

马钢 Gary MA magang@gmail.com

<http://magang.name>

2009 年 7 月 13 日

本人承接各种网络规划设计咨询和设备选型安装配置服务，如有需要欢迎联系。

I provided network planning and design consulting services, please contact me.

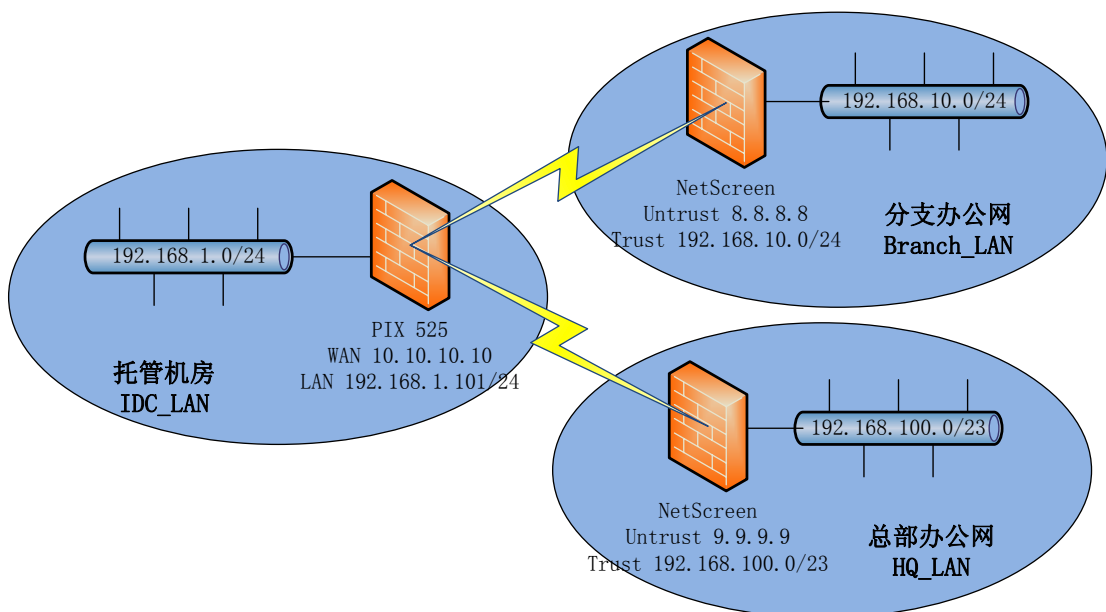
需求

某公司有总部和分支两个办公网，并在托管机房放置了若干服务器。公司需要从两个办公网安全的访问托管机房的服务器。

两个办公网各用一台 Juniper NetScreen 安全设备作为出口路由器。托管机房的服务器前使用 Cisco PIX525 进行保护。这些设备均支持 IPSec VPN，于是考虑部署 Site-to-Site IPSec VPN 来实现上述需求。

This article introduces a method of how to deploy multiple Site-to-Site IPSec VPN tunnels between a Cisco PIX 525 firewall and Juniper NetScreen security appliances.

拓扑



实现

本配置重点在 PIX 525 上要同时启两条和 NetScreen 互联的 IPSec VPN。

主要介绍 PIX 525 的相关配置，NetScreen 的配置即一般的 Policy-based VPN 配制方法，请自行阅读 Juniper 设备文档。

```
: Saved
:
PIX Version 8.0(4)
!
hostname -firewall
names
name 9.9.9.9 HQ_NS204 description HQ 204          (定义地址对象)
name 8.8.8.8 Branch_NS25 description Branch 25
name 192.168.100.0 HQ_LAN
name 192.168.10.0 Branch_LAN

dns-guard
!
interface Ethernet0          (配置接口)
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.101 255.255.255.0
!
interface Ethernet2
 nameif intf2
 security-level 10
 no ip address
!
clock timezone BJT 8
access-list acl_outside extended permit icmp any any
access-list outside_cryptomap_1 extended permit ip 192.168.1.0 255.255.255.0 HQ_LAN
255.255.254.0          (定义从机房到总部的 ACL)
access-list outside_cryptomap_2 extended permit ip 192.168.1.0 255.255.255.0 Branch_LAN
255.255.255.0          (定义从机房到分支的 ACL)
access-list no_NAT extended permit ip 192.168.1.0 255.255.255.0 Branch_LAN
255.255.255.0          (配置不被 NAT 的流量列表)
access-list no_NAT extended permit ip 192.168.1.0 255.255.255.0 HQ_LAN 255.255.254.0
```

(配置不被 NAT 的流量列表)

```
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip verify reverse-path interface outside
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-61557.bin
asdm history enable
arp timeout 14400
nat-control
global (outside) 1 10.10.10.10
nat (inside) 0 access-list no_NAT (使 no_NAT 的流量不被 NAT)
nat (inside) 1 192.168.1.0 255.255.255.0
access-group acl_outside in interface outside
route outside 0.0.0.0 0.0.0.0 10.10.10.11 1 (配置 PIX 默认路由)
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
http server enable
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association
lifetime seconds 28800
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set security-association
lifetime kilobytes 4608000
:配置机房到总部的VPN
crypto map outside_map1 1 match address outside_cryptomap_1(定义匹配流量)
crypto map outside_map1 1 set peer HQ_NS204 (配置远程网关地址)
crypto map outside_map1 1 set transform-set ESP-AES-128-SHA ESP-3DES-SHA(配置 ESP 算
法)
crypto map outside_map1 1 set security-association lifetime seconds 28800(配置 SA 生存时
间)
```

```
crypto map outside_map1 1 set security-association lifetime kilobytes 4608000
crypto map outside_map1 1 set nat-t-disable(禁用 NAT 穿透, 如果需要也可以启用)
:配置机房到分支的 VPN
crypto map outside_map1 2 match address outside_cryptomap_2
crypto map outside_map1 2 set peer Branch_NS25
crypto map outside_map1 2 set transform-set ESP-AES-128-SHA ESP-3DES-SHA
crypto map outside_map1 2 set security-association lifetime seconds 28800
crypto map outside_map1 2 set security-association lifetime kilobytes 4608000
crypto map outside_map1 2 set nat-t-disable
crypto map outside_map1 interface outside
crypto isakmp identity address
crypto isakmp enable outside
crypto isakmp policy 5
  authentication pre-share
  encryption aes
  hash sha
  group 2
  lifetime 86400
ssh timeout 5
ssh version 2
console timeout 0
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 192.168.1.20 source inside
ssl server-version tlsv1
ssl encryption aes128-sha1 3des-sha1
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol IPSec
:配置机房到分支的 VPN 类型和预共享密钥
tunnel-group 9.9.9.9 type ipsec-l2l
tunnel-group 9.9.9.9 ipsec-attributes
  pre-shared-key YOUR-PRE-SHARED-KEY
:配置机房到总部的 VPN 类型和预共享密钥
tunnel-group 8.8.8.8 type ipsec-l2l
tunnel-group 8.8.8.8 ipsec-attributes
  pre-shared-key YOUR-PRE-SHARED-KEY
```