SDM ：Cisco IOS 路由器上的 URL 过滤配置示例

目录

简介
先决条件
防火墙 Websense URL 过滤的限制
使用的组件
规则
背景信息
使用 CLI 配置路由器
网络图
标识过滤服务器
配置过滤策略
运行 Cisco IOS 12.4 版的路由器的配置
使用 SDM 配置路由器
路由器 SDM 配置
验证
故障排除
错误消息
相关信息

简介

本文档介绍如何在 Cisco IOS 路由器上配置 URL 过滤。通过 URL 过滤可对经过 Cisco IOS 路由器的数据流进行更好的控制。Cisco IOS 12.2(11)YU 版及更高版本支持 URL 过滤。

注意： 由于 URL 过滤比较占用 CPU，因此使用外部过滤服务器可确保其他数据流的吞吐量不受影响。根据您的网络速度和 URL 过滤服务器的容量，使用外部过滤服务器过滤数据流时，初始连接所需的时间可能会明显加长。

先决条件

防火墙 Websense URL 过滤的限制

Websense 服务器要求：要启用此功能，必须拥有至少一个 Websense 服务器； 但如果拥有两个或多个 Websense 服务器，则效果更佳。尽管对于可拥有的 Websense 服务器数量没有限制，并且您也可以随心所欲地配置多个服务器，但在任何特定的时间点，只能有一个服务器处于活动状态，即主服务器。URL 查找请求只会发送到主服务器。

URL 过滤支持限制：此功能一次仅支持一个活动的 URL 过滤方案。（启用 Websense URL 过滤之

前，必须始终确保没有配置其他 URL 过滤方案，如 N2H2。）

用户名限制：此功能不会将用户名和组信息传送给 Websense 服务器，但 Websense 服务器可以根据基于用户的策略执行操作，因为它拥有另一种机制，使用户名能够与 IP 地址相对应。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有Cisco IOS软件版本12.4(15)T的Cisco 2801路由器
- Cisco 安全设备管理器 (SDM) 版本 2.5

注意： 为了允许使用 SDM 配置路由器，请参阅使用 SDM 执行基本路由器配置。

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

防火墙 Websense URL 过滤功能使您的 Cisco IOS 防火墙（也称为 Cisco 安全集成软件 [CSIS]）能够与 Websense URL 过滤软件进行交互。这样您就可以基于某种策略阻止用户访问指定的网站。Cisco IOS 防火墙与 Websense 服务器协同工作，以确定是允许还是拒绝（阻止）某个特定的 URL。

使用 CLI 配置路由器

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。

网络图

本文档使用以下网络设置：

在本示例中，URL 过滤服务器位于内部网络。网络内部的最终用户尝试通过 Internet 访问网络外部的 Web 服务器。

在用户请求访问 Web 服务器时，一般会完成以下步骤：

1. 最终用户浏览到 Web 服务器上的某个页面，然后浏览器发送 HTTP 请求。
2. Cisco IOS 防火墙收到此请求后，将其转发给 Web 服务器。同时，防火墙将提取 URL，并向 URL 过滤服务器发送查找请求。
3. URL 过滤服务器收到查找请求后，检查其数据库以确定是允许还是拒绝该 URL。URL 过滤服务器对 Cisco IOS® 防火墙做出查找响应，同时返回允许或拒绝状态。
4. Cisco IOS® 防火墙收到该查找响应，并执行以下功能之一：如果查找响应允许该 URL，则向

最终用户发送 HTTP 响应。如果查找响应拒绝该 URL，则 URL 过滤服务器将用户重定向到自己的内部 Web 服务器，此服务器将显示一条消息，说明该 URL 的阻止类别。然后，两端的连接都将重置。

标识过滤服务器

您需要使用 **ip urlfilter server vendor** 命令标识过滤服务器的地址。必须根据所使用的过滤服务器的类型以适当的形式使用此命令。

注意： 在您的配置中，您只能采用一种服务器类型，即 Websense 或 N2H2。

Websense

Websense 是一种可根据以下策略过滤 HTTP 请求的第三方过滤软件：

- 目标主机名
- 目的 IP 地址
- 关键字
- 用户名

此软件维护有一个 URL 数据库，该数据库拥有超过 2 千万个站点，并将这些站点归入 60 多种类别和子类别。

ip urlfilter server vendor 命令可指定运行 N2H2 或 Websense URL 过滤应用程序的服务器。要配置供应商服务器以进行 URL 过滤，请在全局配置模式下使用 **ip urlfilter server vendor** 命令。要从您的配置中删除服务器，请使用此命令的 no 形式。以下是 **ip urlfilter server vendor** 命令的语法：

```
hostname(config)# ip urlfilter server vendor {websense | n2h2} ip-address [port port-number]
[timeout seconds] [retransmit number] [outside] [vrf vrf-name]
```

使用 Websense 服务器的 IP 地址替换 ip-address。使用 IOS 防火墙需要继续尝试连接过滤服务器的秒数替换 seconds。

例如，要配置一个 Websense 过滤服务器以进行 URL 过滤，请发出以下命令：

```
hostname(config)#
   ip urlfilter server vendor websense 192.168.15.15
```

配置过滤策略

注意： 启用 URL 过滤之前，必须标识并启用 URL 过滤服务器。

截断较长的 HTTP URL

要允许 URL 过滤器将较长的 URL 截断到服务器中，请在全局配置模式下使用 ip urlfilter truncate 命令。要禁用截断选项，请使用此命令的 no 形式。Cisco IOS 12.4(6)T 版及更高版本支持此命令。

`ip urlfilter truncate {script-parameters|`hostname} 为此命令的语法。

script-parameters：仅发送截止到脚本选项相关内容的 URL。例如，如果整个 URL 为 http://www.cisco.com/dev/xxx.cgi?when=now，则仅发送 http://www.cisco.com/dev/xxx.cgi 这一段 URL（在不超过所支持的 URL 最大长度的情况下）。

主机名：仅发送主机名。例如，如果整个 URL 为 http://www.cisco.com/dev/xxx.cgi?when=now，则仅发送 http://www.cisco.com。

如果同时配置了关键字 script-parameters 和 hostname，则前者优先于后者。如果同时配置了这两个关键字并且截断了脚本参数 URL，但超过了所支持的 URL 最大长度，则将 URL 截断到主机名为止。

注意： 如果同时配置关键字 script-parameters 和 hostname，则必须配置于不同的行中，如下所示。不能将二者组合在同一行中。

注意： `ip urlfilter truncate script-parameters`

注意： `ip urlfilter truncate hostname`

运行 Cisco IOS 12.4 版的路由器的配置

此配置包含本文档中介绍的命令：

运行 Cisco IOS 12.4 版的路由器的配置

```
R3#show running-config : Saved version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec service password-encryption ! hostname R3
! ! !--- username cisco123 privilege 15 password 7
104D000A061843595F ! aaa session-id common ip subnet-
zero ! ! ip cef ! ! ip ips sdf location
flash://128MB.sdf ip ips notify SDEE ip ips po max-
events 100 !--- use the ip inspect name command in
global configuration mode to define a set of inspection
rules. This Turns on HTTP inspection. The urlfilter
keyword associates URL filtering with HTTP inspection.
ip inspect name test http urlfilter !--- use the ip
urlfilter allow-mode command in global configuration
mode to turn on the default mode (allow mode) of the
filtering algorithm. ip urlfilter allow-mode on !--- use
the ip urlfilter exclusive-domain command in global
configuration mode to add or remove a domain name to or
from the exclusive domain list so that the firewall does
not have to send lookup requests to the vendor server.
Here we have configured the IOS firewall to permit the
URL www.cisco.com without sending any lookup requests to
the vendor server. ip urlfilter exclusive-domain permit
www.cisco.com !--- use the ip urlfilter audit-trail
command in global configuration mode to log messages
into the syslog server or router. ip urlfilter audit-
trail !--- use the ip urlfilter urlf-server-log command
in global configuration mode to enable the logging of
system messages on the URL filtering server. ip
urlfilter urlf-server-log !--- use the ip urlfilter
server vendor command in global configuration mode to
configure a vendor server for URL filtering. Here we
have configured a websense server for URL filtering ip
urlfilter server vendor websense 192.168.15.15 no ftp-
server write-enable ! ! !--- Below is the basic
interface configuration on the router interface
FastEthernet0 ip address 192.168.5.10 255.255.255.0 ip
virtual-reassembly !--- use the ip inspect command in
interface configuration mode to apply a set of
inspection rules to an interface. Here the inspection
name TEST is applied to the interface FastEthernet0. ip
```

```
inspect test in duplex auto speed auto ! interface
FastEthernet1 ip address 192.168.15.1 255.255.255.0 ip
virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 ip address 10.77.241.109 255.255.255.192
ip virtual-reassembly duplex auto speed auto ! interface
FastEthernet2 no ip address ! interface Vlan1 ip address
10.77.241.111 255.255.255.192 ip virtual-reassembly ! ip
classless ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65 ! ! !---
Configure the below commands to enable SDM access to the
cisco routers ip http server ip http authentication
local no ip http secure-server ! ! line con 0 line aux 0
line vty 0 4 privilege level 15 transport input telnet
ssh ! end
```

使用 SDM 配置路由器

路由器 SDM 配置

要在 Cisco IOS 路由器上配置 URL 过滤，请完成以下步骤：

注意： 要使用 SDM 配置 URL 过滤，请在全局配置模式下通过 **ip inspect name** 命令定义一组检查规则。这样就会启用 HTTP 检查。关键字 urlfilter 会将 URL 过滤与 HTTP 检查相关联。然后，所配置的检查名称就会映射到要执行过滤的接口上，例如：

```
hostname(config)#ip inspect
   name test http urlfilter
```

1. 打开浏览器并输入 **https://<为访问 SDM 而配置的路由器接口的 IP 地址>**，以访问路由器上的 SDM。请确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空。路由器显示此窗口以允许下载 SDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。
2. SDM 下载现在开始。下载 SDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco SDM 启动程序。
3. 输入**用户名和口令**（如果已指定），然后单击 OK。此示例使用 **cisco123** 作为用户名并使用 cisco123 作为口令。
4. 选择 **Configuration->Additional Tasks**，并在 SDM 主页上单击 URL Filtering。然后单击 **Edit Global Settings**，如下所示：
5. 在出现的新窗口中，启用 URL 过滤所需的参数，如 **Allow-Mode**、**URL Filter Alert**、**Audit-Trial** 和 URL Filtering Server Log。选中每个参数旁边的复选框，如下所示。现在请提供 **Cache Size** 和 HTTP Buffer 信息。另外，请在 Advanced 部分下提供 **Source Interface** 和 URL Truncate 方法（如下所示），以允许 URL 过滤器将较长的 URL 截断到服务器中。（此处选择的 Truncation 参数为 **Hostname**。）现在请单击 **OK**。
6. 现在请选择 URL Filtering 选项卡中的 **Local URL List** 选项。单击 **Add** 添加域名并配置防火墙以允许或拒绝所添加的域名。如果所需的 URL 列表是文件形式，您也可以选择 **Import URL List** 选项。您可以根据 URL 列表的要求和可用性自行选择 **Add URL** 或 Import URL List 选项。
7. 在本示例中，单击 **Add** 添加 URL 并配置 IOS 防火墙，以便根据要求允许或拒绝该 URL。现在将出现一个标题为 **ADD Local URL** 的新窗口，用户必须在其中提供域名并决定是允许还是拒绝该 URL。单击 Permit 或 Deny 选项旁边的单选按钮，如下所示。此处，域名为 **www.cisco.com**，并且用户允许该 URL www.cisco.com。同样地，您可以单击 **Add**，根据需要添加多个 URL，并配置防火墙根据要求允许或拒绝这些 URL。

8. 选择 URL Filtering 选项卡中的 **URL Filter Servers** 选项，如下所示。单击 **Add** 添加执行 URL 过滤功能的 URL 过滤服务器名称。
9. 单击 **Add** 后，选择 Websense 作为过滤服务器（如下所示），因为本示例中使用的是 Websense 过滤服务器。
10. 在 **Add Websense Server** 窗口中，提供 Websense 服务器的 IP 地址以及进行过滤的 Direction 和 Port Number（Websense 服务器的默认端口号为 15868）。另外，请提供 **Retransmission Count** 和 Retransmission Timeout 值，如下所示。单击 **OK** 即可完成 URL 过滤配置。

验证

使用本部分中的命令查看 URL 过滤信息。可使用这些命令验证您的配置。

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。

- **show ip urlfilter statistics** - 显示有关过滤服务器的信息和统计数据例如：`Router# show ip urlfilter statistics URL filtering statistics ================ Current requests count:25 Current packet buffer count(in use):40 Current cache entry count:3100 Maxever request count:526 Maxever packet buffer count:120 Maxever cache entry count:5000 Total requests sent to URL Filter Server: 44765 Total responses received from URL Filter Server: 44550 Total requests allowed: 44320 Total requests blocked: 224`
- **show ip urlfilter cache** - 显示可缓存至缓存表中的最大条目数，以及在特权 EXEC 模式下使用 show ip urlfilter cache 命令时缓存至缓存表中的条目数和目标 IP 地址
- **show ip urlfilter filter config** - 显示过滤配置例如：`hostname#show ip urlfilter config URL filter is ENABLED Primary Websense server configurations ==================================== Websense server IP address Or Host Name: 192.168.15.15 Websense server port: 15868 Websense retransmission time out: 6 (in seconds) Websense number of retransmission: 2 Secondary Websense servers configurations == None Other configurations ===================== Allow Mode: ON System Alert: ENABLED Audit Trail: ENABLED Log message on Websense server: ENABLED Maximum number of cache entries: 5000 Maximum number of packet buffers: 200 Maximum outstanding requests: 1000`

故障排除

错误消息

`%URLF-3-SERVER_DOWN:`Connection to the URL filter server 10.92.0.9 is down - 当配置的 UFS 发生故障时，会显示这种第 3 级 LOG_ERR 类型的消息。发生这种情况时，防火墙会将配置的服务器标记为辅助服务器，然后尝试启动其他辅助服务器之一并将其标记为主服务器。如果没有配置其他服务器，防火墙将进入允许模式并显示 URLF-3-ALLOW_MODE 消息。

`%URLF-3-ALLOW_MODE:URL`此LOG_ERR类型信息显示，当所有UFSs发生故障时，并且系统回车允许模式。

注意： 每当系统进入允许模式（所有过滤服务器均发生故障），都会触发一个周期性保活计时器，尝试打开 TCP 连接并启动服务器。

`%URLF-5-SERVER_UP:Connection to an URL filter server 10.92.0.9 is made;`the system is returning from ALLOW MODE - 当检测到 UFS 启动并且系统从允许模式返回时，会显示这种 LOG_NOTICE 类型的消息。

%URLF-4-URL_TOO_LONG:URL (3072)- 当查找请求中的 URL 过长时，会显示这种 LOG_WARNING 类型的消息；长度超过 3K 的所有 URL 都将被丢弃。

%URLF-4-MAX_REQ:The number of pending request exceeds the maximum limit <1000> - 当系统中挂起请求的数量超过最大限制时，会显示这种 LOG_WARNING 类型的消息，而且所有进一步的请求都将被丢弃。

相关信息

- Cisco IOS 防火墙
- Firewall Websense URL Filtering（防火墙 Websense URL 过滤）
- Cisco IOS 安全配置指南 12.4 版 - 支持
- 技术支持和文档 - Cisco Systems