strongSwan - Issue #3485

IPSec VPN between AWS CSR1000v and Strongswan VPN server in AWS

15.06.2020 16:10 - Manivannan Kanagasooriyam

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	

Description

I am new to strongswan; and trying to setup site-to-site IPSec VPN between CSR1000v in AWS and a Strongswan Ubuntu server in another AWS account.

Scenario ========
CSR VPC =======
VPC CIDR 10.10.2.0/24
Pub Subnet 10.10.2.0/26
Pri Subnet 10.10.2.64/26
Pub Route Table 0.0.0.0--> IGW
Pri Route Table 0.0.0.0--> Inside ENI of CSR
WAN SG SSH <-- 0.0.0.0, UDP 500, 4500 <-- From Peer WAN IP (VPN Server Pub IP)
LAN SG Allow all traffic from 0.0.0.0
Disabled SRC/DST check for both inside & ouside interfaces of CSR and the interface of private instace in private subnet
I can ping the LAN interfaces of CSR and private instance from each other.

Strongswan VPC ========================
VPC CIDR 172.16.0.0/16
Pub Subnet 172.16.0.0/24
Pri Subnet 172.16.1.0/24
Pub Route Table 0.0.0.0--> IGW , 10.10.2.0/24(CSR VPC) --> GW of the VPN Server
Pri Route Table 0.0.0.0--> ENI of VPN Server
Out SG SSH <-- 0.0.0.0, UDP 500,4500 <-- From Peer WAN IP (CSR Pub IP), ICMP - All
Disabled SRC/DST check for both inside & ouside interfaces of CSR and the interface of private instace in private subnet
I can ping the LAN interfaces of CSR and private instance from each other.

10.10.2.100 client |
CSR 1000V: Gig1 10.10.2.26
Gig2 10.10.2.70 | | |
Strongswan: eth0 |
Appserver 172.16.1.215

`Below I have given my configs and error.`

Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 05[CFG] received stroke: add connection 'vpc2-to-vpc1'
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 05[CFG] added configuration 'vpc2-to-vpc1'
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 07[CFG] received stroke: initiate 'vpc2-to-vpc1'
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 07[IKE] initiating IKE_SA vpc2-to-vpc1[1] to 3.88.xx.xx
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 07[IKE] initiating IKE_SA vpc2-to-vpc1[1] to 3.88.xx.xx
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 07[ENC] generating IKE_SA_INIT request 0 [SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP)]
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 07[NET] sending packet: from 172.16.0.203[500] to 3.88.xx.xx[500] (894 bytes)
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 09[NET] received packet: from 3.88.xx.xx[500] to 172.16.0.203[500] (36 bytes)
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 09[ENC] parsed IKE_SA_INIT response 0 [N(NO_PROP)]
Jun 15 05:37:10 ip-172-16-0-203 charon[7157]: 09[IKE] received NO_PROPOSAL_CHOSEN notify error

ubuntu@ip-172-16-0-203:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.6.2, Linux 5.3.0-1023-aws, x86_64):
uptime: 6 hours, since Jun 15 05:37:09 2020
malloc: sbrk 1622016, mmap 0, used 537792, free 1084224
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
loaded plugins: charon aesni aes rc2 sha2 sha1 md4 md5 mgf1 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default

```
connmark stroke updown eap-mschapv2 xauth-generic counters
Listening IP addresses:
172.16.0.203
Connections:
vpc2-to-vpc1:  %any...3.88.xx.xx  IKEv2
vpc2-to-vpc1:   local:  [35.182.xx.xx] uses pre-shared key authentication
vpc2-to-vpc1:   remote: [3.88.xx.xx] uses pre-shared key authentication
vpc2-to-vpc1:   child:  172.16.0.0/16 === 10.10.2.0/24 TUNNEL
Security Associations (0 up, 0 connecting):
none

/etc/ipsec.conf ===============
conn %default
ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
authby=secret
keyexchange=ikev2
mobike=no

conn vpc2-to-vpc1
type=tunnel
left=%defaultroute
leftnexthope=%defaultroute
leftid=35.182.xx.xx
leftsubnet=172.16.0.0/16
right=3.88.xx.xx
rightsubnet=10.10.2.0/24
auto=start

/etc/ipsec.secrets ==================
35.182.xx.xx 3.88.xx : PSK "cisco123"
```

Note: I was able to setup the VPN between 2 Strongswan instances in different AWS account using the above config.

CSR Configngfig ==============

```
crypto ikev2 proposal ikev2proposal
encryption aes-cbc-256
integrity sha1
group 2
!
crypto ikev2 policy ikev2policy
match fvrf any
proposal ikev2proposal
!
crypto ikev2 keyring keys
peer strongswan
address 35.182.xx.xx
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
!
!
crypto ikev2 profile ikev2profile
match identity remote address 35.182.xx.xx 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local keys
!
!
!
crypto isakmp policy 10
authentication pre-share
group 2
!
```

```
!
crypto ipsec transform-set TS esp-aes esp-sha-hmac
mode tunnel
!
!
!
crypto map cmap 10 ipsec-isakmp
set peer 35.182.xx.xx
set transform-set TS
set ikev2-profile ikev2profile
match address cryptoacl
!
!
interface VirtualPortGroup0 <--- Default config on the CSR; didn't change anything
vrf forwarding GS
ip address 192.168.35.101 255.255.255.0
ip nat inside
no mop enabled
no mop sysid
!
interface GigabitEthernet1
ip address dhcp
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map cmap
!
interface GigabitEthernet2
ip address 10.10.2.70 255.255.255.192
ip nat inside
negotiation auto
no mop enabled
no mop sysid
!
iox
ip forward-protocol nd
ip tcp window-size 8192
ip http server
ip http authentication local
ip http secure-server
!
ip nat inside source list NATList interface GigabitEthernet1 overload
ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 vrf GS overload <--- Default config on the CSR
ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 10.10.2.1
ip route vrf GS 0.0.0.0 0.0.0.0 GigabitEthernet1 10.10.2.1 global<--- Default config on the CSR
ip ssh rsa keypair-name ssh-key
ip ssh version 2
ip ssh pubkey-chain
username ec2-user
key-hash ssh-rsa 791ED7536A4ED5E5E344 ec2-user
ip ssh server algorithm publickey ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-rsa
x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp521
ip scp server enable
!
ip access-list standard GS_NAT_ACL <--- Default config on the CSR
10 permit 192.168.35.0 0.0.0.255
!
ip access-list extended NATList
10 deny   ip 10.10.2.64 0.0.0.63 172.16.1.0 0.0.0.255
20 permit ip 10.10.2.64 0.0.0.63 any
ip access-list extended cryptoacl
10 permit ip 10.10.2.64 0.0.0.63 172.16.1.0 0.0.0.255

=====================================================

Linux strongSwan U5.6.2/K5.3.0-1023-aws
```

History

#1 - 15.06.2020 17:12 - Tobias Brunner

- Status changed from New to Feedback

- Assignee deleted (Andreas Steffen)

- Priority changed from Urgent to Normal

The Cisco box is configured to use weak DH group (group 2 = *modp1024*), which has been removed from strongSwan's default proposal years ago. You should change that to a stronger group (at least use group 14 = *modp2048*), see IKEv2CipherSuites for more infos.