ASA verzeichnet eine hohe CPU-Auslastung aufgrund einer Datenverkehrsschleife, wenn VPN-Clients die Verbindung trennen

Inhalt

Einführung

Dieses Dokument beschreibt ein häufiges Problem, das auftritt, wenn VPN-Clients von einer Cisco Adaptive Security Appliance (ASA) getrennt werden, die als VPN-Headend für den Remote-Zugriff ausgeführt wird. In diesem Dokument wird auch die Situation beschrieben, in der eine Datenverkehrsschleife auftritt, wenn VPN-Benutzer von einer ASA-Firewall getrennt werden. Dieses Dokument behandelt nicht die Konfiguration oder Einrichtung des Remote-Zugriffs auf das VPN, sondern nur die spezifische Situation, die sich aus bestimmten gängigen Routing-Konfigurationen ergibt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Remote Access VPN-Konfiguration auf der ASA
- Grundlegende Layer-3-Routing-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem ASA-Modell 5520, das den ASA-Code

Version 9.1(1) ausführt.

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.

Zugehörige Produkte

Dieses Dokument kann mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Beliebiges ASA-Modell
- Beliebige ASA-Codeversion

Hintergrundinformationen

Wenn ein Benutzer eine Verbindung zur ASA als VPN-Konzentrator für Remote-Zugriff herstellt, installiert die ASA eine hostbasierte Route in der ASA-Routing-Tabelle, die den Datenverkehr an diesen VPN-Client über die externe Schnittstelle (zum Internet) weiterleitet. Wenn dieser Benutzer die Verbindung trennt, wird die Route aus der Tabelle entfernt, und die Pakete im internen Netzwerk (die für diesen getrennten VPN-Benutzer bestimmt sind) können zwischen der ASA und einem internen Routing-Gerät Schleifen aufweisen.

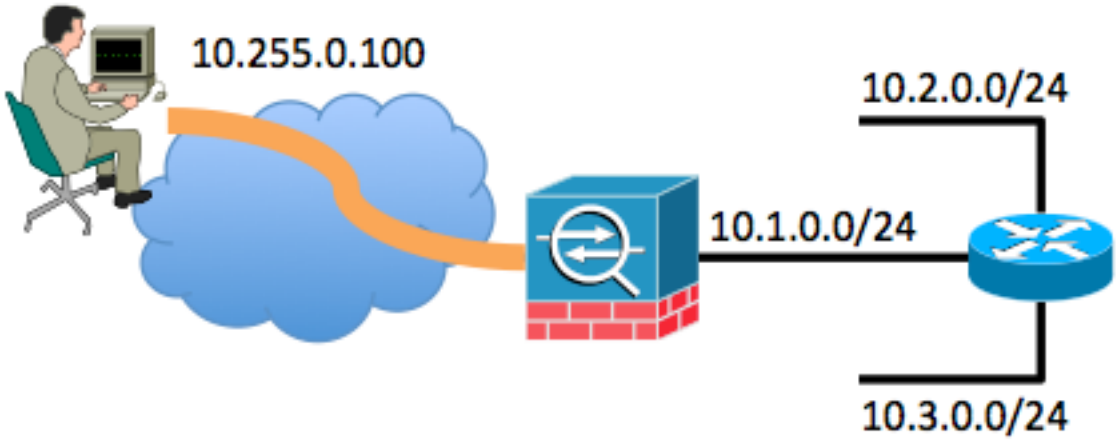
Ein weiteres Problem besteht darin, dass die ASA gezielte (Netzwerk-)Broadcast-Pakete (die durch Entfernen der VPN-Clients generiert werden) als Unicast-Frame an das interne Netzwerk weiterleiten kann. Dadurch wird das Paket möglicherweise an die ASA zurückgeleitet, wodurch es Schleifen erzeugt, bis die "Time to Live" (TTL) abläuft.

Dieses Dokument erläutert diese Probleme und zeigt, welche Konfigurationstechniken verwendet werden können, um das Problem zu vermeiden.

Problem: Pakete, die für eine nicht verbundene VPN-Client-Schleife im internen Netzwerk bestimmt sind

Wenn ein VPN-Benutzer mit Remote-Zugriff die Verbindung zu einer ASA-Firewall trennt, können die im internen Netzwerk vorhandenen Pakete (für diese getrennten Benutzer bestimmt) und die zugewiesene IP-VPN-Adresse im internen Netzwerk Loopback übertragen werden. Diese Paketschleifen können dazu führen, dass die CPU-Nutzung auf der ASA erhöht wird, bis die Schleife entweder aufgrund des IP-TTL-Werts im IP-Paket-Header auf 0 absinkt, oder der Benutzer eine erneute Verbindung herstellt und die IP-Adresse einem VPN-Client erneut zugewiesen wird.

Um dieses Szenario besser zu verstehen, sollten Sie folgende Topologie berücksichtigen:



In diesem Beispiel wurde dem Remotezugriffsclient die IP-Adresse 10.255.0.100 zugewiesen. Die ASA in diesem Beispiel ist zusammen mit einem Router mit demselben internen Netzwerksegment verbunden. Der Router hat zwei zusätzliche Layer-3-Netzwerksegmente verbunden. Die relevanten Schnittstellen- (Routing-) und VPN-Konfigurationen von ASA und Router sind in den Beispielen aufgeführt.

In diesem Beispiel werden die wichtigsten Punkte der ASA-Konfiguration dargestellt:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Die wichtigsten Punkte der Router-Konfiguration sind in diesem Beispiel dargestellt:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

In der Routing-Tabelle des Routers, der mit der ASA-Innenseite verbunden ist, wird einfach eine Standardroute auf die ASA-interne Schnittstelle 10.1.0.1 gezeigt.

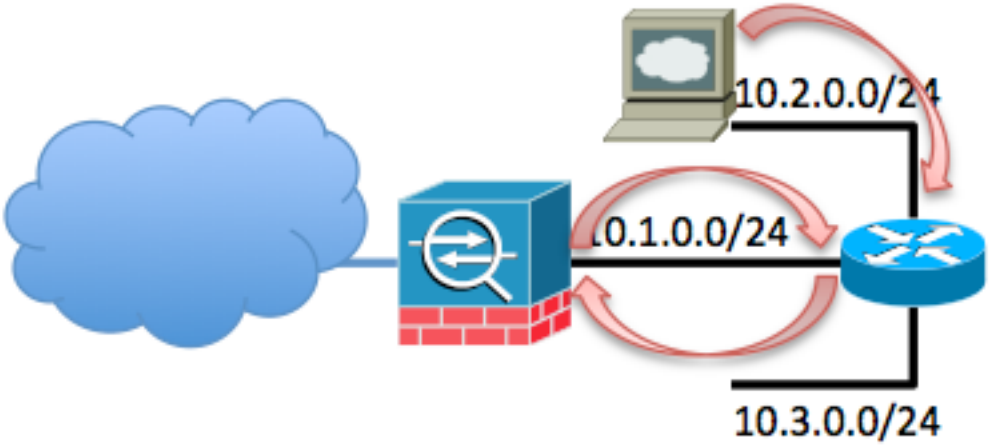
Während der Benutzer über VPN mit der ASA verbunden ist, wird in der ASA-Routing-Tabelle Folgendes angezeigt:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Das Problem tritt auf, wenn der VPN-Benutzer mit Remote-Zugriff vom VPN getrennt wird. An diesem Punkt wird die hostbasierte Route aus der ASA-Routing-Tabelle entfernt. Wenn ein Host im Netzwerk versucht, Datenverkehr an den VPN-Client zu senden, wird dieser Datenverkehr vom Router an die interne ASA-Schnittstelle weitergeleitet. Die folgenden Schritte werden durchgeführt:

1. Das für 10.255.0.100 bestimmte Paket kommt an der internen Schnittstelle der ASA an.
2. Standard-ACL-Prüfungen werden durchgeführt.
3. Die ASA-Routing-Tabelle wird überprüft, um die Ausgangsschnittstelle für diesen Datenverkehr zu bestimmen.
4. Das Ziel des Pakets entspricht der breiten 10.0.0.0/8-Route, die von der internen Schnittstelle zum Router zurückzeigt.
5. Die ASA überprüft, ob der Datenverkehr zum Pinning von Haaren zulässig ist. Sie sucht **in der Intra-Schnittstelle nach derselben Sicherheitsberechtigung** und stellt fest, dass diese zulässig ist.
6. Eine Verbindung wird von und zur internen Schnittstelle hergestellt, und das Paket wird als nächster Hop an den Router zurückgesendet.
7. Der Router empfängt ein Paket, das auf der ASA-Schnittstelle auf 10.255.0.100 festgelegt ist. Der Router überprüft seine Routing-Tabelle auf einen geeigneten nächsten Hop. Der Router stellt fest, dass der nächste Hop die ASA-interne Schnittstelle ist, und das Paket wird an die ASA gesendet.
8. Kehren Sie zu Schritt 1 zurück.

Ein Beispiel ist hier dargestellt:



Diese Schleife tritt auf, bis die TTL dieses Pakets auf 0 sinkt. Beachten Sie, dass die ASA Firewall bei der Verarbeitung eines Pakets den TTL-Wert **nicht** standardmäßig herabsetzt. Der Router senkt die TTL, wenn er das Paket weiterleitet. Dadurch wird das Auftreten dieser Schleife auf unbestimmte Zeit verhindert. Diese Schleife erhöht jedoch die Datenverkehrslast auf der ASA und führt zu einem Anstieg der CPU-Auslastung.

Problem: Von VPN-Clients generierte Directed (Netzwerk) Broadcast Packets werden in einem internen Netzwerk gepoopt

Dieses Problem ähnelt dem ersten Problem. Wenn ein VPN-Client ein lokales Broadcast-Paket an sein zugewiesenes IP-Subnetz generiert (im vorherigen Beispiel 10.255.0.255), kann dieses Paket von der ASA als Unicast-Frame an den internen Router weitergeleitet werden. Der interne Router leitet ihn dann möglicherweise zurück an die ASA, wodurch das Paket schleift, bis die TTL abläuft.

Diese Ereignisserie tritt auf:

1. Das VPN-Client-System generiert ein Paket, das für die Broadcast-Adresse des Netzwerks 10.255.0.255 bestimmt ist, und das Paket erreicht die ASA.
2. Die ASA behandelt dieses Paket als Unicast-Frame (aufgrund der Routing-Tabelle) und leitet es an den internen Router weiter.

3. Der interne Router, der das Paket auch als Unicast-Frame behandelt, senkt die TTL des Pakets und leitet es zurück an die ASA.

4. Der Prozess wiederholt sich, bis die TTL des Pakets auf 0 reduziert ist.

Problemlösung

Es gibt mehrere mögliche Lösungen für dieses Problem. Je nach Netzwerktopologie und der spezifischen Situation ist eine Lösung möglicherweise einfacher zu implementieren als eine andere.

Lösung 1 - Statische Route für Null0-Schnittstelle (ASA Version 9.2.1 und höher)

Wenn Sie Datenverkehr an eine **Null0-**Schnittstelle senden, werden die Pakete, die für das

angegebene Netzwerk bestimmt sind, verworfen. Diese Funktion ist hilfreich, wenn Sie RTBH (Remoremote Triggered Black Hole) für Border Gateway Protocol (BGP) konfigurieren. Wenn Sie in dieser Situation eine Route für das Subnetz des Clients für den Remote-Zugriff auf Null0 konfigurieren, wird die ASA gezwungen, Datenverkehr für Hosts in diesem Subnetz zu verwerfen, wenn keine spezifischere Route (bereitgestellt durch "Reverse Route Injection") vorhanden ist.

```
route Null0 10.255.0.0 255.255.255.0
```

Lösung 2 - Verwenden eines anderen IP-Pools für VPN-Clients

Bei dieser Lösung wird den Remote-VPN-Benutzern eine IP-Adresse zugewiesen, die sich nicht mit einem internen Netzwerk-Subnetz überschneidet. Dies würde verhindern, dass die ASA Pakete, die an dieses VPN-Subnetz gerichtet sind, zurück an den internen Router weiterleitet, wenn der VPN-Benutzer nicht verbunden war.

Lösung 3: Spezifische ASA-Routing-Tabelle für interne Routen

Diese Lösung soll sicherstellen, dass die Routing-Tabelle der ASA keine sehr breiten Routen enthält, die sich mit dem VPN-IP-Pool überschneiden. Für dieses spezielle Netzwerkbeispiel entfernen Sie die 10.0.0.0/8-Route von der ASA, und konfigurieren Sie spezifischere statische Routen für die Subnetze, die sich außerhalb der internen Schnittstelle befinden. Abhängig von der Anzahl der Subnetze und der Netzwerktopologie kann dies eine große Anzahl statischer Routen sein, was möglicherweise nicht möglich ist.

Lösung 4: Hinzufügen einer spezifischeren Route für das VPN-Subnetz, Back-Out von der externen Schnittstelle

Diese Lösung ist komplizierter als die anderen, die in diesem Dokument beschrieben werden. Cisco empfiehlt, dass Sie versuchen, die anderen Lösungen zuerst zu verwenden, da die in der Anmerkung weiter unten in diesem Abschnitt beschriebene Situation vorliegt. Diese Lösung soll verhindern, dass die ASA IP-Pakete, die vom VPN-IP-Subnetz stammen, an den internen Router zurücksendet. Sie können dies tun, wenn Sie über die externe Schnittstelle eine spezifischere Route für das VPN-Subnetz hinzufügen. Da dieses IP-Subnetz für externe VPN-Benutzer reserviert ist, sollten Pakete mit einer Quell-IP-Adresse aus diesem VPN-IP-Subnetz niemals an die interne ASA-Schnittstelle eingehen. Am einfachsten lässt sich dies erreichen, indem eine Route für den VPN-IP-Pool für den Remote-Zugriff von der externen Schnittstelle mit einer Next-Hop-IP-Adresse des Upstream-ISP-Routers hinzugefügt wird.

In diesem Beispiel für die Netzwerktopologie würde diese Route wie folgt aussehen:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Fügen Sie zusätzlich zu dieser Route den Befehl **ip verify reverse path inside** hinzu, damit die ASA alle eingehenden Pakete, die über die interne Schnittstelle eingehen, die vom VPN-IP-Subnetz stammen, aufgrund der bevorzugten Route, die auf der externen Schnittstelle vorhanden ist, verwirft:

```
ip verify reverse-path inside
```

Nachdem diese Befehle implementiert wurden, sieht die ASA-Routing-Tabelle bei der Verbindung mit dem Benutzer ähnlich aus:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Wenn der VPN-Client verbunden ist, wird die hostbasierte Route zu dieser VPN-IP-Adresse in der Tabelle angezeigt und bevorzugt. Wenn der VPN-Client die Verbindung trennt, wird der von der Client-IP-Adresse stammende Datenverkehr, der über die interne Schnittstelle eingeht, mit der Routing-Tabelle abgeglichen und aufgrund des Befehls **ip verifiziert, dass der umgekehrte Pfad innerhalb des** Befehls **vorhanden ist**.

Wenn der VPN-Client eine gezielte Netzwerk-Broadcast zum VPN IP-Subnetz generiert, wird dieses Paket an den internen Router weitergeleitet und vom Router an die ASA weitergeleitet, wo es aufgrund des Befehls **ip verify reverse path inside** verworfen wird.

> **Hinweis**: Wenn nach der Implementierung dieser Lösung der Befehl **derselbe** Befehl **für die Intra-Security-Berechtigung** in der Konfiguration vorhanden ist und die Zugriffsrichtlinien dies zulassen, kann Datenverkehr, der von einem VPN-Benutzer stammt und für einen Benutzer, der nicht verbunden ist, an eine IP-Adresse im VPN-IP-Pool gerichtet ist, in Klartext aus der externen Schnittstelle weitergeleitet werden. Dies ist eine seltene Situation, die durch die Verwendung von VPN-Filtern innerhalb der VPN-Richtlinie abgeschwächt werden kann. Diese Situation tritt nur ein, wenn der Befehl **derselbe** Befehl **für** die **Intra-Interface-**Berechtigung für **Sicherheit** in der Konfiguration der ASA vorhanden ist.
>
> Wenn interne Hosts Datenverkehr an eine IP-Adresse im VPN-Pool generieren und diese IP-Adresse keinem Remote-VPN-Benutzer zugewiesen ist, kann dieser Datenverkehr in Klartext an die Außenseite der ASA geleitet werden.