Problemen met het verkeer op CSF CLI oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u Cisco Secure Firewall CLI kunt gebruiken om verkeersproblemen op te lossen door routering, pakketstroom en snortgedrag te valideren.

Voorwaarden

Er zijn geen specifieke vereisten van toepassing op dit document.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beleid en objectconfiguratie van Firepower Management Center (FMC)
- Cisco Secure Firewall (CSF)-routering en interfacelogica

- Concepten voor pakketcontrole en probleemoplossing voor firewalls

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardwareversies voor CSF. Het apparaat dat in het document wordt gebruikt, heeft code 7.6.5.

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

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- Secure Firewall Management Center (FMC)
- Cisco Secure Firewall (CSF)
- Firepower Threat Defense CLI-tools

Belangrijke informatie

Wanneer een apparaat te maken heeft met een verhoogd CPU-, geheugen- of I/O-gebruik, kan het uitvoeren van opdrachten voor probleemoplossing de prestatieachteruitgang verergeren. Het wordt aanbevolen om eerst de uitputtingsconditie van de bron te onderzoeken en op te lossen en vervolgens verder te gaan met de diagnose van verkeersproblemen. Diagnostische opdrachten verbruiken extra systeembronnen, wat de beschikbaarheid verder kan verslechteren en de hersteltijd kan verlengen.

Achtergrondinformatie

Het oplossen van verkeersproblemen op CSF begint vaak met het bevestigen van het logische pad dat een pakket door de firewall moet nemen. Zodra de route en interface mapping zijn begrepen, is de volgende stap om het verwachte pad te vergelijken met de werkelijke pakketstroom. Dit kan worden uitgevoerd met behulp van route lookups, packet-tracer simulatie, packet captures, en Snort engine tracing.

Elke tool biedt een andere zichtbaarheidslaag:

- Toon route bevestigt het routeringspad van het pakket en de interface-identiteit.
- packet-tracer simuleert de verkeersstroom en identificeert ACL-, NAT- en interfacebeslissingen.
- Packet Captures inspecteert live verkeer dat de firewall doorkruist.
- System Support Trace legt de besluitvorming van Snoort bloot voor beleidsgerelateerde blokken of inspectiegebeurtenissen.

Tip: Begin met routering en packet-tracer-validatie voordat u verkeer vastlegt, zodat u kunt bevestigen of de verwachte pad- en toegangscontrolebeslissingen correct zijn voordat u live verkeer analyseert.

Probleem

Een verkeersstroom werkt niet zoals verwacht, en de beheerder moet bepalen of het pakket het juiste pad volgt, of de firewall de verbinding toestaat of weigert en of Snoort of beleidsinspectie het verkeer blokkeert.

Stap 1: Zoek de route

Identificeer het routeringspad en bepaal de logische interfacenamen die zijn gekoppeld aan de bron- en bestemming-IP-adressen. De logische interfacenamen zijn vereist voor de meeste opdrachten voor probleemoplossing, dus dit moet de eerste stap zijn in de werkstroom voor probleemoplossing.

Voer de opdracht voor het bron- en bestemmings-IP-adres uit:

```
show route <IP>
```

Voor internetverkeer dat afhankelijk is van de standaardroute, is identificatie van de logische uitganginterface vereist. De logische interfacenaam kan worden bepaald door deze stap uit te voeren:

```
show route 0.0.0.0
```

Voorbeeld uitvoer:

```
FTD1# show route 192.168.0.11


Routing entry for 192.168.0.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:

    directly connected, via Inside
    Route metric is 0, traffic share count is 1
```

```
FTD1# show route 0.0.0.0

Routing entry for 0.0.0.0 0.0.0.0, supernet
Known via "static", distance 1, metric 0, candidate default path
Routing Descriptor Blocks:

    128.107.0.1, via Outside
    Route metric is 0, traffic share count is 1
```

In dit voorbeeld is de logische interface Inside en de interface Outside.

Waarschuwing: Network Address Translation (NAT) kan verkeer omleiden via verschillende interfaces dan de routeringstabel aangeeft wanneer het NAT-beleid overeenkomt met de verkeersstroom. Controleer bij het oplossen van problemen met de connectiviteit of de NAT-configuratie is afgestemd op het verwachte verkeerspad.

Tip: De logische interfacenamen worden gebruikt in CLI-opdrachten voor probleemoplossing. Let op de logische naam voor toekomstige referentie.

Stap 2: Voer Packet-Tracer uit

Gebruik packet-tracer om te simuleren hoe de firewall een specifieke verkeersstroom evalueert. Deze tool helpt te bevestigen welke interfaces worden gebruikt, of een NAT-beleid wordt toegepast en of een ACL het verkeer toestaat of ontkent.

Gebruik deze opdrachtsyntaxis:

```
packet-tracer input <source interface> <protocol> <source IP> <source port> <destination IP> <destinati
```

Voorbeeld, opdracht:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443
```

Controleer de uitvoer om te bevestigen dat het pakket het verwachte pad volgt en is toegestaan tijdens de simulatie. Dit is handig wanneer u moet bepalen of het probleem verband houdt met routering, NAT of beleidsmatching voordat u live pakketanalyse uitvoert.

Het zend-trefwoord in packet-tracer zorgt ervoor dat het gesimuleerde pakket wordt geïnjecteerd in de interface, waardoor het alle verwerkingsfasen van de firewall kan doorlopen in plaats van als een simulatie te blijven.

Voorbeeld, opdracht:

```
FTD1# packet-tracer input Inside tcp 192.168.0.11 55555 72.163.4.161 443 transmit
```

Stap 3: Captures uitvoeren

Gebruik pakketopnames om live verkeer te inspecteren terwijl het door de firewall gaat. Packet captures zijn anders dan packet-tracer omdat ze het werkelijke verkeer vastleggen en daarom moeten overeenkomen met de echte stroom die de firewall doorkruist op het moment dat de capture actief is. Packet captures zijn bidirectioneel en documenteren beide kanten van de verbinding.

Configureer voor de meeste scenario's voor het oplossen van verkeersproblemen de volgende opnamen:

- Ingress Capture — legt verkeer vast dat aankomt op de interface aan de bronzijde
- Egress Capture — legt het verkeer vast dat op de interface aan de bestemmingszijde achterblijft
- ASP Drop Capture: hiermee worden pakketten vastgelegd die door de firewall zijn gedropt en die voldoen aan de geconfigureerde criteria

Algemene capture syntax:

```
capture <name> interface <interface name> trace match ip host <source IP> host <destination IP>
```

Voorbeeld Ingress capture:

```
FTD1# capture in interface trace Inside match ip host 192.168.0.11 host 72.163.4.161
```

Voorbeeld van Egress-vastlegging:

```
FTD1# capture out interface trace Outside match ip host 128.107.0.22 host 72.163.4.161
```

Voorbeeld van ASP-dropcapture:

```
FTD1# cap asp type asp-drop match ip host 192.168.0.11 host 72.163.4.161
```

Packet captures zijn bidirectioneel, wat betekent dat zowel het forward- als het retourverkeer kan worden vastgelegd op basis van de gedefinieerde wedstrijdcriteria. De traceringsfunctie maakt het mogelijk om de beslissingen die de firewall neemt over het werkelijke verkeer te visualiseren.

Waarschuwing: Als NAT wordt uitgevoerd, moet de egress capture het vertaalde bron-IP gebruiken, niet het oorspronkelijke bron-IP, om het post-NAT-verkeer correct vast te leggen.

Stap 4: System Support Trace uitvoeren

Gebruik System Support Trace om het realtime Snort-inspectieproces voor een specifieke verkeersstroom te bekijken. Dit is vooral handig wanneer het verkeer overeenkomt met een ACL-vergunningsregel, maar nog steeds wordt geblokkeerd door beleidsinspectie. Standaard pakketopnames laten zien dat een pakket is geblokkeerd, maar systeemondersteuningstrace biedt inzicht in waarom het pakket op die manier is behandeld. Systeemondersteuningstrace is bidirectioneel, wat betekent dat het verkeer van beide kanten ontvangt. Dit betekent dat de volgorde waarin de IP's in de tool worden toegevoegd, niet van belang is.

Voer deze opdracht uit en reageer op de volgende vragen:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 72.163.4.161
Please specify a server port: 443
```

Deze tool is vooral handig wanneer de omgeving gebruikmaakt van applicatie- of URL-regels, identiteitsgebaseerde regels, bestandsbeleid of inbraakbeleid. Deze functies worden geëvalueerd na de ACL-wedstrijd, dus een pakket kan worden toegestaan door het toegangscontrolebeleid, maar nog steeds geblokkeerd door Snort-inspectie.

Opmerking: de clientpoort kan leeg blijven als de exacte bronpoort onbekend is.

Verifiëren

Gebruik de uitvoer van het opzoeken van de route, pakkettracer-simulatie, pakketopnames en systeemondersteuningstrace samen om het gedrag van de verkeersstroom te bevestigen. Het doel is om te bepalen of het pakket het juiste pad volgt, of de firewall het toestaat of ontkent en of Snort het blokkeert op basis van diepere inspectie.

Een volledige probleemoplossingsstroom bevestigt doorgaans:

- De route lookup toont de logische ingress en egress interfaces.
- Packet-tracer bevestigt het beoogde doorstuurtraject en de beleidsevaluatie.
- Packet captures bevestigen of het verkeer aankomt en vertrekt zoals verwacht.
- Systeemondersteuningssporen bevestigen of de inspectie van de snort of het beleid het blok veroorzaakt.

Problemen oplossen

Als er een verkeersprobleem blijft optreden, controleert u de volgende gebieden:

- Controleer of het opzoeken van de route overeenkomt met de verwachte bron- en bestemmingsinterfaces.
- Controleer of de packet-tracer-uitgang het verkeer weergeeft dat wordt geweigerd in de ACL- of NAT-fase.

- Controleer de vastleggingen van het ingress- en egress-pakket om te bevestigen dat het verkeer de firewall bereikt en op de juiste interface vertrekt.
- Gebruik ASP drop captures om te bevestigen of de firewall het verkeer intern laat vallen.
- Gebruik System Support Trace om te bepalen of Snort het verkeer blokkeert na de ACL-vergunningsbeslissing.

Gerelateerde informatie

- Firewall-opnamen analyseren om netwerkproblemen op te lossen
- Gebruik Firepower Threat Defense Captures en Packet Tracer

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.