PIX/ASA作为有扩展认证的远程VPN服务器使用CLI和ASDM配置示例

目录

简介

本文档介绍如何使用自适应安全设备管理器 (ASDM) 或 CLI 将 Cisco 5500 系列自适应安全设备 (ASA) 配置为充当远程 VPN Server。ASDM 通过一个直观且易于使用的基于 Web 的管理界面提供一流的安全管理和监控。完成 Cisco ASA 配置后，可以使用 Cisco VPN 客户端对其进行验证。

要在 Cisco VPN 客户端（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Windows 2003 IAS RADIUS（针对 Active Directory）进行身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。远程 VPN 客户端用户使用 Microsoft Windows 2003 Internet 身份验证服务 (IAS) RADIUS 服务器根据 Active Directory 进行身份验证。

要使用 Cisco 安全访问控制服务器 (ACS 版本 3.2) 进行扩展身份验证 (Xauth) 以在 Cisco VPN 客户端（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Cisco 安全 ACS 身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。

先决条件

要求

本文档假设 ASA 处于完全运行状态，并配置为允许 Cisco ASDM 或 CLI 进行配置更改。

注意： 请参阅允许对 ASDM 进行 HTTPS 访问或 PIX/ASA 7.x：内部和外部接口上的 SSH 配置示例以允许通过 ASDM 或Secure Shell (SSH) 远程对设备进行配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备软件版本 7.x 及更高版本
- 自适应安全设备管理器版本 5.x 及更高版本
- Cisco VPN 客户端 4.x 及更高版本

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

此配置也可用于 Cisco PIX 安全设备版本 7.x 及更高版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

远程访问配置提供对 Cisco VPN 客户端（如移动用户）的安全远程访问。远程访问 VPN 使远程用户可以安全地访问集中的网络资源。Cisco VPN 客户端遵守 IPSec 协议并专门设计为可与安全设备配合使用。但是，安全设备可以与许多协议兼容客户端建立 IPSec 连接。有关 IPSec 的详细信息，请参阅 ASA 配置指南。

组和用户是 VPN 安全管理和安全设备配置中的核心概念。它们指定确定用户访问和使用 VPN 的属性。组是被视为单个实体的用户集合。用户从组策略获得他们的属性。隧道组标识特定连接的组策略。如果不为用户分配特定组策略，则应用连接的默认组策略。

隧道组由确定隧道连接策略的一组记录构成。这些记录标识了用来对隧道用户进行身份验证的服务器，以及向其发送连接信息的记账服务器（如果有）。它们还标识连接的默认组策略，并且它们包含协议特定的连接参数。隧道组包括与隧道自身创建相关的少量属性。隧道组包括指向定义面向用户的属性的组策略的一个指针。

注意： 在本文档的示例配置中，使用本地用户帐户进行身份验证。如果希望使用其他服务，如 LDAP 和 RADIUS，请参阅配置用于授权和身份验证的外部 RADIUS 服务器。

Internet 安全连接和密钥管理协议 (ISAKMP)（也称为 IKE）是主机对如何就建立 IPSec 安全连接达成协议的协商协议。每个 ISAKMP 协商分为两个部分，第 1 阶段和第 2 阶段。第 1 阶段创建用于保护后来 ISAKMP 协商消息的第一条隧道。第 2 阶段创建用于保护通过安全连接传输的数据的隧道。有关 ISAKMP 的详细信息，请参阅 CLI 命令的 ISAKMP 策略关键字。

配置

使用 ASDM 将 ASA/PIX 配置为远程 VPN Server

要使用 ASDM 将 Cisco ASA 配置为远程 VPN Server，请完成以下步骤：

1. 从主窗口中选择 **Wizards > VPN Wizard**。
2. 选择 **Remote Access VPN** 隧道类型，并确保按照要求设置 VPN 隧道接口。
3. 已选择了唯一的可用 VPN 客户端类型。单击 **Next**。
4. 为“Tunnel Group Name”输入名称。提供要使用的身份验证信息。本示例中选择了 **Pre-shared Key**。**注意：** ASDM 上没有用来隐藏/加密预共享密钥的方法。原因是 ASDM 应该只由配置 ASA 的人员或帮助客户进行此配置的人员使用。
5. 选择是希望使用本地用户数据库对远程用户进行身份验证，还是希望使用外部 AAA 服务器组对远程用户进行身份验证。**注意：** 您将在步骤 6 中将用户添加到本地用户数据库中。**注意：** 有关如何通过 ASDM 配置外部 AAA 服务器组的信息，请参阅 PIX/ASA 7.x 通过 ASDM 为 VPN 用户配置身份验证和授权服务器组的配置示例。
6. 如果需要，将用户添加到本地数据库中。**注意：** 请不要从此窗口中删除现有用户。在 ASDM 主窗口中选择 **Configuration > Device Administration > Administration > User Accounts**，以编辑数据库中的现有条目或将这些条目从数据库中删除。
7. 定义一个要在远程 VPN 客户端进行连接时动态分配给它们的本地地址池。
8. ***可选：***指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。
9. 为 IKE 指定参数，也称为 IKE 第 1 阶段。隧道两端的配置必须完全一致。但 Cisco VPN 客户端会自动为自己选择正确的配置。因此，无需在客户端 PC 上执行 IKE 配置。
10. 为 IPSec 指定参数，也称为 IKE 第 2 阶段。隧道两端的配置必须完全一致。但 Cisco VPN 客户端会自动为自己选择正确的配置。因此，无需在客户端 PC 上执行 IKE 配置。
11. 指定哪些内部主机或网络（如果有）应向远程 VPN 用户公开。如果将此列表留空，则将允许远程 VPN 用户访问 ASA 的整个内部网络。您还可以在此窗口上启用分割隧道。分割隧道对发往本过程中前面所定义的资源的数据流进行加密，并通过不以隧道形式传输该数据流提供对整个 Internet 的未加密访问。如果*未*启用分割隧道，则来自远程 VPN 用户的所有数据流将通过隧道传输到 ASA。这可能导致很高的带宽和处理器使用率，具体取决于您的配置。
12. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。

使用 CLI 将 ASA/PIX 配置为远程 VPN Server

完成以下步骤以通过命令行配置远程 VPN 接入服务器。有关所使用的每个命令的详细信息，请参阅配置远程接入 VPN 或 Cisco ASA 5500 系列自适应安全设备命令参考。

1. 在全局配置模式下输入 **ip local pool** 命令以配置要用于 VPN 远程接入隧道的 IP 地址池。要删除地址池，请输入此命令的 no 形式。安全设备使用基于隧道组的地址池进行连接。如果为一个隧道组配置多个地址池，安全设备将按配置这些地址池的顺序使用它们。发出此命令以创建可用于向远程访问 VPN 客户端分配动态地址的本地地址池：`ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`
2. 发出以下命令：`ASA-AIP-CLI(config)#username marty password 12345678`
3. 发出此组命令以配置特定隧道：ASA-AIP-CLI(config)#isakmp **policy 1 authentication pre-share**ASA-AIP-CLI(config)#isakmp **policy 1 encryption 3des**ASA-AIP-CLI(config)#isakmp **policy 1 hash sha**ASA-AIP-CLI(config)#isakmp **policy 1 group 2**ASA-AIP-CLI(config)#isakmp **policy 1 lifetime 43200**ASA-AIP-CLI(config)#isakmp **enable outside**ASA-AIP-CLI(config)#crypto **ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)#crypto dynamic-map **outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)-crypto dynamic-map **outside_dyn_map 10 set reverse-route**ASA-AIP-CLI(config)#crypto dynamic-map **outside_dyn_map 10 set security-association lifetime seconds 288000**ASA-AIP-CLI(config)-crypto**地图outside_map 10 ipsec-isakmp动态**

outside_dyn_mapASA-AIP-CLI(config)#crypto **map outside_map interface outside**ASA-AIP-CLI(config)#crypto **isakmp nat-traversal**

4. ***可选：***如果希望连接绕过已应用于接口的访问列表，请发出此命令：ASA-AIP-CLI(config)#**sysopt connection permit-ipsec** **注意：** 此命令对 7.2(2) 之前的 7.x 映像有效。如果使用映像 7.2(2)，请发出 ASA-AIP-CLI(config)#sysopt connection permit-vpn 命令。
5. 发出以下命令：ASA-AIP-CLI(config)#**group-policy hillvalleyvpn internal**
6. 发出以下命令以配置客户端连接设置：ASA-AIP-CLI(config)#group-policy hillvalleyvpn **attributes**ASA-AIP-CLI(config)#(config-group-policy)#dns-server **value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#vpn-tunnel-protocol **IPSec**ASA-AIP-CLI(config)#(config-group-policy)#default-domain **value test.com**
7. 发出以下命令：ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**
8. 发出以下命令：ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**
9. 发出以下命令：ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**
10. 发出以下命令：ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**
11. 发出此命令以使用本地用户数据库进行身份验证。ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**
12. 将组策略与隧道组关联ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**
13. 在 hillvalleyvpn 隧道组的常规属性模式下发出此命令，以将步骤 1 中创建的 vpnpool 分配给 hillvalleyvpn 组。ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

在 ASA 设备上运行配置

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASAwAIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif outside security-level 0 ip
address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name
corp.com pager lines 24 mtu outside 1500 mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal group-policy
hillvalleyvpn1 attributes dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac crypto dynamic-map outside_dyn_map 10
set transform-set ESP-3DES-SHA crypto dynamic-map
outside_dyn_map 10 set security-association lifetime
seconds 288000 crypto map outside_map 10 ipsec-isakmp
dynamic outside_dyn_map crypto map outside_map interface
outside crypto isakmp enable outside crypto isakmp
policy 10 authentication pre-share encryption 3des hash
sha group 2 lifetime 86400 crypto isakmp nat-traversal
20 tunnel-group hillvalleyvpn type ipsec-ra tunnel-group
```

```
hillvalleyvpn general-attributes address-pool vpnpool
default-group-policy hillvalleyvpn tunnel-group
hillvalleyvpn ipsec-attributes pre-shared-key * telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192 : end
ASA-AIP-CLI(config)#
```

Cisco VPN 客户端口令存储配置

如果您有许多 Cisco VPN 客户端，是很难记住所有 VPN 客户端的用户名和口令的。要将口令存储在 VPN 客户端计算机中，请如本部分中所述配置 ASA/PIX 和 VPN 客户端。

ASA/PIX

在全局配置模式下使用 **group-policy attributes** 命令：

```
group-policy VPNusers attributes password-storage enable
```

Cisco VPN 客户端

编辑 **.pcf 文件**并修改以下参数：

```
SaveUserPassword=1 UserPassword= <type your password>
```

禁用扩展身份验证

在隧道组模式下，输入此命令以禁用 PIX/ASA 7.x 上在默认情况下处于启用状态的扩展身份验证：

```
asa(config)#tunnel-group client ipsec-attributes asa(config-tunnel-ipsec)#isakmp ikev1-user-
authentication none
```

禁用扩展身份验证后，VPN 客户端不会弹出用户名/口令以进行身份验证 (Xauth)。因此，ASA/PIX 不需要配置用户名和口令以对 VPN 客户端进行身份验证。

验证

尝试使用 Cisco VPN 客户端连接到 Cisco ASA 以验证是否成功配置了 ASA。

1. 选择 **Connection Entries > New**。
2. 填写新连接的详细信息。“Host”字段应包含以前配置的 Cisco ASA 的 IP 地址或主机名。组身份验证信息应与步骤 4 中使用的组身份验证信息对应。完成后单击 **Save**。
3. 选择新创建的连接，然后单击 **Connect**。
4. 输入用于扩展身份验证的用户名和口令。此信息应与在步骤 5 和步骤 6 中指定的信息一致。
5. 成功建立连接后，从“Status”菜单中选择 **Statistics** 以验证隧道的详细信息。此窗口显示数据流和加密信息：此窗口显示分割隧道信息：

故障排除

使用本部分可排除配置故障。

不正确的加密 ACL

已知 ASDM 5.0(2) 会创建并应用一个加密访问控制列表 (ACL)，该加密访问控制列表可能导致使用分割隧道的 VPN 客户端和处于网络扩展模式的硬件客户端出现问题。使用 ASDM 版本 5.0(4.3) 或更高版本可避免此问题。有关详细信息，请参阅 Cisco Bug ID CSCsc10806（仅限注册用户）。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- Cisco ASA 5500 系列自适应安全设备故障排除和警报
- 技术支持和文档 - Cisco Systems