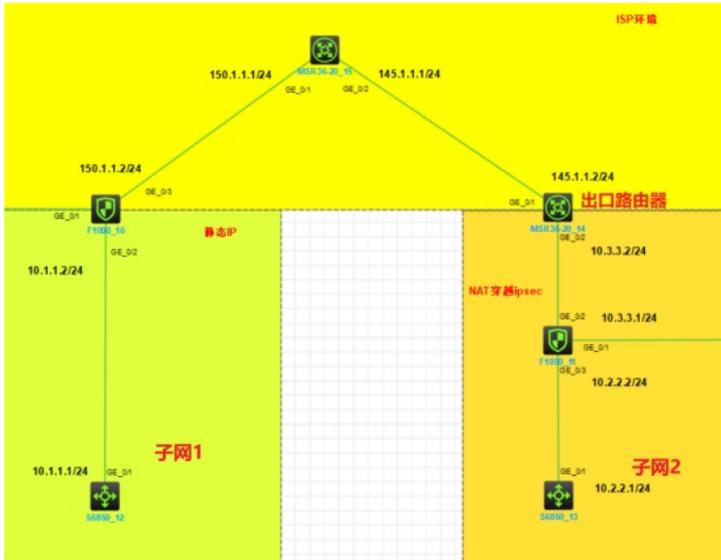


知 F1090 IPSEC典型组网配置案例 (NAT穿越)

IPSec VPN zhiliao_FQbqDB 2022-12-17 发表

组网及说明

本案例采用H3C HCL模拟器的F1090防火墙来模拟IPSEC NAT穿越的典型组网配置。在网络拓扑图中存在子网1和子网2。为了保障子网1和子网2相互传输数据的安全性，因此需要在FW10与FW11采用建立IPSEC VPN隧道，由于FW11的出接口地址不固定且出口路由器为NAT设备，因此采用IKE野蛮模式。



配置步骤

- 1、按照网络拓扑图正确配置IP地址，确保主干链路网络互通正常
- 2、FW10，FW11和出口路由器均配置NAT
- 3、FW10与FW11的互联接口加入安全域，并放通域间策略
- 4、FW1与FW2建立IPSEC VPN隧道，采用IKE野蛮模式

配置关键点

一、主要设备的配置 (web和命令行)

出口路由器:

```
interface GigabitEthernet0/1 //配置接口地址和接口SNAT
```

```
port link-mode route
```

```
combo enable copper
```

```
ip address 145.1.1.2 255.255.255.0
```

```
nat outbound 3000
```

```
#
```

```
interface GigabitEthernet0/2 //配置接口地址
```

```
port link-mode route
```

```
combo enable copper
```

```
ip address 10.3.3.2 255.255.255.0
```

```
#
```

```
ip route-static 0.0.0.0 0 145.1.1.1 //默认路由
```

```
#
```

```
acl advanced 3000 //定义用于SNAT的ACL
```

```
rule 1 permit ip counting
```

FW10:

基本配置

策略名称: 和对端pppoe建立 **自定义名称** (1-46字符)

优先级: 1 **优先级** (1-65535)

设备角色: 对等/分支节点 中心节点

IP地址类型: IPv4 IPv6

智能选路: 开启

接口: GE1/0/3 **外网口** [配置]

本地地址: 150.1.1.2

不进行NAT转换: 开启

对端IP地址/主机名: 145.1.1.2 **对端公网** (1-253字符)

描述: 对端公网地址 (1-80字符)

IKE策略

协商模式: 主模式 野蛮模式 **模式**

认证方式: 预共享密钥 数字认证

预共享密钥: **输入两边一致的密钥** (1-128字符)

IKE提议: 1 (预共享密钥; SHA1; DES-CBC; DH group 1) **IKE提议**

本地ID: IPv4 地址 150.1.1.2

对端ID: IPv4 地址 145.1.1.2/255.255.255.255 **两边的公网IP**

保护的流量流

源IP地址	目的IP地址	VRF	协议	源端口	目的端口	动作	编辑
10.1.1.0/255.255.255.0	10.2.2.0/255.255.255.0	公网	any	any	any	保护	

感兴趣流网段，两边互为相反

共 1 条

需要配置受保护数据目的地址的路由信息，如果没有请进行配置。

需要为本端访问对端业务的流量，配置放行动作的安全策略，如果没有请进行配置。

需要为对端访问本端业务的流量，配置放行动作的安全策略，如果没有请进行配置。

触发模式: 流量触发 自动触发 **建议自动触发**

高级配置

IPsec参数

封装模式: 隧道模式 传输模式 **一般隧道模式**

安全协议: ESP AH AH-ESP

ESP认证算法: SHA1 **参数和对端保持一致**

ESP加密算法: AES-CBC-128

PFS: [未配置]

IPsec SA生存时间: [未配置] 秒 (180-604800)

基于时间: [未配置]

基于流量: [未配置] 千字节 (2560-4294967295)

IPsec SA空闲超时时间: [未配置] 秒 (60-86400)

DPD检测: 开启

内网VRF: 公网

QoS预分类: 开启

确定 取消

```
interface GigabitEthernet1/0/2 //定义内网口
```

```
port link-mode route
combo enable copper
地址为192.168.1.255/255.255.0
#
interface GigabitEthernet1/0/3 //定义外网口和应用ipsec策略
```