UDP-verkeer door ASA-falen nadat Primaire ISP-link online terugkomt in een dubbele ISP-instelling

Inhoud

Inleiding

Als een adaptieve security applicatie (ASA) twee strips-interfaces per doelnet heeft en de voorkeurroute naar een bestemming enige tijd uit de routingtabel wordt verwijderd, kunnen de verbindingen van User Datagram Protocol (UDP) mislukken wanneer de voorkeurroute opnieuw aan de routingtabel wordt toegevoegd. De TCP-verbindingen kunnen ook door het probleem worden beïnvloed, maar omdat TCP pakketverlies detecteert, worden deze verbindingen automatisch afgebroken door de endpoints en opnieuw gebouwd via de meer optimale routes na de routeverandering.

Dit probleem kan ook worden gezien als een routeringsprotocol wordt gebruikt en een topologie verandering veroorzaakt een verandering in de routingtabel op de ASA.

Voordat u begint

Vereisten

Om dit probleem te ervaren moet de routingtabel van de ASA veranderen. Dit is gebruikelijk met dubbele ISP links op een redundante manier of wanneer de ASA routes via een IGP (OSPF, DHCP, RIP) leert.

Dit probleem doet zich voor wanneer de primaire ISP-link online terugkomt of de genoemde IGP een teruggang ziet, waardoor een minder geprefereerde route die door de ASA werd gebruikt, wordt vervangen door de voorkeursroute met lagere metriek. U zou dan langlevende verbindingen zien, zoals UDP SIP-registraties, GRE, etc., mislukken zodra de primaire of voorkeurroute opnieuw is geïnstalleerd in de ASA-routingtabel.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- AnyCisco ASA 5500 Series adaptieve security applicatie
- ASA versies 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) en later

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Probleem

Als een routingtabelingang van de ASA's routingtabel wordt verwijderd en er geen routes vanuit een interface zijn om een bestemming te bereiken, zullen de verbindingen die door de firewall met die buitenlandse bestemming zijn gemaakt, door de ASA worden verwijderd. Dit komt voor zodat de verbindingen opnieuw kunnen worden gebouwd gebruik makend van een andere interface met het verzenden van ingangen voor de huidige bestemming.

Als echter meer specifieke routes aan de tabel worden toegevoegd, zullen de verbindingen niet worden aangepast om de nieuwe, meer specifieke routes te gebruiken en zullen zij de minder optimale interface blijven gebruiken.

Bedenk bijvoorbeeld dat de firewall twee interfaces heeft die met het internet worden geconfronteerd - "buiten" en "back-up" - en deze twee routes bestaan in de configuratie van de ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Als zowel de buitenkant als de reservekoppen "omhoog" zijn, dan zullen de verbindingen die door de firewall zijn uitgebouwd de buiteninterface gebruiken, omdat het de voorkeursmetriek van 1 heeft. Als de buiteninterface is afgesloten (of de SLA-controlefunctie die de route volgt, ondervindt een verlies van connectiviteit op het getraceerde IP), zouden verbindingen die de buiteninterface gebruiken worden afgebroken en opnieuw gebouwd met de back-up-interface, omdat de enige interface is met een route bestemming.

Het probleem doet zich voor wanneer de externe interface wordt teruggebracht of de getraceerde route opnieuw de geprefereerde route wordt. De routingtabel wordt bijgewerkt om de oorspronkelijke route te prefereren, maar de bestaande verbindingen blijven bestaan op de ASA en verplaatsen de reservetrajectinterface en worden NIET verwijderd en opnieuw gecreëerd op de buiteninterface met de meer-voorkeursmetriek. Dit is omdat de reservekredietstandaardroute nog steeds bestaat in de interface-specifieke routingtabel van de ASA. De verbinding blijft de interface met de minder geprefereerde route gebruiken tot de verbinding wordt geschrapt; In het geval van UDP zou dit voor onbepaalde duur kunnen zijn.

Deze situatie kan problemen opleveren met langlevende verbindingen, zoals externe SIP-registraties of andere UDP-verbindingen.

Oplossing

Om dit specifieke probleem aan te pakken werd een nieuwe eigenschap toegevoegd aan de ASA die zal veroorzaken dat de verbindingen zullen worden afgebroken en op een nieuwe interface opnieuw gebouwd als een meer geprefereerde route aan de bestemming aan de routingtabel wordt toegevoegd. Om de optie te activeren (deze is standaard uitgeschakeld), stelt u een niet-nulpunt in op de **tijdelijke** waarde **voor zwevende-komma**. Deze timeout (gespecificeerd in HH:MM:SS) specificeert de tijd die de ASA wacht voordat deze de verbinding afbreekt zodra een meer geprefereerde route terug naar de routing tabel is toegevoegd:

Dit is een CLI voorbeeld van het inschakelen van de functie. Met deze CLI, als een pakket wordt ontvangen op een bestaande verbinding waarvoor er nu een andere, meer voorkeurroute naar de bestemming is, zal de verbinding 1 minuut later worden afgebroken (en opnieuw worden gebouwd met de nieuwe, meer voorkeurroute):

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

Deze optie wordt aan het ASA-platform toegevoegd in de versies 8.2(5), 8.3(2)12, 8.4(1)1 en 8.5(1), inclusief latere versies van ASA-software.

Als u een versie van ASA-code uitvoert die deze optie niet implementeert, dan zal een tijdelijke oplossing voor de kwestie zijn om de UDP-verbindingen handmatig te spoelen die de minder wenselijke route blijven uitvoeren ondanks dat er een betere route beschikbaar is via een **duidelijke lokale host *<IP>*** of een **duidelijke verbinding *<IP>*.**

De opdrachtreferentie maakt een lijst van deze nieuwe optie onder het gedeelte **timeout**.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems