Strongswan 配置site-to-site vpn

环境centos6

安装

Yum install –y Openssl openssl-devel gmp gmp-devel

下载Strongswan

Wget <https://download.strongswan.org/strongswan-5.4.0.tar.gz>

Tar xzvf strongswan-5.4.0.tar.gz

Cd strongswan-5.4.0

./configure --prefix=/usr/local --enable-openssl

Make

Make install

Site A配置，/usr/local/etc/ipsec.conf

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup

# strictcrlpolicy=yes

# uniqueids = no

charondebug="all"

uniqueids=yes

strictcrlpolicy=no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed

# leftsubnet=10.1.0.0/16

# leftcert=selfCert.der

# leftsendcert=never

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightcert=peerCert.der

# auto=start

#conn sample-with-ca-cert

# leftsubnet=10.1.0.0/16

# leftcert=myCert.pem

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightid="C=CH, O=Linux strongSwan CN=peer name"

# auto=start

conn %default

conn tunnel #

#left=47.89.18.125

left=172.31.225.29

leftid=47.89.18.125

leftsubnet=172.31.224.0/20

right=121.43.184.193

rightsubnet=192.168.3.0/24

ike=aes256-sha2\_256-modp1024!

esp=aes256-sha2\_256!

keyingtries=0

ikelifetime=1h

lifetime=8h

dpddelay=30

dpdtimeout=120

dpdaction=restart

authby=secret

auto=start

keyexchange=ikev2

type=tunnel

预共享密钥 ipsec.secrets

121.43.184.193 47.89.18.125 : PSK 'pyyx123'

Site B 配置，/usr/local/etc/ipsec.conf

# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup

# strictcrlpolicy=yes

# uniqueids = no

charondebug="all"

uniqueids=yes

strictcrlpolicy=no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed

# leftsubnet=10.1.0.0/16

# leftcert=selfCert.der

# leftsendcert=never

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightcert=peerCert.der

# auto=start

#conn sample-with-ca-cert

# leftsubnet=10.1.0.0/16

# leftcert=myCert.pem

# right=192.168.0.2

# rightsubnet=10.2.0.0/16

# rightid="C=CH, O=Linux strongSwan CN=peer name"

# auto=start

conn %default

conn tunnel #

leftid=121.43.184.193

left=192.168.3.8

leftsubnet=192.168.3.0/24

right=47.89.18.125

rightsubnet=172.31.224.0/20

ike=aes256-sha2\_256-modp1024!

esp=aes256-sha2\_256!

keyingtries=0

ikelifetime=1h

lifetime=8h

dpddelay=30

dpdtimeout=120

dpdaction=restart

authby=secret

auto=start

keyexchange=ikev2

type=tunnel

预共享密钥 ipsec.secrets

121.43.184.193 47.89.18.125 : PSK 'pyyx123'

启动ipsec

ipsec start

查看状态

[root@hz-t-php-x-x-x-x etc]# ipsec statusall

Status of IKE charon daemon (strongSwan 5.4.0, Linux 2.6.32-642.6.2.el6.x86\_64, x86\_64):

uptime: 58 minutes, since Dec 13 17:15:40 2016

malloc: sbrk 397312, mmap 0, used 310384, free 86928

worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 4

loaded plugins: charon aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp xcbc cmac hmac attr kernel-netlink resolve socket-default stroke vici updown xauth-generic

Listening IP addresses:

192.168.3.8

Connections:

tunnel: 192.168.3.8...47.89.18.125 IKEv2, dpddelay=30s

tunnel: local: [121.43.184.193] uses pre-shared key authentication

tunnel: remote: [47.89.18.125] uses pre-shared key authentication

tunnel: child: 192.168.3.0/24 === 172.31.224.0/20 TUNNEL, dpdaction=restart

Security Associations (1 up, 0 connecting):

tunnel[3]: ESTABLISHED 18 minutes ago, 192.168.3.8[121.43.184.193]...47.89.18.125[47.89.18.125]

tunnel[3]: IKEv2 SPIs: b147958f477e0b6a\_i 7dfca6376a4ca791\_r\*, pre-shared key reauthentication in 23 minutes

tunnel[3]: IKE proposal: AES\_CBC\_256/HMAC\_SHA2\_256\_128/PRF\_HMAC\_SHA2\_256/MODP\_1024

tunnel{3}: INSTALLED, TUNNEL, reqid 3, ESP in UDP SPIs: ce26a467\_i ce67569e\_o

tunnel{3}: AES\_CBC\_256/HMAC\_SHA2\_256\_128, 0 bytes\_i, 0 bytes\_o, rekeying in 7 hours

tunnel{3}: 192.168.3.0/24 === 172.31.224.0/20