Cisco IOS Classic Firewall/IPS: Konfigurieren der kontextbasierten Zugriffskontrolle (CBAC) für Denial-of-Service-Schutz

Inhalt

Einführung

Dieses Dokument beschreibt das Abstimmungsverfahren für DoS-Parameter (Denial of Service) in der Cisco IOS® Classic Firewall mit CBAC.

CBAC bietet erweiterte Funktionen zur Datenverkehrsfilterung und kann als integraler Bestandteil Ihrer Netzwerk-Firewall verwendet werden.

DoS bezieht sich im Allgemeinen auf Netzwerkaktivitäten, die Netzwerkressourcen wie WAN-Verbindungsbandbreite, Firewall-Verbindungstabellen, End-Host-Speicher, CPU oder Servicefunktionen bewusst oder unbeabsichtigt überfordern. Im schlimmsten Fall überfordert die DoS-Aktivität die anfällige (oder zielgerichtete) Ressource so weit, dass die Ressource nicht mehr verfügbar ist, und untersagt die WAN-Verbindung oder den Dienstzugriff für berechtigte Benutzer.

Die Cisco IOS Firewall kann zur Eindämmung von DoS-Aktivitäten beitragen, wenn sie Zähler für die Anzahl der halb offenen TCP-Verbindungen sowie die Gesamtverbindungsrate über die Firewall und die Intrusion Prevention-Software in der klassischen Firewall (**ip inspect**) und der zonenbasierten Firewall beibehält.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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 (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Half-open-Verbindungen sind TCP-Verbindungen, die den dreiteiligen SYN-SYN/ACK-ACK-Handshake nicht abgeschlossen haben, der immer von TCP-Peers verwendet wird, um die Parameter ihrer gegenseitigen Verbindung auszuhandeln. Eine große Anzahl an halb offenen Verbindungen kann auf schädliche Aktivitäten wie DoS- oder DDoS-Angriffe (Distributed Denial-of-Service) hinweisen. Ein Beispiel für einen DoS-Angriff ist eine bösartige, absichtlich entwickelte Software, wie Würmer oder Viren, die mehrere Hosts im Internet infizieren und versuchen, bestimmte Internet-Server mit SYN-Angriffen zu überlasten, bei denen eine große Anzahl von SYN-Verbindungen von mehreren Hosts im Internet oder im privaten Netzwerk einer Organisation an einen Server gesendet werden. SYN-Angriffe stellen eine Gefahr für Internetserver dar, da die Verbindungstabellen der Server mit "betrügerischen" SYN-Verbindungsversuchen geladen werden können, die schneller eintreffen, als der Server mit den neuen Verbindungen umgehen kann. Dies ist eine Art von DoS-Angriff, da die große Anzahl von Verbindungen in der TCP-Verbindungsliste des angegriffenen Servers einen legitimen Benutzerzugriff auf die angegriffenen Internetserver verhindert.

Cisco IOS Firewall betrachtet User Datagram Protocol (UDP)-Sitzungen mit Datenverkehr in nur einer Richtung auch als "halb offen", da viele Anwendungen, die UDP für den Transport verwenden, den Empfang von Daten bestätigen. UDP-Sitzungen ohne Rückgabeverkehr deuten wahrscheinlich auf DoS-Aktivitäten oder Verbindungsversuche zwischen zwei Hosts hin, wenn einer der Hosts nicht mehr reagiert. Viele Arten von UDP-Datenverkehr, z. B. Protokollmeldungen, SNMP-Netzwerkmanagement-Datenverkehr, Streaming von Sprach- und Videomedien und Signalisierungsverkehr, verwenden zur Übertragung des Datenverkehrs nur Datenverkehr in eine Richtung. Viele dieser Arten von Datenverkehr wenden anwendungsspezifische Informationen an, um zu verhindern, dass sich unidirektionale Datenverkehrsmuster negativ auf das Firewall- und IPS-DoS-Verhalten auswirken.

Vor der Cisco IOS Software-Version 12.4(11)T und 12.4(10) bot Cisco IOS Stateful Packet Inspection standardmäßig Schutz vor DoS-Angriffen, wenn eine Überprüfungsregel angewendet wurde. In der Cisco IOS Softwareversion 12.4(11)T und 12.4(10) wurden die Standard-DoS-Einstellungen so geändert, dass der DoS-Schutz nicht automatisch angewendet wird, die Verbindungsaktivitätszähler jedoch weiterhin aktiv sind. Wenn der DoS-Schutz aktiv ist, d. h. wenn die Standardwerte bei älteren Softwareversionen verwendet werden oder die Werte auf den Bereich angepasst wurden, der den Datenverkehr beeinflusst, wird der DoS-Schutz auf der

Schnittstelle aktiviert, auf der die Überprüfung angewendet wird, in der Richtung, in der die Firewall angewendet wird, damit die Firewall-Richtlinienkonfigurationsprotokolle überprüft werden. Der DoS-Schutz ist nur dann im Netzwerkverkehr aktiviert, wenn der Datenverkehr eine Schnittstelle betritt oder verlässt, deren Prüfung in der gleichen Richtung des ursprünglichen Datenverkehrs (SYN-Paket oder erstes UDP-Paket) für eine TCP-Verbindung oder UDP-Sitzung durchgeführt wird.

Die Cisco IOS Firewall Inspection bietet verschiedene einstellbare Werte, um den Schutz vor DoS-Angriffen zu gewährleisten. Cisco IOS Software-Versionen vor 12.4(11)T und 12.4(10) verfügen über Standard-DoS-Werte, die den ordnungsgemäßen Netzwerkbetrieb stören können, wenn sie nicht für die entsprechende Netzwerkaktivität in Netzwerken konfiguriert sind, in denen die Verbindungsraten die Standardwerte überschreiten. Mit diesen Parametern können Sie die Punkte konfigurieren, an denen der DoS-Schutz Ihres Firewall-Routers wirksam wird. Wenn die DoS-Zähler Ihres Routers die standardmäßigen oder konfigurierten Werte überschreiten, setzt der Router für jede neue Verbindung, die die konfigurierten Höchstwerte für unvollständige oder einminütige Verbindungen überschreitet, eine alte halb offene Verbindung zurück, bis die Anzahl der Sitzungen unter die maximal unvollständigen niedrigen Werte fällt. Der Router sendet eine Syslog-Meldung, wenn die Protokollierung aktiviert ist und ein Intrusion Prevention System (IPS) auf dem Router konfiguriert ist, sendet der Firewall-Router eine DoS-Signaturmeldung über Security Device Event Exchange (SDEE). Wenn die DoS-Parameter nicht an das normale Verhalten Ihres Netzwerks angepasst sind, kann eine normale Netzwerkaktivität den DoS-Schutzmechanismus auslösen, der Anwendungsfehler, eine schlechte Netzwerkleistung und eine hohe CPU-Auslastung auf dem Cisco IOS Firewall-Router verursacht.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Denial-of-Service-Tuning für Cisco IOS Software Classic (IP Inspect) Firewall und Intrusion Prevention System

Die klassische Cisco IOS Firewall unterhält eine globale Gruppe von DoS-Zählern für den Router, und alle Firewall-Sitzungen für alle Firewall-Richtlinien auf allen Schnittstellen werden auf die globalen Firewalls-Zähler angewendet.

Cisco IOS Classic Firewall Inspection bietet standardmäßig Schutz vor DoS-Angriffen, wenn eine klassische Firewall angewendet wird. Der DoS-Schutz ist für alle Dienste oder Protokolle, für die die Firewall-Richtlinie konfiguriert ist, an allen Schnittstellen aktiviert, an denen die Überprüfung angewendet wird, und zwar in der Richtung, in der die Firewall angewendet wird. Die klassische Firewall bietet verschiedene einstellbare Werte, um sich vor DoS-Angriffen zu schützen. Die in Tabelle 1 gezeigten Legacy-Standardeinstellungen (aus Software-Images vor Version 12.4(11)T) können den ordnungsgemäßen Netzwerkbetrieb beeinträchtigen, wenn sie nicht für die entsprechende Netzwerkaktivität in Netzwerken konfiguriert sind, in denen die Verbindungsraten die Standardwerte überschreiten. Die DoS-Einstellungen können mit dem Befehl exec **show ip inspect config** angezeigt werden, und die Einstellungen sind in der Ausgabe von **sh ip inspect all** enthalten.

CBAC legt mithilfe von Timeouts und Schwellenwerten fest, wie lange die Zustandsinformationen für eine Sitzung verwaltet werden müssen, und wann Sitzungen, die nicht vollständig eingerichtet sind, verworfen werden sollen. Diese Zeitüberschreitungen und Schwellenwerte gelten global für alle Sitzungen.

Tabelle 1: Standard-DoS-Schutzbeschränkungen für klassische Firewall		
Vorteile des DoS-Schutzes	**vor 12.4(11)T/12.4(10)**	**12.4(11)T/12.4(10) und spätere Version**
max. unvollständiger hoher *Wert*	500	Unbegrenzt
max-unvollständiger niedriger *Wert*	400	Unbegrenzt
ein Minute hoher *Wert*	500	Unbegrenzt
einminütiger niedriger *Wert*	400	Unbegrenzt
tcp max-unvollständiger Host-*Wert*	50	Unbegrenzt

Router, die für die Anwendung der Cisco IOS VRF-kompatiblen Firewall konfiguriert sind, verwalten für jede VRF-Instanz einen Zählersatz.

Der Zähler für "ip inspect one minute high" und "ip inspect one minute low" behält eine Summe aller Verbindungsversuche im TCP-, UDP- und Internet Control Message Protocol (ICMP) innerhalb der vorherigen Minute des Betriebs des Routers bei, unabhängig davon, ob die Verbindungen erfolgreich waren oder nicht. Eine steigende Verbindungsrate kann auf eine Wurminfektion in einem privaten Netzwerk oder einen versuchten DoS-Angriff auf einen Server hinweisen.

Sie können den DoS-Schutz Ihrer Firewall zwar nicht "deaktivieren", den DoS-Schutz jedoch so anpassen, dass er nicht wirksam wird, es sei denn, in der Sitzungstabelle des Firewall-Routers sind sehr viele halb offene Verbindungen vorhanden.

DoS-Firewall-Schutz

Gehen Sie folgendermaßen vor, um den DoS-Schutz Ihrer Firewall an die Aktivität Ihres Netzwerks anzupassen:

1. Stellen Sie sicher, dass Ihr Netzwerk nicht mit Viren oder Würmern infiziert ist, die zu irrtümlich großen halb offenen Verbindungswerten oder versuchter Verbindungsrate führen können. Wenn Ihr Netzwerk nicht "sauber" ist, gibt es keine Möglichkeit, den DoS-Schutz Ihrer Firewall korrekt anzupassen. Sie müssen die Aktivitäten Ihres Netzwerks innerhalb eines Zeitraums beobachten, der für Sie typisch ist. Wenn Sie die DoS-Schutzeinstellungen Ihres Netzwerks innerhalb einer Zeit geringer oder inaktiver Netzwerkaktivität anpassen, übersteigen die normalen Aktivitätsstufen wahrscheinlich die DoS-Schutzeinstellungen.

2. Legen Sie die maximal unvollständigen hohen Werte auf sehr hohe Werte fest:

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

   Dies verhindert, dass der Router einen DoS-Schutz bietet, während Sie die Verbindungsmuster Ihres Netzwerks beobachten. Wenn Sie den DoS-Schutz deaktiviert lassen möchten, beenden Sie dieses Verfahren jetzt.**Hinweis:** Wenn auf Ihrem Router die Cisco IOS-Softwareversion 12.4(11)T oder höher oder Version 12.4(10) oder höher ausgeführt wird, müssen Sie die Standard-DoS-Schutzwerte nicht erhöhen. Sie sind bereits standardmäßig auf ihre Höchstgrenzen festgelegt.**Hinweis:** Wenn Sie den aggressiveren TCP-Host-spezifischen Denial-of-Service-Schutz aktivieren möchten, der die Blockierung der Verbindungsauslösung für einen Host umfasst, müssen Sie die im Befehl **ip inspect tcp max-uncomplete host** angegebene Blockzeit festlegen.
3. Löschen Sie die Statistiken der Cisco IOS-Firewall mit dem folgenden Befehl:

```
show ip inspect statistics reset
```

4. Lassen Sie den Router für eine gewisse Zeit, vielleicht 24 bis 48 Stunden, so können Sie das Netzwerkmuster über mindestens einen ganzen Tag des typischen Netzwerkaktivitätszyklus beobachten.**Hinweis:** Obwohl die Werte auf sehr hohe Werte angepasst werden, profitiert Ihr Netzwerk nicht von Cisco IOS Firewall- oder IPS DoS-Schutz.
5. Überprüfen Sie nach dem Beobachtungszeitraum die DoS-Zähler mit dem folgenden Befehl:

```
show ip inspect statistics
```

   Die Parameter, die Sie beachten müssen, um den DoS-Schutz anzupassen, sind **fett** hervorgehoben:

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. Konfigurieren Sie **ip inspect max-uncomplete high** auf einen Wert, der um 25 Prozent höher ist als der angegebene Wert für die maximale Anzahl von Sitzungen, die halb offen sind, in

Ihrem Router. Ein 1,25-Multiplikator bietet 25 Prozent mehr Reserven als beobachtetes Verhalten, z. B.:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

Konfigurieren:

```
router(config)
   #ip inspect max-incomplete high 70
```

Hinweis: Dieses Dokument beschreibt die Verwendung eines Multiplikators, der dem 1,25-fachen der typischen Aktivität Ihres Netzwerks entspricht, um Beschränkungen für den DoS-Schutz festzulegen. Wenn Sie Ihr Netzwerk innerhalb typischer Netzwerkaktivitäts-Peaks beobachten, muss dies genügend Reserven bereitstellen, um die Aktivierung des DoS-Schutzes des Routers unter allen, aber ungewöhnlichen Umständen zu vermeiden. Wenn in Ihrem Netzwerk regelmäßig große Mengen legitimer Netzwerkaktivitäten verzeichnet werden, die diesen Wert überschreiten, aktiviert der Router die DoS-Schutzfunktionen, die negative Auswirkungen auf einen Teil des Netzwerkverkehrs haben können. Sie müssen Ihre Router-Protokolle auf Erkennungen von DoS-Aktivitäten überwachen und die **ip inspect max-uncomplete high** und/oder **ip inspect one minute** limits anpassen, um die Auslösung von DoS zu vermeiden, nachdem Sie festgestellt haben, dass die Einschränkungen durch legitime Netzwerkaktivität erreicht wurden. Sie können die DoS-Schutzanwendung durch das Vorhandensein von Protokollmeldungen wie den folgenden erkennen:

7. Konfigurieren Sie **ip inspect max-uncomplete low** auf den Wert, den der Router für die maximale Anzahl an Sitzungen angezeigt hat, halb offen, z. B.:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   ```

   Konfigurieren:

   ```
   router(config)
      #ip inspect max-incomplete low 56
   ```

8. Der Zähler für die **IP-Prüfung** behält **eine Minute** hoch und **eine Minute tief** eine Summe aller Verbindungsversuche im TCP-, UDP- und Internet Control Message Protocol (ICMP)-Bereich innerhalb der vorherigen Minute des Router-Betriebs bei, unabhängig davon, ob die Verbindungen erfolgreich waren oder nicht. Eine steigende Verbindungsrate kann ein Hinweis auf eine Wurminfektion in einem privaten Netzwerk oder einen versuchten DoS-Angriff auf einen Server sein. In den Ausgaben 12.4(11)T und 12.4(10) der **show ip inspect-Statistiken** wurde eine zusätzliche Inspektionsstatistik hinzugefügt, um das hohe Wasserzeichen für die Sitzungserstellungsrate aufzuzeigen. Wenn Sie eine Cisco IOS Software-Version vor 12.4(11)T oder 12.4(10) ausführen, enthält die Überprüfungsstatistik nicht die folgende Zeile:

   ```
   Maxever session creation rate [value]
   ```

   Cisco IOS Software-Versionen, die älter als 12.4(11)T und 12.4(10) sind, behalten keinen Wert für die Überprüfung bei, da die maximale einminütige Verbindungsrate nicht erreicht werden kann. Daher müssen Sie den Wert, den Sie anwenden, anhand der Werte für die maximale Anzahl von Sitzungen berechnen. Beobachtungen von mehreren Netzwerken, die die Stateful Inspection der Cisco IOS Firewall Version 12.4(11)T in der Produktion verwenden, haben gezeigt, dass die Maxever Session Creation Rates tendenziell die Summe der drei Werte (etabliert, halb offen und terminiert) in der "Maxever Session Count" um etwa zehn Prozent übersteigt. Zur Berechnung der ip inspect eine Minute niedriger Wert, multiplizieren Sie den angegebenen "ermittelten" Wert mit 1,1, z. B.:

   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   ```

```
(207 + 56 + 35) * 1.1 = 328
```

Konfigurieren:

```
ip inspect one-minute low 328
```

Wenn der Router die Cisco IOS Software Version 12.4(11)T oder höher oder 12.4(10) oder höher ausführt, können Sie einfach den Wert anwenden, der in der Überprüfungsstatistik für die "Maximale Sitzungserstellungsrate" angezeigt wird:

```
Maxever session creation rate 330
```

Konfigurieren:

```
ip inspect one-minute low 330
```

9. Berechnen und konfigurieren Sie die **IP-Prüfung eine Minute hoch**. Der hohe Wert der einminütigen IP-Prüfung muss um 25 Prozent größer sein als der berechnete niedrige Wert von einer Minute, z. B.:

   ```
   ip inspect one-minute low (330) * 1.25 = 413
   ```

   Konfigurieren:

   ```
   ip inspect one-minute high 413
   ```

   Hinweis: Dieses Dokument beschreibt die Verwendung eines Multiplikators, der dem 1,25-fachen der typischen Aktivität Ihres Netzwerks entspricht, um Beschränkungen für den DoS-Schutz festzulegen. Wenn Sie Ihr Netzwerk innerhalb typischer Netzwerkaktivitäts-Peaks beobachten, muss dies genügend Reserven bereitstellen, um die Aktivierung des DoS-Schutzes des Routers unter allen, aber ungewöhnlichen Umständen zu vermeiden. Wenn in Ihrem Netzwerk regelmäßig große Mengen legitimer Netzwerkaktivitäten verzeichnet werden, die diesen Wert überschreiten, aktiviert der Router die DoS-Schutzfunktionen, die negative Auswirkungen auf einen Teil des Netzwerkverkehrs haben können. Sie müssen Ihre Router-Protokolle auf Erkennungen von DoS-Aktivitäten überwachen und die **ip inspect max-uncomplete high** und/oder **ip inspect one minute** limits anpassen, um die Auslösung von DoS zu vermeiden, nachdem Sie festgestellt haben, dass die Einschränkungen durch legitime Netzwerkaktivität erreicht wurden. Sie können die DoS-Schutzanwendung durch das Vorhandensein von Protokollmeldungen wie den folgenden erkennen:

10. Sie müssen einen Wert für **ip inspect tcp max-uncomplete host** definieren, entsprechend Ihrer Kenntnis der Funktionalität Ihrer Server. Dieses Dokument kann keine Richtlinien für die Konfiguration des DoS-Schutzes pro Host bereitstellen, da dieser Wert je nach Hardware- und Softwareleistung des End-Hosts sehr unterschiedlich ist. Wenn Sie sich nicht sicher sind, welche Beschränkungen für die Konfiguration des DoS-Schutzes geeignet sind, haben Sie im Prinzip zwei Optionen, um die DoS-Grenzwerte zu definieren:Die vorzuziehende Option besteht darin, den routerbasierten DoS-Schutz pro Host auf einen hohen Wert (kleiner oder gleich 4.294.967.295) zu konfigurieren und den Host-spezifischen Schutz anzuwenden, der vom Betriebssystem jedes Hosts oder einem externen Host-basierten Intrusion Protection System wie Cisco Security Agent (CSA) geboten wird.Überprüfen Sie die Aktivitäts- und Leistungsprotokolle auf Ihren Netzwerk-Hosts, und ermitteln Sie deren höchste nachhaltige Verbindungsrate. Da die klassische Firewall nur einen globalen Zähler anbietet, müssen Sie den maximalen Wert anwenden, den Sie bestimmen, nachdem Sie alle Ihre Netzwerk-Hosts auf die maximalen Verbindungsraten überprüft haben. Es wird weiterhin empfohlen, betriebssystemspezifische Aktivitätsgrenzen und ein hostbasiertes IPS wie CSA zu verwenden.**Hinweis: Die** Cisco IOS Firewall bietet nur eingeschränkten Schutz vor gezielten Angriffen auf bestimmte Schwachstellen in Betriebssystemen und Anwendungen. Der DoS-Schutz der Cisco IOS Firewall bietet keine Garantie für Kompromittierung von End-Host-Services, die potenziell gefährlichen Umgebungen ausgesetzt sind.

11. Überwachen Sie die DoS-Schutzaktivitäten in Ihrem Netzwerk. Im Idealfall müssen Sie einen Syslog-Server oder idealerweise eine Cisco Monitoring and Reporting Station (MARS) verwenden, um Vorfälle der Erkennung von DoS-Angriffen aufzuzeichnen. Wenn die Erkennung sehr häufig auftritt, müssen Sie Ihre DoS-Schutzparameter überwachen und anpassen.Weitere Informationen zu TCP-SYN-DoS-Angriffen finden Sie unter Defining Strategies to Protect Against TCP SYN Denial of Service Attacks.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems