ASA-Durchsatz und Verbindungsgeschwindigkeit Fehlerbehebung und Analyse der Paketerfassung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Probleme mit dem Durchsatz und der Verbindungsgeschwindigkeit der Cisco Adaptive Security Appliance (ASA) beheben können.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA).

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

Bei einigen Kunden kann es zu Problemen kommen, wenn sie zum ersten Mal eine ASA bereitstellen oder neue Verbindungen testen. Das Problem ist, dass der TCP-Durchsatz für

Verbindungen, die über die ASA laufen, viel niedriger ist als wenn sich die ASA nicht im Verbindungspfad befindet (oder die Verbindungen sind viel langsamer als vor der Implementierung der ASA im Netzwerk).

Beispielsweise könnte ein Kunde einen Low-End-D-Link-Router (oder ein anderes Routing-Gerät) durch eine ASA 5505 oder eine ASA 5510 ersetzen. Nach dem Austausch des Routers wird die Verbindungsgeschwindigkeit jedoch deutlich reduziert. Der Kunde kann beim Cisco TAC ein Ticket erstellen, da er der Ansicht ist, dass die ASA die Verbindungsgeschwindigkeit verringert hat.

Fehlerbehebungsmethode

TCP wird langsamer, wenn im Netzwerk Paketverluste oder Paketverzögerungen auftreten. Um die genaue Ursache des Problems zu ermitteln, müssen die Daten die tatsächlichen TCP-Pakete auf der Leitung für diese Verbindung und deren Auswirkungen auf das Netzwerk anzeigen. Normalerweise wird ein Netzwerkadministrator auf das Problem hingewiesen, wenn er eine bestimmte Aktion ausführt, z. B. eine FTP-Dateiübertragung oder einen Online-Geschwindigkeitstest. Oft kann das Problem reproduziert werden. Daher kann der Administrator die erforderlichen Daten sammeln, um die Ursache zu ermitteln.

Um die erforderlichen Daten zu erfassen, muss der Befehl **show tech** vor und nach dem Test von der ASA ausgeführt werden. Dieser Befehl zeigt Konfigurations- und Paketstatistiken an (hauptsächlich aus **der Anzeige von Service-Richtlinien**) und zeigt auch an, ob die Schnittstellenfehler inkrementiert werden.

Zur vollständigen Diagnose der Problemursache sind bidirektionale, gleichzeitige Paketerfassungen (basierend auf den beiden betroffenen ASA-Schnittstellen, die die Verbindung durchläuft) erforderlich.

In diesen Dokumenten finden Sie Beispiele für die Anwendung von Paketerfassungen auf die ASA:

- Fehlerbehebung bei Verbindungen über PIX und ASA
- TAC Security Podcast - Episode #1 - Verwenden des ASA-Paketerfassungs-Utility für die Fehlerbehebung

Datenanalyse

Nachdem Sie die erforderlichen Daten erfasst haben, können Sie mithilfe der Paketerfassungen ermitteln, welche der folgenden Probleme aufgetreten sein könnten:

- Die Pakete vom externen Host werden verworfen oder verzögert, bevor sie die externe ASA-Schnittstelle erreichen.
- Die Pakete werden von der ASA verzögert oder verworfen.
- Die Pakete werden irgendwo im internen Netzwerk verzögert oder verworfen.

  Hinweis: Bei dieser Analyse wird davon ausgegangen, dass die Daten von einem Host auf der externen Schnittstelle an einen Host auf der internen Schnittstelle gesendet werden.

Dieses Video zeigt ein Beispiel für die Durchführung der Analyse bei der Paketerfassung:

Die TCP-Stream-Kodierung ist ein technischer Aspekt, der speziell auf dieses Problem zugeschnitten ist, da die Firewall bei der Aktivierung bestimmter Funktionen auf der ASA den TCP-Stream, der sie durchläuft, vollständig kodiert.

Wenn die ASA z. B. ein fehlendes Paket im Netzwerk erkennt (da es nicht bei der ASA empfangen wird), sendet sie eine ACK für den anderen TCP-Endpunkt, um die fehlenden Daten zu erhalten. Dieses Szenario ist am häufigsten. Wenn die ASA Pakete erkennt, die nicht in der richtigen Reihenfolge ankommen, ordnet die ASA die Pakete neu und leitet sie an den Empfänger weiter. Wenn es keine Netzwerkverluste oder Paketumstellungen gibt, hat die Aktivierung dieser Funktion keine Nebenwirkungen. Wenn alle Pakete, die von einem TCP-Endpunkt gesendet wurden, erfolgreich über das Netzwerk und die ASA weitergeleitet wurden, wissen Sie nicht, dass diese Funktion aktiviert ist, da sie keine Aktionen für die Paketflüsse ausführt. Nur wenn Probleme mit der TCP-Verbindung im Netzwerk auftreten, wird diese Funktion den Netzwerkverkehr weiter verlangsamen. Die Kodierung des TCP-Streams ist für die ASA sehr ressourcenintensiv. Für jedes im Netzwerk verworfene Paket muss die ASA nicht nur eine TCP-Paketanforderung für die erneute Übertragung des Pakets senden, sondern auch die Pakete puffern, die der Absender nach dem Verfehlen des Pakets weiterhin sendet.

Häufige Probleme

Falsch konfigurierte Geschwindigkeits- und Duplex-Werte auf der Schnittstelle, die ASA mit benachbarten Geräten verbindet

Dieses Problem tritt häufig auf, wenn ein Gerät durch ein ASA-Gerät ersetzt wird. Wenn die Geschwindigkeits- und Duplexwerte der ASA-Schnittstelle nicht mit den Werten auf dem benachbarten Gerät übereinstimmen, treten Paketverluste auf dieser Schnittstelle auf. Überprüfen Sie die Geschwindigkeits- und Duplexwerte der ASA-Schnittstelle und der angrenzenden Schnittstelle.

Prüfen Sie die Ausgabe der **show interface** der ASA auf offensichtliche Fehler, die Symptome dieses Problems sind:

```
Interface Ethernet0/0 "Outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0019.2f58.c324, MTU 1500
IP address 192.168.222.122, subnet mask 255.255.255.252
124047996 packets input, 35340918453 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
156918660 packets output, 40931551514 bytes, 0 underruns
1 output errors, 4286634 collisions, 0 interface resets
0 babbles, 123332 late collisions, 4752834 deferred
0 lost carrier, 0 no carrier
input queue (curr/max blocks): hardware (0/0) software (0/0)
output queue (curr/max blocks): hardware (0/245) software (0/0)
Traffic Statistics for "Outside":
124047995 packets input, 33107957301 bytes
157041993 packets output, 38195084709 bytes
103480 packets dropped
1 minute input rate 2140 pkts/sec, 477200 bytes/sec
1 minute output rate 2630 pkts/sec, 396763 bytes/sec
1 minute drop rate, 0 pkts/sec
```

```
5 minute input rate 2152 pkts/sec, 525496 bytes/sec
5 minute output rate 2701 pkts/sec, 421215 bytes/sec
5 minute drop rate, 0 pkts/sec
```

Datenverkehr an IPS-Modul senden

Wenn die ASA so konfiguriert ist, dass Datenverkehr an das IPS-Modul gesendet wird, wird die TCP-Stream-Koalisierungsfunktion auf der ASA aktiviert. Weitere Informationen zur Funktion zum Zusammenführen von TCP-Streams finden Sie im Abschnitt *Datenanalyse* dieses Dokuments.

ASA-Änderung der TCP-MSS-Option führt zu geringer Leistungsminderung

Standardmäßig legt die ASA die TCP-MSS-Option in den SYN-Paketen auf 1380 fest. TCP-Endpunkte sollten daher kein TCP-Segment mit mehr als 1380 Byte übertragen. Dieser Wert ist niedriger als der oft voreingestellte Wert von 1460 Byte und stellt einen TCP-Leistungsrückgang von etwa sechs Prozent (6 %) dar. Die Leistung kann sich verbessern, wenn Sie die maximale MSS-Einstellung auf der ASA erhöhen oder die MSS-Anpassung deaktivieren. Bevor Sie den Standardbefehl auf der ASA ändern, sollten Sie sich über die Risiken im Zusammenhang mit der potenziellen Fragmentierung informieren, wenn das Paket weiter in den Pfad eingekapselt wird.

Weitere Informationen finden Sie im Abschnitt sysopt connection tcpmss der *Befehlsreferenz zur Cisco Serie ASA 5500*.

Zugehörige Informationen

- Cisco ASA 5500 Series Command Reference, 8.2
- Technischer Support und Dokumentation - Cisco Systems