第七天

VPN===“虚拟” “专用”网

专线-----贵----10M，稳定，专用

VPN====== 外网（内网）====穿越公网，能够让公网承载内网数据
      ======安全
      ======怎么区分不同VPN

MPLS VPN === ISP解决方案====花钱买服务=====华为必考
IPSEC VPN === 企业解决方案====不花钱，只需要技术===思科偶尔考

VPN=====隧道=====tunnel====虚拟接口
MPLS： 多协议标签交换技术====目的
传统网络：IP路由表===从头查到尾----最长掩码匹配规则===硬件转发（性能上限）
          标签----路由的标记----S-D---转发等价类FEC=====加快转发
          芯片转发=====不查表转发-CEF
MPLS====路由
MPLS =====一层标签
MPLS VPN====二层标签=====外网|内网
MPLS TE=====三层标签

CE：企业边界路由器
PE：运营商边界路由器
P：运营商中心路由器

CE----PE：将内网网段发布给运营商
为了让PE能够区分不同公司的CE的路由，我们需要引入 VPN-instance（VRF）

PE--PE：如何将内网网段互相发布
BGP----跨设备传递路由
MP-BGP======VPNv4

PE--P--PE：如何形成外网标签
======MPLS LDP 标签动态协议

MPLS VPN配置思路：

1，配置PE1，P，PE2的公网接口地址以及动态路由协议（ospf、isis)===实现骨干网三层互通（环回口---后期配置MPLS LSR-id以及BGP VPNv4邻居）

2，配置PE1，P，PE2的MPLS 和MPLS LDP====构建公网MPLS隧道（公网标签）

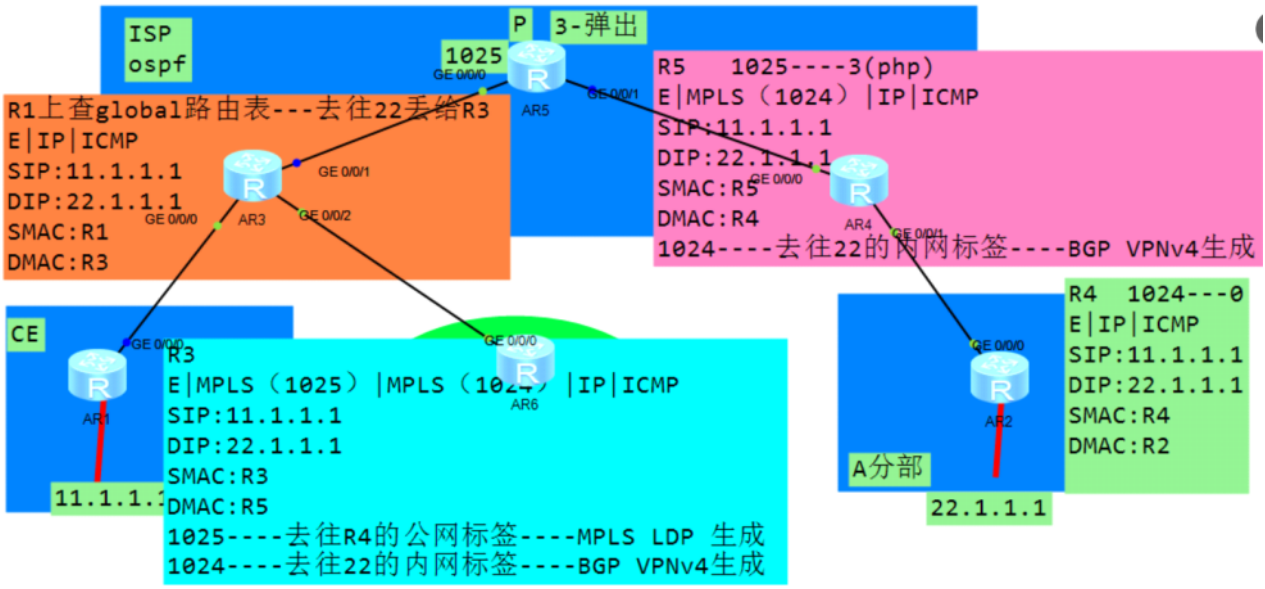
全局配置MPLS lsr-id ，MPLS ，MPLS LDP

接口配置MPLS ， MPLS LDP

3，建立PE1和PE2的MP-BGP VPNv4邻居

4，PE1和PE2上创建VPN实例，推荐实例名一致，RT一致（强制），RD也一致，将连接CE的接口绑定实例，配置地址

5，建立基于实例的PE-CE的路由协议（静态/动态），如果PE和CE不是采用的BGP协议，还需要配置双向重分布



IPSEC --- IP security 安全措施

加密：

对称加密： 只有一把密钥S 设备A用S加密数据，然后将加密后的数据和密钥S一起发给设备B，设备B用密钥S对该加密数据解密，从而获取数据====容易造成密钥泄露，好处是快

=======DES，3DES，AES（wifi），RC4

非对称加密：一台设备一对密钥（公钥和私钥）

设备A产生公钥A和私钥A，设备B产生公钥B和私钥B，设备A和设备B互相交互公钥，设备A用公钥B加密数据，然后将加密的数据和公钥B发给设备B，设备B用公钥B对应的私钥B进行数据解密=====密钥非常安全，缺点：慢，数据包增大

======RSA（SSH），DH（IPSEC），ECC。。。。

整合加密：用对称加密来加密数据，用非对称加密来加密对称加密的那把钥匙

完整性===哈希==散列函数======MD5，SHA

Windows电脑更新补丁=====官网下载补丁==MD5校验文件

雪崩效应======哪怕有一个标点符号的改变都会导致哈希值发生改变

定长==========哈希值是固定长度

不可逆推性====无法通过哈希值逆推出文件内容

冲突避免=====不可能出现不同的文件是相同的哈希值

Ospf 邻居认证===md5认证

A（密码：Huawei@123） --------- B（密码：Huawei@123）

Hello+密码===哈希值1

Hello+哈希值1----------》 hello+密码B==哈希值2

1是否=2，等于表示密码相同

封装协议：
ESP==50==加密，完整性，源认证，抵御重放攻击（DOS）====只保护IP的载荷数据，对原始的IP头部不做任何安全防护
ESP包的字段：
SPI（安全参数索引）：一个32bit的字段，主要用于标识处理数据包的安全关联（SA）
SN（序列号）：标识一个ESP数据包----X---X+1----X+2=====抵御重放攻击

AH==51==完整性，源认证，抵御重放攻击，不加密====绝大多数情况下都采用ESP

数据封装模式：
传输模式（transport mode）=====在原始IP头部和IP负载之间插入一个ESP头部，在结尾处追加一个ESP尾部和ESP验证=======加密点=通信点
老IP|ESP|TCP
隧道模式（tunnel mode）======在原始IP头部之前加入ESP，同时封装一个新的IP头脑不新IP|ESP|老IP|TCP=======加密点≠通信点

密钥有效期=====3600s

IKE----互联网密钥交换协议=======执行协商任务
协商成功之后的结果叫做SA
IKE SA维护了安全防护（加密协议，散列函数，认证模式，密钥有效期等等）IKE协议的细节
IPSEC SA维护了安全防护实际用户流量的细节
IKE是一个混合协议，包括了三种子协议：
SKEME====决定了IKE的密钥交换方式========DH来实现密钥交换
Oakley=====决定了IPSEC的框架设计====让IPSEC能够支持更多的协议
ISAKMP=====IKE的本质协议，决定了包封装与交换以及模式切换====UDP 500

VPN
Site--to---Site
Site--to---PC

IKE的两个阶段，3种模式（主流使用6+3）
1.第一个阶段有两种模式：=====主要目的是对建立IPSEC的双方进行认证，以确保只有合法的邻居才会建立IPSEC VPN=====协商得到的结果就是IKE SA
6个包的主模式

1-2
通过核对收到ISAKMP数据包的yuanIP地址，来确认收到的ISAKMP数据包是否来源于合法的邻居；
协商IKE策略(包含5个内容：加密策略---对56789加密，并不是对感兴趣流去加密，散列函数，DH组，认证方式，密钥有效期）=====一台设备上可以配置多套IKE策略

```
crypto isakmp policy 1
 encr aes
 hash md5
 authentication pre-share
 group 2
```

3-4====密钥--DH（非对称密钥算法）

5-6======认证（安全环境下==加密）

1234---在为56的认证做铺垫

预共享====双方预先配置一个相同的共享密钥===散列交互（类似于OSPF认证）

crypto isakmp key cisco address 45.1.1.5

证书认证

RSA加密随机树认证

或者

3个包的主动模式=====远程VPN

2.第二个阶段只有一种模式=======主要目的就是根据需要加密的实际流量（感兴趣流）来协商保护这些流量的策略=====协商得到的结果就是IPSEC SA

3个包的快速模式

78=======协商加密策略---用于实际数据流加密

crypto ipsec transform-set R12 esp-aes esp-md5-hmac
 mode transport

9========定义感兴趣流

E|IP（SIP：12.1.1.1　DIP：45.1.1.5）|GRE|IP（SIP：11.1.1.1　　DIP：55.1.1.1）|ICMP