无线局域网控制器(WLCs)安全

目录

简介

本文提供必要的几个重要方面概述处理无线局域网控制器(WLCs)和他们连接的网络之间的安全交互作用。本文着重主要数据流控制和不讨论WLAN安全策略， AAA或WPS。

影响与目的地的主题流量“对控制器”在本文包括和与与“网络的用户涉及”的流量没有涉及。

注意： 在应用他们前验证更改对您的网络，和某些在本文的示例能阻止对您的控制器的管理访问，如果不正确地应用。

先决条件

要求

Cisco 建议您了解以下主题：

- 关于如何配置WLC和轻量级接入点(LAP)以满足基本运作的知识
- OSI模型的基础知识
- 知道访问控制表(ACL)如何工作

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 2000/2100/运行固件4.2.130.0， 5.2.157.0或以后的4400系列WLC

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。

在WLCs的流量处理

在网络安全的一关键组件是数据流控制。在所有部署，对到达在设备的流量块类型是非常重要为了防止潜在的安全问题(DoS、信息损耗、权限逐步升级等等)。

在WLC，数据流控制是受一个重要事实的影响的：有处理在设备的两个组件流量：

- CPU —照料所有管理行为、RRM， LWAPP控制、验证、DHCP等等的主处理器。
- NPU —照料已验证客户端的快速流量转发的网络处理器(配线对无线反之亦然)。

此体系结构允许一快速流量转发，并且减少在主CPU的负载，能然后投入高层次任务的所有其资源。

此体系结构在4400， WiSM和3750个集成的控制器被找到。对于2106和NM-WLC和相关控制器，转发在软件方面完成，也由主CPU。所以，它采取在CPU的更高的税金。所以这些平台提供一更低用户和AP计数支持。

控制流量

您希望对过滤数据流关于WLC，知道是重要的这是否是用户对网络流量或是往主CPU。

- 对于对CPU的所有流量，例如，管理协议例如SNMP、HTTPS、SSH、Telnet或者网络服务协议例如Radius或DHCP，使用“CPU ACL”。
- 对于到/从一个无线客户端的所有流量，包括通过EoIP通道(访客访问)的流量，每个用户ACL使用接口ACL、WLAN ACL或者a。

流量定义“对CPU”，作为输入控制器，有目的地对管理IP地址，任何动态接口或服务端口地址的流量。Ap-manager不处理除了LWAPP/CAPWAP的其他流量。

控制的管理访问

WLCs有管理协议的“会话级别”访问控制。知道是重要的他们如何工作为了防止在什么的不正确评估由控制器允许或没有允许。

命令限制什么管理协议允许是(在一个全局范围)：

- **设置网络SSH enable (event)|禁用**—这启用或禁用在控制器的SSH服务。默认情况下启用该接口。一旦禁用，端口(TCP 22)不会可及的。
- **设置网络telnet enable (event)|禁用**—这启用或禁用在控制器的Telnet服务。默认情况下它是禁用的。一旦禁用，端口(TCP 23)不会可及的。
- **设置网络http enable (event)|禁用**—这启用或禁用在控制器的http服务。端口(TCP 80)不更加长可及的。默认情况下它是禁用的。
- **设置网络https enable (event)|禁用**—这启用或禁用在控制器的https服务。默认情况下启用该接口。一旦禁用，端口(TCP 443)不会可及的。
- **设置snmp版本v1|v2|v3 enable (event)|禁用**—这启用或禁用SNMP服务特定版本在控制器的。您需要禁用所有防止对控制器的SNMP访问，除非曾经ACL。
- **设置网络mgmt通过无线enable (event)|禁用**—这防止客户端关联对此控制器能访问管理协议对它(SSH、https等等)。这不从无线设备角度看防止也不关闭TCP对应的端口。这意味着无线设备，当这设置禁用时，能打开SSH连接，如果协议启用。用户也许发现SSH守护程序生成的用户名提示，然而会话关闭，当您尝试键入用户名。
- **设置网络mgmt通过动态接口enable (event)|禁用**—这防止在VLAN的设备和控制器一样能访问管理协议对它(SSH、https等等)对在该VLAN的对应的动态接口地址。这不从设备角度看防止也不关闭TCP对应的端口。这意味着设备，当这设置禁用时，能打开SSH连接，如果协议启用。用户也许发现SSH守护程序生成的用户名提示，然而会话关闭，当您尝试键入用户名。另外，除非CPU ACL在地方，管理地址永远将依然是可访问从动态接口VLAN。

例如，使用上述信息，这是配置：

```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled
```

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................. NOT CONFIGURED
Wireless Traffic.......................... Disabled
Wired Traffic............................. Disabled
```

您能认为， ：

- Telnet和HTTP不会是可用的，因此对控制器的所有交互管理数据流通过HTTPS/SSH将被执行(加密)。
- 无线用户关联对此控制器不能获得管理访问。
- 如果无线用户，关联对此控制器，执行端口扫描， show SSH和HTTP如开放，即使管理访问没有允许。
- 如果一个有线的用户(VLAN和动态接口一样)执行端口扫描， show SSH和HTTP如开放，即使管理访问没有允许。

请注意在环境用超过在同样移动组的一个控制器，什么的关系是无线客户端仅是到当前相关的控制器。所以，如果一个客户端关联到控制器A，然后对于在同样移动组的一个控制器B，此客户端是来自VLAN/dynamic接口的设备。这是重要考虑到在无线设置的管理。在哪里请参阅此图表关于示例放置流量限制，并且什么命令能影响每个进入点：

CPU ACL

每当设备能与主CPU谈的您要控制，使用CPU ACL。提及这些的几种特性是重要的：

- CPU往CPU的ACL过滤数据流和没有CPU退出或生成的仅任何流量。**注意：** 对于WLC 5500系列在版本6.0和以上， CPU ACL为于WLC起源的流量是可适用的。对于其他WLC平台，此行为在版本7.0和以上实现。并且，当创建CPU ACL方向时字段没有任何影响。
- CPU ACL的完全支持所有控制器IP管理和动态地址的只存在4.2.130.0和以后。
- CPU ACL阻塞服务端口流量只是存在5.0及以上版本。
- 当CPU ACL设计时，允许控制器之间的控制流量是重要的。**嘘规则**命令能提供流量一张快速视图允许对在正常情况的CPU ACL。
- 控制器有一套内部进程的过滤规则，可以用**嘘规则**命令检查。ACL不影响这些规则，亦不可能正在进行中修改这些规则。CPU ACL优先于他们。
- LWAPP或CAPWAP数据流没有受在4400个基于控制器的CPU ACL规则的影响，控制流量受影响(如果执行严格ACL，您需要明确地允许它)。**注意：** CAPWAP控制流量没有影响的是受CPU ACL的。

示例

例如，您也许要阻塞来自动态接口/VLAN (192.168.20.0/24)的所有流量用户关联，往CPU的地方，但是其他流量允许。这不应该防止无线客户端得到DHCP协商得到的地址。

1. 作为第一步，访问列表创建：
2. 单击**添加新规则**，并且设置它阻塞来自192.168.20.0/24的所有源数据流到所有目的地。
3. 增加第二个规则， DHCP流量的，用目标服务器端口，但是与permit操作：然后，每公司安全策略，其他流量允许：

测试在CPU ACL前

为了验证CPU ACL的效果，您可执行从一个相关的无线客户端的一快速扫描RAN状态的为了根据配

置发现当前开放端口，在应用CPU ACL前：

测试在CPU ACL以后

去**安全> Management> CPU访问控制表**。点击**Enable (event) CPU ACL**，并且选择以前创建的ACL。然后，请从在动态接口VLAN的其它设备选择**两个，**方向为了确保此应用对从无线客户端的流量，和：

注意： 向前没有cpu ACL流量的方向从仅7.0所有WLC平台的和在6.0的WLC5500的。

现在，如果同样扫描使用前面被重复，控制器的所有端口显示如关闭：

严格CPU ACL

如果安全策略的需求“拒绝其中任一”作为策略的最后线路，请注意有几种流量类型发送在同样移动组的控制器RRM的，移动性和其他任务之间，并且您也许由控制器有流量被代理的到本身一些操作的，特别是DHCP，其中在DHCP代理模式(默认)的控制器能生成流量到本身与处理的目的地UDP 1067。

对于内部默认转发规则允许的端口完整列表，请检查**嘘规则**命令的输出。完整列表分析是超出本文的范围之外。

您能检查哪些ACL规则由与**start命令设置ACL的计数器的**流量点击。计数器可以用**嘘ACL详细信息ACLNAME**命令显示。

控制层面策略

保护网络设备的一个方面，是确保，没有淹没与能处理的更多管理数据流。在所有控制器上，在4.1编码后，默认情况下有启用的控制层面限制，起动，如果CPU的流量超出2 mbps。

在繁忙网络，是可能的观察实际上限制(例如，丢弃的监视器ping对CPU)。功能可以用**config advanced rate**命令控制。您能只启用或禁用它，但是没设置的速率或者哪个流量它首先将操作。

在正常操作，推荐这被离开已启用。

HTTPS流量的强加密

默认情况下，在HTTPS设置期间，控制器提供两高和低优点密码器确保兼容性用更老的浏览器。控制器有从40个位RC4的可得到， 56个比特DES，至AES 256比特。最强的密码器的选择由浏览器完成。

为了确保，使用仅强密码器，您能启用他们与**enable命令的config network secureweb cipher-option high**，那么仅168 3DES或128个AES和更高的密码器长度由HTTPS管理访问的控制器提供。

会话控制

Telnet/SSH设置

默认情况下，控制器允许最多5个并发用户，有5分钟超时的。非常重要的是这些值在您的环境足够

配置，因为设置他们对无限个(零)能打开门到潜在的拒绝服务控制器，如果用户将尝试暴力攻击他们。这是默认设置示例：

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

切记故意地，即使在无线或动态接口的管理禁用，设备能仍然建立对控制器的SSH联系。这是纳税任务的CPU，使用这些参数，并且WLC多久限制同步会话数量，和。

值可以调节与**sessions命令的设置**。

控制台端口

串行端口有被分离的超时值，默认情况下设置为5分钟，但是通常更改到0 (无限个)在故障排除过程期间。

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)..... 5
Baud Rate..................................... 9600
Character Size................................ 8
Flow Control:................................. Disable
Stop Bits..................................... 1
Parity Type:.................................. none
```

使用5分钟默认是可行的。万一控制台端口的一个登录用户打开会话，这防止访问的任何人物理访问控制器获得管理访问。值可以用**设置连续命令**调节。

汇集所有

在检查不同方面以后保护WLC，这能汇总：

- 防止设备除缩进的管理站之外访问WLC，不仅禁用的未使用的协议，而且通过限制在层与CPU ACL的4/layer 3的访问是重要的。
- 应该启用速率限制默认情况下(是)。
- 控制访问通过**在X**命令的**管理不**是足够为安全安装，用户仍然能访问管理协议谈直接地与管理IP地址，使用CPU和内存资源。

安全做法

这是某些安全实践：

- 创建下降访问的CPU ACL从所有动态接口VLAN或子网。然而，请允许DHCP流量到服务器端口(67)，因此客户端能得到DHCP协商得到的地址，如果DHCP代理启用默认情况下(是)。如果动态接口有一公网IP地址，推荐有拒绝从未知源的ACL规则所有流量到动态接口地址。
- 设置所有ACL规则一样入站或与方向其中**任一**，并且标记他们象应用作为**两个**(配线和Wireless选项)。如何验证：`(Cisco Controller) >show acl cpu`

  ```
  CPU Acl Name.................................. acl1
  Wireless Traffic.............................. Enabled
  Wired Traffic................................. Enabled
  ```
- Enable (event)控制层面限制默认情况下(启用)。如何验证：`(Cisco Controller) >show advanced`

```
rate

Control Path Rate Limiting.....................  Enabled
```

- 总是请使用已加密管理协议(HTTPS， SSH)。这是交互管理的默认配置。对于您也许需要使V3允许已加密/的SNMP验证SNMP流量。如果做对SNMP配置的变动请切记重新加载控制器。这是如何验证：`(Cisco Controller) >show network summary`

```
RF-Network Name.............................. 4400
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High........... Enable
Secure Web Mode Cipher-Option SSLv2.......... Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Disable
...
```

- HTTPS的Enable (event)高加密默认情况下(这禁用)。
- 它是一个好想法设置HTTPS访问的一验证的服务器证书对您的控制器(签字由您的委托CA)默认情况下，替换安装的自签证书。
- 设置会话和控制台超时为5分钟。`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)......... 5
Baud Rate.................................... 9600
Character Size............................... 8
Flow Control:................................ Disable
Stop Bits.................................... 1
Parity Type:................................. none


(Cisco Controller) >show sessions

CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions......... 5
```

相关信息

- 轻量接入点常见问题
- 无线 LAN 控制器 (WLC) 故障排除常见问题
- Cisco 无线 LAN 控制器模块问题与解答
- 统一无线网络中的无线电资源管理
- 技术支持和文档 - Cisco Systems