

403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载
CyberArticle。注册版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。点击[这里](#)下载
CyberArticle。注册版本不会显示该信息。 [删除广告](#)

本电子书由CyberArticle制作。点击[这里](#)下载
CyberArticle。注册版本不会显示该信息。 [删除广告](#)

V7防火墙使用默认证书配置 SSL VPN IP资源典型案例 (命令行配置)

目录

[V7防火墙使用默认证书配置SSL VPN IP资源典型案例（命令行配置）](#)

[1 配置需求及说明](#)

[1.1 适用的产品系列](#)

[1.2 配置需求及实现的效果](#)

[2 组网图](#)

[3 配置步骤](#)

[3.1 防火墙上网配置](#)

[3.2 配置SSL VPN网关](#)

[3.3 配置SSL VPN实例](#)

[3.4 新建SSL VPN用户，关联SSLVPN资源组](#)

[3.5 将SSL VPN端口加入安全域，放通对应安全策略](#)

[3.6 保存配置](#)

[3.7 配置验证，查看拨号成功的用户](#)

[4 注意事项](#)

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：
F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

*注：本案例是在F1000-C-G2的Version 7.1.064,
Release 9323P19版本上进行配置和验证的。*

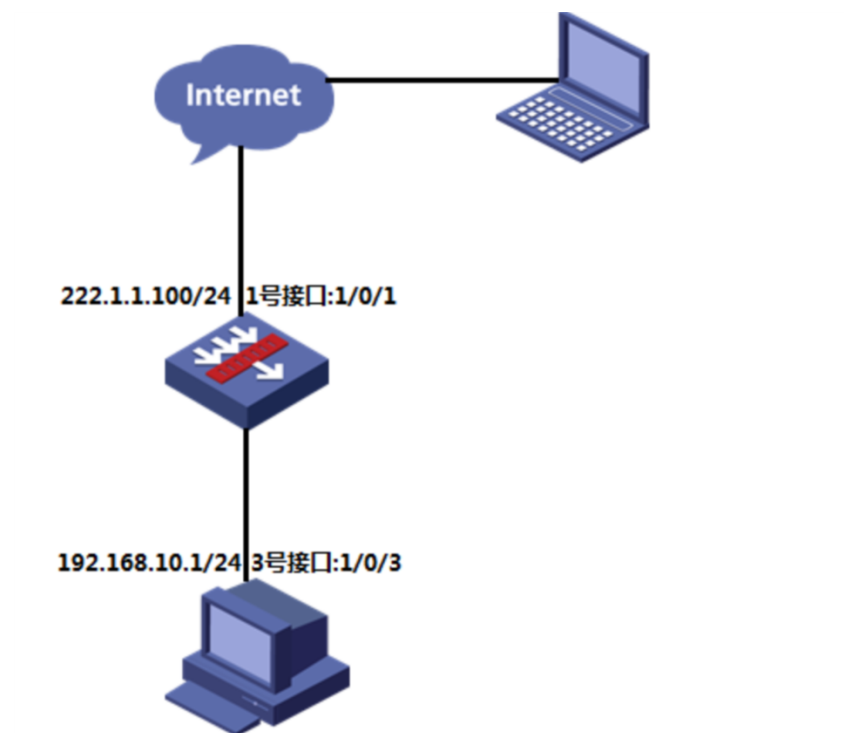
1.2 配置需求及实现的效果

V7防火墙设备作为出口设备，外网PC通过inode软件拨SSLVPN，认证成功后可以访问内网192.168.10.0网段的资源。IP地址及接口规划如下表所示：

外网接	公网地址/掩	内网接	内网地址/掩

口	码	口	码
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24

2 组网图



3 配置步骤

3.1 防火墙上网配置

防火墙上网配置请参考“2.2.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对SSLVPN配置

进行介绍。

3.2 配置SSL VPN网关

#SSLVPN 网关 IP 地址填写防火墙 1 口地址 222.1.1.1.00，端口号修改为4433，缺省端口为443，443端口和https端口冲突，然后使能网关配置。

```
<H3C>sys
```

```
[H3C]sslvpn gateway SSLVPNGW
```

```
[H3C-sslvpn-gateway-SSLVPNGW]ip address
```

```
222.1.1.100 port 4433
```

```
[H3C-sslvpn-gateway-SSLVPNGW]service
```

```
enable
```

```
[H3C-sslvpn-gateway-SSLVPNGW]quit
```

#创建SSL VPN AC接口1,配置接口IP为10.10.10.1/24

```
[H3C]interface SSLVPN-AC 1
```

```
[H3C-SSLVPN-AC1] ip address 10.10.10.1
```

```
255.255.255.0
```

```
[H3C-SSLVPN-AC1]quit
```

#创建地址池名称为“SSLPOOL”，指定IP地址范围为10.10.10.2——10.10.10.254

```
[H3C]sslvpn ip address-pool SSLPOOL
```

```
10.10.10.2 10.10.10.254

#创建ACL 3999，允许SSL VPN用户访问的内网资源
192.168.10.0/24网段
[H3C]acl advanced 3999

[H3C-acl-ipv4-adv-3999]rule      permit      ip
destination 192.168.10.0 0.0.0.255

[H3C-acl-ipv4-adv-3999]quit
```

3.3 配置SSL VPN实例

配置SSL VPN访问实例“SSLVPNSL” 引用SSL VPN
网关“SSLVPNGW”

```
[H3C] sslvpn context SSLVPN

[H3C-sslvpn-context-SSLVPN]gateway
SSLVPNGW
```

#引用SSL VPN接口1

```
[H3C-sslvpn-context-SSLVPN]      ip-tunnel

interface SSLVPN-AC1
```

#引用SSL VPN地址池，掩码和dns

```
[H3C-sslvpn-context-SSLVPN]ip-tunnel
address-pool SSLPOOL mask 255.255.255.0

[H3C-sslvpn-context-SSLVPN]ip-tunnel
```

```
dns-server primary 114.114.114.114
```

**# 创建路由列表“NEIWANG”，添加路由表项
192.168.10.0/24**

```
[H3C-sslvpn-context-SSLVPN] ip-route-  
list NEIWANG
```

```
[H3C-sslvpn-context-SSLVPN-route-list-  
NEIWANG] include 192.168.10.0  
255.255.255.0
```

创建SSL VPN策略组“SSLVPNZIYUAN”，引用路由列表“NEIWANG”，配置ACL限制，只有通过ACL检查的报文才可以访问IP资源

```
[H3C-sslvpn-context-SSLVPN] policy-group  
SSLVPNZIYUAN
```

```
[H3C-sslvpn-context-SSLVPN-policy-group-  
SSLVPNZIYUAN]filter ip-tunnel acl 3999
```

```
[H3C-sslvpn-context-SSLVPN-policy-group-  
SSLVPNZIYUAN]ip-tunnel access-route ip-  
route-list NEIWANG
```

```
[H3C-sslvpn-context-SSLVPN-policy-group-  
SSLVPNZIYUAN]quit
```

```
[H3C-sslvpn-context-SSLVPN]          service
enable

[H3C-sslvpn-context-SSLVPN]quit
```

3.4 新建SSL VPN用户，关联SSLVPN资源组

#创建SSLVPN本地用户,配置用户名密码user1,服务类型sslvpn，引用之前创建的SSLVPN资源组

```
[H3C]local-user user1 class network

[H3C-luser-network-user1]password simple
user1

[H3C-luser-network-user1]service-type
sslvpn

[H3C-luser-network-user1]authorization-
attribute          sslvpn-policy-group
SSLVPNZIYUAN

[H3C-luser-network-user1]quit
```

3.5 将SSL VPN端口加入安全域，放通对应安全策略

#新建安全域，名称为“SSLVPN”，将SSL VPN端口

1加入到安全域“SSLVPN”

```
[H3C]security-zone name SSLVPN

[H3C-security-zone-SSLVPN]import
interface SSLVPN-AC1

[H3C-security-zone-SSLVPN]quit

#创建服务对象组，组名称为4433，匹配SSLVPN端

[H3C]object-group service 4433

[H3C-obj-grp-service-4433]service      tcp
destination eq 4433

[H3C-obj-grp-service-4433]quit

#配置配置安全策略将Untrust到Local域目的端口为
TCP4433端口放通

[H3C]security-policy ip

[H3C-security-policy-ip]rule      5      name
Untrst-Local

[H3C-security-policy-ip-5-Untrst-Local]
action pass

[H3C-security-policy-ip-5-Untrst-Local]
source-zone Untrust

[H3C-security-policy-ip-5-Untrst-Local]
```



```
destination-zone Local
```

```
[H3C-security-policy-ip-5-Untrst-Local]
```

```
service 4433
```

```
[H3C-security-policy-ip-5-Untrst-Local]
```

```
quit
```

#配置配置安全策略,放通源安全域为SSLVPN, 目前安全域为“Trust”的数据流量

```
[H3C-security-policy-ip]rule 10 name
```

```
SSLVPN-Trust
```

```
[H3C-security-policy-ip-10-SSLVPN-Trust]
```

```
action pass
```

```
[H3C-security-policy-ip-10-SSLVPN-Trust]
```

```
source-zone SSLVPN
```

```
[H3C-security-policy-ip-10-SSLVPN-Trust]
```

```
destination-zone Trust
```

```
[H3C-security-policy-ip-10-SSLVPN-Trust]
```

```
quit
```

3.6 保存配置

```
save force
```

3.7 配置验证，查看拨号成功的用户

```
<H3C>dis sslvpn session verbose
```

```
User                : user1
Context             : SSLVPN
Policy group        : SSLVPNZHIYUAN
Idle timeout        : 30 min
Created at          : 18:16:02 UTC Sun
08/26/2018
Lastest             : 18:32:32 UTC Sun
08/26/2018
User IPv4 address   : 222.1.1.99
Alloced IP          : 10.10.10.2
Session ID          : 3
Web browser/OS      : Windows
```

4 注意事项

1、本案例适应的是默认证书，不需要手工导入CA证书和本地正常

2、不需要配置SSL服务器端策略，SSLVPN网关不需要引用SSL服务器端策略