使用ASDM在Firepower模块中为系统/流量事件配置日志记录（机上管理）

目录

简介

本文档介绍Firepower模块的系统/流量事件以及将这些事件发送到外部日志记录服务器的各种方法。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解ASA（自适应安全设备）防火墙、ASDM（自适应安全设备管理器）。
- Firepower设备知识。
- 系统日志、SNMP协议知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本5.4.1及更高版本的ASA Firepower模块(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。
- 运行软件版本6.0.0及更高版本的ASA Firepower模块(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。
- ASDM 7.5(1)及更高版本。

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。

背景信息

事件类型

Firepower模块事件可分为两类：-

1. 流量事件（连接事件/入侵事件/安全情报事件/SSL事件/恶意软件/文件事件）。
2. 系统事件(Firepower操作系统(OS)事件)。

配置

配置输出目标

步骤1.系统日志服务器配置

要为流量事件配置系统日志服务器，请导航至Configuration > ASA Firepower Configuration > Policies > Actions Alerts，然后单击Create Alert 下拉菜单并选择Create Syslog Alert选项。输入系统日志服务器的值。

名称： 指定唯一标识系统日志服务器的名称。

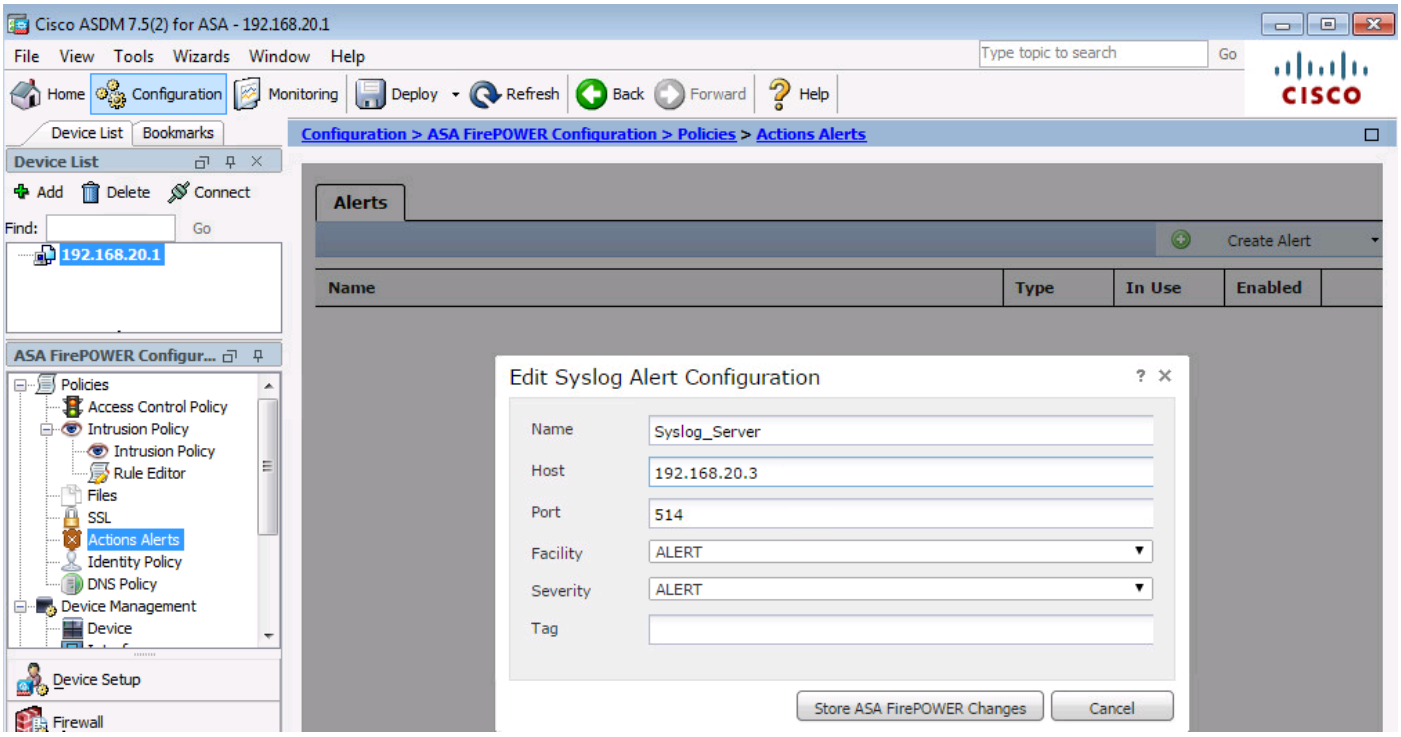
Host：指定系统日志服务器的IP地址/主机名。

端口： 指定系统日志服务器的端口号。

设施： 选择在系统日志服务器上配置的任何设施。

严重级别: 选择在系统日志服务器上配置的任何严重性。

标记： 指定要随系统日志消息一起显示的标记名称。



第二步：SNMP服务器配置

要为流量事件配置SNMP陷阱服务器，请导航到**ASDM Configuration > ASA Firepower Configuration > Policies > Actions Alerts**，然后单击**Create Alert**下拉菜单并选择**Create SNMP Alert。**

名称： 指定唯一标识SNMP陷阱服务器的名称。

陷阱服务器： 指定SNMP陷阱服务器的IP地址/主机名。

版本： Firepower模块支持SNMP v1/v2/v3。从下拉菜单中选择SNMP版本。

公用字符串: 如果在版本选项中选择v1**或v2**，请指定SNMP社区名称。

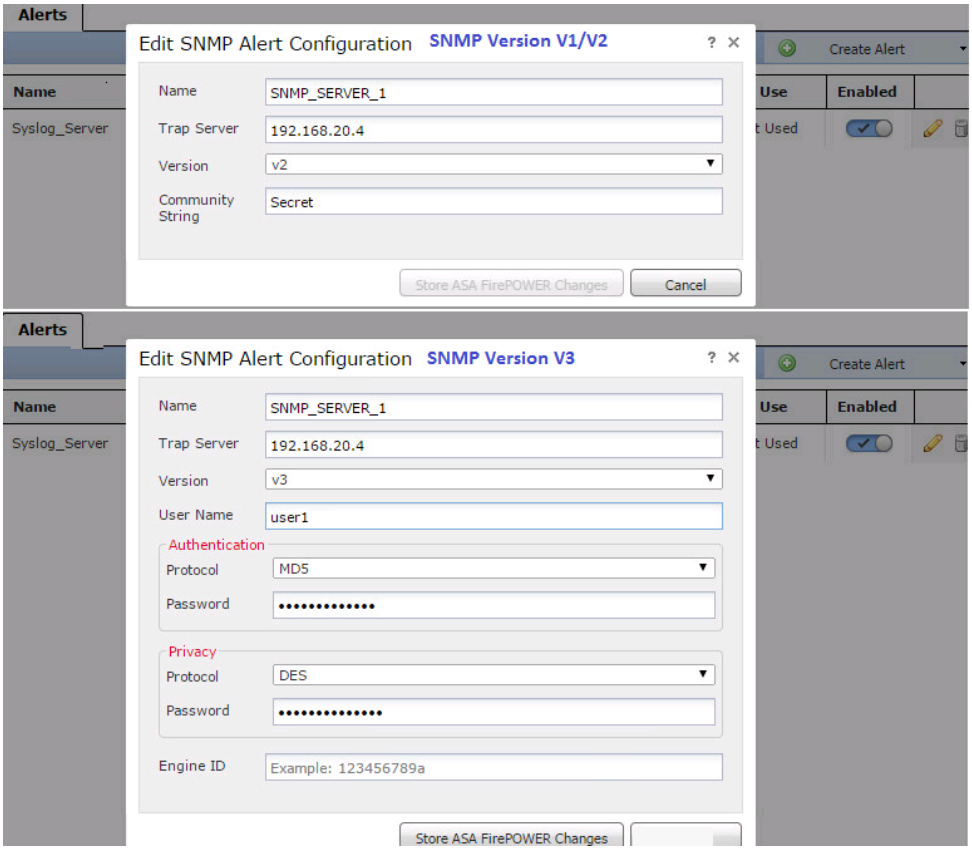
username： 如果在“版本”选项中**选择**v3，系统会提示**“用户名”**字段。指定用户名。

身份验证: 此选项是SNMP v3配置的一部分。它提供基于哈希的身份验证

算法。在“协**议**”下拉菜单中，选择哈希算法并输入

密码选项**中的**密码。如果不想使用此功能，则选择“无**”选**项。

隐私:此选项是SNMP v3配置的一部分。它使用DES算法提供加密。在协**议下**拉菜单中，选择选项**DES并**在密码字段中**输入密**码。如果不想使用数据加密功能，请选择“无”**选**项。



发送流量事件的配置

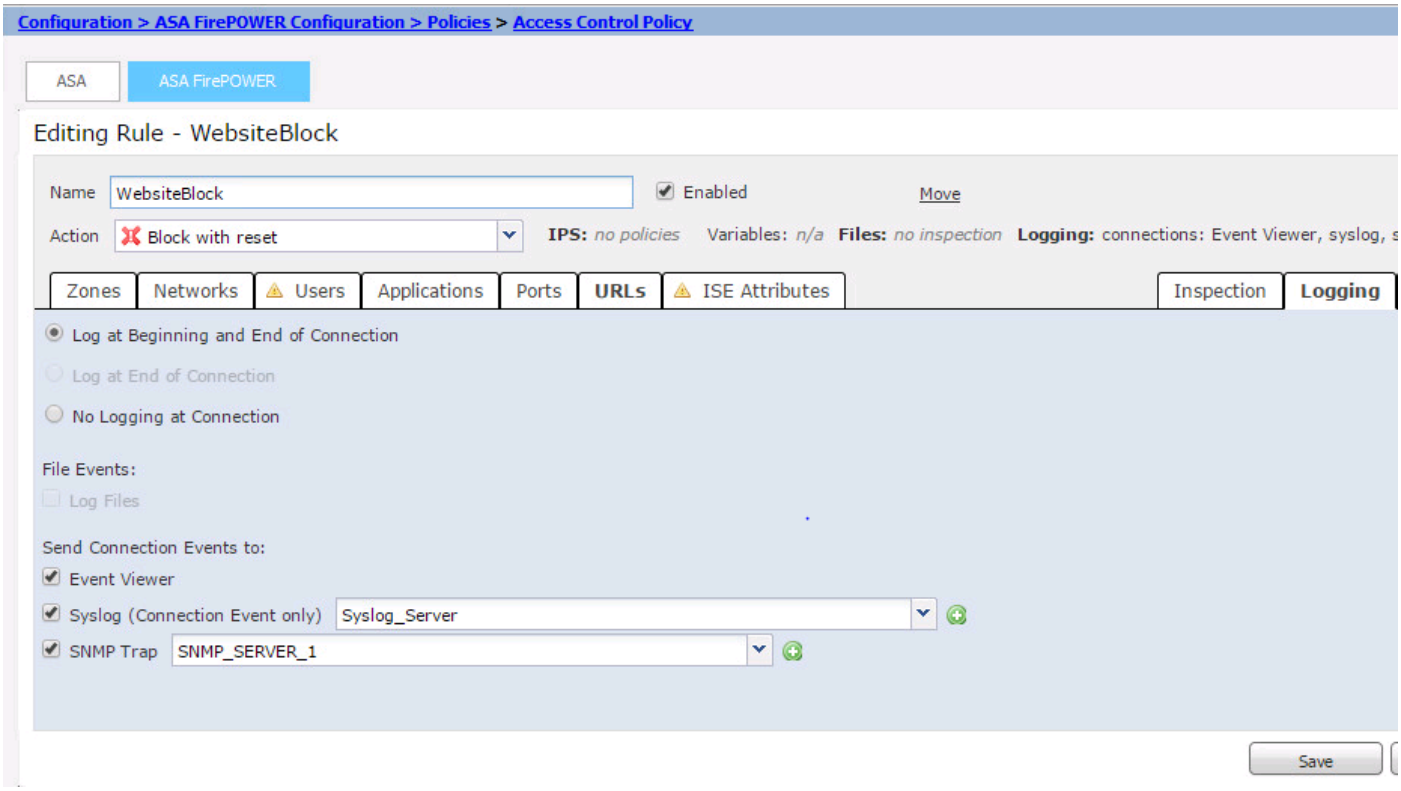
为连接事件启用外部日志记录

当流量到达启用日志记录的访问规则时，会生成连接事件。要为连接事件启用外部日志记录，请导航至**(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy)**编辑**访问规**则并导航至**logging**选项。

选择logging选项**log at Beginning and End of Connection**或**log at End of Connection**。导航至“**将连接事件发送**到”选项并指定将事件发送到何处。

要将事件发送到外部系统日志服务器，请选择**Syslog**，然后从下拉列表中选择Syslog警报响应。或者，您可以通过点击添加图标添加系统日志警**报响应**。

要将连接事件发送到SNMP陷阱服务器，请选择**SNMP陷阱**，然后从下拉列表中选择SNMP警报响应。或者，您可以通过点击添加图标添加SNMP警**报响应**。



为入侵事件启用外部日志记录

当签名（snort规则）匹配某些恶意流量时，会生成入侵事件。要为入侵事件启用外部日志记录，请导航至**ASDM Configuration > ASA Firepower Configuration > Policies> Intrusion Policy > Intrusion Policy。**创建新入侵策略或编辑现有入侵策略。导航至“高**级设置”>**“外**部响应”。**

要将入侵事件发送到外部SNMP服务器，请在SNMP警报**中选**择启用**选项，**然后单击**编辑**选项。

陷阱类型：陷阱类型用于警报中显示的IP地址。如果网络管理系统正确呈现INET_IPV4地址类型，则可以选择为二进制。否则，选择为字符串。

SNMP 版本: 选择 **Version 2** 或 **V 3** 单选按钮.

SNMP v2选项

陷阱服务器：指定SNMP陷阱服务器的IP地址/主机名，如此图所示。

公用字符串:指定社区名称。

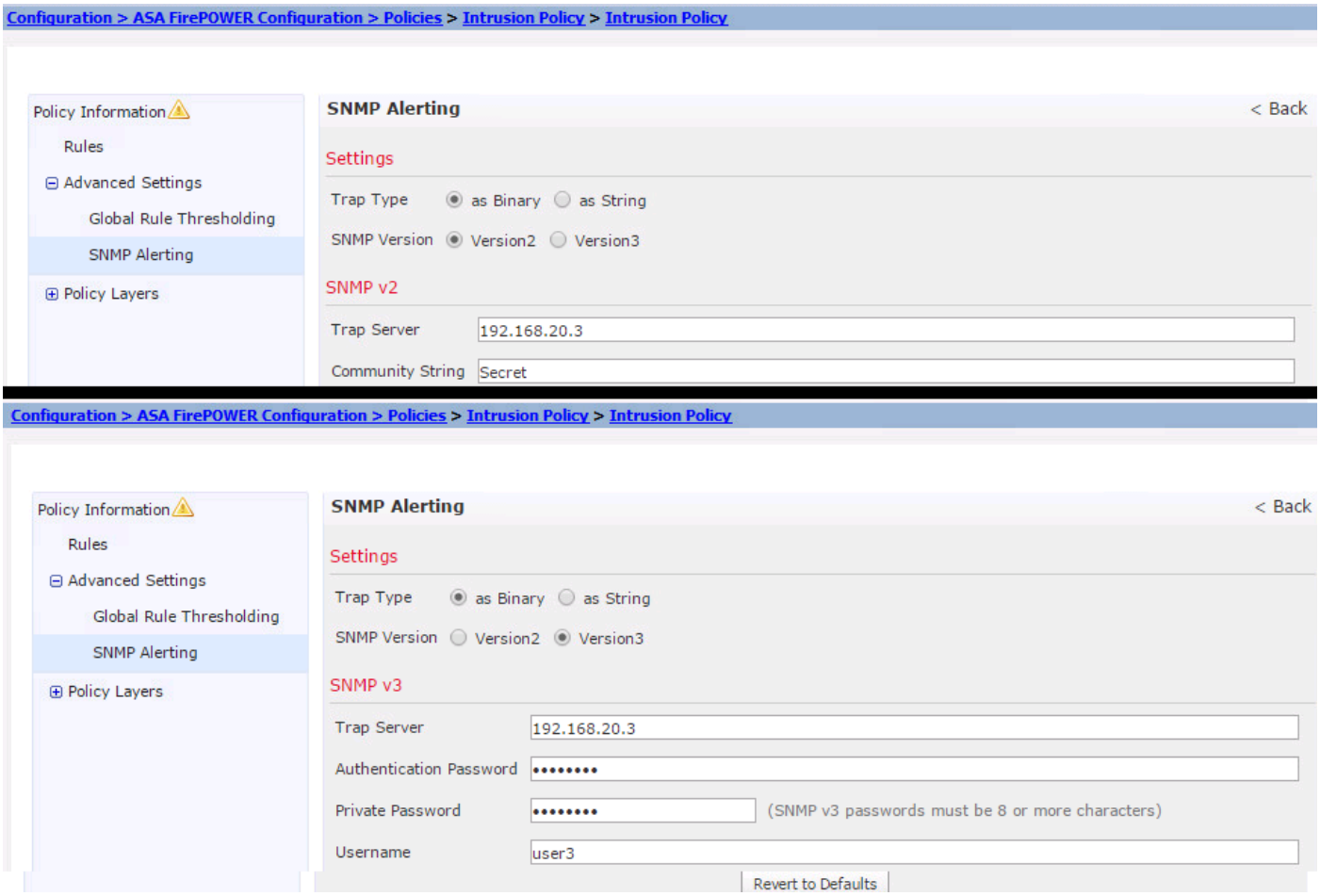
SNMP v3选项

陷阱服务器：指定SNMP陷阱服务器的IP地址/主机名，如此图所示。

身份验证口令指定身份验证所需的密码。SNMP v3使用哈希函数对口令进行身份验证。

专用密码：指定加密的密码。SNMP v3使用数据加密标准(DES)分组密码来加密此密码。

用户名：指定用户名。



要将入侵事件发送到外部系统日志服务器，请选择选项 **启用** 在系**统日志 警报** 然后单击 **编辑** 选项，如下图所示。

日志记录主机:指定系统日志服务器的IP地址/主机名。

设施： 选择任何设施 在系统日志服务器上配置。

严重级别:选择在系统日志服务器上配置的任何严重性。

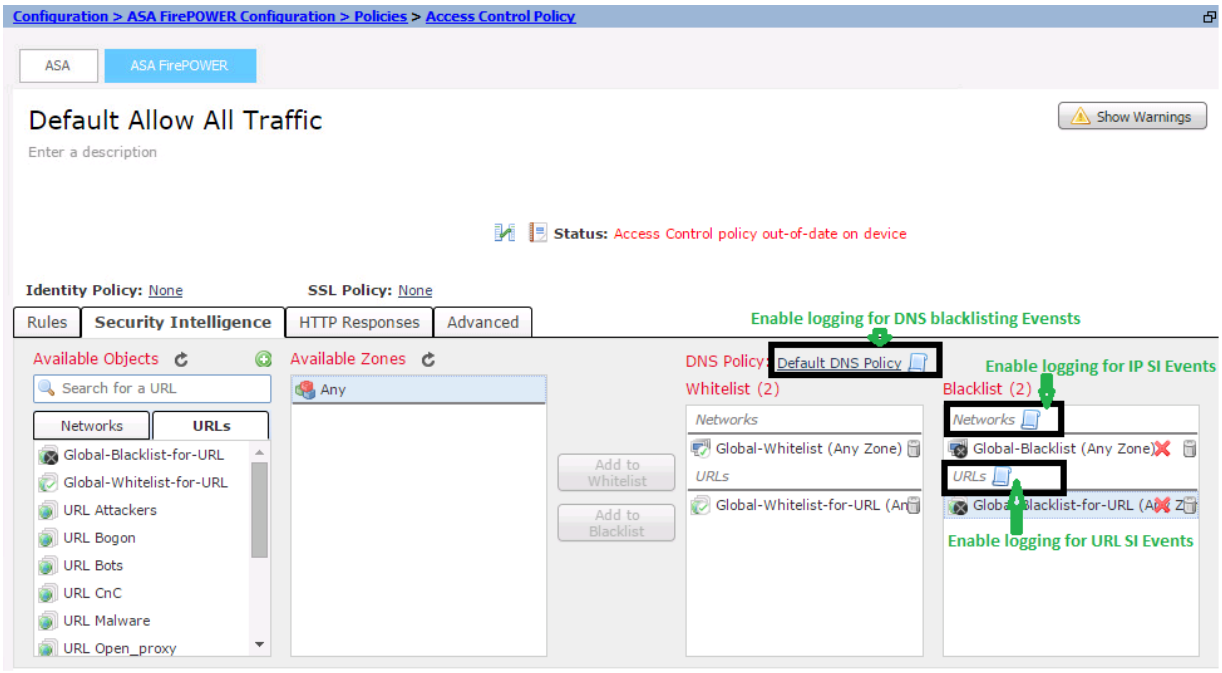
为IP安全情报/DNS安全情报/URL安全情报启用外部日志记录

当流量与任何IP地址/域名/URL安全情报数据库匹配时，生成IP安全情报/DNS安全情报/URL安全情报事件。要为IP/URL/DNS安全情报事件启用外部日志记录，请导航至**(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy > Security Intelligence)**,

单击图像中所示的图标以启用IP/DNS/URL安全情报的日志记录。单击图标将提示对话框启用日志记录，并选择将事件发送到外部服务器。

要将事件发送到外部系统日志服务器，请选择**Syslog**，然后从下拉列表中选择Syslog警报响应。或者，您可以通过点击添加图标添加系统日志警报响应。

要将连接事件发送到SNMP陷阱服务器，请选择**SNMP陷阱**，然后从下拉列表中选择SNMP警报响应。或者，您可以通过点击添加图标添加SNMP警报响应。



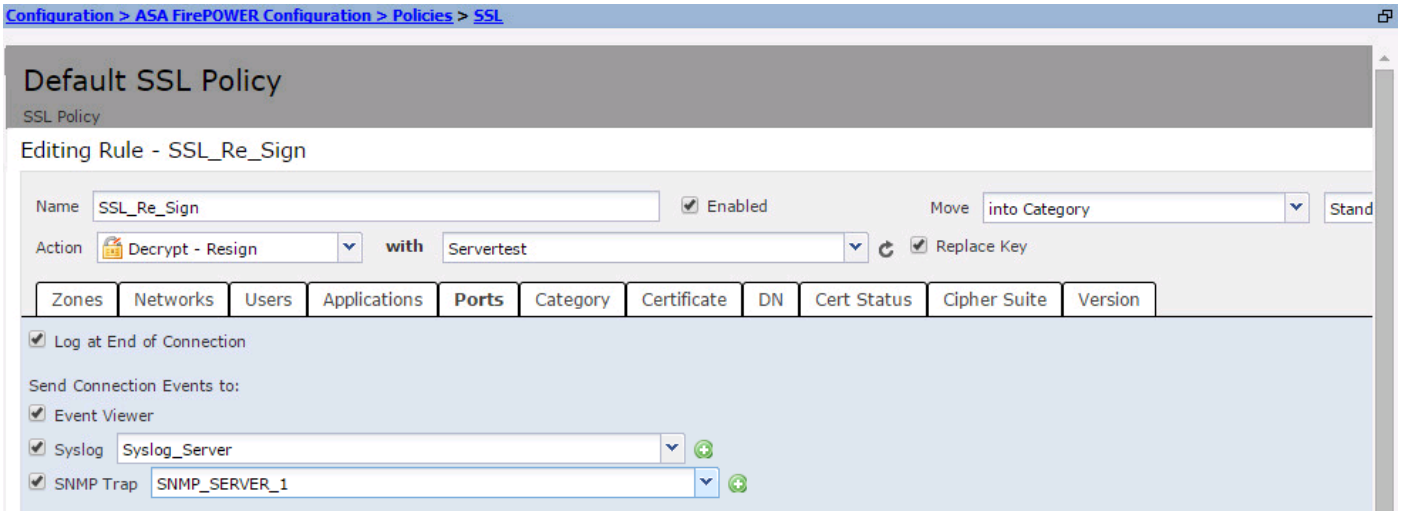
为SSL事件启用外部日志记录

当流量与SSL策略中启用日志记录的任何规则匹配时，会生成SSL事件。要为SSL流量启用外部日志记录，请导航至**ASDM Configuration > ASA Firepower Configuration > Policies > SSL。**编辑现有规则或创建新规则并导航至**logging** 选项。选择**End of Connection**选项。

然后导航至**Send Connection Events to，**并指定将事件发送到何处。

要将事件发送到外部系统日志服务器，请选择**Syslog**，然后从下拉列表中选择Syslog警报响应。或者，您可以通过点击添加图标添加系统日志警报响应。

要将连接事件发送到SNMP陷阱服务器，请选择**SNMP陷阱**，然后从下拉列表中选择SNMP警报响应。或者，您可以通过点击添加图标添加SNMP警报响应。



发送系统事件的配置

为系统事件启用外部日志记录

系统事件显示Firepower操作系统的状态。SNMP管理器可用于轮询这些系统事件。

要配置SNMP服务器以从Firepower模块轮询系统事件，您需要配置系统策略，使信息在Firepower MIB（管理信息库）中可用，该信息可由SNMP服务器轮询。

导航至**ASDM Configuration > ASA Firepower Configuration > Local > System Policy**，然后单击**SNMP**。

SNMP 版本: Firepower模块支持SNMP v1/v2/v3。请指定SNMP版本。

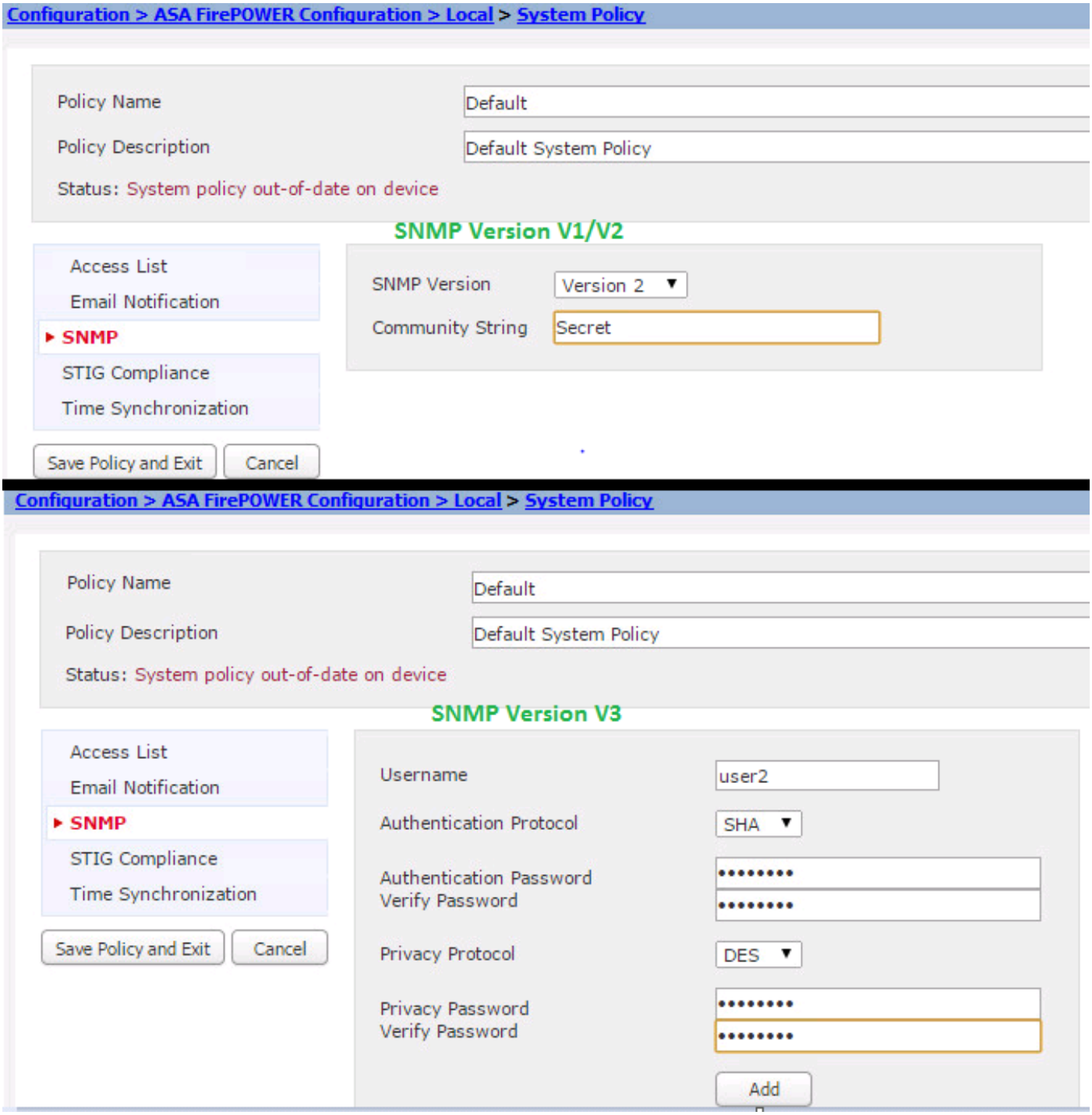
公用字符串: 如果在SNMP version选项中选择v1/ v2，请在Community String字段中键入SNMP社区名称。

username： 如果在版本选**项中**选择v3选项。单击“**添加用**户”按钮，并在“**用户**名”字段中指定用户名。

身份验证: 此选项是SNMP v3配置的一部分。它使用MD5或SHA算法根据散列消息验证代码提供身份验证。为哈希**算法**选择协议并输入密码

在**密码**字段中。如果不想使用身份验证功能，请选择“无”**选**项。

隐私: 此选项是SNMP v3配置的一部分。它使用DES/AES算法提供加密。选择加密协议并在密码字**段中输**入密码。如果不需要数据加密功能，请选择**None选**项。



:(MIB)FirepowerMIB(DCEALERT.MIB)(/etc/sf/DCEALERT.MIB)

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems