strongSwan - Issue #3537

IPv6 Packets are not transferred from server to client through IPSec using RPC protocol

06.08.2020 14:59 - Gnaneswara Seshu Bheesetty

Status:	Feedback		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.1.3	**Resolution:**	

Description

Hi Team,
We have defined IPSec policy using IPv6 networks and have established security Association between the server and client.But when traffic is initiated we don't see any packets transfer through ipsec(checked with ipsec statusall command) when we used RPC prtocol. Below are the ipsec.conf files on both the systems.

Server side:
conn BAT_PC
type=transport
left=2001:1b70:8294:4700::178
lifetime=2
ike=aes256-sha512-modp4096
ikelifetime=2
esp=aes256-sha512-modp4096-noesn
right=2001:1b70:8294:4403:3::6
keyexchange=ikev2
rightsubnet=2001:1b70:8294:4403::/24
#leftsubnet=2001:1b70:8294:4700::/24
leftauth=psk
rightauth=psk
auto=add

Client side:
conn BAT_PC
type=transport
left=2001:1b70:8294:4700::178
lifetime=2
ike=aes256-sha512-modp4096
ikelifetime=2
esp=aes256-sha512-modp4096-noesn
right=2001:1b70:8294:4403:3::6
keyexchange=ikev2
rightsubnet=2001:1b70:8294:4403::/24
leftauth=psk
rightauth=psk
auto=add

ipsec statusall command output:
vAPZ023-SC-2-2:# ipsec statusall
Status of IKE charon daemon (strongSwan 5.1.3, Linux 4.4.121-92.129-default, x86_64):
uptime: 24 seconds, since Aug 06 05:41:25 2020
malloc: sbrk 2838528, mmap 0, used 664512, free 2174016
worker threads: 10 of 16 idle, 6/0/0/0 working, job queue: 0/0/0/0, scheduled: 6
loaded plugins: charon ldap pkcs11 aes des blowfish rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem openssl gcrypt af-alg fips-prf gmp agent xcbc cmac hmac ctr ccm gcm curl soup attr kernel-netlink resolve socket-default farp stroke smp updown eap-identity eap-sim eap-sim-pcsc eap-aka eap-aka-3gpp2 eap-simaka-pseudonym eap-simaka-reauth eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap eap-tnc xauth-generic xauth-eap xauth-pam tnc-imc tnc-imv tnc-tnccs tnccs-20 tnccs-11 tnccs-dynamic dhcp certexpire led duplicheck radattr addrblock unity
Listening IP addresses:
192.168.169.2
192.168.169.33
10.33.33.165

10.33.33.166
2001:1b70:8294:4403:3::6
2001:1b70:8294:4403:3::5
192.168.170.2
192.168.170.33
169.254.213.2
169.254.208.2
169.254.208.100
169.254.208.101
Connections:
BAT_PC: 2001:1b70:8294:4403:3::6...2001:1b70:8294:4700::178 IKEv2
BAT_PC: local: [2001:1b70:8294:4403:3::6] uses pre-shared key authentication
BAT_PC: remote: [2001:1b70:8294:4700::178] uses pre-shared key authentication
BAT_PC: child: 2001:1b00::/24 === 2001:1b00::/24 TRANSPORT
Security Associations (1 up, 0 connecting):
BAT_PC[1]: ESTABLISHED 14 seconds ago,
2001:1b70:8294:4403:3::6[2001:1b70:8294:4403:3::6]...2001:1b70:8294:4700::178[2001:1b70:8294:4700::178]
BAT_PC[1]: IKEv2 SPIs: 46cbc3dc4ffd4366_i* 4d2c2cff21ea6f54_r, pre-shared key reauthentication in 21 minutes
BAT_PC[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096
BAT_PC{7}: INSTALLED, TUNNEL, ESP SPIs: cad38c97_i cce1e59a_o
BAT_PC{7}: AES_CBC_256/HMAC_SHA2_512_256, 0 bytes_i, 0 bytes_o, rekeying disabled
BAT_PC{7}:   2001:1b00::/24 === 2001:1b70:8294:4700::178/128

We tried with similar configuration but with IPv4 networks and RPC protocol but this time were able to see packets transfer from server to client.Below are the ipsec.conf files.

Server side:
conn BAT_PC
type=transport
right=10.35.15.178
lifetime=2
ike=aes256-sha512-modp4096
ikelifetime=2
esp=aes256-sha512-modp4096-noesn
left=10.33.33.166
keyexchange=ikev2
leftsubnet=10.33.33.0/24
rightsubnet=10.35.15.0/24
leftauth=psk
rightauth=psk
auto=add

Client side:
conn BAT_PC
type=transport
left=10.35.15.178
lifetime=2
ike=aes256-sha512-modp4096
ikelifetime=2
esp=aes256-sha512-modp4096-noesn
right=10.33.33.166
keyexchange=ikev2
rightsubnet=10.33.33.0/24
leftauth=psk
rightauth=psk
auto=add

ipsec statusall command output:
root@tp403vapz023lbat1:/home/administrator/Billing# ipsec statusall
Status of IKE charon daemon (strongSwan 5.7.2, Linux 5.3.0-62-generic, x86_64):
uptime: 20 minutes, since Aug 06 04:57:33 2020
malloc: sbrk 2822144, mmap 0, used 1573216, free 1248928
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 5
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:

10.35.15.178
2001:1b70:8294:4700:20c:29ff:fe7a:33ac
2001:1b70:8294:4700::178
Connections:
BAT_PC: 10.35.15.178...10.33.33.166 IKEv2
BAT_PC: local: [10.35.15.178] uses pre-shared key authentication
BAT_PC: remote: [10.33.33.166] uses pre-shared key authentication
BAT_PC: child: dynamic === 10.33.33.0/24 TRANSPORT
Security Associations (1 up, 0 connecting):
BAT_PC[1]: ESTABLISHED 20 minutes ago, 10.35.15.178[10.35.15.178]...10.33.33.166[10.33.33.166]
BAT_PC[1]: IKEv2 SPIs: 9500b62564ee2e07_i f0d51234dc0de1c1_r*, pre-shared key reauthentication in 34 minutes
BAT_PC[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096
BAT_PC{590}: INSTALLED, TUNNEL, reqid 590, ESP SPIs: c4847cd5_i c9438169_o
BAT_PC{590}: AES_CBC_256/HMAC_SHA2_512_256/MODP_4096, **9188680 bytes_i (6481 pkts, 0s ago), 126704 bytes_o (2302 pkts, 2s ago)**, rekeying disabled
BAT_PC{590}:   10.35.15.178/32 === 10.33.33.0/24

Please help us resolve this issue.

Thanks in advance.

Regards
Gnaneswara Seshu

History

#1 - 17.08.2020 15:40 - Tobias Brunner

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

I guess your RPC client/server doesn't use IPv6 or those specific addresses.

#2 - 01.09.2020 11:25 - Gnaneswara Seshu Bheesetty

Tobias Brunner wrote:

> I guess your RPC client/server doesn't use IPv6 or those specific addresses.

We were able to see packet transfer if ipsec.conf on remote is updated by adding leftsubnet parameter.

conn BAT_PC
type=transport
left=2001:1b70:8294:4700::178
lifetime=2
ike=aes256-sha512-modp4096
ikelifetime=2
esp=aes256-sha512-modp4096-noesn
right=2001:1b70:8294:4403:3::6
keyexchange=ikev2
rightsubnet=2001:1b70:8294:4403::/24
leftsubnet=2001:1b70:8294:4700::/24
leftauth=psk
rightauth=psk
auto=add

But by adding leftsubnet parameter we are facing some connectivity issue with other protocols like ftp,sftp protocol.

Is it suggested to use the same configuration for all protocols or we need to use different configurations for different protocols ?

#3 - 01.09.2020 11:35 - Tobias Brunner

> type=transport

Note that this is incorrect for non-host-to-host configs (tunnel mode is automatically negotiated in this case as you can see in the status output).

> Is it suggested to use the same configuration for all protocols or we need to use different configurations for different protocols ?

It's completely your own choice whether you restrict the policies further (protocol/port) or, for instance, use marks to perhaps dynamically decide what traffic to tunnel.

#4 - 01.09.2020 12:50 - Gnaneswara Seshu Bheesetty

Tobias Brunner wrote:

> type=transport

> Note that this is incorrect for non-host-to-host configs (tunnel mode is automatically negotiated in this case as you can see in the status output).

> Is it suggested to use the same configuration for all protocols or we need to use different configurations for different protocols ?

> It's completely your own choice whether you restrict the policies further (protocol/port) or, for instance, use marks to perhaps dynamically decide what traffic to tunnel.

We have traffic which will be transferred between two hosts using ftp/sftp or rpc protocols,is it possible to restrict such protocol as well?I guess we can use port for restriction in our case. Can I get some reference about marks option?

Files

ipsec_ipv4_file.txt	803 Bytes	06.08.2020	Gnaneswara Seshu Bheesetty
IPSEC_conf_ipv6.txt	889 Bytes	06.08.2020	Gnaneswara Seshu Bheesetty