Auswahlprozess für ASA VPN Load Balancing Director

Inhalt

Einführung

Dieses Dokument beschreibt den Director-Auswahlprozess in einem VPN-Lastenausgleichsszenario mit der Cisco Adaptive Security Appliance (ASA) der Serie 5500-X.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA 5500-X, die die Software Version 9.2 ausführt.

> **Hinweis**: Dieses Dokument gilt auch für alle Softwareversionen, da die Funktion erstmals in Version 7.0(1) eingeführt wurde.

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.

Hintergrundinformationen

VPN-Lastenausgleich ist ein Mechanismus, der verwendet wird, um Netzwerkverkehr gleichmäßig auf die Geräte in einem virtuellen Cluster zu verteilen. Lastenausgleich basiert auf einer einfachen Verteilung. sie berücksichtigt nicht die Durchsatznutzung oder andere Faktoren. Ein Lastenausgleichs-Cluster besteht aus zwei oder mehr Geräten, einem Director und einem oder mehreren sekundären Geräten. Diese Geräte müssen nicht identisch konfiguriert werden.

Load-Balancing-Algorithmus

Im Folgenden finden Sie eine Übersicht über den Lastenausgleichsalgorithmus:

- Das Director-Gerät verwaltet eine sortierte Liste sekundärer Cluster-Mitglieder in aufsteigender Reihenfolge der internen IP-Adressen.
- Die Last wird als ganzzahliger Prozentsatz (Anzahl der aktiven/maximalen Sitzungen) berechnet, der von jedem sekundären Cluster-Mitglied bereitgestellt wird.
- Das Director-Gerät leitet den IPSec/Secure Sockets Layer (SSL)-VPN-Tunnel an ein Gerät mit der niedrigsten Last um, bis diese um ein Prozent höher ist als die anderen Geräte.
- Das Director-Gerät leitet sich nur dann selbst um, wenn alle sekundären Cluster-Mitglieder um ein Prozent höher sind als das Director-Gerät.

Das folgende Beispiel zeigt einen Director und zwei sekundäre Cluster-Mitglieder:

- Alle Knoten beginnen mit einer 0 %-Last, und alle Prozentsätze werden auf die nächsten 5 % gerundet.
- Das Director-Gerät übernimmt die Verbindung, wenn alle Mitglieder eine Last haben, die um ein Prozent höher ist als das Director-Gerät.
- Wenn das Director-Gerät die Verbindung nicht übernimmt, wird die Sitzung vom Backup-Gerät übernommen, das derzeit den niedrigsten Lastprozentsatz aufweist.
- Wenn alle Mitglieder den gleichen Auslastungsprozentsatz haben, wird die Sitzung vom Sicherungsgerät mit der geringsten Anzahl an Sitzungen übernommen.
- Wenn alle Mitglieder den gleichen Auslastungsprozentsatz und die gleiche Anzahl von Sitzungen haben, wird die Sitzung vom Sicherungsgerät mit der geringsten Anzahl von IP-Adressen übernommen.

Prozess der Direktorenwahl

Der VPN Load Balancing Director-Auswahlprozess wird auf dem externen Cluster-Netzwerk durchgeführt. Es gibt zwei Arten von Daten, die im externen Netzwerk ausgetauscht werden:

- Adressenauflösungsprotokolle (Address Resolution Protocol, ARP)-Pakete für die Cluster-IP-

Adresse, die für die Director Discovery verwendet werden, werden ausgetauscht. Die maximale Anzahl an ARP-Paketen, die für die Cluster-IP-Adresse gesendet werden, um den Director zu ermitteln, ist:

(10 - Priorität) + 1

Hier wird die *Priorität* wie im **priority**-Unterbefehl des **VVPN Load Balancing**-Befehls konfiguriert.

- UDP-Pakete an der Außenseite für die Hello-Anfrage-/Antwortnachrichten werden ausgetauscht. Die Portnummer wird im Unterbefehl **für den** Lastenausgleich für den **Cluster-Port** angegeben und lautet standardmäßig **9023**.

Wenn beispielsweise die *Priorität* fünf für ein Lastverteilungsgerät beträgt, versucht es, bis zu sechs ARP-Pakete zu senden, um zu sehen, ob ein Director-Gerät die Cluster-IP-Adresse besitzt. Wenn ein Director-Gerät erkannt wird, sendet die ASA keine weiteren ARP-Nachrichten und wartet 15 Sekunden, bevor die UDP Hello-Anfrage gesendet wird. Das Director-Gerät antwortet dann mit einer UDP Hello-Antwort.

Probleme bei Neustarts

Bei einem Neustart mit zwei ASAs in einem Load Balancing-Cluster:

- Vor dem Neustart war entweder ASA-1 oder ASA-2 der Director.
- ASA-1 wird neu gestartet.
- ASA-2 wird zum Director, wenn es zuvor nicht der Director war.
- ASA-1 tritt einfach nach dem Neustart als Mitglied in den Cluster ein.

Der Lastenausgleichsalgorithmus kann durch eine Konfiguration des Switches beeinflusst werden, mit dem auch die externe Schnittstelle der Cluster-Geräte verbunden ist. Ein Spanning-Tree-Algorithmus kann beispielsweise zu Verbindungsverzögerungen führen, wenn das mit dem Switch verbundene Gerät neu gestartet wird.

Tipp: Der Befehl spanning-tree port fast beschleunigt den Prozess.

In einigen Fällen versucht eine neu startete ASA mit aktiviertem Lastenausgleich, zum Director-Gerät zu werden (selbst wenn bereits ein Director-Gerät vorhanden ist), da sie aufgrund einer Verbindungsverzögerung im Switch nicht das aktuelle Director-Gerät erreichen kann. Wird ein Directorship-Konflikt infolge einer ARP-Kollision erkannt, gewinnt die ASA mit einer MAC-Adresse (Low Media Access Control), während die ASA mit einer höheren MAC-Adresse die Rolle des Director-Geräts aufgibt.

Wiederwahl von Direktoren

Es gibt zwei Situationen, die zu einer Wiederwahl des Director-Geräts führen.

Director-Gerät aus Cluster entfernt

Wenn Sie die Funktion auf der ASA deaktivieren, wird eine Broadcast-Nachricht an alle Cluster-Mitglieder gesendet, um die Änderung zu informieren. Anschließend wird der zuvor beschriebene Auswahlprozess durchgeführt.

Director Device reagiert nicht auf Hello-Nachrichten von Clustermitgliedern

Wenn das Director-Gerät nicht auf eine Hello-Nachricht eines Clusters reagiert, benötigt ein ASA-Cluster ungefähr 20 Sekunden, um festzustellen, dass der Director nicht mehr vorhanden ist. Die Hello-Nachrichten werden alle fünf Sekunden gesendet (nicht konfigurierbar). Wenn Cluster-Mitglieder nach vier Hello-Nachrichten keine Antwort vom Director-Gerät erhalten, wird der Auswahlprozess ausgelöst.

Fehlerbehebung

> **Hinweis**: Lesen Sie den Cisco-Artikel Wichtige Informationen über Debug-Befehle, bevor Sie **Debug-**Befehle verwenden.

Diese Debug-Befehle können bei der Behebung von Systemproblemen hilfreich sein:

- **debug fsm 255** - Verwenden Sie diesen Befehl, um das allgemeine Finite State Machine-Debuggen zu aktivieren. Geben Sie den Befehl **no debug all** ein, um die Aktivierung durchzuführen.
- **debug menu vpnlb 3** - Verwenden Sie diesen Befehl, um die Debugverfolgung für den VPN-Lastenausgleich zu aktivieren. Geben Sie den Befehl **debug menu vpnlb 3** erneut ein, um die Aktivierung durchzuführen.
- **debug menu vpnlb 4** - Verwenden Sie diesen Befehl, um die Ablaufverfolgung der VPN Load Balancing-Funktion zu aktivieren. Geben Sie den Befehl **debug menu vpnlb 4** erneut ein, um die Aktivierung durchzuführen.

Zugehörige Informationen

- Lastenausgleich
- Technischer Support und Dokumentation - Cisco Systems