

ASA I/O en -verbinding snelle probleemoplossing en analyse van pakketvastlegging

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Methode voor probleemoplossing](#)

[Gegevensanalyse](#)

[Vaak voorkomende problemen](#)

[Misingesteld snelheid en duplexwaarden op interface die ASA op een aangesloten apparaat verbindt](#)

[Verkeer naar IPS-module](#)

[ASA Change-ding van TCP MSS optie veroorzaakt lichte prestatievermindering](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij de doorvoersnelheid en verbindingssnelheid van Cisco adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco adaptieve security applicatie (ASA).

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.

Achtergrondinformatie

Sommige klanten kunnen een probleem ervaren wanneer zij eerst een ASA opstellen of wanneer zij nieuwe connectiviteit testen. Het probleem is de TCP-doorvoersnelheid voor verbindingen die door de ASA stromen veel lager is dan wanneer de ASA niet in het verbindingspad is (of de verbindingen zijn veel langzamer dan voordat de ASA werd geïmplementeerd in het netwerk).

Een klant kan bijvoorbeeld een router met lage-end D-Link (of een ander routingapparaat) vervangen door een ASA 5505 of een ASA 5510; wanneer de router echter is vervangen, wordt de verbindingssnelheid sterk verlaagd. De klant kan een case opnemen met Cisco TAC omdat zij geloven dat de ASA de reductie in verbindingssnelheid veroorzaakt heeft.

Methode voor probleemoplossing

TCP stroomt langzaam wanneer er pakketverlies of pakketvertraging op het netwerk is. Om de nauwkeurige oorzaak van het probleem te begrijpen, moeten de gegevens de daadwerkelijke pakketten TCP op de draad voor die verbinding tonen en hoe het netwerk hen zou kunnen beïnvloeden. Meestal wordt een netwerkbeheerder op het probleem gewezen wanneer ze een specifieke actie uitvoeren, zoals een FTP-bestandsoverdracht of een online snelheidstest. Meestal kan het probleem worden gereproduceerd. Daarom kan de beheerder de vereiste gegevens verzamelen om de grondoorzaak te vinden.

Om de vereiste gegevens te verzamelen, dient de **show tech** opdracht van de ASA te worden uitgevoerd vóór en na de test. Deze opdracht toont configuratie- en pakketstatistieken (vooral van **show service-beleid**) en toont ook of de toename van de interfacefouten.

Bidirectionele, simultane pakketvastlegging (overgenomen van de twee ASA interfaces die beïnvloed hebben dat de verbindingsverplaatsingen) vereist zijn om de oorzaak van het probleem volledig te diagnosticeren.

Raadpleeg deze documenten voor voorbeelden van hoe u pakketvastlegging op de ASA kunt toepassen:

- [Probleemoplossing met verbindingen via PIX en ASA](#)
- [TAC Security podcast Episode #1 - Gebruik van het ASA Packet Capture Utility voor Troubleshooter](#)

Gegevensanalyse

Nadat u de benodigde gegevens hebt verzameld, kunt u de pakketvastlegging gebruiken om te bepalen welke van deze problemen er mogelijk zijn geweest:

- De pakketten van de buitengastheer worden ingetrokken of uitgesteld voordat zij de interface van de ASA bereiken.
- De pakketten worden uitgesteld of laten vallen door de ASA.
- De pakketten worden uitgesteld of ergens op het binnennetwerk gelaten.

Opmerking: Deze analyse veronderstelt de gegevens van een gastheer op de buiteninterface naar een gastheer op de binneninterface worden verzonden.

Deze video toont een voorbeeld van hoe de analyse op een pakketvastlegging moet worden uitgevoerd:

TCP-stream coalescing is een technische overweging specifiek voor dit probleem omdat, wanneer je bepaalde functies in de ASA toepast, de firewall de TCP-stream volledig samenstelt die erdoor passeert.

Bijvoorbeeld, als de ASA een ontbrekende pakket op het netwerk ontdekt (aangezien het niet in de ASA wordt ontvangen), stuurt het een ACK namens het andere TCP eindpunt voor de ontbrekende gegevens. Dit scenario komt het meest voor. Als de ASA pakketten ontdekt die uit orde komen, herstelt de ASA de pakketten en geeft ze door aan de ontvanger in de juiste volgorde. Als er geen netwerkdruppels of pakje opnieuw bestellen zijn er geen bijwerkingen om deze functie in te schakelen. Als alle pakketten die door een of ander TCP-eindpunt werden verzonden door het netwerk en de ASA succesvol werden doorgegeven, zou u niet weten dat deze optie is ingeschakeld omdat het geen actie onderneemt op de pakketstromen. Alleen wanneer er problemen zijn met de TCP verbinding op het netwerk zal deze optie verder vertragen netwerkverkeer mogelijk maken. Het samensmelten van de TCP-stroom is zeer bron-intensief voor de ASA. Voor elk pakket dat op het netwerk is gevallen, moet de ASA niet alleen een TCP-pakketverzoek verzenden om het opnieuw verzenden van dat pakket, maar ook de pakketten bufferen die de zender verder heeft verzonden nadat het pakje vermist was geraakt.

Vaak voorkomende problemen

Misingesteld snelheid en duplexwaarden op interface die ASA op een aangesloten apparaat verbindt

Dit probleem doet zich vaak voor wanneer een apparaat wordt vervangen door een ASA. Als de snelheid en duplexwaarden op de ASA interface niet hetzelfde zijn als de waarden op het aangrenzende apparaat, komen pakketdalingen op die interface voor. Controleer de snelheid en duplexwaarden op de ASA interface evenals de aangrenzende interface.

Controleer de **uitvoer van de** interface van de show van de ASA voor de hand liggende fouten die symptomen van dit probleem zijn:

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Verkeer naar IPS-module

Wanneer de ASA is geconfigureerd om verkeer naar de IPS-module te sturen, is de TCP-stream-coalescing ingeschakeld in de ASA-band. Raadpleeg het gedeelte *Dataanalyse* van dit document voor meer informatie over de TCP-stream coalescing-functie.

ASA Change-ding van TCP MSS optie veroorzaakt lichte prestatievermindering

Standaard wordt de TCP MSS-optie in de SYN-pakketten ingesteld op 1380. Daarom moeten TCP-endpoints geen TCP-segment verzenden dat groter is dan 1380 bytes. Deze waarde is lager dan de vaak standaard waarde van 1460 bytes en vertegenwoordigt een TCP-prestatiedaling van ongeveer zes procent (6%). Prestaties kunnen verbeteren als u de maximum MSS instelling op de ASA verhoogt of de MSS aanpassing uitschakelt. Alvorens u de standaardopdracht op de ASA aan te passen, begrijp de risico's verbonden met potentieel fragmentatie als het pakket verder ingekapseld is in het pad ergens.

Raadpleeg voor meer informatie het [gedeelte](#) van de [cpmss](#)-verbinding van het [systeem](#) van de *Cisco ASA 5500 Series opdrachtreferentie*.

Gerelateerde informatie

- [Cisco ASA 5500 Series commando referentie, 8.2](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)