Verwendung von CAR bei DOS-Angriffen

Inhalt

Einführung

Manchmal erhält ein Netzwerk neben dem regulären Netzwerkverkehr einen Stream von DoS-Angriffspaketen. In solchen Situationen können Sie einen Mechanismus namens "Ratenbegrenzung" verwenden, um eine Beeinträchtigung der Netzwerkleistung zu ermöglichen, sodass das Netzwerk aktiv bleibt. Sie können die Cisco IOS® Software verwenden, um eine Ratenbegrenzung zu erreichen:

- Committed Access Rate (CAR)
- Traffic Shaping
- Shaping und Richtlinienvergabe über modulare QoS-CLI (Quality of Service Command Line Interface)

In diesem Dokument wird CAR zur Verwendung bei DoS-Angriffen behandelt. Die anderen Schemata sind nur Varianten des Grundkonzepts.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Software Release 11.1CC und 12.0 Mainline, die CAR unterstützen.
- Cisco IOS Software, Version 11.2 und höher, die Traffic Shaping unterstützt.
- Cisco IOS Software-Versionen 12.0XE, 12.1E und 12.1T, die modulare QoS-CLI unterstützen.

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Übertragungsratenlimit - ICMP/Smurf

Konfigurieren Sie diese Zugriffslisten:

```
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

```
interface <interface> <interface #>
  rate-limit input access-group 102 256000 8000 8000 conform-action transmit
  exceed-action drop
```

Um CAR zu aktivieren, müssen Sie Cisco Express Forwarding (CEF) im Paket aktivieren. Darüber hinaus müssen Sie eine CEF-Switched-Schnittstelle für CAR konfigurieren.

Die Beispielausgabe verwendet Bandbreitenwerte für DS3-Bandbreiten. Wählen Sie Werte basierend auf der Schnittstellenbandbreite und der Geschwindigkeit aus, mit der Sie eine bestimmte Art von Datenverkehr begrenzen möchten. Für kleinere Eingangsschnittstellen können Sie niedrigere Raten konfigurieren.

Übertragungsratenlimit TCP-SYN-Pakete

11.1(X)CC

Wenn Sie wissen, welcher Host angegriffen wird, konfigurieren Sie diese Zugriffslisten:

```
access-list 103 deny tcp any host 10.0.0.1 established
```

```
!--- Let sessions in progress run. access-list 103 permit tcp any host 10.0.0.1 !--- Rate limit
the initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 103
8000 8000 8000 conform-action transmit exceed-action drop
```

Hinweis: In diesem Beispiel ist der von einem Angriff betroffene Host 10.0.0.1.

Wenn Sie nicht wissen, welcher Host unter einem DoS-Angriff steht, und ein Netzwerk schützen möchten, konfigurieren Sie die folgenden Zugriffslisten:

```
access-list 104 deny tcp any any established
!--- Let sessions in progress run. access-list 104 permit tcp any any !--- Rate limit the
initial TCP SYN packet, because the other packets !--- in the TCP session would have hit the
earlier entry in the ACL. interface <interface> <interface #> rate-limit input access-group 104
64000 8000 8000 conform-action transmit exceed-action drop
```

Hinweis: Übertragungsratenlimit von 64.000 bps für alle TCP-SYN-Pakete.

12.0(X)[S/T/M]

Wenn Sie wissen, welcher Host angegriffen wird, konfigurieren Sie diese Zugriffslisten:

```
access-list 105 permit tcp any host 10.0.0.1 syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 105 8000 8000 8000 conform-action transmit exceed-action drop
```

Hinweis: In diesem Beispiel ist 10.0.0.1 der Host, der angegriffen wird.

Wenn Sie nicht sicher sind, welcher Host angegriffen wird, und ein Netzwerk schützen möchten, konfigurieren Sie die folgenden Zugriffslisten:

```
access-list 106 permit tcp any any syn
!--- Remember that your interest lies in syn packets only. interface <interface> <interface #>
rate-limit input access-group 106 64000 8000 8000 conform-action transmit exceed-action drop
```

Hinweis: Übertragungsratenlimit von 64.000 bps für alle TCP-SYN-Pakete.

CAR - Häufig gestellte Fragen

Wie werden die Werte identifiziert, die für die CAR-Regeln verwendet werden sollen, um SYN-Pakete zu begrenzen?

Machen Sie sich mit Ihrem Netzwerk vertraut. Der Datenverkehrstyp bestimmt die Anzahl der aktiven TCP-Sitzungen für eine bestimmte Datenmenge.

- Der WWW-Datenverkehr weist eine deutlich höhere Mischung von TCP-SYN-Paketen auf als der FTP-Serverfarm-Datenverkehr.
- PC-Client-Stacks erkennen tendenziell mindestens alle anderen TCP-Pakete an. Andere Stacks können seltener oder häufiger bestätigen.
- Überprüfen Sie, ob Sie diese CAR-Regeln am Edge für Privatkunden oder am Edge des Kundennetzwerks anwenden müssen.

```
users ---- { ISP } --- web farm
```

Für WWW gibt es den Datenverkehrsmix:

Für jede 5.000-Datei, die Sie von der Webfarm herunterladen, erhält die Webfarm 560 Byte, wie hier gezeigt:

- 80 Byte [SYN, ACK]
- 400 Byte [HTTP-Struktur mit 320 Byte, 2 ACKs]
- 80 Byte [FIN, ACK]

Angenommen, das Verhältnis zwischen ausgehendem Datenverkehr von der Webfarm zum eingehenden Datenverkehr von der Webfarm beträgt 10:1. Die Menge des Datenverkehrs, aus dem SYN-Pakete bestehen, beträgt 120:1.

Wenn Sie über einen OC3 Link verfügen, begrenzen Sie die TCP-SYN-Paketrate auf 155 Mbit/s / 120 = 1,3 Mbit/s.

Konfigurieren Sie auf der Eingangsschnittstelle des Webfarm-Routers Folgendes:

```
rate-limit input access-group 105 1300000 256000 256000 conform-action transmit
exceed-action drop
```

Die TCP-SYN-Paketrate wird kleiner, wenn die Länge Ihrer TCP-Sitzungen länger wird.

```
users ---- { ISP } --- MP3/FTP Farm
```

MP3-Dateien haben im Durchschnitt eine Größe von 4 bis 5 Mbit/s. Beim Herunterladen einer 4-Mbit/s-Datei wird ein Datenverkehr von 3160 Byte erzeugt:

- 80 Byte [SYN, ACK]
- 3.000 Byte [ACKs + FTP get]
- 80 Byte [FIN, ACK]

Die Geschwindigkeit der TCP-SYNs für den ausgehenden Datenverkehr beträgt 155 Mbit/s / 12.000 = 1,3 Kbit/s.

Konfigurieren:

```
 rate-limit input access-group 105 1300 1200 1200 conform-action transmit
exceed-action drop
```

Woher weiß ich, ob ich zu viele SYN-Pakete einschränken kann?

Wenn Sie Ihre übliche Verbindungsrate auf Ihren Servern kennen, können Sie die Zahlen vor und nach der Aktivierung der CAR vergleichen. Mithilfe des Vergleichs können Sie feststellen, dass die Verbindungsrate abnimmt. Wenn die Rate sinkt, erhöhen Sie die CAR-Parameter, um weitere Sitzungen zuzulassen.

Überprüfen Sie, ob Benutzer problemlos TCP-Sitzungen einrichten können. Wenn Ihre CAR-Grenzwerte zu restriktiv sind, müssen Benutzer mehrere Versuche unternehmen, um eine TCP-Sitzung einzurichten.

Kann ich CAR auf einem Gigabit Switch Router (GSR) aktivieren?

Ja. Line Cards der Engine 0 und Engine 1 unterstützen CAR. Cisco IOS Software Release 11.2(14)GS2 und höher bieten CAR-Unterstützung. Die Auswirkungen der CAR auf die Leistung hängen von der Anzahl der CAR-Regeln ab, die Sie anwenden.

Die Auswirkungen auf die Leistung sind auch bei Line Cards der Engine 1 größer als bei Line Cards der Engine 0. Wenn Sie CAR auf Engine 0 Line Cards aktivieren möchten, müssen Sie die Cisco Bug ID CSCdp80432 kennen (nur registrierte Kunden). Wenn Sie die CAR aktivieren möchten, um Multicast-Datenverkehr zu begrenzen, stellen Sie sicher, dass die Cisco Bug-ID CSCdp32913 (nur registrierte Kunden) Sie nicht beeinträchtigt. Die Cisco Bug-ID CSCdm56071 (nur registrierte Kunden) ist ein weiterer Bug, über den Sie Bescheid wissen müssen, bevor Sie CAR aktivieren.

Kann ich die verteilte CAR (dCAR) auf einem Cisco 7500 aktivieren?

Ja, die RSP/VIP-Plattform unterstützt dCAR in der Cisco IOS Software-Version 11.1(20)CC und allen 12.0-Softwareversionen.

CAR wirkt sich bis zu einem gewissen Grad auf die Leistung aus. Basierend auf der CAR-Konfiguration können Sie eine Leitungsrate [für Internet-Mix-Datenverkehr] mit einem VIP2-50 [durch dCAR] auf einem OC3 erreichen. Stellen Sie sicher, dass die Cisco Bug-ID CSCdm56071 (nur registrierte Kunden) Sie nicht beeinträchtigt. Wenn Sie die CAR der Ausgabe verwenden möchten, kann die Cisco Bug-ID CSCdp52926 (nur registrierte Kunden) Ihre Konnektivität beeinträchtigen. Wenn Sie dCAR aktivieren, kann die Cisco Bug-ID CSCdp58615 (nur registrierte Kunden) einen VIP-Absturz verursachen.

Kann ich CAR auf einem Cisco 7200 aktivieren?

Ja. Der NPE unterstützt CAR in der Cisco IOS Software-Version 11.1(20)CC und allen 12.0-Softwareversionen.

CAR wirkt sich in gewissem Umfang auf die Leistung aus, basierend auf der CAR-Konfiguration. Behebung dieser Bugs: Cisco Bug ID CSCdm85458 (nur registrierte Kunden) und Cisco Bug ID CSCdm56071 (nur registrierte Kunden).

Hinweis: Eine große Anzahl von CAR-Einträgen in einer Schnittstelle/Subschnittstelle beeinträchtigt die Leistung, da der Router eine lineare Suche in den CAR-Anweisungen durchführen muss, um die übereinstimmende "CAR"-Anweisung zu finden.

Weitere Funktionen und Alternativen

IP Receive-ACL

Die Cisco IOS Softwareversion 12.0(22)S enthält die IP Receive ACL-Funktion auf dem Cisco Internet Router der Serie 12000.

Die IP Receive ACL-Funktion bietet grundlegende Filter für Datenverkehr, der zum Erreichen des Routers bestimmt ist. Der Router kann den Datenverkehr des Routing-Protokolls mit hoher Priorität vor einem Angriff schützen, da die Funktion alle ACLs (Input Access Control List) an der Eingangs-Schnittstelle filtert. Die IP Receive ACL-Funktion filtert den Datenverkehr auf den verteilten Linecards, bevor der Routingprozessor Pakete empfängt. Mit dieser Funktion können Benutzer DoS-Floods (Denial of Service) auf den Router filtern. Daher verhindert diese Funktion

eine Leistungsminderung des Routingprozessors.

Weitere Informationen finden Sie unter IP Receive APL.

IP Source Tracker

Cisco IOS Software Release 12.0(21)S unterstützt die IP Source Tracker-Funktion auf dem Cisco Internet Router der Serie 12000. Cisco IOS Software Release 12.0(22)S unterstützt diese Funktion auf dem Cisco Router der Serie 7500.

Mit der IP Source Tracker-Funktion können Sie Informationen über den Datenverkehr sammeln, der zu einem Host fließt, von dem Sie vermuten, dass dieser angegriffen wird. Mit dieser Funktion können Sie auch Angriffe einfach bis zum Eintrittspunkt im Netzwerk zurückverfolgen. Wenn Sie über diese Funktion den Netzwerkeingangspunkt identifizieren, können Sie ACLs oder CAR verwenden, um den Angriff effektiv zu blockieren.

Weitere Informationen finden Sie im IP Source Tracker.

Zugehörige Informationen

- Schutz des Netzwerks vor dem Nimda-Virus
- IP Receive-APL
- IP Source Tracker
- Technischer Support und Dokumentation - Cisco Systems