配置登陆系统流量事件的Firepower模块使用ASDM (在箱上管理)

目录

简介

本文描述Firepower模块的系统流量事件和发送这些事件多种方法对一外部日志服务器。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA (可适应安全工具)防火墙知识， ASDM (可适应安全设备管理器)。
- Firepower设备知识。
- Syslog， 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的ASA Firepower模块(ASA 5506X/5506H-X/5506W-X， ASA 5508-X， ASA 5516-X)以上。
- ASA Firepower模块(ASA 5515-X， ASA 5525-X， ASA 5545-X， ASA 5555-X)运行软件版本6.0.0以上。
- ASDM 7.5(1)以上。

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

事件的类型

Firepower模块事件在两个类型可以分类：--

1. 流量事件(连接事件/Intrusion事件/安全智能Events/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

要配置流量事件的一个系统日志服务器，导航到**Configuration> ASA Firepower Configuration>策略>操作警报**和点击**创建警报**下拉菜单和选择选项请**创建Syslog警报。**输入系统日志服务器的值。

名称： 指定独特识别系统日志服务器的名称。

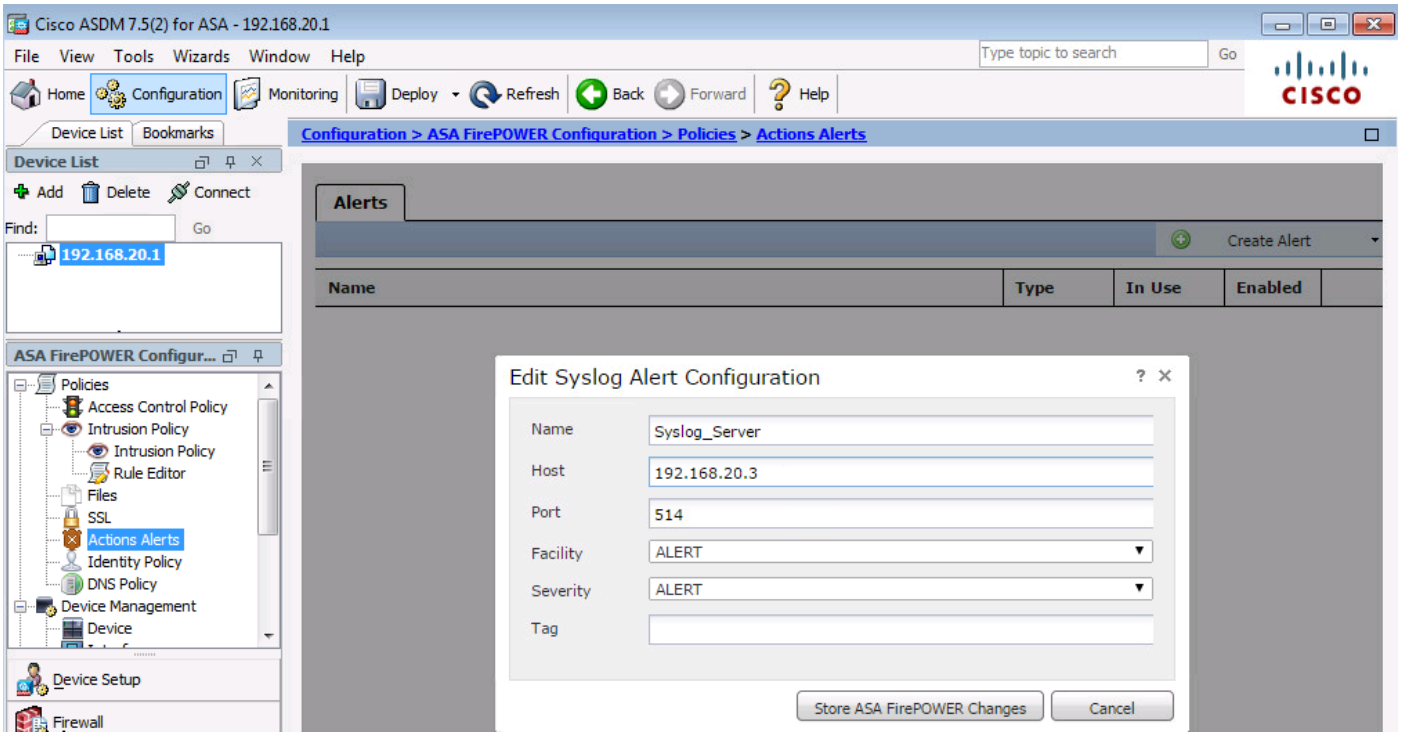
主机： 指定系统日志服务器IP地址/主机名。

波尔特： 指定系统日志服务器端口号。

设备： 选择在您的系统日志服务器配置的所有设备。

严重性： 选择在您的系统日志服务器配置的所有严重性。

标记： 指定您希望显现系统消息的标记名称。



步骤2.SNMP服务器配置

要配置流量事件的一个SNMP陷阱服务器，导航到**ASDM Configuration> ASA Firepower Configuration>策略>操作警报**和点击**创建警报**下拉菜单和选择选项请**创建SNMP警报。**

名称： 指定独特识别SNMP陷阱服务器的名称。

陷阱服务器： 指定SNMP陷阱服务器IP地址/主机名。

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

社区字符串： 如果选择v1或v2在**版本**选项，请指定SNMP团体名称。

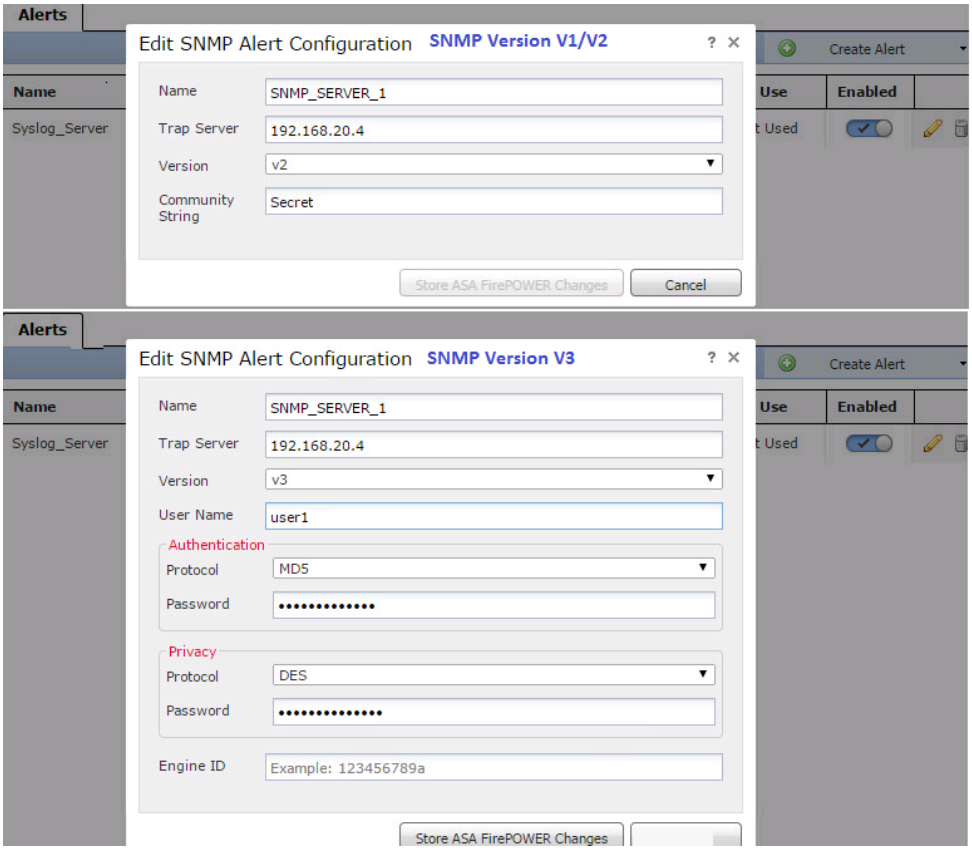
用户名： 如果选择在**版本**选项的v3，系统提示**用户名字段**。指定用户名。

验证： 此选项是SNMP v3配置的部分。它提供根据哈希的验证

算法使用MD5或SHA算法。在**协议**下拉菜单请选择散列算法&回车

在**Password选项的**密码。如果不要使用此功能，则请勿选择选项。

保密性：此选项是SNMP v3配置的部分。使用DES算法，它提供加密。在**协议**丢弃菜单请在**密码字段**选择选项， **DES&**回车密码。如果不要使用数据加密功能，则请勿选择选项。



发送的流量事件配置

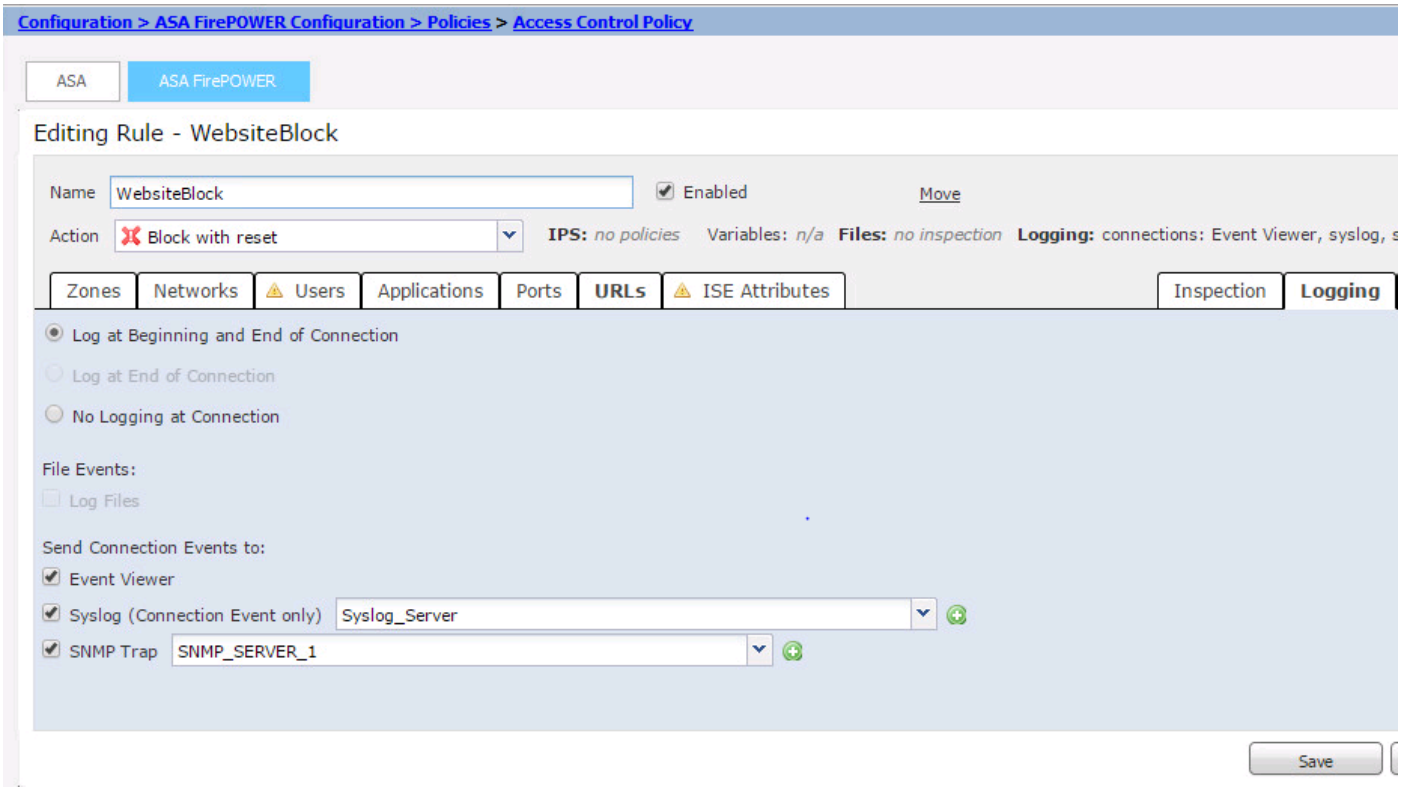
连接事件的Enable (event)外部记录日志

当流量点击与启用时的记录日志的一个访问规则连接事件生成。为了启用连接事件的外部记录日志，请导航对**(ASDM Configuration> ASA Firepower Configuration>策略>访问控制策略)**编辑**访问规则**并且导航对**日志选项**。

选择日志选项**连接日志在开始和末端**或**记录在连接结束时**。在哪里导航**发送连接事件到**选项和指定发送事件。

为了发送事件到外部系统日志服务器，请选择**Syslog**，然后选择从下拉列表的一Syslog警报答复。随意地，您能通过单击Add图标添加Syslog警报答复。

要发送连接事件到SNMP陷阱服务器，请选择**SNMP陷阱**，然后选择从下拉列表的一SNMP警报答复。随意地，您能通过单击Add图标添加SNMP警报答复。



入侵事件的Enable (event)外部记录日志

入侵事件生成，当签名(喷鼻息规则)时匹配某恶意流量。 为了启用入侵事件的外部记录日志，请导航对**ASDM Configuration> ASA Firepower Configuration> Policies>入侵策略>入侵策略。**请创建一项新的入侵策略或编辑现有入侵Policy.Navigate对**高级设置>外部答复。**

为了发送入侵事件到外部SNMP服务器，请选择在**警告的SNMP的已启用**选项然后单击**Edit选项。**

陷阱类型：陷阱类型使用在警报出现的IP地址。如果您的网络管理系统正确地回报INET_IPV4地址类型，则您能选择作为二进制。否则，请选择作为字符串。

SNMP版本： 选择**版本2**或**版本3**单选按钮。

SNMP v2选项

陷阱服务器：如此镜像所显示，指定SNMP陷阱服务器IP地址/主机名。

公用字符串:指定属性名称。

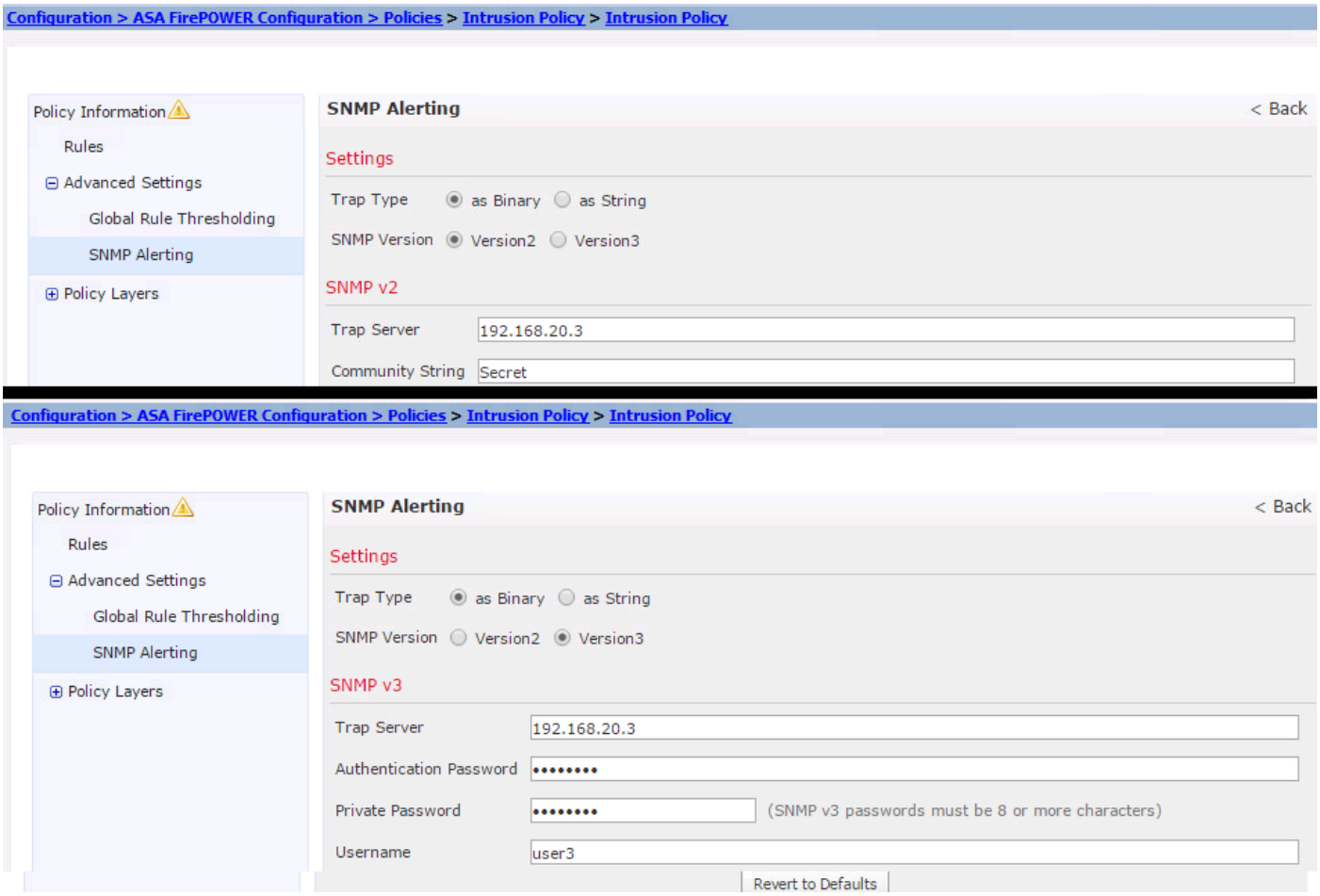
SNMP v3选项

陷阱服务器：如此镜像所显示，指定SNMP陷阱服务器IP地址/主机名。

身份验证口令Specifypassword为验证要求。SNMP v3使用散列函数验证密码。

私有密码： 指定加密的密码。SNMP v3使用数据加密标准(DES)分组加密加密此密码。

用户名：指定用户名。



如此镜像所显示，为了发送入侵事件到外部系统日志服务器，在**Syslog启用的**挑选选项然后**警告**单击**Edit选项**。

日志主机：指定系统日志服务器IP地址/主机名。

设备：选择在您的系统日志服务器配置的所有设备。

严重性：选择在您的系统日志服务器配置的所有严重性。

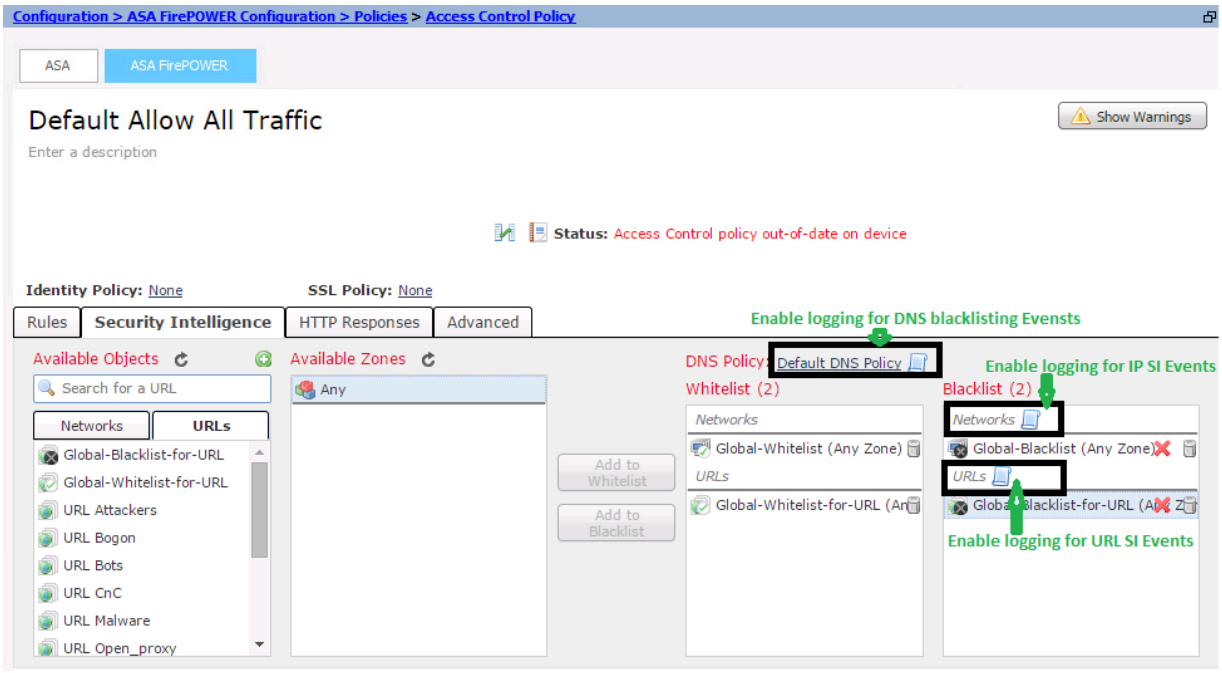
启用IP安全Intelligence/DNS安全Intelligence/URL安全智能的外部记录日志

当流量匹配所有IP地址/域名/URL安全智能数据库时，**IP安全Intelligence/DNS安全Intelligence/URL安全智能**事件生成。为了启用IP URL/DNS安全智能事件的外部记录日志，请导航对**(ASDM Configuration> ASA Firepower Configuration>策略>访问控制策略> Security智能)**，

单击**图标**如镜像所显示启用IP/DNS/URL安全智能的记录日志。单击图标提示对话框对启用日志和选项发送事件到外部服务器。

为了发送事件到外部系统日志服务器，请选择**Syslog**，然后选择从下拉列表的一Syslog警报答复。随意地，您能通过单击Add图标添加Syslog警报答复。

为了发送连接事件到SNMP陷阱服务器，请选择**SNMP陷阱**，然后选择从下拉列表的一SNMP警报答复。随意地，您能通过单击Add图标添加SNMP警报答复。



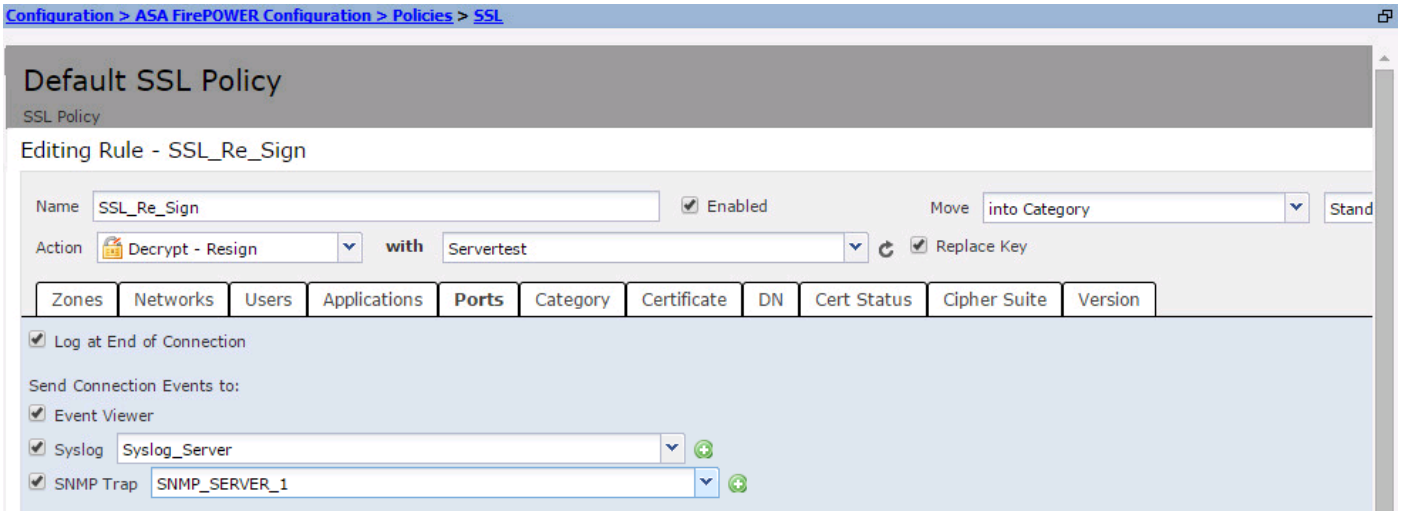
SSL事件的Enable (event)外部记录日志

SSL事件生成，当流量匹配在SSL策略时的所有规则，记录日志启用。为了启用SSL流量的外部记录日志，请导航对**ASDM Configuration> ASA Firepower Configuration>策略> SSL。** 编辑存在或创建新规则并且导航对**日志选项**。选择**日志在连接选项结束时**。

然后在哪里请导航**发送连接事件对**和指定发送事件。

要发送事件到外部系统日志服务器，请选择**Syslog**，然后选择从下拉列表的一Syslog警报答复。随意地，您能通过单击Add图标添加Syslog警报答复。

要发送连接事件到SNMP陷阱服务器，请选择**SNMP陷阱**，然后选择从下拉列表的一SNMP警报答复。随意地，您能通过单击Add图标添加SNMP警报答复。



发送的系统事件配置

系统事件的Enable (event)外部记录日志

系统事件显示Firepower操作系统状况。SNMP Manager可以使用轮询这些系统事件。

要配置SNMP服务器为了轮询从Firepower模块的系统事件，您需要配置做在可以由SNMP服务器轮询。的火力MIB的有用的资料的系统策略(管理信息库)

导航对**ASDM Configuration> ASA Firepower Configuration>本地>System策略**并且点击**SNMP**。

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

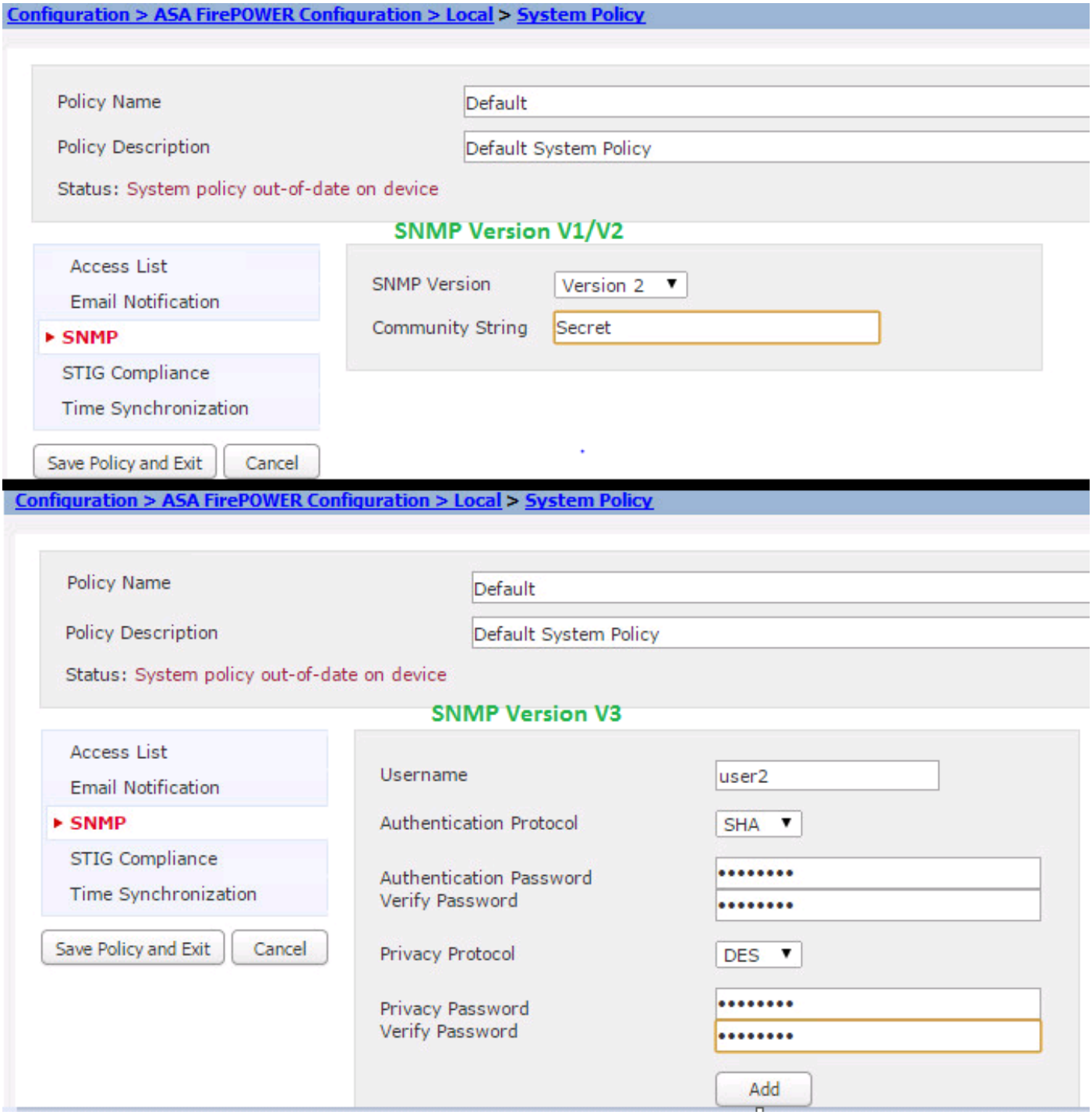
社区字符串： 如果选择在SNMP版本选项的**v1/ v2**，请在社区字符串字段键入SNMP团体名称。

用户名： 如果选择在版本选项的**v3**选项。在用户名字段点击**添加用户时**按钮并且指定**用户名**。

验证： 此选项是SNMP v3配置的部分。它提供根据被切细的消息认证编码的验证使用MD5或SHA算法。选择散列算法的**协议**&输入密码

在**密码字段**。如果不要使用认证功能然后请勿选择选项。

保密性： 此选项是SNMP v3配置的部分。使用DES/AES算法，它提供加密。加密&回车密码的挑选协议在**密码字段**。如果不想要数据加密功能然后请勿选择选项。



Note: (MIB) MIB(DCEALERT.MIB) Firepower(/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