Cisco IOS经典Firewall/IPS ：配置基于上下文的访问控制(CBAC)的拒绝服务保护

目录

简介

本文档介绍使用CBAC的Cisco IOS®传统防火墙中的拒绝服务(DoS)参数的调整过程。

CBAC提供高级流量过滤功能，可用作网络防火墙的组成部分。

DoS通常指有意或无意地压垮网络资源（如WAN链路带宽、防火墙连接表、终端主机内存、CPU或服务功能）的网络活动。在最坏的情况下，DoS活动会将易受攻击（或目标）的资源压垮，使资源变得不可用，并禁止对合法用户进行WAN连接或服务访问。

如果Cisco IOS防火墙在传统防火墙(**ip inspect**)和基于区域的策略防火墙中维护“半开”TCP连接数以及通过防火墙和入侵防御软件的总连接速率的计数器，则它有助于缓解DoS活动。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

半开连接是未完成三次SYN-SYN/ACK-ACK握手的TCP连接，TCP对等体始终使用三次SYN-SYN/ACK-ACK握手来协商其相互连接的参数。大量半开连接可能表示恶意活动，例如DoS或分布式拒绝服务(DDoS)攻击。一种DoS攻击的示例是由恶意的、有意开发的软件（如感染Internet上多台主机的蠕虫或病毒）发起，并尝试用SYN攻击淹没特定Internet服务器，其中大量SYN连接由Internet上的多台主机或组织的专用网络中的多台主机发送到服务器。SYN攻击对Internet服务器构成风险，因为服务器的连接表可以加载“伪造的”SYN连接尝试，这些尝试的到达速度比服务器处理新连接的速度快。这是一种DoS攻击，因为受害服务器的TCP连接列表中的大量连接会阻止合法用户访问受害Internet服务器。

Cisco IOS防火墙还将仅单向流量的用户数据报协议(UDP)会话视为“半开放”，因为许多使用UDP进行传输的应用程序都确认接收了数据。没有返回流量的UDP会话可能表示DoS活动或尝试在两台主机之间连接，其中一台主机已无响应。许多类型的UDP流量（如日志消息、SNMP网络管理流量、流语音和视频媒体以及信令流量）仅使用单向流量来传输其流量。许多此类流量都应用特定于应用的智能，以防止单向流量模式对防火墙和IPS DoS行为产生不利影响。

在Cisco IOS软件版本12.4(11)T和12.4(10)之前，Cisco IOS状态数据包检测在应用检测规则时提供DoS攻击的默认保护。思科IOS软件版本12.4(11)T和12.4(10)修改了默认DoS设置，因此DoS保护不会自动应用，但连接活动计数器仍处于活动状态。当DoS保护处于活动状态时，即当在较旧的软件版本上使用默认值，或者这些值已调整到影响流量的范围时，在应用防火墙的方向上应用检测的接口上启用DoS保护，以检查防火墙策略配置协议。只有当流量进入或离开接口时，才会在网络流量上启用DoS保护，该接口对TCP连接或UDP会话的初始流量（SYN数据包或第一个UDP数据包）的相同方向应用检测。

Cisco IOS防火墙检测提供多个可调值，以防范DoS攻击。12.4(11)T和12.4(10)之前的Cisco IOS软件版本具有默认DoS值，如果未针对网络活动的适当级别进行配置，而网络连接速率超过默认值，则这些DoS值可能会干扰网络的正常运行。这些参数允许您配置防火墙路由器的DoS保护开始生效的点。当路由器的DoS计数器超过默认值或已配置值时，路由器会重置每个新连接的一个旧的半开连接，该连接超过已配置的最大未完成值或一分钟高值，直到半开会话数降至最大未完成低值以下。如果启用日志记录，路由器会发送系统日志消息，如果路由器上配置了入侵防御系统(IPS)，则防火墙路由器会通过安全设备事件交换(SDEE)发送DoS签名消息。 如果DoS参数未根据网络的正常行为进行调整，则正常网络活动可能会触发DoS保护机制，从而导致Cisco IOS防火墙路由器上的应用故障、网络性能差和CPU使用率高。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

Cisco IOS软件经典（IP检查）防火墙和入侵防御系统的拒绝服务调整

传统Cisco IOS防火墙为路由器维护一组全局DoS计数器，并且所有接口上所有防火墙策略的所有防

火墙会话都应用于全局防火墙计数器集。

默认情况下，当应用传统防火墙时，Cisco IOS传统防火墙检测可提供DoS攻击保护。对于配置防火墙策略以检查的每项服务或协议，在应用防火墙的方向上应用检查的所有接口上启用DoS保护。传统防火墙提供多个可调值，以防范DoS攻击。如表1所示，旧版默认设置(来自12.4(11)T之前的软件映像)如果未针对连接速率超过默认值的网络中适当的网络活动级别进行配置，则可能会干扰正确的网络操作。DoS设置可使用exec命令**show ip inspect config**查看，并且这些设置包含在sh ip inspect all**的输出中**。

CBAC使用超时和阈值来确定管理会话状态信息的时间，并确定何时丢弃未完全建立的会话。这些超时和阈值全局应用于所有会话。

表1传统防火墙默认DoS保护限制		
DoS保护价值	**12.4(11)T/12.4(10)之前**	**12.4(11)T/12.4(10)及更高版本**
max-incomplete high *value*	500	无限
max-incomplete low *value*	400	无限
一分钟高*值*	500	无限
一分钟低*值*	400	无限
tcp最大不完整主机*值*	50	无限

配置为应用Cisco IOS VRF感知防火墙的路由器为每个VRF维护一组计数器。

“ip inspect one-minute high”和“ip inspect one-minute low”的计数器在路由器运行的前一分钟内保持所有TCP、UDP和互联网控制消息协议(ICMP)连接尝试的总和，无论连接是否成功。连接速率的提高可能表示私有网络上的蠕虫感染或对服务器的DoS攻击尝试。

虽然不能“禁用”防火墙的DoS保护，但可以调整DoS保护，使其不会生效，除非防火墙路由器的会话表中存在大量半打开连接。

DoS防火墙保护

按照以下步骤调整防火墙的DoS保护以适应网络活动：

1. 请确保您的网络未感染病毒或蠕虫，这些病毒或蠕虫可能导致连接值错误增大或尝试的连接速率。如果网络不“干净”，则无法正确调整防火墙的DoS保护。您必须观察网络在典型活动期间的活动。如果在网络活动较少或空闲的时段内调整网络的DoS保护设置，则正常活动级别可能超过DoS保护设置。
2. 将max-incomplete high值设置为非常高的值：

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

这会阻止路由器在观察网络连接模式时提供DoS保护。如果希望禁用DoS保护，请立即停止此过程。**注意：**如果您的路由器运行Cisco IOS软件版本12.4(11)T或更高版本，或12.4(10)或更高版本，则无需提高默认DoS保护值；默认情况下，它们已设置为最大限制。**注意：**如果要启

用更主动的TCP主机特定拒绝服务防御，包括阻止对主机的连接启动，则必须设置在**ip inspect tcp max-incomplete host命令中指定的阻止时间。**

3. 使用以下命令清除Cisco IOS防火墙统计信息：

```
show ip inspect statistics reset
```

4. 将路由器配置为此状态一段时间（可能长达24到48小时），这样您就可以在典型网络活动周期的至少一整天内观察网络模式。**注意：**虽然这些值已调整到非常高的级别，但您的网络不会从Cisco IOS防火墙或IPS DoS保护中获益。
5. 观察期结束后，使用以下命令检查DoS计数器：

```
show ip inspect statistics
```

要调整DoS保护，必须观察的参数以粗体突出显示:

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. 将**ip inspect max-incomplete high配置为比您的路由器的指定maxever会话计数半开值高25%的值。**1.25倍的乘数提供25%的空间，高于观察到的行为，例如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

配置:

```
router(config)
   #ip inspect max-incomplete high 70
```

注意：本文档介绍如何使用倍数1.25倍于网络典型活动的倍数来设置限制以实施DoS保护。如果在典型网络活动高峰期观察网络，这必须提供足够的净空，以避免在非典型情况下激活路由器的DoS保护。如果您的网络定期发现大量合法网络活动爆发超过此值，则路由器会启用DoS保护功能，这可能会对某些网络流量造成负面影响。您必须监控路由器日志以检测DoS活动，并调整**ip inspect max-incomplete high**和/或**ip inspect one-minute high limits**以避免触发DoS，前提是您确定这些限制是由于合法网络活动而发生的。您可以通过以下日志消息识别DoS保护应用：

7. 将**ip inspect max-incomplete low配置为**您的路由器为其maxever会话计数半开值显示的值，例

如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
```

配置:

```
router(config)
   #ip inspect max-incomplete low 56
```

8. **ip inspect one-minute high**和**one-minute low**计数器在路由器操作的前一分钟内保持所有TCP、UDP和Internet控制消息协议(ICMP)连接尝试的总和，无论连接是否成功。连接速率的上升可能表示私有网络上的蠕虫感染，或者对服务器的DoS攻击尝试。在12.4(11)T和12.4(10)中的**show ip inspect statistics**输出中添加了额外的检查统计信息，以揭示会话创建速率的高水位标记。如果运行12.4(11)T或12.4(10)之前的Cisco IOS软件版本，则检测统计信息不包含此行：

```
Maxever session creation rate [value]
```

12.4(11)T和12.4(10)之前的Cisco IOS软件版本不维护检查最大一分钟连接速率的值，因此您必须根据观察到的“最大会话计数”值计算您应用的值。对生产中使用Cisco IOS防火墙版本12.4(11)T状态检查的几个网络的观察表明，Maxever会话创建速率往往超过“maxever session count”中三个值（已建立、半开和终止）之和，大约为10%。要计算ip inspect 1-minute low值，请将指示的“established”值乘以1.1，例如：

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
(207 + 56 + 35) * 1.1 = 328
```

配置:

```
ip inspect one-minute low 328
```

如果路由器运行Cisco IOS软件版本12.4(11)T或更高版本，或12.4(10)或更高版本，则只需应用“Maxever session creation rate”检查统计信息中显示的值：

```
Maxever session creation rate 330
```

配置:

```
ip inspect one-minute low 330
```

9. 计算并配置**ip inspect one-minute high**。ip inspect 1-minute high值必须比计算的1-minute low值大25%，例如：

```
ip inspect one-minute low (330) * 1.25 = 413
```

配置:

```
ip inspect one-minute high 413
```

注意：本文档介绍如何使用倍数1.25倍于网络典型活动的倍数来设置限制以实施DoS保护。如果在典型网络活动高峰期观察网络，这必须提供足够的净空，以避免在非典型情况下激活路由器的DoS保护。如果您的网络定期发现大量合法网络活动爆发超过此值，则路由器会启用DoS保护功能，这可能会对某些网络流量造成负面影响。您必须监控路由器日志以检测DoS活动，并调整**ip inspect max-incomplete high**和/或**ip inspect one-minute high limits**以避免触发DoS，前提是您确定这些限制是由于合法网络活动而发生的。您可以通过以下日志消息识别DoS保护应用：

10. 您需要根据您对服务器**功能的了解，为ip inspect tcp max-incomplete host**定义一个值。本文档无法提供每主机DoS保护配置的准则，因为此值因终端主机硬件和软件性能而异。如果您不确定要为DoS保护配置的适当限制，您实际上有两个选项来定义DoS限制：首选方案是将基于路由器的每主机DoS保护配置为高值（小于或等于最大值4,294,967,295），并应用由每台主机的操作系统或基于外部主机的入侵保护系统（如思科安全代理[CSA]）提供的主机特定保护。检查网络主机上的活动和性能日志并确定其峰值可持续连接速率。由于传统防火墙仅提供一个全局计数器，因此您必须应用在检查所有网络主机的最大连接速率后确定的最大值。仍建议您使用特定于操作系统的活动限制和基于主机的IPS（例如CSA）。**注意：**Cisco IOS防火墙针对特定操作系统和应用漏洞提供有限的定向攻击保护。Cisco IOS防火墙的DoS保护无法保证对可能暴露在潜在恶意环境中的终端主机服务的危害提供保护。

11. 监控网络的DoS保护活动。理想情况下，您必须使用系统日志服务器，或者理想情况下，必须使用思科监控和报告站(MARS)记录DoS攻击检测的发生。如果检测频繁发生，您需要监控和调整DoS保护参数。有关TCP SYN DoS攻击的详细信息，请参阅定义防御TCP SYN拒绝服务攻击的策略。

验证

当前没有可用于此配置的验证过程。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems