NP、无线局域网控制器和无线网络配置示例

目录

简介

本文为Protected Extensible Authentication Protocol (PEAP)提供一配置示例微软询问握手认证协议在Cisco Unified无线网络的版本2验证Microsoft网络策略服务器(NP)作为RADIUS服务器。

先决条件

要求

保证您熟悉这些步骤，在您尝试此配置前：

- 基本Windows 2008年安装知识
- 思科控制器安装知识

保证这些需求符合了，在您尝试此配置前：

- 安装在其中每一个的MS Windows服务器2008操作系统在测试实验室的服务器。
- 更新所有服务包。

- 安装控制器和轻量级接入点(拉普)。
- 配置最新的软件更新。

初始安装和配置信息Cisco 5508系列无线控制器的，参考Cisco 5500系列无线控制器安装指南。

注意： 本文打算提供读者在PEAP-MS-CHAP验证的Microsoft服务器要求的配置的一示例。在本文提交的MS Windows服务器配置在实验室里测试了并且被发现工作正如所料。如果有与配置的困难，与帮助的Microsoft联系。Cisco技术支持中心(TAC)不支持MS Windows服务器配置。

Microsoft Windows 2008个安装和配置指南可以在Microsoft技术网络找到。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 5508运行固件版本7.4的无线控制器
- 与轻量级接入点协议(LWAPP)的Cisco Aironet 3602接入点(AP)
- 有NP、Certificate Authority (CA)、动态主机控制协议(DHCP)和安装的域名系统(DNS)服务的Windows 2008年企业服务器
- Microsoft Windows 7客户端PC
- Cisco Catalyst 3560系列交换机

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。

PEAP 概述

PEAP使用传输级安全性(TLS)创建在一个验证的PEAP客户端之间的一个已加密信道，例如一无线笔记本电脑和一PEAP验证器，例如Microsoft NP或所有RADIUS服务器。PEAP不指定一认证方法，然而提供附加安全性其他扩展验证协议的(EAPs)，例如EAP-MS-CHAP v2，能通过PEAP提供的Tls加密的信道运行。PEAP认证过程包括两个主要阶段。

PEAP 第一阶段：Tls加密的信道

有AP的无线客户端关联。在一个安全关联创建在客户端和接入点之间前， IEEE 802.11根据关联提供开放式系统或共享密钥认证。在IEEE基于802.11的关联成功设立在客户端和接入点之间后，TLS会话协商与AP。在验证顺利地完成在无线客户端和NP之间后， TLS会话协商在客户端和NP之间。在此协商中派生的密钥将用来加密随后的所有通信。

PEAP 第二阶段：采用 EAP 身份验证的通信

EAP 通信（包括 EAP 协商）发生在由 PEAP 在 PEAP 认证过程的第一阶段中创建的 TLS 通道内。NP验证有EAP-MS-CHAP v2的无线客户端。LAP和仅控制器转发消息在无线客户端和RADIUS服

务器之间。无线局域网控制器(WLC)和LAP不能解密这些消息，因为它不是TLS端点。

成功认证尝试的RADIUS数据顺序(其中用户把PEAP-MS-CHAP v2供给有效基于密码的凭证)是：

1. NP发送Request信息的标识给客户端：EAP 请求/身份。
2. 客户端回复一个身份响应消息：EAP 响应/身份。
3. NP传送MS-CHAP v2询问消息：EAP 请求/EAP 类型=EAP MS-CHAP-V2（质询）。
4. 客户端回复一个 MS-CHAP v2 质询和响应：EAP 响应/EAP 类型=EAP-MS-CHAP-V2（响应）。
5. 当服务器顺利地验证客户端时， NP退还MS-CHAP v2成功数据包：EAP 请求/EAP 类型=EAP-MS-CHAP-V2（成功）。
6. 当客户端对服务器的身份验证成功时，该客户端回复一个 MS-CHAP v2 成功数据包：EAP 响应/EAP 类型=EAP-MS-CHAP-V2（成功）。
7. NP发送指示成功认证的EAP类型长度值(TLV)。
8. 客户端回复一个 EAP-TLV 状态成功消息。
9. 服务器完成验证并且传送在纯文本的EAP成功信息。如果部署了 VLAN 用于客户端隔离，则此消息中还包含 VLAN 属性。

配置

在此部分，您提交以信息配置PEAP-MS-CHAP v2。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

此配置使用以下网络设置：

在此设置， Microsoft Windows 2008服务器执行这些角色：

- 域的wireless.com域控制器
- DHCP/DNS 服务器
- CA 服务器
- NP ？验证无线用户
- 活动目录？维护用户数据库

服务器连接对有线网络通过第二层交换机如显示。 WLC和已注册LAP也连接对网络通过第二层交换机。

无线客户端使用wi-fi受保护的访问2 (WPA2) - PEAP-MS-CHAP v2验证连接到无线网络。

配置

此示例目标将配置Microsoft 2008服务器、无线局域网控制器和轻量AP验证有PEAP-MS-CHAP v2验证的无线客户端。有在此进程的三个主要步骤：

1. 配置Microsoft Windows 2008服务器。
2. 配置WLC和轻量AP。

3. 配置无线客户端。

配置Microsoft Windows 2008服务器

在本例中， Microsoft Windows 2008服务器的完整的配置包括这些步骤：

1. 配置服务器作为域控制器。
2. 安装并且配置DHCP服务。
3. 安装并且配置服务器作为CA服务器。
4. 联络客户端对域。
5. 安装NP。
6. 安装证书。
7. 配置PEAP验证的NP。
8. 添加用户到活动目录。

配置Microsoft Windows 2008服务器作为域控制器

完成这些步骤为了配置Microsoft Windows 2008服务器作为域控制器：

1. 点击**启动**>Server**管理器**。

2. 点击**角色**>Add**角色**。

3. 单击 **Next**。

4. 选择服务**活动目录域服务**，并且**其次**单击。

5. 查看介绍对活动目录域服务，并且**其次**单击。

6. 点击**安装**开始安装过程。

   安装继续并且完成。

7. 点击**Close此向导并且启动活动目录域服务安装向导(dcpromo.exe)**继续活动目录的安装和配置。

8. 单击**在旁边**运行活动目录域服务安装向导。

9. 查看关于操作系统的Compatbilty的信息，并且**其次**单击。

10. **在一个新的森林里**单击**创建一新域>其次**为了创建新域。

11. 输入全双工DNS名对于新域(**在本例中的**wireless.com)，并且其次单击**。**

12. 选择您的域的森林功能级，并且**其次**单击。

13. 选择您的域的域功能级，并且**其次**单击。

14. 保证DNS服务器选择，并且**其次**单击。

15. 点击安装向导的**是**能创建在DNS的一新区域域的。

16. 选择活动目录应该使用其文件的文件夹，并且**其次**单击。

17. 输入管理员密码，并且**其次**单击。

18. 查看您的选择，并且**其次**单击。

安装收益。

19. 点击**芬通社**关闭向导。

20. 重新启动服务器，使更改生效。

安装并且配置在Microsoft Windows 2008服务器的DHCP服务

在Microsoft 2008服务器的DHCP服务用于提供IP地址给无线客户端。完成这些步骤为了安装和配置DHCP服务：

1. 点击**启动**>Server**管理器**。

2. 点击**角色**>Add**角色**。

3. 单击 **Next**。

4. 选择service dhcp**服务器**，并且**其次**单击。

5. 查看介绍对DHCP服务器，并且**其次**单击。

6. 选择DHCP服务器应该为请求监控的接口，并且**其次**单击。

7. 配置DHCP服务器应该提供给客户端的默认DNS设置，并且**其次**单击。

8. 如果网络支持WINS，请配置WINS。

9. 单击**添加**使用向导创建DHCP范围或单击**在旁边**请创建后的DHCP范围。单击“下一步”继续。

10. 启用或禁用在服务器的DHCPv6支持，并且**其次**单击。

11. 如果DHCPv6在前面的步骤，启用请配置IPv6 DNS设置。单击“下一步”继续。

12. 提供域管理员凭证授权在活动目录的DHCP服务器，并且**其次**单击。

13. 查看在确认页的配置，并且点击**安装**完成安装。

    安装收益。

14. 单击**接近**close向导。

    DHCP服务器当前安装。

15. 点击**配置DHCP服务的Start > Administrative Tools > DHCP**。

16. 展开DHCP服务器(在本例中的win-mvz9z2umms.wireless.com)，用鼠标右键单击IPv4，并且选择**新的范围**。创建DHCP范围。

17. 单击**在旁边**通过新的范围向导配置新的范围。

18. 为新的范围(在本例中的无线客户端提供一名称)，并且**其次**单击。

19. 输入能使用DHCP租约的范围可用的IP地址。单击“下一步”继续。

20. 建立不包括地址一可选列表。单击“下一步”继续。

21. 配置租用时间，并且**其次**单击。

22. 点击**是，我要当前配置这些选项**，并且**其次**单击。

23. 输入默认网关的IP地址此范围的，**其次**单击**Add>**。

24. 配置客户端和DNS服务器将使用的DNS域名。单击“下一步”继续。

25. 如果网络支持WINS，请输入此范围的WINS信息。单击“下一步”继续。

26. 要启动此范围，请点击**是，我要当前>其次启动此范围**。

27. 点击**芬通社**完成和关闭向导。

安装并且配置Microsoft Windows 2008服务器作为CA服务器

与EAP-MS-CHAP v2的PEAP验证根据证书的RADIUS服务器在服务器。另外，即由客户端计算机委托必须由公共CA发出的服务器证书(公共CA证书在客户端计算机证书存储的可靠的根证书颁发机构文件夹已经存在)。

完成这些步骤为了配置Microsoft Windows 2008服务器作为发行证书对NP的CA服务器：

1. 点击**启动>**Server**管理器**。

2. 点击**角色>**Add**角色**。

3. 单击 **Next**。

4. 选择服务**活动目录证书服务**，并且**其次**单击。

5. 查看介绍对活动目录证书服务，并且**其次**单击。

6. 选择**认证机关**，并且**其次**单击。

7. 选择**企业**，并且**其次**单击。

8. 选择**根CA**，并且**其次**单击。

9. 选择**创建一新的专用密钥**，并且**其次**单击。

10. 单击**其次**在配置CA的加密算法。

11. 单击**在旁边**接受此CA的默认公用名称。

12. 选择此CA证书有效的时间长度，并且**其次**单击。

13. 单击**在旁边**接受默认证书数据库位置。

14. 查看配置，并且点击**安装**开始活动目录证书服务。

15. 在安装完成后，请点击**Close**。

将客户端连接到域

完成这些步骤为了联络客户端到有线网络和下载从新域的专门领域信息：

1. 使用直通以太网电缆将客户端连接到有线网络。
2. 启动客户端，并且登陆与客户端用户名和密码。
3. 点击**Start > Run**，输入**cmd**，并且点击OK键。
4. 在prompt命令，请输入**ipconfig**，并且按回车验证DHCP正确地运作，并且客户端接收从DHCP服务器的一个IP地址。
5. 为了加入客户端到域，请点击**开始**，用鼠标右键单击**计算机**，选择**属性**，并且选择**崔凡吉莱设置**在右下。
6. 单击 **Change**。
7. 点击**域**，输入**wireless.com**，并且点击OK键。
8. 输入用户名**管理员**和密码特定对客户端加入的域。这是在活动目录的管理员帐户在服务器。
9. 点击OK键，并且再点击OK键。
10. 点击**当前**重新启动计算机的**Close >重新启动**。
11. 计算机重新启动后，用以下信息进行登录：用户名 = **Administrator**；密码 = **<域密码>**；域 =无线。
12. 点击**开始**，用鼠标右键单击**计算机**，选择**属性**，并且选择**崔凡吉莱设置**在右下验证您是在wireless.com域。
13. 下一步是验证客户端从服务器收到了 CA 证书（信任）。
14. 点击**开始**，输入**mmc**，并且按回车。
15. 单击**文件**，然后单击“添加/删除”管理单元。
16. 选择**“证书”**，并单击“添加”。
17. 点击**计算机帐户**，并且**其次**单击。
18. 点击**本地计算机**，并且**其次**单击。
19. 单击 **Ok**。
20. 展开**证书(本地计算机)**和**可靠的根证书颁发机构**文件夹，并且点击**证书**。查找在列表的**无线域 CA cert**。在本例中， CA cert呼叫wireless-WIN-MVZ9Z2UMNMS-CA。

21. 重复此过程，以便将更多客户端添加到域中。

安装在Microsoft Windows 2008服务器的网络策略服务器

在此设置， NP用于作为RADIUS服务器验证有PEAP验证的无线客户端。 完成这些步骤为了安装和配置在Microsoft Windows 2008服务器的NP ：

1. 点击**启动**>Server**管理器**。

2. 点击**角色**>Add**角色**。

3. 单击 **Next**。

4. 选择服务**网络策略并且访问服务**，并且**其次**单击。

5. 查看介绍对网络策略并且访问服务，并且**其次**单击。

6. 选择**网络策略服务器**，并且**其次**单击。

7. 查看确认，并且点击**安装**。

   在安装完成后，屏幕类似于这一个显示。

8. 单击 **Close**。

安装证书

完成这些步骤为了安装NP的计算机证书：

1. 点击**开始**，输入**mmc**，并且按回车。
2. 点击**File>添加/删除管理单元**。
3. 选择**"证书"**，并单击"添加"。

4. 选择**计算机帐户**，然后单击"下一步"。

5. 选择**本地计算机**，并且点击**芬通社**。

6. 点击OK键返回到微软管理控制台(MMC)。

7. 展开**证书(本地计算机)**和**个人**文件夹，并且点击**证书**。

8. 用鼠标右键单击在CA证书下的空白，并且选择**所有任务>请求新证书**。

9. 单击 **Next**。

10. 选择**域控制器**，并且单击**登记**。

11. 一旦证书安装，请点击**芬通社**。

NP证书当前安装。

12. 保证证书的打算的目的读**客户端验证，服务器验证**。

配置PEAP-MS-CHAP v2验证的网络策略服务器服务

完成这些步骤为了配置验证的NP ：

1. 点击**Start > Administrative Tools >网络策略服务器**。

2. 用鼠标右键单击**NP (本地)**，并且选择**在活动目录的寄存器服务器**。

3. 单击 **Ok**。

4. 单击 **Ok**。

5. 添加无线局域网控制器作为NP的一个验证、授权和统计(AAA)客户端。
6. 扩展**RADIUS客户端和服务器**。右键单击 **RADIUS 客户端**，然后选择“新建 RADIUS 客户端”。

7. 输入友好名称(在本例中的WLC)， WLC (在本例中的192.168.162.248的)管理IP地址和一共享机密。同样共享机密用于配置WLC。

8. 点击OK键返回到上一屏幕。

9. 创建无线用户的一个新的网络策略。展开**策略**，用鼠标右键单击**网络策略**，并且选择**新**。

10. 进入此规则的(在本例中的无线PEAP一策略名称)，并且**其次**单击。

11. 要安排此策略允许只有无线域用户，请添加这三个情况，并且**其次**单击：

- Windows组-域用户
- NAS端口类型-无线- IEEE 802.11
- 认证类型- EAP

12. 点击**授权的访问**授权匹配此策略的连接尝试，并且**其次**单击。

13. 禁用所有认证方法在较少下安全认证方法。

14. 单击**添加**，挑选PEAP，并且点击OK键启用PEAP。

15. 选择**Microsoft ：Protected EAP (PEAP)**，和单击**编辑**。保证证书在证书发出的下拉列表选择的以前已创建域控制器，并且点击OK键。

16. 单击 **Next**。

17. 单击 **Next**。

18. 单击 **Next**。

19. 单击 **完成**。

将用户添加到 Active Directory

在本例中，用户数据库在活动目录维护。 完成这些步骤为了添加用户到活动目录数据库：

1. 打开 **Active Directory 用户和计算机**。点击**Start > Administrative Tools >激活目录用户和计算机**。
2. 在激活目录用户和计算机控制台结构树中，请展开域，用鼠标右键单击**用户**>New，并且选择**用户**。
3. 在新的对象？用户对话框，输入无线用户的名称。此示例在First Name字段使用命名Client1和Client1在登录名字名称字段。单击 **Next**。

4. 在新的对象？用户对话框，输入您的在密码的选择密码并且确认密码字段。不选定**用户必须更改密码在下个登录**复选框，并且**其次**单击。

5. 在新的对象？用户对话框，点击**芬通社**。

6. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

配置无线局域网控制器和拉普

配置无线设备(无线局域网控制器和拉普)此设置的。

配置RADIUS验证的WLC

配置WLC使用NP作为认证服务器。必须配置WLC为了转发用户凭证到外部RADIUS服务器。外部RADIUS服务器然后验证用户凭证和提供访问对无线客户端。

完成这些步骤为了添加NP作为在**Security>RADIUS验证**页的一个RADIUS服务器：

1. 从显示RADIUS验证服务器页的控制器接口选择**Security>RADIUS >验证**。单击**新**为了定义RADIUS服务器。

2. 定义RADIUS服务器参数。这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。网络用户和管理复选框确定基于RADIUS的验证是否适用于管理和网络(无线)用户。此示例使用NP作为RADIUS服务器与192.168.162.12的IP地址。单击 **Apply**。

为客户端配置 WLAN

配置identfier的服务集(SSID) (WLAN)无线客户端连接。本示例中将创建 SSID，并将其命名为**PEAP**。

定义Layer2验证作为WPA2，以便客户端执行基于EAP的验证(在本例中的PEAP-MS-CHAP v2)并且使用高级加密标准(AES)作为加密机制。将其他所有值均保留默认值。

注意： 本文档将 WLAN 与管理接口绑定。当您的网络中有多个 VLAN 时，可以创建一个单独的 VLAN 并将其绑定到 SSID。有关如何在 WLC 上配置 VLAN 的信息，请参阅无线局域网控制器上的 VLAN 配置示例。

完成这些步骤为了配置在WLC的一WLAN ：

1. 点击从控制器接口的**WLAN**为了显示WLAN页。此页列出了控制器上现有的 WLAN。
2. 选择**新建**创建新的 WLAN。输入 WLAN 的 WLAN ID 和 WLAN SSID，然后单击**应用**。

3. 要配置802.1x的SSID，请完成这些步骤： 点击**常规选项卡**并且启用WLAN。

   点击**安全> Layer2**选项卡，设置第2层安全为**WPA+WPA2**，检查需要的WPA+WPA2参数(例如， WPA2 AES)检查boxesas，并且单击**802.1x**作为认证密钥管理。

点击**安全**>AAA**服务器**选项卡，从**Server1**下拉列表选择NP的IP地址，并且单击**应用**。

配置PEAP-MS-CHAP v2验证的无线客户端

完成这些步骤配置无线客户端以Windows零个设置工具连接到PEAP WLAN。

1. 点击**网络图标**在任务栏。点击**PEAP** SSID，并且点击**连接**。

2. 客户端应该当前连接到网络。

3. 如果连接发生故障，请设法重新连接到WLAN。如果问题仍然存在，参考Troubleshoot部分。

验证

当前没有可用于此配置的验证过程。

故障排除

如果您的客户端没有连接对WLAN，您能使用排除故障配置的此部分提供信息。

有能使用诊断802.1x认证失败的两个工具：**client命令的调试**和在Windows的**事件查看器**。

执行从WLC的调试不是密集的资源并且不imnpact服务的客户端。启动调试会话，打开WLC的命令行界面(CLI)和回车**调试客户端MAC地址**， MAC地址是无线客户端无线MAC地址无法连接。当此调试运行时，请设法联络客户端;在看起来类似于此示例WLC的CLI应该输出那里：

这是可能发生在误配置问题的示例。这里， WLC调试显示WLC搬入正在验证状态，含义WLC等待从NP的一答复。这通常归结于在WLC或NP的一不正确共享机密。您能通过Windows服务器事件查看器确认此。如果没找到一本日志，请求未曾使它到NP。

从WLC调试被找到的另一示例是访问拒绝。访问拒绝显示那接收的NP并且拒绝客户机证书的。这是接收访问拒绝的客户端的示例：

当您看到访问拒绝时，请检查注册Windows服务器事件日志确定NP为什么响应给有访问拒绝的客户端。

成功认证有一access-accept在客户端调试，如在此示例中看到：

排除故障访问拒绝和响应超时要求对RADIUS服务器的访问。WLC作为传递EAP消息在客户端和RADIUS服务器之间的验证器。应该响应与访问拒绝或响应超时的RADIUS服务器由RADIUS服务的制造商诊断检查和。

注意：TAC为第三方RADIUS服务器不提供技术支持;然而，注册RADIUS服务器通常解释客户端的要求为什么拒绝或忽略。

为了排除故障访问拒绝和响应超时从NP，请检查NP登陆Windows事件查看器在服务器。

1. 点击启动事件查看器**和检查NP日志的启动>管理员Tools > Event Viewer**。
2. 展开**自定义视图**>Server**角色>网络策略并且访问**。

在事件视图的此部分，有合格和失败的认证日志。检查这些日志排除故障客户端为什么不通过验证。通过和失败的认证出现如信息性。通过日志移动查找有失败的认证的用户名，并且接收访问拒绝根据WLC调试。

这是拒绝用户访问的NP的示例：

当查看在事件查看器时的一拒绝语句，请检查验证细节部分。在本例中，您能看到NP拒绝用户访问由于不正确的用户名：

如果WLC不接收从NP的一答复上一步在NP的事件视图也协助故障排除。 这由在NP和WLC之间的一不正确共享机密通常造成。

在本例中， NP丢弃从WLC的请求由于一不正确共享机密：

相关信息

- [技术支持和文档 - Cisco Systems]