确定ASA威胁检测功能和配置

目录

简介

本文档介绍威胁检测功能和配置的三个主要组件。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍思科自适应安全设备(ASA)的威胁检测功能的功能和基本配置。威胁检测为防火墙管理员提供了必要的工具，以便在攻击到达内部网络基础设施之前识别、了解和阻止攻击。为此，该功能依赖于许多不同的触发器和统计信息，这将在以下各节中进一步详细说明。

威胁检测可用于运行8.0(2)或更高软件版本的任何ASA防火墙。虽然威胁检测不能替代专用IDS/IPS解决方案，但是可以在IPS不可用的环境中使用，为ASA的核心功能提供额外的保护层。

威胁检测功能

威胁检测功能有三个主要组件：

1. 基本威胁检测
2. 高级威胁检测
3. 扫描威胁检测

以下各节将详细介绍这些组件中的每一个。

基本威胁检测（系统级速率）

默认情况下，在运行8.0(2)及更高版本的所有ASA上启用基本威胁检测。

基本威胁检测监控由于各种原因而由整个ASA丢弃数据包的速率。这意味着基本威胁检测生成的统计信息仅应用于整个设备，通常不够精细，无法提供有关威胁源或特定性质的信息。相反，ASA会监控以下事件的丢弃数据包：

- ACL丢弃(acl-drop) — 访问列表拒绝数据包。
- Bad Pkts(bad-packet-drop) — 无效的数据包格式，包括不符合RFC标准的L3和L4报头。
- Conn Limit(conn-limit-drop) — 超过已配置或全局连接限制的数据包。
- DoS攻击(dos-drop) — 拒绝服务(DoS)攻击。
- 防火墙(fw-drop) — 基本的防火墙安全检查。
- ICMP攻击(icmp-drop) — 可疑ICMP数据包。
- Inspect(inspect-drop) — 应用检测拒绝。
- Interface(interface-drop) — 接口检查丢弃的数据包。
- 扫描（扫描威胁） — 网络/主机扫描攻击。
- SYN攻击(syn-attack) — 不完整的会话攻击，包括没有返回数据的TCP SYN攻击和单向UDP会话。

每个事件都有一组用于识别威胁的特定触发器。大多数触发器与特定的ASP丢弃原因关联，但也会考虑某些系统日志和检查操作。某些触发器由多个威胁类别监控。下表列出了一些最常见的触发因素，但并未列出所有触发因素：

基本威胁	触发器/ASP丢弃原因
ACL 丢包	ACL 丢包
数据包损坏丢包	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-too-long inspect-dns-id-not-matched
连接限制丢包	连接限制
DOS 丢包	sp-security-failed
防火墙丢包	inspect-icmp-seq-num-not-matched inspect-dns-pak-too-long inspect-dns-id-not-matched sp-security-failed ACL 丢包
ICMP 丢包	inspect-icmp-seq-num-not-matched
检查丢包	由检测引擎触发的帧丢弃
接口丢包	sp-security-failed no-route
扫描威胁	tcp-3whs-failed tcp-not-syn sp-security-failed ACL 丢包 inspect-icmp-seq-num-not-matched inspect-dns-pak-too-long inspect-dns-id-not-matched
SYN 攻击	%ASA-6-302014 syslog的终止原因为“SYN超时”

对于每种事件，基本威胁检测都会测量在配置的时间段内发生这些丢弃的速率。这段时间称为平均速率间隔(ARI)，范围为600秒至30天。如果ARI内发生的事件数量超过配置的速率阈值，ASA会将这些事件视为威胁。

基本威胁检测具有两个可配置的阈值，当它将事件视为威胁时：平均速率和突发速率。平均速率只是已配置ARI时间段内的平均每秒丢弃数。例如，如果将ACL丢弃的平均速率阈值配置为400，且ARI为600秒，则ASA将计算ACL在最后600秒丢弃的数据包的平均数量。如果此数值大于400每秒，则ASA会记录威胁。

同样，突发速率非常相似，但查看的快照数据周期更短，称为突发速率间隔(BRI)。BRI始终小于ARI。例如，在前一个示例的基础上，ACL丢弃的ARI仍然是600秒，现在突发速率为800。使用这些值，ASA计算ACL在20秒内丢弃的数据包的平均数量，其中20秒为BRI。如果此计算值超过每秒800个丢包，则记录威胁。为了确定使用哪种BRI，ASA会计算ARI的1/30的值。因此，在先前使用的示例中，600秒的第1/30秒为20秒。但是，威胁检测的最低BRI为10秒，因此，如果ARI的1/30小于10,ASA仍使用10秒作为BRI。此外，必须注意的是，在8.2(1)之前的版本中，此行为有所不同，8.2(1)使用的值是ARI的1/60，而不是1/30。所有软件版本的最低BRI均为10秒。

当检测到基本威胁时，ASA仅生成系统日志%ASA-4-733100，以提醒管理员已识别出潜在威胁。使用show threat-detection rate命令可以查看每个威胁类别的平均事件数、当前事件数和事件总数。累积事件总数是指在最近30个BRI样本中看到的事件总数。

系统日志中的突发速率根据当前BRI中到目前为止已丢弃的数据包数量计算。计算在BRI中定期进行。一旦发生漏洞，就会生成系统日志。 限制在BRI中仅生成一个系统日志。“show threat-detection rate”中的突发速率根据上一个BRI中丢弃的数据包数量计算。区别在于，系统日志具有时间敏感性，因此，如果当前BRI发生漏洞，将有机会捕获该漏洞。 “show threat-detection rate”对时间不太敏感，因此使用来自上一个BRI的编号。

基本威胁检测不会采取任何操作来阻止异常流量或防止未来攻击。从这个意义上讲，基本威胁检测纯粹是信息性的，可以用作监控或报告机制。

高级威胁检测（对象级别统计数据和前N个）

与基本威胁检测不同，高级威胁检测可用于跟踪更精细对象的统计信息。ASA支持对受TCP拦截保护的主机IP、端口、协议、ACL和服务器的跟踪统计信息。高级威胁检测仅对ACL统计信息默认启用。

对于主机、端口和协议对象，威胁检测会跟踪该对象在特定时间段内发送和接收的数据包、字节数和丢包数。对于ACL，威胁检测会跟踪特定时间段内攻击最多的前10个ACE（包括允许和拒绝）。

在所有这些情况下，跟踪的时间段分别为20分钟、1小时、8小时和24小时。尽管时间段本身不可配置，但每个对象跟踪的期间数可以使用“number-of-rate”关键字进行调整。有关详细信息，请参阅配置部分。例如，如果“number-of-rate”设置为2，您将看到20分钟、1小时和8小时的所有统计信息。如果“number-of-rate”设置为1，您将看到20分钟、1小时的所有统计信息。无论发生什么情况，始终显示20分钟速率。

启用TCP拦截后，威胁检测可以跟踪被视为遭受攻击并受TCP拦截保护的前10台服务器。TCP拦截的统计数据与基本威胁检测类似，因为用户可以配置测量的速率间隔以及特定平均值(ARI)和突发(BRI)速率。TCP拦截的高级威胁检测统计信息仅在ASA 8.0(4)及更高版本中可用。

通过show threat-detection statistics和show threat-detection statistics top命令查看高级威胁检测统计信息。此功能还负责填充ASDM防火墙控制面板上的“顶部”图形。高级威胁检测生成的系统日志只有%ASA-4-733104和%ASA-4-733105，当TCP拦截统计信息的平均和突发率（分别为）超过时触发这些系统日志。

与基本威胁检测类似，高级威胁检测也只是提供信息。根据高级威胁检测统计信息，不采取任何操作来阻止流量。

扫描威胁检测

扫描威胁检测用于跟踪在子网中创建过多主机或主机/子网中多个端口连接的可疑攻击者。默认情况下禁用扫描威胁检测。

扫描威胁检测基于基本威胁检测的概念，基本威胁检测已经定义了扫描攻击的威胁类别。因此，基本威胁检测和扫描威胁检测之间共享速率间隔、平均速率(ARI)和突发速率(BRI)设置。两种功能之间的区别在于，虽然基本威胁检测仅表示超过平均或突发速率阈值，但扫描威胁检测会维护一个包含攻击者和目标IP地址的数据库，可以帮助提供扫描所涉及主机周围的更多情景。此外，扫描威胁检测仅考虑目标主机/子网实际接收的流量。即使流量被ACL丢弃，基本威胁检测仍可以触发扫描威胁。

扫描威胁检测可选择性地通过避开攻击者IP来应对攻击。这使得扫描威胁检测成为威胁检测功能中唯一可以主动影响通过ASA的连接的子集。

当扫描威胁检测检测到攻击时，将为攻击者和/或目标IP记录%ASA-4-733101。如果将此功能配置为避开攻击者，则扫描威胁检测生成避开时，会记录%ASA-4-733102。删除shun时，会记录%ASA-4-733103。show threat-detection scanning-threat命令可用于查看整个扫描威胁数据库。

限制

- 威胁检测仅在ASA 8.0(2)及更高版本中可用。ASA 1000V平台不支持此功能。
- 仅在单情景模式下支持威胁检测。
- 仅能检测到通过设备的威胁。威胁检测不考虑发送到ASA本身的流量。
- 由目标服务器重置的TCP连接尝试不计为SYN攻击或扫描威胁。

配置

基本威胁检测

使用threat-detection basic-threat命令启用基本威胁检测。

<#root>

```
ciscoasa(config)#
```

threat-detection basic-threat

可以使用show run all threat-detection命令查看默认速率。

```
<#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
```

为了使用这些自定义值调整这些速率，只需为相应的威胁类别重新配置threat-detection rate命令。

```
<#root>

ciscoasa(config)#

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

每个威胁类别最多可以定义3种不同的速率（速率ID为1、速率2和速率3）。在%ASA-4-733100 syslog中引用了超过的特定速率ID。

在上一个示例中，仅当在1200秒内ACL丢弃数超过250个丢包/秒或在40秒内550个丢包/秒时，威胁检测才会创建系统日志733100。

高级威胁检测

使用threat-detection statistics命令以启用高级威胁检测。如果未提供特定功能关键字，该命令将启用所有统计信息的跟踪。

```
<#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>
```

要配置主机、端口、协议或ACL统计信息跟踪的速率间隔数，请使用number-of-rate关键字。

```
<#root>
ciscoasa(config)#
threat-detection statistics host number-of-rate 2
```

number-of-rate关键字将威胁检测配置为仅跟踪最短n个间隔。

要启用TCP拦截统计信息，请使用threat-detection statistics tcp-intercept命令。

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept
```

要配置TCP拦截统计数据的自定义速率，请使用rate-interval、average-rate和burst-rate关键字。

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

扫描威胁检测

要启用扫描威胁检测，请使用threat-detection scanning-threat命令。

```
<#root>
ciscoasa(config)#
```

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

要调整扫描威胁的速率，请使用基本威胁检测所用的threat-detection rate命令。

```
<#root>

ciscoasa(config)#

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

要允许ASA避开扫描攻击者IP，请将shun关键字添加到threat-detection scanning-threat命令。

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

这样，扫描威胁检测可以为攻击者创建一个避开一小时的时间。要调整shun的持续时间，请使用threat-detection scanning-threat shun duration命令。

```
<#root>

ciscoasa(config)#

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

在某些情况下，您可以防止ASA避开某些IP。为此，请使用threat-detection scanning-threat shun except命令创建例外。

```
<#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
```

性能

基本威胁检测对ASA的性能影响非常小。高级和扫描威胁检测需要占用更多的资源，因为它们必须跟踪内存中的各种统计信息。只有启用了shun功能的扫描威胁检测才能主动影响本来可以允许的流量。

随着ASA软件版本的改进，威胁检测的内存利用率已显着优化。但是，必须注意在启用威胁检测之前和之后监控ASA的内存利用率。在某些情况下，最好在主动排除特定问题的同时临时启用某些统计信息（例如，主机统计信息）。

有关威胁检测内存使用情况的更多详细信息，请运行show memory app-cache threat-detection [detail]命令。

推荐的操作

这些部分提供了一些一般建议，用于说明在发生各种威胁检测相关事件时可以采取的操作。

当超过基本丢包率并生成%ASA-4-733100时

确定%ASA-4-733100系统日志中提及的特定威胁类别，并将其与 show threat-detection rate .使用此信息，检查 show asp drop 以确定流量被丢弃的原因。

要获得因特定原因丢弃的流量的更详细视图，请使用具有所述原因的ASP丢弃捕获，以查看丢弃的所有数据包。例如，如果记录了ACL Drop威胁，请捕获ASP丢弃原因 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
```

此捕获显示丢弃的数据包是从10.10.10.10到192.168.1.100的UDP/53数据包。

如果%ASA-4-733100报告扫描威胁，暂时启用扫描威胁检测也很有用。这允许ASA跟踪攻击中涉及的源IP和目标IP。

由于基本威胁检测主要监控ASP已丢弃的流量，因此无需直接操作即可阻止潜在威胁。例外情况是SYN攻击和扫描威胁，这些威胁涉及通过ASA的流量。

如果在ASP丢弃捕获中看到的丢弃是合法和/或网络环境的预期丢弃，请将基本速率间隔调整为更合适的值。

如果丢弃显示非法流量，则必须在流量到达ASA之前采取措施阻止流量或限制流量速率。这可能包括上游设备上的ACL和QoS。

对于SYN攻击，可以在ASA上的ACL中阻止流量。也可以将TCP拦截配置为保护目标服务器，但这可能只会导致记录的Conn Limit威胁。

对于扫描威胁，也可以在ASA上的ACL中阻止流量。使用扫描威胁检测 shun可以启用该选项，以允许ASA在定义的时间段内主动阻止来自攻击者的所有数据包。

检测到扫描威胁且已记录%ASA-4-733101时

%ASA-4-733101必须列出目标主机/子网或攻击者IP地址。有关目标和攻击者的完整列表，请查看 show threat-detection scanning-threat.

在ASA接口上捕获面向攻击者和/或目标的数据包也有助于明确攻击的性质。

如果检测到的扫描不是预期扫描，则必须在流量到达ASA之前采取措施阻止流量或限制流量的速率。这可能包括上游设备上的ACL和QoS。当 shun选项已添加到扫描威胁检测配置中，它允许ASA在定义的时间段内主动丢弃来自攻击者IP的所有数据包。作为最后手段，还可以通过ACL或TCP拦截策略在ASA上手动阻止流量。

如果检测到的扫描是误报，请将Scanning Threat rate intervals调整为更适合网络环境的值。

当避开攻击者并且%ASA-4-733102被记录时

%ASA-4-733102列出回避的攻击者的IP地址。请使用 show threat-detection shun 命令，以便查看威胁检测专门避开的攻击者的完整列表。请使用 show shun 命令，以查看ASA主动避开的所有IP的完整列表（这包括来自威胁检测之外的来源）。

如果shun是合法攻击的一部分，则无需进一步操作。但是，最好手动阻止攻击者的流量尽量往上游到源地址。这可以通过ACL和QoS来实现。这可确保中间设备无需在非法流量上浪费资源。

如果触发避开的扫描威胁为误报，请手动使用 clear threat-detection shun [IP_address] 命令。

当记录%ASA-4-733104和/或%ASA-4-733105时

%ASA-4-733104和%ASA-4-733105列出当前受TCP拦截保护的攻击所针对的主机。有关攻击率和受保护服务器的更多详细信息，请查看 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)
```

当高级威胁检测检测到此类攻击时，ASA已通过TCP拦截保护目标服务器。检验已配置的连接限制，以确保它们为攻击的性质和速率提供充分的保护。此外，最好手动阻止攻击者的流量，使其尽可能向上游到达源地址。这可以通过ACL和QoS来实现。这可确保中间设备无需在非法流量上浪费资源。

如果检测到的攻击是误报，请将TCP拦截攻击的速率调整为更合适的值，并使用 threat-detection statistics tcp-intercept 命令。

如何手动触发威胁

要测试和排除故障，手动触发各种威胁非常有用。本节包含如何触发几种常见威胁类型的提示。

基本威胁 — ACL丢弃、防火墙和扫描

要触发特定的基本威胁，请参阅上一功能部分中的表。选择特定的ASP丢弃原因，并通过ASA发送由相应的ASP丢弃原因丢弃的流量。

例如，ACL Drop、Firewall和Scanning威胁都会考虑acl-drop丢弃的数据包的速率。完成以下步骤以同时触发这些威胁：

1. 在ASA的外部接口上创建一个ACL，明确丢弃发送到ASA(10.11.11.11)内部的目标服务器的所有TCP数据包：

   ```
   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. 从ASA外部的攻击者(10.10.10.10)使用nmap对目标服务器上的每个端口运行TCP SYN扫描：

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

> 注意：T5配置nmap以尽快运行扫描。根据攻击者PC的资源，这仍不足以触发某些默认速率。如果是这种情况，只需降低您想要查看的威胁的已配置速率。当您将ARI和BRI设置为0时，基本威胁检测将始终触发威胁，无论其速率如何。

3. 请注意，检测到ACL丢弃、防火墙和扫描威胁的基本威胁：

```
%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
```


注意：在本示例中，ACL丢弃和防火墙ARI和BRI已设置为0，因此它们始终会触发威胁。这就是最大配置速率列为0的原因。

高级威胁 — TCP拦截

1. 在外部接口上创建ACL，以允许发送到ASA(10.11.11.11)内部目标服务器的所有TCP数据包：

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

2. 如果目标服务器实际上并不存在，或者它重置了攻击者的连接尝试，请在ASA上配置一个虚假ARP条目，以便将攻击流量从内部接口黑洞出去：

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

3. 在ASA上创建简单TCP拦截策略：

```
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
```

从ASA外部的攻击者(10.10.10.10)使用nmap对目标服务器上的每个端口运行TCP SYN扫描：

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

请注意，威胁检测会跟踪受保护的服务器：

<#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)
```

扫描威胁

1. 在外部接口上创建ACL，以允许发送到ASA(10.11.11.11)内部目标服务器的所有TCP数据包：

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

> 注意：为了让扫描威胁检测跟踪目标和攻击者IP，必须允许流量通过ASA。

2. 如果目标服务器实际上并不存在，或者它重置了攻击者的连接尝试，请在ASA上配置一个虚假ARP条目，以便将攻击流量从内部接口黑洞出去：

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

> 注：由目标服务器重置的连接不计入威胁的一部分。

3. 从ASA外部的攻击者(10.10.10.10)使用nmap对目标服务器上的每个端口运行TCP SYN扫描：

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

> 注意：T5配置nmap以尽快运行扫描。根据攻击者PC的资源，这仍不足以触发某些默认速率。如果是这种情况，只需降低您想要查看的威胁的已配置速率。当您将ARI和BRI设置为0时，基本威胁检测将始终触发威胁，无论其速率如何。

4. 请注意，检测到扫描威胁，跟踪攻击者的IP，并避开攻击者：

```
%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
```

相关信息

- ASA配置指南
- ASA命令参考
- 思科安全防火墙ASA系列系统日志消息
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。