

Cisco Unified无线网络协议和端口矩阵

Contents

[Introduction](#)

[背景信息](#)

[使用的术语](#)

[网络概述](#)

[协议和端口号信息](#)

[表1 - WCS/NCS/PI协议和端口](#)

[表2 - MSE - AwIPS协议](#)

[表3 - MSE -上下文协议](#)

[表4 - WLC协议](#)

[表5 - AP协议](#)

[表6 - OEAP600防火墙协议](#)

Introduction

本文提供关于在整个产品系列间和端口号的信息使用的协议，当他们在全面的Cisco Unified无线网络(CUWN)配置呼应。此信息根据软件版本7.0.220.0系列代码版本系列。在本文被创建了时候，此信息没有被认为替换或取代在现有配置指南找到的特定产品文档，但是只担当可用一个统一的信息源。

背景信息

本文的主要目的将提供合并一个CUWN解决方案通信协议的一个统一的来源。目标是实现适当的根据此信息的防火墙和安全策略适当地巩固CUWN基础设施。

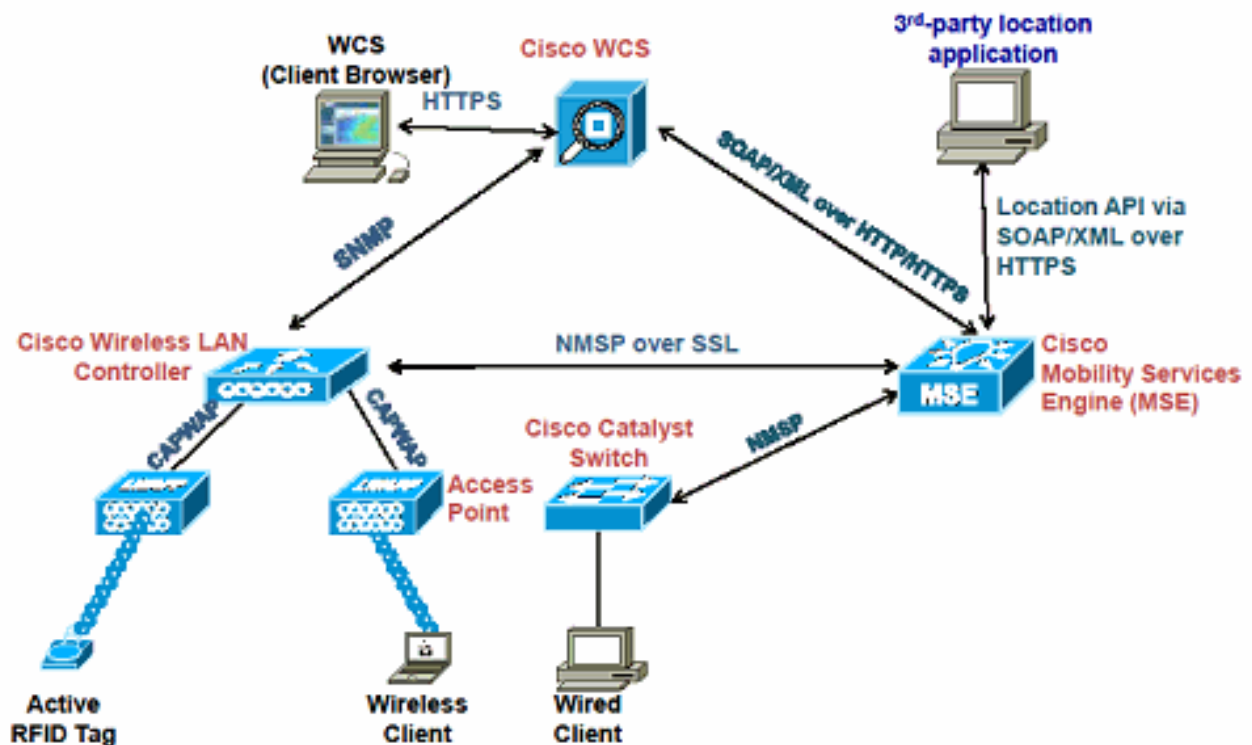
使用的术语

这是用于本文术语目录：

- WCS -无线控制系统
- NCS -网络控制系统
- PI -Cisco最初基础设施
- WLC -无线局域网控制器
- MSE -[移动服务引擎](#)
- OS -操作系统
- AP -接入点
- SSH -Secure Shell
- SMTP -简单邮件转发协议
- AAA -验证、授权和记帐
- DNS -域名系统
- ISE -[身份服务引擎](#)
- NTP -网络时间协议 (NTP)

- 肥皂-简单的对象访问协议
- HA -高可用性
- QoS -服务质量
- DB -数据库
- RDP -远程桌面协议
- VNC -虚拟网络计算
- TLS -传输层安全
- LOCP - Cisco位置控制协议
- ICMP -互联网控制消息协议
- SNMP -简单网络管理协议 (SNMP)
- NMSP -网络移动服务协议
- AwIPS -可适应的无线入侵防御系统
- EoIP -在IP的以太网
- RDLP -恶意位置发现协议
- CAPWAP -无线访问访问接入点控制和设置
- LWAPP -轻量级接入点协议
- NSI -网络光谱接口
- OEAP - OfficeExtend接入点

网络概述



协议和端口号信息

这是在本文的表列表：

- [表1 - WCS/NCS/PI协议](#)
- [表2 - MSE AwIPS协议](#)
- [表3 - MSE上下文协议](#)
- [表4 - WLC协议](#)
- [表5 - CAPWAP AP协议](#)
- [表6 - OEAP600防火墙协议](#)

表1 - WCS/NCS/PI协议和端口

WCS/NCS/PI协议

源设备	目的地设备	协议	目的地端口	说明
WCS/NCS/PI	WLC和MSE	TCP	21	FTP -用于调用到/从设备的文件
多种管理站	WCS主服务器OS Linux	TCP	22	SSH -使用远程Linux主机访问
WCS /NCS/PI	Cisco aIOS [®] AP	TCP	23	Telnet -使用Cisco aIOS AP配置
WCS /NCS/PI	SMTP邮件服务器	TCP	25	用于故障通知-的SMTP
AAA服务器/ISE	WCS /NCS/PI	TCP/UDP	49	TACACS+
WCS /NCS/PI	aIOS AP	UDP	53	用于Cisco aIOS AP配置-的DNS
WLC	WCS /NCS/PI	UDP	69	TFTP -用于调用到/从设备的文件
多种管理站	WCS /NCS/PI	TCP	80	HTTP (可配置在安装时间)
Ntp server	WLC	UDP	123	NTP
WLC和MSE	WCS /NCS/PI	UDP	161	SNMP发现，库存Cisco aIOS AP和其他
WLC和MSE	WCS /NCS/PI	UDP	162	SNMP陷阱接收器
多种管理站	WCS /NCS/PI	TCP	443	HTTPS (可配置在安装时间)
MSE	WCS /NCS/PI	TCP	443	SOAP/XML (用于MSE管理的肥皂)
WLC	WCS /NCS/PI	UDP	514	Syslog (可选)
仅本地	WCS /NCS/PI	TCP	1299	RMI注册端口(仅本地)
多种和HA服务器	WCS /NCS/PI	TCP	1315	数据库服务器HA (QoS)
WCS HA服务器	WCS /NCS/PI	TCP	1316-1320	HA DB端口
AAA服务器/ISE	WCS /NCS/PI	UDP	1812/1645	RADIUS
AAA服务器/ISE	WCS /NCS/PI	UDP	1813/1646	RADIUS
多种管理站	WCS主服务器OS Microsoft Windows	TCP/UDP	3389	RDP -微软视窗远程桌面(可选)
多种	WCS /NCS/PI	TCP	5001	Apache轴肥皂监控：Java监听程序
多种管理站	WCS主服务器OS Microsoft Windows	TCP	5500	用于远程微软视窗主机访问- (可选) VNC
多种管理站	WCS主服务器OS Microsoft Windows	TCP	5800	用于远程微软视窗主机访问- (可选) VNC
多种管理站	WCS主服务器OS Microsoft Windows	TCP/UDP	5900	用于远程微软视窗主机访问- (可选) VNC
仅本地	WCS /NCS/PI	TCP	6789	RMI服务器端口(仅本地)
MSE位置工具	WCS /NCS/PI	TCP	8001	位置服务器数据同步。通信端口

仅本地	WCS /NCS/PI	TCP	8005	Tomcat关闭端口
仅本地	WCS /NCS/PI	TCP	8009	Web服务器/Java服务器连接器(仅本
HA Web服务器	WCS /NCS/PI	TCP	8082	HA Web服务器端口 : WCS HA的侧
多种管理站	WCS /NCS/PI	TCP	8456	监控
多种管理站	WCS /NCS/PI	TCP	8457	HTTP 接口
多种管理站	WCS /NCS/PI	TCP	16113	HTTP重定向
WLC	WCS /NCS/PI	UDP	29001-29005	LOCP TLS端口
多种	AP	ICMP		TFTP儿童线程
		NMSP ,		ICMP -可选
		AoA ,	16113 , 2003年 ,	
WLC	CMX 10.2.X	80 ,	HTTP , HTTPS ,	
		443 ,	ICMP , SNMP	
		161,162		

表2 - MSE - AwIPS协议

MSE - AwIPS协议

源设备	目的地设备	协议	目的地端口	说明
WCS /NCS/PI	MSE	TCP	21	FTP -用于调用到/从设备的文件
多种管理站	MSE主服务器OS Linux	TCP	22	SSH -使用远程Linux主机访问
WCS /NCS/PI	MSE	TCP	80	HTTP (可配置在安装时间)
Ntp server	WLC	UDP	123	NTP
WCS /NCS/PI	MSE	UDP	161	SNMP
MSE	WCS /NCS/PI	UDP	162	SNMP陷阱接收器
WCS /NCS/PI	MSE	TCP	443	HTTPS (可配置在安装时间)
WCS /NCS/PI	MSE	TCP	443	SOAP/XML
WCS /NCS/PI	MSE	TCP	8001	HTTPS (可配置在安装时间)
WLC	MSE和光谱专家	TCP	16113	NMSP
多种	AP	ICMP		ICMP -可选

表3 - MSE - 上下文协议

MSE - 上下文意识和AwIPS协议

源设备	目的地设备	协议	目的地端口	说明
WCS /NCS/PI	MSE	TCP	21	FTP -用于调用到/从设备的文件
多种管理站	MSE主服务器OS Linux	TCP	22	SSH -使用远程Linux主机访问
WCS /NCS/PI	MSE	TCP	80	HTTP (可配置在安装时间)
Ntp server	WLC	UDP	123	NTP
WCS /NCS/PI	MSE	UDP	161	SNMP
MSE	WCS /NCS/PI	UDP	162	SNMP陷阱接收器
WCS /NCS/PI	MSE	TCP	443	HTTPS (可配置在安装时间)
WCS /NCS/PI	MSE	TCP	443	SOAP/XML
WCS /NCS/PI	MSE	TCP	8001	HTTPS (可配置在安装时间)
WLC和Catalyst LAN交换机	MSE和光谱专家	TCP	16113	NMSP
多种	AP	ICMP		ICMP -可选

表4 - WLC协议

WLC协议

源设备	目的地设备	协议	目的地端口	源端口	说明
WCS /NCS/PI	WLC	TCP	21	0:65535	FTP -用于调用到/从设备的文件

WCS和多种管理站	WLC	TCP	22	0:65535 SSH -使用远程管理(可选)
WCS和多种管理站	WLC	TCP	23	0:65535 Telnet -使用远程管理(可选)
AAA服务器/ISE	WLC	TCP/UDP	49	0:65535 TACACS+
WCS和多种管理站	WLC	UDP	69	0:65535 TFTP -用于调用到/从设备的文
多种管理站	WLC	TCP	80	0:65535 HTTP (可配置在安装时间)
WLC	WLC	TCP	91	0:65535
WLC移动组成员	WLC	EoIP IP协 议97	EoIP IP协议 97	0:65535 EoIP隧道-客户端锚点/通道流量
Ntp server	WLC	UDP	123	0:65535 NTP
WCS /NCS/PI	WLC	UDP	161	161 SNMP
WCS /NCS/PI	WLC	UDP	162	0:65535 SNMP陷阱接收器
多种管理站	WLC	TCP	443	0:65535 HTTPS (可配置在安装时间)
WLC和多种系统日志服务器	WLC	UDP	514	0:65535 Syslog (可选)
AAA服务器/ISE	WLC	UDP	1812/1645	0:65535 RADIUS
AAA服务器/ISE	WLC	UDP	1813/1646	0:65535 RADIUS
AP	WLC	UDP	6352	0:65535 RDLP
多种管理站(MSE , 光谱专家)	WLC	TCP	16113	0:65535 LOCP TLS端口NMSP
WLC	WLC	UDP	16666	16666 -非被巩固的移动性
WLC	WLC	UDP	16667	移动性-获取**在版本。5.2+删除
AP	WLC	UDP	5246-5247	0:65535 CAPWAP Ctl/数据
AP	WLC	UDP	5248	0:65535 CAPWAP Mcast。
AP	WLC	UDP	12222-12223	0:65535 LWAPP Ctl/数据
AP	WLC	UDP	12224	0:65535 LWAPP Mcast。
多种	AP	ICMP		ICMP -可选

表5 - AP协议

AP CAPWAP-LWAPP协议

源设备	目的地设备	协议	目的地端口	说明
多种	AP	UDP	69	用于远程代码更新-的TFTP
多种	AP	TCP	22	用于可选的远程故障排除访问-的SSH。可以是
多种	AP	TCP	23	用于可选的远程故障排除访问-的Telnet。可以是
AP	DNS服务器	TCP/UDP	53	DNS
AP	DHCP服务器	UDP	68	DHCP
AP	多种	UDP	514	Syslog -可配置的目的地。默认值是255.255.255
WLC	AP	UDP	1024 - 65535 *	CAPWAP Ctl/数据
WLC	AP	UDP	5248	CAPWAP Mcast。
AP	WLC	UDP	6352	RDLP
WLC	AP	UDP	12222-12223	LWAPP Ctl/数据
WLC	AP	UDP	12224	LWAPP Mcast。
AP	监控程序PC	TCP	37540 5GHz的2.4千兆赫 的37550	NSI协议为SE连接
多种	AP	ICMP		ICMP -可选

* - , 当AP加入WLC时, 任意端口号分配到从范围1024 - 65535的每个AP。只要AP被连接, WLC使用编号作为目的地端口CAPWAP Ctl/数据。

表6 - OEAP600防火墙协议

AP CAPWAP-LWAPP协议

源设备	目的地设备	协议	目的地端口	说明
WLC	AP	UDP	5246-5247	CAPWAP Ctl/数据

OfficeExtend AP in DMZ of Network

Sample Firewall Configuration

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 128.107.234.10 255.255.255.224
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host 128.107.234.14 eq 5246
access-list Outside extended permit udp any host 128.107.234.14 eq 5247
access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) 128.107.234.14 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

Note: The following ports need to be open on the firewall between the WLAN Controller and the 600 series: **CAPWAP UDP 5246 and 5247**