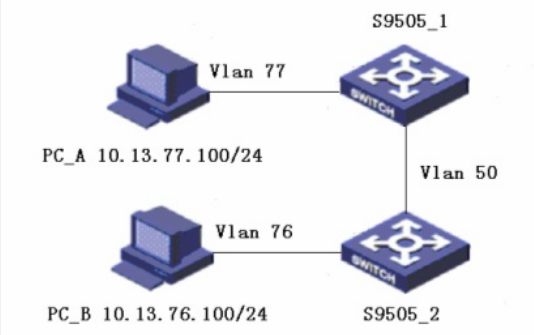
H3C S9500交换机IPSec功能的配置

刘志伟 2006-12-06 发表

H3C S9500交换机IPSec功能的配置

一、组网需求:
在网络中，当发送方和接收方都对数据的安全性和完整性有较高的要求时使用。通过将需要发送的流量转到IPSec板进行相应的处理来实现。
二、组网图:



IPSec组网组网图
以上组网图中Vlan 76和Vlan 77之间的私网报文通过S9505上所连接的IPSEC单板的加密处理实现了安全通信
三、配置步骤:
软件版本：S9500交换机R1327版本及以后的升级版本
硬件版本：需要S9500 LSB1IPSEC8DB0单板
按照上面的组网图，要实现PC_A和PC_B之间进行互相访问时采用IPSec协议族对其数据进行加密，需要对网络进行如下配置:
1．S9505_1设备上的配置过程
配置VLAN，并将连接PC的接口以及S9505之间互连的接口加入到各自的VLAN当中
[S9505_1] vlan 50
[S9505_1-vlan50] port Ethernet 2/1/1
[S9505_1-vlan50] quit
[S9505_1] vlan 77
[S9505_1-vlan77] port Ethernet 2/1/2
[S9505_1-vlan77] quit
配置SecBlade的Module，并将vlan 50和vlan 77配置为security-vlan，同时将配置好的module和插入的IPSec单板关联起来
[S9505_1] secblade module test
[S9505_1-secblade-test] security-vlan 50
[S9505_1-secblade-test] security-vlan 77
[S9505_1-secblade-test] map to slot 3
2．S9505_1设备上的SecBlade的配置过程
配置接口IP地址
[SecBlade_VPN] interface GigabitEthernet 0/0.50
[SecBlade_VPN-GigabitEthernet0/0] ip address 172.16.50.2 24
[SecBlade_VPN-GigabitEthernet0/0] vlan-type dot1q vid 50
[SecBlade_VPN-GigabitEthernet0/0] quit
[SecBlade_VPN] interface GigabitEthernet 0/0.77
[SecBlade_VPN -GigabitEthernet0/0] ip address 10.13.77.2 24
[SecBlade_VPN -GigabitEthernet0/0] vlan-type dot1q vid 77
[SecBlade_VPN -GigabitEthernet0/0] quit
配置ACL规则
[SecBlade_VPN] acl number 3000
[SecBlade_VPN -acl-adv-3000] rule permit ip source 10.13.77.0 0.0.0.255 destination 10.13.76.0 0.0.0.255
[SecBlade_VPN -acl-adv-3000] quit
配置IPSec IKE
[SecBlade_VPN] ike peer peer
[SecBlade_VPN-ike-peer-peer] pre-shared-key vpn
[SecBlade_VPN-ike-peer-peer] remote-address 172.16.50.1

[SecBlade_VPN] quit
配置IPSec提议
[SecBlade_VPN Router] ipsec proposal h3c
[SecBlade_VPN Router-ipsec-proposal-tran] encapsulation-mode tunnel
[SecBlade_VPN Router-ipsec-proposal-tran] transform ah-esp
[SecBlade_VPN Router-ipsec-proposal-tran] ah authentication-algorithm sha1
[SecBlade_VPN Router-ipsec-proposal-tran] esp encryption-algorithm 3des
[SecBlade_VPN Router-ipsec-proposal-tran] esp authentication-algorithm sha1
配置IPSEC策略
[SecBlade_VPN] ipsec policy h3cpolicy 10 isakmp
[SecBlade_VPN-ipsec-policy-isakmp-h3cpolicy-10] ike-peer peer
[SecBlade_VPN-ipsec-policy-isakmp-h3cpolicy-10] proposal h3c
[SecBlade_VPN-ipsec-policy-isakmp-h3cpolicy-10] security acl 3000
[SecBlade_VPN-ipsec-policy-isakmp-h3cpolicy-10] quit
在外网子接口上应用安全策略
[SecBlade_VPN] interface GigabitEthernet 0/0.50
[SecBlade_VPN-GigabitEthernet0/0.50] ipsec policy h3cpolicy
[SecBlade_VPN-GigabitEthernet0/0.50] quit
配置静态路由
[SecBlade_VPN] ip route-static 10.13.76.0 255.255.255.0 172.16.50.1
3．S9505_2设备上的配置过程
该设备的配置过程同S9505_1设备上的配置过程
4．S9505_2设备上的SecBlade的配置过程
该设备的配置过程同S9505_1设备上的SecBlade的配置过程
四、配置关键点:
1. 配置IPSec功能业务需要S9500 IPSEC单板支持。