## 网络访问安全要求

应支持基于源IP地址（IPv4和IPv6）、目的IP地址（IPv4和IPv6）、IP Protocol/Next Header、源TCP/UDP端口、目的TCP/UDP端口接入控制。

集中控制型WLAN热点接入设备应支持以下防攻击要求，并及时自动告警给AP/AC网管；应支持配置AC、部分AP或全部AP启用以下功能，包括但不限于：

1. 支持ARP/ND合法性检测：对不合法的ARP报文丢弃；
2. 支持ARP/ND源抑制：限制同一个源发送的大量ARP报文；
3. 支持防ARP/ND欺骗：包括AP仿冒和用户仿冒；
4. 支持防MAC等手段攻击行为；
5. 支持防“中间人”手段攻击行为；
6. 应支持一定的防DoS攻击能力，防止系统受到流量攻击和表项资源攻击，如ICMP Flooding、ARP/ND Flooding、UDP Flooding攻击等；
7. 应支持防非法报文（包括：泛洪攻击报文、Spoofing攻击报文等）攻击能力。

应支持如下无线入侵检测（WIDS）功能：

1. 应支持“非法AP”、“干扰AP”和“合法AP”的判定策略和处理方式设置；应包括MAC地址、SSID、供应商等信息的判定策略；应支持对相应处理方式的设置；
2. 应支持对无线信道的扫描检测功能，建议不采用专用监听AP的方式；
3. 根据无线信道扫描的结果和预先设置的策略，将AP判定为“非法AP”、“干扰AP”和“合法AP”；可选支持根据预先设置的方式对“非法”AP的进一步处理；
4. 应在不影响用户接入及数据转发的情况下，支持根据指定SSID检测“钓鱼AP”（非本AC所管理的或所信任的且广播与指定SSID相同或相似的SSID的“非法AP”）的能力，并向AP/AC网管自动告警；通过AC指定部分AP或全部AP启用此功能，出厂默认配置为关闭；
5. 基于支持检测“钓鱼AP”能力基础上，支持压制“钓鱼AP”的能力，功能可配置。

还应支持以下安全要求：

1. 轻量级AP与AC分别建立管理隧道和业务隧道，其隧道应支持不加密和加密二种方式，并可配置；
2. 为了防范非法的DHCP服务器，建议支持DHCP Snooping功能；
3. 可选支持防端口扫描功能；
4. 可选支持本地安全日志存储和查看，并提供至少存储1000条安全日志的能力；
5. 可选支持P2P流量限制功能；
6. 可选支持自带防火墙功能；
7. 支持ND-Snooping安全特性；
8. WLAN热点接入设备应支持基于MAC地址的接入控制，包括黑名单和白名单；
9. AC应支持二层隔离功能。

安全要求

## 网络访问安全要求

WLAN热点接入设备应支持基于MAC地址的接入控制，包括黑名单和白名单。

## WLAN接入安全要求

WLAN热点接入设备应支持以下接入安全要求。

* + - * 1. 应同时支持WAPI和802.11i两种安全机制：

应支持WAPI、802.11i、不加密三种工作模式基于SSID的配置；

同一SSID可选同时支持不同的加密和认证方式(WAPI、802.11i和明文)，此功能的开启应可配置，默认为关闭；

当采用WAPI模式时，应支持GB 15629.11-2003和GB 15629.11-2003/XG1-2006标准，应支持ECC和SMS4算法；

当采用WAPI模式时，应支持CBWIPS-Z 010-2009《WAPI多信任证书实施技术》要求，即同时支持安装设备证书（AP证书，格式为PKCS12）、可信任的鉴别服务器公钥证书（AS证书）、颁发者公钥证书（CA证书，为中国电信WAPI二级根证书），并在安装证书过程具有安装成功和安装出错的提示信息；

当采用802.11i模式时，应支持PSK（Preshared Key）、IEEE 802.1X机制，应支持TKIP、CCMP算法，设备与认证服务器之间的协议应支持Radius。

* + - * 1. 应支持同一SSID下、不同SSID之间不同用户之间的二层隔离功能，包括对所有单播包、组播包和广播包同时隔离。集中控制型设备还应再支持以下情况的二层隔离功能：

1. 同一AP下的不同用户之间的二层隔离功能；
2. 同一AC不同AP下的不同用户之间的二层隔离功能。
   * + - 1. 如果支持用户侧以太网口，则用户侧的有线和无线网段之间应二层隔离。
         2. 应支持VPN（IPsec，PPTP，L2TP）透传功能。

## 无线入侵检测（WIDS）功能要求

应支持与AC配合实现如下无线入侵检测（WIDS）功能：

* + - * 1. 应支持“非法AP”、“干扰AP”和“合法AP”的判定策略和处理方式设置；应包括MAC地址、SSID、供应商等信息的判定策略；应支持对相应处理方式的设置；
        2. 应支持对无线信道的扫描检测功能，建议不采用专用监听AP的方式；
        3. 根据无线信道扫描的结果和预先设置的策略，将AP判定为“非法AP”、“干扰AP”和“合法AP”；可选支持根据预先设置的方式对“非法”AP的进一步处理；
        4. 应在不影响用户接入及数据转发的情况下，支持根据指定SSID检测“钓鱼AP”（非本AC所管理的或所信任的且广播与指定SSID相同或相似的SSID的“非法AP”）的能力，并向AP/AC网管自动告警；通过AC指定部分AP或全部AP启用此功能，出厂默认配置为关闭；

基于支持检测“钓鱼AP”能力基础上，支持抑制“钓鱼AP”的能力，功能可配置。