确定ASA威胁检测功能和配置

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

威胁检测功能

- 基本威胁检测（系统级速率）
- 高级威胁检测（对象级别统计数据和前N个）
- 扫描威胁检测
- 针对VPN服务的威胁检测(9.20(3)+/所列系列)

限制

配置

- 基本威胁检测
- 高级威胁检测
- 扫描威胁检测
- 针对VPN服务的威胁检测

性能

推荐的操作

- 当超过基本丢包率并生成%ASA-4-733100时
- 检测到扫描威胁且已记录%ASA-4-733101时
- 当避开攻击者并且%ASA-4-733102被记录时
- 当记录%ASA-4-733104和/或%ASA-4-733105时
- 当VPN主机被避开且%ASA-4-733201被记录时

如何手动触发威胁

- 基本威胁 — ACL丢弃、防火墙和扫描
- 高级威胁 — TCP拦截
- 扫描威胁

相关信息

简介

本文档介绍思科安全防火墙ASA上的威胁检测功能和配置。

先决条件

要求

思科建议了解ASA CLI、访问控制和（用于VPN威胁检测）远程访问VPN。

使用的组件

- 传统威胁检测（基本、高级、扫描）：ASA软件8.0(2)及更高版本。TCP拦截统计信息需要8.0(4)/8.1(2)或更高版本。避开持续时间可配置为8.0(4)/8.1(2)。
- 针对VPN服务的威胁检测:在9.20列车上以9.20(3)的时速引入。 思科还记录了9.16(4)67、9.17(1)45、9.18(4)40、9.19(1)。37和9.22(1.1)(9.22(1)未发布)下的其他列车中的这些最低要求。

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

ASA上的威胁检测提供第3/4层前线防御。它基于丢包统计信息和可选对象级别“top”报告构建基线。它不能取代专用IPS或下一代IPS模块，后者会检查第7层之前允许的流量；这两者可以协同工作。



注意：本文介绍ASA CLI功能集。思科安全防火墙威胁防御(FTD)在“访问控制策略高级设置”(Access Control Policy Advanced Settings)下显示相关但并不相同的威胁检测功能。请勿将FTD威胁检测视为这些命令的1:1映射。有关详细信息，请参阅ASA到威胁防御功能映射文章。

威胁检测为防火墙管理员提供识别、了解和（用于扫描和VPN服务）阻止攻击的工具。它依赖于速率触发器、对象级别统计信息和可选的自动调速。

此功能有四个组件：

1. 基本威胁检测（系统级丢包率）— 默认启用
2. 高级威胁检测（对象级别统计数据和前N）— 默认情况下启用ACL统计信息
3. 扫描威胁检测（攻击者/目标数据库，可选shun）— 默认情况下禁用

4. 针对VPN服务的威胁检测（RA VPN DoS保护、自动规避） — 默认情况下禁用；9.20(3)+/列车

威胁检测功能

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ASA上启用基本威胁检测。

它监控整个ASA因各种原因丢弃数据包的速率。统计信息适用于整个设备，通常不够精细以识别源主机。ASA监控这些事件的丢弃数据包：

- ACL丢弃(acl-drop)：访问列表拒绝的数据包。
- 错误数据包（错误数据包丢弃）:无效的数据包格式，包括不符合RFC标准的L3和L4报头（例如，invalid-ip-header或invalid-tcp-hdr-length）。
- 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):拒绝服务攻击（例如，无效SPI或状态防火墙检查失败。）
- 防火墙（防火墙丢弃）:此列表中与防火墙相关的丢弃的合并速率。它不包括非防火墙丢弃，例如接口过载、检查故障或检测到的扫描攻击。
- ICMP攻击(icmp-drop):可疑ICMP数据包。
- 检查(inspect-drop):通过应用检测拒绝。
- 接口（接口丢弃）:接口检查丢弃的数据包（过载）。
- 扫描（扫描威胁）:网络/主机扫描攻击（例如，第一个TCP数据包不是SYN，或三次握手失败。）完全扫描威胁检测使用此速率对主机进行分类并选择性地避开主机。
- SYN攻击（syn攻击）:不完整的会话攻击，包括TCP SYN攻击和无返回数据的单向UDP会话。

大多数触发器映射到特定ASP丢弃原因；某些系统日志和检查操作也会计数。某些触发器出现在多个威胁类别中。常见映射（并非详尽无遗）：

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”

对于每个事件，基本威胁检测都会测量配置平均速率间隔(ARI)内从600秒到30天的丢弃率。如果ARI中的事件超过配置的阈值，ASA会将其视为威胁。

有两个阈值：平均速率和突发速率。ARI上的平均速率是每秒丢弃数。突发速率使用较短的突发速率间隔(BRI)。 自8.2(1)以来，BRI是ARI的1/30，或10秒，以较高者为准。在8.2(1)之前，BRI是ARI的1/60。10秒的最小值适用于所有软件版本。

示例：ARI 600秒的ACL丢弃平均速率400意味着ASA在过去600秒内平均ACL丢弃，如果平均值超过每秒400，则记录威胁。具有相同ARI的突发速率800使用20秒(600 / 30)的BRI。 如果20秒窗口中ACL丢弃超过800秒，则记录威胁。

当检测到基本威胁时，ASA生成系统日志%ASA-4-733100。如果超过平均速率和突发速率，ASA可以发送两个733100消息（每个速率类型一个），每个突发周期每个速率类型最多一个消息。

运行show threat-detection rate命令查看平均事件、当前事件、触发器计数和事件总数。ASA在每个突发周期结束时为30个已完成的BRI存储计数。未完成的当前BRI通常从平均值中排除。总事件计数是这30个BRI样本中的事件总和（如果未完成的BRI已超过最早的样本，则实时例外）。

系统日志中的突发速率根据当前BRI中到目前为止的丢弃进行计算，并定期采样，因此可以在BRI完成之前报告漏洞（每个BRI的每种速率类型对应一个系统日志）。 show threat-detection rate中的突发/当前速率使用最后完成的BRI。

基本威胁检测不会丢弃或回避流量。它仅供参考（监控和报告）。 性能影响微不足道，主要发生于出现丢包或潜在威胁时。

高级威胁检测（对象级别统计数据和前N个）

高级威胁检测可跟踪更精细对象的统计信息：受TCP拦截保护的主机IP、端口、协议、ACL和服务器。默认情况下仅启用ACL统计信息。主机统计信息在高流量下对性能有显着影响；在需要时临时启用它们。端口统计信息产生的影响较为温和。

对于主机、端口和协议对象，ASA跟踪在固定窗口中发送和接收的数据包、字节和丢包。对于ACL，它会跟踪这些窗口中的前10个ACE（允许和拒绝）命中。在顶部ACL显示中，未区分允许和拒绝的ACE命中。

固定窗口为20分钟、1小时、8小时和24小时。窗口本身不可配置。速率数{1 | 2 | 3}关键字（仅主机、端口和协议）控制保留多少个较长的间隔：

- 1（默认） — 仅最短速率间隔，以使内存使用率较低
- 2 — 两个最短间隔
- 3 - 1小时、8小时和24小时

当主机在扫描威胁主机数据库中处于活动状态时，主机统计信息会累积，并在处于非活动状态10分钟后清除。

启用TCP Intercept后，威胁检测可以跟踪遭受攻击的前10台服务器。TCP拦截统计信息使用可配置的监控窗口以及平均阈值和突发阈值(在8.0(4)及更高版本中可用)。 默认值：

- 速率间隔（历史记录窗口）：30分钟（范围为1-1440）。 ASA在窗口期间采样30次（默认情况下每60秒）。
- 脉冲率:400次攻击/秒 — 系统日志%ASA-4-733104
- 平均速率:200次攻击/秒 — 系统日志%ASA-4-733105

通过运行show threat-detection statistics和show threat-detection statistics top命令查看统计信息。此功能还填充了传统ASDM防火墙控制面板上的“顶部”图形。

高级威胁检测只是提供信息，但TCP拦截已保护服务器。仅从这些统计信息中不会应用其他块。

扫描威胁检测

扫描威胁检测会跟踪在子网中太多主机或主机或子网中太多端口上创建连接的主机。默认情况下禁用该技术。与基于IPS签名的扫描检测不同，ASA扫描威胁检测维护主机数据库（无返回活动的连接、封闭端口访问、某些TCP行为等）。

它与基本扫描威胁类别共享速率间隔、平均速率(ARI)和突发速率(BRI)。不能为基本与扫描配置不同的速率。区别在于扫描威胁检测可保留攻击者和目标IP数据库。仅统计允许通过ASA并创建流量的流量。基本威胁检测仍然可以对ACL拒绝的流733100发出扫描威胁检测；扫描威胁检测则不会。

如果超过来自主机的流量的扫描速率，则该主机就是攻击者。如果发往主机的流量超过，则该主机为目标。已记录系统日志%ASA-4-733101。您可以选择避开攻击者(%ASA-4-733102（添加避开时），%ASA-4-733103（删除时）。 默认回避持续时间为3600秒（1小时），可配置为10到2592000秒。

使用shun扫描威胁检测是能够主动丢弃其他允许的流量的两个功能之一（另一个是VPN威胁检测）。

对攻击者/目标数据库运行show threat-detection scanning-threat命令，仅对扫描威胁规避运行show threat-detection shun。



注意：对于发送高合法控制平面或组播流量（例如PIM路由器）且具有threat-detection scanning-threat shun except的主机，免除这些主机，或者当安装了shun时可以丢弃这些数据包。

针对VPN服务的威胁检测(9.20(3)+/所列系列)

VPN威胁检测可保护ASA远程访问VPN头端免受IPv4 DoS式攻击。默认情况下禁用所有三项服务。当服务已启用且主机超过其阈值时，ASA会自动对该IPv4地址进行分流，直到您删除分流。

服务：

- remote-access-authentication:连续RA VPN登录失败（密码喷射/暴力）。 停下1-1440分钟；阈值1-100。不计算SAML身份验证失败。
- remote-access-client-initiations:重复的SSL/IKEv2连接会启动，但并非从一台主机完成。停下1-1440分钟；阈值5-100。
- invalid-vpn-access：尝试访问仅用于内部设备操作的内置隧道组。匹配的IPv4地址会立即避开（按下/阈值实际上是1/1。）

即使这些攻击失败，它们也会消耗身份验证和会话资源。当您设置抑制和阈值时，记入PAT（酒店、CGNAT）：许多有效用户可以共享一个公有IP。使用更高的值，以便合法用户能够完成连接。

仅VPN威胁检测监控到预置的IPv4。Shuns出现在show shun中，而不是show threat-detection shun中。相关系统日志：%ASA-6-733200（信息）和%ASA-4-733201(超过阈值；shun已安装。)

限制

- 传统威胁检测需要ASA 8.0(2)或更高版本。以前的ASA 1000V平台不支持此功能（该平台已停产）。
- 安全情景:除高级威胁统计信息和VPN服务外，仅支持单情景模式中的威胁检测。在多情景模式下，TCP拦截统计信息是支持的高级统计信息。多模式也支持VPN威胁检测。
- 防火墙模式:在路由和透明模式下受支持。
- 对于基本、高级和扫描统计信息，仅监控通过设备的流量。发送到ASA本身的流量不计入。

- 对于VPN服务，仅监控到机箱内的IPv4。
- ACL拒绝的流量不会触发扫描威胁检测（攻击者/目标跟踪）。 基本扫描威胁率在ACL丢弃时可能会增加。
- 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。
- VPN authentication-failure检测不包括SAML故障。

配置

基本威胁检测

默认情况下启用基本威胁检测，您可以通过以下方式重新启用基本威胁检测：

<#root>

```
ciscoasa(config)#
```

threat-detection basic-threat

禁用no threat-detection basic-threat。使用show run all threat-detection的默认速率视图：

<#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
```

通过运行threat-detection rate命令调整类别。每个类别最多可以有三种速率（速率1、2和3）。 在以下位置引用超出的速率733100:

<#root>

```
ciscoasa(config)#

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

在本示例中，当ACL丢弃超过250/sec（1200秒）或550/sec(550/sec（40秒）(1200/30)时，将生成733100。

此命令中的scanning-threat关键字与扫描威胁检测共享。即使禁用基本威胁检测，也可以设置扫描速率。

高级威胁检测

运行threat-detection statistics命令以启用高级统计信息。如果没有关键字，则启用所有统计类型：

<#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>
```

---

no threat-detection statistics(no options)删除所有统计命令，包括默认threat-detection statistics access-list。

ACL统计信息（默认为）：

<#root>

ciscoasa(config)#

threat-detection statistics access-list

主机、端口或协议，具有可选数量的速率间隔：

<#root>

ciscoasa(config)#

threat-detection statistics host number-of-rate 2

ciscoasa(config)#

threat-detection statistics port number-of-rate 2

ciscoasa(config)#

threat-detection statistics protocol number-of-rate 3

TCP拦截统计信息（也可用于多情景模式）：

<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept

ciscoasa(config)#

threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600

扫描威胁检测

<#root>

ciscoasa(config)#

threat-detection scanning-threat

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20

ciscoasa(config)#

threat-detection scanning-threat shun

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000

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

---

您可以在一行中组合使用shun和except，并多次输入命令以免除更多地址或对象组。

<#root>

ciscoasa(config)#

threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0

针对VPN服务的威胁检测

<#root>

ciscoasa(config)#

threat-detection service invalid-vpn-access

ciscoasa(config)#

```
threat-detection service remote-access-client-initiations hold-down 10 threshold 20

ciscoasa(config)#

threat-detection service remote-access-authentication hold-down 10 threshold 20
```

使用同一命令的no形式禁用服务。使用clear threat-detection service重置计数器。

有关专用演练，请参阅[在安全防火墙ASA上配置远程访问VPN服务的威胁检测](#)（文档ID 222315。）

性能

基本威胁检测对性能的影响很小。高级主机统计信息和扫描威胁检测会占用更多的资源，因为它们存储的是每个主机和每个对象的数据。对特定问题进行故障排除时，暂时启用主机统计信息。

可丢弃其他允许的流量的功能：

- 使用shun扫描威胁检测
- VPN威胁检测服务（自动回避）

在启用高级或扫描功能之前和之后监控内存：

<#root>

```
ciscoasa#

show threat-detection memory

ciscoasa#

show memory app-cache threat-detection detail
```

---

show threat-detection memory(8.3(1)+)是用于高级统计信息内存的已编档命令。show memory app-cache threat-detection [detail]显示应用区块缓存。

推荐的操作

当超过基本丢包率并生成%ASA-4-733100时

请注意图中的威胁733100别，并与show threat-detection rate关联。然后检查show asp drop以了解丢弃原因。

出于特定原因，请使用ASP丢弃捕获：

<#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
```

本示例是从10.10.10.10到192.168.1.100的UDP/53数据包。

如果733100报告扫描，请暂时启用扫描威胁检测，以便ASA可以记录攻击者和目标IP。

基本威胁检测主要计算ASP已丢弃的流量，因此不需要额外的丢弃操作。SYN攻击和扫描威胁除外，这些威胁涉及通过ASA的流量。

如果丢弃对于环境是合法的，则提高基本速率间隔。如果是攻击流量，则在ASA之前阻止或阻止上行速率限制(ACL、QoS)。

对于SYN攻击，请拒绝ACL中的源，或启用TCP拦截以保护目标（这样可改为生成连接限制威胁）。 对于扫描，您可以在ACL中拒绝或使用shun启用扫描威胁检测。

检测到扫描威胁且已记录%ASA-4-733101时

733101列出目标主机/子网或攻击者。对于完整列表，请运行show threat-detection scanning-threat命令。

在面向攻击者和面向目标的接口上捕获有助于确认扫描。

如果扫描意外进行，则阻止或速率限制上游。添加shun允许ASA在配置的持续时间内丢弃来自攻击者的所有数据包。作为最后手段，使用ACL或TCP拦截功能在ASA上阻止。

如果为误报，请提高扫描威胁率间隔。

当避开攻击者并且%ASA-4-733102被记录时

733102列出扫描威胁规避目标。运行show threat-detection shun命令，仅扫描 — threat shun。对ASA上的每个活动shun运行show shun（扫描、VPN威胁检测和手动shun。）

对于真正的攻击，也尽可能地阻止上游，因此中间设备不会处理流量。对于误报，请删除扫描回避：

<#root>

ciscoasa#

clear threat-detection shun

ciscoasa#

clear threat-detection shun 10.1.1.6

当记录%ASA-4-733104和/或%ASA-4-733105时

这些系统日志将已受TCP拦截保护的主机命名为。733104是突发速率；733105是平均速率。检查：

<#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)
```

检验连接限制是否足够。尽可能阻止攻击者上游。对于误报，请调整threat-detection statistics tcp-intercept速率。

当VPN主机被避开且%ASA-4-733201被记录时

733201命名超出阈值的服务和对等体。确认方式：

```
<#root>

ciscoasa#

show threat-detection service

ciscoasa#

show threat-detection service remote-access-authentication details

ciscoasa#

show shun
```

被避开的IP从服务条目列表中删除；阻止计数器增加。如果主机是合法的（共享PAT，客户端配置错误），请删除shun:

```
<#root>

ciscoasa#

no shun 192.168.100.101

ciscoasa#
```

```
no shun 192.168.100.101 interface outside
```

如果地址在多个接口上被避开并且您省略了接口，则no shun仅从一个接口移除该避开(route-lookup)。 指定接口以清除其他接口；clear shun将删除所有接口上的所有分路。

请勿对VPN分流运行clear threat-detection shun;该命令仅适用于扫描威胁检测。

如果回避了有效用户，请提高抑制/阈值（尤其是在PAT之后）或禁用服务，直到您调整服务。

如何手动触发威胁

使用这些实验方法来测试和排除故障。仅在隔离环境中运行它们。

基本威胁 — ACL丢弃、防火墙和扫描

ACL Drop、Firewall和Scanning基本类别都考虑acl-drop。要同时触发它们，请执行以下操作：

1.在外部接口上创建拒绝TCP到达内部目标(10.11.11.11)的ACL:

```
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.从外部攻击者(10.10.10.10)运行TCP SYN扫描：

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



注意：T5以尽可能快的速度运行nmap。对于默认速率，攻击者PC仍可能太慢。降低您想要查看的类别的已配置速率。将ARI和BRI设置为0会导致基本威胁检测触发，而不考虑速率

。

3.记录基本威胁，例如：

```
%ASA-4-733100: [ 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-4-733100: [ 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-4-733100: [ 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/BRI设置为0，因此它们始终触发（最大配置速率显示为0。）

高级威胁 — TCP拦截

1.允许TCP到达内部目标：

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

2.如果目标不存在或重置连接，则使用静态ARP条目将黑洞设置为：

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

3.创建简单的TCP拦截（半期/连接限制）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
```

从攻击者处，扫描：

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

<#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)
```

扫描威胁

1.允许TCP到达目标（扫描威胁检测仅跟踪允许的已创建流量）：

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

2.如果需要，使用静态ARP建立黑洞。不计算实际服务器重置的连接。

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

3.从攻击者处扫描。如果nmap不够快，则降低速率或将ARI/BRI设置为0。

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

4.启用shun时的预期日志：

```
%ASA-4-733100: [ 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

- 思科安全防火墙ASA防火墙CLI配置指南，9.20 — 威胁检测（也针对9.23/9.24发布）
- 在安全防火墙ASA上配置远程访问VPN服务的威胁检测（文档ID 222315）
- ASA命令参考 — 威胁检测命令
- ASA命令参考 — show threat-detection命令
- Cisco安全防火墙ASA系列系统日志消息(733100-733105、733200-733201)
- ASA到威胁防御功能映射 — 威胁检测
- 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）。