WX系列AC实现ADOS报文流量攻击防护的典型配置

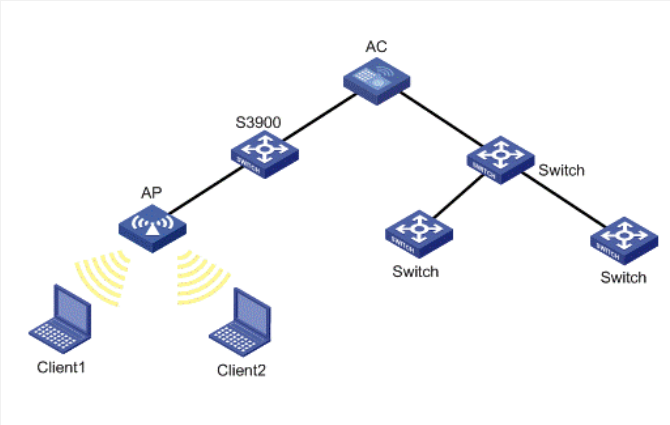
攻击检测及防范 **张利兵** 2012-07-19 发表

WX系列AC实现ADOS报文流量攻击防护的典型配置

一、组网需求

WX系列AC 1台、FIT AP、交换机、便携机2台（安装有无线网卡）

二、组网图



本配置举例中的AC使用的是WX5002无线控制器，AP使用的是WA2100无线局域网接入点。无线客户端Client1和Client2通过无线局域网络连到无线控制器AC上。

三、特性介绍

DoS（Denial of Service，拒绝服务）攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。针对DoS攻击采用下列处理流程进行防护：对各种报文依据相应的流量门限值进行测速。如果流量超限则将报文丢弃；否则根据管理协议报文为高优先级、用户数据报文为低优先级、其他应用协议报文为中优先级的分类原则将其送入软件优先级队列。管理协议报文包括：目的IP为本机的TELNET、SNMP、HTTP协议报文。其他协议报文包括：802.11 MAC管理、802.1X、ARP、DHCP、HWTACACS、ICMP、IGMP、MLD、LWAPP、ND、NTP、PIM、RADIUS。

ADOS功能用于防止正常的协议报文过多而对无线局域网络中的无线控制器AC进行访问，大量占用无线控制器AC的CPU的处理能力。同时ADOS功能用于防止限制业务报文的流量，避免某个业务流量占用大量的带宽，达到合理分配带宽的目的。ADOS报文流量攻击防护是专门针对协议报文目的地是无线控制器的攻击，访问目的地不是AC的协议报文不进行防护。业务报文攻击防护是指经由AC转发的业务报文，这类报文的防护没有访问的目的地的限制。在快转开启的情况下，ADOS攻击防护功能不起作用，所以需要关闭快转功能。ADOS攻击防护可能检测攻击来源的MAC，IP或是端口。

四、配置信息

```
[AC]display current-configuration
#
 version 5.00, ESS 1102
#
 sysname AC
#
 domain default enable system
#
undo l2fw fast-forwarding
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
```

```
 self-service-url disable
#
dhcp server ip-pool test
 network 1.1.1.0 mask 255.255.255.0
#
wlan radio-policy 1
#
wlan service-template 1 clear
 ssid TEST_AP1
 bind WLAN-ESS 1
 authentication-method open-system
 service-template enable
#
wlan rrm
 11a mandatory-rate 6 12 24
 11a supported-rate 9 18 36 48 54
 11b mandatory-rate 1 2
 11b supported-rate 5.5 11
 11g mandatory-rate 1 2 5.5 11
 11g supported-rate 6 9 12 18 24 36 48 54
#
interface NULL0
#
interface Vlan-interface1
ip address 1.1.1.250 255.255.255.0
#
interface GigabitEthernet1/0/1
#
interface GigabitEthernet1/0/2
#
interface M-Ethernet1/0/1
#
interface WLAN-ESS1
#
wlan ap test_ap1 model WA2100
 serial-id 210235A29G007C000020
 radio 1 type 11g
  radio-policy 1
  service-template 1
  radio enable
#
 dhcp enable
user-interface aux 0
user-interface vty 0 4
#
return
```

五、主要配置步骤

1、使能ADOS防攻击

```
system-view
[AC]anti-attack enable
```

2、取消快转使能后，ADOS防攻击才生效

```
[AC]undo l2fw fast-forwarding
```

3、配置AC的地址

```
[AC]interface vlan 1
[AC-Vlan-interface1]ip address 1.1.1.250 24
```

4、配置用户地址池

```
# 使能DHCP服务。
[AC]dhcp enable
# 创建名称为test的DHCP普通模式地址池。
[AC]dhcp server ip-pool test
# 配置DHCP地址池test动态分配的地址范围为1.1.1.0/24。
[AC-dhcp-pool-test]network 1.1.1.0  24
```

5、配置AP

```
# 创建clear类型的服务模板1。
```

[AC]wlan service-template 1 clear

设置当前服务模板的SSID（服务模板的标识）为test_ap1。

[AC-wlan-st-1]ssid test_ap1

设置无线客户端接入该无线服务（SSID）的认证方式为开放式系统认证。

[AC-wlan-st-1]authentication-method open-system

将WLAN-ESS1接口绑定到服务模板1。

[AC-wlan-st-1]bind WLAN-ESS 1

使能服务模板。

[AC-wlan-st-1]service-template enable

[AC-wlan-st-1]quit

创建一个名为1的射频策略。

[AC]wlan radio-policy 1

[AC-wlan-rp-1]quit

创建AP管理模板，其名称为test_ap1，型号名称这里选择WA2100。

[AC]wlan ap test_ap1 model wa2100

设置AP的序列号为210235A29G007C000020。

[AC-wlan-ap-test_ap1]serial-id 210235A29G007C000020

设置radio1的射频类型为802.11g。

[AC-wlan-ap-test_ap1]radio 1 type 11g

将在AC上配置的clear类型的服务模板1与射频1进行关联。

[AC-wlan-ap-test_ap1-radio-1]service-template 1

将射频策略1映射到射频1。

[AC-wlan-ap-test_ap1-radio-1]radio-policy 1

使能AP的radio 1。

[AC-wlan-ap-test_ap1-radio-1]radio enable

[AC-wlan-ap-test_ap1-radio-1]quit

[AC-wlan-ap-test_ap1]quit

六、验证结果

(1) 下面以几个比较典型的报文的攻击防护为例验证结果：

(2) AC在做了以上的配置后，正常情况下无ADOS攻击时的攻击统计。

[AC-ui-vty0]display anti-attack all

The number of total all attack packets is 0

The number of the lastest all attack sources in buffer is 0

Mac Ip Bssid Interface Time

---

(3) AC在收到超过了系统门限的管理报文后，ADOS功能监测到该攻击来于源IP地址是1.1.1.3，且丢掉了超过门限的包共1470个以及攻击发生的最新时间。

[AC]display anti-attack admin

The number of total admin attack packets is 1470

The number of the lastest admin attack sources in buffer is 1

Mac Ip Bssid Interface Time

1.1.1.3 05:12:33 02/12/2007

(4) AC的接口GigabitEthernet1/0/1在收到超过了系统门限的ICMP报文后的攻击防护统计：

[AC]dispaly anti-attack icmp

The number of total icmp attack packets is 376

The number of the lastest icmp attack sources in buffer is 1

Mac Ip Bssid Interface Time

GigabitEthernet1/0/1 05:24:56 02/12/2007

(5) AC收到超过了系统门限的ARP报文后的攻击防护统计：

[AC]dispaly anti-attack arp

The number of total arp attack packets is 191

The number of the lastest arp attack sources in buffer is 1

Mac Ip Bssid Interface Time

000f-e212-7700 05:28:54 02/12/2007

(6) AC收到超过了系统门限的802.1X报文后的攻击防护统计：

[AC]dispaly anti-attack dot1x

The number of total dot1x attack packets is 304

The number of the lastest dot1x attack sources in buffer is 1

Mac	Ip	Bssid	Interface	Time
000f-e212-7700				05:34:28 02/12/2007

(7) AC收到超过了系统门限的DHCP报文后的攻击防护统计：

[AC]dispaly anti-attack dhcp

The number of total dhcp attack packets is 1478

The number of the lastest dhcp attack sources in buffer is 3

Mac	Ip	Bssid	Interface	Time
000f-e212-5100				05:48:51 02/12/2007
000f-e2cc-0052				05:47:34 02/12/2007
000f-e212-7702				05:39:31 02/12/2007