EAP-FAST版本1.02配置指南

目录

简介

本文为扩展验证灵活协议验证提供一配置示例通过获取建立隧道(EAP-FAST)版本1.02。

先决条件

要求

在尝试此配置前，请保证您符合这些要求：

- 与固件版本5.40和驱动版本8.5 (是CB21AG的客户端的IOS AP 12.2(13)JA3， 350或者CB20A客户端支持的2H CY2004)
- 访问控制服务器(ACS) 3.2.3， Windows 2000或者XP与已安装的ACU 6.3。

使用的组件

本文档不限于特定的软件和硬件版本。

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。

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

在 ACS 上设置 AP

完成这些步骤设置在ACS的接入点(AP) ：

1. 在 ACS 服务器上，单击左侧的 **Network Configuration**。
2. 要添加AAA客户端可以，单击**添加条目**。
3. 在框中输入以下值：AAA客户端IP地址- IP_of_your_AP关键字-组成密钥(请确定关键字符合AP共有的密钥)认证使用- RADIUS (Cisco Aironet)
4. 单击 **submit**。
5. 重新启动 。

设置EAP-FAST的ACS

完成这些步骤设置EAP-FAST的ACS ：

1. 选择**系统配置>全局验证设置**。
2. 检查**允许EAP-FAST**方框。
3. 输入在info字段权限的ID的一个值(不支持空间)。
4. 检查**设置**方框的**允许自动PAC。注意：** 自动PAC设置是提供客户端一个低顶上的方法PAC带内。有一些个警告对自动供应：自动供应要求最初的EAP-FAST验证发生故障。LDAP用户不自动调配的，并且必须手工设置。自动供应是易受MITM攻击在初始设置期间。
5. 检查**EAP-FAST重要的服务器**方框。
6. 单击 **submit**。
7. 重新启动 。

配置 AP

完成这些步骤配置AP ：

1. 选择**安全>Server经理**。
2. 从当前服务器列表下拉列表，请选择RADIUS。
3. 输入ACS IP地址。
4. 输入共享机密(必须匹配在ACS的密钥)。
5. 单击 **Apply**。
6. 从EAP验证下拉列表，请选择RADIUS服务器的IP地址。
7. 单击 **Apply**。

加密管理器(仅WEP加密)

完成仅WEP加密的这些步骤：

1. 选择 **Security > Encryption Manager**。
2. 点击**WEP加密**单选按钮。
3. 从下拉列表，请选择必须。
4. 点击**加密密钥1**单选按钮。
5. 输入密钥。
6. 从密钥大小下拉列表，请选择128。
7. 单击 **Apply**。

加密管理器(WPA密钥管理)

完成WPA密钥管理的这些步骤：

1. 选择 **Security > Encryption Manager**。
2. 点击**密码器**单选按钮。
3. 从下拉列表，请选择TKIP。
4. 单击 **Apply**。

SSID管理器(仅WEP加密)

完成仅WEP加密的这些步骤：

1. 从当前SSID列表选择SSID或者进入在SSID字段的一新的SSID。
2. 检查**开放式验证**方框。
3. 从下拉列表，请选择与EAP。
4. 检查**网络EAP**方框。
5. 单击 **Apply**。

SSID管理器(WPA密钥管理)

完成WPA密钥管理的这些步骤：

1. 从当前SSID列表选择SSID或者进入在SSID字段的一新的SSID。
2. 检查**开放式验证**方框。
3. 从下拉列表，请选择与EAP。
4. 检查**网络EAP**方框。
5. 选择验证密钥管理。
6. 从下拉列表，请选择必须。
7. 检查**WPA**方框。
8. 单击 **Apply**。

设置EAP-FAST的客户端

仅WEP加密

完成仅WEP加密的这些步骤：

1. 打开 ACU。

2. 选择管理配置文件。
3. 创建配置文件(或请编辑一)。
4. 进入AP的客户端名称和SSID。
5. 点击**Network Security选项**。
6. 选择EAP-FAST。
7. 单击 **Configure**。
8. 检查**设置允许自动的PAC此配置文件**方框。**注意：** 自动PAC设置是提供客户端一个低顶上的方法PAC带内。有一些个警告对自动供应：自动供应要求最初的EAP-FAST验证发生故障。LDAP用户不自动调配的，并且必须手工设置。自动供应是易受MITM攻击在初始设置期间。
9. 单击 **Ok**。
10. 单击 **Ok**。
11. 单击 **Ok**。
12. 选择您创建的配置文件。

WPA密钥管理

完成WPA密钥管理的这些步骤：

1. 打开 ACU。
2. 选择管理配置文件。
3. 创建配置文件(或请编辑一)。
4. 进入AP的客户端名称和SSID。
5. 点击**Network Security选项**。
6. 检查**WiFi受保护的访问(WPA)**方框。
7. 对于网络安全类型，请选择EAP-FAST (WPA)。
8. 单击 **Configure**。
9. 检查**设置允许自动的PAC此配置文件**方框。**注意：** 自动PAC设置是提供客户端一个低顶上的方法PAC带内。有一些个警告对自动供应：自动供应要求最初的EAP-FAST验证发生故障。LDAP用户不自动调配的，并且必须手工设置。自动供应是易受MITM攻击在初始设置期间。
10. 单击 **Ok**。
11. 单击 **Ok**。
12. 单击 **Ok**。
13. 选择您创建的配置文件。

设置补充的手工的PAC

此部分包括从为配置手工PAC设置已经提交的那些变化的步骤。

注意： 选项**EAP-FAST PAC文件生成不**是可用的在ACS为windows，并且必须手工执行步骤使用在此部分定义的步骤。

设置EAP-FAST的ACS选项

这些步骤可选。如果希望一些客户端使用自动供应，请留给此选项被检查。

1. 选择**系统配置>全局验证设置**。
2. 不选定**设置**方框的**允许自动PAC**。

使用CSUtil.exe，创建PAC

此步骤能根据您的需求非常地变化。参考Cisco Secure ACS for Windows服务器的3.2用户指南欲知更多信息。

剪切的PAC基本语法与CSUtil.exe是：

```
csutil [-t] [-filepath <full filepath>] [-passwd <password>] [[-a] [-g <group number>] [-u <user name>] [-f <full filepath>]]
```

-可选并且指定输出的目录(目录必须已经存在)。如果未指定， PACs在安置能获得杂乱的ACS使用情况目录(如果创建很多PACs)。

-可选并且指定密码保护PAC。如果未指定，那里是没有默认密码。

有效PAC创建一些示例发出命令的这些区域：

- **csutil - t -文件路径c:\acspac -密码5p0rk5 - f c:\acspac\pac.txt** —创建在文件列出的用户的PAC名为pac.txt。
- **csutil - t -文件路径c:\acspac -密码5p0rk5 - g 0** —创建用户的PAC在ACS组0中。
- **csutil - t -文件路径c:\acspac -密码5p0rk5 - u vadablam** —创建用户名vadablam的PAC在ACS。
- **csutil - t -文件路径c:\acspac -密码5p0rk5 - a** —创建*所有*用户的PAC ACS的(这能相当一会儿采取)。

为了便于测试完成这些步骤创建单个用户的PAC ：

1. 创建目录输出PAC对(可选)。
2. 验证用户在ACS存在。
3. 打开命令提示框。
4. 导航对ACS使用情况目录。
5. 输入**csutil -t -filepath <filepath> -passwd <password> -u <user>命令**。
6. 复制新的.pac文件对客户主机。

完成这些步骤配置手工PAC设置的客户端：

1. 在选择EAP-FAST以后作为您的网络安全请输入ACU，单击**配置**。
2. 不选定**设置为此配置文件**方框的**允许自动PAC**。
3. 单击 **Import**。
4. 浏览对.pac。
5. 选择.pac。
6. 输入密码(如果提示)。
7. 单击 **Ok**。
8. 单击 **Ok**。
9. 单击 **Ok**。
10. 单击 **Ok**。
11. 选择您创建的配置文件。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

有关详细信息，请参阅以下文档：

- INFO ：错误代码在Windows NT第1部分2中(条款I)
- 如何对错误代码在Windows NT第2部分2中

相关信息

- Cisco Secure ACS for Windows 支持页
- Cisco Secure ACS for UNIX 支持页
- 技术支持和文档 - Cisco Systems