与LAP和ACS 5.2配置示例的基于端口的验证

目录

简介

本文描述如何配置一轻量级接入点(LAP)，当802.1x请求方为了验证一个RADIUS服务器例如访问控制服务器(ACS) 5.2。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 有无线局域网控制器(WLC)和拉普的基础知识。
- 有AAA服务器的功能知识。
- 有无线网络和无线安全安全性问题详尽的知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本7.0.220.0的思科5508 WLC
- Cisco 3502系列LAP
- 运行版本5.2的Cisco Secure ACS
- Cisco 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。

背景信息

拉普设备安装X.509证书-签字由-烧录到设备在制造时的专用密钥。拉普使用此证书为了验证与WLC在加入进程。此方法描述另一个方式验证拉普。使用WLC软件，您能配置在Cisco Aironet接入点(AP)和Cisco交换机之间的802.1x验证。在这种情况下， AP作为802.1x请求方和由该的RADIUS服务器(ACS)的交换机验证EAP-FAST的用途与匿名PAC设置。一旦它为802.1x验证配置，交换机不允许任何流量除802.1x流量之外穿过端口，直到设备连接对端口成功验证。AP可以验证或者，在加入WLC前或，在加入WLC后，在您配置在交换机情况下的802.1x，在LAP加入WLC后。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：

下面是此图中使用的组件的配置详细信息：

- ACS (RADIUS)服务器的IP地址是192.168.150.24。
- WLC的管理和Ap-manager接口地址是192.168.75.44。
- DHCP服务器寻址192.168.150.25。
- LAP在VLAN 253安置。
- VLAN 253 ：192.168.153.x/24.网关：192.168.153.10
- VLAN 75 ：192.168.75.x/24.网关：192.168.75.1

假定

- 交换机为所有第3层VLAN配置。
- DHCP服务器分配DHCP范围。
- 第3层连通性存在网络的所有设备之间。
- LAP已经加入对WLC。
- 每个VLAN有一/24掩码。
- ACS 5.2有安装的一自签证书。

配置步骤

此配置分为三类：

1. 配置LAP。
2. 配置交换机。
3. 配置 RADIUS 服务器。

配置LAP

假定:

使用选项43， LAP已经注册对WLC， DNS或者静态配置的WLC管理接口IP。

完成这些步骤：

1. 去**Wireless>Access指向>所有AP**为了验证在WLC的LAP注册。
2. 您能配置802.1x凭证(即用户名/密码)所有拉普的用两种方式：**全局**对于已经加入的LAP，您能设置凭证全局，因此加入WLC的每个LAP将继承那些凭证。**个别地**配置802.1x配置文件每个AP。在我们的示例中，我们将配置凭证每个AP。去**无线>所有AP**，并且选择担心的AP。在**802.1x请求方凭证**字段添加用户名和密码。**注意：** 登录凭证用于远程登录， SSH或者控制台到AP。
3. 配置高性能的部分，并且单击**应用**。**注意：** 一旦保存，这些凭证在WLC和AP重启间保留。凭证更改，只有当LAP加入一新的WLC。在新的WLC配置的LAP假设用户名和密码。如果AP未加入WLC，您必须控制到LAP为了设置凭证。发出此CLI命令在特权模式：**LAP#lwapp ap dot1x用户名*<username>*密码*<password>*或LAP#capwap ap dot1x用户名*<username>*密码*<password>*注意：** 此命令为运行恢复镜像的AP是仅可用的。默认用户名和密码LAP的分别为cisco和。

配置交换机

交换机作为LAP的一验证器并且利用RADIUS服务器验证LAP。如果交换机没有兼容软件，请升级交换机。在交换机CLI中，请发出这些命令为了启用在交换机端口的802.1x验证：

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

注意： 如果有在同一交换机的其他AP，并且不希望他们使用802.1x，您能离开端口没有配置为

802.1x或发出此命令：

```
switch(config-if)authentication port-control force-authorized
```

配置RADIUS服务器

LAP验证与EAP-FAST。确保RADIUS服务器您使用支持此EAP方法，如果不使用Cisco ACS 5.2。

RADIUS服务器配置分开成四个步骤：

1. Configure network资源。
2. 配置用户。
3. 定义策略元素。
4. 运用访问策略。

ACS 5.x是一基于策略的ACS。换句话说， ACS 5.x使用一个基于规则的策略型号而不是用于4.x版本的基于组的型号。

更加强大ACS 5.x基于规则的策略型号的提供和灵活访问控制与更旧的基于组的方法比较。

在更旧的基于组的型号中，因为包含并且配合信息的三种类型组定义了策略：

- **身份信息**-此信息在AD或LDAP组中可以根据会员或内部ACS用户的一个静态分配。
- **其他限制或情况**-时间限制，设备限制，等等。
- **权限**- VLAN或Cisco IOS权限级别。

ACS 5.x策略型号根据表的规则：

如果情况然后发生

例如，我们使用描述的信息基于组的型号：

如果标识条件，限制条件然后授权配置文件。

结果，这提供我们灵活性限制下用户允许访问网络并且的条件在什么授权级别允许，当特定情况符合时。

Configure network资源

在此部分，我们配置交换机的AAA客户端在RADIUS服务器。

此步骤如何解释添加交换机作为RADIUS服务器的一个AAA客户端，以便交换机能通过LAP的用户凭证到RADIUS服务器。

完成这些步骤：

1. 从ACS GUI，请点击**网络资源**。
2. 点击**网络设备组**。
3. 去**位置>创建**(在底部)。

4. 添加必填字段并且单击**提交**。
5. 窗口刷新：
6. 点击**设备类型>创建**。
7. 单击 **submit**。一旦完成，窗口刷新：
8. 去**网络资源>网络设备和AAA客户端**。
9. 单击**创建**，并且填写详细信息如表示此处：
10. 单击 **submit**。窗口刷新：

配置用户

在此部分，您将看到如何创建以前配置的ACS的一个用户。您将分配用户到组呼叫“LAP用户”。

完成这些步骤：

1. 去**用户，并且标识存储>标识Groups>创建**。
2. 单击“Submit”。
3. 创建**3502e**并且分配它分组“LAP用户”。
4. 去**用户，并且标识存储>标识Groups>用户>创建**。
5. 您将看到更新信息：

定义策略元素

验证**Permit访问**设置。

运用访问策略

在此部分，您将选择EAP-FAST，因为用于拉普的认证方法为了验证。您然后将创建根据上一个步骤的规则。

完成这些步骤：

1. 去**访问策略**>Access **Services>默认网络网络访问**> Edit ：**“默认网络网络访问”**。
2. 确保您启用**EAP-FAST**和**匿名带内PAC设置**。
3. 单击 **submit**。
4. 验证您选择的标识组。在本例中，(在ACS创建)的使用**内部用户**和保存更改。
5. 去**访问策略**>Access **Services>默认网络网络访问>授权**为了验证授权配置文件。您能在什么情况下定制您将提供对网络的一次用户访问，并且什么授权配置文件(属性)您将通过一次已验证。此粒度只是可用的在ACS 5.x。在本例中，**位置**、**设备类型**、**协议**、**标识组**和**EAP验证方法**选择。
6. 点击OK键，并且**保存更改**。
7. 下一步是创建规则。如果规则没有定义，LAP允许访问，不用任何情况。
8. 单击**创建> Rule-1**。此规则是为用户在组“LAP用户”中。
9. 点击**Save Changes**。如果想要不匹配的用户将拒绝的条件，请编辑默认规则说“请拒绝访问”。
10. 最后一步是定义服务选择规则。请使用此页配置一项简单或基于规则的策略为了确定适用的哪服务于流入请求。例如：

验证

一旦802.1x在交换机端口启用，所有流量，除了802.1x流量通过端口阻塞。LAP，已经注册对WLC，获得不相关。在一成功的802.1x验证之后是通过通过的其他允许的流量。LAP的成功的注册对WLC的，在802.1x在交换机后启用表明LAP验证是成功的。

AP控制台：

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN

*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
```

ACS日志：

1. 查看命中数计数：如果在15分钟检查日志验证内，请确保您刷新命中数计数。在同一个页，在底部您有一**命中数计数**选项卡。
2. 点击**监听，并且报告**和一新的弹出窗口发表。点击**认证– RADIUS –今天**。您能也单击服务选择规则应用的**详情**为了验证。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科安全访问控制系统
- 技术支持和文档 - Cisco Systems