**IPsec-VPN--virtual private network**

**什么是VPN--虚拟专用网**

**VPN作用--通过公网实现远程连接，将私有网络联系起来**

**VPN的类型：**

**1、overlay的VPN，例如IPsec-VPN**

**2、peer-to-peer的VPN，例如MPLS-VPN**

**还可以分为二层VPN和三层VPN**

**IPsec-VPN是三层的VPN**

**IPsec-VPN的分类:**

**1、site-to-site VPN 也叫 LAN-to-LAN VPN （要求两个站点都要有固定的IP）**

**2、EASY-VPN 也叫 remote VPN （通常用于连接没有固定IP的站点）**

**IPsec-VPN提供三个特性：**

**1、authentication 每一个IP包的认证**

**2、data integrity 验证数据完整性,保证在传输过程中没有被人为改动**

**3、confidentiality （私密性）数据包的加密**

**《知识准备》**

**在学习IPsec技术之前，先要学习以下几点知识**

**1、加密机制**

**2、DH密钥交换算法**

**3、认证机制**

**4、散列机制**

**加密机制--密码学分为两类：**

**对称加密算法---使用一把密匙来对信息提供安全的保护。只有一个密匙，即用来加密，也用来解密**

**特点：**

**1、速度快**

**2、密文紧凑**

**3、用于大量数据的传送**

**缺点:**

**1.密钥分发**

**2.密钥管理**

**对称加密代表：DES、3DES、AES**

**3DES--有三个密匙，用第一个密匙加密，用第二个密匙解密，再用第三个密匙加密**

**非对称加密---有一对密匙，一个叫公匙，一个叫私匙，如果用其中一个加密，必须用另一个解密。**

**特点：**

**1、速度慢**

**2、密文不紧凑**

**3、通常只用于数字签名，或加密一些小文件。**

**非对称加密的代表：RSA、ECC**

**非对称加密代表RSA--有一对密匙，一个公匙，一个私匙，私匙加密，公匙解密,或者公匙加密，私匙解密**

**非对称加密可以有两种应用：**

**1、公钥加密，私钥解密，叫加密**

**2、私钥加密，公钥解密，叫数字签名**

**理想的应用方法，用非对称加密法来传送对称加密的密匙，或用在数字签名当中。用对称加密法来加密实际的数据。**

**数字签名不但证明了消息的内容，还证明了发送方的身份。**

**密钥化的HASH--使用密钥对生成的消息摘要进行加密时，被称为加密的消息摘要。**

**diffie-hellman key exchange--DH算法**

**是一种安全的让通信双方协商出一个共享密匙的方法。**

**用对方的公匙和自已的私匙产生一个双方都能知道的KEY(也叫共享的密秘)，作对称加密用**

**DH group 1的长度是768位 (产生出的KEY的长度)**

**DH group 2的长度是1024位**

**认证机制--（这里所指的是设备的认证，而不是用户的认证）**

**现代的基本加密技术要依赖于消息之目标接收者已知的一项秘密，关键的问题是如何保障密钥的安全。**

**1、用户名和密码**

**2、OTP（one time password）一次性密码**

**3、生物认证（指纹、眼膜）**

**4、预共享密钥**

**5、数字证书**

**6、加密临时值**

**散列机制--用来做完整性检验**

**散列函数（就是HASH）--把一大堆数据经过计算得到一个较小的、定长的值，散列是一种不可逆函数。这意味着一旦明文生成散列，就不可能或者说极端困难再将其由散列转换成明文。**

**HASH的特点：**

**1、不管输入什么数据，输出是定长的**

**2、只要输入有一点微小变化，输出就会发生很大的变化，也就是雪崩效应**

**3、不可逆**

**HASH的算法：**

**1、md5 提供128位的输出 md5是验证，不是加密技术，用来做哈希**

**2、SHA 提供160位的输出**

**HMAC--使用散列的消息认证编码，或者叫密钥化的HASH，是一种使用HASH来进行认证的机制。可以用来做预共享密钥的认证。**

**----------------------------------------------------------------------------------------**

**IP sec 的组成--IPsec协议集包括三个协议：**

**1、internet key exchange(IKE)密匙交换协议**

**协议双方使用的算法，密匙，协商在两个对等体之间建立一条遂道的参数，协商完成再用下面的方法封装数据。**

**IKE动态的，周期性的在两个PEER之间更新密钥**

**2、encapsulating secutity payload(ESP)封装安全负载**

**可以对数据包认证，加密,封装，IP中协议号--50，通常使用3DES来进行加密**

**3、authentication header (AH)**

**只提供认证，封装，不提供加密，明文传送,IP中协议号--51**

**IPsecVPN的两种模式--**

**一、传输模式：**

**不产生新的IP头，在原包头之后插入一个字段,当通信点等于加密点用这种方法**

**原始IP头 | (ESP或AH) | Data**

**二、通道模式：**

**产生一个新IP包头，当通信点不等于加密点用这种方法，site-to-site的VPN就是这种模式,因为通信点的IP头通常不是一个公网上可路由的头部，而新的IP头用的是两个peer之间的IP地址。**

**新IP头 | (ESP或AH) | 原始IP头 | Data**

**通信点：实际通信的设备**

**加密点：进行加密的设备**

****

**ESP封装中只对原始IP分组进行完整性检验**

**AH封装中进行完整性检验还包括新的IP头**

**--------------------------------------------------------------------------------------------**

**IKE密匙交换协议**

**IKE的作用：用于在两个peer之间协商建立IPsec-VPN通道**

**1、协商参数**

**2、产生KEY，交换KEY、更新KEY**

**3、对双方进行认证**

**4、对密钥进行管理**

**也是由三个不同的协议组成：**

**1、ISAKMP--定义了信息交换的体系结构,也就是格式**

**2、SKEME--实现公钥加密认证的机制**

**3、Oakley--提供在两个IPsec对等体间达成相同加密密钥的基于模式的机制**

**ISAKMP基于UDP，源目端口都是500**

**site-to-site ipsec VPN的协商过程,分两个阶段**

**要想在两个站点之间安全的传输IP数据流，它们之间必须要先进行协商，协商它们之间所采用的加密算法，封装技术以及密钥。这个协商过程是通过IKE来完成的，IKE协商分两个阶段运行：**

**阶段一：在两个对等体设备之间建立一个安全的管理连接。没有实际的数据通过这个连接。这个管理连接是用来保护第二阶段协商过程的。**

**阶段二：当对等体之间有了安全的管理连接之后，它们就可以接着协商用于构建安全数据连接的安全参数，这个协商过程是安全的，加了密的。协商完成后，将在两个站点间形成安全的数据连接。用户就可以利用这些安全的数据连接来传输自已的数据了。**

**第一阶段：建立ISAKMP SA 协商的是以下信息：**

**1、对等体之间采用何种方式做认证，是预共享密钥还是数字证书。**

**2、双方使用哪种加密算法**

**3、双方使用哪种HMAC方式，是MD5还是SHA**

**4、双方使用哪种Diffie-Hellman密钥组**

**5、使用哪种协商模式（主模式或主动模式）**

**6、还要协商SA的生存期**

**第二阶段：建立IPsec SA 协商的是以下信息：**

**1、双方使用哪种封装技术，AH还是ESP**

**2、双方使用哪种加密算法**

**3、双方使用哪种HMAC方式，是MD5还是SHA**

**4、使用哪种传输模式，是隧道模式还是传输模式**

**5、还要协商SA的生存期**

**第一阶段的协商过程总共有6条消息：**

**1、消息1和消息2用于peer之间协商加密机制**

**ISAKMP包含有ISAKMP头、SA负载、提议负载、转换负载等字段**

**总之是让双方协商好我们之间使用啥子协议、加密方法**

**具体是要协定四个东东：加密机制、散列机制、DH组、认证机制**

**2、消息3和消息4用于相互之间交换公共密匙**

**两端的peer先各自生成自已的私匙和公匙，同时还产生一个临时值。然后再使用消息3或消息4将各自的公匙和临时值进行交换。**

**交换完公匙后，每个peer先根据对方的公匙和自已的私匙生成一个共享秘密（使用DH算法），再根据共享秘密、对方和自已的临时值、预共享密钥产生出三个SKEY：**

**SKEYID\_d--此密匙被用于计算后续IPsec密匙资源**

**SKEYID\_a--此密匙被用于提供后续IKE消息的数据完整性以及认证**

**SKEYID\_e--此密匙被用于对后续IKE消息进行加密**

**消息3和4的ISAKMP包含以下字段：ISAKMP包头、密匙交换负载（KE）、临时值负载**

**3、消息5和消息6用于两个peer之间进行认证，这两个消息是用SKEYID\_e进行过加密的。**

**每个peer根据一大堆东东(包括SKEYID-a、预共享密钥、标识ID)生成一个Hash值，再将这个值和自已的标识ID（通常是IP或主机名）发送给对方。当然，使用的就是消息5或消息6。**

**每个peer收到对方的ID和Hash值后，先根据对方的ID找到对方的公匙，再计算本地Hash值,如果本地Hash值和对方的Hash值一样，就表示认证成功。**

**这一步完成后，IKE SA被建立，主模式认证完成**

**第二阶段的协商过程总共有3条消息：**

**1、第一、二条信息是两个peer之间协商形成IPsec SA的封装协议、模式、加密算法，还要互发用DH重新生成的新的公匙和临时值，以及其它一些参数，像SPI、ID等等。**

**2、第三条消息通常由发起者发送给响应者，起一个确认的作用，也用来验证通信信道的有效性**

**第三条信息发送前，两端的peer必须先用和DH相关的信息（新的私钥和对方公钥）生成一个新的DH秘密，然后用该值和SKEYID\_d以及其他一些参数一起来生成最终加解密的KEY。**

**--------------------------------------------------------------------------------------------**

**SA--安全关联**

**SA是两个通信实体经协商建立起来的一种协定，它们决定了用来保护数据包安全的IPsec协议、转码方式、密钥、以及密钥的有效存在时间等等。任何IPsec实施方案始终会构建一个SA数据库（SA DB），由它来维护IPsec协议用来保障数据包安全的SA记录。**

**SA是单向的--如果两个主机（比如A和B）正在通过ESP进行安全通信，那么主机A就需要有一个SA，即SA（OUT），用来处理外发的数据包，另外还需要有一个不同的SA，即SA（IN）用来处理进入的数据包。主机A的SA（OUT）和主机B的SA（IN）将共享相同的加密参数（比如密钥）。**

**SA还要根据协议来区分，如果两个主机间同时使用ESP和AH，对于ESP和AH会生成不同的SA。**

**SADB--安全关联数据库，包含双方协商的IKE和IPsec安全信息**

**SPI--安全参数索引，是一个32位的值，用来标识用于处理数据包的特定的那个安全联盟。或者这样理解，用于唯一定义一条单向的IPsec通道。这个号码存在于ESP包头中，通道两端必须一致。**

**SA分为两种--**

**1、IKE（ISAKMP）SA 协商对IKE数据流进行加密以及对对等体进行验证的算法**

**2、IPsec SA 协商对对等体之间的IP数据流进行加密的算法**

**对等体之间的IKE SA只能有一个**

**对等体之间的IPsec SA可以有多个**

**PFS--完善转发安全性，是一种IKE协商中发起者可以向响应者提供建议的属性，是一种强制对等体双方在快速模式交换中产生新的DH秘密的属性。这允许使用新的DH秘密生成用于加密数据的加密密钥。**

**--------------------------------------------------------------------------------------------**

**配置实例：**

**步骤：**

**1、configure crypto ACL 配置感兴趣流,需要加密的流量就是感兴趣流。**

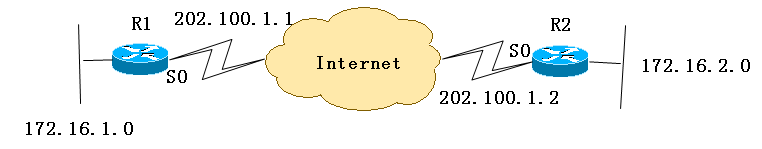
**2、establish ISAKMP policy 第一阶段的策略**

**3、configure IPsec transform set 第二阶段的策略**

**4、configure crypto map**

**5、apply crypto map to the interface 在接口下应用**

**6、configure interface ACL 确定在外网接口放行哪些流量**

****

**一、定义感兴趣流：**

**ip access-list extended VPN**

**permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255**

**二、IKE第一阶段**

**crypto isakmp policy 10**

**encryption des**

**hash md5**

**authentication pre-share**

**group 2**

**crypto isakmp key 0 cisco address 202.100.1.2 pre-share key 的定义 0不加密,6加密**

**三、IKE第二阶段**

**crypto ipsec transform-set MYSET esp-des esp-md5-hmac**

**mode tunnel**

**四、把感兴趣流与转换集映射一下**

**crypto map MYMAP 100 ipsec-isakmp 100为序列号**

**set peer 202.100.1.2 设置VPN对等体的地址**

**set tranform-set MYSET 设置转换集**

**match address VPN 感兴趣流和转换集的绑定**

**五、MAP与接口绑定**

**int s0**

**crypto map MYMAP**

**六、设定接口只允许跑VPN流量,在接口入设置**

**access-list 100 permit udp any eq 500 any eq isakmp**

**access-list 100 permit esp any any**

**access-list 100 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255 由于ACL会二次查找，所以还要放行私网的流量**

**show crypto isakmp policy**

**show crypto isakmp sa 第一阶段的SA status active**

**show crypto ipsec sa 第二阶段的SA**

**show crypto engine connections active 加减密的状况**

**show crypto map**

**crypto ipsec security-association lifetime [seconds|kilobytes] 第二阶段的一个协商时间，也就是说多长时间后重新协商密匙。也可按已发了多少流量来进行协商。哪个数值先到就先起效。**

**cryto isakmp keepalive 10 3**

**IPsec通道的终结：**

**当流量超过上限后或者超时自动终结**

**clear crypto isakmp 清第一阶段**

**clear crypto sa 清第二阶段**

**clear crypto session 在新版的IOS中，用这条命令全清**

**debug crypto isakmp**

**debug crypto ipsec**

**配置IPsec-VPN的注意点：**

**1、路由**

**2、感兴趣流量**

**3、策略**

**4、调用**

**接口设定ACL：**

**设定接口只允许跑VPN流量,在接口入设置**

**access-list 100 permit udp any eq 500 any eq isakmp**

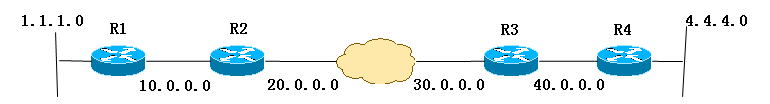
**access-list 100 permit esp any any**

**或access-list 100 permit ahp any any**

**注意：在老IOS中，对包解密后还会再匹配一次访问列表，新的IOS中就不会，所以在老的IOS中要加入一条**

**access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255**

**IPsec中的路由问题：**

****

**R1 需要有4.4.4.0的路由**

**R2 需要有4.4.4.0 1.1.1.0 30.0.0.0的路由**

**R3 需要有1.1.1.0 4.4.4.0 20.0.0.0的路由**

**R4 需要有1.1.1.0的路由**

**-------------------------------------------------------------------------------------------**

**-------------------------------------------------------------------------------------------**

**GRE**

**GRE通用路由封装---一个三层协议，能够将各种不同的数据包封装成IP包，然后通过IP网络进行传输。也就是说能对其它的IP包或非IP包进行再封装，在原始包头的前面增加一个GRE包头和一个新IP包头。明文传送，没有安全性。在IP中的协议号47。**

**GRE封装格式：**

****

**20字节 4字节**

**GRE有很好的隧道特性**

**1、支持多协议**

**2、支持组播**

**缺点是不安全**

**IPsec的特点：**

**1、能提供安全的传输保证**

**2、但只能支持IP，不能支持其他协议**

**小知识：在tunnal中，指定目标地址之后，只要在本地路由表中有这个地址，tunnal就会up**

**GRE over IPsec(实用性很高的技术，不像IPsecVPN那样麻烦)**

**原理：在tunnel中，先用GRE对数据包封装成IP包，再用IPsec加密，默认是通道模式**

**红色部分是加密的部分**

**IPsec只能对IP包加密，不能对非IP包加密。**

**注意在GRE over IPsec中感兴趣流的定义：（所有的GRE流量都是感兴趣流）**

**access-list 100 permit gre host 202.100.13.3 host 202.100.12.2 必须定义公网地址**

**因为当感兴趣流量过来时：**

**1、先查路由，进入tunnel口**

**2、封装GRE后，进入S口撞击map**

**当封装了GRE后，外部的IP地址用的就是公网地址了，所以感兴趣流量必须定义为公网地址。**

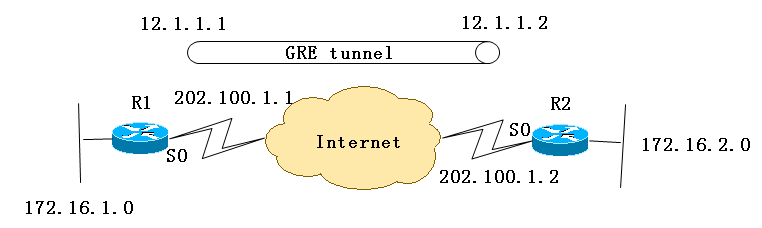
**由于在接口下会两次检查ACL，所以如果在物理接口下放ACL，要同时放行ESP和GRE流量，还有isakmp的协商流量。**

**GRE over IPsec 技术建议使用传输模式**

**因为通信点等于加密点**

****

**试验：**

****

**一、配置tunnel**

**interface tunnel 1**

**tunnel source 202.100.1.1**

**tunnel destination 202.100.1.2**

**tunnel gre ip**

**ip address 12.1.1.1**

**二、运行路由协议**

**router eigrp 90**

**network 172.16.1.0 0.0.0.255**

**network 12.1.1.0 0.0.0.255**

**三、开始配置IPsec，先定义感兴趣流：(注意这里的定义)**

**ip access-list extended VPN**

**permit gre any any**

**四、IKE第一阶段**

**crypto isakmp policy 10**

**encryption des**

**hash md5**

**authentication pre-share**

**group 2**

**crypto isakmp key cisco address 202.100.1.2 pre-share key 的定义**

**五、IKE第二阶段**

**crypto ipsec transform-set MYSET esp-des esp-md5-hmac**

**mode tunnel**

**六、把感兴趣流与转换集映射一下**

**crypto map MYMAP 100 ipsec-isakmp**

**set peer 202.100.1.2 设置VPN对等体的地址**

**set tranform-set MYSET 设置转换集**

**match address VPN 感兴趣流和转换集的绑定**

**七、MAP与接口绑定**

**int s0**

**crypto map MYMAP**

**八、设定接口只允许跑VPN流量,在接口入方向设置**

**用在物理接口下--**

**access-list 100 permit udp any eq 500 any eq isakmp**

**access-list 100 permit esp any any**

**access-list 100 permit gre any any**

**-----------------------------------------------------------------------------------------**

**-----------------------------------------------------------------------------------------**

**site-to-site VPN的缺点：**

**1、需要两端有固定的公网IP**

**2、两端的配置太过复杂**

**RemoteVPN--easyVPN---remote access 使用这种方法**

**实现两个主要目的：**

**1、简单的client配置,easy VPN remote**

**2、中心的server，动态的推送配置到client,easy VPN server**

**所以client很easy,server端的配置一点都不easy**

**远程连接有哪些困难需要克服：**

**1、IPsec的客户端使用server端未知的IP地址来连接网关，这样就不可能在两端定义一个预共享密钥。**

**2、IPsec的客户端通常希望用私网IP进入专用网络，而不是公网IP**

**3、IPsec的客户端必须使用DNS服务器、DHCP服务器和其他一些在专用网络上作为信息主要来源的服务器，而不是使用ISP的服务器。**

**4、IPsec客户端常在PAT设备之后进行连接，但由于ESP要加密TCP或UDP头中的信息，端口自然也加密了，PAT将不能正常工作。**

**为解决以上难题，设计了IKE协商的1.5阶段。**

**IKE的1.5阶段由两部分组成--**

**1、x-auth扩展认证**

**2、模式配置**

**在远程IPsec连接中，通常使用IKE主动模式。只有三条消息交换。**

**扩展认证--允许认证IPsec客户端的使用者，被IPsec网关认证。**

**可以先让所有的客户都使用同一个预共享密钥连接到IPsec网关，然后再使用扩展认证来确定用户的身份，等于要进行两次认证。这样就解决了第一个问题（IPsec两端无法定义预共享密钥的难题）。**

**扩展认证是基于每一个用户的，一般靠IPsec网关与AAA服务器结合来实现。**

**扩展认证在IKE第一阶段完成后进行，扩展认证总共有四个消息的交换。**

**消息一：IPsec网关发向客户端，询问用户名和密码**

**消息二：客户端发向IPsec网关，回应用户名和密码**

**消息三：IPsec验证完毕后，通知客户端成功或失败**

**消息四：如果收到成功的消息，客户端返回一个确认**

**模式配置：**

**允许IPsec网关为客户端推送一个内部的IP地址和DNS服务器等信息。这样客户端就可以用这个内部的IP地址进入专用网络。**

**NAT-T也叫NAT透明**

**用于解决在发生PAT的情况下进行正确的地址转换**

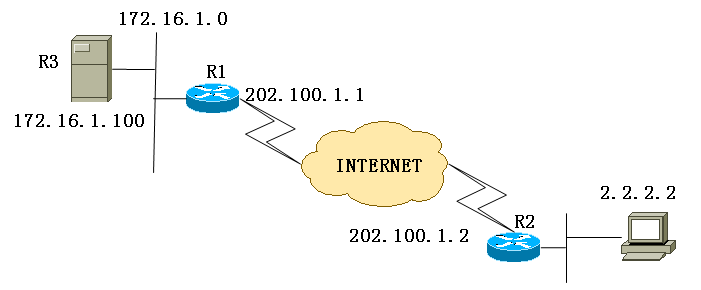
**解决方法--将ESP分组再封装进一个UDP头中。**

**VPN 3005以上的设备都可以做server**

**1700、1800可以做client，实际上不光可以用硬件来做client，软件也可以做，在移动办公中就是软件做**

**1800以上都可以做server**

**remote-VPN配置**

****

**server端配置**

**aaa new-model //启用AAA**

**aaa authentication login REMOTE local**

**aaa authorization network REMOTE local**

**username cisco password 0 cisco //建立本地数据库**

**crypto isakmp policy 10**

**hash md5**

**authentication pre-share**

**group 2**

**encryption des**

**crypto isakmp client configuration group IPSEC-GROUP 组名，设不同组的目地是为内部不同的部门分配不同的IP**

**key xiangweixing 组密码 组名和组密码是一对，需要用户端也是一样的配置**

**pool IP-POOL**

**crypto ipsec transform-set MYSET esp-des esp-md5-hmac**

**crypto dynamic-map MYMAP 10**

**set transform-set MYSET**

**reverse-route 反向路由注入**

**crypto map CISCO client authentication list REMOTE 启用XAUTH**

**crypto map CISCO isakmp authorization list REMOTE**

**crypto map CISCO client configuration address respond 地址推送方式(分强制推送和请求推送)**

**crypto map CISCO 10 ipsec-isakmp dynamic MYMAP**

**interface s1/0**

**crypto map CISCO**

**ip local pool IP-POOL 172.16.1.20 172.16.1.50**

**----------------------------------------------------------------**

**client端配置**

**crypto ipsec client ezvpn EZVPN**

**group IPSEC-GROUP key xiangweixing**

**conn manual**

**peer 202.100.1.1 对端地址**

**mode client**

**int s1/0**

**crypto ipsec client ezvpn EZVPN outside**

**int e0/0**

**crypto ipsec client ezvpn EZVPN inside**

**ip route 0.0.0.0 0.0.0.0 s1/0**

**R2#crypto ipsec client ezvpn connect**

**R2#crypto ipset client ezvpn xauth**

**在客户端查看：**

**show crypto session**

**show crypto ipsec client ezvpn**

**在服务器端查看：**

**show crypto session group**

**show crypto session summary**

**-------------------------------------------------------------------------------------**

**用SDM配置ipsec-VPN**

**HTTPS: tcp 443端口**

**SSH: tcp 22端口**

**http://www.cisco.com/go/sdm**

**安装时要先装一个JAVE虚拟机**

**路由器上要先配置：**

**ip domain-name cisco.com**

**clock timezone GMT +8**

**clock set**

**ip http secure-server**

**username ccnp privilege 15 password cisco**

**line vty 0 4**

**login local 只能用local**

**transport input ssh 只允许ssh**

**测试：从R3上登录R2一下：**

**R3# ssh -l ccnp 202.100.12.2**

**password:cisco**

**----------------------------------------**

**crypto isakmp keepalive 10 3 开启DBD检测**

**crypto map MYMAP 10 ipsec-isakmp**

**set peer 202.100.13.3 default**

**set peer 202.100.1.2 设置两个peer 冗余备份**

**set tranform-set MYSET**

**match address VPN**

**--------------------------------------------------------**

**UDP 500协商过程所用的端口**

**NAT-T使用UDP 4500端口**

**PKI--公共密匙架构，基于证书的VPN**

**DPD(Dead peer detection)失效对等体检测--用来检测链路是否可用，远端设备是否有效。通常用在redun-VPN中**

**原理：通过向对端对等体发送出一个DPD的检测消息来查询对端是否依然存活，当对端对等体收到后会回一个确认。**

**配置命令：**

**crypto isakmp keeplive 60 2**

**第一个计时器是空闲间隔计时器，第二个计时器是重传间隔计时器。默认重传三次。**

**注意：在两端有数据流传输的时候不会发出DPD报文。**

**必须满足两个条件才会发出DPD检测：**

**1、空闲定时器到期**

**2、本端有数据流要发向对端**

**=====================================================================================================================**

**IPSEC 框架中 ， IKE 之上的都是 协商之后的 数据的加密和封装。 而 IKE 就是探讨如何协商的以及 KEY 的问题。**

**SA 双方协商的结果和达成的共识**

**phase 1**

**authenticate the peers /dh key**

**negotiate a bidirectional SA**

**main mode or aggressive mode (LAN TO LAN --MAIN MODE)**

**iskamp udp 500 ,协商数据协议，属于控制层面**

**negotiate the -------------> negotiate the**

**policy<-------------- policy**

**crypto isakmp policy 10 (本地有效，samll good ,对端序号可以不一样)**

**authentication per-share**

**encryption 3des 加密协商数据包 udp 500 ,**

**hash md5**

**group 2 (加密协商数据包、MD5 认证的KEY , 后续ESP 加密的KEY，都是在第一阶段完成)**

**DH exchange --------------> (group 2、5.等 配置对了，就自动 产生交互)**

**<--------------- DH exchange**

**----------------------> verify the peer 第5个包 开始加密**

**<--------------------- identity**

**==》 SA 形成 （可以理解成 ： 暂时存放DH 生成的 3个KEY ，后来这些KEY 都给了 ipsec sa ）**

**phase 2**

**crypto ipsec transform-set TS (对真正的数据加密和认证了,TS 是个TAG)**

**crypto ipsec transform-set TS esp-des esp-md5-hmac**

**mode tunle**

**====》 SA 形成 ，双向， 发出数据，接受数据。**

**SA DB**

**:destination ip address**

**:SPI 安全索引号**

**:protocal (ESP OR AH)**

**phase 2**

**ipsec SAs /SPIs**

**Quick mode**

**crypto map MYMPY 10 ipsec-isakmp (这里的 ipsec-isakmp 指定的是 这是一个什么VPN ，是 ipsec vpn ,还是 GETvpn ,还是老式手动VPN)**

**set peer 202.100.45.5 (对等体)**

**match ip add VPN (命名ACL)**

**set transform- set TS**

**调用**

**cryro map MYMPY**

**debug ipsec sa**

**debug isakmp sa**

**debug crypto ipsec error**