ASA/PIX 7.x und höher: Eindämmung von Netzwerkangriffen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe der Cisco Security Appliance (ASA/PIX) die verschiedenen Netzwerkangriffe, wie z. B. Denial-of-Services (DoS), abwehren 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) der Serie 5500, die Softwareversion 7.0 und höher ausführt.

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.

Zugehörige Produkte

Dieses Dokument kann auch mit Cisco PIX der Serie 500 verwendet werden, auf dem die Softwareversion 7.0 und höher ausgeführt wird.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Schutz vor SYN-Angriffen

Wie können Sie die SYN-Angriffe (Transmission Control Protocol (TCP) synchronisieren/starten) auf ASA/PIX eindämmen?

TCP-SYN-Angriff

TCP SYN-Angriff ist eine Art von DoS-Angriff, bei dem ein Sender ein Volumen von Verbindungen überträgt, das nicht abgeschlossen werden kann. Dadurch werden die Verbindungswarteschlangen gefüllt, wodurch legitimen TCP-Benutzern der Dienst verweigert wird.

Wenn eine normale TCP-Verbindung gestartet wird, empfängt ein Ziel-Host ein SYN-Paket von einem Quellhost und sendet ein SYN ACK (Synchronize Bestätigungsbestätigung) zurück. Der Ziel-Host muss dann eine ACK der SYN ACK hören, bevor die Verbindung hergestellt wird. Dies wird als Drei-Wege-Handshake von TCP bezeichnet.

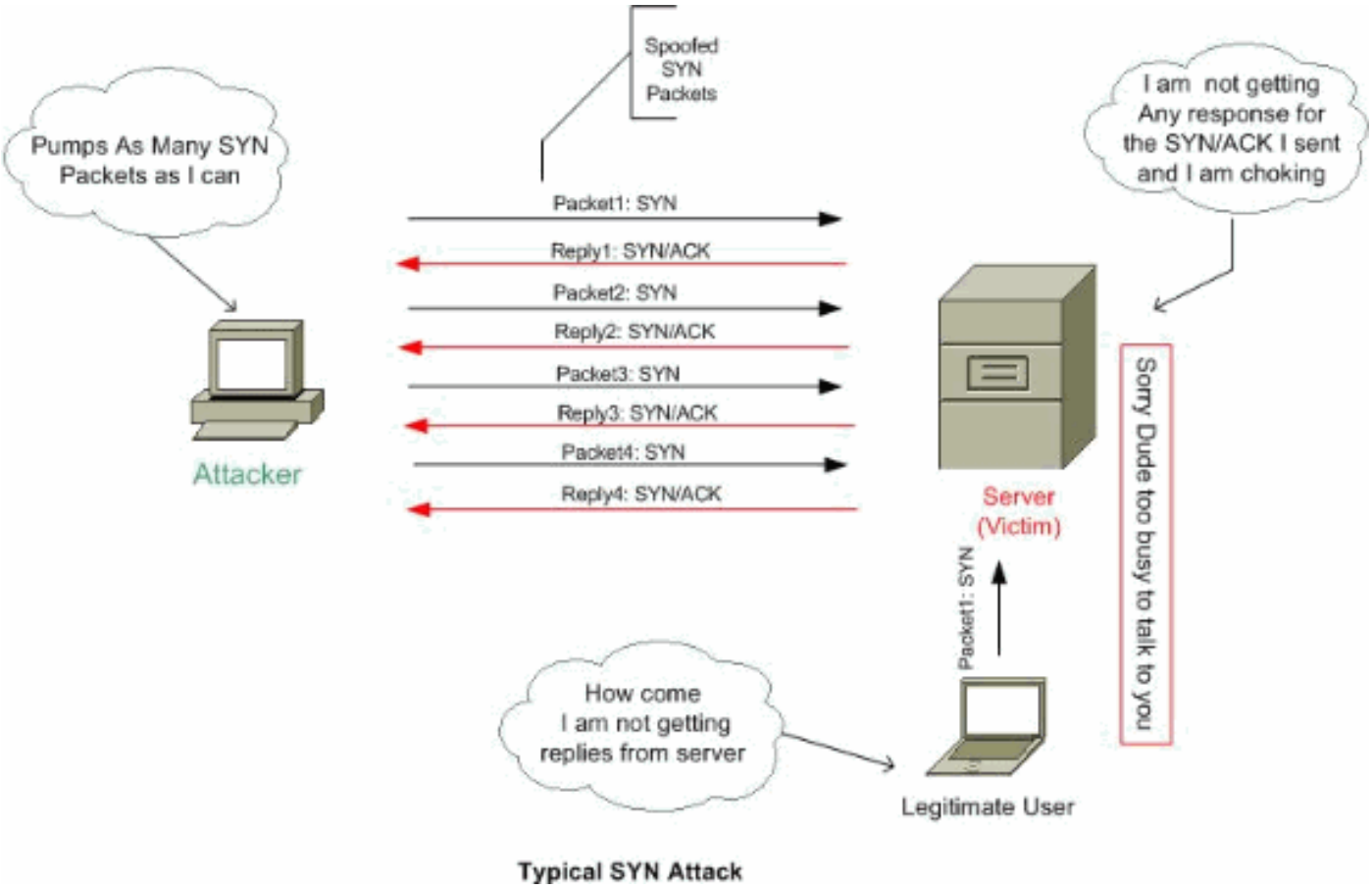
Während Sie auf die ACK für die SYN-ACK warten, verfolgt eine Verbindungswarteschlange mit begrenzter Größe auf dem Ziel-Host alle Verbindungen, die auf ihre Fertigstellung warten. Diese Warteschlange wird in der Regel schnell geleert, da die ACK voraussichtlich einige Millisekunden nach der SYN ACK-Nachricht eintreffen wird.

Der TCP SYN-Angriff nutzt dieses Design aus, indem ein angreifender Quellhost TCP-SYN-Pakete mit zufälligen Quelladressen für einen angegriffenen Host generiert. Der Ziel-Host des Opfers sendet eine SYN-ACK zurück an die zufällige Quelladresse und fügt einen Eintrag in die Verbindungswarteschlange hinzu. Da die SYN ACK für einen falschen oder nicht vorhandenen Host bestimmt ist, wird der letzte Teil des "Drei-Wege-Handshake" nie abgeschlossen, und der Eintrag bleibt in der Verbindungswarteschlange, bis ein Timer abläuft, normalerweise für etwa eine Minute. Durch das schnelle Generieren von gefälschten TCP-SYN-Paketen von zufälligen IP-Adressen ist es möglich, die Verbindungswarteschlange zu füllen und TCP-Dienste (z. B. E-Mail, Dateiübertragung oder WWW) legitimen Benutzern zu verweigern.

Es gibt keine einfache Möglichkeit, den Urheber des Angriffs zu verfolgen, da die IP-Adresse der Quelle gefälscht ist.

Zu den externen Manifestationen des Problems gehören die Unfähigkeit, E-Mails zu erhalten, die Unfähigkeit, Verbindungen zu WWW- oder FTP-Diensten zu akzeptieren, oder eine große Anzahl von TCP-Verbindungen auf Ihrem Host im Zustand SYN_RCVD.

Weitere Informationen zu TCP-SYN-Angriffen finden Sie unter Abwehr von TCP-SYN-Flooding-Angriffen.



Eindämmung

In diesem Abschnitt wird beschrieben, wie Sie die SYN-Angriffe durch Festlegen der maximalen TCP- und UDP-Verbindungen (User Datagram Protocol), der maximalen Anzahl an embryonalen Verbindungen, Verbindungszeitüberschreitungen und das Deaktivieren der Randomisierung von TCP-Sequenzen mindern.

Wenn die Grenze für die embryonale Verbindung erreicht ist, antwortet die Sicherheits-Appliance auf jedes SYN-Paket, das mit SYN+ACK an den Server gesendet wird, und übergibt das SYN-Paket nicht an den internen Server. Wenn das externe Gerät mit einem ACK-Paket antwortet, weiß die Sicherheits-Appliance, dass es sich um eine gültige Anfrage handelt (und nicht um einen Teil eines potenziellen SYN-Angriffs). Die Sicherheits-Appliance stellt dann eine Verbindung mit dem Server her und verbindet die Verbindungen miteinander. Wenn die Sicherheits-Appliance kein ACK vom Server zurückerhält, wird diese embryonale Verbindung aggressiv abgebrochen.

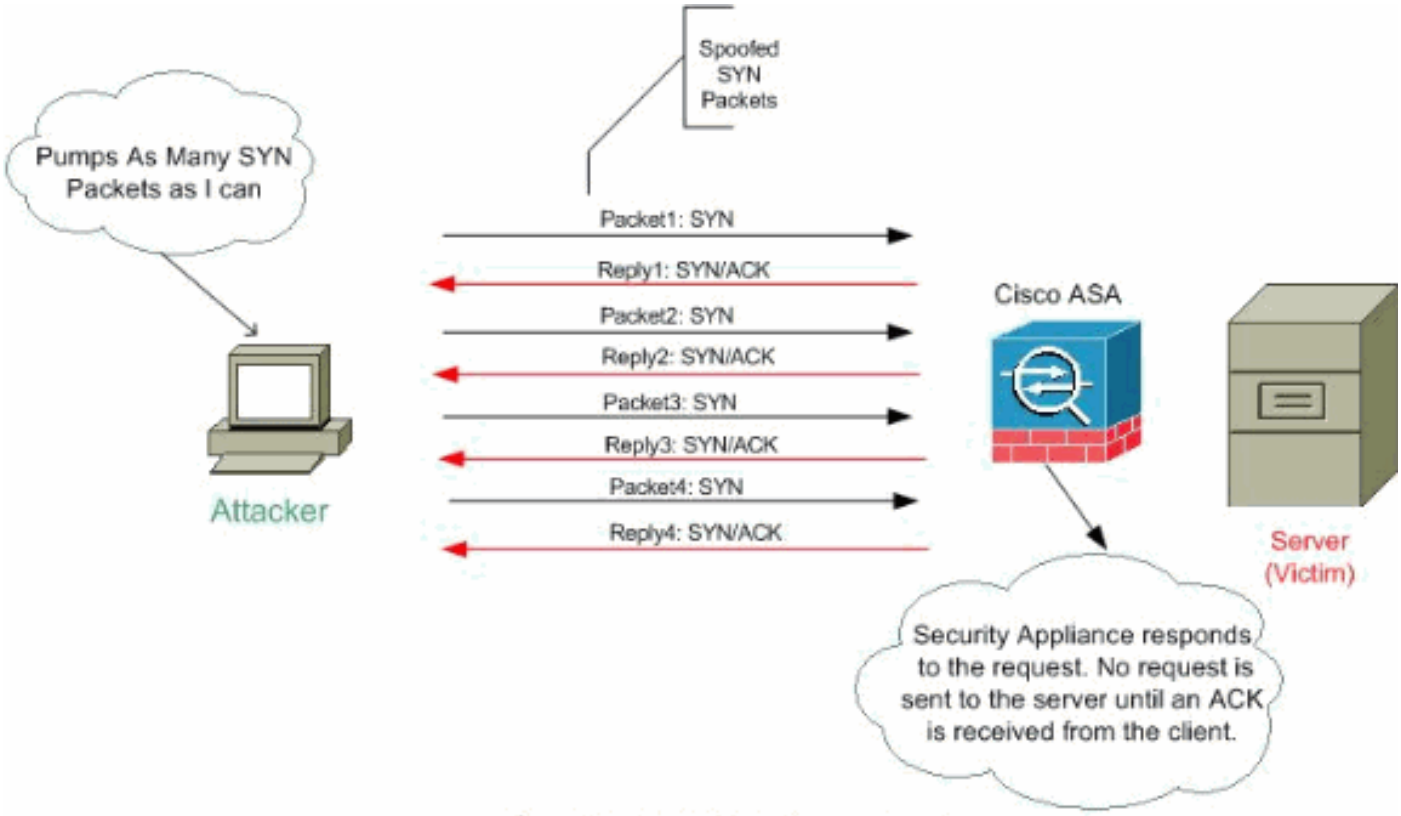
Jede TCP-Verbindung hat zwei Initial Sequence Number (ISNs): eine vom Client und eine vom Server generiert. Die Sicherheits-Appliance randomisiert die ISN der TCP-SYN, die sowohl die eingehende als auch die ausgehende Richtung übergibt.

Die Randomisierung der ISN des geschützten Hosts hindert einen Angreifer daran, die nächste ISN für eine neue Verbindung vorherzusagen und die neue Sitzung möglicherweise zu entführen.

Die Randomisierung der anfänglichen TCP-Sequenznummer kann bei Bedarf deaktiviert werden. Beispiel:

- Wenn eine andere Inline-Firewall auch die anfänglichen Sequenznummern zufällig wählt, müssen beide Firewalls diese Aktion durchführen, obwohl sich diese Aktion nicht auf den Datenverkehr auswirkt.
- Wenn Sie externe BGP (eBGP)-Multi-Hop über die Sicherheits-Appliance verwenden und die eBGP-Peers MD5 verwenden, wird bei der Randomisierung die MD5-Prüfsumme aufgehoben.
- Sie verwenden ein WAAS-Gerät (Wide Area Application Services), bei dem die Sicherheits-Appliance die Anzahl der Verbindungen nicht nach dem Zufallsprinzip zuordnen muss.

Hinweis: Sie können in der NAT-Konfiguration auch maximale Verbindungen, maximale embryonale Verbindungen und die Randomisierung von TCP-Sequenzen konfigurieren. Wenn Sie diese Einstellungen für denselben Datenverkehr mit beiden Methoden konfigurieren, verwendet die Sicherheits-Appliance die untere Grenze. Wenn die TCP-Sequenzzufälligkeit mithilfe einer der beiden Methoden deaktiviert ist, deaktiviert die Sicherheits-Appliance die Randomisierung der TCP-Sequenz.



Security Appliance acts as a proxy

Gehen Sie wie folgt vor, um Verbindungsgrenzen festzulegen:

1. Um den Datenverkehr zu identifizieren, fügen Sie mithilfe des Befehls **class-map** gemäß Using Modular Policy Framework eine Klassenzuordnung hinzu.
2. Um eine **Richtlinienzuordnung** hinzuzufügen oder zu bearbeiten, die die Aktionen für den Klassenzuordnungs-Datenverkehr festlegt, geben Sie den folgenden Befehl ein:
   `hostname(config)#policy-map name`
3. Um die Klassenzuordnung (aus Schritt 1) zu identifizieren, der Sie eine Aktion zuweisen möchten, geben Sie den folgenden Befehl ein:
   `hostname(config-pmap)#class class_map_name`
4. Um die maximale Anzahl an Verbindungen (sowohl TCP als auch UDP), die maximale

Anzahl an embryonalen Verbindungen, pro Client-embryonal-max, pro Client-max oder für die Deaktivierung der Randomisierung der TCP-Sequenz festzulegen, geben Sie den folgenden Befehl ein:

```
hostname(config-pmap-c)#set connection {[conn-max number]
[embryonic-conn-max number] [per-client-embryonic-max number]
[per-client-max number][random-sequence-number {enable |
disable}}
```

wobei number eine ganze Zahl zwischen 0 und 65535 ist. Der Standardwert ist 0, d. h. es gibt keine Beschränkung für Verbindungen.Sie können diesen Befehl in einer Zeile eingeben (in beliebiger Reihenfolge) oder jedes Attribut als separaten Befehl eingeben. Der Befehl wird in der aktuellen Konfiguration auf einer Zeile kombiniert.

5. Geben Sie den folgenden Befehl ein, um die Zeitüberschreitung für Verbindungen, embryonale Verbindungen (halb geöffnet) und halb geschlossene Verbindungen festzulegen:

   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```

   Dabei ist **die** Embryonalzeit [:mm[:ss] eine Zeit zwischen 0:0:5 und 1192:59:59. Der Standardwert ist 0:0:30. Sie können diesen Wert auch auf 0 setzen, d. h. die Verbindung wird nie beendet.Die **halb geschlossenen** hh[:mm[:ss]- und **tcp** hh[:mm[:ss]-Werte liegen zwischen 0:5:0 und 1192:59:59. Der Standardwert für **halb geschlossen** ist 0:10:0 und der Standardwert für **tcp** 1:0:0. Sie können diese Werte auch auf 0 setzen, d. h. die Verbindung überschreitet nie ihr Zeitlimit.Sie können diesen Befehl in einer Zeile eingeben (in beliebiger Reihenfolge) oder jedes Attribut als separaten Befehl eingeben. Der Befehl wird in der aktuellen Konfiguration auf einer Zeile kombiniert.**Embryonale (halb geöffnete) Verbindung** - Eine embryonale Verbindung ist eine TCP-Verbindungsanforderung, die den erforderlichen Handshake zwischen Quelle und Ziel noch nicht abgeschlossen hat.**Half-Closed Connection** (Halb geschlossene Verbindung): Eine halb geschlossene Verbindung besteht dann, wenn die Verbindung nur in eine Richtung durch Senden von FIN geschlossen wird. Die TCP-Sitzung wird jedoch weiterhin vom Peer verwaltet.**Per-client-embryonic-max**: Die maximal zulässige Anzahl gleichzeitiger embryonaler Verbindungen pro Client zwischen 0 und 65535. Der Standardwert ist 0, wodurch unbegrenzte Verbindungen möglich sind.**Per-client-max**: Die maximal zulässige Anzahl gleichzeitiger Verbindungen pro Client zwischen 0 und 65.535. Der Standardwert ist 0, wodurch unbegrenzte Verbindungen möglich sind.

6. Um die Richtlinienzuordnung auf einer oder mehreren Schnittstellen zu aktivieren, geben Sie den folgenden Befehl ein:

   ```
   hostname(config)#service-policy policymap_name {global | interface interface_name}
   ```

   Wenn **global** die Richtlinienzuordnung auf alle Schnittstellen angewendet wird und **Schnittstelle** die Richtlinie auf eine Schnittstelle anwendet. Es ist nur eine globale Richtlinie zulässig. Sie können die globale Richtlinie für eine Schnittstelle überschreiben, indem Sie eine Dienstrichtlinie auf diese Schnittstelle anwenden. Sie können auf jede Schnittstelle nur eine Richtlinienzuordnung anwenden.

Beispiel:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
```

```
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Hinweis: Verwenden Sie den folgenden Befehl, um die Gesamtzahl der halbgeöffneten Sitzungen für einen bestimmten Host zu überprüfen:

```
ASA-5510-8x# show local-host all

Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited

    UDP flow count/limit = 0/unlimited
```

Hinweis: Die Zeile `TCP-Embryonenzahl zum Hosten` zeigt die Anzahl der halb geöffneten Sitzungen an.

Schutz vor IP-Spoofing-Angriffen

Kann die PIX/ASA IP-Spoof-Angriffe blockieren?

IP-Spoofing

Um Zugriff zu erhalten, erstellen Eindringlinge Pakete mit gefälschten Quell-IP-Adressen. Dabei werden Anwendungen ausgenutzt, die auf IP-Adressen basierende Authentifizierung verwenden, was zu nicht autorisierten Benutzern und möglicherweise zum Root-Zugriff auf das Zielsystem führt. Beispiele sind die rsh- und rlogin-Dienste.

Es ist möglich, Pakete über Filterrouter-Firewalls weiterzuleiten, wenn sie nicht zum Filtern eingehender Pakete konfiguriert sind, deren Quelladresse sich in der lokalen Domäne befindet. Es ist wichtig zu beachten, dass der beschriebene Angriff auch dann möglich ist, wenn keine Antwortpakete den Angreifer erreichen können.

Folgende Konfigurationen sind potenziell anfällig:

- Proxy-Firewalls, bei denen die Proxyanwendungen die Quell-IP-Adresse für die Authentifizierung verwenden
- Router zu externen Netzwerken, die mehrere interne Schnittstellen unterstützen
- Router mit zwei Schnittstellen, die Subnetzwerke im internen Netzwerk unterstützen

Eindämmung

Unicast Reverse Path Forwarding (uRPF) schützt vor IP-Spoofing (ein Paket verwendet eine falsche Quell-IP-Adresse, um seine wahre Quelle zu verdecken), indem es sicherstellt, dass alle Pakete über eine Quell-IP-Adresse verfügen, die mit der richtigen Quell-Schnittstelle gemäß Routing-Tabelle übereinstimmt.

Normalerweise überprüft die Sicherheits-Appliance nur die Zieladresse, wenn sie feststellt, wohin das Paket weitergeleitet werden soll. Unicast RPF weist die Security Appliance an, auch die Quelladresse zu prüfen. Deshalb wird sie als **Reverse Path Forwarding** bezeichnet. Für jeden Datenverkehr, der über die Security Appliance zugelassen werden soll, muss die Routing-Tabelle der Security Appliance eine Route zurück zur Quelladresse enthalten. Weitere Informationen finden Sie unter RFC 2267 .

Hinweis: The `:- %PIX-1-106021:` Wenn `die` Rückwärtswegüberprüfung `des Protokolls von src_addr auf dest_addr für die Schnittstelle int_name`-Protokollmeldung aktiviert ist, kann diese `Überprüfung` angezeigt werden. Deaktivieren Sie die Prüfung des umgekehrten Pfads mit dem Befehl **no ip verify reverse path interface (Schnittstellenname)**, um dieses Problem zu beheben:

`no ip verify reverse-path interface (interface name)`

Beispielsweise kann die Sicherheits-Appliance für externen Datenverkehr die Standardroute verwenden, um den Unicast-RPF-Schutz zu erfüllen. Wenn Datenverkehr von einer externen Schnittstelle eingeht und die Quelladresse der Routing-Tabelle nicht bekannt ist, verwendet die Security Appliance die Standardroute, um die externe Schnittstelle korrekt als Quellschnittstelle zu identifizieren.

Wenn der Datenverkehr von einer Adresse, die der Routing-Tabelle bekannt ist, aber der internen Schnittstelle zugeordnet ist, in die externe Schnittstelle eingeht, verwirft die Sicherheits-Appliance das Paket. Wenn Datenverkehr von einer unbekannten Quelladresse in die interne Schnittstelle eingeht, verwirft die Sicherheitsappliance das Paket, da die übereinstimmende Route (die Standardroute) die externe Schnittstelle angibt.

Unicast-RPF wird wie folgt implementiert:

- ICMP-Pakete haben keine Sitzung, daher wird jedes Paket überprüft.
- UDP und TCP verfügen über Sitzungen, sodass für das ursprüngliche Paket eine umgekehrte Route-Suche erforderlich ist. Die nachfolgenden Pakete, die während der Sitzung eingehen, werden mithilfe eines vorhandenen Status überprüft, der während der Sitzung beibehalten wird. Nicht initiale Pakete werden überprüft, um sicherzustellen, dass sie an derselben Schnittstelle eintreffen, die auch vom ursprünglichen Paket verwendet wird.

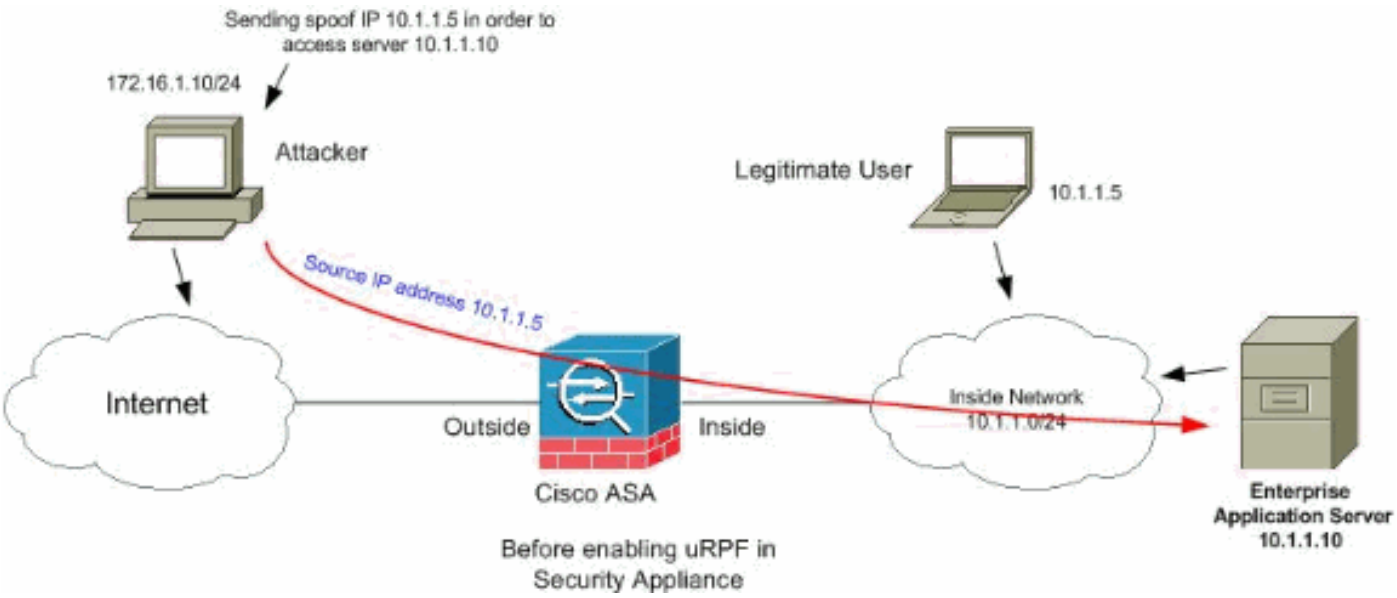
Um Unicast RPF zu aktivieren, geben Sie den folgenden Befehl ein:

```
hostname(config)#ip verify reverse-path interface interface_name
```

Beispiel:

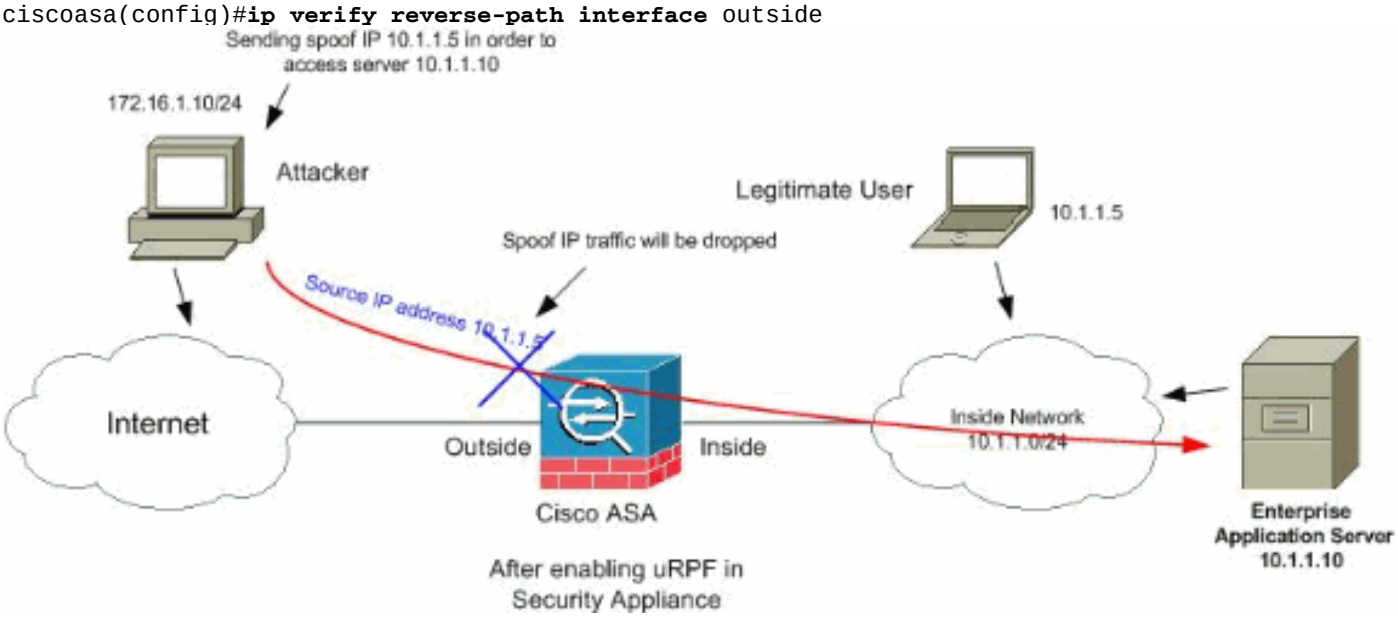
Wie in dieser Abbildung gezeigt, sendet der Angreifer-PC eine Anforderung an den Anwendungsserver 10.1.1.10, indem er ein Paket mit einer gefälschten Quell-IP-Adresse 10.1.1.5/24 sendet, und der Server sendet ein Paket als Antwort auf die Anfrage an die

tatsächliche IP-Adresse 10.1.1.5/24. Diese Art von illegalem Paket greift sowohl den Anwendungsserver als auch legitime Benutzer im internen Netzwerk an.



Unicast-RPF kann Angriffe durch Spoofing der Quelladresse verhindern. Sie müssen den uRPF in der externen Schnittstelle der ASA konfigurieren, wie hier gezeigt:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Spoofing-Identifizierung mithilfe von Syslog-Meldungen

Die Sicherheits-Appliance empfängt weiterhin Syslog-Fehlermeldungen wie abgebildet. Dies weist auf potenzielle Angriffe hin, die gefälschte Pakete verwenden oder die aufgrund von asymmetrischem Routing ausgelöst werden könnten.

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

ErläuterungDies ist eine verbindungsbezogene Nachricht. Diese Meldung tritt auf, wenn ein

Verbindungsversuch mit einer internen Adresse von der Sicherheitsrichtlinie abgelehnt wird, die für den angegebenen Datenverkehrstyp definiert ist. Mögliche *tcp_flags*-Werte entsprechen den Flags im TCP-Header, die vorhanden waren, als die Verbindung verweigert wurde. Beispielsweise wurde ein TCP-Paket angekommen, für das in der Sicherheits-Appliance kein Verbindungsstatus vorhanden ist und das verworfen wurde. Die *tcp_flags* in diesem Paket sind FIN und ACK.Die *tcp_flags* lauten wie folgt:ACK (Bestätigung): Die Bestätigungsnummer wurde empfangen.FIN - Es wurden Daten gesendet.PSH: Der Empfänger hat Daten an die Anwendung weitergeleitet.RST - Die Verbindung wurde zurückgesetzt.SYN - Sequenznummern wurden synchronisiert, um eine Verbindung zu starten.URG: Der Eilzeiger wurde für gültig erklärt.Es gibt viele Gründe dafür, dass statische Übersetzungen auf PIX/ASA fehlschlagen. Ein häufiger Grund ist jedoch, dass die DMZ-Schnittstelle mit derselben Sicherheitsstufe (0) konfiguriert ist wie die externe Schnittstelle.Um dieses Problem zu beheben, weisen Sie allen Schnittstellen eine andere Sicherheitsstufe zu.Weitere Informationen finden Sie unter Konfigurieren von Schnittstellenparametern.Diese Fehlermeldung wird auch angezeigt, wenn ein externes Gerät ein IDENT-Paket an den internen Client sendet, das von der PIX-Firewall verworfen wird. Weitere Informationen finden Sie unter PIX Performance Issues Ursprüngliche by IDENT Protocol (PIX-Leistungsprobleme).

2.

```
%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port
to inside_address/inside_port due to DNS {Response|Query}
```

ErläuterungDies ist eine verbindungsbezogene Nachricht. Diese Meldung wird angezeigt, wenn die angegebene Verbindung aufgrund eines **Deny-**Befehls fehlschlägt. Die Protokollvariable kann ICMP, TCP oder UDP sein.**Empfohlene Aktion:** Mit dem Befehl **show outbound (Ausgehend anzeigen**) können Sie ausgehende Listen überprüfen.

3.

```
%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst
interface_name: IP_address (type dec, code dec)
```

ErläuterungDie Sicherheits-Appliance verweigerte allen eingehenden ICMP-Paketzugriff. Standardmäßig wird allen ICMP-Paketen der Zugriff verweigert, sofern dies nicht ausdrücklich gestattet ist.

4.

```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```

ErläuterungDiese Meldung wird generiert, wenn ein Paket an der Schnittstelle der Sicherheits-Appliance eingeht, die eine Ziel-IP-Adresse von 0.0.0.0 und eine Ziel-MAC-Adresse der Schnittstelle der Sicherheits-Appliance hat. Darüber hinaus wird diese Nachricht generiert, wenn die Sicherheits-Appliance ein Paket mit einer ungültigen Quelladresse verworfen hat, die eine der folgenden oder eine andere ungültige Adresse enthalten kann:Loopback-Netzwerk (127.0.0.0)Broadcast (begrenzt, netzgerichtet, subnetzgerichtet und vollständig subnetzgerichtet)Der Ziel-Host (land.c)Um die Spoof-Paketerkennung weiter zu verbessern, verwenden Sie den Befehl **icmp**, um die Sicherheits-Appliance so zu konfigurieren, dass Pakete mit Quelladressen, die zum internen Netzwerk gehören, verworfen werden. Dies liegt daran, dass der Befehl **access-list** veraltet wurde und nicht mehr garantiert korrekt funktioniert.**Empfohlene Aktion:** Bestimmen Sie, ob ein externer Benutzer versucht, das geschützte Netzwerk zu kompromittieren. Auf falsch konfigurierte Clients prüfen.

5.
```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```
ErläuterungDie Sicherheits-Appliance erhielt ein Paket mit der IP-Quelladresse, die dem IP-Ziel entspricht, und dem Ziel-Port, der dem Quell-Port entspricht. Diese Meldung weist auf ein gefälschtes Paket hin, das für Angriffe auf Systeme entwickelt wurde. Dieser Angriff wird als Landangriff bezeichnet.**Empfohlene Aktion:** Wenn diese Meldung erhalten bleibt, wird möglicherweise ein Angriff ausgeführt. Das Paket liefert nicht genügend Informationen, um zu bestimmen, woher der Angriff stammt.
6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
ErläuterungEin Angriff wird durchgeführt. Jemand versucht, eine IP-Adresse bei einer eingehenden Verbindung zu imitieren. Unicast RPF, auch Reverse Route Lookup genannt, erkannte ein Paket, das keine Quelladresse durch eine Route repräsentiert und geht davon aus, dass es Teil eines Angriffs auf Ihre Sicherheitslösung ist.Diese Meldung wird angezeigt, wenn Sie Unicast RPF mit dem Befehl **ip verify reverse path** aktiviert haben. Diese Funktion funktioniert bei der Paketeingabe an eine Schnittstelle. Wenn sie auf der Außenseite konfiguriert ist, prüft die Sicherheits-Appliance Pakete, die von außen eintreffen.Die Sicherheits-Appliance sucht eine Route anhand der Quelladresse. Wenn kein Eintrag gefunden wird und keine Route definiert ist, wird diese Systemprotokollmeldung angezeigt und die Verbindung wird getrennt.Wenn eine Route vorhanden ist, prüft die Sicherheits-Appliance, welche Schnittstelle sie darstellt. Wenn das Paket an einer anderen Schnittstelle eingeht, handelt es sich entweder um einen Spoof oder um eine asymmetrische Routing-Umgebung, die über mehr als einen Pfad zu einem Ziel verfügt. Die Security Appliance unterstützt kein asymmetrisches Routing.Wenn die Sicherheits-Appliance auf einer internen Schnittstelle konfiguriert ist, prüft sie statische **Route-**Befehlsanweisungen oder RIP. Wenn die Quelladresse nicht gefunden wird, imitiert ein interner Benutzer seine Adresse.**Empfohlene Aktion:** Obwohl ein Angriff ausgeführt wird, ist bei Aktivierung dieser Funktion keine Benutzeraktion erforderlich. Die Security Appliance wehrt den Angriff ab.**Hinweis:** Der Befehl **show asp drop** zeigt die Pakete oder Verbindungen an, die vom beschleunigten Sicherheitspfad (ASP) verworfen wurden. Dies kann Ihnen bei der Problembehebung helfen. Sie gibt auch an, wann die ASP-Dropdownzähler zuletzt gelöscht wurden. Verwenden Sie den Befehl **show asp drop rpf-violated**, mit dem der Zähler erhöht wird, wenn **ip verifiziert, dass** der **Reverse Path** auf einer Schnittstelle konfiguriert ist und die Sicherheits-Appliance ein Paket empfängt, für das die Routensuche der Quell-IP nicht die gleiche Schnittstelle wie die Schnittstelle bietet, auf der das Paket empfangen wurde.
```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```
Hinweis: Empfehlung: Verfolgen Sie die Quelle des Datenverkehrs anhand der Quell-IP, die in dieser nächsten Systemnachricht gedruckt wurde, und untersuchen Sie, warum der Datenverkehr gefälscht wird.**Hinweis: Systemprotokollmeldungen:** 106.021
7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
ErläuterungEin Paket, das mit einer Verbindung übereinstimmt, erreicht eine andere Schnittstelle als die Schnittstelle, auf der die Verbindung begann.Wenn ein Benutzer beispielsweise eine Verbindung über die interne Schnittstelle startet, aber die Sicherheits-Appliance erkennt, dass dieselbe Verbindung über eine Perimeterschnittstelle eingeht, verfügt die Sicherheits-Appliance über mehr als einen Pfad zu einem Ziel. Dies wird als

asymmetrisches Routing bezeichnet und von der Sicherheits-Appliance nicht unterstützt.Ein Angreifer könnte auch versuchen, Pakete von einer Verbindung an eine andere anzuhängen, um in die Sicherheits-Appliance einzudringen. In beiden Fällen zeigt die Sicherheits-Appliance diese Meldung an und verwirft die Verbindung.**Empfehlungsaktion:** Diese Meldung wird angezeigt, wenn der Befehl **ip verify reverse path** nicht konfiguriert ist. Stellen Sie sicher, dass das Routing nicht asymmetrisch ist.

8.
```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```
ErläuterungEin IP-Paket wurde von der ACL abgelehnt. Diese Meldung wird auch angezeigt, wenn die **Log-**Option für eine ACL nicht aktiviert ist.**Empfehlungsaktion:** Wenn Nachrichten von derselben Quelladresse aus gesendet werden, kann dies auf einen Fußdruck oder Port-Scanversuch hinweisen. Kontaktieren Sie die Administratoren des Remote-Hosts.

9.
```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```

10.
```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```
ErläuterungDiese Systemprotokollmeldung gibt an, dass das Herstellen einer neuen Verbindung über das Firewall-Gerät dazu führt, dass mindestens eine der konfigurierten maximalen Verbindungsgrenzen überschritten wird. Die Systemprotokollmeldung gilt sowohl für Verbindungsbeschränkungen, die mit einem statischen Befehl konfiguriert wurden, als auch für solche, die mit dem Cisco Modular Policy Framework konfiguriert wurden. Die neue Verbindung wird erst durch das Firewall-Gerät zugelassen, wenn eine der vorhandenen Verbindungen beendet ist, wodurch die aktuelle Anzahl der Verbindungen unter den konfigurierten Höchstwert fällt.*cnt* - Aktuelle Verbindungsanzahl*limit* - konfigurierte Verbindungsgrenze*dir* - Richtung des eingehenden oder ausgehenden Datenverkehrs*sip* - Quell-IP-Adresse*sport* - Quellport*dip* - Ziel-IP-Adresse*dport* - Zielport*if_name*: Name der Schnittstelle, auf der die Datenverkehrseinheit empfangen wird, entweder Primär oder Sekundär.**Empfehlungsaktion:** Da Verbindungsgrenzen aus gutem Grund konfiguriert werden, könnte diese Systemprotokollmeldung auf einen möglichen DoS-Angriff hinweisen. In diesem Fall könnte die Quelle des Datenverkehrs wahrscheinlich eine gefälschte IP-Adresse sein. Wenn die Quell-IP-Adresse nicht vollständig zufällig ist, kann es hilfreich sein, die Quelle zu identifizieren und sie mithilfe einer Zugriffsliste zu blockieren. In anderen Fällen können Sniffer-Traces abgerufen und die Quelle des Datenverkehrs analysiert werden, um unerwünschten Datenverkehr von legitimem Datenverkehr zu isolieren.

Grundlegende Funktion zur Bedrohungserkennung in ASA 8.x

Die Cisco Security Appliance ASA/PIX unterstützt die Funktion zur Erkennung von Sicherheitsrisiken aus der Software Version 8.0 und höher. Mithilfe der grundlegenden Bedrohungserkennung überwacht die Sicherheits-Appliance aus folgenden Gründen die Rate der verlorenen Pakete und Sicherheitsereignisse:

- Verweigerung durch Zugriffslisten

- Falsches Paketformat (z. B. invalid-ip-header oder invalid-tcp-hdr-length)
- Verbindungsgrenzen überschritten (systemweite Ressourcenbeschränkungen und -beschränkungen in der Konfiguration festgelegt)
- Erkannter DoS-Angriff (z. B. ungültiger SPI, Fehler bei Stateful Firewall-Prüfung)
- Grundlegende Firewall-Überprüfungen sind fehlgeschlagen (Bei dieser Option handelt es sich um eine kombinierte Rate, die alle Firewall-bezogenen Paketverluste in dieser Aufzählung enthält. Nicht enthalten sind Verwerfungen, die nicht mit der Firewall zusammenhängen, wie z. B. Überlastung der Schnittstellen, fehlgeschlagene Pakete bei der Anwendungsinspektion und erkannter Scan-Angriff.)
- Verdächtige ICMP-Pakete erkannt
- Anwendungsprüfung für Pakete fehlgeschlagen
- Schnittstellenüberlastung
- Scan-Angriff erkannt (Diese Option überwacht Scanning-Angriffe; Beispielsweise ist das erste TCP-Paket kein SYN-Paket, oder die TCP-Verbindung ist beim 3-Wege-Handshake fehlgeschlagen. Die vollständige Scanning-Bedrohungserkennung (weitere Informationen finden Sie unter Konfigurieren der Bedrohungserkennung) verarbeitet diese Informationen zur Scanrate und wirkt auf sie durch Klassifizierung von Hosts als Angreifer und automatisches Abschalten dieser Informationen (z. B.).
- Unvollständige Sitzungserkennung, z. B. TCP SYN-Angriff erkannt oder kein Daten-UDP-Sitzungsangriff erkannt.

Wenn die Sicherheits-Appliance eine Bedrohung erkennt, sendet sie sofort eine Systemprotokollmeldung (730100).

Die grundlegende Erkennung von Sicherheitsrisiken beeinträchtigt die Leistung nur bei Verlusten oder potenziellen Bedrohungen. Selbst in diesem Szenario sind die Auswirkungen auf die Leistung unerheblich.

Der Befehl **show Threat Detection** (Bedrohungserkennungsrate anzeigen) wird verwendet, um potenzielle Angriffe zu identifizieren, wenn Sie bei der Sicherheits-Appliance angemeldet sind.

```
ciscoasa#show threat-detection rate
                        Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                0              0       0                16
  1-hour ACL  drop:                0              0       0               112
  1-hour SYN attck:                5              0       2             21438
  10-min  Scanning:                0              0      29               193
  1-hour  Scanning:              106              0      10            384776
  1-hour Bad  pkts:               76              0       2            274690
  10-min  Firewall:                0              0       3                22
  1-hour  Firewall:               76              0       2            274844
  10-min DoS attck:                0              0       0                 6
  1-hour DoS attck:                0              0       0                42
  10-min Interface:                0              0       0               204
  1-hour Interface:               88              0       0            318225
```

Weitere Informationen zum Konfigurationsteil finden Sie im Abschnitt Konfigurieren der grundlegenden Bedrohungserkennung im ASA 8.0-Konfigurationsleitfaden.

Syslog-Meldung 733100

Fehlermeldung:

`%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt`

Das angegebene Objekt in der Systemprotokollmeldung hat die angegebene Burst-Schwellenwertrate oder die durchschnittliche Schwellenwertrate überschritten. Bei dem Objekt kann es sich um die Drop-Aktivität eines Hosts, eines TCP/UDP-Ports, eines IP-Protokolls oder verschiedene Drops aufgrund potenzieller Angriffe handeln. Sie weist darauf hin, dass das System möglicherweise angegriffen wird.

Hinweis: Diese Fehlermeldungen mit Auflösung gelten nur für ASA 8.0 und höher.

1. Object (Objekt): Die allgemeine oder bestimmte Quelle einer Drop Rate Count, die Folgendes enthalten kann:FirewallFehlerhafte PkteDurchsatzgrenzeDoS-AngriffACL-DropConn-GrenzwertICMP-AngriffScannenSYN-AngriffInspektionSchnittstelle
2. rate_ID: Die konfigurierte Rate, die überschritten wird. Die meisten Objekte können für unterschiedliche Intervalle mit bis zu drei unterschiedlichen Raten konfiguriert werden.
3. rate_val: Ein bestimmter Wert für die Rate.
4. total_cnt: Die Gesamtanzahl seit dem Erstellen oder Löschen des Objekts.

Diese drei Beispiele zeigen, wie diese Variablen auftreten:

- Bei einem Schnittstellenausfall aufgrund einer CPU- oder Busbeschränkung:
```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
    second,
max configured rate is 8000; Current average rate is 2030 per second,
max configured rate is 2000; Cumulative total count is 3930654
```
- Bei Scanning-Dropdown aufgrund potenzieller Angriffe:
```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
    second_
max configured rate is 10; Current average rate is 245 per second_
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```
- Bei schädlichen Paketen aufgrund potenzieller Angriffe:
```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

Empfohlene Aktion:

Führen Sie diese Schritte entsprechend dem in der Meldung angegebenen Objekttyp aus:

1. Wenn das Objekt in der Syslog-Meldung eines der folgenden Elemente ist:FirewallFehlerhafte PkteDurchsatzgrenzeDoS-AngriffACL-DropConn-GrenzwertICMP-AngriffScannenSYN-AngriffInspektionSchnittstelleÜberprüfen Sie, ob die Abbruchrate für die aktuelle Umgebung akzeptabel ist.
2. Passen Sie die Schwellenwertrate des jeweiligen Abwurfs an einen geeigneten Wert an, indem Sie den Befehl *xxx **Bedrohungserkennungsrate ausführen***, wobei *xxx* einer der folgenden Werte ist:ACL-DropPaketverlustconn-limit-dropdos-DropFw-DropICMP-Dropinspect-dropinterface-dropScanbedrohungSyn-Angriff
3. Wenn es sich bei dem Objekt in der Syslog-Meldung um einen TCP- oder UDP-Port, ein IP-Protokoll oder einen Host-Drop handelt, prüfen Sie, ob die Abbruchrate für die aktuelle Umgebung akzeptabel ist.
4. Passen Sie die Schwellenwertrate des jeweiligen Abwurfs an einen geeigneten Wert an, indem Sie den Befehl **zur Erkennung von schädlichen Paketen** ausführen. Weitere

Informationen finden Sie im Abschnitt Konfigurieren der grundlegenden Bedrohungserkennung im ASA 8.0-Konfigurationshandbuch.

Hinweis: Wenn die Drop-Rate die Warnungen nicht überschreiten soll, können Sie sie deaktivieren, indem Sie den Befehl **Keine Bedrohungserkennung** ausführen.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie 5500
- Support-Seite für Cisco PIX der Serie 500
- Abwehr von TCP SYN Flooding-Angriffen
- Cisco Applied Mitigation Bulletin: Identifizieren und Verringern der Ausnutzung von Denial-of-Service-Schwachstellen im Content-Switching-Modul
- Cisco Applied Mitigation Bulletin: Identifizieren und Minimieren der Ausnutzung der zahlreichen Schwachstellen in Cisco PIX- und ASA-Appliances und Firewall-Services-Modulen
- IP-Spoofing
- Technischer Support und Dokumentation - Cisco Systems