NAC 带外 (OOB) 无线配置示例

目录

简介

本文档提供在 Cisco 统一无线网络部署中部署带外 (OOB) Cisco 网络准入控制 (NAC) 设备终点安全功能的设计指导。这些最佳实践建议假设，已根据企业移动性设计指南 3.0 版中提供的准则部署了 Cisco 统一无线网络。

建议的设计是虚拟网关（网桥模式）和使用 RADIUS 单一登录的中央部署 OOB 解决方案。无线局域网控制器 (WLC) 必须放置在邻近 NAC 服务器的第 2 层上。客户端关联到 WLC，WLC 对用户进行身份验证。完成身份验证后，用户数据流将通过隔离 VLAN 从 WLC 进入 NAC 服务器。会进行状态评估和修正过程。一旦用户获得认证，该用户的 VLAN 将在 WLC 中从隔离 VLAN 更改为接入 VLAN。数据流在移至接入 VLAN 时将绕过 NAC 服务器。

先决条件

要求

本文档配置特定于 NAC 4.5 和 WLC 5.1 版本

使用的组件

本文档限于特定的软件和硬件版本。

- NAC 服务器 3350 4.5
- NAC 管理器 3350 4.5
- WLC 2106 5.1

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

Cisco NAC 概述

Cisco NAC 使用网络基础架构强制所有需要访问网络计算资源的设备遵守安全策略。使用 Cisco NAC 设备，网络管理员可以在有线、无线和远程用户及其计算机访问网络之前对其进行身份验证、授权、评估和修正。Cisco NAC 设备先确定网络设备（如便携式计算机、IP 电话或游戏控制台）是否与网络安全策略相符，并修复任何漏洞，然后再允许它们访问网络。

下面将讨论建议设计的术语：

虚拟网关模式（网桥模式）

当 NAC 设备被配置为虚拟网关时，它充当最终用户和受管客户端子网的默认网关（路由器）之间的网桥。对于给定客户端 VLAN，NAC 设备将数据流从其不受信任的接口桥接到其受信任的接口。它充当从设备的不受信任端到受信任端的网桥时，将使用两个 VLAN。例如，客户端 VLAN 110 被定义在无线局域网控制器 (WLC) 和 NAC 设备的不受信任接口之间。在分布层交换机上，没有与 VLAN 110 关联的路由接口或交换虚拟接口 (SVI)。VLAN 10 被配置在 NAC 设备的受信任接口和客户端子网的下一跳路由器接口/SVI 之间。将到达 VLAN 110 的数据包向外转发到 VLAN 10 的 NAC 设备交换 VLAN 标记信息时，会在该设备中建立一个映射规则，如图 1-1 所示。对于返回客户端的数据包，过程正好相反。请注意，在此模式下，不会将 BPDU 从不受信任端 VLAN 传送到其受信任端对等 VLAN。将 NAC 设备以逻辑内联方式放置在客户端和受保护的网络之间时，通常选择 VLAN 映射选项。如果要将 NAC 设备部署在使用统一无线部署的虚拟网关模式下，则必须使用此桥接选项。由于 NAC 服务器知道*上层协议*，因此默认情况下它明确允许要求它以已经过身份验证的角色连接到网络的协议，例如，DNS 和 DHCP。

图 1-1 使用 VLAN 映射的虚拟网关

带外模式

带外部署要求用户数据流仅在身份验证、状态评估和修正过程中通过 NAC 设备。当用户经过身份

验证并通过所有策略检查后，数据流将正常地通过网络交换并绕过 NAC 服务器。有关详细信息，请参阅 Cisco NAC Appliance-Clean Access Manager 安装和管理指南的第 4 章。

以这种方式配置 NAC 设备时，WLC 是 NAC 管理器中的一个受管设备，NAC 管理器以同样的方式管理 Cisco 交换机。当用户经过身份验证并通过状态评估后，NAC 管理器将指示 WLC 标记从 NAC VLAN 到提供访问权限的接入 VLAN 的用户数据流。

图 1-2 带外模式下使用虚拟网关模式的 NAC 设备

单一登录

单一登录 (SSO) 是一个不需要用户干预且实施过程相当简单的选项。它利用 NAC 解决方案的 VPN SSO 功能，外加客户端 PC 上运行的 Clean Access 代理软件。VPN SSO 使用 RADIUS 记账记录通知 NAC 设备有关连接到网络的已经过身份验证的远程访问用户的情况。同样地，可以将此功能与 WLAN 控制器结合使用以自动通知 NAC 服务器有关连接到网络的已经过身份验证的无线客户端的情况。

有关通过 NAC 设备执行 SSO 身份验证、状态评估、修正和网络访问的无线客户端的示例，请参见图 1-3 到 1-6。

图 1-3 中显示以下过程序列：

1. 无线用户通过 WLAN 控制器对上游 AAA 服务器执行 802.1x/EAP 身份验证。
2. 客户端从 AAA 或 DHCP 服务器获得 IP 地址。
3. 客户端收到 IP 地址后，WLC 会将 RADIUS 记账（开始）记录转发给 NAC 设备，其中包括无线客户端的 IP 地址。**注意：** WLC 控制器对 802.1x 客户端身份验证和 IP 地址分配使用一条 RADIUS 记账记录（开始），而 Cisco Catalyst 交换机会发送两条记账记录：在 802.1x 客户端身份验证后将发送一条记账开始记录，在为客户端分配 IP 地址后将发送一条临时更新记录。
4. 检测到网络连接后，NAC 代理会尝试连接到 CAM（使用 SWISS 协议）。数据流被 NAC 服务器拦截，NAC 服务器转而查询 NAC 管理器以确定用户是否位于联机用户列表中。只有经过身份验证的客户端才位于联机用户列表中，这是以上示例中作为第 3 步中 RADIUS 更新结果的情况。
5. NAC 代理执行客户端计算机的本地安全/风险状态评估，并将评估转发给 NAC 服务器以进行网络准入决定。**图 1-3 客户端身份验证过程和状态评估**

图 1-4 中发生以下过程序列：

1. NAC 设备将代理评估转发给 NAC 设备管理器 (CAM)。
2. 在本示例中，CAM 确定客户端不符合要求并指示 NAC 设备将用户放到隔离角色中。
3. 然后，NAC 设备向客户端代理发送修正信息。**图 1-4 从 CAS 到 CAM 的状态评估信息**

图 1-5 中发生以下过程序列：

1. 客户端代理显示完成剩余修正所需的时间。
2. 代理指导用户逐步完成修正过程；例如，在防病毒定义文件的更新中。
3. 修正完成后，代理会更新 NAC 服务器。
4. CAM 向用户显示一个可接受使用政策 (AUP) 声明。**图 1-5 使用 CAS 作为实施设备的客户端修正过程**

图 1-6 中发生以下过程序列：

1. 接受 AUP 后，NAC 设备会将用户转换为联机（已授权）角色。
2. SSO 功能使用客户端 IP 地址填充联机用户列表。修正后，会将一个主机条目添加到已认证列表中。这两个表（与已发现客户端表一起）都由 CAM（NAC 设备管理器）进行维护。
3. NAC 管理器向 WLC 发送一个 SNMP 写通知以将用户 VLAN 从隔离 VLAN 更改为接入 VLAN。
4. 带有接入 VLAN 标记的用户数据流开始离开 WLC。NAC 服务器不再位于此特定用户数据流的路径中。**图 1-6 已认证客户端通过切换到接入 VLAN 绕过 CAS**

有助于进行无线用户身份验证的最简单的方法是，在 NAC 服务器上启用 VPN-SSO 身份验证并配置 WLC 以将 RADIUS 记账记录转发到 NAC 服务器。如果需要将记账记录转发到位于网络上游的 RADIUS 服务器，则可以配置 NAC 服务器以将记账数据包转发到 RADIUS 服务器。

注意： 如果启用了 VPN-SSO 身份验证而未在客户端 PC 上安装 Clean Access 代理，则仍会自动对用户进行身份验证。但是，在打开用户 Web 浏览器并进行连接尝试之前，不会通过 NAC 设备自动连接这些用户。在这种情况下，当用户打开他们的网络浏览器时，会在“无代理”阶段中暂时重定向他们（没有登录提示）。SSO 进程完成后，会将他们连接到他们最初请求的 URL。

配置 NAC OOB 无线解决方案

本部分提供有关如何配置本文档所述功能的信息。

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。

在当前 NAC 实施中，WLC 仅在带内模式下与 Cisco NAC 设备集成，在带内模式下，NAC 设备必须保留在数据路径中，即使在用户已获得认证后也是如此。NAC 设备完成其状态验证后，员工/访客将收到基于其角色的网络访问权限。

使用 NAC 4.5 和 WLC 5.1 版本，无线 NAC 解决方案支持将 OOB 与 NAC 设备集成。客户端关联并完成第 2 层身份验证后，会检查隔离接口是否已关联到 WLAN/SSID。如果是，则在隔离接口上发送初始数据流。客户端数据流将流入已中继到 NAC 设备的隔离 VLAN 中。状态验证完成后，NAC 管理器会发送一条更新接入 VLAN ID 的 SNMP 设置消息；控制器使用接入 VLAN ID 更新它自身，并且数据流开始从控制器直接交换到网络，而不经过 NAC 服务器。

图 2-1 通过交换机连接到 WLC 的网桥模式下的独立 CAS 示例

在图 2-1 中，WLC 连接到一个中继端口，该中继端口连接隔离 VLAN 和接入 VLAN（176 和 175）。在交换机上，隔离 VLAN 数据流将中继到 NAC 设备，接入 VLAN 数据流将直接中继到第 3 层交换机。到达 NAC 设备上的隔离 VLAN 的数据流将被映射，以根据静态映射配置访问 VLAN。当客户端关联完成第 2 层身份验证后，它会检查是否已关联隔离接口；如果是，则在隔离接口上发送数据。客户端数据流将流入已中继到 NAC 设备的隔离 VLAN 中。状态验证完成后，NAC 服务器 (CAS) 会向控制器发送一条更新接入 VLAN ID 的 SNMP 设置消息，数据流开始从 WLC 直接交换到网络，而不经过 NAC 服务器。

限制

- 没有关联的端口配置文件
- 未在 NAC 管理器上指定 VLAN ID：定义在 WLC 上
- MAC 过滤器支持无法使用角色设置中的 VLAN ID
- 仅带外虚拟网关美洲台服务器模式支持
- WLC 和 NAC 服务器之间的第 2 层关联
- NAC ISR 和 WLC NM 不能设置为执行无线 OOB NAC

注意： 参考在Cisco NAC设备的虚拟网关模式部分的VLAN映射- Clean Access服务器配置指南，发布4.8(1)关于如何安全配置在虚拟网关模式的VLAN的更多信息。

Catalyst 交换机配置

```
interface GigabitEthernet2/21
 description NAC SERVER UNTRUSTED INTERFACE switchport switchport trunk native vlan 998
switchport trunk allowed vlan 176 switchport mode trunk no ip address ! interface
GigabitEthernet2/22 description NAC SERVER TRUSTED INTERFACE switchport switchport trunk native
vlan 999 switchport trunk allowed vlan 11,175 switchport mode trunk no ip address ! interface
GigabitEthernet2/23 description NAC MANAGER INTERFACE switchport switchport access vlan 10 no ip
address spanning-tree portfast ! interface GigabitEthernet2/1 description WLC switchport
switchport trunk allowed vlan 75,175,176 switchport trunk native vlan 75 switchport mode trunk
no ip address ! interface Vlan75 Description WLC Management VLAN ip address 10.10.75.1
255.255.255.0 ! interface Vlan175 Description Client Subnet Access VLAN ip address 10.10.175.1
255.255.255.0 end
```

在 WLC 和 NAC 管理器上配置 NAC OOB 的步骤

请按照以下步骤在 WLC 和 NAC 管理器上配置 NAC OOB：

1. 在控制器上启用 SNMP v2 模式。
2. 在 CAM 管理器上为 WLC 创建一个配置文件。单击 **OOB Management Profile > Device > New**。
3. 在 CAM 上创建配置文件后，请在配置文件中添加 WLC；转至 **OOB Management > Devices > New** 并输入 WLC 的管理 IP 地址。现在已在 CAM 管理器中添加了控制器。
4. 在 WLC 中添加 CAM 作为 SNMP 陷阱接收器。请使用 CAM 中作为 SNMP 接收器的陷阱接收器的确切名称。
5. 以同样的名称在 CAM 中配置 SNMP 陷阱接收器，该名称在控制器上指定；单击 **OOB Management > SNMP Receiver** 下的 Profiles。在此阶段，WLC 和 CAM 可以相互通信以进行客户端状态验证和访问/隔离状态更新。
6. 在控制器中，创建连接接入 VLAN 和隔离 VLAN 的动态接口。
7. 创建 WLAN，并将其与动态接口关联。
8. 最后，在 WLAN 中启用 NAC。
9. 在 CAS 服务器中添加客户端子网作为受管子网；单击 **CAS server > Select your CAS server > Manage >Advanced > Managed Subnets >Add Unused IP address from the client subnet** 并输入受管子网的隔离 VLAN（不受信任的 VLAN）。
10. 在 CAS 上创建 VLAN 映射。选择**CAS服务器>选择您的CAS服务器>管理>Advanced > VLAN映射**。添加接入 VLAN 作为受信任的 VLAN 并添加隔离 VLAN 作为不受信任的 VLAN。

使用 OOB 无线解决方案配置单一登录 (SSO)

以下是启用无线 SSO 的要求：

1. 在 NAC 服务器上启用 VPN 身份验证 - WLC 在 NAC 设备中被定义为“VPN 集中器”。
2. 在 WLC 上启用 RADIUS 记账 - 在 NAC 设备中定义的控制器必须配置为针对每个 802.1x/EAP WLAN（NAC 中的受管子网）向 NAC 设备发送 RADIUS 记账记录。

在 NAC 管理器上配置 SSO 的步骤

请按照以下步骤在 NAC 管理器上配置 SSO：

1. 在 CAM 左侧菜单中的 Device Management 下，选择 **CCA Server**，然后单击 NAC Server 链接。
2. 从 Server Status 页中，选择 **Authentication** 选项卡，然后选择 VPN Auth 子菜单。请参阅图 3-1。**图 3-1 启用单一登录 NAC 服务器**
3. 选择 **VPN Concentrators Setting**（图 3-2）以添加一个新的 WLC 条目。填充 WLC 管理 IP 地址和您要在 WLC 和 NAC 服务器之间使用的共享密钥的输入字段。**图 3-2 在 VPN Concentrator 部分下添加 WLC 作为 RADIUS 客户端**
4. 对于角色映射，请在 User Management > Auth Servers 下添加类型为 **VPN sso** 的新身份验证服务器。
5. 单击 **Mapping** 图标，然后添加映射规则。映射根据 WLC 在记账数据包中发送的类属性 25 值的不同而异。此属性值在 RADIUS 服务器中配置，并根据用户授权的不同而异。在本示例中，属性值为 **ALLOWALL**，它位于角色 AllowAll 中。

在无线局域网控制器上配置 SSO 的步骤

需要在 WLC 上配置 RADIUS 记账以通过 NAC 服务器实现单一登录功能。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

用于验证的 CISCO WLC CLI 命令

```
(Cisco Controller) >show interface summary

Interface Name    Port Vlan Id    IP Address      Type    Ap Mgr Guest
------------------------------------------------ ---- -------- ------
ap-manager        1    untagged   10.10.75.3      Static  Yes    No
management        1    untagged   10.10.75.2      Static  No     No
nac-vlan          1    175        10.10.175.2     Dynamic No     No
service-port      N/A  N/A        192.168.1.1     Static  No     No
virtual           N/A  N/A        1.1.1.1         Static  No     No


(Cisco Controller) >show interface detailed management

Interface Name..................................... management
MAC Address........................................ 00:18:73:34:b2:60
IP Address......................................... 10.10.75.2
IP Netmask......................................... 255.255.255.0
IP Gateway......................................... 10.10.75.1
VLAN............................................... untagged
Quarantine-vlan.................................... 0
Active Physical Port............................... 1
Primary Physical Port.............................. 1
Backup Physical Port............................... Unconfigured
Primary DHCP Server................................ 10.10.75.1
Secondary DHCP Server.............................. Unconfigured
DHCP Option 82..................................... Disabled
```

```
ACL.......................................... Unconfigured
AP Manager................................... No
Guest Interface.............................. No

(Cisco Controller) >show interface detailed nac-vlan

Interface Name............................... nac-vlan
MAC Address.................................. 00:18:73:34:b2:63
IP Address................................... 10.10.175.2
IP Netmask................................... 255.255.255.0
IP Gateway................................... 10.10.175.1
VLAN......................................... 175 Quarantine-
vlan............................... 176 Active Physical Port.......................... 1
Primary Physical Port........................ 1 Backup Physical
Port......................... Unconfigured Primary DHCP Server.........................
10.10.175.1 Secondary DHCP Server........................ Unconfigured DHCP Option
82............................... Disabled ACL.....................................
Unconfigured AP Manager..................................... No Guest
Interface............................... No
```

从 WLC GUI 进行的客户端状态验证

最初，客户端处于隔离状态，直到在 NAC 设备中完成状态分析。

完成状态分析后，客户端的 NAC 状态必须为 **Access**。

使用 WLC 验证 NAC 服务器上的单一登录

在 VPN Auth 下，转至 **Active Client** 子部分以验证记账开始数据包是否已从 WLC 到达。此条目显示已在客户端计算机上安装的 CCA 代理。

您需要打开浏览器来完成不需要代理的单一登录进程。当用户打开浏览器时，将执行 SSO 进程，并且用户将显示在联机用户列表 (OUL) 中。使用 RADIUS 记账停止数据包，会将用户从活动客户端列表中删除。

故障排除

目前没有针对此配置的故障排除信息。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- 远程用户拨入认证系统(RADIUS)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems