UDP-Datenverkehr durch ASA schlägt fehl, nachdem der primäre ISP-Link in einem Dual-ISP-Setup wieder online ist

Inhalt

[Einführung](#)
[Bevor Sie beginnen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Problem](#)
[Lösung](#)
[Zugehörige Informationen](#)

Einführung

Wenn eine Adaptive Security Appliance (ASA) über zwei Ausgangs-Schnittstellen pro Zielsubnetz verfügt und die bevorzugte Route zu einem Ziel für einige Zeit aus der Routing-Tabelle entfernt wird, können User Datagram Protocol (UDP)-Verbindungen ausfallen, wenn die bevorzugte Route der Routing-Tabelle erneut hinzugefügt wird. TCP-Verbindungen können ebenfalls von dem Problem betroffen sein. Da TCP jedoch Paketverluste erkennt, werden diese Verbindungen automatisch von den Endpunkten entfernt und mithilfe der optimalen Routen neu erstellt, sobald sich die Routen ändern.

Dieses Problem kann auch beobachtet werden, wenn ein Routing-Protokoll verwendet wird und eine Topologieänderung eine Änderung der Routing-Tabelle auf der ASA auslöst.

Bevor Sie beginnen

Anforderungen

Um diesem Problem zu begegnen, muss die Routing-Tabelle der ASA geändert werden. Dies ist bei dualen ISP-Links auf redundante Weise oder wenn die ASA Routen über ein IGP (OSPF, EIGRP, RIP) lernt.

Dieses Problem tritt auf, wenn die primäre ISP-Verbindung wieder online ist oder das genannte IGP eine Neukonvergenz erkennt, aufgrund derer eine weniger bevorzugte Route, die von der ASA verwendet wurde, durch die bevorzugte untermetrische Route ersetzt wird. In diesem Fall werden langlebige Verbindungen wie UDP SIP-Registrierungen, GRE usw. nach der Neuinstallation der primären oder bevorzugten Route in der Routing-Tabelle der ASA ausfallen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Alle Cisco Adaptive Security Appliances der Serie ASA 5500
- ASA-Versionen 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) und höher

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Problem

Wenn eine Routing-Tabelle aus der Routing-Tabelle der ASA entfernt wird und keine Routen aus einer Schnittstelle zum Erreichen eines Ziels vorhanden sind, werden von der ASA die über die Firewall mit diesem ausländischen Ziel erstellten Verbindungen gelöscht. Dies geschieht, damit die Verbindungen erneut über eine andere Schnittstelle mit Routingeinträgen für das vorhandene Ziel erstellt werden können.

Wenn der Tabelle jedoch spezifischere Routen hinzugefügt werden, werden die Verbindungen nicht aktualisiert, um die neuen, spezifischeren Routen zu verwenden, und es wird weiterhin die weniger optimale Schnittstelle verwendet.

Betrachten Sie zum Beispiel, dass die Firewall über zwei Schnittstellen verfügt, die mit dem Internet verbunden sind - "extern" und "backup" - und diese beiden Routen existieren in der ASA-Konfiguration:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Wenn sowohl die Außen- als auch die Backup-Schnittstellen "aktiv" sind, wird für ausgehende Verbindungen, die über die Firewall erstellt werden, die externe Schnittstelle verwendet, da die bevorzugte Metrik 1 ist. Wenn die externe Schnittstelle deaktiviert wird (oder die SLA-Überwachungsfunktion, die die Route verfolgt, einen Verbindungsverlust mit der verfolgten IP feststellt), werden Verbindungen über die externe Schnittstelle abgebrochen und mithilfe der Backup-Schnittstelle neu erstellt, da die Backup-Schnittstelle die einzige Schnittstelle mit einer Route zum Ziel ist.

Das Problem tritt auf, wenn die externe Schnittstelle wieder aktiviert wird oder die verfolgte Route wieder zur bevorzugten Route wird. Die Routing-Tabelle wird aktualisiert, um die ursprüngliche Route vorzuziehen. Bestehende Verbindungen bestehen jedoch weiterhin auf der ASA und durchlaufen die Backup-Schnittstelle. Sie werden NICHT gelöscht und auf der externen Schnittstelle mit der bevorzugten Metrik neu erstellt. Der Grund hierfür ist, dass die Backup-Standardroute in der schnittstellenspezifischen Routing-Tabelle der ASA noch vorhanden ist. Die Verbindung verwendet weiterhin die Schnittstelle mit der weniger bevorzugten Route, bis die Verbindung gelöscht wird. im Falle von UDP kann dies unbegrenzt sein.

Diese Situation kann Probleme bei langlebigen Verbindungen verursachen, wie z. B. externe SIP-Registrierungen oder andere UDP-Verbindungen.

Lösung

Um dieses spezifische Problem zu beheben, wurde der ASA eine neue Funktion hinzugefügt, durch die Verbindungen auf einer neuen Schnittstelle beendet und neu aufgebaut werden, wenn der Routing-Tabelle eine bevorzugte Route zum Ziel hinzugefügt wird. Um die Funktion zu aktivieren (standardmäßig deaktiviert), legen Sie ein Timeout von nicht null auf den Befehl **timeout Floating-conn** fest. Diese Zeitüberschreitung (in HH:MM:SS angegeben) gibt an, wie lange die ASA wartet, bevor die Verbindung beendet wird, sobald eine weitere bevorzugte Route der Routing-Tabelle wieder hinzugefügt wird:

Dies ist ein CLI-Beispiel für die Aktivierung der Funktion. Wenn mit dieser CLI ein Paket auf einer bestehenden Verbindung empfangen wird, für die es jetzt eine andere, bevorzugte Route zum Ziel gibt, wird die Verbindung 1 Minute später abgebrochen (und mithilfe der neuen, bevorzugten Route neu erstellt):

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

Diese Funktion wird der ASA-Plattform in den Versionen 8.2(5), 8.3(2)12, 8.4(1)1 und 8.5(1), einschließlich neuerer Versionen der ASA-Software, hinzugefügt.

Wenn Sie eine Version von ASA-Code ausführen, die diese Funktion nicht implementiert, besteht eine Problemumgehung darin, die UDP-Verbindungen, die weiterhin die weniger bevorzugte Route nutzen, manuell zu leeren, obwohl eine bessere Route über einen **klaren lokalen Host *<IP>*** **oder clear-conn *<IP>*** verfügbar ist.

Die Befehlsreferenz listet diese neue Funktion im Abschnitt **Timeout** auf.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems