**江苏科技大学**

**课程设计报告**

课 程： 计算机网络与安全课程设计

课 题： IPSec VPN中的加密设备NAT

学 院： 计算机学院

小组成员： 182210710119 陈四贵

182210710118 陈 鳌

182210710108 李川越

182210710137 张震宇

班 级： 1822107101

指导老师： 张笑非

目 录

[一、 实验目的 1](#_Toc59906787)

[二、 实验原理暨实验步骤 1](#_Toc59906788)

[三、 实验内容暨实验结果 1](#_Toc59906789)

[四、 实验总结与思考 6](#_Toc59906790)

# 实验目的

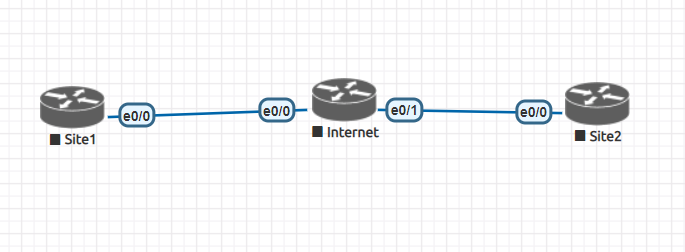
1. 通过加密设备NAT问题进一步理解影响IPsec vpn的网络问题；

2. 熟悉eve的使用。

# 实验原理暨实验步骤

配置基本网络与经典IPSec VPN，测试地址转换对IPSec VPN的影响。

# 实验内容暨实验结果

**Step 1**，创建加密设备NAT问题分析实验拓扑，其中，Site1和Site2是两个VPN站点连接的网关路由器，也是IPSec VPN的加密设备。

**Step 2**，配置路由器的IP地址与路由，即执行基本网络配置。

2.1 Center上的基本网络配置

1. enable
2. config t
3. hostname Site1
4. crypto isakmp policy 10
5. authentication pre-share
6. crypto isakmp key cisco address 61.128.1.1
7. crypto ipsec transform-set cisco esp-des esp-md5-hmac
8. crypto map cisco 10 ipsec-isakmp
9. set peer 61.128.1.1
10. set transform-set cisco
11. match address vpn
13. interface  Loopback0
14. ip address 1.1.1.1 255.255.255.0
15. interface e0/0
16. ip address 202.100.1.1 255.255.255.0
17. crypto map cisco
18. no shutdown
19. ip route 0.0.0.0 0.0.0.0 202.100.1.10
20. ip access-list extended vpn
21. permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255
22. end

2.2 Internet上的基本网络与Telnet登录配置

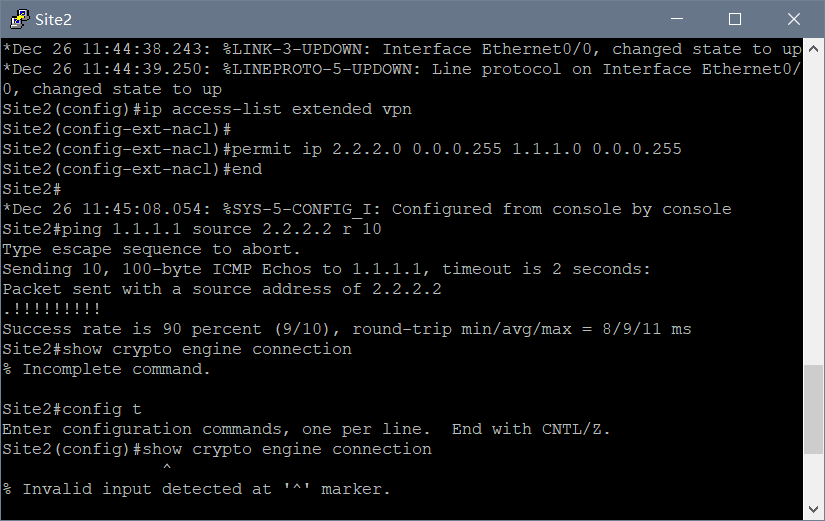
1. enable
2. config t
3. enable password cisco
4. no ip domain lookup
5. hostname Internet
6. interface e0/0
7. ip address 202.100.1.10 255.255.255.0
8. no shutdown
9. interface e1/0
10. ip address 61.128.1.10 255.255.255.0
11. no shutdown
12. line vty 0 4
13. password cisco
14. end

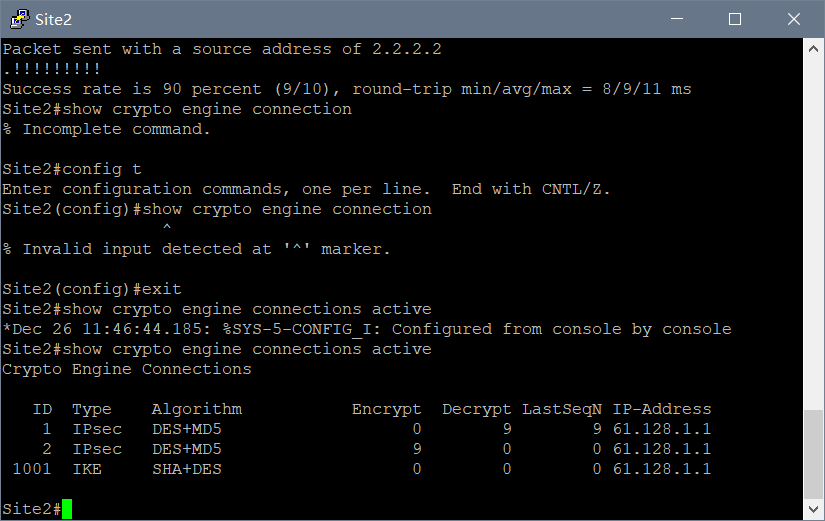
2.3 Site2上的基本网络与经典IPSec VPN配置

1. enable
2. config t
3. hostname Site2
4. crypto isakmp policy 10
5. authentication pre-share
6. crypto isakmp key cisco address 202.100.1.1
7. crypto ipsec transform-set cisco esp-des esp-md5-hmac
8. crypto map cisco 10 ipsec-isakmp
9. set peer 202.100.1.1
10. set transform-set cisco
11. match address vpn
12. interface Loopback0
13. ip address 2.2.2.2 255.255.255.0
14. interface e0/0
15. ip address 61.128.1.1 255.255.255.0
16. crypto map cisco
17. no shutdown
18. ip route 0.0.0.0 0.0.0.0 61.128.1.10
19. ip access-list extended vpn
20. permit ip 2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255
21. end

**Step 3**，测试并且查看IPSec VPN状态。

涉及命令：

3.1 在Site2路由器上执行ping操作，以测试这个IPSec VPN是否可以正常工作

3.2 在Site2路由器上，查看IPSec VPN的加解密状态

**Step 4**，在Site2上配置PAT转换。

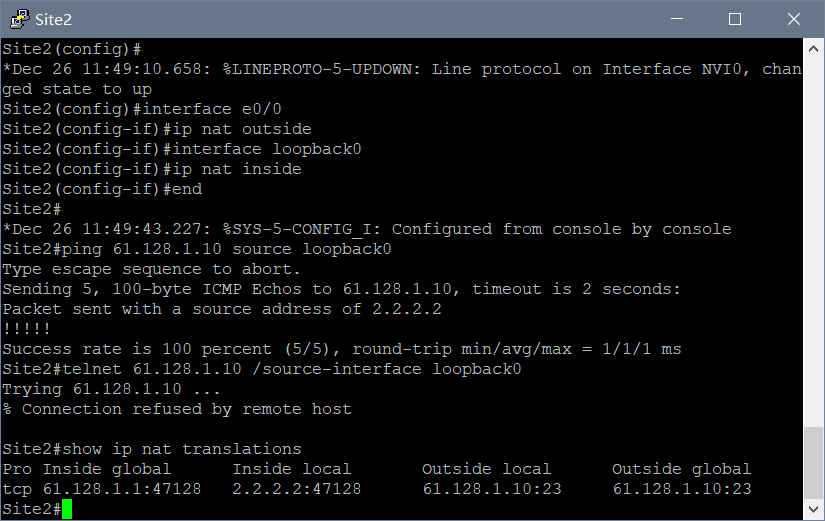
1. ip access-list extended PAT
2. permit ip 2.2.2.0 0.0.0.255 any
3. ip nat inside source list PAT interface e0/0 overload
4. interface e0/0
5. ip nat outside
6. interface loopback0
7. ip nat inside

**Step 5**，测试并查看PAT转换状态。

5.1 在Site2上产生满足地址转换条件的ICMP流量

5.2在Site2上产生满足地址转换条件的Telnet流量

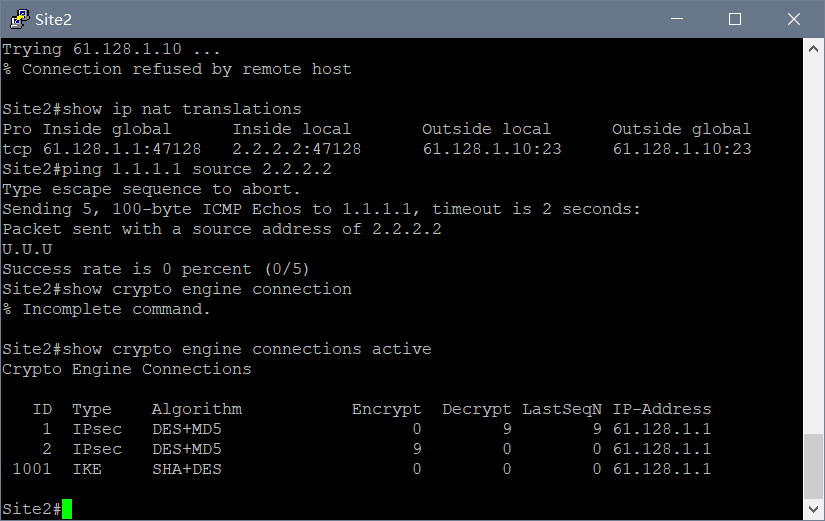
5.3查看PAT地址转换工作状况



**Step 6**, 再次测试并且查看IPSec VPN状态。

6.1 再次在Site2上测试IPSec VPN

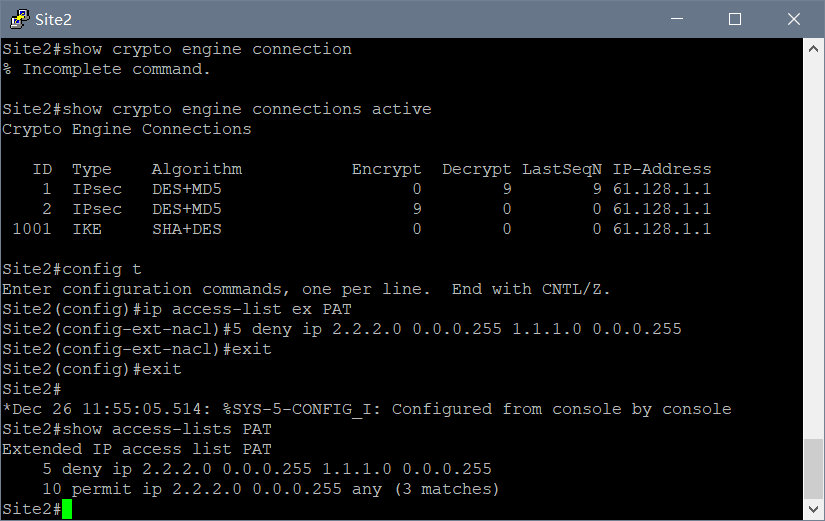
6.2 在Site2上查看IPSec VPN加解密状态



**Step 7**，配置PAT列表排除IPSec VPN感兴趣流

7.1 修改Site2上的地址转换列表，排除IPSec VPN感兴趣流

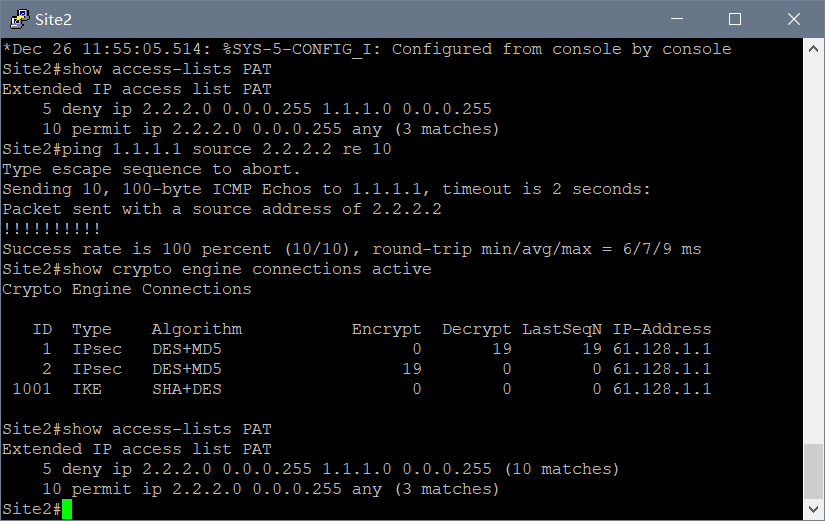
7.2 查看修改后的列表



**Step 8**，测试IPSec VPN。

8.1 在Site2上使用ping测试IPSec VPN

8.2 在Site2上查看加解密数据包

8.3旁路感兴趣流的列表条目有匹配项

# 实验总结与思考

NAT优先于加密导致无法联通的问题只会出现在经典配置的IPSec VPN中，而使用虚拟隧道技术的IPSec VPN不受影响。因为对于拥有虚拟隧道接口的路由器而言，感兴趣流是从隧道口离开的，在隧道口上并没有配置ip nat outside，因此感兴趣流并不会被转换。简而言之，NAT技术并不会影响使用虚拟隧道技术的IPSec VPN.