S7502E侧挂方式下与CAMS配合实现Portal认证的配置

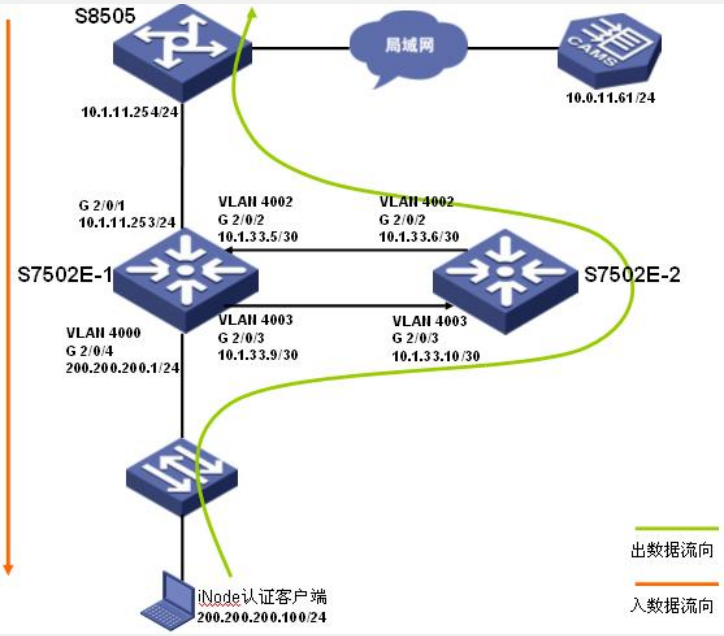
王涛1　2007-09-25 发表

S7502E侧挂方式下与CAMS配合实现Portal认证的配置

一、 组网需求：

7502E侧挂在汇聚层交换机上，对下联交换机上的终端用户启用Portal认证。此组网方式适用于某些旧网改造的场景，最大程度上减少对已有网络设备的调整，并且与802.1x认证不同，此方式下对接入层交换机型号没有限制，从而大大降低了用户的部署成本。

二、 组网图：



CAMS版本：2.10-R0208P02

S7502E版本：Version 5.20, Ess 6101L01

iNode版本：2.40-C0328

三、 配置步骤：

适用设备和版本：CAMS所有版本、S7502E Version 5.20, Ess 6101L01及以后所有版本。

1. 配置S7502E - 1

1) 配置重定向，将所有经过S7502E-1的流量重定向到S7502E-2

```
acl number 3000
 rule 0 permit ip
#
traffic classifier test operator and
 if-match acl 3000
#
traffic behavior test
 redirect next-hop 10.1.33.10
#
qos policy test
 classifier test behavior test
#
interface GigabitEthernet2/0/4
 port access vlan 4000
 description Test
 qos apply policy test inbound
```

2) 配置缺省路由

```
 ip route-static 0.0.0.0 0.0.0.0 10.1.11.254
```

3) 增加一条静态ARP配置，防止ARP老化导致流量重定向失败

```
 arp static 10.1.33.10 000f-e260-0062 4003 GigabitEthernet2/0/3
```

2. 配置S7502E - 2

1) 全局模式下配置Portal服务器相关信息
portal server cams ip 10.0.11.61 key cams url http://10.0.11.61/portal
2) 全局模式下将Portal Server的IP地址配置为Portal免认证用户
portal free-rule 0 source ip 10.0.11.61 mask 255.255.255.255 vlan 4003 destination any
3) 在连接用户的VLAN虚接口下使能Portal三层认证
interface Vlan-interface4003
 description To_S7502E-1_OUT
 ip address 10.1.33.10 255.255.255.252
 portal server cams method layer3
4) 配置Radius认证方案
radius scheme cams
 primary authentication 10.0.11.61
 primary accounting 10.0.11.61
 key authentication cams
 key accounting cams
 user-name-format without-domain
5) 配置认证域
domain cams
 authentication portal radius-scheme cams
 authorization portal radius-scheme cams
 accounting portal radius-scheme cams
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
6) 指定缺省认证域
domain default enable cams
7) 配置缺省路由
ip route-static 0.0.0.0 0.0.0.0 10.1.33.5
8) 配置用户网段的明细路由
ip route-static 200.200.200.0 255.255.255.0 10.1.33.9

3. 配置S8505

1) 配置静态路由
ip route-static 10.1.33.4 255.255.255.252 10.1.11.253 preference 60
ip route-static 10.1.33.8 255.255.255.252 10.1.11.253 preference 60
ip route-static 200.200.200.0 255.255.255.0 10.1.11.253 preference 60

4. 配置CAMS服务器

1) 配置接入设备

2) 配置IP地址组

3) 配置Portal设备信息，密钥务必与设备侧配置保持一致

4) 配置设备端口组

CAMS服务器上配置服务和开户的步骤这里不再详述。

四、 配置关键点：

1) S7502E-1上配置一条静态ARP，指定重定向下一跳地址的ARP信息，防止ARP老化导致流量重定向失败。

2) 在本案例的组网模式下，需要在Portal设备上全局模式下将Portal Server的IP地址配置为Portal免认证用户。

3) 虽然入数据流不经过S7502E-2，但S7502E-2上仍必须配置用户网段的路由，与CAMS服务器上指定用户认证的IP地址范围的概念类似。

4) CAMS服务器上增加Portal设备时，IP地址必须指定为使能Portal认证的VLAN虚接口的接口IP地址，这点与添加接入设备时配置IP地址为设备上行口（与Radius服务器最近的接口）地址不同。

5) 在本案例的组网模式下，S8505上必须配置两台S7502E互连的两个地址段的路由。因为在设备V5版本中，用于Portal协议通讯的设备侧地址不再是上行VLAN虚接口的地址，而是使能Portal认证的VLAN虚接口的地址。用于Radius协议通讯的设备侧地址还是上行VLAN虚接口的地址。以典型配置为例，10.1.33.8网段的路由用于Portal协议通讯，10.1.33.4网段的路由用于Radius协议的通讯。