使用 RADIUS 服务器将用户锁定到 VPN 3000 集中器组

目录

简介

Cisco VPN 3000集中器有能力锁定用户到改写组用户在Cisco VPN 3000客户端配置的集中器组。这样，访问限制可以应用对在有保证的VPN集中器配置的多种组用户锁定到该组用RADIUS服务器。

本文详细信息如何设置在Cisco Secure ACS for Windows的此UNIX的(CSUnix)功能和Cisco Secure。

在VPN集中器的配置类似于标准配置。能力锁定用户到在VPN集中器定义的组通过定义在RADIUS用户配置文件的回归属性启用。此属性包含管理员希望用户锁定的VPN集中器组名。此属性是类别属性(IETF RADIUS属性第25)，并且必须返回到在此格式的VPN集中器：

```
OU=groupname;
```

那里*组名*是组的名称用户锁定的VPN集中器的。*OU*必须用大写字母是，并且必须有分号在末端。

在本例中， VPN客户端软件被分配给有现有连接配置文件的所有用户使用*组名*“大家”和密码“任何”。每个用户有一个分离用户名/密码(在本例中，用户名/密码是TEST/TEST)。当用户名被发送到RADIUS服务器时， RADIUS服务器发送在关于*实时组的*信息下用户将。在示例中，它是“filtergroup”。

通过该执行，您能完全控制在RADIUS服务器的组分配透明对用户。如果RADIUS服务器不分配组到用户，用户在“大家”保持组。因为“大家”组有非常限制性过滤器，用户不能通过任何流量。如果RADIUS服务器分配组到用户，用户继承属性，包括限制较少过滤器，特定给组。在本例中，您应用过滤器给组“filtergroup”在VPN集中器允许所有流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

注意： 这成功也测试与ACS 3.3， VPN集中器4.1.7和VPN客户端4.0.5。

- Cisco VPN 3000集中器系列版本4.0(1)Rel
- Cisco VPN客户端软件版本4.0(1)Rel
- Cisco Secure ACS for Windows版本2.4到3.2
- UNIX版本的2.3， 2.5和2.6 Cisco Secure

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Cisco VPN 3000集中器

注意： 此配置假设， VPN集中器已经设置IP地址，默认网关，地址池，等等。用户一定能在继续前本地验证。如果那不工作，则这些更改不会工作。

1. 在**Configuration > System > Servers > Authentication下**，请添加RADIUS服务器的IP地址。
2. 一旦添加了服务器，请使用**Test按钮**验证您能成功验证用户。如果这不工作，组锁定不工作。
3. 定义丢包访问对一切在内部网络的过滤器。这应用分组“大家”，以便，即使用户在它能验证到此组和逗留，他们仍然不能访问任何东西。
4. 在**Configuration > Policy Management > Traffic Management > Rules下**，请增加呼叫**丢弃的**一个规则**全部**并且留下一切在默认。
5. 在**Configuration > Policy Management > Traffic Management > Filters下**，请创建呼叫**丢弃的**过滤器**全部**，留下一切在默认，并且添加丢弃所有规则到它。
6. 在**Configuration > User Management > Groups下请**添加一组呼叫**大家**。这是所有用户在VPN客户端预先了配置的组。他们最初验证到此组，然后锁定到一不同的组在用户认证以后。通常定义组。确保您添加丢弃所有过滤器(您创建)在常规选项卡下。为了使用RADIUS验证用户在此组中，请设置组类型(在Identity选项下)是**内部**和验证(在IPSec选项下)对**RADIUS**。确保组功能没有被检查此组的洛克。**注意：** 即使您不定义了丢弃所有过滤器，请确保那里是定义的至少一个过滤器此处。
7. 定义用户的最终目的地组(示例是“filtergroup”)，应用过滤器。**注意：** 您必须定义过滤器此处。如果不要阻塞这些用户的任何流量，请创建“允许所有”过滤器并且运用“其中任一在”，并且“其中任一”排除对它。您必须定义过滤器某亲切为了通过流量。为了使用RADIUS验证用户在此组中，请设置组类型(在Identity选项下)是**内部**和验证(在IPSec选项下)对**RADIUS**。确保组功能没有被检查此组的洛克。

配置 RADIUS 服务器

Cisco Secure ACS for Windows

这些步骤设置您的Cisco Secure ACS for Windows RADIUS服务器锁定用户到在VPN集中器配置的特定组。记住在RADIUS服务器定义的组与在VPN集中器定义的组无关。您能使用RADIUS服务器的组使管理您的用户更加容易。名称不必须匹配什么在VPN集中器配置。

1. 添加VPN集中器作为一个网络接入服务器(NAS)在RADIUS服务器在Network Configuration部分下。添加VPN集中器的IP地址在NAS IP地址框的。添加您在钥匙箱的VPN集中器定义前的同一密钥。从验证使用下拉菜单，请选择**RADIUS (IETF)**。单击 **Submit+ Restart**。
2. 在接口配置下，挑选**RADIUS (IETF)**和确保属性**25 (中集集团)**被检查。这允许您在组/用户配置中更改它。
3. 添加用户。在本例中，用户呼叫“TEST”。此用户可以是在任何Cisco Secure ACS for Windows组中。除在属性25下之外告诉VPN集中器什么的通过组使用用户，那里是Cisco Secure ACS for Windows组和VPN集中器组之间的没有相关性。此用户在"Group_1."安置
4. 在组建立下，请编辑在组的设置(在我们的示例，这是"Group_1")。
5. 点击绿色**IETF RADIUS**按钮把您带到适当的属性。
6. 移下来和修改团体25。
7. 添加属性如显示此处。替代组名您要锁定用户到filtergroup的。确保OU用大写字母是，并且那那里是分号在组名以后。
8. 单击 **Submit+ Restart**。

UNIX的Cisco Secure

这些步骤设置您的Cisco Secure UNIX RADIUS服务器锁定用户到在VPN集中器配置的特定组。记住在RADIUS服务器定义的组与在VPN集中器定义的组无关。您能使用RADIUS服务器的组使管理您的用户更加容易。名称不必须匹配什么在VPN集中器配置。

1. 添加VPN集中器作为在RADIUS服务器的NAS在Advanced部分下。选择允许作为回复属性25将发送的属性的字典。例如， IETF或Ascend。
2. 添加用户。在本例中，用户是“TEST”。此用户可以是在任何Cisco Secure UNIX组或没有组中。除在属性25下之外告诉VPN集中器什么的通过组使用用户，那里是Cisco Secure UNIX组和VPN集中器组之间的没有相关性。
3. 在用户/组配置文件下，请定义RADIUS (IETF)返回属性。
4. 添加类别属性，属性编号**25**，并且做其值**OU=filtergroup;**。用filtergroup替代在VPN集中器定义的组。**注意：** 在Cisco Secure UNIX中，请定义引号包围的属性。当属性发送到VPN集中器时，他们剥离。用户/组配置文件应该看起来类似于此。
5. 单击**提交**保存每个条目。已完成Cisco Secure UNIX条目看起来与此输出相似：#

```
./ViewProfile -p 9900 -u NAS.172.18.124.132
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}
```

```
# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

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

- VPN 3000 集中器上的 Cisco VPN 3000 客户端用户与组属性处理
- RADIUS (远程拨入用户验证服务)技术支持页
- Cisco VPN 3000系列集中器支持页面
- Cisco VPN 3000 客户端支持页
- IP安全协议(IPSec)产品支持页
- 请求注解 (RFC)
- Cisco Secure ACS for Windows产品支持页
- 安全产品问题信息通告(Field Notice)
- 用于UNIX的Cisco Secure ACS产品支持页
- 技术支持 - Cisco Systems