通过 FMC 在 FTD 上配置日志记录

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 配置全局系统日志配置
  - 日志设置
  - 基本日志记录设置
  - VPN日志记录设置
  - FTP服务器信息（可选）
  - 闪存大小（可选）
  - 事件列表
  - 速率限制系统日志
  - Syslog 设置
- 配置本地日志记录
- 配置外部日志记录
  - 远程系统日志服务器
  - 用于日志记录的电子邮件设置

验证

故障排除

相关信息

简介

本文档介绍如何通过 Firepower 管理中心 (FMC) 为 Firepower Threat Defense (FTD) 配置日志记录。

先决条件

要求

Cisco 建议您了解以下主题：

- FirePOWER技术

- 自适应安全设备 (ASA)
- 系统日志协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMC版本6.0.1及更高版本。
- 适用于运行软件版本6.0.1及更高版本的ASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)的ASA Firepower威胁防御映像。
- 适用于运行软件版本6.0.1及更高版本的ASA(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)的ASA Firepower威胁防御映像。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FTD系统日志提供用于监控和排除FTD设备故障的信息。这些日志在日常故障排除和事件处理中都非常有用。FTD设备支持本地和外部日志记录。

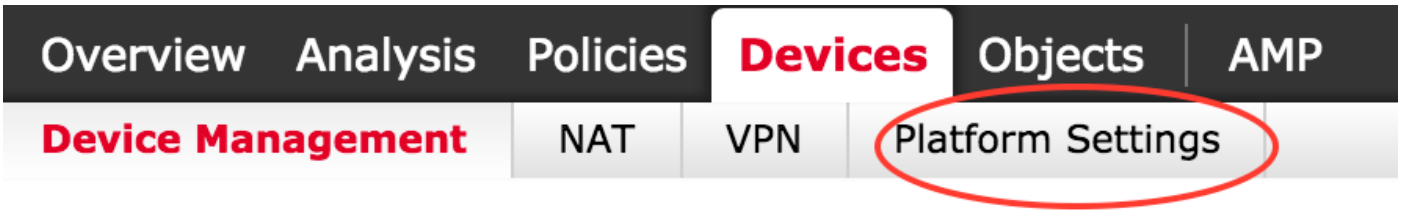
本地日志记录可帮助解决实时问题，而外部日志记录是从FTD设备到外部系统日志服务器的日志收集方法。记录到中央服务器有助于聚合日志和警报。外部日志记录可帮助记录关联和事件处理。

对于本地日志记录，FTD设备支持控制台、内部缓冲区选项和安全外壳(SSH)会话日志记录。对于外部日志记录，FTD设备支持外部系统日志服务器和邮件中继服务器。

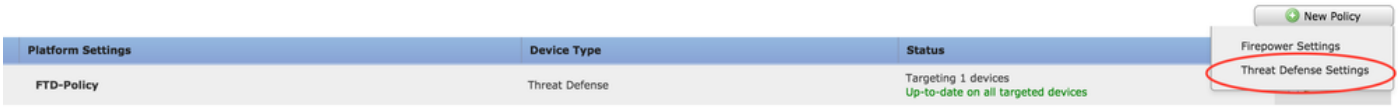
注意：如果大量流量通过设备，请注意日志记录/严重性/速率限制的类型。这样做是为了限制日志数量，从而避免影响防火墙。

配置

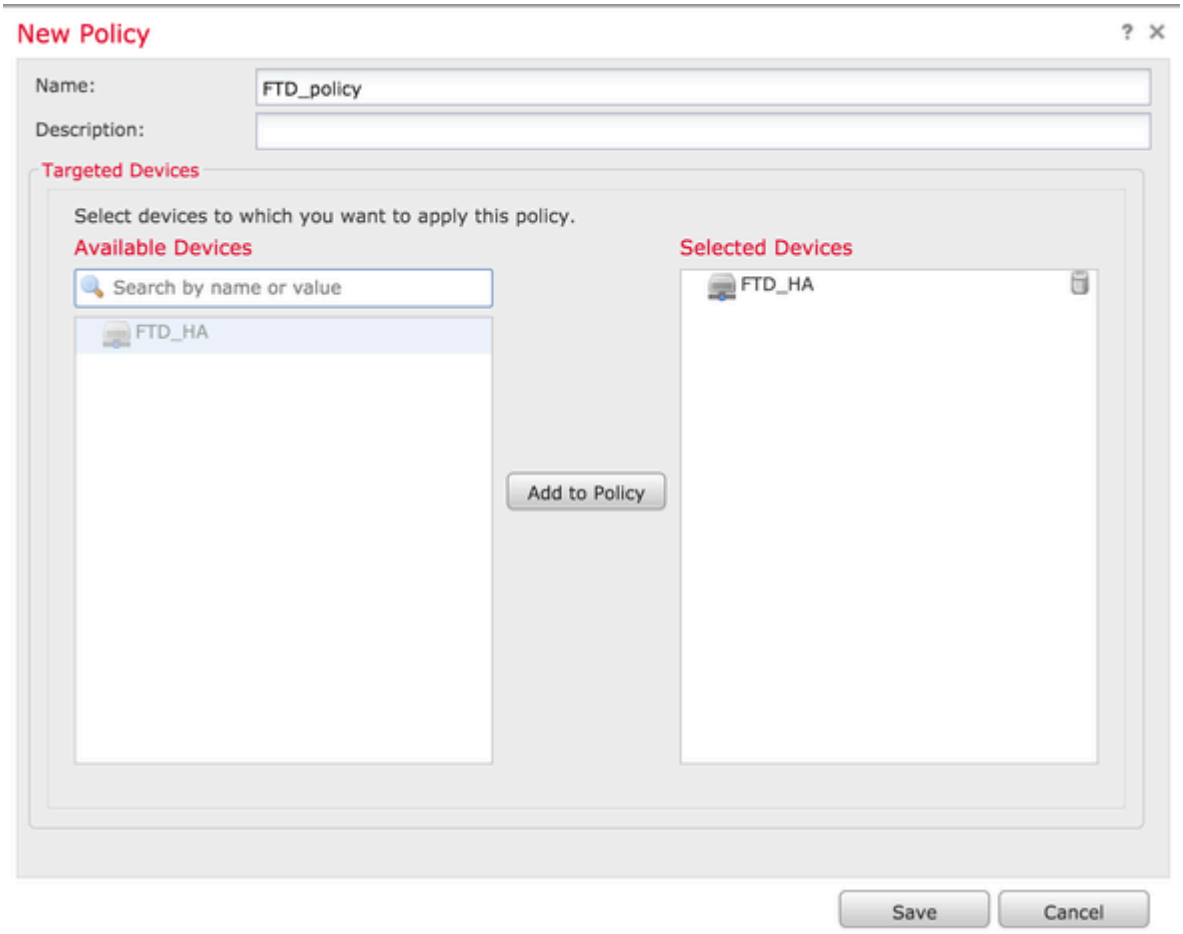
1.导航到Devices（设备）选项卡下的Platform Settings（平台设置）选项卡时，可以配置所有与日志记录相关的配置。选择Devices > Platform Settings，如下图所示：



2.单击铅笔图标编辑存在的策略，或者单击New Policy，然后选择Threat Defense Settings以创建新的FTD策略：



3.选择要应用策略的FTD设备，然后单击Save:



配置全局系统日志配置

有些配置适用于本地和外部日志记录。本节详细介绍可为系统日志配置的必需和可选参数。

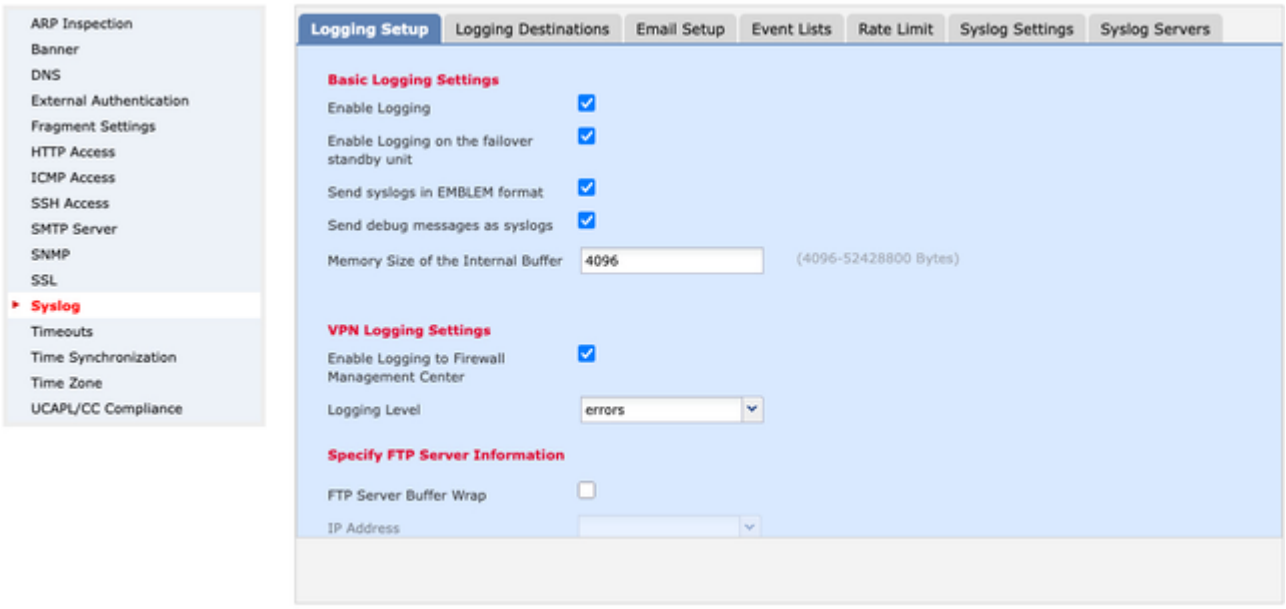
日志设置

1.日志记录设置选项适用于本地和外部日志记录。要配置日志记录设置，请选择Devices > Platform Settings。

2.选择**Syslog > Logging Setup**。

基本日志记录设置

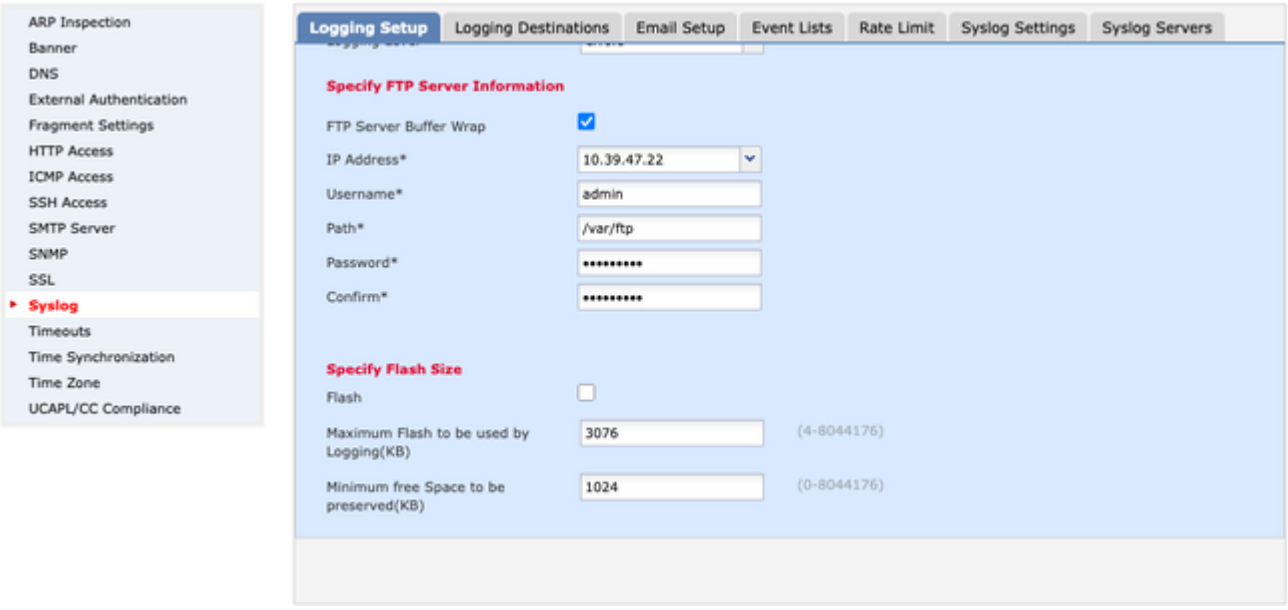
- 启用日志:选中Enable Logging复选框以启用日志记录（这是强制选项。）
- 在故障切换备用设备上启用日志记录:选中Enable Logging on the failover standby unit复选框以配置备用FTD(它是FTD高可用性(HA)集群的一部分)上的日志记录。
- 以EMBLEM格式发送系统日志:选中Send syslogs in EMBLEM format复选框，为每个目标启用格式系统日志作为EMBLEM。EMBLEM格式主要用于CiscoWorks Resource Manager Essentials(RME)系统日志分析器。此格式与路由器和交换机生成的Cisco IOS软件系统日志格式匹配。它仅可用于UDP系统日志服务器。
- 以系统日志形式发送调试消息：选中Send debug messages as syslogs复选框以将调试日志作为系统日志消息发送到系统日志服务器。
- 内部缓冲区的内存大小:输入FTD可以保存日志数据的内部内存缓冲区大小。如果达到其缓冲区限制，则轮换日志数据。



VPN日志记录设置

您可以为FTD设备的VPN故障排除系统日志启用记录。所有VPN系统日志显示的默认严重性级别为errors或更高的严重性（除非更改）。 您可以通过FTD平台设置管理VPN日志记录，并且可以通过编辑目标设备的VPN日志记录设置来调整消息严重性级别。将VPN日志记录级别设置为4级以上（警告、通知、信息或调试）可能会使FMC过载。

注意：当您为设备配置站点到站点或远程访问VPN时，默认情况下，它会自动启用向FMC发送VPN系统日志。



FTP服务器信息（可选）

如果要在日志数据覆盖内部缓冲区之前将其发送到FTP服务器，请指定FTP服务器详细信息。

- FTP服务器缓冲区包:选中FTP Server Buffer Wrap复选框以将缓冲区日志数据发送到FTP服务器。
- IP Address:输入FTP服务器的IP地址。
- username：输入FTP服务器的用户名。
- 路径:输入FTP服务器的目录路径。
- 密码：输入FTP服务器的密码。
- 确认:再次输入相同的密码。

闪存大小（可选）

指定闪存大小，以在内部缓冲区已满后将日志数据保存到闪存。

- flash:选中Flash复选框以将日志数据发送到内部闪存。
- 日志记录使用的最大闪存(KB):输入用于日志记录的最大闪存大小（以KB为单位）。
- 要保留的最小可用空间(KB):输入要保留的最小闪存大小（以KB为单位）。

单击Save以保存平台设置。选择Deploy选项，然后选择要在其中应用更改的FTD设备。单击Deploy开始部署平台设置。

事件列表

通过Configure Event Lists选项，可以创建/编辑事件列表并指定要在事件列表过滤器中包含的日志数据。在日志记录目标下配置日志记录过滤器时，可以使用事件列表。

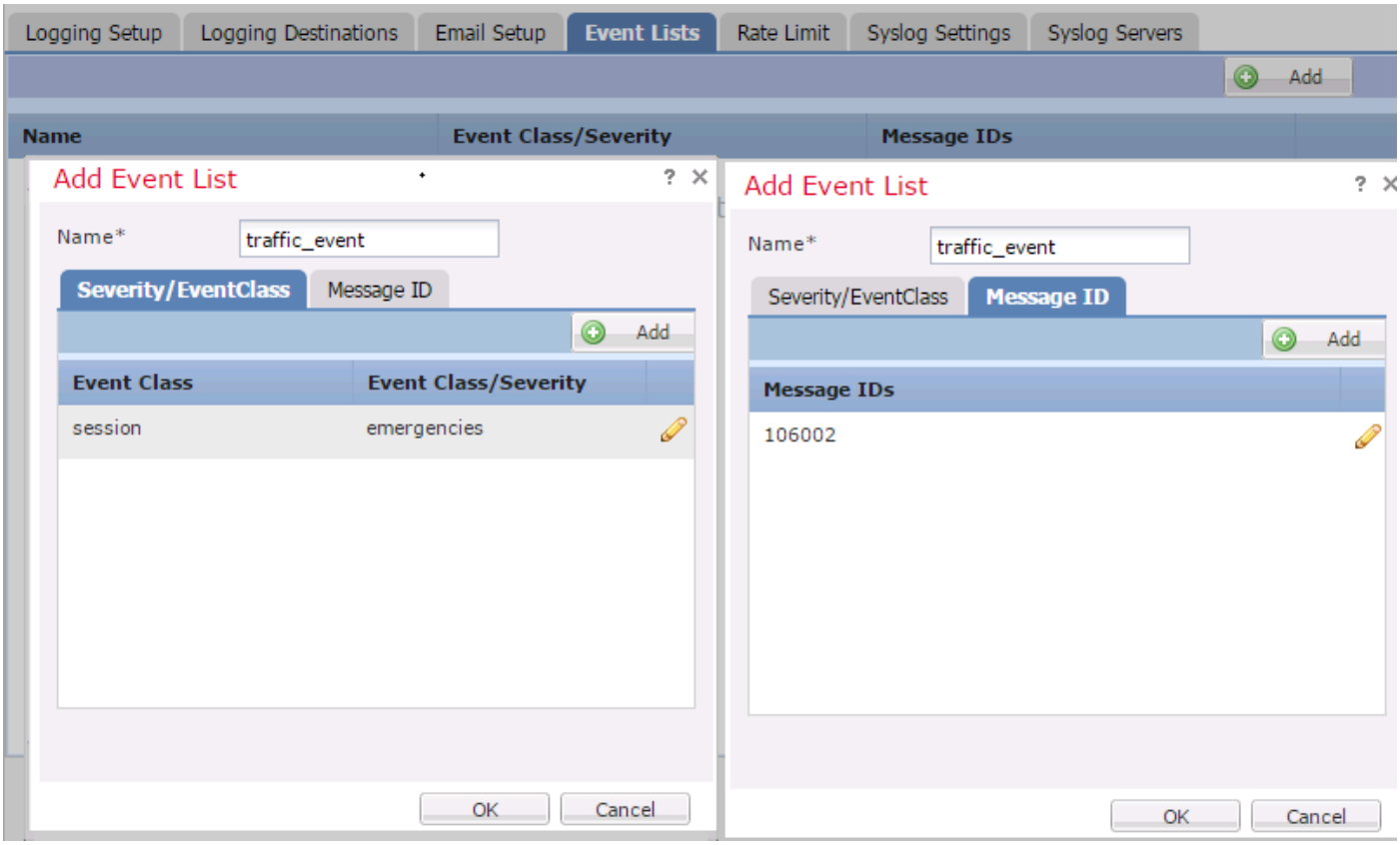
系统允许两个选项使用自定义事件列表的功能。

- 类别和严重性
- 消息 ID

1.要配置自定义事件列表，请选择Device > Platform Setting > Threat Defense Policy > Syslog > Event List，然后单击Add。这些选项包括：

- 名称：输入事件列表的名称。
- 严重性/事件类：在Severity/Event Class部分，单击Add。
- 事件类:从下拉列表中选择所需的日志数据类型事件类。Event Class定义一组表示相同功能的Syslog规则。例如，会话的Event Class包含与该会话相关的所有系统日志。

- 系统日志严重性:从下拉列表中选择所选Event Class的严重性。严重性范围为0（紧急）至7（调试）。
- 消息 ID:如果您对与消息ID相关的特定日志数据感兴趣，请单击Add以基于消息ID放置过滤器。
- 消息ID:将消息ID指定为单独/范围格式。



2.单击OK保存配置。

3.单击保存以保存平台设置。选择Deploy，选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

速率限制系统日志

Rate limit选项定义可以发送到所有已配置目标的消息数量，并定义要分配速率限制的消息的严重性。

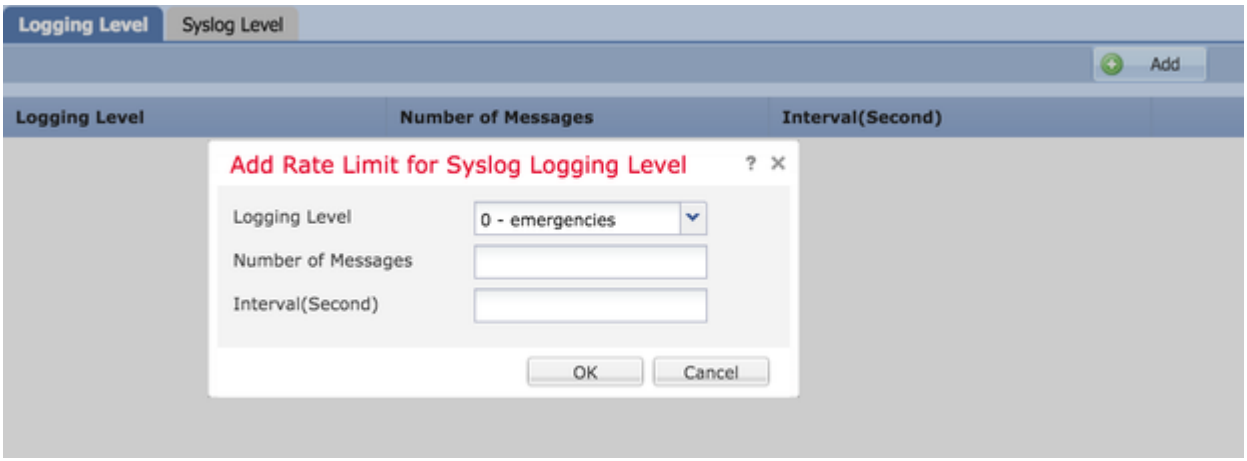
1.要配置系统日志的速率限制，请选择Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit。您可以使用两个选项指定速率限制：

- 日志记录级别
- 系统日志级别

2.要启用基于日志记录级别的速率限制，请选择日志记录级别，然后单击添加。

- 日志记录级别:从Logging Level下拉列表中选择要添加速率限制的日志记录级别。
- 消息数量:输入在指定时间间隔内接收的最大系统日志消息数。
- 间隔（秒）:根据之前配置的参数Number of Messages，输入要接收的固定系统日志消息集的时间间隔。

系统日志的速率是消息/间隔数。



3.单击OK保存日志记录级别配置。

4.要启用基于系统日志级别的速率限制，请选择系统日志级别，然后单击添加。

- 系统日志ID:系统日志ID用于唯一标识系统日志消息。从Syslog ID下拉列表中，选择Syslog ID。
- 消息数量:输入在指定时间间隔内接收的系统日志消息的最大数量。

- 间隔（秒）:根据之前配置的参数Number of Messages，输入要接收的固定系统日志消息集的时间间隔。

系统日志的速率是消息数/间隔。



5.单击OK以保存系统日志级别配置。

6.单击保存以保存平台设置。选择Deploy，然后选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

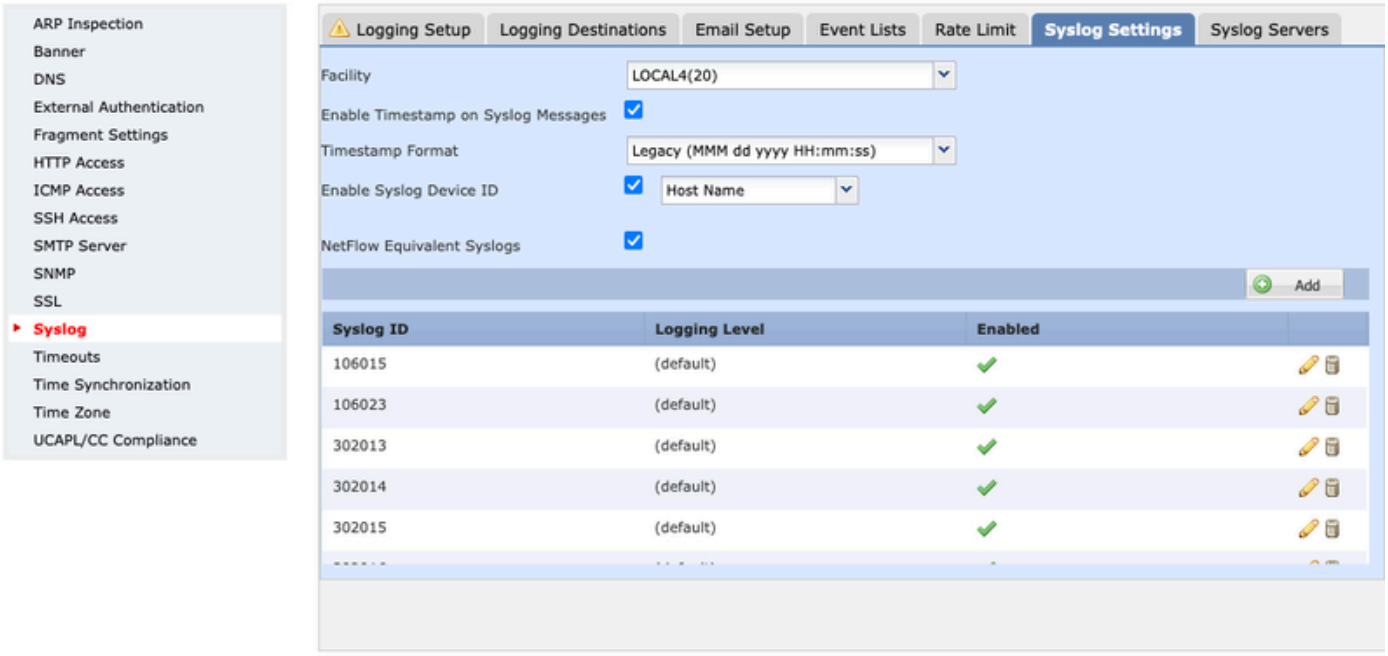
Syslog 设置

系统日志设置允许配置设备值包括在系统日志消息中。您可以在日志消息和其他特定于系统日志服务器的参数中包含时间戳。

1.要配置自定义事件列表，请选择Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings。

- 设施:设备代码用于指定记录消息的程序类型。具有不同设施的报文可以不同方式处理。从Facility下拉列表中，选择设施值。
- 在系统日志消息上启用时间戳:选中Enable Timestamp on Syslog Messages框以在Syslog消息中包含时间戳。启用此选项后，可以选择Timestamp Format。
- 启用系统日志设备ID:选中Enable Syslog Device ID复选框以在非EMBLEM格式的系统日志消息中包含设备ID。
- Netflow等效系统日志:选中Netflow Equivalent Syslogs复选框以发送NetFlow等效系统日志。它可能会影响设备的性能。

- 添加特定系统日志ID:要指定其他系统日志ID，请点击Add并指定Syslog ID/Logging Level复选框。



2.单击Save以保存平台设置。选择Deploy，然后选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

配置本地日志记录

Logging Destination部分可用于配置记录到特定目标。

可用的内部日志记录目标包括：

- 内部缓冲区:日志记录到内部日志记录缓冲区（日志记录缓冲区）。
- 控制台:将日志发送到控制台（日志控制台）。
- SSH会话:将系统日志记录到SSH会话（终端监控）。

配置本地日志记录有三个步骤。

1.选择Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations。

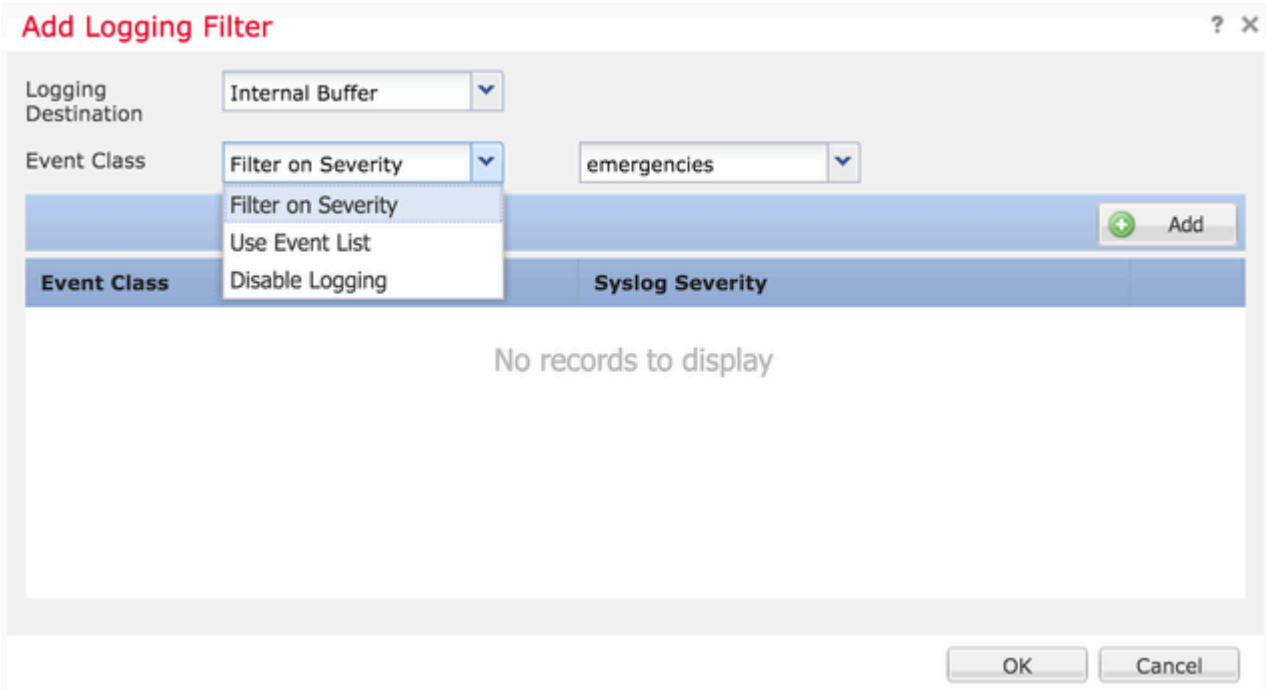
2.单击Add为特定日志记录目标添加日志记录过滤器。

3.日志记录目标:从Logging Destination下拉列表中选择所需的日志记录目标作为Internal Buffer、Console或SSH会话。

事件类:从Event Class下拉列表中，选择Event类。事件类是表示相同功能的一组系统日志。可以通过三种方式选择事件类：

- 按严重性过滤:事件类根据系统日志的严重性进行过滤。
- 用户事件列表:管理员可以使用自己的自定义事件类创建特定的事件列表，并在本节中引用它们。
- 禁用日志记录：使用此选项可禁用所选日志记录目标和日志记录级别的日志记录。

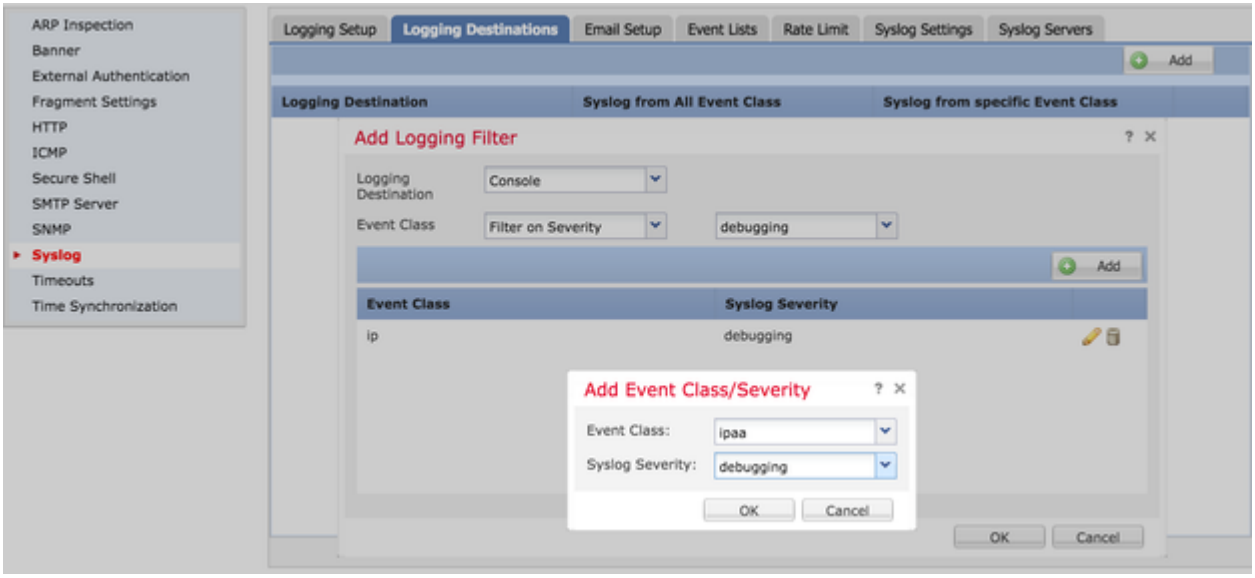
日志记录级别:从下拉列表中选择日志记录级别。日志记录级别范围为0（紧急）至7（调试）。



4.要向此日志记录过滤器添加单独的Event类，请单击Add。

事件类:从Event Class下拉列表选择Event Class。

系统日志严重性:从Syslog Severity下拉列表中选择系统日志严重性。



5.一旦过滤器配置为添加特定日志记录目标的过滤器，请单击确定。

6.单击保存以保存平台设置。选择Deploy，选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

配置外部日志记录

要配置外部日志记录，请选择Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations。

FTD支持这些类型的外部日志记录。

- syslog 服务器:将日志发送到远程系统日志服务器。
- SNMP 陷阱:以SNMP陷阱形式发送注销。
- 电子邮件:使用预配置的邮件中继服务器通过邮件发送日志。

外部日志记录和内部日志记录的配置相同。日志记录目标的选择决定了所实施的日志记录类型。可以根据自定义事件列表为远程服务器配置事件类。

远程系统日志服务器

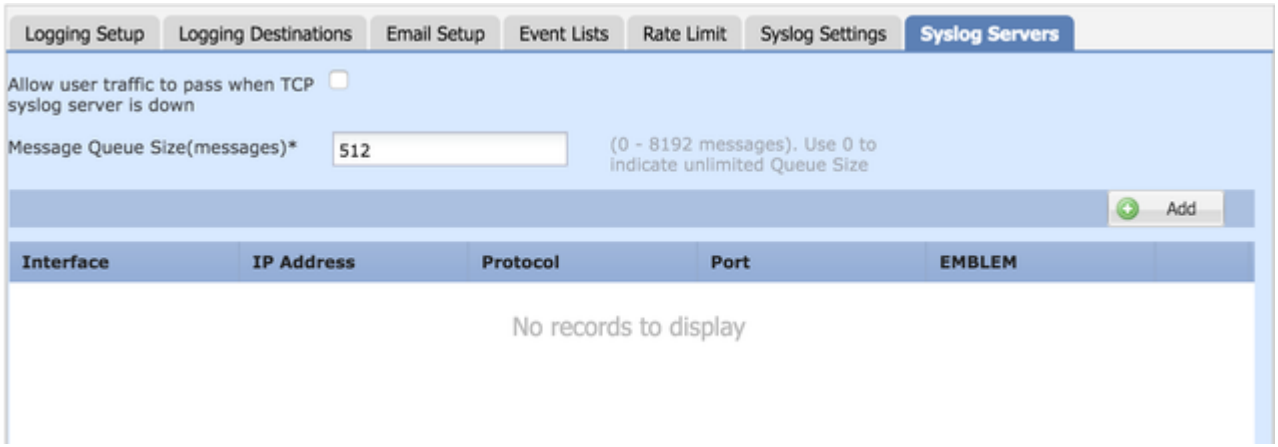
系统日志服务器可以配置为从FTD远程分析和存储日志。配置远程系统日志服务器有三个步骤。

1.选择Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers。

2.配置与系统日志服务器相关的参数。

3.当TCP系统日志服务器关闭时，允许用户流量通过。如果网络中部署了TCP系统日志服务器且无法访问，则会拒绝通过ASA的网络流量。仅当ASA和Syslog服务器之间的传输协议为TCP时，此选项才适用。选中Allow user traffic to pass when TCP syslog server is down复选框，以在Syslog server is down时允许流量通过接口。

4.消息队列大小:消息队列大小是当远程系统日志服务器繁忙并且不接受任何日志消息时，在FTD中排队的消息数。默认值为512条消息，最小值为1条消息。如果在该选项中指定0，则队列大小被视为无限制。



5.要添加远程系统日志服务器，请单击Add。

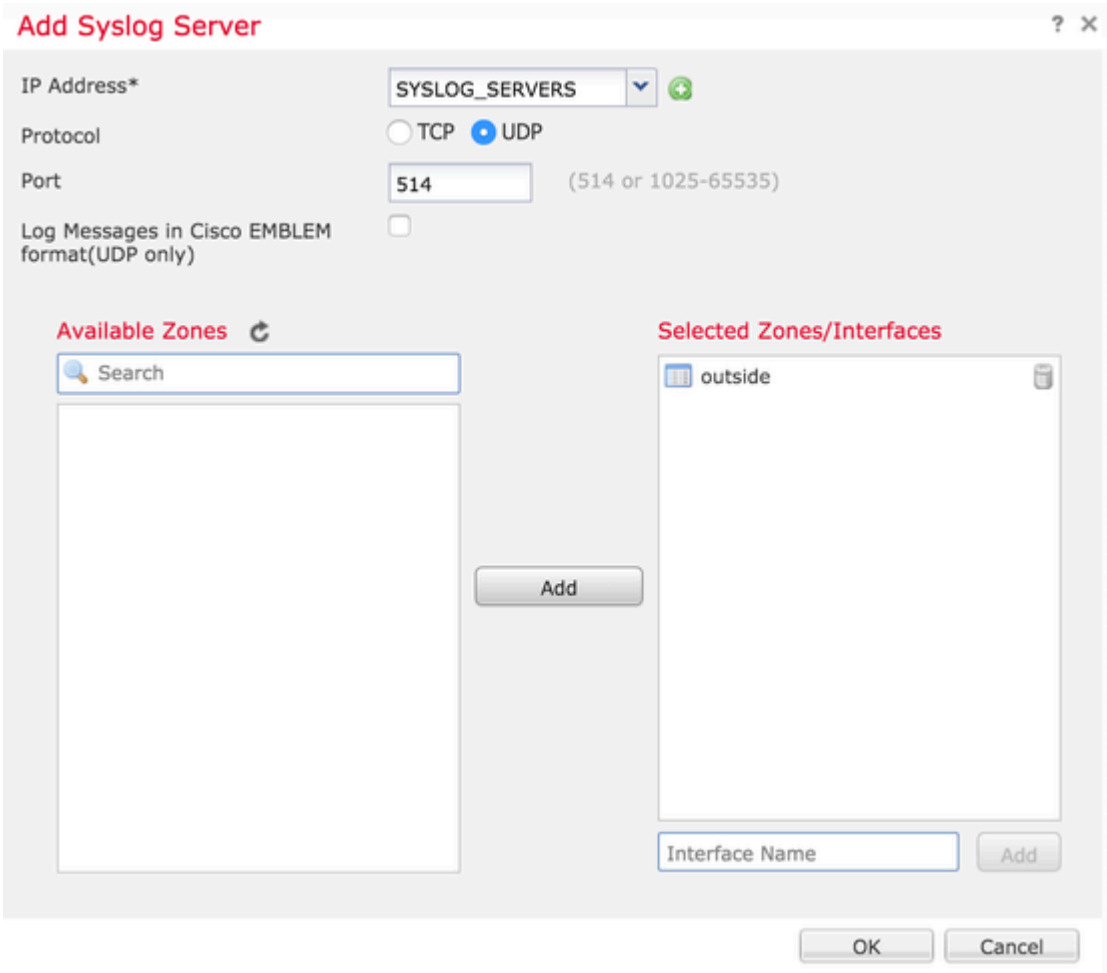
IP Address:从IP Address下拉列表中，选择列出系统日志服务器的网络对象。如果尚未创建网络对象，请点击加号(+)图标以创建新对象。

协议：单击TCP或UDP单选按钮进行系统日志通信。

端口:输入系统日志服务器端口号。默认值为514。

Cisco EMBLEM格式的日志消息（仅限UDP）:单击Log Messages in Cisco EMBLEM format（仅UDP）复选框以启用此选项。如果需要以思科EMBLEM格式记录消息（仅适用于基于UDP的系统日志）。

可用区域:输入可访问系统日志服务器的安全区域，并将其移至Selected Zones/Interfaces列。



6.单击确定和保存以保存配置。

7.单击保存以保存平台设置。选择Deploy并选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

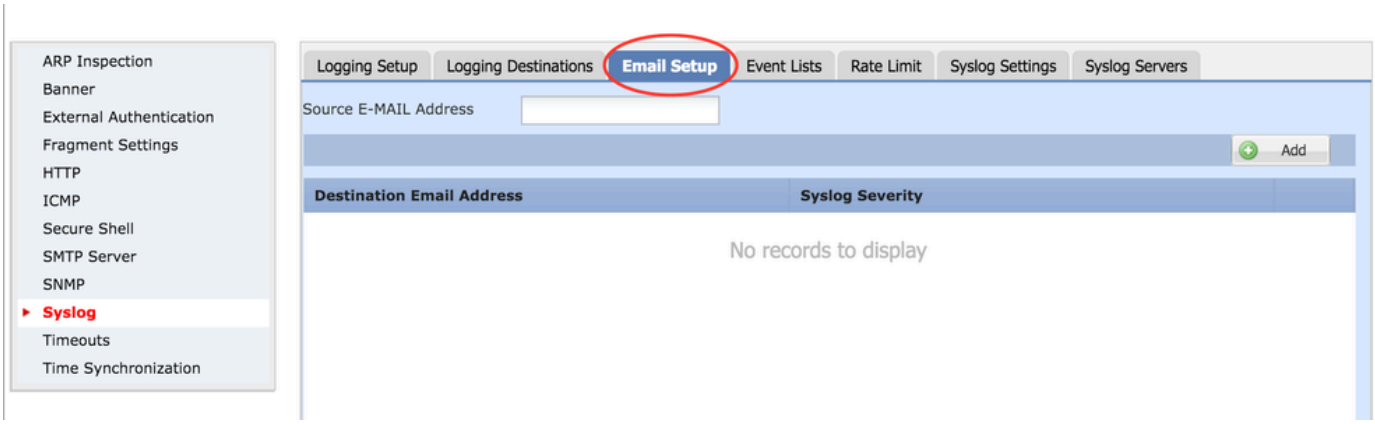
用于日志记录的电子邮件设置

FTD允许您将系统日志发送到特定邮件地址。只有在已配置邮件中继服务器的情况下，才能将邮件用作日志记录目标。

配置系统日志的邮件设置有两个步骤。

1.选择Device > Platform Setting > Threat Defense Policy > Syslog > Email Setup。

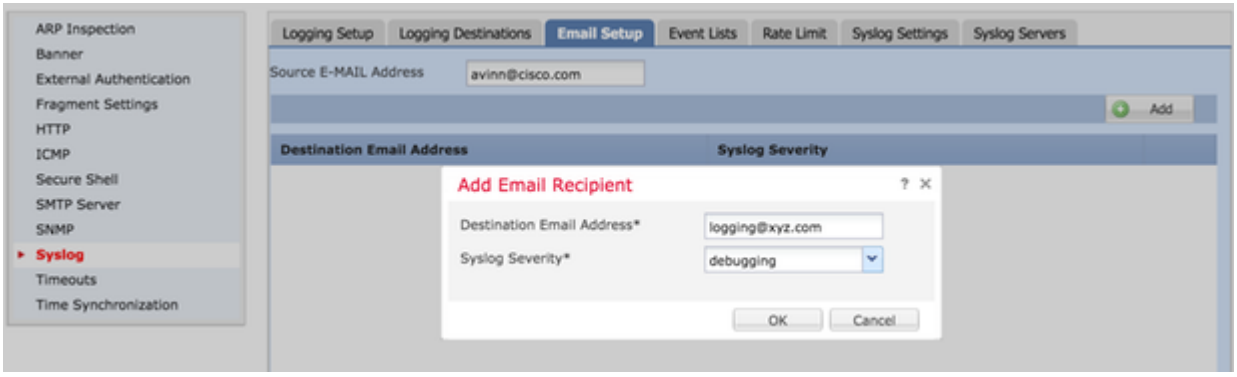
源电子邮件地址:输入源邮件地址，该地址显示在包含系统日志的FTD发送的所有邮件上。



2.要配置目标电子邮件地址和系统日志严重性，请单击Add。

目标邮件地址:输入发送系统日志消息的目标邮件地址。

系统日志严重性:从Syslog Severity下拉列表中选择系统日志严重性。



3.单击OK保存配置。

4.单击保存以保存平台设置。选择Deploy，然后选择要应用更改的FTD设备。单击Deploy开始部署平台设置。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

在FTD CLI中验证FTD系统日志配置。登录到FTD的管理界面，然后运行system support diagnostic-cli命令以通过控制台连接到诊断CLI。

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

确保可以从FTD访问系统日志服务器。通过SSH登录到FTD管理接口，并使用ping命令验证连接。

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

您可以进行数据包捕获，以验证FTD和系统日志服务器之间的连接。通过SSH登录到FTD管理界面并运行system support diagnostic-cli命令。有关数据包捕获命令，请参阅使用CLI和ASDM捕获ASA数据包的配置示例。

确保策略部署已成功应用。

相关信息

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。