ASA/PIX：转接使用ACS配置示例的VPN客户端的流量核算

目录

简介

本文为占提供一配置示例VPN客户端(IPsec/SSL)使用PIX/ASA以ACS。可适应安全工具能发送记帐信息到关于穿过可适应安全工具的所有TCP或UDP流量的一个RADIUS或TACACS+服务器。如果该流量也验证，则AAA服务器能由用户名维护记帐信息。如果流量没有验证， AAA服务器能由IP地址维护记帐信息。记帐信息包括，当穿过会话、被使用的服务和每会话的持续时间的可适应安全工具的会话开始并且终止，用户名，字节数。

在您能使用此命令前，您必须首先选定一个AAA服务器用**aaa-server命令**。使用核算**模式**in命令aaa-server协议配置模式，除非启用同时核算记帐信息在服务器组中仅发送到活动服务器。

当**aaa accounting包括**并且**排除**命令，您不能使用**AAA记帐匹配**in命令相同的配置。我们建议您使用**match命令**而不是**包括**并且**排除**命令;和**排除**命令ASDM不支持**包括**。

本文假设，远程访问VPN使用与IPSec VPN Client/SSL VPN客户端(Anyconnect)配置的ASA/PIX与验证的ACS已经做并且适当地运作。本文着重如何配置VPN客户端的Aaa accounting ASA有ACS的安全工具的。

参考的Cisco Secure ACS身份验证配置示例的PIX/ASA 7.x和Cisco VPN Client 4.x为了得知更多如何设置Cisco VPN Client (4.x Windows的)和PIX 500系列安全工具7.x之间的一个远程访问虚拟专用网连接使用一思科安全访问控制服务器(ACS版本3.2)扩展认证的。

参考的ASA 8.x ：公共互联网的VPN AnyConnect VPN客户端棍子配置示例的为了得知更多如何设置可适应安全工具(ASA) 8.0.2执行在忠心于的SSL VPN Cisco AnyConnect VPN客户。

先决条件

要求

确保VPN客户端能建立连接和适当地到达端对端。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 5500系列Cisco的ASA运行7.x和以后
- Cisco Secure ACS 4.x

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。

相关产品

本文可能也与有软件版本的7.x Cisco PIX 500系列安全工具一起使用和以后。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

ASA 配置

要配置核算，请执行这些步骤：

1. 如果希望可适应安全工具提供帐户数据每个用户，您必须启用认证。如果希望可适应安全工具提供帐户数据每个IP地址，启用验证不是必要的，并且您能继续到步骤2。
2. 使用**访问列表命令**，请建立识别源地址，并且流量目的地址您希望认为的访问列表。**注意：** 如果配置验证并且想要验证的所有流量的帐户数据，您能使用您创建为了用在**AAA验证匹配**命令上的同一访问列表。
3. 为了启用帐户，输入此命令：`hostname(config)# aaa accounting match acl_name interface_name server_group` Where:*acl_name*参数是在**访问列表命令**设置的访问列表名称。*interface_name*参数是在**nameif命令**设置的接口名称。*server_group*参数是在**aaa-server命令**设置的服务器组组名。**注意：** 或者，您能使用**include命令的aaa accounting** (识别在命令内的流量)，但是您不能在相同的配置里使用两个方法。欲知更多信息，请参阅Cisco ASA 5580自适应安全设备命令参考。

这些命令验证，授权，并且占出站流量：

ASA
`!--- Using the aaa-server command, identify your AAA servers. If you have already !--- identified your AAA servers, continue to the next step.` hostname(config)# **aaa-server AuthOutbound protocol RADIUS** hostname(config-

```
aaa-server-group)# exit !--- Identify the server,
including the AAA server group it belongs to and !---
enter the IP address, Shared key of the AAA Server.
hostname(config)# aaa-server AuthOutbound (inside) host
10.1.1.1 hostname(config-aaa-server-host)# key
TACPlusUauthKey hostname(config-aaa-server-host)# exit
!--- Using the access-list command, create an access
list that identifies the source !--- addresses
anddestination addresses of traffic you want to
authenticate. hostname(config)# access-list TELNET_AUTH
extended permit tcp any any eq telnet !--- Using the
access-list command, create an access list that
identifies the source !--- addresses anddestination
addresses of traffic you want to Authorize and
Accounting. hostname(config)# access-list SERVER_AUTH
extended permit tcp any any !--- configure
authentication, enter this command: hostname(config)#
aaa authentication match TELNET_AUTH inside AuthOutbound
!--- configure authorization, enter this command:
hostname(config)# aaa authorization match SERVER_AUTH
inside AuthOutbound
!--- This command causes the PIX Firewall to send !---
RADIUS accounting packets for RADIUS-authenticated
outbound sessions to the AAA !--- server group named
"AuthOutbound": hostname(config)# aaa accounting match
SERVER_AUTH inside AuthOutbound
```

认为使用ACS配置的RADIUS

记录的属性的CSV记录器记录数据在逗号分离的列()。您能导入此格式到各种各样的第三方应用，例如Microsoft Excel或Microsoft访问。在您导入从CSV文件的数据到这样应用程序后，您可准备图或执行查询，例如确定在给的期限，多少个小时用户登录网络。关于如何使用CSV文件的信息在第三方应用例如Microsoft Excel，请参阅从第三方供应商的文档。

您能访问在ACS服务器硬盘驱动器的CSV文件或您能下载从Web接口的CSV文件。

默认情况下，ACS在对日志是唯一的目录保留日志文件。您能配置CSV日志日志文件位置。所有日志的默认目录位于**sysdrive ：\程序文件\ CiscoSecure ACS vx.x。**

为了配置CiscoSecure ACS执行认为使用CSV的RADIUS，请执行这些步骤：

1. 在导航条，请点击**系统配置**。
2. 点击**记录日志**。操作日志配置页出版。
3. 挑选**CSV RADIUS核算**。
4. 确认**日志到CSV RADIUS认为的报告**复选框选择。如果它没有选择，当前请选择它。
5. 在**记录**表的**挑选属性**，请确保您在RADIUS记帐日志要发现的RADIUS属性在**已登录Attributes列表**出现。除标准RADIUS属性之外，有提供由CiscoSecure ACS，例如真名，ExtDB资讯台和远程被记录的几个特殊记录日志属性。
6. (可选)，如果使用CiscoSecure ACS Windows版服务器，您能指定日志文件文件管理，确定大RADIUS帐户文件如何多久可以是，多少保留，并且他们在哪里存储。
7. 如果做了对RADIUS认为的配置的变动，请单击**提交**。CiscoSecure ACS保存并且实现您做对其RADIUS认为的配置的更改。

这些主题描述如何查看，并且下载ACS CSV报告：

- CSV日志文件名称

- 查看CSV报告
- 下载CSV报告

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

- 思科安全访问控制服务器的4.2用户指南-记录和报告
- Cisco ASA 5500 系列自适应安全设备支持页
- PIX/ASA：使用 TACACS+ 和 RADIUS 服务器的网络访问直通代理配置示例
- 用于 Windows 的 Cisco 安全访问控制服务器
- Cisco PIX 500 系列安全设备
- 技术支持和文档 - Cisco Systems