Portal直接认证上下线过程简析

Portal　王森森　2013-05-06 发表

Portal直接认证上下线过程简析

一、Portal直接认证上下线过程可以分为四个阶段

1．客户端、接入设备之间的交互过程（HTTP重定向）

客户端访问任意IP地址（1.1.1.1）的目的网页，AC作为接入设备在配置了Portal认证的接口伪装成客户端想要访问的目的网页，并通过HTTP重定向将Portal服务器的认证页面返回客户端。客户端、接入设备、Portal服务器之间的交互过程（HTTP重定向）对应下图的HTTP-GET、HTTP重定向。

2．客户端、Portal服务器、接入设备之间的交互过程（认证前）

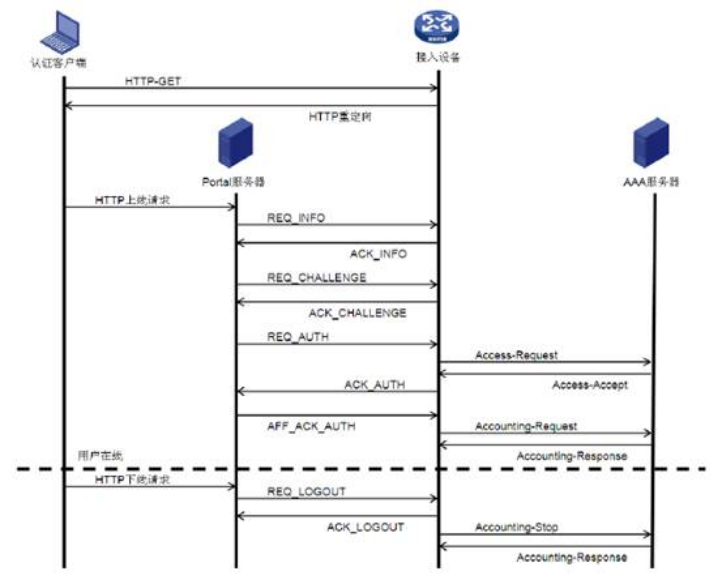
客户端访问重定向的Portal服务器认证页面，输入用户名和密码，通过点击上线提交用户名和密码给Portal服务器。Portal服务器通过与接入设备交互INFO报文获取客户端相关信息，Portal服务器通过与接入设备交互CHALLENGE报文协商用于CHAP加密的Challenge（Portal服务器采用CHAP认证方式的情况，采用PAP认证方式时没有此过程）。客户端、Portal服务器、接入设备之间的交互过程（认证前）对应下图的HTTP上线请求、REQ_INFO、ACK_INFO、REQ_CHALLENGE、ACK_CHALLENGE。

3．Portal服务器、接入设备、Radius服务器之间的交互过程（认证中）

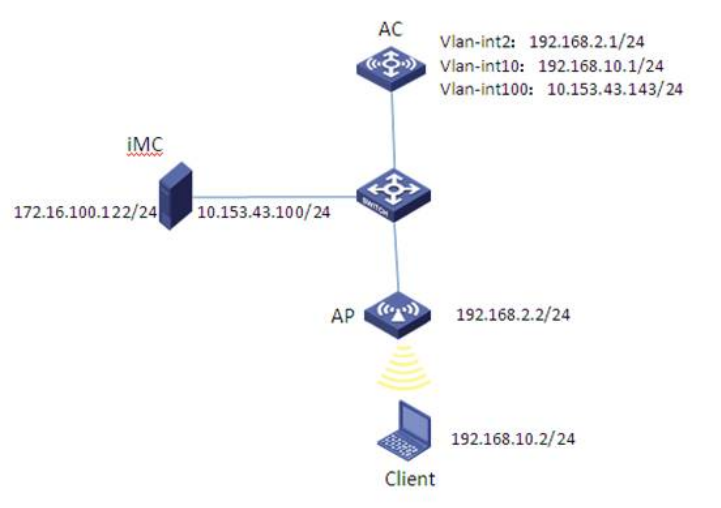
Portal服务器通过REQ_AUTH向接入设备发起认证，接入设备与Radius服务器进行通信，对用户信息进行认证，如果认证成功，接入设备回应Portal服务器ACK_AUTH告知客户端认证成功，Portal服务器通过AFF_ACK_AUTH对此再进行一次回应。最后，接入设备向Radius服务器发起计费开始过程。Portal服务器、接入设备、Radius服务器之间的交互过程（认证中）对应下图的REQ_AUTH、Access-Request、Access-Accept、ACK_AUTH、AFF_ACK_AUTH、Accouting- Request、Accouting- Response。

4．客户端、Portal服务器、接入设备、Radius服务器之间的交互过程（下线）

客户端通过点击下线将下线请求告知Portal服务器，Portal服务器通过REQ_LOGOUT向接入设备发送下线请求报文，接入设备通过ACK_LOGOUT进行回应。最后，接入设备向Radius服务器发起计费结束过程。客户端、Portal服务器、接入设备、Radius服务器之间的交互过程（下线）对应下图的HTTP下线请求、REQ_LOGOUT、ACK_LOGOUT、Accouting- Stop、Accouting- Response。



二、组网图



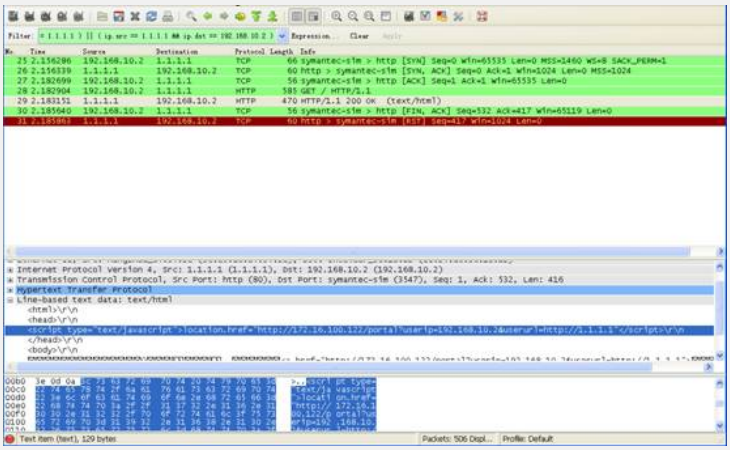
AC作为AP网关（Vlan-int2：192.168.2.1/24）和Client网关（Vlan-int10：192.168.10.1/24），设置互联地址（Vlan-int100：10.153.43.143/24）与iMC进行通信，iMC的IP地址172.16.100.122提供Portal服务和AAA服务。

三、抓包显示

AP采用本地转发，在Client网关开启Portal认证，在AC的有线口对一次Portal直接上下线过程进行抓包显示。

1．客户端、接入设备之间的交互过程（HTTP重定向）

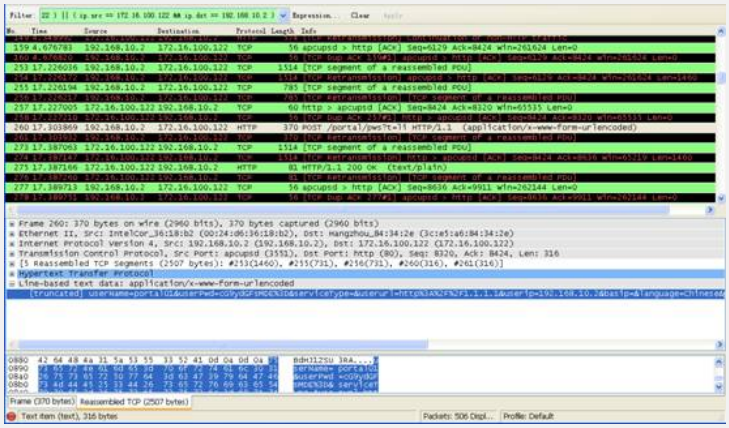
通过(ip.src == 192.168.10.2 && ip.dst == 1.1.1.1) || (ip.src == 1.1.1.1 && ip.dst == 192.168.10.2)对客户端与接入设备之间的交互报文进行过滤。



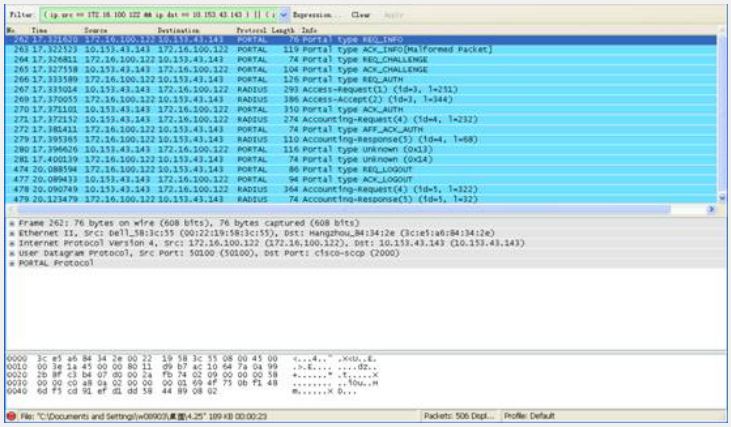
No.25、No.26、No.27为TCP三次握手建立连接的过程（配置了Portal 认证的接口会接受任何未上线客户端的 TCP连接，伪装成客户端想要访问的目的网页），No.28号报文显示客户端通过HTTP-GET试图访问1.1.1.1的页面内容，No.29号报文显示接入设备向客户端重定向Portal服务器的认证页面，报文中包含认证页面的URL信息，随后客户端对认证页面进行访问。

2．客户端、Portal服务器、接入设备之间的交互过程（认证前）

通过(ip.src == 192.168.10.2 && ip.dst == 172.16.100.122) || (ip.src == 172.16.100.122 && ip.dst == 192.168.10.2)对客户端与Portal服务器之间的交互报文进行过滤。



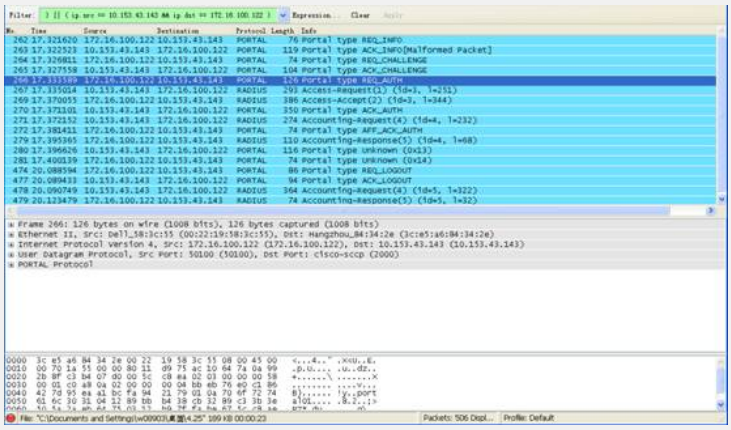
通过(ip.src == 172.16.100.122 && ip.dst == 10.153.43.143) || (ip.src == 10.153.43.143 && ip.dst == 172.16.100.122) 对Portal服务器与接入设备之间的交互报文进行过滤。



No.260号HTTP - POST报文显示客户端提交用户名和密码给Portal服务器，报文中包含客户端的用户名和密码信息。No.262为REQ_INFO报文（Portal服务器使用UDP端口50100，接入设备使用UDP端口2000），No.263为ACK_INFO报文，No.264为REQ_CHALLENGE报文，No.265为ACK_CHALLENGE报文。

3．Portal服务器、接入设备、Radius服务器之间的交互过程（认证中）

通过(ip.src == 172.16.100.122 && ip.dst == 10.153.43.143) || (ip.src == 10.153.43.143 && ip.dst == 172.16.100.122) 对Portal服务器与接入设备之间和接入设备与Radius服务器之间的交互报文进行过滤。

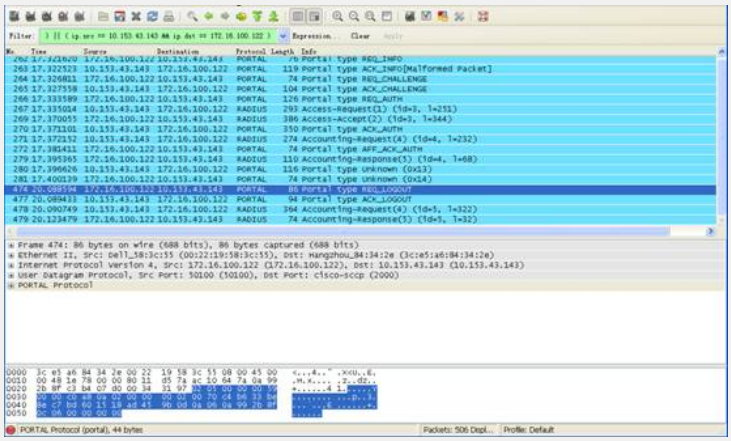


No.266号REQ_AUTH报文显示Portal服务器向接入设备发起认证，随后接入设备与Radius服务器进行Radius报文交互，No.267为Access-Request认证请求报文，No.269为Access-Accept认证接受报文，No.270为接入设备回应Portal服务器ACK_AUTH报文告知客户端认证成功，No.272为Portal服务器通过AFF_ACK_AUTH报文进行一次回应。No.271为Start类型（Acct-Status-Type=1）的Accounting-Request计费请求报文，No.279为Accounting-Response计费响应报文。

4．客户端、Portal服务器、接入设备、Radius服务器之间的交互过程（下线）

通过(ip.src == 172.16.100.122 && ip.dst == 10.153.43.143) || (ip.src == 10.153.43.143 && ip.dst == 172.16.100.122) 对Portal服务器与接入设备之间和接入

设备与Radius服务器之间的交互报文进行过滤。



No.474号REQ_LOGOUT报文显示客户端通过点击下线将下线请求告知Portal服务器后，Portal服务器向接入设备发送下线请求报文，No.477为接入设备通过ACK_LOGOUT报文进行回应。No.478为Stop类型（Acct-Status-Type=2）的Accounting-Request计费请求报文，No.479为Accounting-Response计费响应报文。

四、debugging显示

通过在AC上开启debugging：debugging portal tcp-cheat、debugging portal packet interface vlan10、debugging radius packet，对一次Portal直接上下线过程进行debugging显示。

1．客户端、接入设备之间的交互过程（HTTP重定向）

该阶段为debugging portal tcp-cheat显示，客户端（192.168.10.2）与接入设备（1.1.1.1）通过TCP三次握手建立连接过程：LISTEN-> SYN_RECVD->ESTABLISHED，随后客户端通过HTTP-GET访问1.1.1.1的页面内容时，接入设备向客户端重定向Portal服务器的认证页面，客户端对认证页面进行访问。

*Apr 18 15:01:41:519 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: Source MAC = 0024-d636-18b2

*Apr 18 15:01:41:549 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: A connection of c0a80a02 added!

*Apr 18 15:01:41:590 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 is LISTEN!

*Apr 18 15:01:41:610 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 changed from LISTEN to SYN_RECVD!

*Apr 18 15:01:41:660 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 is SYN_RECVD!

*Apr 18 15:01:41:680 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 changed from SYN_RECVD to ESTABLISHED!

*Apr 18 15:01:41:701 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 is ESTABLISHED!

2．客户端、Portal服务器、接入设备之间的交互过程（认证前）

该阶段为debugging portal packet interface vlan10显示。

Portal packet head:

Type:9 SN:96 ReqId:0 AttrNum:1 ErrCode:0 UserIP:192.168.10.2

//Portal服务器发送给接入设备的客户端IP地址为192.168.10.2的REQ_INFO报文（Type:9）。

Portal packet head:

Type:10 SN:96 ReqId:0 AttrNum:3 ErrCode:0 UserIP:192.168.10.2

//接入设备发送给Portal服务器的客户端IP地址为192.168.10.2的ACK_INFO报文（Type:10）。

Portal packet head:

Type:1 SN:96 ReqId:0 AttrNum:0 ErrCode:0 UserIP:192.168.10.2

//Portal服务器发送给接入设备的客户端IP地址为192.168.10.2的REQ_CHALLENGE

报文（Type:1）。

Portal packet head:

Type:2 SN:96 ReqId:3 AttrNum:3 ErrCode:0 UserIP:192.168.10.2

//接入设备发送给Portal服务器的客户端IP地址为192.168.10.2的ACK_CHALLENGE报文（Type:2）。

3．Portal服务器、接入设备、Radius服务器之间的交互过程（认证中）

该阶段为debugging portal packet interface vlan10、debugging radius packet显示。

Portal packet head:

Type:3 SN:96 ReqId:3 AttrNum:4 ErrCode:0 UserIP:192.168.10.2

//Portal服务器发送给接入设备的客户端IP地址为192.168.10.2的REQ_AUTH报文（Type:3）。

[1 User-name] [10] [portal01]

*Apr 18 15:01:54:989 2014 AC RDS/7/DEBUG: Send: IP=[172.16.100.122], UserIndex=[3], ID=[10], RetryTimes=[0], Code=[1], Length=[251]

//接入设备发送给Radius服务器的用户名为portal01的Access-Request认证请求报文（Code=[1]）。

[1 User-name] [10] [portal01]

*Apr 18 15:01:55:372 2014 AC RDS/7/DEBUG: Receive:IP=[172.16.100.122],Code=[2],Length=[344]

//Radius服务器发送给接入设备的用户名为portal01的Access-Accept认证接受报文（Code=[2]）。

Portal packet head:

Type:4 SN:96 ReqId:3 AttrNum:5 ErrCode:0 UserIP:192.168.10.2

//接入设备发送给Portal服务器的客户端IP地址为192.168.10.2的ACK_AUTH报文（Type:4）。

Portal packet head:

Type:7 SN:96 ReqId:3 AttrNum:0 ErrCode:0 UserIP:192.168.10.2

//Portal服务器发送给接入设备的客户端IP地址为192.168.10.2的AFF_ACK_AUTH报文（Type:7）。

[1 User-name] [10] [portal01]

[40 Acct-Status-Type] [6] [1]

*Apr 18 15:01:55:845 2014 AC RDS/7/DEBUG: Send: IP=[172.16.100.122], UserIndex=[3], ID=[11], RetryTimes=[0], Code=[4], Length=[232]

//接入设备发送给Radius服务器的用户名为portal01的Start类型（Acct-Status-Type=1）的Accounting-Request计费请求报文（Code=[4]）。

*Apr 18 15:01:56:117 2014 AC RDS/7/DEBUG: Receive:IP=[172.16.100.122],Code=[5],Length=[68]

//Radius服务器发送给接入设备的Accounting-Response计费响应报文（Code=[5]）。

4．客户端、Portal服务器、接入设备、Radius服务器之间的交互过程（下线）

该阶段为debugging portal packet interface vlan10、debugging radius packet显示。

Portal packet head:

Type:5 SN:97 ReqId:0 AttrNum:2 ErrCode:0 UserIP:192.168.10.2

//Portal服务器发送给接入设备的客户端IP地址为192.168.10.2的REQ_LOGOUT报文（Type:5）。

Portal packet head:

Type:6 SN:97 ReqId:0 AttrNum:3 ErrCode:0 UserIP:192.168.10.2

//接入设备发送给Portal服务器的客户端IP地址为192.168.10.2的ACK_LOGOUT报文（Type:6）。

[1 User-name] [10] [portal01]

[40 Acct-Status-Type] [6] [2]

*Apr 18 15:02:25:524 2014 AC RDS/7/DEBUG: Send: IP=[172.16.100.122], UserIndex=[3], ID=[12], RetryTimes=[0], Code=[4], Length=[322]

//接入设备发送给Radius服务器的用户名为portal01的Stop类型（Acct-Status-Type=2）的Accounting-Request计费请求报文（Code=[4]）。

*Apr 18 15:02:25:765 2014 AC RDS/7/DEBUG: Receive:IP=[172.16.100.122],Code=[5],Length=[32]

//Radius服务器发送给接入设备的Accounting-Response计费响应报文（Code=[5]）。

备注:

关于详细的Portal直接认证上下线过程的分析请见协议案例中的“协议案例集（2011年度）”。