Die Site-to-Site-VPN-Konfiguration für mehrere Kontexte: ASA 9.x erhält Fehlermeldung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Fehlermeldung "Die maximal zulässige Tunnelanzahl wurde erreicht" bei der Konfiguration eines Site-to-Site-VPN auf den Adaptive Security Appliances (ASA) 9.x (Multiple Context Adaptive Security Appliances) behoben wird.

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ASA Software Version 9.0 und höher. Mit dieser Version wurde die Site-to-Site-VPN-Konfiguration im Multiple-Context-Modus eingeführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Wenn Sie versuchen, mehrere Site-to-Site-VPN-Tunnel auf der ASA zu aktivieren, schlägt dies fehl und generiert die Syslog-Meldung "Die maximal zulässige Tunnelanzahl wurde erreicht".

Die spezifische Syslog-Meldung ist unten aufgeführt:

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

- **<**LocalAddr**>** - Lokale Adresse für diesen Verbindungsversuch
- **<**RemoteAddr**>** - Remote-Peer-Adresse für diesen Verbindungsversuch
- **<**Benutzername**>** - Benutzername für Peer-Verbindung, die versucht, eine Verbindung herzustellen
- **<**licenseType**>** - Lizenztyp, der überschritten wurde (Andere VPN oder AnyConnect Premium/Essentials)

Hintergrundinformationen

Das Protokoll zeigt an, dass eine Sitzungserstellung fehlschlug, weil die maximale Lizenzgrenze für VPN-Tunnel überschritten wurde, was dazu führt, dass eine Tunnelanforderung nicht initiiert oder nicht beantwortet wurde.

Die Implementierung von VPN im Multiple-Mode erfordert die Aufteilung der insgesamt verfügbaren VPN-Lizenzen auf die konfigurierten Kontexte. Der ASA-Administrator kann konfigurieren, wie viele Lizenzen pro Kontext zugewiesen sind.

Standardmäßig sind den Kontexten keine VPN-Tunnel-Lizenzen zugewiesen, und die Zuweisung des Lizenztyps muss vom Administrator manuell erfolgen.

Empfohlene Aktion

Stellen Sie sicher, dass genügend Lizenzen für alle zulässigen Benutzer verfügbar sind und/oder erhalten Sie mehr Lizenzen, um die abgelehnten Verbindungen zuzulassen. Weisen Sie dem Kontext, der den Fehler gemeldet hat, möglichst mehr Lizenzen für Multi-Context zu.

Lösung

Die Aufteilung der Lizenzen auf die Kontexte erfolgt durch die Erweiterung des Ressourcen-Managers mit einer "VPN Other"-Ressource, die die Aufteilung des "Other VPN"-Lizenzpools verwaltet, der für Site-to-Site-VPNs zwischen den konfigurierten Kontexten verwendet wird.

Die nachfolgende CLI für Limit-Ressourcen ermöglicht diese Konfiguration im Ressourcen-Klassenmodus.

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

Bereich mit **<**Wert**>**: 1- Plattformlizenzlimit oder 1-100 % der installierten Lizenzen.

Bei Bursts liegt der Bereich zwischen 1 und nicht zugewiesenen Lizenzen bzw. zwischen 1 und 100 % der nicht zugewiesenen Lizenzen.
Standard: 0; einer Klasse sind keine VPN-Ressourcen zugewiesen.

Um 10 % der installierten Lizenzen einen Kontext zuzuweisen, müssen Sie eine

Ressourcenklasse definieren. Wenden Sie anschließend die Klasse auf Kontexte an, die Sie benötigen, um diese Ressource in der Systemkontextkonfiguration abrufen zu können.

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

Um einen Kontext von 250 VPN-Peers der installierten Lizenzen zuzuweisen, müssen Sie eine Ressource als 'Class' definieren. Wenden Sie dann die Klasse auf die Kontexte an, bei denen Sie diese Ressource in der Systemkontextkonfiguration abrufen möchten.

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

Um die obige Klasse "vpn" auf einen Kontext mit dem Namen "administrator" anzuwenden, gehen Sie wie folgt vor:

1. Ändern/Wechseln in den Systemkontext und Anwenden der Klasse-VPN für den Kontext "administrator". Dies konnte nur im Systemkontext durchgeführt werden.
2. Unten sehen Sie den Konfigurationsausschnitt, um die Klasse "vpn" dem Kontext "administrator" zuzuweisen.

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

Zugehörige Informationen

- Cisco Firewalls der nächsten Generation der Serie ASA 5500 - Referenzhandbücher
- Konfigurationsanleitungen für die Firewalls der nächsten Generation der Cisco Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems