




004-华为eNSP实验-防火墙 USG6000V

原创

周周见  于 2021-11-27 16:11:32 发布  3702  收藏 1

分类专栏: [数通HCIE](#) 文章标签: [ar](#) [网络](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_37736190/article/details/121432986

版权



[数通HCIE 专栏收录该内容](#)

6 篇文章 0 订阅

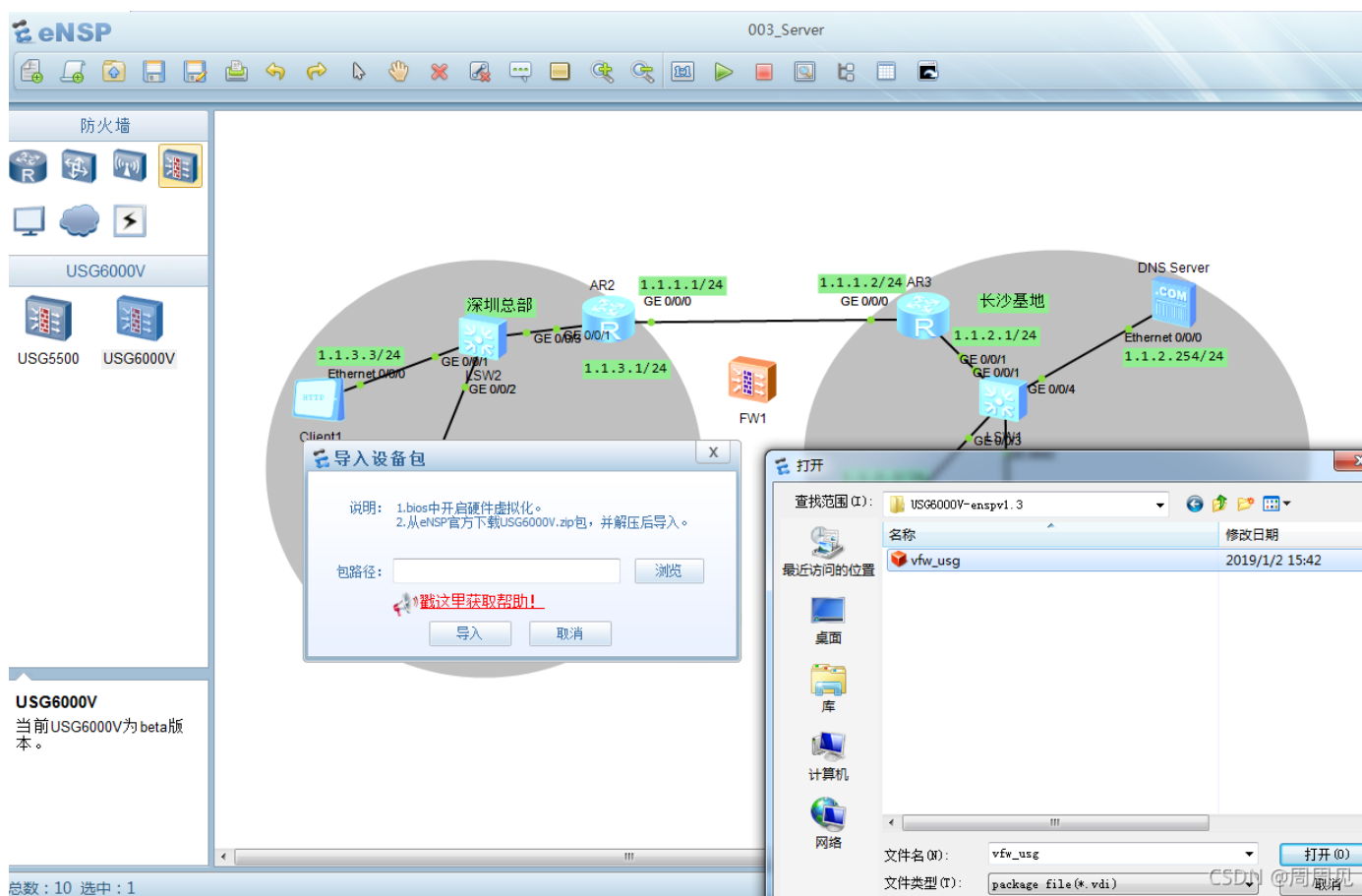
订阅专栏

本章知识点

- 导入USG6000V防火墙设备
- 熟悉云设备的使用, 在宿主机访问USG6000的web页面
- 放通local区域的ACL, 以便从防火墙PING其它设备
- 配置简单的IPsec VPN

1、导入防火墙USG6000V设备

- 新建一个USG6000V
- 导入一个设备包（从 陈海峰 分享拿 <https://forum.huawei.com/enterprise/zh/thread-584872.html#pid3269990>）



2、启动USG6000V

- 关闭防火墙
- 关闭杀软
- 启用硬件虚拟化（在VirtualBox里面直接设置就好了）

参考：

<https://www.cnblogs.com/lzkalislw/p/14707342.html>

2.1 登陆并修改密码

默认账号admin

初始密码：Admin@123

首次登陆需要修改密码

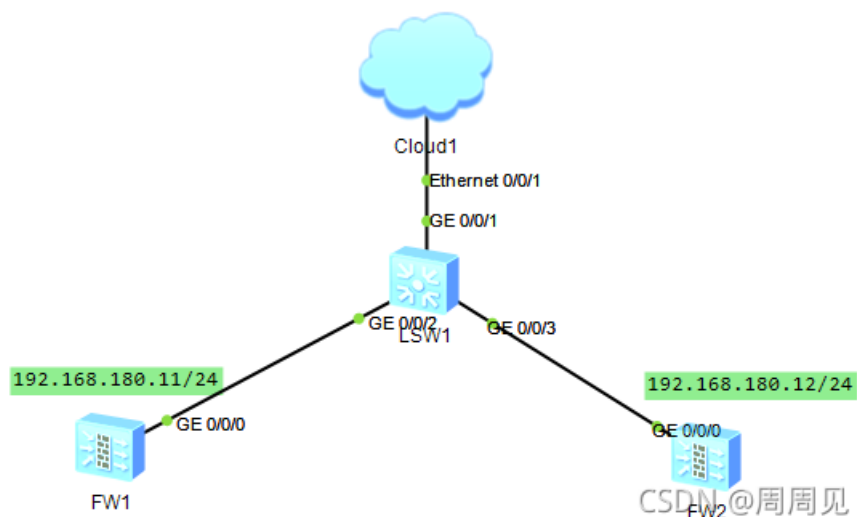
2.2 配置管理口IP和启动管理口服务

- 仅G0/0/0可以登陆web控制台

在接口模式下启动服务

```
[GigabitEthernet0/0/0]service-manage all permit
```

2.3 通过云连接宿主机网卡和防火墙



将宿主机网卡192.168.180.1加入到云中，并设置双向通道

The screenshot shows the 'Cloud1' configuration window. The 'IO配置' (IO Configuration) tab is active. Under '端口创建' (Port Creation), the binding information is 'VMware Network Adapter VMnet1 -- IP: 192.168.180.1'. A warning message states: '警告：请勿绑定公网网卡，否则可能会引起网络瘫痪。' (Warning: Do not bind public network cards, otherwise it may cause network paralysis). The port type is 'Ethernet' and '开放UDP端口' (Open UDP ports) is unchecked. The listening port is set to '30000'. The '对端IP' (Peer IP) is '0.0.0.0' and the '对端口' (Peer Port) is '0'. There are '增加' (Add) and '删除' (Delete) buttons. Below this is a table with the following data:

No.	端口类型	端口编号	UDP端口号	端口开放状态	绑定信息
1	Ethernet	1	2583	Internal	UDP
2	Ethernet	2	None	Public	VMware Network Adapter VMnet1 -- IP: 192.168.180.1

Under '端口映射设置' (Port Mapping Settings), the port type is 'Ethernet', the input port number is '2', and the output port number is '1'. The '双向通道' (Bidirectional Channel) checkbox is checked. There is an '增加' (Add) button. To the right is the '端口映射表' (Port Mapping Table) with the following data:

No.	入端口编号	出端口编号	端口类型
1	2	1	Ethernet
2	1	2	Ethernet

A watermark 'CSDN@周周见' is visible in the bottom right of the screenshot.

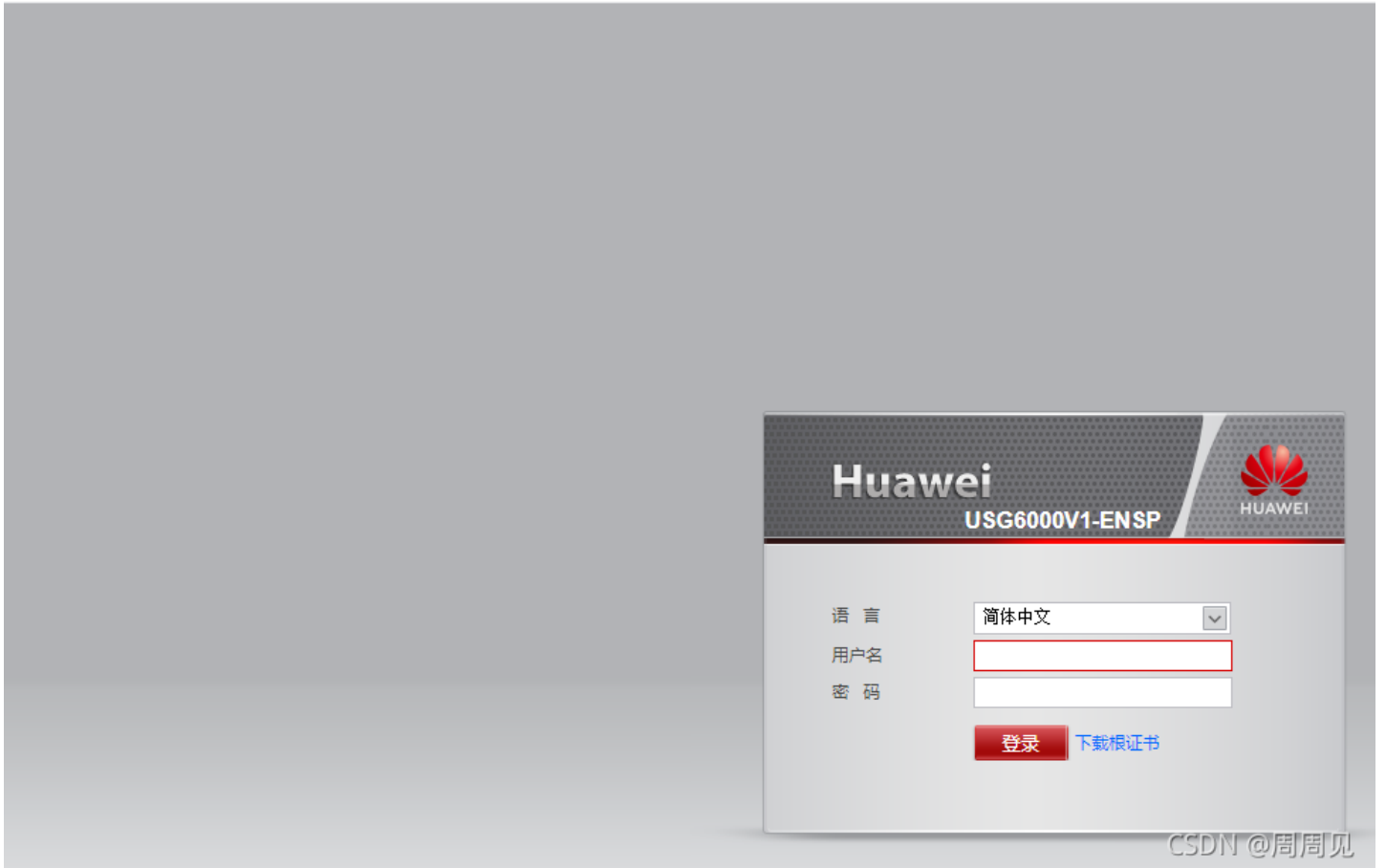
2.4 登陆web控制台

格式如下：

<https://192.168.180.11:8443/>

https://192.168.180.11:8443

度一下 python autoit3 hcie数通 CSDN windows NOW直播 flash游戏 腾讯视频 从 360安全浏览器 网络厂商 af805



2.5 PING不通防火墙

- 开启接口的PING服务
- 放通local区域的ACL策略（PING出去属于LOCAL区域到其它区域）
直接放通所有（或者放通local到其它区域）

序号	名称	描述	标签	VLAN ID	源安全区域	目的安全区域	源地址/地区	目的地址/地区	用户	服务	应用	时间段	动作	内容安全	命中次数	启用	编辑
1	2			any	local trust untrust dmz	local trust untrust dmz	any	any	any	any	any	any	允许		0 清除	<input checked="" type="checkbox"/>	
2	default	This is the ...		any	any	any	any	any	any	any	any	any	禁止		162 清除	<input checked="" type="checkbox"/>	

CSDN @周周见

验证:

从本机防火墙的管理口（G0/0/0，该口有提示做了default的端口映射）

[USG6000V1]ping -vpn-instance default 192.168.180.1

```
[USG6000V1]ping -vpn-instance default 192.168.180.1
PING 192.168.180.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.180.1: bytes=56 Sequence=1 ttl=64 time=26 ms
  Reply from 192.168.180.1: bytes=56 Sequence=2 ttl=64 time=29 ms

--- 192.168.180.1 ping statistics ---
  2 packet(s) transmitted
  2 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 26/27/29 ms
```

从本机防火墙的内网口（G1/0/1）

```
[USG6000V1]ping -i G1/0/1 11.1.1.1
PING 11.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 11.1.1.1: bytes=56 Sequence=1 ttl=128 time=28 ms
  Reply from 11.1.1.1: bytes=56 Sequence=2 ttl=128 time=24 ms
```

从内网PC ping 防火墙（内网口所在网口要放通acl策略）

```
PC>ping 11.1.1.254


Ping 11.1.1.254: 32 data bytes, Press Ctrl_C to break
From 11.1.1.254: bytes=32 seq=1 ttl=255 time=47 ms
From 11.1.1.254: bytes=32 seq=2 ttl=255 time=47 ms
```

2.6 配置IPSec VPN

两边大致一样

修改IPSec策略

场景 点对点 点到多点



- 适用于对端为单台网关的情况。
- 本端为隧道两端的任意一台网关，或星型组网中的分支网关。
- 对端网关一般有固定的IP地址或域名。

场景选项 IPSec智能选路

1 虚拟系统配置

虚拟系统

虚拟系统 public

2 基本配置

策略名称: VPN01 *

本端接口: GE1/0/0 * [配置]

本端地址: 11.0.0.1

对端地址: 11.0.0.2

提示: 为保证协商报文互通, 需要开启双向安全策略. [新建安全策略]

认证方式: 预共享密钥 RSA签名 RSA数字信封

预共享密钥: ***** *

本端ID: IP地址 11.0.0.1

对端ID: 接受任意对端ID

3 待加密的数据流

地址类型: IPv4 IPv6

源地址/地址组	目的地址/地址组	协议	源端口	目的端口	动作	编辑
<input type="checkbox"/> LAN11.1.1.0	REMOTE_LAN11.2.2.0	any	any	any	加密	

共 1 条

反向路由注入

CSDN @周周见

检查连通性
协商报文完毕

策略名称	虚拟系统	场景	本端接口	本端地址	对端地址	协商状态
<input type="checkbox"/> VPN01	public	点到点	GE1/0/0	11.0.0.1	11.0.0.2	成功: 1 失败: 0 正在协商: 0 [详情][诊断]

策略...	IKE用户描述	虚拟...	状态	本端地址	对端地址	算法	协商数据流	持续时...	发送/接收速...	最近一次建...	最近一次
<input type="checkbox"/> VPN01	public		<input checked="" type="checkbox"/> IKE协商成功 <input checked="" type="checkbox"/> IPSec协商成功	11.0.0.1	11.0.0.2	ESP-AES-256	源地址(端口): 11.1.1.0/2... 目的地址(端口): 11.2.2.0... 协议: any	195	0/0	2021-11-27 ...	

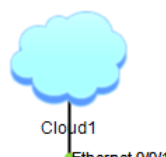
CSDN @周周见

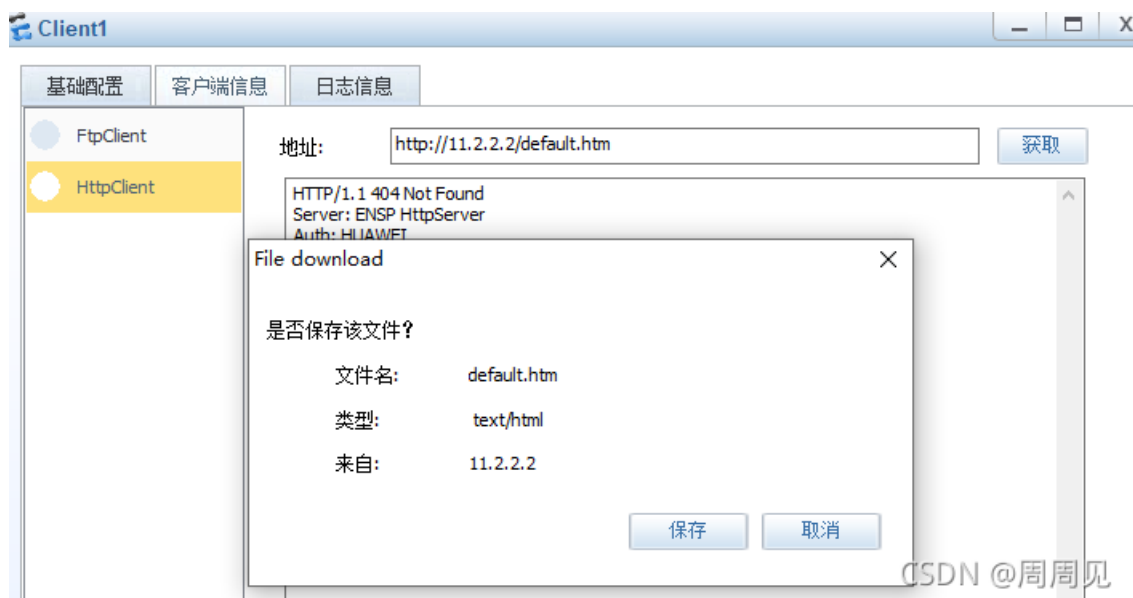
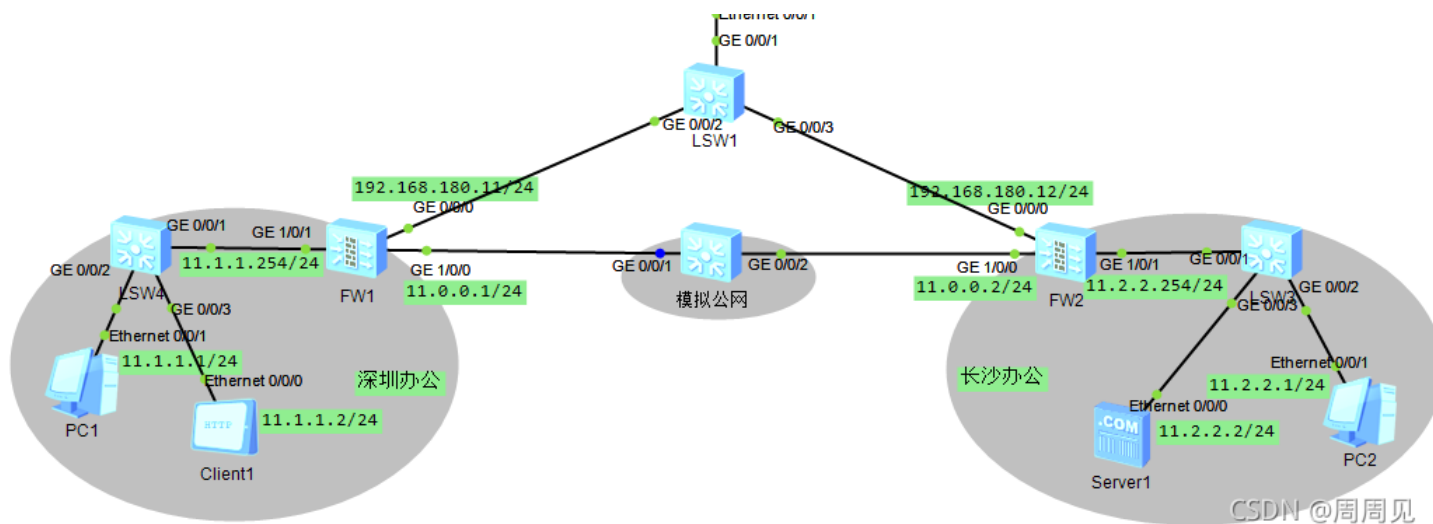
从深圳办公PC1 (11.1.1.1) PING长沙办公PC2 (11.2.2.1)

```
PC>ping 11.2.2.1

Ping 11.2.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 11.2.2.1: bytes=32 seq=2 ttl=126 time=78 ms
From 11.2.2.1: bytes=32 seq=3 ttl=126 time=110 ms
From 11.2.2.1: bytes=32 seq=4 ttl=126 time=78 ms
From 11.2.2.1: bytes=32 seq=5 ttl=126 time=78 ms
```

加一个HTTP服务器测试
从client1 向 Server1获取http请求





2.7 没有解决的问题

在公网中抓包发现流通的IPsec Vpn报文没有加密，感觉是走了静态路由。。。

(有个“自动反向路由注入”的选项)

查看路由表，确实自动学习到了静态路由。先留着以后解决吧。