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

本文描述拒绝服务参数的调整的步骤在与CBAC的Cisco IOS经典防火墙。

CBAC提供先进的流量过滤功能，并且可以使用作为您的网络防火墙的必要组成部分。

DoS通常是指有意或无意淹没网络资源例如广域网链路带宽、防火墙连接表、终端-主机内存、CPU或者服务能力的网络活动。在最坏局面中， DoS活动淹没易受攻击(或瞄准)资源到点资源变得不可用，并且禁止WAN连接或服务访问对合法用户。

Cisco IOS防火墙能造成DoS活动，如果维护计数器数量“半打开” TCP连接，以及总连接速度通过防火墙和在经典防火墙(**IP inspect**)和基于区域的策略防火墙的入侵防御软件的缓解。

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

半开连接是未完成三通的SYN-SYN/ACK-ACK握手由TCP对等体总是使用协商他们的相互连接参数的TCP连接。很大数量的半开连接可以是预示的恶意活动，例如DoS或分布式拒绝服务(DDos)攻击。DOS攻击的一种类型示例由感染互联网的多台主机并且尝试淹没特定Internet服务器与SYN攻击，很大数量的SYN连接发送到服务器由多台主机在互联网或在组织的私有网络内的有恶意，专门开发的软件，例如蠕虫病毒或病毒执行。SYN攻击代表危险等级到Internet服务器，因为服务器连接表可以装载与“比服务器能处理新连接到达快速的假” SYN连接尝试。因为在受害者服务器的TCP连接列表的很大数量的连接防止对受害者Internet服务器的合法用户用户访问这是DOS攻击的类型。

Cisco IOS防火墙只也认为有流量的用户数据报协议(UDP)会话在一个方向“半打开”，因为使用UDP传输的许多应用程序确认数据的接收。没有回程数据流的UDP会话可能是预示的DoS活动或尝试连接在两台主机之间，其中一台主机变得无答复。UDP流量的许多类型，例如日志消息，SNMP网络管理数据流，放出语音和视频媒介和信令流量，在一个方向的仅使用流量运载他们的流量。许多这些流量类型应用专用智能防止单向数据流交通图相反影响防火墙和IPS DoS行为。

在Cisco IOS软件版本12.4(11)T和12.4(10)之前，当检查规则应用， Cisco IOS有状态的包侦测提供从DOS攻击的防护作为默认。Cisco IOS软件版本12.4(11)T和12.4(10)修改了默认DoS设置，以便DoS保护没有自动地应用，但是连接活动计数器是活跃的。当DoS保护是活跃的时，即，当默认值在更旧的软件版本或者影响流量的值时使用调节对范围， DoS保护在检查应用的接口启用，在防火墙应用的方向，防火墙策略配置协议的能检查。DoS保护在网络流量只启用，如果流量进入或离开与在最初的流量(SYN数据包或第一UDP数据包)的同一个方向应用的检查的一个接口为TCP连接或UDP会话。

Cisco IOS防火墙检查提供几个可调整的值防止受到DOS攻击。在12.4(11)T和12.4(10)之前的Cisco IOS软件版本有默认能干涉适当网络操作的DoS值，如果他们没有为适当级别在连接速度超出默认的网络的网络活动配置。这些参数允许您配置您的防火墙路由器DoS保护开始生效的点。当您的路由器DoS计数器超过默认或配置值时，路由器重置超过在max-incomplete低值之下配置的max-incomplete或直到半打开会话丢包数量的一分钟高值的每个新连接的一旧有半开连接。路由器传送系统消息，如果记录启用，并且，如果入侵防御系统(IPS)在路由器配置，防火墙路由器通过安全设备事件Exchange (SDEE)传送DoS签名信息。如果DoS参数没有调节对您的网络正常行为，正常的网络活动能触发DoS保护机制，导致应用程序故障、恶劣的网络性能和高CPU利用率在Cisco IOS防火墙路由器。

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（仅限注册用户）可获取有关本部分所使用命令的详细信息。

调整为Cisco IOS软件经典(IP inspect)防火墙和入侵防御系统的拒绝服务

标准的Cisco IOS防火墙维护全局套路由器的DoS计数器，并且所有防火墙策略的所有防火墙会话在所有接口应用对全局套防火墙计数器。

默认情况下，当一经典防火墙应用时， Cisco IOS经典防火墙检查提供从DOS攻击的防护。DoS保护在检查应用的所有接口启用，在防火墙应用的方向，防火墙策略配置检查的每份服务或协议的。经典防火墙提供几个可调整的值防止受到DOS攻击。在表(从在版本12.4(11)T)之前的软件镜像显示的传统默认设置1能干涉适当网络操作，如果他们没有为适当级别在连接速度超出默认的网络的网络活动配置。DoS设置可以查看与exec命令**show ip inspect设置**，并且设置包括与**噓IP inspect**输出**全部**。

CBAC多久什么时候使用超时和阈值确定管理会话的状态信息，以及确定丢弃不变得充分地已建立的会话。这些超时和阈值适用全局于所有会话。

表1经典防火墙默认DoS保护限额		
DoS保护值	**在12.4(11)T/12.4(10)之前**	**12.4(11)T/12.4(10)及以后**
max-incomplete高值	500	无限个
max-incomplete低值	400	无限个
一分钟高值	500	无限个
一分钟低值	400	无限个
tcp max-incomplete主机*值*	50	无限个

应用Cisco IOS VRF感知防火墙的配置的路由器维护一套每个VRF的计数器。

“IP inspect一分钟高”和“IP inspect一分钟低的”计数器在路由器的操作的前期分钟内维护所有TCP，UDP的一个总和和互联网控制消息协议(ICMP)连接尝试，是否连接是成功的。上涨的连接速度可以是预示的在私有网络的一蠕虫病毒传染或一次已尝试DOS攻击服务器。

当您不能“禁用”您的防火墙的DoS保护时，您能调节DoS保护，以便不生效，除非一个非常大数目的半开连接是存在您的防火墙路由器里会话表。

DoS防火墙保护

遵从此步骤调整您的防火墙的DoS保护到您的网络的活动：

1. 请务必您的网络没有感染可能导致不正确大半开连接值或已尝试连接速度的病毒或蠕虫病毒。如果您的网络不是“干净的”，没有办法适当地调节您的防火墙的DoS保护。您必须观察您的在期间的网络的活动典型的活动。如果调整您的在期间的网络DoS保护设置低或空闲网络活动，正常操作活动程度可能超出DoS保护设置。
2. 设置max-incomplete高值为非常高值：
   `ip inspect max-incomplete high 20000000 ip inspect one-minute high 100000000 ip inspect tcp max-incomplete host 100000 block-time 0` 当您观察您的网络时，连接模式这防止路由器提供DoS防护。如果希望留给DoS保护禁用，当前请终止此步骤。**注意：** 如果您的路由器运行Cisco IOS软件版本12.4(11)T或以后或者12.4(10)或者以后，您不需要提高默认DoS保护值;默认情况下他们已经设置为他们的最大限制。**注意：** 如果要启用包括连接发起阻塞到主机的更加积极的TCP特定主机的拒绝服务预防，您必须设置在**ip inspect tcp max-incomplete host命令**指定的块时间
3. 清除Cisco IOS防火墙统计信息用此命令：
   `show ip inspect statistics reset`

4. 或许，只要24个到48个小时，因此您能观察网络模式典型的网络活动活动周期的至少一个整天，请离开路由器有一段时间了配置在此状态。**注意：** 当值调节对高级时，您的网络不受益于Cisco IOS防火墙或IPS DoS保护。
5. 在观察期之后，请用此命令检查DoS计数器：

   show ip inspect statistics 您必须观察与哪些调整您的DoS保护的参数用黑体字表示：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. 高于指示的maxever会话计数半打开值配置**ip inspect max-incomplete high**对值25百分比您的路由器。在观察行为上的例如1.25 multiplier提供25百分比空间，：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：** 本文描述使用1.25倍multiplier您的网络的典型的活动定限额从事DoS保护。如果观察您的在典型的网络活动峰顶内的网络，这必须提供足够的空间避免路由器的DoS保护的激活在几乎下非典型情况。如果您的网络周期地看到超过此值合法网络活动的大突发流量，路由器从事DoS保护功能，能导致在某些的负面影响网络流量。您必须监控您的DoS活动的检测的路由器日志和调节**ip inspect max-incomplete high**和**IP inspect一分钟高**限额避免触发DoS，在您确定后由于合法网络活动，限额遇到。您能由日志消息出现识别DoS保护应用程序例如此：
7. 例如配置**IP inspect max-incomplete低**对您的路由器为其maxever会话计数半打开值显示的值，：Maxever session counts
   (estab/half-open/terminating) [207:56:35]**配置**：router(config)
   #ip inspect max-incomplete low 56
8. **IP inspect一分钟高**和**一分钟低的**计数器在路由器操作的前期分钟内维护所有TCP，UDP的一个总和和互联网控制消息协议(ICMP)连接尝试，是否连接是成功的。上涨的连接速度可以是预示的在私有网络的一蠕虫病毒传染或者一次已尝试DOS攻击服务器。一另外的检查统计信息被添加到在12.4(11)T的**show ip inspect统计信息**输出和12.4(10)显示会话创建速率的最高使用标记。如果早于12.4(11)T或12.4(10)运行Cisco IOS软件版本，检查统计信息不包含此线路：Maxever session creation rate [value]在12.4(11)T和12.4(10)之前的Cisco IOS软件版本不维护检查maxever一分钟连接速度的一个值，因此您必须计算您运用基于观察的“maxever会话计数”值的值。在制作使用Cisco IOS防火墙版本12.4(11)T状态检测几网络的观察显示Maxever会话创建速率倾向于由大致十百分比超过三个值的总和(设立，半打开和终止)在“maxever会话计数”。例如为了计算IP inspect一分钟低值，请倍增指示的“由1.1设立了”值，：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或以后或者12.4(10)或者以后，您能运用在“Maxever会话创建速率”检查统计信息显示的值：Maxever

session creation rate 330**配置**：ip inspect one-minute low 330

9. 计算并且配置**IP inspect一分钟高**。例如IP inspect一分钟高值比计算的一分钟低值必须是25百分比极大，：ip inspect one-minute low (330) * 1.25 = 413 **配置**：ip inspect one-minute high 413**注意：** 本文描述使用1.25倍multiplier您的网络的典型的活动定限额从事DoS保护。如果观察您的在典型的网络活动峰顶内的网络，这必须提供足够的空间避免路由器的DoS保护的激活在几乎下非典型情况。如果您的网络周期地看到超过此值合法网络活动的大突发流量，路由器从事DoS保护功能，能导致在某些的负面影响网络流量。您必须监控您的DoS活动的检测的路由器日志和调节**ip inspect max-incomplete high**和**IP inspect一分钟高**限额避免触发DoS，在您确定后由于合法网络活动，限额遇到。您能由日志消息出现识别DoS保护应用程序例如此：
10. 您需要定义**IP inspect tcp max-incomplete主机的**一个值符合您的您的服务器的功能的知识。因为此值变化广泛基于终端-主机硬件与软件性能，本文不能为每主机DoS保护配置提供指南。如果是不定的关于适当的限额为DoS保护配置，您有效有定义DoS限制的两个选项：更可取的选项是配置基于路由器的每主机DoS保护对高值(小于或等于最大值4,294,967,295)，并且应用每台主机或一个外部招待基础的入侵保护安全系统操作系统提供的特定主机的保护例如Cisco Security Agent (CSA)。检查活动，并且性能注册您的网络主机并且确定他们的高峰能承受的连接速度。因为经典防火墙只提供一个全局计数器，您必须运用您确定的最大值，在您检查所有您的网络主机他们的最大连接速率后。是可行的您使用特殊活动限额和招待基础的IPS例如CSA。**注意：** Cisco IOS防火墙提供有限的保护在特定操作系统和应用程序漏洞的处理的攻击。Cisco IOS防火墙的DoS保护不提供保护保证从妥协的在显示在潜在敌对的环境的终端-主机服务。
11. 监控DoS保护活动您的网络。理论上来讲，必须使用系统日志服务器或者理想地说，思科监控和报告站点(火星)的您对DOS攻击检测记录具体值。如果检测非常频繁地发生，您需要监控和调整您的DoS保护参数。关于TCP SYN DOS攻击的更多信息，参考定义策略防止受到TCP SYN拒绝服务攻击。

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