ASA威胁检测功能和配置

目录

简介

本文描述思科可适应安全工具(ASA)的威胁检测功能的功能和基本配置。在他们到达内部网络基础设施前，威胁检测提供防火墙管理员必要的工具识别，了解和终止攻击。为了执行如此，功能依靠一定数量不同的触发和统计信息，在这些部分的更详细的资料描述。

威胁检测在运行软件版本8.0(2)或以后的所有ASA防火墙可以使用。虽然威胁检测不是一专用的IDS/IPS解决方案的一种替代品，可以用于IPS不是可用提供防护一块已添加层给ASA的核心功能的环境。

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. 先进的威胁检测
3. 扫描的威胁检测

这些组件中的每一个在这些部分详细描述。

基本威胁检测(系统层速率)

默认情况下基本威胁检测在所有ASA运行8.0(2)启用及以后。

基本威胁检测监控数据包由整体上ASA由于多种原因丢弃的速率。这意味着基本威胁检测生成的统计信息在威胁的来源或特性只适用于整个设备并且通常不是足够粒状提供信息。反而， ASA监控这些事件的丢弃的数据包：

- **ACL丢弃(ACL丢弃)** -数据包由访问列表拒绝
- **Bad数据包(BAD数据包丢弃)** -无效的信息包格式化，包括L3和L4报头不依照RFC标准
- **Conn限制(CONN限制丢弃)** -超过一已配置的或全球连接限制的数据包
- **DOS攻击(DOS丢弃)** -拒绝服务攻击
- **防火墙(FW丢弃)** -基本防火墙安全安全性检查
- **ICMP攻击(ICMP丢弃)** -可疑ICMP数据包
- **Inspect (Inspect丢弃)** -由应用检查的否认
- **接口(接口丢弃)** -由接口检查的被丢弃的数据包
- **扫描(扫描威胁)** -扫描攻击的网络/host
- **SYN攻击(SYN攻击)** -不完整会话攻击，包括TCP SYN攻击和单向的UDP会话没有回归数据

这些事件中的每一个有使用识别威胁的特定的触发。多数触发附加回到特定ASP丢弃原因，虽然某些Syslog和检查操作也考虑。一些触发按多威胁类别监控。某些最普通的触发在此表里概述，虽然它不是详尽列表：

基本威胁	**触发/ASP丢弃原因**
ACL 丢包	ACL 丢包
数据包损坏丢包	无效TCP hdr长度 无效IP报头 Inspect dns PAK太龙牌 Inspect dns id没有匹配
连接限制丢包	CONN限制
DOS 丢包	SP安全失败
防火墙丢包	Inspect ICMP顺序努姆没有匹配 Inspect dns PAK太龙牌 Inspect dns id没有匹配 SP安全失败
ICMP 丢包	ACL 丢包 Inspect ICMP顺序努姆没有匹配
检查丢包	检测引擎触发的帧丢包
接口丢包	SP安全失败 NO-路由 tcp-3whs-failed TCP没有SYN SP安全失败
扫描威胁	ACL 丢包 Inspect ICMP顺序努姆没有匹配 Inspect dns PAK太龙牌 Inspect dns id没有匹配

SYN 攻击　　%ASA-6-302014与“SYN超时”卸载原因的Syslog

对于每个事件，基本威胁检测测量这些丢包发生一个配置的周期时间的速率。此时期呼叫**平均速率间隔(ARI)**并且能范围自600秒到30天。如果在ARI内发生事件的数量超出配置速率阈值， ASA认为这些事件威胁。

当认为事件威胁时，基本威胁检测有两可配置阈值为：**平均速率**和**突发速率**。平均速率是丢包平均数每在已配置的ARI的时间的秒。例如，如果ACL丢包的平均速率阈值为400配置与600秒ARI，ASA计算由ACL丢弃在最后600秒内数据包的平均数。如果此编号比400结果极大每秒， ASA记录威胁。

同样，突发速率是非常类似，但是看看更加小的期限快照数据，呼叫**突发速率间隔(BRI)**。BRI小于ARI总是。例如，构件在前一个示例， ACL丢包的ARI仍然是600秒和当前有突发速率800。使用这些值， ASA由ACL计算被丢弃的数据包平均数在最后20秒内， 20秒是BRI。如果此计算值超出800丢包每秒，威胁被记录。为了确定使用什么BRI， ASA计算值1/30th ARI。所以，在以前使用的示例， 1/30th 600秒是20秒。然而，威胁检测有10秒最低BRI，因此，如果1/30th ARI少于10是，ASA仍然使用10秒作为BRI。并且，请注意此行为是不同的在版本在8.2(1)之前，使用值1/60th ARI，而不是1/30th。10秒最低BRI是相同的为所有软件版本。

当一个基本威胁检测时， ASA生成Syslog %ASA-4-733100警告管理员潜在的威胁识别。事件平均值、当前和总数每个威胁类别的能在**rate命令显示的威胁检测**看到。 渐增事件的总数是事件数量的总和在最后30 BRI示例看到的。

基本威胁检测不采取任何行动为了终止冲突的数据流或防止将来攻击。这样，基本威胁检测是纯信息的，并且可以使用作为监听或报告机制。

先进的威胁检测(对象级别统计信息和顶部N)

不同于基本威胁检测，先进的威胁检测可以用于跟踪更加粒状的对象的统计信息。ASA支持主机IP，端口、协议、TCP拦截保护的ACL和服务器的跟踪统计信息。默认情况下先进的威胁检测为ACL统计信息只启用。

对于主机、端口和协议对象，威胁检测记录由在特定的时间的该对象发送并且接收数据包、字节和丢包的数量。对于ACL，威胁检测记录最是点击的在特定的时间的名列前茅10 ACE (permit和拒绝)。

总计跟踪的时间这些案件是20分钟、1个小时、8个小时和24个小时。当时间不可配置时，每个对象被跟踪期限的数量可以调节与‘编号速率’关键字。欲知更多信息，请参阅配置部分。例如，如果‘编号速率’设置到2，您看到所有统计信息20分钟、1个小时和8个小时。如果‘编号速率’设置到1，您看到所有统计信息20分钟， 1个小时。不管， 20分钟速率总是显示。

当TCP拦截启用时，威胁检测能记录认为在攻击下并且由TCP拦截保护的名列前茅10个服务器。TCP拦截的统计信息类似于基本威胁检测，也就是说用户能与特定平均值(ARI)和突发流量(BRI)速率一起配置被测量的速率间隔。TCP拦截的先进的威胁检测统计信息只可用在ASA 8.0(4)及以后。

先进的威胁检测统计信息通过**显示威胁检测统计信息**查看并且**显示威胁检测统计信息顶部**命令。这也是功能负责对填充在ASDM防火墙控制板的“顶部”图表。由先进的威胁检测生成的唯一的Syslog是%ASA-4-733104和%ASA-4-733105，被触发，当平均值和突发速率(分别)时为TCP拦截统计信息被超出。

类似基本威胁检测，先进的威胁检测是纯信息的。行动没有采取阻塞根据先进的威胁检测统计信息的流量。

扫描的威胁检测

扫描的威胁检测用于为了记录创建连接在子网的许多主机的怀疑的攻击者，或者主机/子网的许多端口。默认情况下扫描的威胁检测禁用。

在基本威胁检测的概念的扫描的威胁检测修造，已经定义了扫描攻击的一个威胁类别。所以，速率间隔、平均速率(ARI)和突发速率(BRI)设置共享在基本和扫描威胁检测之间。2个功能之间的差异是，当基本威胁检测只表明时平均值或突发速率阈值被超过了，扫描的威胁检测维护可帮助在扫描涉及的主机附近提供更多上下文攻击者和目标IP地址的数据库。另外，由目标主机/子网实际上接收仅的流量通过扫描威胁检测考虑。基本威胁检测能仍然触发扫描威胁，即使流量由ACL丢弃。

扫描的威胁检测能或者起反应到攻击通过避开攻击者IP。这做扫描威胁检测能通过ASA积极地影响连接的唯一的子集威胁检测功能。

当扫描的威胁检测检测攻击时， %ASA-4-733101为攻击者和目标IP被记录。如果功能配置避开攻击者， %ASA-4-733102被记录，当扫描的威胁检测生成避开时。当避开删除时， %ASA-4-733103被记录。**显示威胁检测扫描威胁**命令可以用于为了查看整个扫描威胁数据库。

限制

- 威胁检测只可用在ASA 8.0(2)及以后。ASA 1000V平台不支持它。
- 单个上下文模式只支持威胁检测。
- 仅通过这方框威胁检测。流量发送对ASA没有由威胁检测考虑。
- 由目标服务器重置的TCP连接尝试没有算作是SYN攻击或扫描威胁。

配置

基本威胁检测

基本威胁检测用威胁**检测基本威胁**命令启用。

```
ciscoasa(config)# threat-detection basic-threat
```

默认速率可以查看与**show run所有威胁检测**命令。

```
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
```

为了调整与自定义值的这些速率，请重新配置威胁**检测rate命令**为适当的威胁类别。

```
ciscoasa(config)# threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate
550
```

每个威胁类别能有定义的最多3不同的速率(与速率ID速率1，速率2和速率3)。被超出的特定的速率ID被参考%ASA-4-733100 Syslog。

在前一个示例中，只有当ACL丢包数量超出250丢包/秒钟1200秒或550丢包/秒钟40秒时，威胁检测创建Syslog 733100。

先进的威胁检测

请使用**statistics命令的威胁检测**为了启动先进的威胁检测。如果没有提供特定功能关键字，命令启用所有统计信息的跟踪。

```
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>
```

为了配置的速率间隔数量为主机、端口、协议或者ACL统计信息被跟踪，请使用编号**速率**关键字。

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

编号速率关键字配置威胁检测跟踪仅最短的*n*间隔的数量。

为了启用TCP拦截统计信息，请使用威胁**检测统计信息TCP拦截**命令。

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

为了配置TCP拦截统计信息的税率，请使用速率**间隔**、**平均速率**和**突发速率**关键字。

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

扫描的威胁检测

为了启动扫描威胁检测，请使用威胁**检测扫描威胁**命令。

```
ciscoasa(config)# threat-detection scanning-threat
```

为了调节扫描威胁的速率，请使用基本威胁检测使用的同样威胁**检测rate命令**。

```
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 250
burst-rate 550
```

为了允许ASA避开扫描攻击者IP，请添加**避开**关键字到威胁**检测扫描威胁**命令。

```
ciscoasa(config)# threat-detection scanning-threat shun
```

这允许扫描威胁检测创建一个一个小时为攻击者避开。为了调整避开的持续时间，请使用威胁**检测**

扫描威胁避开持续时间命令。

```
ciscoasa(config)# threat-detection scanning-threat shun duration 1000
```

有时，您可以仍然要防止ASA避开的某些IP。为了执行此，请创建与威胁**检测扫描威胁的**一例外**避开except命令**。

```
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

基本威胁检测有在ASA的很少性能影响。因为他们必须记录在内存的多种统计信息先进和扫描威胁检测是密集更多的资源。与启用的避开功能的仅扫描的威胁检测能积极地影响将否则允许的流量。

当ASA软件版本进步了，威胁检测存储器利用率显著优化。然而，在威胁检测启用前后，应该采取注意监控ASA存储器利用率。有时，临时地只启用某些统计信息(例如，主机统计信息)也许是更加好的，当积极地排除故障一个特定问题时。

对于威胁检测的内存使用更多详细信息，请运行**show memory APP缓存威胁检测[detail]**命令。

推荐的操作

这些部分提供可以采取的行动的一些一般建议，当多种威胁检测相关事件发生时。

当基本丢弃速率被超出，并且时%ASA-4-733100生成

确定在%ASA-4-733100 Syslog提及的特定威胁类别并且关联此与输出**显示威胁检测速率**。有此信息，请检查输出**显示asp丢弃**为了确定原因为什么流量降低。

对于为一个特定原因降低流量的更多详细信息，请以有问题的原因使用一个ASP丢弃捕获为了发现被丢弃的所有数据包。例如，如果ACL丢弃威胁被记录，在ACL**丢弃**ASP丢弃原因的捕获：

```
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的一UDP/53数据包到192.168.1.100。

如果%ASA-4-733100报告扫描威胁，临时地启动扫描威胁检测可以也是有用的。这允许ASA记录在攻击IP涉及的源和目的。

因为基本威胁检测主要监控由ASP已经丢弃的流量，直接作用没有要求终止潜在的威胁。对此的例外是SYN攻击和扫描威胁，介入通过通过ASA的流量。

如果被看到的丢包在ASP丢弃捕获为网络环境是合法并且/或者预计，请调整基本速率间隔对一个appropriate值。

如果丢包显示非法流量，应该采取行动阻塞或速率限制流量，在到达ASA前。这能包括ACL和QoS在上行设备。

对于SYN攻击，流量在ASA的ACL可以阻塞。TCP拦截可能也配置保护目标服务器，但是这可能导致被记录的Conn限制威胁。

对于扫描的威胁，流量在ASA的ACL可能也阻塞。与**避开**选项的扫描的威胁检测可以启用允许ASA主动地阻塞从攻击者的所有信息包一个定义时期。

当扫描威胁检测，并且时%ASA-4-733101被记录

%ASA-4-733101应该列出任一目标主机/子网或者攻击者IP地址。对于目标和攻击者详尽列表，请检查输出**显示威胁检测扫描威胁**。

面对攻击者和目标的ASA接口的数据包捕获可也帮助澄清攻击的本质。

如果检测的扫描一不预计，应该采取行动阻塞或速率限制流量，在到达ASA前。这能包括ACL和QoS在上行设备。添加**避开**选项到扫描威胁检测设置能也允许ASA主动地从攻击者IP丢弃所有信息包一个定义时期。作为最后一招，流量在ASA可能手工也阻塞通过ACL或TCP拦截策略。

如果检测的扫描是错误肯定，请调节扫描威胁速率间隔对一个appropriate值网络环境的。

当攻击者避开，并且时%ASA-4-733102被记录

%ASA-4-733102列出避开的攻击者的IP地址。请使用**shun命令显示的威胁检测**为了查看由威胁检测特别地避开了攻击者的详尽列表。请使用**show shun命令**为了查看由ASA积极地避开所有IP的详尽列表(除威胁检测之外的包括从来源)。

如果避开是一合法攻击的一部分，进一步操作没有要求。然而，手工阻塞攻击者的流量如上行往来源尽可能是有利的。这可以通过ACL和QoS执行。这保证中间设备不需要浪费处理非法流量的资源。

如果触发避开的扫描威胁是错误肯定，请手工取消与**清楚威胁检测的**避开**避开[IP_address]**命令。

当%ASA-4-733104和%ASA-4-733105被记录

%ASA-4-733104和%ASA-4-733105列出由TCP拦截当前保护的攻击瞄准的主机。欲了解更详细的信息在发病率和已保护服务器，请检查输出**显示威胁检测统计信息顶部TCP拦截**。

```
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)
```

当先进的威胁检测检测此性质时攻击， ASA通过TCP拦截已经保护目标服务器。验证配置连接限额保证他们为攻击的本质和速率提供足够的防护。并且，手工阻塞攻击者的流量如上行往来源尽可能是有利的。这可以通过ACL和QoS执行。这保证中间设备不需要浪费处理非法流量的资源。

如果检测的攻击是错误肯定，请调节TCP拦截攻击的速率对一个appropriate值用威胁**检测统计信息TCP拦截**命令。

如何手工触发威胁

对于测试和故障排除目的，手工触发多种威胁可以是有用的。此部分包含触发的一些个普通的威胁类型提示。

基本威胁- ACL丢弃、防火墙和扫描

为了触发一个特定的基本威胁，参考在上一个功能部分的表。选择特定ASP丢弃原因并且通过将由适当的ASP丢弃原因下降的ASA发送流量。

例如， ACL丢弃、防火墙和扫描威胁全部由ACL丢弃考虑速率拒绝的数据包。完成这些步骤为了同时触发这些威胁：

1. 创建在明确地下降所有TCP发送的数据包到在ASA ASA的外部接口的ACL (10.11.11.11)的里面的一个目标服务器： `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)
   ```
2. 从在ASA (10.10.10.10)的外部的一名攻击者，请使用nmap为了执行TCP SYN扫描目标服务器的每个端口： `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)
   ```
   注意：T5配置nmap尽可能快运行扫描。根据攻击者PC的资源，这可能不仍然是足够快速触发某些默认速率。如果这是实际情

形，请降低您要发现的威胁的配置速率。不管速率，设置ARI和BRI到0造成基本威胁检测总是触发威胁。

3. 注意基本威胁为ACL丢弃、防火墙和扫描威胁检测： `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)
```

注意：在本例中， ACL丢弃和防火墙阿利斯和BRI设置到0，因此他们总是触发威胁。这就是为什么最大配置速率列出作为0。

先进的威胁- TCP拦截

1. 创建在允许所有TCP发送的数据包到在ASA的外部接口的ACL (10.11.11.11)的里面的一个目标服务器： `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)
```

2. 如果目标服务器实际上不存在，或者重置攻击者的连接尝试，请配置在ASA的假ARP条目对黑洞攻击流量内部接口： `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)
```

3. 创建在ASA的一项简单TCP拦截策略： `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)
```

从在ASA (10.10.10.10)的外部的一名攻击者，请使用nmap执行TCP SYN扫描目标服务器的每个端口：`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)
```

注意威胁检测记录已保护服务器：`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)
```

扫描的威胁

1. 创建在允许所有TCP发送的数据包到在ASA的外部接口的ACL (10.11.11.11)的里面的一个目标服务器：`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)
```

注意：为了扫描威胁检测能跟踪目标和攻击者IP，必须通过ASA允许流量。
2. 如果目标服务器实际上不存在，或者重置攻击者的连接尝试，请配置在ASA的假ARP条目对黑洞攻击流量内部接口：`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)
```

注意：由目标服务器重置作为威胁一部分的连接没有计数。
3. 从在ASA (10.10.10.10)的外部的一名攻击者，请使用nmap执行TCP SYN扫描目标服务器的每

个端口： `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)
```

注意：T5配置nmap尽可能快运行扫描。根据攻击者PC的资源，这可能不仍然是足够快速触发某些默认速率。如果这是实际情形，请降低您要发现的威胁的配置速率。不管速率，设置ARI和BRI到0造成基本威胁检测总是触发威胁。

4. 注意扫描威胁检测，攻击者的IP被跟踪，并且攻击者避开： `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)
```

相关信息

- ASA配置指南
- ASA命令参考
- ASA Syslog指南
- 技术支持和文档 - Cisco Systems