Site-To-Site VPN-configuratie op de meervoudige context ASA 9.x ontvangt een foutmelding

Inhoud

Inleiding

Dit document beschrijft hoe u het foutbericht moest oplossen, "De maximaal toegestane tunneltelling is bereikt", wanneer u een Site-To-Site VPN configureren op de Multicontext Adaptieve security applicaties (ASA) 9.x.

Voorwaarden

Gebruikte componenten

De informatie in dit document is gebaseerd op ASA-softwareversie 9.0 en hoger. Met deze versie werd de configuratie van Site-To-Site VPN in meerdere contextmodus geïntroduceerd.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Wanneer u probeert om meerdere Site-To-Site VPN-tunnels in de ASA op te zetten, faalt het en genereert het syslig bericht "Het maximum aantal tunnels dat is toegestaan is bereikt".

Het specifieke syslogbericht is hieronder:

```
%ASA-4-751019: Local:<LocalAddr> Remote:<RemoteAddr> Username:<username> Failed to obtain a
<licenseType> license.
```

- **<**Local Address**>** - Local Address voor deze verbinding
- **<**Remote-Adres**>** - Remote-peer-adres voor deze verbindingspoging
- **<**gebruikersnaam**>** - gebruikersnaam voor een peer-verbinding
- **<**licentietype**>** - licentietype dat is overschreden (ander VPN of AnyConnect Premium/Essentials)

Achtergrondinformatie

Het logbestand geeft aan dat een sessie is gemaakt omdat de maximale licentielimiet voor VPN-tunnels is overschreden. Dit veroorzaakt een storing om een tunnelaanvraag te initiëren of op een tunnelverzoek te reageren.

De implementatie van VPN in multi-mode vereist de verdeling van de totale beschikbare VPN-licenties onder de geconfigureerde contexten. De ASA-beheerder kan configureren hoeveel licenties elke context wordt toegewezen.

Standaard worden er geen VPN-tunnellicenties toegewezen aan de contexten, en de toewijzing van het licentietype moet handmatig door de beheerder worden uitgevoerd.

Aanbevolen actie

Zorg ervoor dat er voldoende licenties beschikbaar zijn voor alle toegestane gebruikers en/of dat u meer licenties hebt aangeschaft om de afgewezen verbindingen mogelijk te maken. Voor multicontext, wijs meer licenties toe aan de context die de fout heeft gemeld, indien mogelijk.

Oplossing

Het verdelen van de licenties onder de contexten wordt gedaan door de augmentatie van de resource manager met een 'VPN ander' resource die de verdeling van de 'Overige VPN' licentiepool die voor site-to-site VPN wordt gebruikt onder de geconfigureerde contexten beheert.

De limiet-resource CLI hieronder staat deze configuratie toe binnen de resource 'class' modus.

```
Limit-resource vpn [burst] other <value> | <value>%
```

Waar, bereik **<**waarde**>**: 1- Persoonsbeperking voor 1-100% van de geïnstalleerde licenties.

Voor bursts is het bereik 1 tot niet-toegewezen licenties of 1-100% van niet-toegewezen licenties. Standaard: 0; VPN-bronnen worden niet aan een class toegewezen.

Om een context aan 10% van de geïnstalleerde licenties toe te wijzen, moet u een resource klasse definiëren. Pas vervolgens de klasse toe op contexten die u deze bron binnen de systeemcontextconfiguratie moet kunnen krijgen.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 10%
```

Om een context van 250 VPN peers van de geïnstalleerde licenties toe te wijzen, moet u een resource 'class' definiëren. Pas vervolgens de klasse toe op de contexten die u liever deze bron binnen de systeemcontextconfiguratie wilt kunnen krijgen.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 250
```

Om de bovenstaande klasse "vpn" toe te passen op een context die "beheerder" wordt genoemd, volgt u deze stappen:

1. Verandert/overschakelt naar de systeemcontext en past de klasse VPN toe voor de context "beheerder". Dit kan alleen binnen de systeemcontext worden gedaan.
2. Hieronder staat het configuratie fragment om de class "vpn" aan de context "beheerder" toe te wijzen.

   ```
   ciscoasa(config)# context administrator
   ciscoasa(config-ctx)# member vpn
   ```

Gerelateerde informatie

- Cisco ASA 5500 Series Next-generation firewalls in de handleidingen
- Cisco ASA 5500 Series configuratie handleidingen voor volgende generatie
- Technische ondersteuning en documentatie – Cisco Systems