在VPN 3000集中器上的Cisco VPN客户端用户和组属性处理

目录

简介

本文档介绍如何在VPN集中器上对Cisco VPN客户端进行身份验证，以及Cisco VPN 3000集中器如何使用用户和组属性。

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Cisco VPN 3000集中器。

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

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

VPN客户端连接到VPN 3000集中器

当VPN客户端连接到VPN 3000集中器时，最多可进行四次身份验证。

1. 组已通过身份验证。（这通常称为“隧道组”。）
2. 用户已通过身份验证。
3. （可选）如果用户是另一组的一部分，则此组接下来进行身份验证。如果用户不属于另一个组或隧道组，则用户默认为基本组，并且不会执行此步骤。
4. 第1步中的“隧道组”再次进行身份验证。(在使用“组锁定”功能时执行此操作。此功能在2.1版或更高版本中可用。)

这是您在事件日志中看到的事件示例，该事件用于通过内部数据库进行身份验证的VPN客户端（“testuser”是组“工程”的一部分）。

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

注：要查看这些事件，您必须在配置> 系统 > 事件 > 类中配置严重性为1-6的身份验证事件类。

组锁定功能 — 如果在Group - Tunnel_Group上启用了组锁定功能，则用户必须是Tunnel_Group的一部分才能连接。在上一个示例中，您看到所有相同的事件，但“testuser”不连接，因为它们是“组 — 工程”的一部分，而不是“组 — 隧道组”的一部分。您还会看到以下事件：

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

有关组锁定功能和配置示例的其他信息，请参阅使用RADIUS服务器将用户锁定到VPN 3000集中器组。

通过RADIUS对组和用户进行外部身份验证

VPN 3000集中器也可配置为通过RADIUS服务器对外部用户和组进行身份验证。这仍要求在VPN集中器上配置组的名称，但组类型配置为“外部”。

- 如果RADIUS服务器支持供应商特定属性(VSA)，则外部组可以返回Cisco/Altiga属性。
- RADIUS未返回的任何思科/Altiga属性都默认为基本组中的值。
- 如果RADIUS服务器不支持VSA，则ALL属性默认为Base Group属性。

注意：RADIUS服务器对组名称的处理与用户名无异。RADIUS服务器上的组配置与标准用户一样。

这些步骤概述了当IPSec客户端连接到VPN 3000集中器时，如果用户和组都通过外部身份验证，会发生什么情况。类似于内部案例，最多可进行四次身份验证。

1. 组通过RADIUS进行身份验证。RADIUS服务器可以返回组的许多属性，也可以不返回任何属性。至少，RADIUS服务器需要返回Cisco/Altiga属性“IPSec Authentication = RADIUS”，以告知VPN集中器如何对用户进行身份验证。否则，需要将基本组的IPSec身份验证方法设置为“RADIUS”。
2. 用户通过RADIUS进行身份验证。RADIUS服务器可以返回用户的许多属性，也可以不返回任何属性。如果RADIUS服务器返回属性CLASS(标准RADIUS属性#25)，则VPN 3000集中器将该属性用作组名称并移至步骤3，否则将转至步骤4。

3. 用户组接下来通过RADIUS进行身份验证。RADIUS服务器可以返回组的许多属性，也可以不返回任何属性。
4. 步骤1中的“隧道组”通过RADIUS再次进行身份验证。身份验证子系统必须再次对隧道组进行身份验证，因为它尚未存储步骤1中身份验证的属性（如果有）。在使用“组锁定”功能时，会执行此操作。

VPN 3000 集中器如何使用用户和组属性

在VPN 3000集中器对用户和组进行身份验证后，它必须组织它已接收的属性。VPN集中器按照此首选项顺序使用属性。身份验证是在内部还是在外部完成并不重要：

1. **用户属**性 — 这些优先于所有其他属性。
2. **组属**性 — “用户”属性中缺少的任何属性都由“组”属性填充。相同的任何属性都会被用户属性覆盖。
3. **隧道组属**性 — “用户”或“组”属性中缺少的任何属性都由“隧道组”属性填充。相同的任何属性都会被用户属性覆盖。
4. **基本组属**性 — “用户”、“组”或“隧道组”属性中缺少的任何属性都由基本组属性填充。

相关信息

- Cisco VPN 3000 系列集中器支持页
- Cisco VPN 客户端支持页
- IPSec 支持页面
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持 - Cisco Systems