为VPN故障排除实施平台设置

目录

简介

本文档介绍如何使用安全防火墙管理中心和安全防火墙威胁防御轻松组织和识别VPN调试日志。

先决条件

要求

Cisco 建议您了解以下主题：

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)

- 基本了解FMC GUI和FTD CLI的导航
- 平台设置的现有策略分配

使用的组件

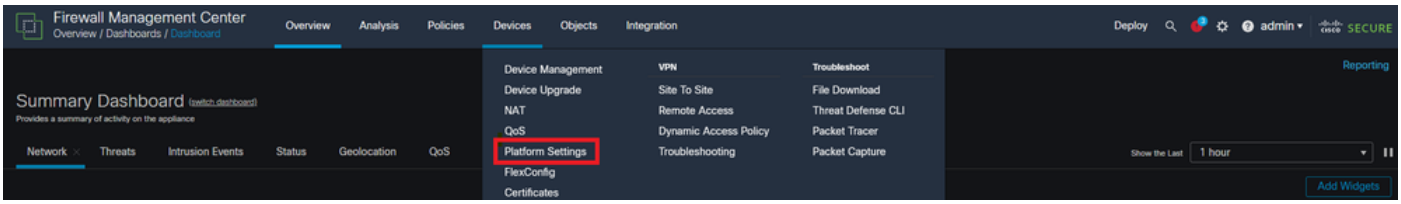
本文档中的信息基于以下软件版本和硬件版本：

- 防火墙管理中心版本7.3
- 防火墙威胁防御版本7.3

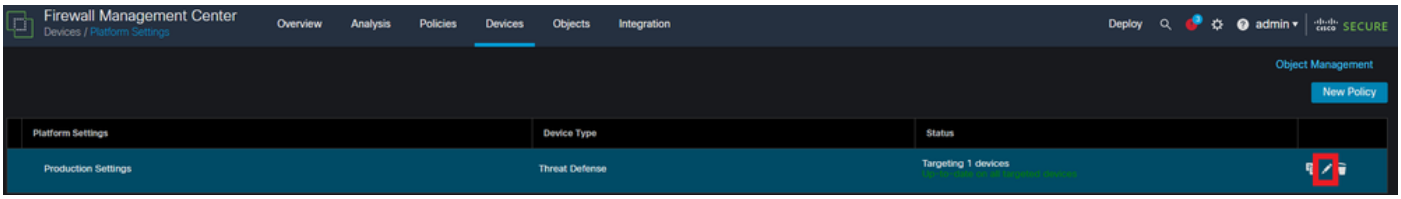
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

防火墙管理中心

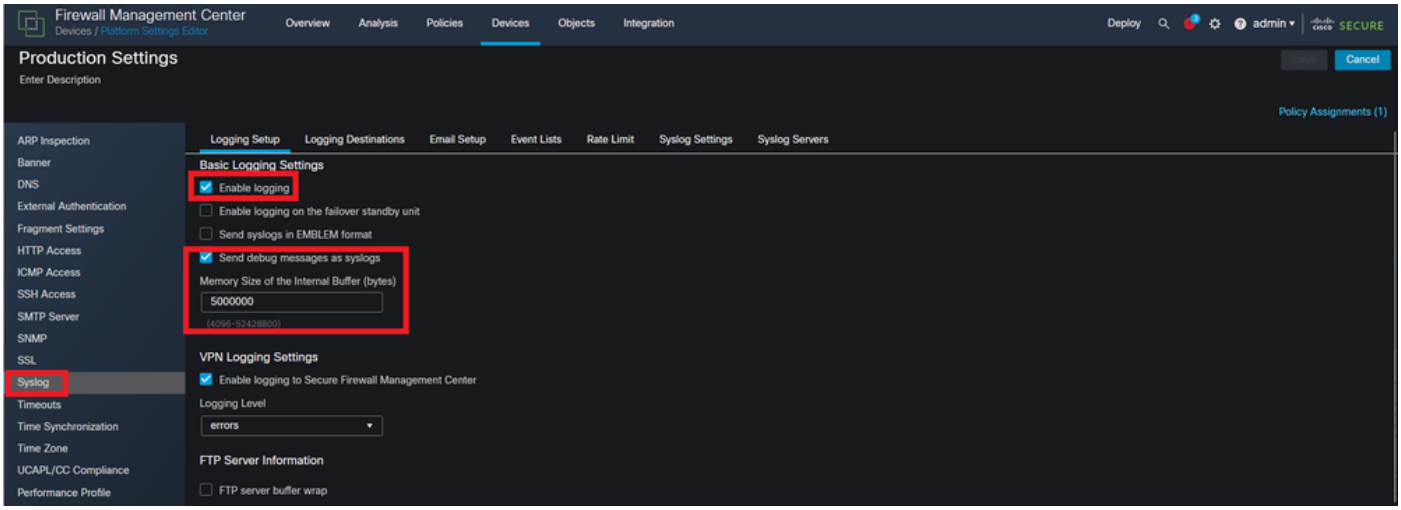
导航至。 Devices > Platform Settings



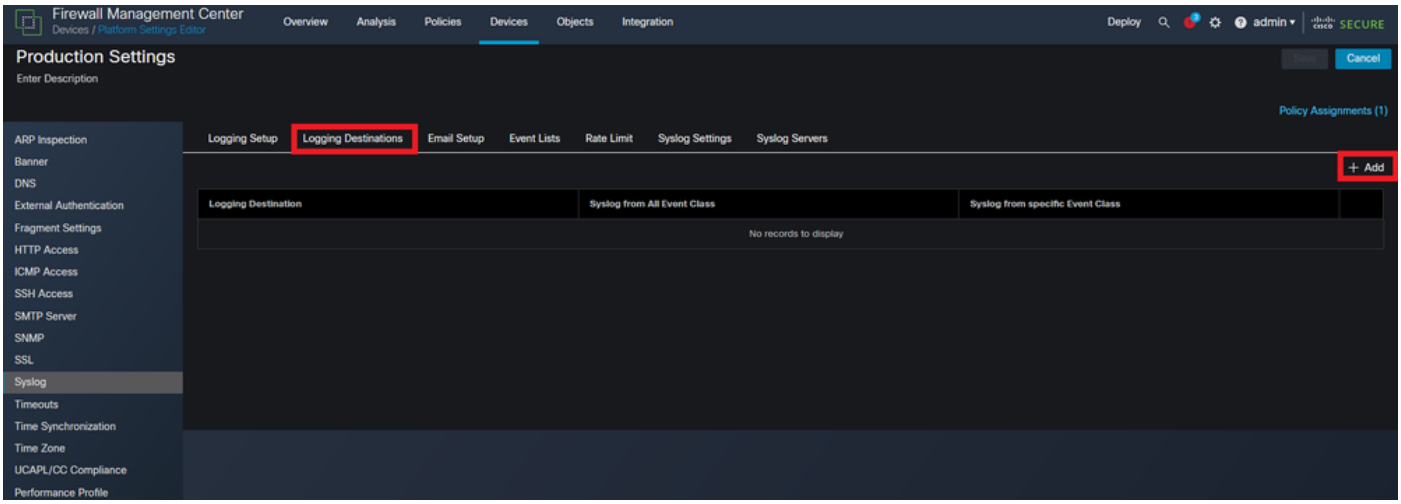
点击与**pencil**删除copy之间的icon。



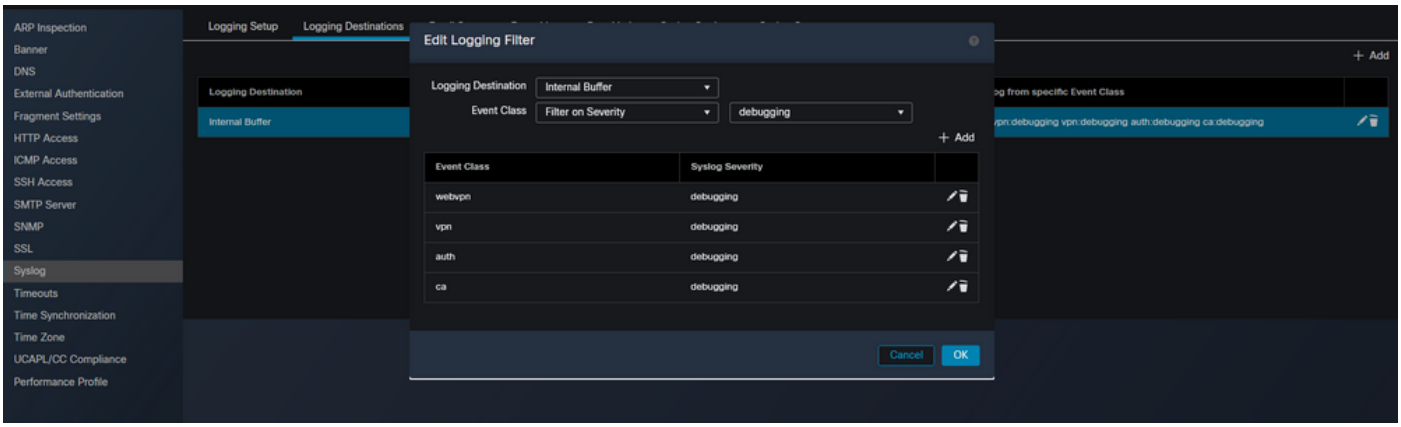
导航至Syslog选项左列并确保和已**Enable Logging**启**Send debug messages as syslog**用。此外，请确保Memory Size of the Internal Buffer，所设置的值足够用于排除故障。



单击 **Logging Destinations** ，然后单击 **+Add**.



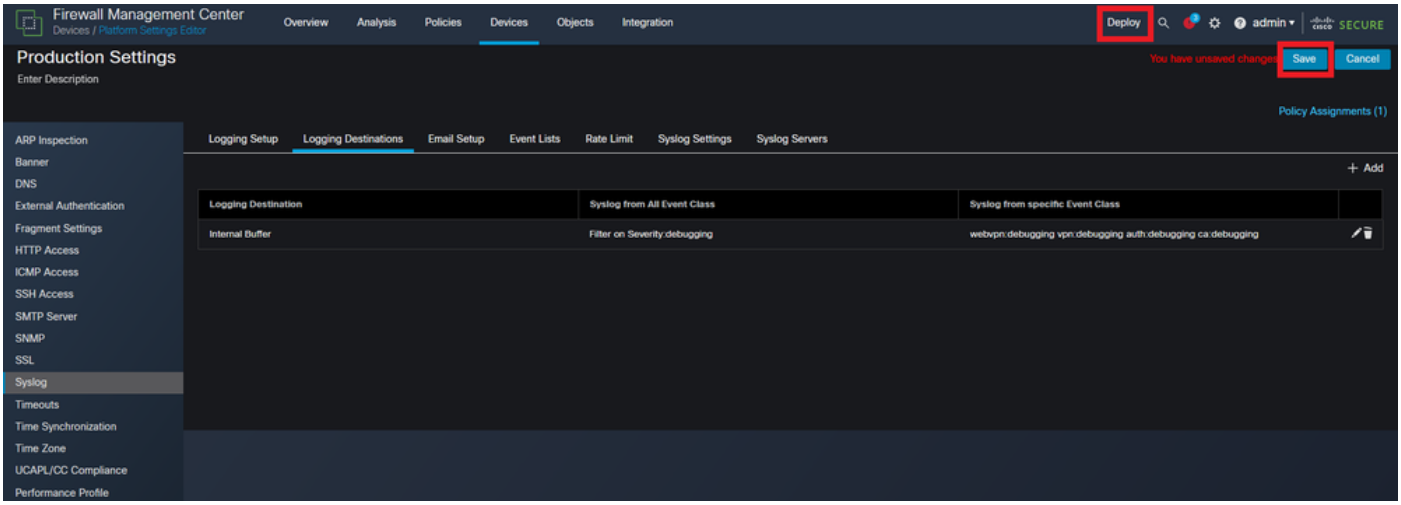
在此部分中，日志记录目标为管理员的首选项并**Internal Buffer**被使用。更改**Event Class**为 **Filter on Severity and debugging**.，完成此操作后，单击+Add并选择webvpn、vpn、和auth,caSyslog严重性为debugging。此步骤允许管理员将这些调试输出过滤到特定系统日志消息711001。这些调试输出可以根据故障排除的类型进行修改。但是，本示例中选择的选项涵盖最常见的站点到站点、远程访问和AAA VPN相关问题。



为调试创建事件类和过滤器。

警告：这会将Buffer Logging Level更改为调试，并将指定类的调试事件记录到内部缓冲区。建议将此日志记录方法用于故障排除目的，而不是长期使用。

Choose Save 然后在右上角更改Deploy配置。



防火墙威胁防御

导航到FTD CLI并发出命令show logging setting。此处的设置反映在FMC上所做的更改。确保启用了debug-trace logging，并且缓冲区日志记录与指定的类和日志记录级别匹配。

```
FTD72# show logging setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled (persistent)
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, class auth vpn webvpn ca, 362685 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, class auth vpn webvpn ca, 27 messages logged
```

在FTD CLI中显示日志记录设置。

最后，应用调试以确保将日志重定向到syslog:711001。在本例中debug webvpn anyconnect 255，应用了。这将触发日志记录debug-trace通知，告知管理员这些调试已重定向。要查看这些调试，请发出命令show log | in 711001。现在，此系统日志ID仅包含管理员应用的相关VPN调试。可以使用清除日志缓冲区清除现有日志。

```
FTD72# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and will not appear in any monitor session
INFO: debug webvpn anyconnect enabled at level 255.
FTD72# show log | in 711001
```

显示所有VPN调试都重定向到系统日志711001。

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）。