ASA-Funktionen und -Konfiguration zur Erkennung von Sicherheitsrisiken ermitteln

Inhalt

Einleitung

In diesem Dokument werden die drei Hauptkomponenten der Funktionen und Konfiguration zur Erkennung von Sicherheitsrisiken beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die

möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument werden der Funktionsumfang und die grundlegende Konfiguration der Funktion zur Bedrohungserkennung der Cisco Adaptive Security Appliance (ASA) beschrieben. Die Bedrohungserkennung bietet Firewall-Administratoren die erforderlichen Tools, um Angriffe zu identifizieren, zu verstehen und zu stoppen, bevor sie die interne Netzwerkinfrastruktur erreichen. Dazu stützt sich die Funktion auf eine Reihe unterschiedlicher Auslöser und Statistiken, die in diesen Abschnitten näher beschrieben werden.

Die Bedrohungserkennung kann auf jeder ASA-Firewall mit der Softwareversion 8.0(2) oder höher eingesetzt werden. Die Erkennung von Sicherheitsrisiken ist zwar kein Ersatz für eine dedizierte IDS/IPS-Lösung, kann jedoch in Umgebungen eingesetzt werden, in denen kein IPS verfügbar ist, um die Kernfunktionen der ASA mit zusätzlichen Schutzschichten zu versehen.

Funktionen zur Bedrohungserkennung

Die Funktion zur Erkennung von Sicherheitsrisiken besteht aus drei Hauptkomponenten:

1. Grundlegende Bedrohungserkennung
2. Erweiterte Bedrohungserkennung
3. Scannen der Bedrohungserkennung

Jede dieser Komponenten wird in diesen Abschnitten ausführlich beschrieben.

Grundlegende Bedrohungserkennung (Durchsatzraten auf Systemebene)

Grundlegende Funktionen zur Erkennung von Sicherheitsrisiken sind standardmäßig auf allen ASAs aktiviert, auf denen 8.0(2) und höher ausgeführt wird.

Die grundlegende Bedrohungserkennung überwacht die Rate, mit der Pakete aus verschiedenen Gründen von der ASA als Ganzes verworfen werden. Das bedeutet, dass die durch die grundlegende Bedrohungserkennung generierten Statistiken nur für die gesamte Appliance gelten und in der Regel nicht detailliert genug sind, um Informationen über die Quelle oder den spezifischen Charakter der Bedrohung bereitzustellen. Stattdessen überwacht die ASA verworfene Pakete auf folgende Ereignisse:

- ACL Drop (acl-drop) - Pakete werden von Zugriffslisten abgelehnt.
- Ungültige Pakete (bad-packet-drop) - Ungültiges Paketformat, einschließlich L3- und L4-Header, die nicht den RFC-Standards entsprechen.
- Conn Limit (conn-limit-drop) - Pakete, die ein konfiguriertes oder globales Verbindungslimit überschreiten.
- DoS-Angriff (dos-drop) - Denial-of-Service-Angriffe (DoS).
- Firewall (fw-drop) - Grundlegende Prüfungen der Firewall-Sicherheit.
- ICMP-Angriff (icmp-drop) - Verdächtige ICMP-Pakete.
- Inspizierung (inspect-drop) - Verweigerung durch Anwendungsinspektion.
- Schnittstelle (interface-drop) - Pakete, die bei Schnittstellenprüfungen verworfen wurden.
- Scanning (Scanning-Threat) - Netzwerk-/Host-Scanning-Angriffe.
- SYN-Angriff (syn-Angriff) - Unvollständige Session-Angriffe, einschließlich TCP-SYN-Angriffe und unidirektionale UDP-Sitzungen, die keine Rückgabedaten haben.

Jedes dieser Ereignisse hat einen bestimmten Satz von Auslösern, die zum Identifizieren der Bedrohung verwendet werden. Die meisten Auslöser sind an bestimmte ASP-Abbruchgründe gebunden, obwohl auch

bestimmte Syslogs und Überprüfungsaktionen berücksichtigt werden. Einige Auslöser werden von mehreren Bedrohungskategorien überwacht. Einige der häufigsten Auslöser sind in dieser Tabelle aufgeführt. Sie enthält jedoch keine abschließende Liste:

Grundlegende Bedrohung	Trigger/s/ASP-Verlustursache(en)
ACL-Drop	ACL-Drop
Paketverlust	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-matching
conn-limit-drop	Verbindungsgrenze
DOS-Drop	sp-security-failed
fw-drop	inspect-icmp-seq-num-not-matching inspect-dns-pak-too-long inspect-dns-id-not-matching sp-security-failed ACL-Drop
ICMP-Drop	inspect-icmp-seq-num-not-matching
inspect-drop	Auslösung von Frame-Drops durch eine Prüfungs-Engine
Interface-Drop	sp-security-failed nicht befahrbar
Scanning-Bedrohung	tcp-3whs-fehlgeschlagen tcp-not-syn sp-security-failed ACL-Drop inspect-icmp-seq-num-not-matching inspect-dns-pak-too-long inspect-dns-id-not-matching

Syn-Angriff	%ASA-6-302014-Syslog mit Abbruchgrund "SYN Timeout"

Für jedes Ereignis misst die grundlegende Bedrohungserkennung die Häufigkeit, mit der diese Verluste über einen konfigurierten Zeitraum auftreten. Dieser Zeitraum wird als ARI (Average Rate Intervall) bezeichnet und kann zwischen 600 Sekunden und 30 Tagen liegen. Wenn die Anzahl der Ereignisse, die innerhalb der ARI auftreten, die konfigurierten Ratenschwellenwerte überschreitet, werden diese Ereignisse von der ASA als Bedrohung angesehen.

Für die grundlegende Bedrohungserkennung gibt es zwei konfigurierbare Schwellenwerte für den Fall, dass Ereignisse als Bedrohung eingestuft werden: die durchschnittliche Rate und die Burst-Rate. Die durchschnittliche Rate ist einfach die durchschnittliche Anzahl von Drops pro Sekunde innerhalb des Zeitraums der konfigurierten ARI. Wenn beispielsweise der Durchschnitts-Durchsatzschwellenwert für ACL-Verwerfungen für 400 mit einer ARI von 600 Sekunden konfiguriert ist, berechnet ASA die durchschnittliche Anzahl von Paketen, die von ACLs in den letzten 600 Sekunden verworfen wurden. Wenn sich herausstellt, dass diese Zahl größer als 400 pro Sekunde ist, protokolliert die ASA eine Bedrohung.

Die Burst-Rate ist ähnlich, untersucht jedoch kleinere Zeiträume von Snapshot-Daten, die als Burst-Rate-Intervall (BRI) bezeichnet werden. Der BRI ist immer kleiner als der ARI. Aufbauend auf dem vorherigen Beispiel beträgt die ARI für ACL-Drops beispielsweise immer noch 600 Sekunden und hat jetzt eine Burst-Rate von 800. Anhand dieser Werte berechnet die ASA die durchschnittliche Anzahl der von den ACLs blockierten Pakete in 20 Sekunden, wobei 20 Sekunden die BRI-Funktion darstellen. Wenn dieser berechnete Wert 800 Drops pro Sekunde überschreitet, wird eine Bedrohung protokolliert. Um festzustellen, welches BRI verwendet wird, berechnet die ASA den Wert von 1/30 des ARI. Daher ist im zuvor verwendeten Beispiel 1/30 von 600 Sekunden 20 Sekunden. Die Bedrohungserkennung verfügt jedoch über eine minimale BRI von 10 Sekunden. Wenn also 1/30 der ARI kleiner als 10 ist, verwendet die ASA weiterhin 10 Sekunden als BRI. Außerdem ist zu beachten, dass sich dieses Verhalten in Versionen vor 8.2(1) unterschied, die einen Wert von 1/60 des ARI anstelle von 1/30 verwendeten. Die minimale BRI von 10 Sekunden ist für alle Softwareversionen identisch.

Wenn ein grundlegendes Risiko erkannt wird, generiert die ASA lediglich das Syslog %ASA-4-733100, um den Administrator darüber zu informieren, dass ein potenzielles Risiko erkannt wurde. Mit dem Befehl **show threat-detection rate** (**Erkennungsrate anzeigen)** können Sie die durchschnittliche Anzahl, die aktuelle Anzahl und die Gesamtanzahl von Ereignissen für jede Bedrohungskategorie anzeigen. Die Gesamtzahl der kumulativen Ereignisse entspricht der Summe der Ereignisse in den letzten 30 BRI-Stichproben.

Die Burst-Rate im Syslog wird auf Basis der Anzahl der Pakete berechnet, die in der aktuellen BRI bisher verworfen wurden. Die Berechnung erfolgt periodisch in einer BRI. Sobald eine Sicherheitsverletzung erfolgt ist, wird ein Syslog ausgelöst. Es ist begrenzt, dass nur ein Syslog in einem BRI generiert wird. Die Burst-Rate in "Show Threat Detection Rate" wird auf Basis der Anzahl der bei der letzten BRI verworfenen Pakete berechnet. Der Unterschied besteht darin, dass Syslog zeitkritisch ist und bei einer Sicherheitsverletzung in der aktuellen BRI eine Chance zur Erfassung hätte. Da die Rate für die Erkennung von Sicherheitsrisiken kürzer ist, wird die letzte BRI verwendet.

Die grundlegende Bedrohungserkennung ergreift keine Maßnahmen, um den abweichenden Datenverkehr zu stoppen oder zukünftige Angriffe zu verhindern. In diesem Sinne dient die grundlegende Bedrohungserkennung lediglich zu Informationszwecken und kann als Überwachungs- oder Berichtsmechanismus verwendet werden.

Erweiterte Bedrohungserkennung (Objektstatistiken und Top-N)

Im Gegensatz zu grundlegender Bedrohungserkennung kann die erweiterte Bedrohungserkennung verwendet werden, um Statistiken für detailliertere Objekte zu verfolgen. Die ASA unterstützt Tracking-

Statistiken für Host-IPs, Ports, Protokolle, ACLs und Server, die durch TCP-Intercept geschützt sind. Die erweiterte Bedrohungserkennung ist nur standardmäßig für ACL-Statistiken aktiviert.

Bei Host-, Port- und Protokollobjekten verfolgt die Bedrohungserkennung die Anzahl der Pakete, Bytes und Datenverluste, die von diesem Objekt innerhalb eines bestimmten Zeitraums gesendet und empfangen wurden. Bei ACLs erfasst Threat Detection die 10 häufigsten ACEs (Zulassen und Ablehnen), die innerhalb eines bestimmten Zeitraums am häufigsten getroffen wurden.

Die in all diesen Fällen verfolgten Zeiträume betragen 20 Minuten, 1 Stunde, 8 Stunden und 24 Stunden. Auch wenn die Zeiträume selbst nicht konfigurierbar sind, kann die Anzahl der Zeiträume, die pro Objekt nachverfolgt werden, mit dem Schlüsselwort "Anzahl der Raten" angepasst werden. Weitere Informationen finden Sie im Abschnitt "Konfiguration". Wenn z. B. "Number-of-Rate" auf 2 festgelegt ist, werden alle Statistiken für 20 Minuten, 1 Stunde und 8 Stunden angezeigt. Wenn "Number-of-Rate" auf 1 festgelegt ist, werden alle Statistiken für 20 Minuten, 1 Stunde angezeigt. Egal was passiert, die 20-Minuten-Rate wird immer angezeigt.

Wenn TCP-Intercept aktiviert ist, kann die Bedrohungserkennung die Top 10 Server verfolgen, die als angegriffen gelten und durch das TCP-Intercept geschützt sind. Die Statistiken für TCP-Intercept ähneln der grundlegenden Bedrohungserkennung insofern, als der Benutzer das gemessene Intervall mit bestimmten Durchschnitts- (ARI) und Burst- (BRI) Raten konfigurieren kann. Statistiken zur erweiterten Bedrohungserkennung für TCP-Intercept sind nur in ASA 8.0(4) und höher verfügbar.

Statistiken zur erweiterten Bedrohungserkennung werden über **Statistiken zur Bedrohungserkennung anzeigen** und **Top**-Befehle zur **Bedrohungserkennung anzeigen** angezeigt. Diese Funktion ist auch für die Auffüllung der "Top"-Diagramme auf dem Firewall-Dashboard von ASDM verantwortlich. Die einzigen Syslogs, die von der erweiterten Bedrohungserkennung generiert werden, sind %ASA-4-733104 und %ASA-4-733105. Diese werden ausgelöst, wenn der Durchschnitt bzw. die Burst-Rate für die TCP-Intercept-Statistik überschritten werden.

Wie bei der grundlegenden Bedrohungserkennung handelt es sich bei der erweiterten Bedrohungserkennung um eine rein informative Erkennung. Basierend auf den Statistiken für die erweiterte Bedrohungserkennung werden keine Maßnahmen zum Blockieren von Datenverkehr ergriffen.

Scannen der Bedrohungserkennung

Die gescannte Bedrohungserkennung wird verwendet, um verdächtige Angreifer zu verfolgen, die zu viele Hosts in einem Subnetz oder viele Ports in einem Host/Subnetz erstellen. Das Scannen der Bedrohungserkennung ist standardmäßig deaktiviert.

Das Scannen der Bedrohungserkennung baut auf dem Konzept der grundlegenden Bedrohungserkennung auf, das bereits eine Bedrohungskategorie für einen Scanangriff definiert. Aus diesem Grund werden die Einstellungen für Übertragungsintervall, durchschnittliche Übertragungsrate (ARI) und Burst-Übertragungsrate (BRI) von der grundlegenden und der Scan-Funktion zur Bedrohungserkennung gemeinsam verwendet. Der Unterschied zwischen den beiden Funktionen besteht darin, dass die grundlegende Bedrohungserkennung nur anzeigt, dass die Durchschnitts- oder Burst-Rate-Schwellenwerte überschritten wurden, die Scan-Bedrohungserkennung jedoch eine Datenbank mit Angreifer- und Ziel-IP-Adressen verwaltet, die mehr Kontext für die am Scan beteiligten Hosts bereitstellen kann. Darüber hinaus wird nur Datenverkehr, der tatsächlich vom Ziel-Host/Subnetz empfangen wird, von der Bedrohungserkennung geprüft. Die grundlegende Bedrohungserkennung kann weiterhin eine Scan-Bedrohung auslösen, selbst wenn der Datenverkehr durch eine ACL verworfen wird.

Die gescannte Bedrohungserkennung kann optional auf einen Angriff reagieren, indem sie die IP des Angreifers meidet. Dadurch ist das Scannen der Bedrohungserkennung die einzige Teilmenge der Funktion zur Bedrohungserkennung, die sich aktiv auf Verbindungen über die ASA auswirken kann.

Wenn die Bedrohungserkennung einen Angriff erkennt, wird %ASA-4-733101 für den Angreifer und/oder die Ziel-IPs protokolliert. Wenn die Funktion so konfiguriert ist, dass der Angreifer gemieden wird, wird %ASA-4-733102 protokolliert, wenn das Scannen der Bedrohungserkennung eine Warnung generiert. %ASA-4-733103 wird protokolliert, wenn der Shun entfernt wird. Der Befehl **show threat-detection scanning-**threat kann verwendet werden, um die gesamte Datenbank zum Scannen von Bedrohungen anzuzeigen.

Einschränkungen

- Die Bedrohungserkennung ist nur in ASA 8.0(2) und höheren Versionen verfügbar. Sie wird von der ASA 1000V-Plattform nicht unterstützt.
- Die Erkennung von Sicherheitsrisiken wird nur im Einzelkontextmodus unterstützt.
- Es werden nur direkte Bedrohungen erkannt. An die ASA selbst gesendeter Datenverkehr wird von der Bedrohungserkennung nicht berücksichtigt.
- TCP-Verbindungsversuche, die vom Zielserver zurückgesetzt werden, werden nicht als SYN-Angriff oder Scanbedrohung gewertet.

Konfiguration

Grundlegende Bedrohungserkennung

Die grundlegende Bedrohungserkennung wird mit dem Befehl **zur Bedrohungserkennung** aktiviert.

<#root>

```
ciscoasa(config)#
```

```
threat-detection basic-threat
```

Die Standardraten können mit dem Befehl **show run all threat-detection** angezeigt werden.

<#root>

```
ciscoasa(config)#
```

```
show run all threat-detection
```

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
```

```
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

Um diese Raten mit benutzerdefinierten Werten abzustimmen, müssen Sie den Befehl **rate** der **Bedrohungserkennung** für die entsprechende Bedrohungskategorie neu konfigurieren.

<#root>

```
ciscoasa(config)#
```

threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550

Für jede Bedrohungskategorie können maximal 3 verschiedene Raten definiert werden (mit Raten-IDs für Rate 1, Rate 2 und Rate 3). Auf die bestimmte Rate-ID, die überschritten wird, wird im %ASA-4-733100-Syslog verwiesen.

Im vorherigen Beispiel wird bei der Erkennung von Sicherheitsrisiken Syslog 733100 nur erstellt, wenn die Anzahl der ACL-Löschungen 250 Löschungen pro Sekunde in 1.200 Sekunden oder 550 Löschungen pro Sekunde in 40 Sekunden überschreitet.

Erweiterte Bedrohungserkennung

Verwenden Sie den Befehl **Bedrohungserkennungsstatistiken**, um die erweiterte Bedrohungserkennung zu aktivieren. Wenn kein bestimmtes Feature-Schlüsselwort angegeben wird, aktiviert der Befehl die Nachverfolgung für alle Statistiken.

<#root>

```
ciscoasa(config)#
```

threat-detection statistics ?

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

Um die Anzahl der Ratenintervalle zu konfigurieren, die für Host-, Port-, Protokoll- oder ACL-Statistiken verfolgt werden, verwenden Sie das Schlüsselwort **number-of-rate**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics host number-of-rate 2
```

Mit dem Schlüsselwort "Anzahl" wird die Bedrohungserkennung so konfiguriert, dass nur die kürzeste *n* Anzahl an Intervallen verfolgt wird.

Um die TCP-Abfangstatistik zu aktivieren, verwenden Sie den Befehl **tcp-intercept** zur **Erkennung von Bedrohungen**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics tcp-intercept
```

Um benutzerdefinierte Raten für TCP-Abfangstatistiken zu konfigurieren, verwenden Sie die Schlüsselwörter **rate-interval**, **average-rate** und **burst-rate**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

Scannen der Bedrohungserkennung

Um das Scannen der Bedrohungserkennung zu aktivieren, verwenden Sie den Befehl **Threat-Detection Scanning-Threat**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat
```

Um die Raten für eine Scan-Bedrohung anzupassen, verwenden Sie den gleichen Befehl zur **Rate der Bedrohungserkennung, der** von der grundlegenden Bedrohungserkennung verwendet wird.

<#root>

```
ciscoasa(config)#
```

```
threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

Damit die ASA eine IP eines scannenden Angreifers ignorieren kann, fügen Sie das Schlüsselwort **shun** zum Befehl **threaderkennungs-scan-threat hinzu**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun
```

Auf diese Weise kann die Bedrohungserkennung einstündig gescannt werden. Um die Dauer des Shuns anzupassen, verwenden Sie den Befehl **Threat-Detection Scanning-Threat Shun Duration**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun duration 1000
```

In einigen Fällen können Sie verhindern, dass die ASA bestimmte IPs scheut. Erstellen Sie dazu eine Ausnahme mit dem Befehl **Threat-Detection Scan-Threat shun except**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except object-group no-shun
```

Leistung

Die grundlegende Bedrohungserkennung hat nur sehr geringe Leistungseinbußen für die ASA. Advanced und Scanning Threat Detection sind sehr viel ressourcenintensiver, da sie verschiedene Statistiken im Arbeitsspeicher verfolgen müssen. Nur das Scannen der Bedrohungserkennung mit aktivierter Shun-Funktion kann den Datenverkehr aktiv beeinflussen, der andernfalls zugelassen worden wäre.

Mit dem Fortschreiten der ASA-Softwareversionen wurde die Speichernutzung durch die Erkennung von Sicherheitsrisiken erheblich optimiert. Die Speichernutzung der ASA muss jedoch vor und nach der Aktivierung der Bedrohungserkennung überwacht werden. In einigen Fällen ist es besser, nur bestimmte Statistiken (z. B. Hoststatistiken) vorübergehend zu aktivieren, während Sie aktiv ein bestimmtes Problem beheben.

Führen Sie den Befehl **show memory app-cache Threat-detection [detail]** aus, um eine detailliertere Ansicht der Speichernutzung durch die **Bedrohungserkennung zu erhalten**.

Empfohlene Maßnahmen

Diese Abschnitte enthalten einige allgemeine Empfehlungen für Maßnahmen, die ergriffen werden können, wenn verschiedene Ereignisse im Zusammenhang mit der Bedrohungserkennung auftreten.

Wenn eine einfache Verlustrate überschritten und %ASA-4-733100 generiert wird

Bestimmen Sie die im %ASA-4-733100-Syslog genannte spezifische Bedrohungskategorie und korrelieren Sie diese mit der Ausgabe von show threat-detection rate . Überprüfen Sie mit diesen Informationen die Ausgabe von show asp drop um die Gründe zu ermitteln, warum der Datenverkehr unterbrochen wird.

Um eine detailliertere Ansicht des Datenverkehrs zu erhalten, der aus einem bestimmten Grund verworfen wurde, verwenden Sie eine ASP-Verwerfungserfassung mit dem betreffenden Grund, um alle verworfenen Pakete anzuzeigen. Wenn beispielsweise ACL Drop-Bedrohungen protokolliert werden, erfassen Sie den Grund für ASP-Drop von acl-drop :

```
<#root>

ciscoasa#

capture drop type asp-drop acl-drop



ciscoasa#

show capture drop



1 packet captured

   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

Diese Erfassung zeigt, dass es sich bei dem verworfenen Paket um ein UDP/53-Paket zwischen 10.10.10.10 und 192.168.1.100 handelt.

Wenn %ASA-4-733100 eine Scanbedrohung meldet, kann es auch hilfreich sein, vorübergehend die Scanbedrohungserkennung zu aktivieren. Auf diese Weise kann die ASA die Quell- und Ziel-IP-Adressen nachverfolgen, die am Angriff beteiligt sind.

Da die grundlegende Bedrohungserkennung hauptsächlich den Datenverkehr überwacht, der bereits vom ASP verworfen wird, sind keine direkten Maßnahmen erforderlich, um eine potenzielle Bedrohung aufzuhalten. Die Ausnahme hiervon bilden SYN-Angriffe und Scan-Bedrohungen, bei denen es sich um Datenverkehr handelt, der über die ASA geleitet wird.

Wenn die in der ASP-Ablagerungserfassung festgestellten Abbrüche für die Netzwerkumgebung legitim und/oder erwartet werden, passen Sie die Intervalle der Basisrate auf einen angemesseneren Wert an.

Wenn bei den Drops unzulässiger Datenverkehr festgestellt wird, müssen Maßnahmen ergriffen werden, um den Datenverkehr zu blockieren oder zu begrenzen, bevor er die ASA erreicht. Dies kann ACLs und QoS auf Upstream-Geräten einschließen.

Bei SYN-Angriffen kann der Datenverkehr in einer ACL auf der ASA blockiert werden. TCP-Intercept kann auch so konfiguriert werden, dass die Zielserver geschützt werden. Dies kann jedoch zu einer Bedrohung durch Conn Limit führen, die stattdessen protokolliert wird.

Zum Scannen von Bedrohungen kann der Datenverkehr auch in einer ACL auf der ASA blockiert werden. Scannen der Bedrohungserkennung mit dem shunkann aktiviert werden, damit die ASA alle Pakete des Angreifers für einen bestimmten Zeitraum proaktiv blockieren kann.

Wenn eine Scan-Bedrohung erkannt und %ASA-4-733101 protokolliert wird

%ASA-4-733101 muss entweder die IP-Adresse des Ziel-Hosts/Subnetzes oder des Angreifers auflisten. Eine vollständige Liste der Ziele und Angreifer finden Sie in der Ausgabe von show threat-detection scanning-threat.

Paketerfassungen an den ASA-Schnittstellen, die dem Angreifer und/oder dem Ziel/den Zielen gegenüberstehen, können ebenfalls dazu beitragen, die Art des Angriffs zu klären.

Wenn der erkannte Scan nicht erwartet wird, müssen Maßnahmen ergriffen werden, um den Datenverkehr zu blockieren oder zu begrenzen, bevor er die ASA erreicht. Dies kann ACLs und QoS auf Upstream-Geräten einschließen. Wenn die shunwird der Konfiguration "Scanning Threat Detection" hinzugefügt, damit die ASA alle Pakete proaktiv über einen definierten Zeitraum von der Angreifer-IP verwerfen kann. Als letzte Möglichkeit kann der Datenverkehr auch manuell auf der ASA über eine ACL- oder TCP-Abfangrichtlinie blockiert werden.

Wenn der erkannte Scan falsch positiv ist, passen Sie die Durchsatzintervalle für Scanning Threat an einen für die Netzwerkumgebung angemesseneren Wert an.

Wenn ein Angreifer gemieden und %ASA-4-733102 protokolliert wird

%ASA-4-733102 listet die IP-Adresse des gemieden Angreifers auf. Verwenden Sie show threat-detection shun , um eine vollständige Liste der von Threat Detection speziell gemieden Angreifer anzuzeigen. Verwenden Sie show shun um die vollständige Liste aller IP-Adressen anzuzeigen, die von der ASA aktiv gemieden werden (dies schließt Quellen ein, die keine Bedrohungserkennung sind).

Wenn der Shun Teil eines legitimen Angriffs ist, sind keine weiteren Maßnahmen erforderlich. Es wäre jedoch von Vorteil, den Datenverkehr des Angreifers so weit stromaufwärts zur Quelle wie möglich manuell zu blockieren. Dies ist über ACLs und QoS möglich. Dadurch wird sichergestellt, dass Zwischengeräte keine Ressourcen für unrechtmäßigen Datenverkehr verschwenden müssen.

Wenn die Scan-Bedrohung, die den Shun ausgelöst hat, falsch war, entfernen Sie den Shun manuell mit dem clear threat-detection shun [IP_address] aus.

Wenn %ASA-4-733104 und/oder %ASA-4-733105 protokolliert wird

%ASA-4-733104 und %ASA-4-733105 listet den Host auf, auf den der Angriff abzielt, der derzeit durch das TCP-Intercept geschützt ist. Weitere Informationen zu den Angriffsraten und geschützten Servern finden Sie in der Ausgabe von show threat-detection statistics top tcp-intercept .

<#root>

```
ciscoasa#
```

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
```

```
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Wenn die erweiterte Bedrohungserkennung einen solchen Angriff erkennt, schützt die ASA den Zielserver bereits über TCP-Intercept. Überprüfen Sie die konfigurierten Verbindungslimits, um sicherzustellen, dass diese einen angemessenen Schutz für die Art und die Geschwindigkeit des Angriffs bieten. Außerdem wäre es von Vorteil, den Datenverkehr des Angreifers so weit stromaufwärts zur Quelle wie möglich manuell zu blockieren. Dies ist über ACLs und QoS möglich. Dadurch wird sichergestellt, dass Zwischengeräte keine Ressourcen für unrechtmäßigen Datenverkehr verschwenden müssen.

Wenn der erkannte Angriff falsch ist, passen Sie die Raten für einen TCP-Intercept-Angriff mit dem threat-detection statistics tcp-interceptaus.

Manuelle Auslösung von Bedrohungen

Für Tests und Fehlerbehebung kann es hilfreich sein, verschiedene Bedrohungen manuell auszulösen. Dieser Abschnitt enthält Tipps zum Auslösen einiger gängiger Bedrohungstypen.

Grundlegende Bedrohung - ACL Drop, Firewall und Scanning

Informationen zum Auslösen einer bestimmten grundlegenden Bedrohung finden Sie in der Tabelle im vorherigen Abschnitt zu den Funktionen. Wählen Sie einen bestimmten ASP-Verwerfungsgrund aus, und senden Sie Datenverkehr über die ASA, der nach dem entsprechenden ASP-Verwerfungsgrund verworfen würde.

Bei ACL Drop-, Firewall- und Scan-Bedrohungen wird beispielsweise die Paketrate nach acl-drop berücksichtigt. Gehen Sie wie folgt vor, um diese Bedrohungen gleichzeitig auszulösen:

1. Erstellen Sie eine ACL an der externen Schnittstelle der ASA, die alle an einen Zielserver innerhalb der ASA (10.11.11.11) gesendeten TCP-Pakete explizit verwirft:

   ```
   access-list outside_in extended line 1 deny tcp any host 10.11.11.11
   access-list outside_in extended permit ip any any
   access-group outside_in in interface outside
   ```

2. Verwenden Sie von einem Angreifer außerhalb der ASA (10.10.10.10) nmap, um einen TCP-SYN-Scan für jeden Port auf dem Zielserver auszuführen:

   ```
   nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
   ```

   > **Hinweis**: T5 konfiguriert nmap so, dass der Scan so schnell wie möglich ausgeführt wird. Auf Basis der Ressourcen des Angreifer-PCs ist dies immer noch nicht schnell genug, um einige der Standardraten auszulösen. Wenn dies der Fall ist, senken Sie einfach die konfigurierten Raten für die Bedrohung, die Sie sehen möchten. Wenn Sie ARI und BRI auf 0 setzen, löst die grundlegende Bedrohungserkennung immer die Bedrohung aus, unabhängig von der Rate.

   ---

3. Beachten Sie, dass grundlegende Bedrohungen für ACL Drop-, Firewall- und Scan-Bedrohungen erkannt werden:

   ```
   %ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
   ```

```
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

Hinweis: In diesem Beispiel wurden die ACL-Drop- und Firewall-ARIs und -BRIs auf 0 gesetzt, sodass sie immer eine Bedrohung auslösen. Aus diesem Grund werden die konfigurierten Höchstsätze mit 0 angegeben.

Komplexe Bedrohung - TCP-Intercept

1. Erstellen Sie eine ACL auf der externen Schnittstelle, die alle an einen Zielserver innerhalb der ASA (10.11.11.11) gesendeten TCP-Pakete zulässt:

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. Wenn der Zielserver nicht vorhanden ist oder die Verbindungsversuche des Angreifers zurückgesetzt werden, konfigurieren Sie einen gefälschten ARP-Eintrag auf der ASA, um den Angriffsverkehr über die interne Schnittstelle zu blockieren:

```
arp inside 10.11.11.11 dead.dead.dead
```

3. Erstellen Sie auf der ASA eine einfache TCP-Abfangrichtlinie:

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

Verwenden Sie von einem Angreifer außerhalb der ASA (10.10.10.10) nmap, um einen TCP-SYN-Scan für jeden Port auf dem Zielserver auszuführen:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Beachten Sie, dass die Erkennung von Sicherheitsrisiken den geschützten Server verfolgt:

<#root>

```
ciscoasa(config)#
```

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

------------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

Scannen von Bedrohungen

1. Erstellen Sie eine ACL auf der externen Schnittstelle, die alle an einen Zielserver innerhalb der ASA (10.11.11.11) gesendeten TCP-Pakete zulässt:

   ```
   access-list outside_in extended line 1 permit tcp any host 10.11.11.11
   access-group outside_in in interface outside
   ```

   Hinweis: Damit das Scannen der Bedrohungserkennung die Ziel- und Angreifer-IP-Adresse verfolgen kann, muss der Datenverkehr über die ASA zugelassen werden.

   ---

2. Wenn der Zielserver nicht vorhanden ist oder die Verbindungsversuche des Angreifers zurückgesetzt werden, konfigurieren Sie einen gefälschten ARP-Eintrag auf der ASA, um den Angriffsverkehr über die interne Schnittstelle zu blockieren:

   ```
   arp inside 10.11.11.11 dead.dead.dead
   ```

   Hinweis: Verbindungen, die vom Zielserver zurückgesetzt werden, werden nicht als Teil der Bedrohung gezählt.

   ---

3. Verwenden Sie von einem Angreifer außerhalb der ASA (10.10.10.10) nmap, um einen TCP-SYN-Scan für jeden Port auf dem Zielserver auszuführen:

   ```
   nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
   ```

   Hinweis: T5 konfiguriert nmap so, dass der Scan so schnell wie möglich ausgeführt wird. Auf Basis der Ressourcen des Angreifer-PCs ist dies immer noch nicht schnell genug, um einige der Standardraten auszulösen. Wenn dies der Fall ist, senken Sie einfach die konfigurierten Raten für die Bedrohung, die Sie sehen möchten. Wenn Sie ARI und BRI auf 0 setzen, löst die grundlegende Bedrohungserkennung immer die Bedrohung aus, unabhängig von der Rate.

   ---

4. Beachten Sie, dass eine Scan-Bedrohung erkannt wird, die IP-Adresse des Angreifers verfolgt wird und der Angreifer gemieden wird:

   ```
   %ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
   max configured rate is 10; Current average rate is 0 per second,
    max configured rate is 5; Cumulative total count is 404
   %ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
    max configured rate is 10; Current average rate is 0 per second,
    max configured rate is 5; Cumulative total count is 700
   ```

```
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Zugehörige Informationen

- **ASA-Konfigurationsleitfaden**
- **ASA-Befehlsreferenz**
- **Syslog-Meldungen der Cisco Secure Firewall ASA-Serie**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.