ASA Syslog配置示例

目录

简介
先决条件
要求
使用的组件
基本 Syslog
对内部缓冲器的发送记录信息
对系统日志服务器的发送记录信息
发送记录信息作为电子邮件
对串行控制台的发送记录信息
对Telnet/SSH会话的发送记录信息
显示在ASDM的日志消息
发送日志到SNMP管理站
添加时间戳到Syslog
示例 1
配置与ASDM的基本Syslog
通过 VPN 将 Syslog 消息发送到 Syslog 服务器
中央ASA配置
远程ASA配置
高级 Syslog
使用消息列表
示例 2
ASDM 配置
使用消息类
示例 3
ASDM 配置
发送对系统日志服务器的调试日志消息
使用记录表和信息分类一起
日志ACL命中数
验证
故障排除
%ASA-3-201008：禁止新连接
解决方案
相关信息

简介

本文提供展示如何配置在可适应安全工具的一配置示例(ASA)的不同的日志选项该运行代码版本8.4或以后。

ASA版本8.4介绍非常粒状过滤技术为了允许将被提交的仅某些指定的系统消息。本文档的基本Syslog 部分说明传统的 Syslog 配置。本文的先进的Syslog部分显示在版本8.4的新的Syslog功能。参考的Cisco安全设备系统日志信息指南，完整系统日志消息指南的版本8.x和9.x。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与ASA软件版本8.4的ASA 5515
- Cisco Adaptive Security Device Manager (ASDM)版本7.1.6

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。

> **注意**：参考的ASA 8.2 ：配置Syslog使用ASDM欲知更多信息关于与ASDM版本7.1和以上的相似的配置细节。

基本 Syslog

> **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。

输入这些命令为了启用日志，查看日志，并且查看配置设置。

- **logging enable** -启用系统消息发射到所有输出位置。
- **no logging enable (event) -**记录对所有输出位置的功能失效。
- **show logging -**列出Syslog缓冲区的内容以及适合于对当前配置的信息和统计信息。

ASA能传送系统消息到多种目的地。输入in命令这些部分为了指定您类似会发送的系统日志信息的位置：

发送记录信息到内部缓冲器

logging buffered severity_level

当您存储在ASA内部缓冲器时的系统消息外部软件或硬件没有要求。输入**show logging命令**为了查看存储的系统消息。内部缓冲器有一个最大大小1 MB (可配置用**记录日志buffer-size**命令)。结果

，它也许非常迅速包裹。请记住此，当您选择内部缓冲器，更加冗长的级别记录也许迅速填装时和换行的一日志级别，内部缓冲器。

发送记录信息到系统日志服务器

```
logging host interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]
logging trap severity_level
logging facility number
```

需要运行 Syslog 应用程序的服务器才能将 Syslog 消息发送到外部主机。默认情况下ASA发送在UDP端口514的系统日志，但是协议和端口可以选择。如果TCP选择作为记录日志协议，这造成ASA通过对系统日志服务器的一TCP连接发送系统日志。如果服务器是不可访问的，或者对服务器的TCP连接不可能被建立，默认情况下， ASA将阻塞所有新连接。此行为可以禁用，如果您启用日志**permithostdown**。请参阅配置指南关于**记录日志permithostdown的更多信息**发出命令。

发送记录信息作为电子邮件

```
logging mail severity_level
logging recipient-address email_address
logging from-address email_address
smtp-server ip_address
```

当您在电子邮件中发送 Syslog 消息时，需要 SMTP 服务器。在SMTP服务器的正确配置是必要为了保证您能顺利地中继从ASA的电子邮件对指定的电子邮件客户端。如果此日志级别设置为一个非常冗长的级别，例如*调试*或*信息性*，您也许生成Syslog一个重大的编号，因为每电子邮件由向上此操作日志配置原因四个或多个另外的日志发送生成。

对串行控制台的发送记录信息

```
logging console severity_level
```

控制台记录显示的enable (event)系统消息在ASA控制台(tty)，他们发生。如果控制台记录配置，所有记录在ASA的生成ratelimited对9800位/秒， ASA串行控制台的速度。这也许造成Syslog丢弃到所有目的地，包括内部缓冲器。为此请勿使用控制台记录冗长的Syslog。

发送记录信息给Telnet/SSH会话

```
logging monitor severity_level
terminal monitor
```

操作日志监控程序使系统消息显示，当他们发生，当您访问有Telnet的ASA控制台或SSH和terminal monitor命令从该会话被执行。为了终止打印日志对您的会话，请输入**没有terminal monitor命令**。

显示在ASDM的日志消息

```
logging asdm severity_level
```

ASDM 也有一个可用来存储 Syslog 消息的缓冲区。输入**show logging asdm命令**为了显示ASDM Syslog缓冲区的内容。

发送日志到SNMP管理站

```
logging history severity_level
snmp-server host [if_name] ip_addr
snmp-server location text
snmp-server contact text
snmp-server community key
snmp-server enable traps
```

用户需要一个现有功能简单网络管理协议(SNMP)环境为了传送与SNMP的系统消息。请参阅命令关于设置和管理输出目标关于在您能使用设置和管理输出目标的命令的一完整参考。请参阅严重级别列出的消息关于严重级别列出的消息。

添加时间戳到Syslog

为了帮助对齐和命令事件，时间戳可以被添加到Syslog。推荐这为了帮助跟踪准时基于的问题。为了启用时间戳，请输入**logging timestamp命令**。这是两Syslog示例，一没有时间戳和一与：

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
442 TCP Reset-I
```

示例 1

此输出显示登录的**缓冲区**一配置示例有严重级别的**调试**。

```
logging enable
logging buffered debugging
```

以下是示例输出。

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

配置与ASDM的基本Syslog

此步骤展示所有可用的Syslog目的地的ASDM配置。

1. 为了启用注册ASA，首先请配置基本记录参数。选择 **Configuration > Features > Properties > Logging > Logging Setup**。检查**启用日志**复选框为了启用Syslog。
2. 为了配置外部服务器作为Syslog的目的地，选择在记录日志的**系统日志服务器**和单击**添加**为了添加系统日志服务器。在 Add Syslog Server 框中输入 Syslog 服务器详细信息，并在完成后选择 **OK**。
3. 选择在登陆命令的**电子邮件设置**传送系统消息作为电子邮件到特定收件人。在 Source E-Mail Address 框中指定源电子邮件地址，并选择 **Add** 以配置电子邮件收件人的目标电子邮件地址和消息严重性级别。完成后单击 **OK**。
4. 选择**设备管理**，**记录日志，**选择**SMTP**，并且输入主服务器IP地址为了指定SMTP服务器IP地址。
5. 如果要发送系统日志作为SNMP陷阱，您必须首先定义SNMP服务器。选择**SNMP**在**管理访问**菜单为了指定SNMP管理站和他们的特殊的财产的地址。
6. 选择 **Add** 以添加 SNMP 管理站。输入 SNMP 主机详细信息并单击 **OK**。
7. 为了启用将发送的日志对任何前期被提及的目的地，请选择在记录日志部分的**记录日志过滤器**。这提交您与每个可能的操作日志目的地和被发送对那些目的地的当前水平日志。选择所需的

日志记录目标并单击 **Edit**。在本例中，修改'系统日志服务器的目的地。

8. 从**在严重性**下拉列表的**过滤器**选择一适当的严重性，在这种情况下**信息性**。完成后单击 **OK**。
9. 返回 Logging Filters 窗口后，单击 **Apply**。

通过 VPN 将 Syslog 消息发送到 Syslog 服务器

在简单站点到站点VPN设计或更加复杂的星型设计，管理员也许要监控所有远程ASA防火墙用SNMP服务器和系统日志服务器查找在中心站点。

为了配置站点至站点IPSec VPN配置，参考PIX/ASA 7.x以上：PIX到PIX VPN隧道配置示例。除VPN 配置外，还必须在中心和本地站点上都配置 SNMP 和 Syslog 服务器的相关数据流。

中央ASA配置

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.

access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.

access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514


logging enable
logging trap debugging

!--- Define logging host information.
logging facility 16
logging host inside 172.22.1.5

!--- Define the SNMP configuration.
snmp-server host inside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

远程ASA配置

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.
access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0

!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
```

```
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514

!--- Define syslog server.
logging facility 23
logging host outside 172.22.1.5

!--- Define SNMP server.
snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

参考监控Cisco Secure ASA防火墙使用通过VPN隧道的SNMP和Syslog关于如何配置ASA版本8.4的更多信息

高级 Syslog

ASA版本8.4提供在组中使您配置与管理系统消息的几机制。这些机制包括消息严重性级别、消息类、消息 ID 或您创建的自定义消息列表。通过使用这些机制，您可以输入应用于小或大组消息的单一命令。通过这种方式设置 Syslog 后，您可以捕获指定消息组中的消息而不再是同一严重性级别的所有消息。

使用消息列表

使用消息列表可以按严重性级别和 ID，仅将感兴趣 Syslog 消息包含在某个组中，然后将此消息列表与所需目标关联。

完成这些步骤为了配置消息列表：

1. 输入 **logging list message_list/level severity_level [class message_class]** 命令以创建包括具有指定严重性级别或消息列表的消息的消息列表。
2. 输入 **logging list message_list message syslog_id-syslog_id2** 命令以向刚创建的消息列表中添加另外的消息。
3. 输入 **logging destination message_list** 命令以指定创建的消息列表的目标。

示例 2

输入这些命令为了建立消息列表，包括所有严重性2个(关键)消息增加消息611101到611323，并且把他们发送对控制台：

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

ASDM 配置

此过程显示使用消息列表的示例 2 的 ASDM 配置。

1. 选择 Logging 下的 **Event Lists**，并单击 Add 以创建消息列表。
2. 在 Name 框中输入消息列表的名称。在本例中，使用 **my_critical_messages**。单击 Event

Class/Severity Filters 下的 **Add**。
3. 从事件类下拉列表选择**所有**。从严重性下拉列表选择**关键**。完成后单击 **OK**。
4. 如果需要另外的消息，请单击 Message ID Filters 下的 **Add**。在本例中，您需要输入 ID 介于 611101-611323 之间的消息。
5. 在 Message IDs 框中输入 ID 范围并单击 **OK**。
6. 返回 **Logging Filters** 菜单并选择 Console 作为目标。
7. 从**使用事件列表**下拉列表选择**my_critical_messages**。完成后单击 **OK**。
8. 返回 Logging Filters 窗口后，单击 **Apply**。

如示例2所显示，这完成与使用的ASDM配置消息列表。

使用消息类

使用消息类可以将与一个类关联的所有消息发送到指定的输出位置。指定严重性级别阈值时，可以限制发送到输出位置的消息数。

```
logging class message_class destination | severity_level
```

示例 3

输入以下命令以将严重性级别为“紧急”或更高级别的所有 ca 类消息发送到控制台。

```
logging class ca console emergencies
```

ASDM 配置

此步骤显示ASDM配置例如3与使用消息列表。

1. 选择 **Logging Filters** 菜单并选择 Console 作为目标。
2. 单击 **Disable logging from all event classes**。
3. 在 Syslogs from Specific Event Classes 下，选择要添加的事件类和严重性。此过程分别使用 **ca** 和 Emergencies。
4. 单击 **Add** 以将此添加到消息类中并单击 OK。
5. 返回 Logging Filters 窗口后，单击 **Apply**。控制台在记录日志过滤器窗口当前收集加州类消息以严重级别紧急状态如显示。

这完成ASDM配置日志消息严重级别的列表的严重级别列出的例如3.参考的消息。

发送对系统日志服务器的调试日志消息

对于高级故障排除，功能/协议特殊化调试日志要求。默认情况下，这些日志消息在终端(SSH/Telnet)显示。如果调试启用，从属于调试种类和速率生成的调试消息，使用CLI也许证明困难。随意地，调试消息可以重定向到系统日志进程和生成作为Syslog。这些系统日志可以发送到所有Syslog目的地和会其他Syslog。为了将调试转变为Syslog，请输入**记录日志debug trace**命令。此配置发送debug输出，比如Syslog，到系统日志服务器。

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

使用记录表和信息分类一起

输入**list命令的记录日志**为了捕获单独LAN对LAN和远程访问IPSec VPN消息的Syslog。本示例捕获具有“调试”级别或更高级别的所有 VPN（IKE 和 IPsec）类系统日志消息。

示例

```
hostname(config)#logging enable
hostname(config)#logging timestamp
hostname(config)#logging list my-list level debugging class vpn
hostname(config)#logging trap my-list
hostname(config)#logging host inside 192.168.1.1
```

日志ACL命中数

添加*日志*到每个访问列表元素(ACE)您希望为了记录，当访问列表点击时。使用以下语法：

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

示例

```
ASAfirewall(config)#access-list 101 line 1 extended permit icmp any any log
```

ACL，默认情况下，记录每被拒绝的数据包。没有需要添加日志选项**拒绝**ACL生成已拒绝数据包的Syslog。当指定 **log** 选项时，它将为其应用到的 ACE 生成 Syslog 消息 106100。系统消息106100为每匹配的permit生成或拒绝穿过ASA防火墙的ACE流。将缓存第一个匹配流。后续匹配会增加 **show access-list** 命令中显示的命中计数。默认访问列表日志记录行为（未指定 **log** 关键字）是：如果数据包被拒绝，则生成消息 106023，如果数据包被允许，则不生成任何 Syslog 消息。

可以为生成的 Syslog 消息 (106100) 指定可选 Syslog 级别 (0 - 7)。如果未指定级别，则为新 ACE 使用默认级别 6（信息性）。如果ACE已经存在，则其当前日志级别依然是不可更改。如果指定 **log disable** 选项，则将完全禁用访问列表日志记录。不生成任何 Syslog 消息，包括消息 106023。**log** default 选项将还原默认访问列表日志记录行为。

要使 Syslog 消息 106100 可以显示在控制台输出中，请完成以下步骤：

1. 输入**logging enable命令**为了启用系统日志信息发射到所有输出位置。必须设置日志记录输出位置才能查看任何日志。
2. 输入**日志消息***<message_number>***级别***<severity_level>*命令为了设置一个特定系统日志信息的严重级别。在这种情况下，请输入**日志消息106100**命令为了启用消息106100。
3. 输入**logging console message_list|severity_level** 命令以使系统日志消息可以在发生时显示在安全设备控制台 (tty) 上。将 severity_level 设置为从 1 到 7 的值或使用级别名称。还可以使用 message_list 变量指定要发送的消息。
4. 输入**show logging消息**命令为了显示的系统日志信息消息列表从默认设置被修改了，是消息分配一不同的严重级别和消息禁用。以下是 **show logging message** 命令的示例输出

   ：
   ```
   ASAfirewall#show logging message 106100
   syslog 106100: default-level informational (enabled)
   ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
   100
   ```

验证

当前没有可用于此配置的验证过程。

故障排除

如果要抑制将发送的一特定系统消息对系统日志服务器，则您必须输入命令如显示。

```
hostname(config)#no logging message <syslog_id>
```

有关详细信息，请参阅 logging message 命令。

%ASA-3-201008：禁止新连接

%ASA-3-201008:`Disallowing new connections.`错误消息被看到，当ASA无法联系系统日志服务器时，并且新连接没有允许。

解决方案

当您已启用 TCP 系统日志消息但无法到达 Syslog 服务器时，或当您使用 Cisco ASA Syslog 服务器 (PFSS) 并且 Windows NT 系统上的磁盘已满时，将显示此消息。要解决此错误消息，请完成以下步骤：

- 如果已启用 TCP 系统日志消息，请禁用它。
- 如果使用 PFSS，请释放 Windows NT 系统上 PFSS 所在的空间。
- 保证系统日志服务器上，并且您能ping从思科ASA控制台的主机。
- 重新启动 TCP 系统消息日志记录以允许数据流。

如果系统日志服务器断开，并且Tcp记录配置，请使用记录日志permithostdown命令或换成UDP记录。

相关信息

- 思科ASA防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems