本地转发是否支持savi功能问题处理经验案例

wlan安全 张燃 2019-08-27 发表

组网及说明

无

问题描述

某局点现场是本地转发，采用psk加密，业务网段在核心交换机上，dhcp服务器旁挂核心，dhcp服务器上做了相关配置，只会给白名单里的终端动态分配ip地址，即不在白名单中的终端是不会通过dhcp的方式动态获取到地址。现场需求是即使黑客终端知道了密码，接入网络也不能ping通内网。

过程分析

首先，我们先来看看这个功能的说明。IP Source Guard功能用于对AP收到的报文进行过滤控制，以防止非法客户端的报文通过，从而限制了对网络资源的非法使用（比如非法客户端仿冒合法客户端IP接入网络），提高了无线网络的安全性。

对于使用IPv4地址的客户端，AP会监听客户端发送的ARP报文或者与DHCP服务器间交互的DHCPv4报文，从报文中获取到客户端的IP地址，并与客户端的MAC地址形成绑定表项。

对于使用IPv6地址的客户端，有以下两种方式可以形成绑定表项。

· DHCPv6方式：AP会监听客户端与DHCPv6服务器间交互的DHCPv6报文，从报文中获取到DHCPv6服务器为客户端分配的完整的IPv6地址，并与客户端的MAC地址形成绑定表项。如果从报文中获取到的是DHCPv6服务器为客户端分配的IPv6地址前缀，则无法与客户端的MAC地址形成绑定表项。

· ND（Neighbor Discovery，IPv6邻居发现）方式：AP会监听网络中的RA（Router Advertisement，路由器通告消息）、NS（Neighbor Solicitation，邻居请求消息）、NA（Neighbor Advertisement，邻居通告消息）报文，从报文中获取IPv6地址，并与客户端的MAC地址形成绑定表项。

开启IP Source Guard功能后，AP在收到客户端报文时，会查找IP源地址绑定表项，如果客户端发送报文的特征项（MAC地址+IP地址）与某个绑定表项匹配，则转发该报文，否则做丢弃处理。对于IPv4地址匹配的条件，还要求客户端使用的IP地址是通过DHCP方式获取的，才转发报文，否则做丢弃处理。

综上所述，savi功能的实现机制是：第一步：ap通过分析报文，学到sta的ip地址，并且会记录下来学地址的来源。比如：如果从arp中学到的，地址来源会记录成来自arp，如果是dhcp中学到的，来源会记录成dhcp；第二步：终端有流量通过时，AP上进行查表和判断，如果这个终端当前的地址来源不是dhcp，就不允许流量通过；如果来源是dhcp，则允许流量通过。

当然，我们的savi功能不控制准入，只控制流量。

实验室测试验证该功能：

实验一:手机终端通过dhcp server拿到地址20.20.20.3，这时如果我的电脑静态绑定该IP地址，仿冒我手机的地址，那么会报网络冲突。

但是如果我给电脑在接入SSID之前配置的是静态的IP地址为20.20.20.8，输入密码之后，那么在AC的probe视图下可以看到： （该电脑从来没有在AC上通过dhcp获取过地址）

```
[H3C-probe]dis sys int wlan client ip
  Current IPv4 address: 20.20.20.8 (source: ARP)
  Current IPv6 address: N/A
  History: N/A
  IPv6 prefix: N/A
```

此时的测试结果是：电脑无法ping通业务网关20.20.20.1.符合原理。

实验二：电脑先通过dhcp拿到一个地址（20.20.20.2）之后,断开WiFi之后（时间较短），再次手动配置一个静态IP（20.20.20.20），输入密码连入网络

```
[H3C-probe]dis sys int wlan client ip
  Current IPv4 address: 20.20.20.2 (source: DHCP)
  Current IPv6 address: N/A
  History: N/A
  IPv6 prefix: N/A
[H3C-probe]%Jul 17 08:21:37:960 2019 H3C STAMGR/6/STAMGR_CLIENT_OFFLINE: Client xxxxx went offline from BSS 80f6-2e4d-4780 with SSID qs on AP qs. State changed to Unauth. Reason:Received deauthentication message in Run state: reason code=1
[H3C-probe]%Jul 17 08:22:38:427 2019 H3C STAMGR/6/STAMGR_CLIENT_ONLINE: Client xxxxx went online from BSS 80f6-2e4d-4780 with SSID qs on AP qs. State changed to Run.
dis sys int wlan client ip
  Current IPv4 address: 20.20.20.20 (source: ARP)
  Current IPv6 address: N/A
  History:
```

20.20.20.2 (source: DHCP)
IPv6 prefix: N/A
测试结果：电脑不能ping通内网，符合原理。
实验三:电脑先通过dhcp拿到一个地址（20.20.20.3）之后,断开WiFi之后（断开较长时间），再次手动配置一个静态IP（20.20.20.3），输入密码连入网络
[H3C-probe]dis sys int wlan cli ip
Current IPv4 address: 20.20.20.3 (**source: DHCP)**
Current IPv6 address: N/A
History: N/A
IPv6 prefix: N/A
等待终端的漫游表项清除后，如下显示漫游表项已经清除。之后在手动配置地址20.20.20.3，进行测试。
[H3C]dis wlan mobility roam-track mac-address xxxxx
Mobility module0
Current entries: 0
BSSID Created at Online time AC IP address RID AP name
[H3C-probe]%Jul 17 13:56:48:675 2019 H3C STAMGR/6/STAMGR_CLIENT_ONLINE: Client xxxxxx went online from BSS 80f6-2e4d-4780 with SSID qs on AP qs. State changed to Run.
dis sys int wlan cli ip
Current IPv4 address: 20.20.20.3 **(source: ARP)**
Current IPv6 address: N/A
History: N/A
IPv6 prefix: N/A
这是看到表项的终端来源已经变成了ARP。此时结果为：电脑ping不通网关。符合原理。
在这里补充一下，为什么要断开时间较长，等待漫游表项清除（默认老化时间3分钟）。因为sta的dhcp表项跟漫游信息相关，老化时间和漫游是相同的，所以终端下线之后，如果在漫游表项老化时间内再次上线，则原来学到的地址会继承，如果sta下线超过一定时间，漫游表项已经老化，则就以全新学到的信息为准。

解决方法

savi功能和报文转发形式无关，本地转发下也会生效。