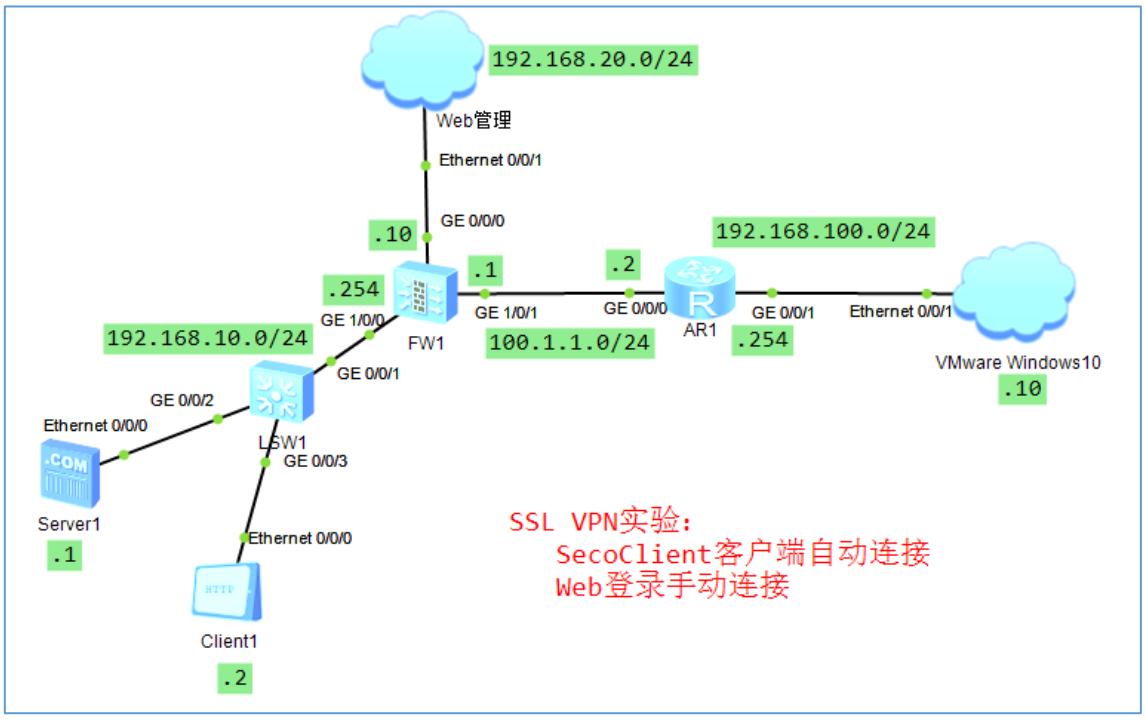
华为 eNSP USG6000V 实现 SSL VPN

摘要：

IPSEC VPN可以实现不同局域网之间通过Internet进行VPN连接，一般由网关设备进行VPN连接。

SSL VPN 可以实现员工到公司内部，由员工电脑进行 VPN 连接。一般由员工 Web 登录虚拟机网关手动连接，或由 SecoClient 客户端自动连接。

本案例以华为 eNSP USG6000V 设备实现 SSL VPN，网络拓扑如下：



一、基本配置

1. 防火基本配置脚本参考

admin
Admin@123
y
Admin@123
admin@123
admin@123

u t m
sys
sysn FW1
web-m time 60
user con 0
idl 60

```
ret
sys
int g0/0/0
ip add 192.168.20.10 24
serv ena
serv https per
serv ping per
ret
```

2. **路由器基本配置**

```
#
interface GigabitEthernet0/0/0
 ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.100.254 255.255.255.0
#
```

3. **登录防火墙**

https://192.168.20.10:8443

4. **配置防火墙接口**

5. **配置路由**

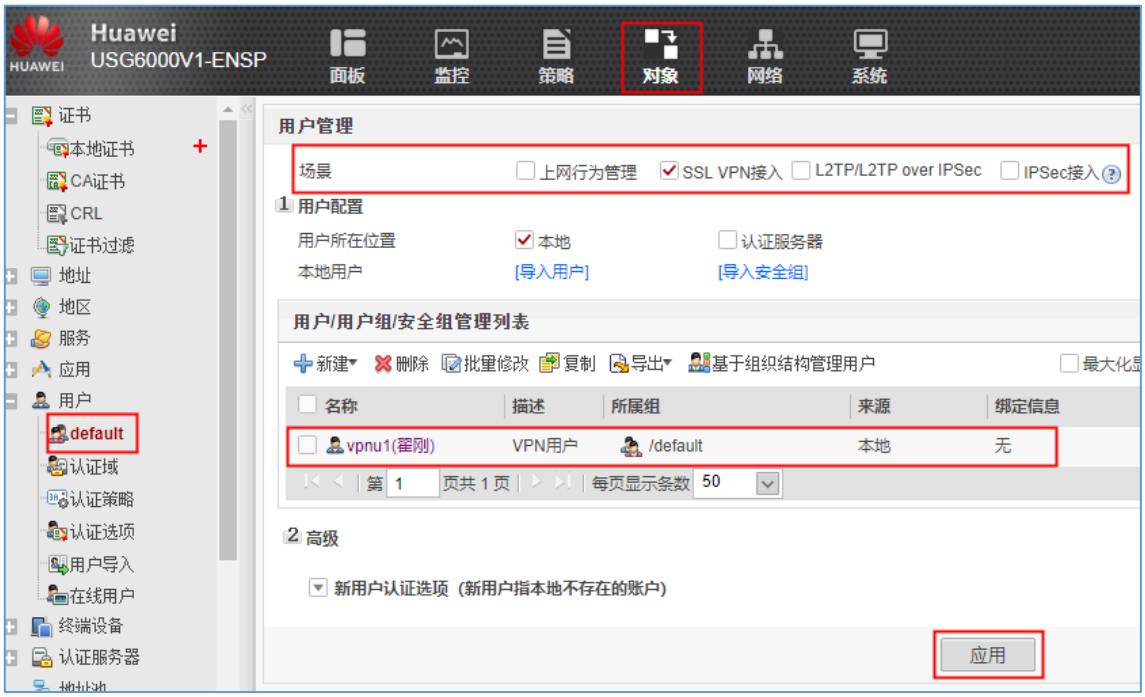
6. 配置 NAT

7. 配置安全策略

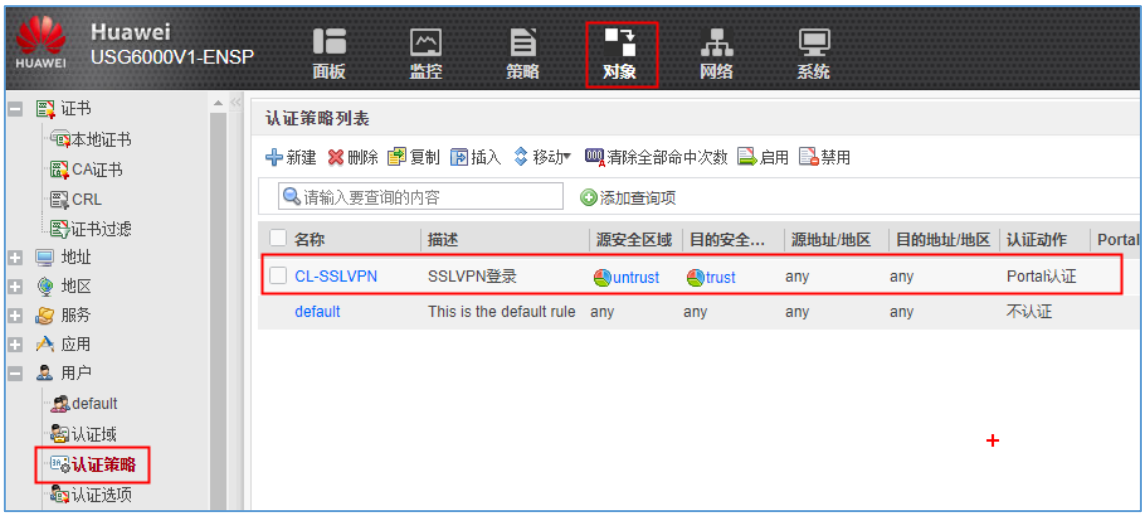
8. 验证结果（此时内网电脑可以访问外部路由）

二、配置 VPN

1. 创建用户

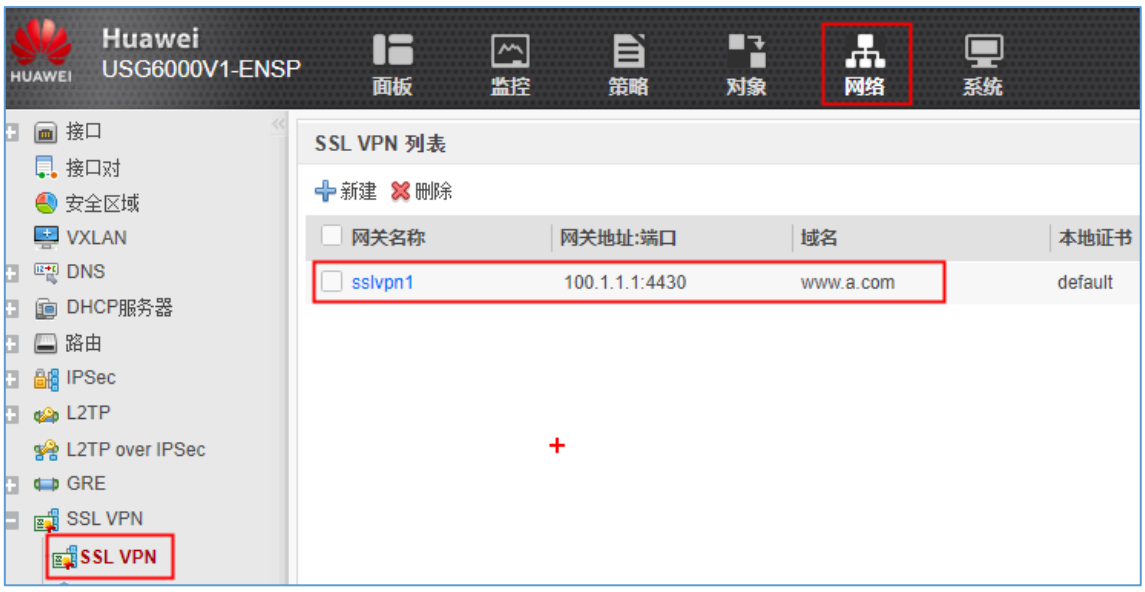


2. 创建认证策略

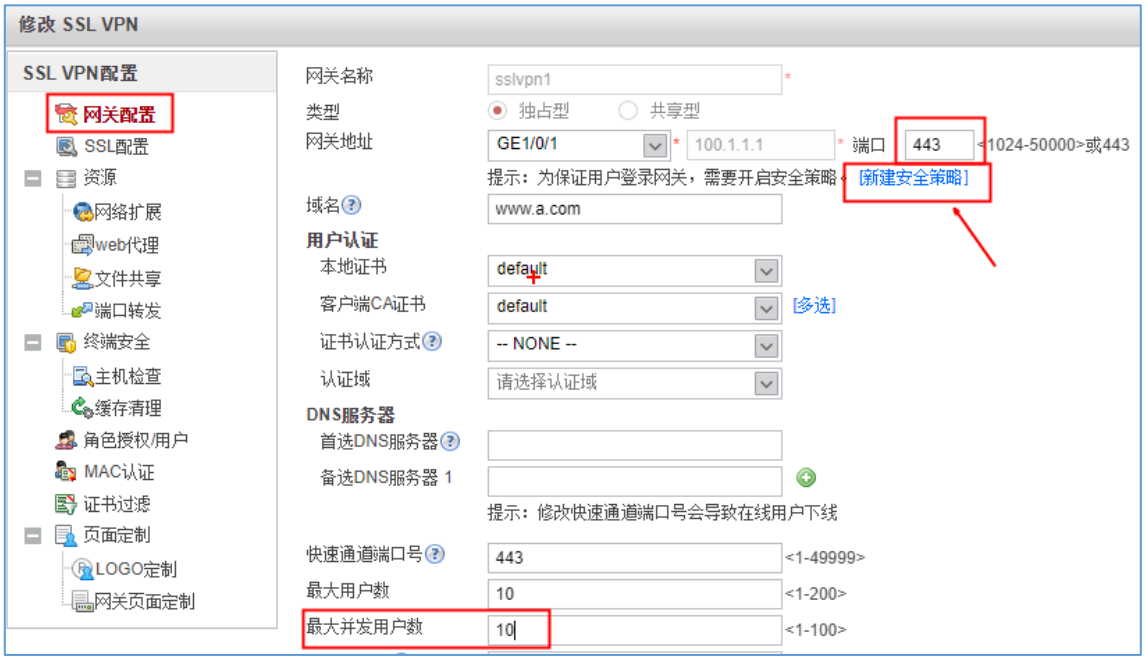


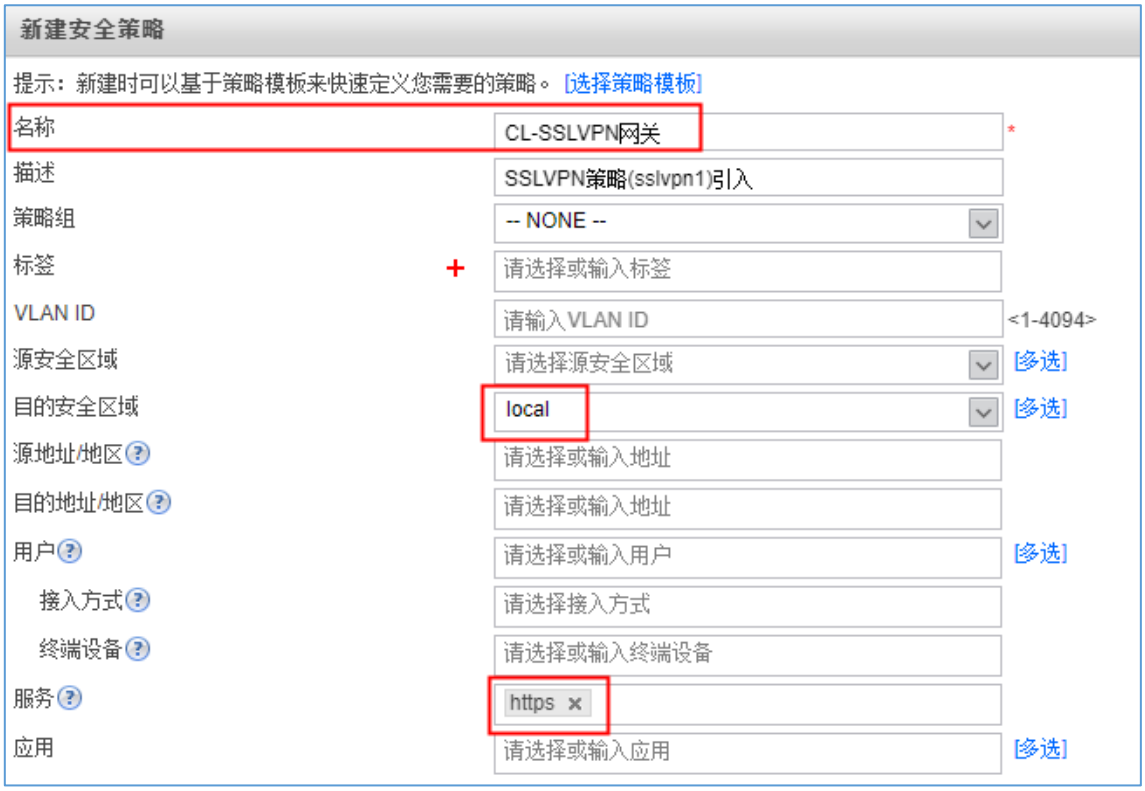
3. 创建 VPN 虚拟网关

[FW1]v-gateway sslvpn1 interface GigabitEthernet 1/0/1 port 4430 private www.a.com



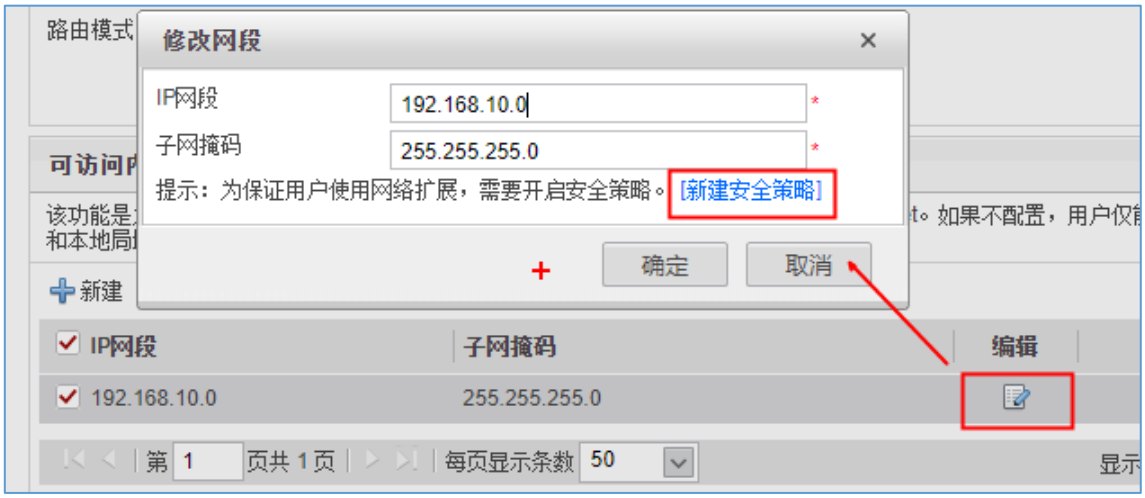
4. 修改 VPN 虚拟网关，网关配置，端口号此处为方便改为 443，为安全建议使用其他端口

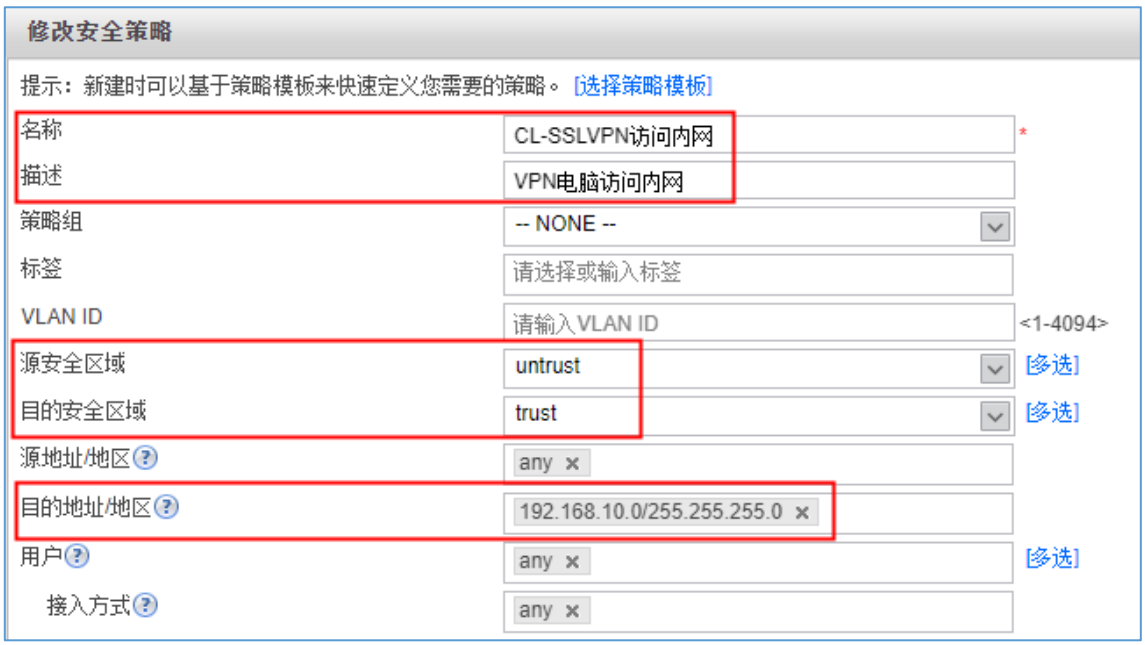




5. 修改 VPN 虚拟网关，网络扩展

6. 修改 VPN 虚拟网关，网络扩展，新建访问内网安全策略





7. 查看安全策略

三、员工从外网使用 SecoClient 客户端登录，一般用于经常性访问

1. 下载 SecoClient 客户端，并按默认安装

参考链接：https://wwi.lanzoup.com/ifKHc0mhwzsf

2. 配置 VPN 相关参数

3. 连接到公司网络

4. 启动成功后，员工电脑正常访问公司内网，电脑桌面右下角出现 SecoClient 客户端图标及相关信息

四、员工从外网使用 Web 方式认证，并进行 SSL VPN 登录，一般用于临时性访问

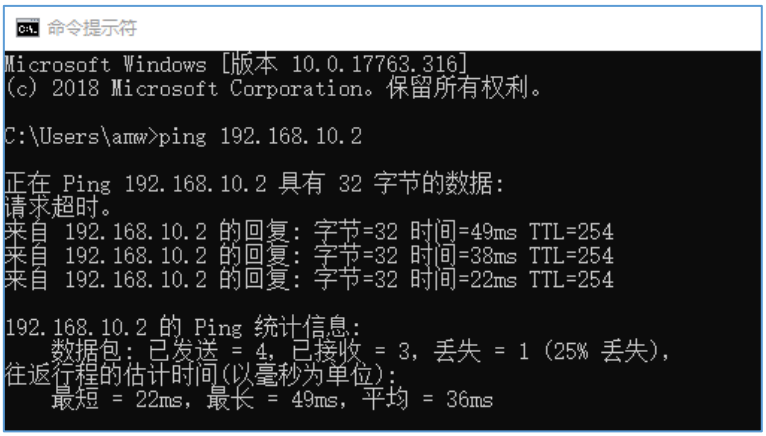
1. 使用 IE 浏览器访问 VPN 网关，https://100.1.1.1，按提示安装控件

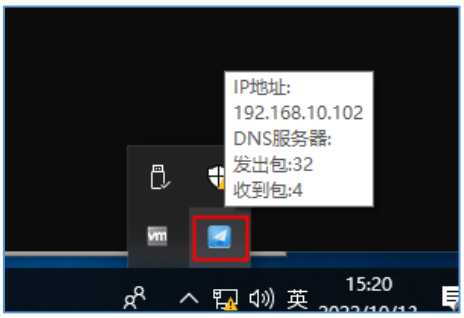
注：因浏览器兼容性原因，需要使用 Windows 10 的 IE 浏览器

2. 登录进行 SSL VPN 认证，输入 vpnu1 用户名和密码

3. 启动“网络扩展”，期间弹出 SVN 网络客户端（SVN Network Extension Client）安装界面，单击“是”进行安装

4. 启动成功后，员工电脑可以正常访问公司内网，电脑桌面右下角出现 SVN 客户端图标及相关信息




IP地址:
192.168.10.102
DNS服务器:
发出包:32
收到包:4
15:20
英