toeneemt, lijden de prestaties op uw ASA het waarschijnlijkst, en u moet de worteloorzaak van het probleem vinden.

Terwijl u de interfacetellers onderzoekt, merk op dat als de interface aan volledig-duplex wordt geplaatst, u geen botsingen, recente botsingen, of uitgestelde pakketten moet ervaren. Omgekeerd, als de interface aan half-duplex wordt geplaatst, moet u botsingen, sommige recente botsingen, en misschien sommige uitgestelde pakketten ontvangen. Het totale aantal botsingen, late botsingen en uitgestelde pakketten mag niet hoger zijn dan 10% van de som van de input en output pakketten. Als uw botsingen 10% van uw totale verkeer overschrijden, dan is de verbinding overbenut, en u moet aan volledig-duplex of aan een snellere snelheid (10 Mbps tot 100 Mbps) bevorderen. Onthoud dat botsingen van 10% betekenen dat de ASA 10% van de pakketten die door die interface gaan laat vallen; elk van deze pakketten moet opnieuw worden verzonden.

Raadpleeg de interface opdracht in [Cisco ASA 5500 Series adaptieve security applicaties en opdrachtreferenties](#) voor gedetailleerde informatie over de interfacetellers.

Processen weergeven

Het **show processes** commando op de ASA toont alle actieve processen die op de ASA draaien op het moment dat het commando wordt uitgevoerd. Deze informatie is handig om te bepalen welke processen te veel CPU-tijd ontvangen en welke processen geen CPU-tijd ontvangen. Om deze informatie te krijgen, geef tweemaal het **show processes** bevel uit; wacht ongeveer 1 minuut tussen elke instantie. Voor het proces in kwestie, trek de Runtime waarde af die in de tweede output wordt getoond van de Runtime waarde die in de eerste output wordt getoond. Dit resultaat toont u hoeveel CPU-tijd (in milliseconden) het proces in dat tijdsinterval heeft ontvangen. Merk op dat sommige processen gepland zijn om met bepaalde intervallen te lopen, en sommige processen lopen alleen wanneer ze informatie te verwerken hebben. Het 577poll-proces heeft waarschijnlijk de grootste Runtime-waarde van al uw processen. Dit is normaal omdat de 577poll proces opiniepeilingen de Ethernet interfaces om te zien of ze hebben gegevens die moeten worden verwerkt.

 **Opmerking:** een onderzoek van elk ASA-proces valt buiten het toepassingsgebied van dit document, maar wordt kort vermeld voor de volledigheid. Raadpleeg [ASA 8.3 en hoger: prestatieproblemen bewaken en oplossen](#) voor meer informatie over de ASA-processen.

Overzicht van opdrachten

Samenvattend, gebruik het show cpu usage bevel om de lading te identificeren dat ASA onder is. Vergeet niet dat de output een lopend gemiddelde is; ASA kan hogere pieken van het gebruik van cpu hebben die door het lopende gemiddelde worden gemaskeerd. Zodra de ASA 80% CPU-gebruik bereikt, neemt de latentie via de ASA langzaam toe tot ongeveer 90% CPU. Wanneer het CPU-gebruik meer dan 90% bedraagt, zal de ASA pakketten neerzetten.

Als het CPU-gebruik hoog is, gebruikt u de **show processes** opdracht om de processen te identificeren die de meeste CPU-tijd gebruiken. Gebruik deze informatie om een deel van de tijd te besparen die door intensieve processen (zoals houtkap) wordt verbruikt.

show interface Als de CPU niet hot is, maar u gelooft dat pakketten nog steeds worden gedropt, gebruikt u de opdracht om de ASA-interface te controleren op geen buffers en botsingen, mogelijk veroorzaakt door een duplexfout. Als het aantal buffers niet toeneemt, maar het CPU-gebruik niet laag is, kan de interface het verkeer dat er doorheen stroomt niet ondersteunen.

Als de buffers goed zijn, controleert u de blokken. Als de huidige CNT-kolom in de show blocks output dicht bij 0 ligt op de 1550-byte-blokken (16384-byte-blokken voor 66 MHz Gig-kaarten), laat de ASA zeer waarschijnlijk Ethernet-pakketten vallen omdat deze te druk is. In dit geval, de CPU pieken hoog.

show conn count Als u problemen ondervindt wanneer u nieuwe verbindingen maakt via de ASA, gebruikt u de opdracht om de huidige telling van verbindingen via de ASA te controleren.

Als het huidige aantal hoog is, controleer dan de uitvoer om er zeker van te zijn dat het show memory ASA geen geheugengebrek heeft. Als het geheugen laag is, onderzoek dan de bron van de verbindingen met show conn of show local-host de opdracht om te verifiëren dat uw netwerk geen denial-of-service aanval heeft ervaren.

U kunt andere opdrachten gebruiken om de hoeveelheid verkeer te meten die door de ASA stroomt. Het **show traffic** bevel toont de gezamenlijke pakketten en bytes per interface, en het show perfmon verdeelt het verkeer in verschillende types die ASA inspecteert.

Gerelateerde informatie

- [Cisco ASA 5500-X Series-firewalls](#)
- [Cisco Technical Support en downloads](#)

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.