ASA VPN-taakverdeling voor Director-selectieproces

Inhoud

Inleiding

Dit document beschrijft het verkiezingsproces van de Directeur in een VPN lading-balancerend scenario met de Cisco 5500-X Series 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 ASA 5500-X dat software versie 9.2 draait.

> Opmerking: Dit document is ook van toepassing op alle softwareversies, aangezien de functie voor het eerst is geïntroduceerd in versie 7.0(1).

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

Het in evenwicht brengen van de lading van VPN is een mechanisme dat wordt gebruikt om netwerkverkeer tussen de apparaten in een virtueel cluster rechtvaardig te verdelen. De taakverdeling is gebaseerd op een eenvoudige verdeling; er wordt geen rekening gehouden met de doorvoerbenutting of andere factoren . Een lastverdelingcluster bestaat uit twee of meer apparaten, een regisseur en een of meer secundaire apparaten, en deze apparaten hoeven niet op identieke wijze te worden geconfigureerd.

Taakverdeling-algoritme

Hier volgt een overzicht van het taakverdeling-algoritme:

- Het regisseapparaat handhaaft een gesorteerde lijst van secundaire clusterleden in oplopende volgorde van binnen IP adressen.
- De lading wordt berekend als een integerpercentage (aantal actieve/maximum sessies) dat door elk secundair clusterlid wordt geleverd.
- Het regisseapparaat wijst de IPSec/Secure Socket Layer (SSL) VPN-tunnel terug naar een apparaat met de laagste lading eerst, tot het één procent hoger is dan de andere apparaten.
- Het regisseapparaat wijst alleen naar zichzelf terug wanneer alle secundaire clusterleden één procent hoger zijn dan het regisseapparaat.

Hier is een voorbeeld met één regisseur en twee secundaire clusterleden:

- Alle knooppunten beginnen met een lading van nul procent, en alle percentages worden afgerond naar de dichtstbijzijnde helft.
- De regisseur maakt de verbinding als alle leden een last hebben die één procent hoger is dan de regisseur.
- Als de regisseur de verbinding niet maakt, wordt de sessie genomen door het back-upapparaat dat momenteel het kleinste laadpercentage heeft.
- Als alle leden hetzelfde laadpercentage hebben, dan neemt het back-upapparaat met de minste hoeveelheid sessies de sessie.
- Als alle leden hetzelfde laadpercentage en hetzelfde aantal sessies hebben, dan neemt het reservemiddel met de minste hoeveelheid IP-adressen de sessie.

verkiezingsproces

Het VPN-taakverdeling Director-verkiezingsproces wordt uitgevoerd op het cluster buiten netwerk. Er worden twee soorten gegevens uitgewisseld op het externe netwerk:

- Adresresolutie Protocol (ARP)-pakketten voor het cluster IP-adres dat wordt gebruikt voor de ontdekking van regisseurs worden uitgewisseld. Het maximum aantal ARP-pakketten dat voor het cluster IP-adres wordt verzonden om de regisseur te ontdekken is:

(10 - prioriteit) + 1

Hier wordt *prioriteit* ingesteld zoals in de **prioritaire** subopdracht van de **VPN load-balancerende** CLI-opdracht.

- UDP-pakketten aan de buitenkant voor de Hallo-aanvraag/antwoordberichten worden uitgewisseld. Het poortnummer wordt gespecificeerd in de subopdracht taakverdeling van de **clusterpoort** en is standaard **9023**.

Als een voorbeeld, als de *prioriteit* vijf is voor een lading-in evenwicht zijnd apparaat, probeert het om tot zes ARP pakketten te verzenden om te zien of een directiemechanisme het cluster IP adres bezit. Als een regisseur apparaat wordt gedetecteerd, stuurt de ASA geen meer ARP-berichten en wacht 15 seconden voordat het de UDP Hallo aanvraag verstuurt. De regisseur reageert dan met een UDP Hallo antwoord.

Beveiliging voor herstart-scenario's

In een herstartsituatie met twee ASA's in een load-balances cluster:

- Of ASA-1 of ASA-2 was de regisseur voor de herstart.
- ASA-1 wordt herstart.
- ASA-2 wordt regisseur als hij niet de regisseur was.
- ASA 1 sluit zich simpelweg aan bij het cluster als lid na de herstart.

Het belastingsbalanceringsalgoritme kan worden beïnvloed door een configuratie van de switch waar ook de externe interface van de clusterapparaten is aangesloten. Een Spanning-Tree algoritme kan bijvoorbeeld connectiviteit vertragen wanneer het apparaat dat op de switch is aangesloten, wordt herstart.

Tip: De overspannende-boomhaven snelle opdracht helpt het proces te versnellen.

In sommige gevallen kan een nieuw herstart ASA die load balances heeft ingeschakeld proberen het regisseuse apparaat te worden (zelfs als er al een regisseur-apparaat bestaat) omdat het de huidige regisseur-apparaat niet kan bereiken door een aansluitingsvertraging in de switch. Wanneer er een conflict van de directie is ontdekt als resultaat van ARP botsing, wint de ASA met een laag adres van de Controle van de Toegang (MAC) van Media, terwijl de ASA met een hoger adres van MAC de functie van het regisseapparaat opgeeft.

Directeur Herverkiezingsproces

Er zijn twee situaties die een herverkiezing van de regisseur veroorzaken.

Director-apparaat verwijderd uit het cluster

Wanneer u de optie op de ASA uitschakelt, wordt een uitzending naar alle clusterleden gestuurd om hen op de hoogte te stellen van de wijziging en wordt het eerder beschreven

verkiezingsproces uitgevoerd.

Director-apparaat reageert niet op Cluster lid Hallo-berichten

Als het regisseur apparaat niet reageert op een clusterlid Hallo bericht, duurt het ongeveer 20 seconden om te ontdekken dat de regisseur niet meer aanwezig is. De boodschappen van Hallo worden om de vijf seconden verstuurd (niet aanpasbaar). Als clusterleden na vier Hallo-berichten geen reactie van de regisseur ontvangen, wordt het verkiezingsproces geactiveerd.

Problemen oplossen

> Opmerking: Raadpleeg het artikel Belangrijke informatie over debug Commands van Cisco voordat u **debug**-opdrachten gebruikt.

Deze debug-opdrachten kunnen nuttig zijn bij pogingen om problemen met uw systeem op te lossen:

- **debug fsm 255** - gebruik deze opdracht om het algehele geluid van de Finite State Machine te activeren. Voer **de** opdracht **niet** uit om deze te deactiveren.
- **debug menu vpnlb 3** - gebruik deze opdracht om het VPN-lading-**in** evenwicht brengen te activeren. Voer de opdracht **debug -menu vpnlb 3** nogmaals in om het programma te deactiveren.
- **debug menu vpnlb 4** - gebruik deze opdracht om het **in** VPN-taakverdeling ingestelde spoor te activeren. Voer de opdracht **debug -menu vpnb 4** nogmaals in om het programma te deactiveren.

Gerelateerde informatie

- Taakverdeling begrijpen
- Technische ondersteuning en documentatie – Cisco Systems