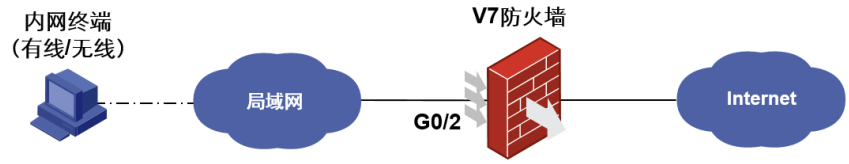
F1000系列V7防火墙跨三层组网下本地portal本地认证配置经验案例

Portal认证 徐猛 2018-09-11 发表

组网及说明

现场使用我司的一台F1000系列防火墙作为网络出口设备。设备上的GigabitEthernet 1/0/1作为内网连接接口，GigabitEthernet 1/0/2作为外网出口。内网中存在有线用户和无线用户，其中有线用户和无线用户的网关都在内网核心交换机上，终端到防火墙内网口之间跨了三层网络。 现场之前仅仅只对无线用户配置了portal认证，无线用户的portal认证点配置在了无线控制器上，之前使用正常。现在现场客户提出了需要对有线用户也做portal认证的需求。如下为现场拓扑，其中2口ip地址为：192.168.1.1。



配置步骤

1. 配置步骤

1） 上网基本配置（省略）

2） 创建portal web服务器，配置portal服务器的url地址为http://192.168.1.1:3000/portal

```
<H3C>system-view
[H3C]portal web-server h3c   //创建portal web服务器名称为h3c
[H3C-portal-websvr-h3c]url http://192.168.1.1:3000/portal   //配置portal认证重定向的url地址
[H3C-portal-websvr-h3c]quit
```

3） 开启IPV4 portal认证，指定为本地认证（需要在三层接口下启用）

```
[H3C]interface GigabitEthernet 0/2
[H3C-GigabitEthernet0/2]portal enable method layer3  //使能portal认证方式为跨三层portal认证
[H3C-GigabitEthernet0/2]portal apply web-server h3c  //引用之前创建的portal web服务器h3c
[H3C-GigabitEthernet0/2]quit
```

4） 创建本地portal web 服务器使用http协议交互认证信息

```
[H3C]portal local-web-server http
[H3C-portal-local-websvr-http]tcp-port 3000  //配置本地Portal Web服务器的HTTP服务侦听的TCP端口号为3000（注意要与前面配置的url地址对应上）
[H3C-portal-local-websvr-http]default-logon-page 123.zip  //配置本地Portal Web服务器提供的缺省认证页面文件（注意认证页面文件需放在设备根目录下）
[H3C-portal-local-websvr-http]quit
```

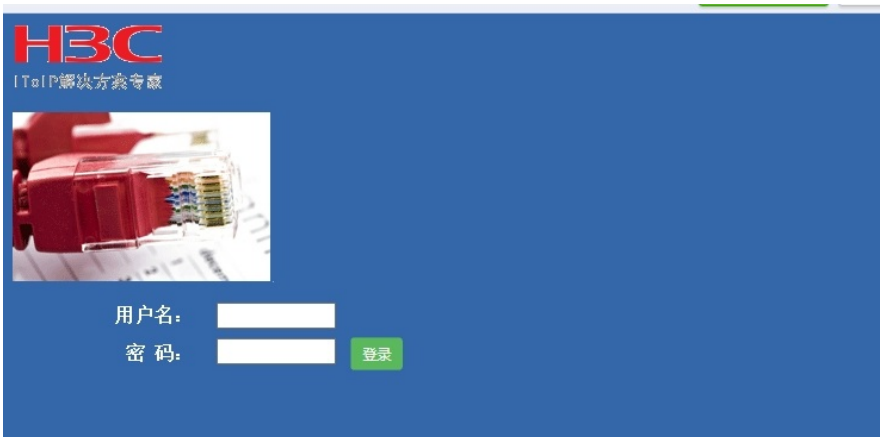
5） 创建本地的认证账户信息

```
[H3C]local-user h3c class network      //创建账号为h3c
[H3C-luser-network-h3c]service-type portal   //服务类型配置为portal
[H3C-luser-network-h3c]password  simple h3c   //创建密码为h3c
[H3C-luser-network-h3c]authorization-attribute user-role level-15
[H3C-luser-network-h3c]quit
```

6） 配置放通DNS的Portal策略

```
[H3C]portal free-rule 1 destination ip 114.114.114.114 32
```

2. 配置验证：portal页面正常弹出，输入用户名密码即可完成认证



配置关键点

如果在终端的网关交换机上配置portal的话，就在终端网关的三层接口上使能portal认证，并配置portal认证方式为直接认证方式即可：

[H3C-GigabitEthernet0/2]portal enable method direct //**使能portal认证方式为直接认证方式**

如果是跨了三层，使用上联的防火墙作为portal认证点，就在防火墙的内联接口上使能portal的时候，配置portal认证方式为可跨三层的认证方式：

[Sysname-GigabitEthernet0/2] portal enable method **layer3** //**layer3：可跨三层认证方式（本案例中采用的该方式）**

另外上述案例是使用缺省认证域的，缺省认证域的认证方案默认是本地的。现场设备如果没有配置其他域参数，可以直接使用上述案例进行快速配置。

如果现场配置使用的自定义其他认证域，后续注意修改配置：

（1）配置认证域

 # 创建并进入名称为dm1的ISP域。

[Device] domain dm1

 # 配置ISP域使用的RADIUS方案rs1。

[Device-isp-dm1] authentication portal local

[Device-isp-dm1] authorization portal local

[Device-isp-dm1] accounting portal local

[Device-isp-dm1] quit

（2）配置缺省域下的认证方案：

[Device] domain default enable dm1

如果不指定该域为缺省认证域，也可以在接口下指定portal认证使用的认证域：

[interface]portal domain dm1