如何配置Cisco VPN 3000集中器以支持管理帐户的TACACS+认证

目录

简介

本文提供逐步指导为了配置Cisco VPN 3000系列集中器支持管理帐户的TACACS+认证。

当TACACS+服务器在VPN 3000集中器配置，本地配置的帐户名，并且例如admin，设置， isp，等等，不再使用密码。对VPN 3000集中器的所有登录发送到用户和密码验证的已配置的外部TACACS+服务器。

一个权限级别的定义每个用户的TACACS+服务器的确定在VPN 3000集中器的权限每TACACS+用户名的。然后，与AAA访问级别定义在VPN 3000集中器的本地配置的用户名下的匹配。这是重点，因为，当TACACS+服务器定义，在VPN 3000集中器的本地配置的用户名不再有效。但是，他们仍然用于为了只配合从TACACS+服务器的返回的权限级别，与AAA访问级别在该本地用户下。TACACS+用户名然后分配本地配置的VPN 3000集中器用户定义在他们的配置文件下的权限。

例如，详细描述在配置部分， TACACS+用户/组配置归还TACACS+权限级别15。在VPN 3000集中器的管理员部分下，管理员用户也安排其AAA访问级别设置到15。此用户允许修改配置在所有部分下和成读/写文件。由于TACACS+权限级别和AAA访问级别配比， TACACS+用户给在VPN 3000集中器的那些权限。

为例，如果决定用户需要能修改配置，但是不读/写文件，指定他们权限级别12在TACACS+服务器。您能选择一个和15范围的任何编号。然后，在VPN 3000集中器，请选其他本地配置的管理员之一。其次，设置其AAA访问级别到12，并且设置权限在此用户为了能修改配置，但是不对读/写文件

。由于匹配的权限/访问级别，当他们登陆时，用户获得那些权限。

不再使用在VPN 3000集中器的本地配置的用户名。但是，访问权限和AAA访问级别在那些用户中的每一个下用于为了定义特定TACACS+用户获得的权限，当您登陆时。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 保证您有IP连通性到从VPN 3000集中器的TACACS+服务器。如果您的TACACS+服务器是往公共接口，请勿忘记打开TACACS+ (TCP端口49)在公共过滤器。
- 通过控制台保证备份访问是可操作的。偶然地锁定所有用户在配置外面，当您第一组这是容易的。恢复访问的唯一方法是通过控制台，仍然使用本地配置的用户名和密码。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 3000集中器软件版本4.7.2.B (二者择一，任何版本3.0和以后OS软件工作。)
- 用于Windows的思科安全访问控制服务器服务器版本4.0 (另一方面，任何版本2.4和以后软件工作。)

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。

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TACACS+服务器

添加VPN 3000集中器的条目在TACACS+服务器

完成这些步骤为了添加VPN 3000集中器的一个条目在TACACS+服务器。

1. 点击**网络配置**在左面板中。在 AAA Clients 下，单击 **Add Entry**。
2. 在下一个窗口上，请填好表添加VPN集中器作为TACACS+客户端。此示例使用：AAA客户端主机名= **VPN3000**AAA客户端IP地址= **10.1.1.2**密钥= **csacs123**验证使用= **TACACS+ (Cisco IOS)**单击 **Submit+ Restart**。

添加在TACACS+服务器的用户帐户

完成这些步骤为了添加在TACACS+服务器的一个用户帐户。

1. 创建在可以以后使用TACACS+认证的TACACS+服务器的一个用户帐户。点击**用户设置**在左面板中，添加用户时“johnsmith”并且单击**添加/编辑**为了执行此。

2. 添加此用户的一个密码，并且分配用户到包含其他VPN 3000集中器管理员的ACS组。**注意**：此示例定义了权限级别在此特定用户ACS组配置文件下。如果这将逐个用户执行，请选择**Interface Configuration > TACACS+ (Cisco IOS)**并且检查**用户**方框Shell (exec)服务。那时是在本文联机描述的TACACS+选项在每用户配置文件下。

编辑TACACS+服务器的组

完成这些步骤编辑TACACS+服务器的组。

1. 点击**组建立**在左面板中。
2. 从下拉菜单，请选择用户被添加到在添加在TACACS+服务器部分的一个用户帐户，是在本例中的Group1的组，并且单击**编辑设置**。
3. 在下一个窗口上，请确保这些属性选择在TACACS+设置下：**Shell (exec)Privilege level=15**一旦完成，请点击**Submit+Restart**。

配置VPN 3000集中器

添加TACACS+服务器的条目在VPN 3000集中器

完成这些步骤为了添加TACACS+服务器的一个条目在VPN 3000集中器。

1. 选择在导航结构树的**Administration > Access Rights > AAA Servers > Authentication**在左面板中，然后单击在右侧面板中**添加**。当您单击请**添加**为了添加此服务器，本地在VPN 3000集中器的已配置的用户名/密码不再使用。通过控制台工作保证备份访问在停工的情况下。
2. 在下一个窗口上，请填好表格如被看到此处：认证服务器= **10.1.1.1** (TACACS+服务器的IP地址)服务器端口= **0** (默认)Timeout= **4**重试次数= **2**服务器秘密= **csacs123**验证= **csacs123**

修改在VPN集中器的管理帐户TACACS+认证的

完成这些步骤修改在VPN集中器的管理帐户TACACS+认证的。

1. 点击用户的admin**修改**为了修改此用户属性。
2. 选择AAA访问级别作为**15**。此值可以是一个和15范围的任何编号。注意它必须匹配TACACS+权限级别定义在TACACS+服务器的用户/组配置文件下。TACACS+用户然后拾起权限定义在配置的修改的此VPN 3000集中器用户下，读/文字文件，等等。

验证

当前没有可用于此配置的验证过程。

故障排除

完成在这些说明的步骤为了排除故障您的配置。

1. 为了测试验证：TACACS+服务器选择**Administration > Access Rights > AAA Servers > Authentication**。选择您的服务器，然后单击**测验**。**注意**：当TACACS+服务器在管理选项卡

配置，没有办法设置用户验证在VPN3000本地数据库。使用另一个外部数据库或TACACS服务器，您能仅fallback。输入TACACS+用户名和密码并且点击OK键。成功认证出现。

2. 如果它失败，有配置问题或IP连通性问题。检查ACS服务器上的Failed Attempts日志与失败相关的消息。如果消息在此日志没出现那么很可能有IP连通性问题。TACACS+请求不到达TACACS+服务器。验证过滤器应用对适当的VPN 3000集中器接口里里外外允许TACACS+(TCP端口49)数据包。如果失败显示作为在日志拒绝的服务， Shell (exec)服务未正确地然后启用在用户或组配置文件下在TACACS+服务器。
3. 如果测验验证是成功的，但是对VPN 3000集中器的登录继续发生故障，请通过控制台端口检查可过滤事件日志。如果看到一个相似的消息：
   65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2 User [johnsmith] Protocol [HTTP] attempted ADMIN logon. Status: <REFUSED> authorization failure. NO Admin Rights 此消息指示在TACACS+服务器分配的权限级别没有匹配的AAA访问级别在任何VPN 3000集中器用户下。例如，用户johnsmith有一个TACACS+权限级别7在TACACS+服务器，但是五个VPN 3000集中器管理员都没有一个AAA访问级别7。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 3000 系列客户端支持页
- IPsec 协商/IKE 协议支持页
- TACACS/TACACS+支持页面
- IOS 文档中的 TACACS+
- 技术支持和文档 - Cisco Systems