Site-To-Site IPSec VPN Palo Alto VM-300-FW with Ubuntu v18.08 & StrongSwan v5.6.2

IKEv1 & IKEv2

On STC OpenStack Cloud

Taher A. Bahashwan

Cloud Advisory Expert

STC Solution

@taher9990

Sept 2019

Contents

Disclaimer 4
WARNING --- IPs Misuse 4
Network Topology 5
Successful Tunnel Status 6
Setup and Prepare VMs Servers 7
Ubuntu VM Machine Specs 7
Server Specs 7
Palo Alto VM Machine Specs 7
Network IPs on both sides: 7
Site-A-Ubuntu Preparation: 8
Site-B-Palo Alto VM-FW Preparation: 9
Site-A-Ubuntu Setup Network Configurations 9
Site-B- Palo Alto Setup Network Configurations 11
Network Show Configurations 13
Site-A-Ubuntu Network Configurations 13
Site-A ifconfig 13
Site-B-Palo Alto Network Configurations 14
Site-B ifconfig 15
IPSec Setup on Ubuntu 18.04 & Palo Alto VM-FW 15
Site-A-Setup IPSec Configurations 16
Site-B-PaloAlto-FW-Setup IPSec Configurations 17
IPSec Show Configurations 19
Site-A IPsec Configurations: 19
Site-B IPsec Configurations: 20
Show and Troubleshooting Commads 23
IPsec Detailed Status and Results 24
Site-A IPsec XFRM Policies and States 24
Site-B IPsec XFRM Policies and States 26
Site-A IPsec status all 29
Site-B IPsec status all 29
Packet Captures and Traces 30

Test Connectivity from a client in Site-A to another client in Site-B resides behind Palo Alto FW 30
Test Connectivity from a client behind Site-B-Palo Ato to another client in Site-A..... 31
Site-A Packet captures..... 33

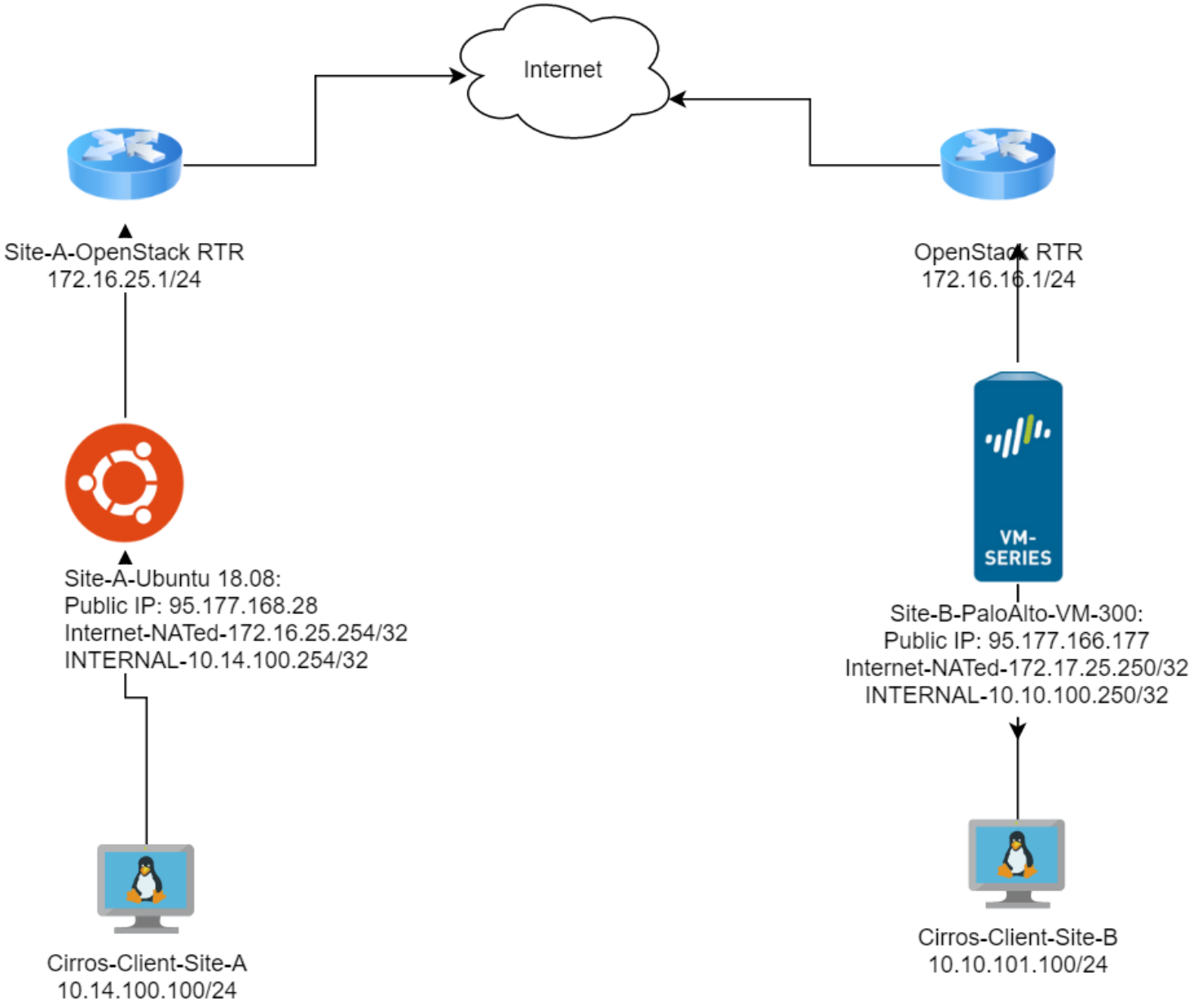
Disclaimer

This article is made for educational and testing purposes, and you might find few settings that are not made for production, please do your full testing and follow your organizations best practices and standards along with the steps and guides in this document to get a full complete working solution.

WARNING --- IPs Misuse

All Public IPs that we use in this article are randomly selected from STC Public Cloud, and they will be deleted from our Cloud tenant after we complete the test, so you are not allowed to use or conduct any activity in to these IPs, if activity identified it will be considered as criminal activity, STC Cloud personnel have the right to take legal actions against you or your organization.

Network Topology



Successful Tunnel Status

Site-A-Ubuntu side Success Status

			IKE Gateway/Satellite				Tunnel Interface				
Name	Status	Type	Interface	Local IP	Peer Address	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
IPSec-To-Linux	Tunnel Info	Auto Key	ethernet1/1	172.16.16.250/24	95.177.168.28	IKE Info	tunnel.1	default (Show Routes)	vsys1	IPSec-Using-Internet-Interface	

Tunnel Info - IPSec-To-Linux

1 item

Name	Local IP	L... P...	Peer IP	M... IP	Remote IP	R... P...	Pkt Encap	Pkt Dec...	Byte Encap	Byte Decap	A...	T...	P...
IPSec-To-Linux:Internal	172.16.16.250	0	95.177.168.28		10.14.100.0/24	0	1192	1385	151776	170000	0	1	0

Site-A-Ubuntu side Success Status

95.177.168.28 - PuTTY

```
root@ipsec-test1-site-a-ubuntu1:~# ipsec up Site-A-To-PaloAlto
generating QUICK_MODE request 4137111492 [ HASH SA No ID ID ]
sending packet: from 172.16.25.254[4500] to 95.177.166.177[4500] (204 bytes)
received packet: from 95.177.166.177[4500] to 172.16.25.254[4500] (172 bytes)
parsed QUICK_MODE response 4137111492 [ HASH SA No ID ID ]
CHILD_SA Site-A-To-PaloAlto{4} established with SPIs ca65f222_i af2edf0e_o and TS 10.14.100.0/24 === 10.10.101.0/24
generating QUICK_MODE request 4137111492 [ HASH ]
sending packet: from 172.16.25.254[4500] to 95.177.166.177[4500] (60 bytes)
connection 'Site-A-To-PaloAlto' established successfully
root@ipsec-test1-site-a-ubuntu1:~#
```

Setup and Prepare VMs Servers

Ubuntu VM Machine Specs

Server Specs

```
CPU: 1 vCPU Memory: 1 GB, HDD: 30 GB

         Icon name: computer-vm

           Chassis: vm

    Virtualization: kvm

  Operating System: Ubuntu 18.04.3 LTS

            Kernel: Linux 4.15.0-64-generic

      Architecture: x86-64
```

Palo Alto VM Machine Specs

```
CPU: 8 vCPU Memory: 8 GB, HDD: 30 GB
STC Cloud: RUH2 - Flavor: R1-Network-8
Palo Alto VM Software:

time: Sat Sep 21 09:34:11 2019
uptime: 0 days, 2:16:52
family: vm
model: PA-VM
vm-license: VM-300
vm-mode: KVM
cloud-mode: non-cloud
sw-version: 8.1.3
logdb-version: 8.1.8
platform-family: vm
vpn-disable-mode: off
multi-vsys: off
operational-mode: normal
```

Network IPs on both sides:

Site-A-Network IPs:

Public IP: 95.177.168.28

Internet-NATed-172.16.25.254/24

INTERNAL-10.14.100.254/24

Client Test Machine: 10.14.100.100/24

Site-B-Network IPs:

Public IP: 95.177.166.177

Internet-NATed-172.16.16.250/24

INTERNAL-10.10.101.250/24

Client Test Machine: 10.10.101.100/24

Site-A-Ubuntu Preparation:

```
timedatectl set-timezone Asia/Riyadh
apt update && sudo apt upgrade -y && apt install strongswan -y
&& apt install -y traceroute && apt install firewall-cmd -y
```

To enable you access Ubuntu with Username and password and access it with root

```
cat >> /etc/ssh/sshd_config << EOF
PubkeyAuthentication yes
AuthenticationMethods publickey password
AuthorizedKeysFile      .ssh/authorized_keys
PermitRootLogin yes
PasswordAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM yes
EOF

vi /root/.ssh/authorized_keys
Remove anything before these words "ssh-rsa"

service sshd restart
```

Site-B-Palo Alto VM-FW Preparation:

Due to an issue in Palo Alto VM FW and STC Cloud we advise you to disable DPDK on Palo Alto VM-FW

```
set system setting dpdk-pkt-io off
request restart system
```

```
You need to do the basic firewall setup:
    - Set Interfaces IPs using GUI
    - Setup Network Services e.g. NTP, DNS
    - Set Management IP for Firewall.
```

Site-A-Ubuntu Setup Network Configurations

```
cat >> /etc/sysctl.conf << EOF
net.ipv4.ip_forward = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
EOF
```

```
List Interface Name + MAC
ip -o link | awk '$2 != "lo:" {print $2, $(NF-2)}'
```

Note: ***After making below configurations make sure that the default route is still maintained by the system, otherwise you will lose the connectivity to the server via eth0 or ens3 after the reboot, we have added the static route config in the below commands under*** routes: ***line***

```
sudo su
cat > /etc/netplan/50-cloud-init.yaml <<EOF
network:
  version: 2
  ethernets:
    ens3:
      addresses: [172.16.25.254/24]
      routes:
        - to: 0.0.0.0/0
          via: 172.16.25.1
      gateway4: 172.16.25.1
      dhcp4: false
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      optional: true
    ens4:
      addresses: [10.14.100.254/24]
      dhcp4: false
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      optional: true
EOF

sudo netplan --debug try
sudo netplan --debug apply
```

Configure the NAT for Network 10.14.100.0/24 to be able to go to Internet

```
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I
POSTROUTING -o ens3 -j MASQUERADE -s 10.14.100.0/24

firewall-cmd --complete-reload

sysctl -p /etc/sysctl.conf
```

Site-B- Palo Alto Setup Network Configurations

Interfaces setup:

Note: Highlighted interfaces are being used in this test:

Ethernet | VLAN | Loopback | Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3	MGMT		172.16.16.250/24	default	Untagged	none	Internet		Internet
ethernet1/2	Layer3	Ping-Only		Dynamic-DHCP Client	default	Untagged	none	MPLS		MPLS
ethernet1/3	Layer3	Ping-Only		Dynamic-DHCP Client	default	Untagged	none	IPSec-Dedicated-Interface		IPSec
ethernet1/4	Layer3	Ping-Only		Dynamic-DHCP Client	default	Untagged	none	Inside		Inside
ethernet1/5	Layer3	Ping-Only		Dynamic-DHCP Client	default	Untagged	none	PRD-LAB-DMZ-LB-VIPs		PRD-LAB-DMZ-LB-VIPs
ethernet1/6	Layer3	Ping-Only		Dynamic-DHCP Client	default	Untagged	none	PRD-LAB-DMZ-VLAN100		PRD-LAB-DMZ-VLAN100
ethernet1/7	Layer3	Ping-Only		10.10.101.250/24	default	Untagged	none	PRD-LAB-DMZ-VLAN101		PRD-LAB-DMZ-VLAN101

Ethernet | VLAN | Loopback | Tunnel

Interface	Management Profile	IP Address	Virtual Router	Security Zone	Features	Comment
tunnel		none	none	none		
tunnel.1	Ping-Only	none	default	IPSec-Using-Internet-Interface		IPSec-To-Linux-95.177.166.177

Routing Configurations:

Name
default

Virtual Router - default

Router Settings
Static Routes
Redistribution Profile
RIP
OSPF
OSPFv3
BGP

IPv4 | IPv6

2 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	M...	BFD	Route Table
To-Internet	0.0.0.0/0	ethernet1/1	ip-address	172.16....	default	10	None	unicast
IPSec-To-Linux	10.14.100.0/24	tunnel.1			default	10	None	unicast

Security & NAT Policies

Security:

				Source				Destination		Rule Usage				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service
1	IPSec-Tunnel	none	universal	Internet IPSec-Using-Internet-Interface PRD-LAB-DMZ-VLAN101	10.10.101.0/24 10.14.100.0/24 95.177.166.177 95.177.168.28	any	any	Internet IPSec-Using-Internet-Interface PRD-LAB-DMZ-VLAN101	10.10.101.0/24 10.14.100.0/24 95.177.166.177 95.177.168.28	2	2019-09-...	2019-09-...	any	any
2	*Temp-Allow-Any*	*none*	*universal*	*any*	*any*	*any*	*any*	*any*	*any*	0	-	-	*any*	*any*

NAT:

			Original Packet						Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit C
1	NAT-To-Internet	none	Inside PRD-LAB-DM... PRD-LAB-DM... PRD-LAB-DM...	Internet	any	any	any	any	dynamic-ip-and-port 172.16.16.250/32	none	10

Network Show Configurations

Site-A-Ubuntu Network Configurations

```
root@ipsec-test1-site-a-ubuntu1:~# cat /etc/netplan/50-cloud-
init.yaml
network:
  version: 2
  ethernets:
    ens3:
      addresses: [172.16.25.254/24]
      gateway4: 172.16.25.1
      dhcp4: false
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      optional: true
    ens4:
      addresses: [10.14.100.254/24]
      #      gateway4: 10.14.100.1
      dhcp4: false
      nameservers:
        addresses: [1.1.1.1,8.8.8.8]
      optional: true
root@ipsec-test1-site-a-ubuntu1:~#
```

Site-A ifconfig

```
root@ipsec-test1-site-a-ubuntu1:~# ifconfig -a
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.25.254  netmask 255.255.255.0  broadcast
172.16.25.255
        inet6 fe80::bd:17ff:fec8:dd90  prefixlen 64  scopeid
0x20<link>
        ether 02:bd:17:c8:dd:90  txqueuelen 1000  (Ethernet)
        RX packets 1089  bytes 147403 (147.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1528  bytes 218395 (218.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
        inet 10.14.100.254  netmask 255.255.255.0  broadcast
10.14.100.255
        inet6 fe80::7c:b5ff:fee5:5f28  prefixlen 64  scopeid
0x20<link>
        ether 02:7c:b5:e5:5f:28  txqueuelen 1000  (Ethernet)
        RX packets 563  bytes 39567 (39.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 125  bytes 6334 (6.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 106  bytes 8350 (8.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 106  bytes 8350 (8.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
0

root@ipsec-test1-site-a-ubuntu1:~#
```

Site-B-Palo Alto Network Configurations

```
admin@PA-VM> test routing fib-lookup virtual-router default ip 10.14.100.100

--------------------------------------------------------------------------------
runtime route lookup
--------------------------------------------------------------------------------
virtual-router:   default
destination:      10.14.100.100
result:
  interface tunnel.1, metric 10
--------------------------------------------------------------------------------
```

Site-B ifconfig

```
admin@PA-VM> show interface all

total configured hardware interfaces: 8

name                      id    speed/duplex/state        mac address
--------------------------------------------------------------------------------
ethernet1/1               16    auto/auto/up              02:02:40:ea:88:3b
ethernet1/2               17    auto/auto/up              02:2b:ae:2f:1d:5b
ethernet1/3               18    auto/auto/up              02:51:47:c1:cb:89
ethernet1/4               19    auto/auto/up              02:82:47:3f:7d:57
ethernet1/5               20    auto/auto/up              02:d3:3c:6d:00:3b
ethernet1/6               21    auto/auto/up              02:62:c4:45:66:72
ethernet1/7               22    auto/auto/up              02:f2:c8:db:c8:2f
tunnel                    4     [n/a]/[n/a]/up            e4:a7:49:fb:4b:04

aggregation groups: 0


total configured logical interfaces: 9

name                 id    vsys zone              forwarding                tag
address
------------------- ----- ---- ---------------- ------------------------- ------ --
----------------
ethernet1/1          16    1    Internet          vr:default                0
172.16.16.250/24
ethernet1/2          17    1    MPLS              vr:default                0
172.16.20.250/32
ethernet1/3          18    1    IPSec-Dedicated- vr:default                0
172.16.30.250/32
ethernet1/4          19    1    Inside            vr:default                0
10.10.11.250/32
ethernet1/5          20    1    PRD-LAB-DMZ-LB-V vr:default                0
10.10.150.250/32
ethernet1/6          21    1    PRD-LAB-DMZ-VLAN vr:default                0
10.10.100.250/32
ethernet1/7          22    1    PRD-LAB-DMZ-VLAN vr:default                0
10.10.101.250/24
tunnel               4     1                      N/A                       0
N/A
tunnel.1             256   1    IPSec-Using-Inte vr:default                0
N/A
```

IPSec Setup on Ubuntu 18.04 & Palo Alto VM-FW

We are going to use IKEv1 and you can use IKE2 by changing this line in below config:

```
keyexchange = ikev1
```

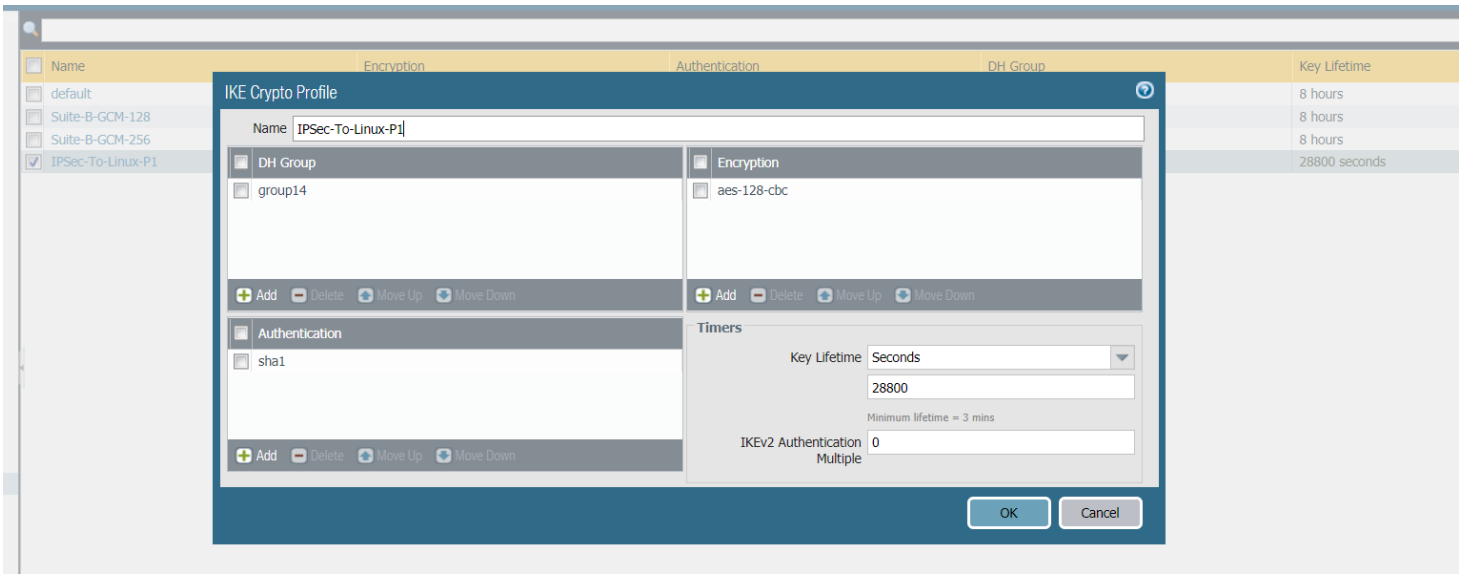
Site-A-Setup IPSec Configurations

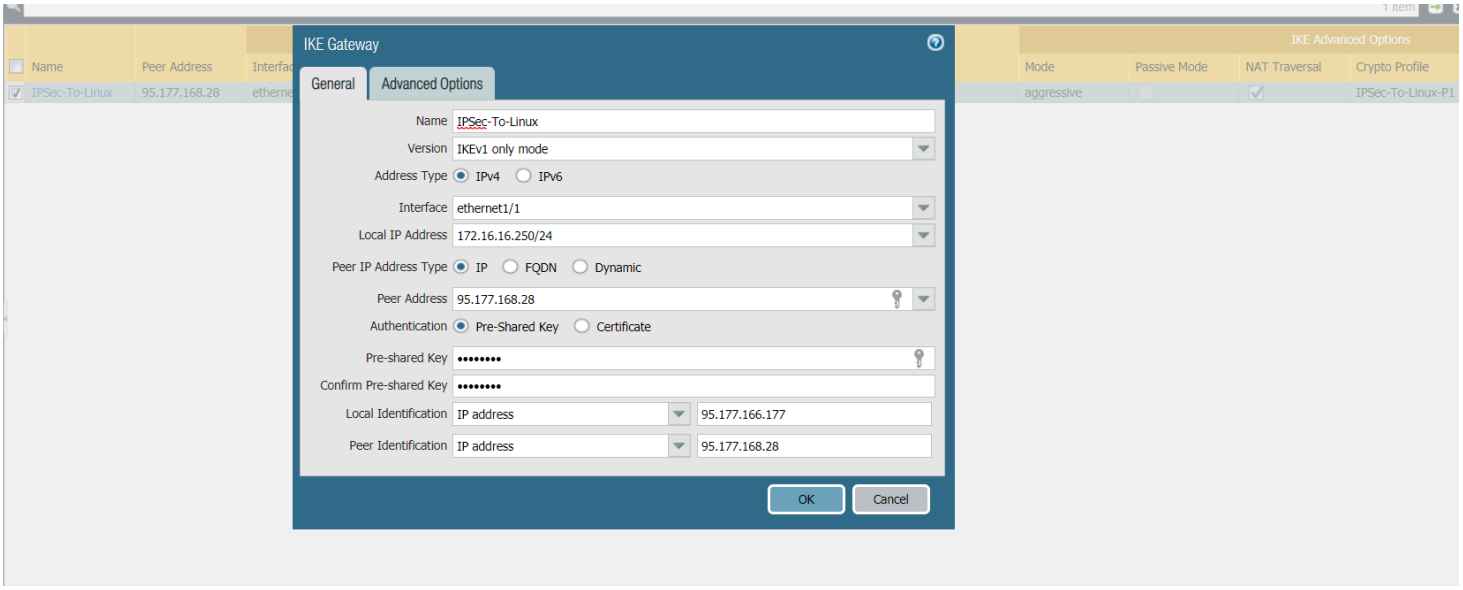
```
cat > /etc/ipsec.secrets <<EOF
95.177.168.28 95.177.166.177 : PSK "P@ssw0rd"
EOF


vi /etc/ipsec.conf
# basic configuration
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no

conn Site-A-To-B         #<----(PaloAlto)
       aggressive = yes
       # fragmentation = yes
        keyexchange = ikev1
        authby=secret
        installpolicy = yes
        type = tunnel
        left=172.16.25.254
        leftid=95.177.168.28
        rightid=95.177.166.177
        leftsubnet=10.14.100.0/24
        right=95.177.166.177
        rightsubnet=10.10.101.254/24
        ike=aes128-sha1-modp2048!
        esp=aes128-sha256
        forceencaps = yes
        keyingtries=0
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=10s
        dpdtimeout=60s
        dpdaction=restart
```

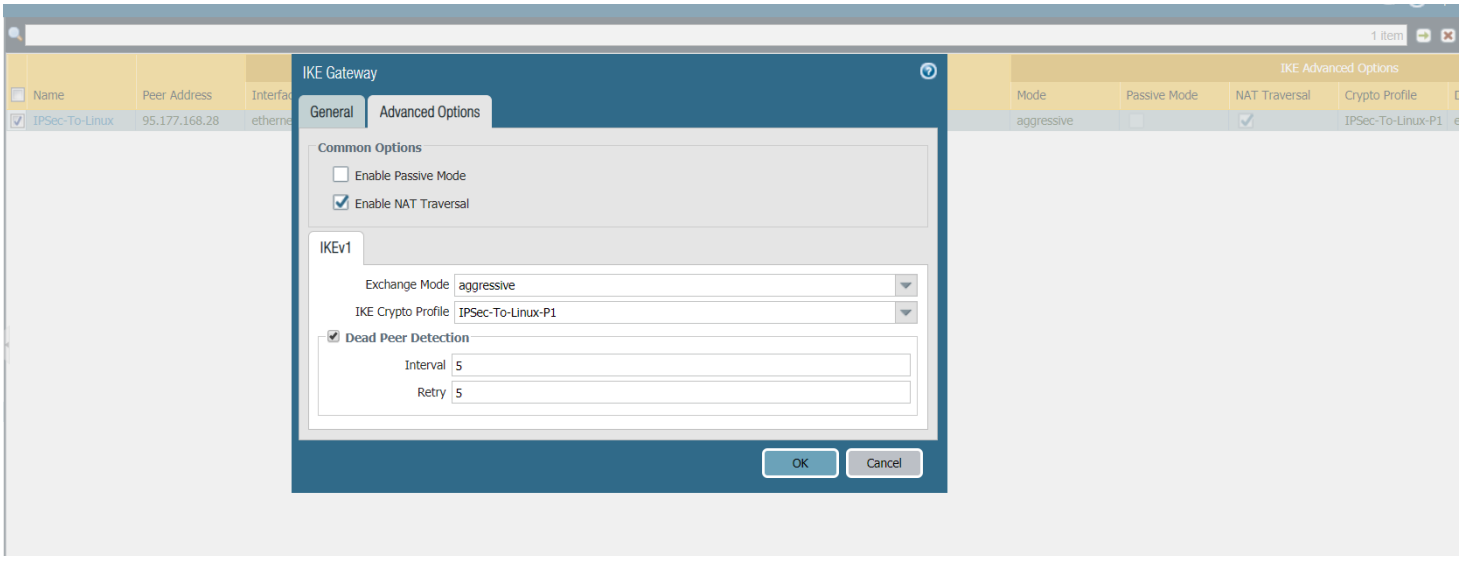
```
        auto=start

sudo ipsec restart
```

Site-B-PaloAlto-FW-Setup IPSec Configurations

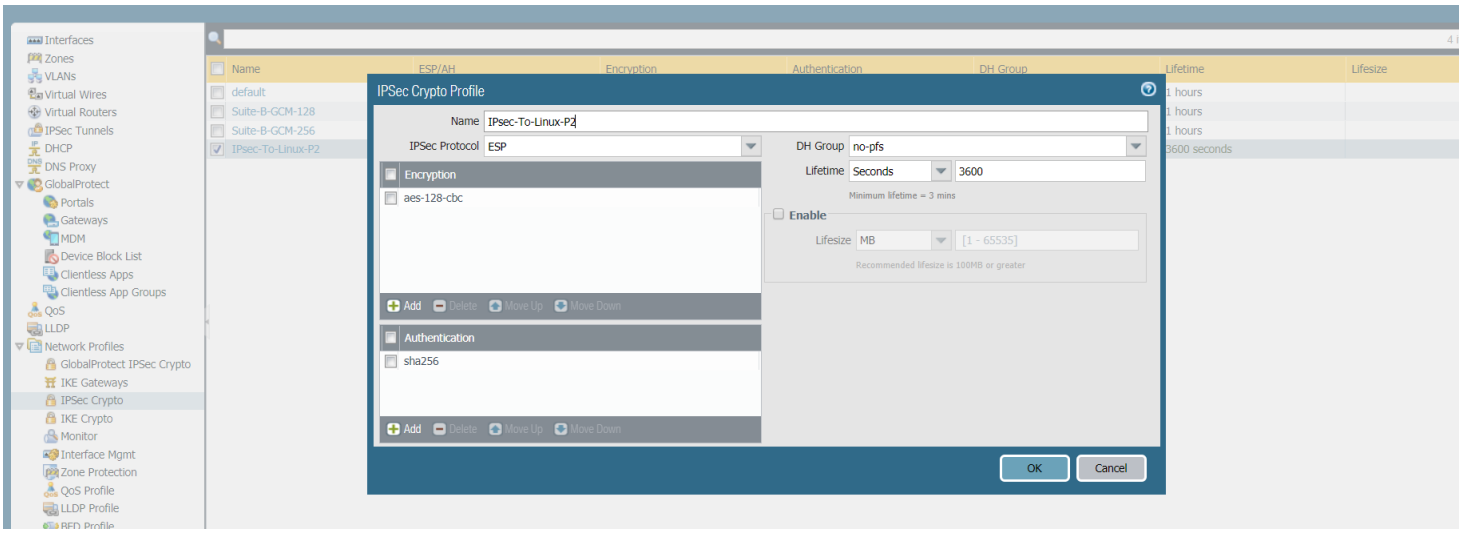
Phase 1 Configurations

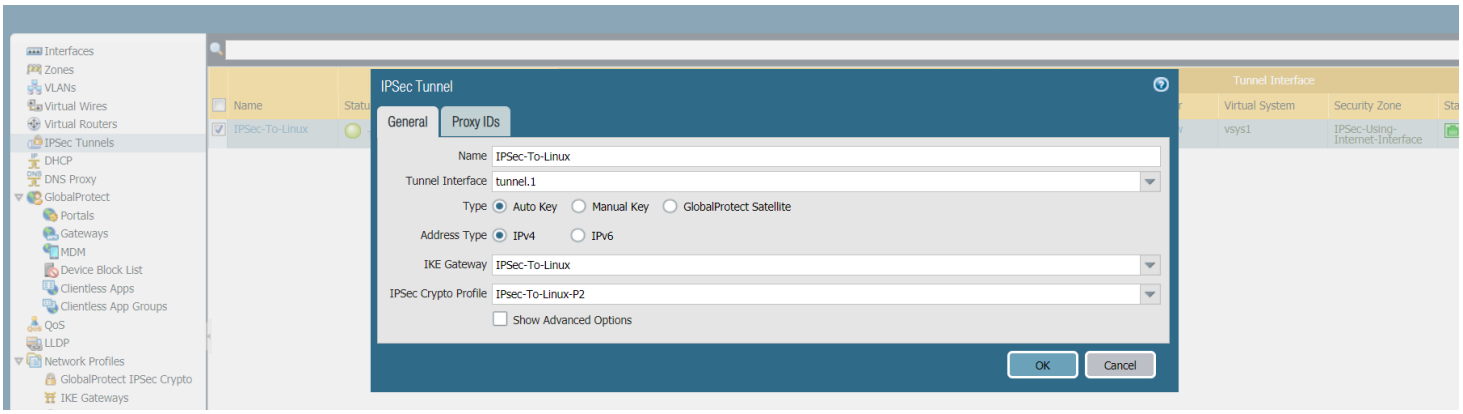


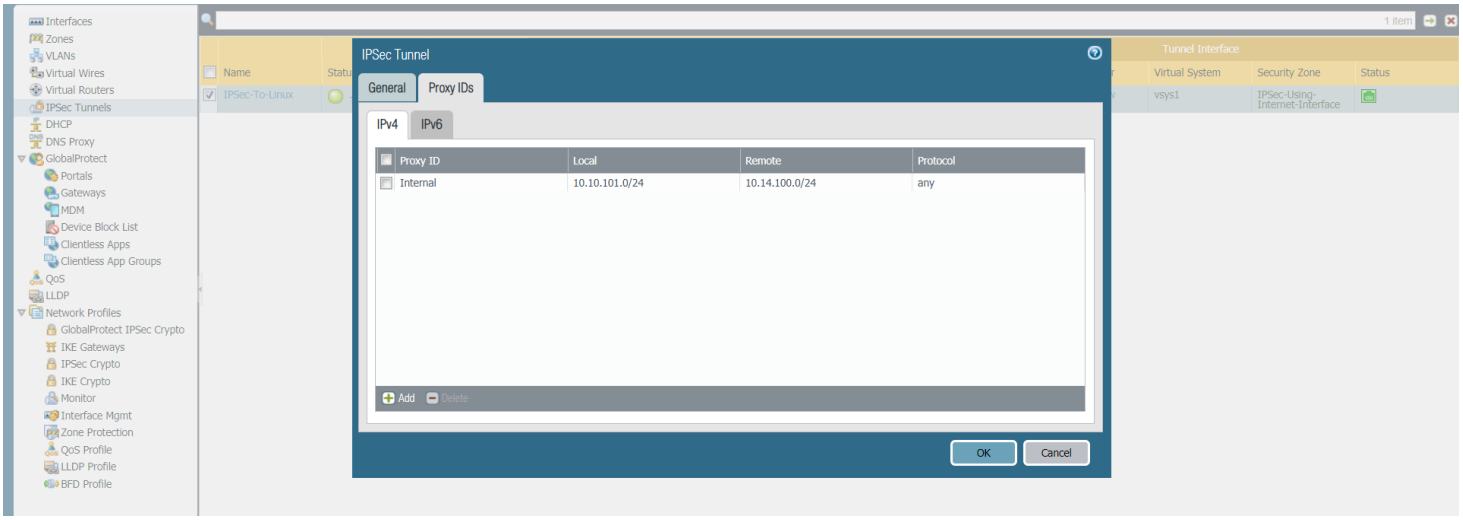




Phase 2 Configurations







IPSec Show Configurations

Site-A IPsec Configurations:

```
root@ipsec-test1-site-a-ubuntu1:~# cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
        charondebug="all"
        uniqueids=yes
        strictcrlpolicy=no
# Add connections here.
conn Site-A-To-PaloAlto
       aggressive = yes
       # fragmentation = yes
        keyexchange = ikev1
```

```
        authby=secret
        installpolicy = yes
        type = tunnel
        left=172.16.25.254
        leftid=95.177.168.28
        rightid=95.177.166.177
        leftsubnet=10.14.100.0/24
        right=95.177.166.177
        rightsubnet=10.10.101.254/24
        ike=aes128-sha1-modp2048!
        esp=aes128-sha256
        forceencaps = yes
        keyingtries=0
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=10s
        dpdtimeout=60s
        dpdaction=restart
        auto=start
```

Note: To add more subnets to the rightsubnet or left you can do it in this way

```
    leftsubnet={10.14.100.0/24,10.12.100.0/24,…}
```

```
root@ipsec-test1-site-a-ubuntu1:~# cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for
authentication.
95.177.168.28 95.177.166.177 : PSK "P@ssw0rd"
```

Site-B IPsec Configurations:

```
admin@PA-VM> show vpn ike-sa detail
> gateway   Show for given IKE gateway

admin@PA-VM> show vpn ike-sa detail gateway
  IPSec-To-Linux   IPSec-To-Linux
  <value>          Show for given IKE gateway

admin@PA-VM> show vpn ike-sa detail gateway IPSec-To-Linux
```

```
IKE Gateway IPSec-To-Linux, ID 1 172.16.16.250:4500     =>
95.177.168.28:4500
  Current time: Sep.21 08:39:51

IKE Phase1 SA:
  Cookie:  53182364A978DAB8:F408F466FC38FAE8  Resp
        State:      Dying
        Mode:       Aggr
        Authentication:  PSK
        Proposal:   AES128-CBC/SHA1/DH14
        NAT:        ME PEER
        Message ID: 0, phase 2: 0
        Phase 2 SA created : 1
        Created:    Sep.21 07:59:35, 40 minutes 16 seconds ago
        Expires:    Sep.21 15:59:35


admin@PA-VM> show vpn ike-sa gateway IPSec-To-Linux

IKEv1 phase-1 SAs
GwID/client IP  Peer-Address           Gateway Name
Role Mode Algorithm             Established     Expiration
V  ST Xt Phase2
--------------  ------------           ------------           --
-- ---- ---------             -----------     ----------      -
-- -- ------
1               95.177.168.28:4500     IPSec-To-Linux
Resp Aggr PSK/DH14/A128/SHA1    Sep.21 07:59:35 Sep.21 15:59:35
v1 13 1  1

Show IKEv1 IKE SA: Total 1 gateways found. 1 ike sa found.


IKEv1 phase-2 SAs
Gateway Name            TnID     Tunnel                  GwID/IP
Role Algorithm           SPI(in)  SPI(out) MsgID    ST Xt
------------            ----     ------                  -------
---- ---------           -------  -------- -----    -- --
```

```
IPSec-To-Linux         1        IPSec-To-Linux:Interna 1
Resp ESP/    /tunl/SHA2 C322893F C38F7B99 33D28876 9  1

Show IKEv1 phase2 SA: Total 1 gateways found. 1 ike sa found.


There is no IKEv2 SA found.

admin@PA-VM>



===================================Palo Alto Phase 2 Show Status
and Configurations====================
admin@PA-VM> show vpn ipsec-sa tunnel
  IPSec-To-Linux:Internal   IPSec-To-Linux:Internal
  <value>                   Show for given VPN tunnel

admin@PA-VM> show vpn ipsec-sa tunnel IPSec-To-Linux:Internal

GwID/client IP  TnID   Peer-Address           Tunnel(Gateway)
Algorithm          SPI(in)  SPI(out) life(Sec/KB)

--------------  ----   ------------           ---------------
---------          -------  -------- ------------

1               1      95.177.168.28:4500     IPSec-To-
Linux:Internal(IPSec-To-Linux)        ESP/A128/SHA256
C322893F C38F7B99 1123/0


Show IPSec SA: Total 1 tunnels found. 1 ipsec sa found.



admin@PA-VM> show vpn tunnel
> match    if the name contains the string or not
> name     Show for given VPN tunnel
  |        Pipe through a command
```

```
  <Enter>  Finish input

admin@PA-VM> show vpn tunnel name
  IPSec-To-Linux:Internal   IPSec-To-Linux:Internal
  <value>                   Show for given VPN tunnel

admin@PA-VM> show vpn tunnel name IPSec-To-Linux:Internal

TnID   Name                            Gateway              Local
Proxy IP       Ptl:Port   Remote Proxy IP      Ptl:Port
Proposals

----   ----                            -------              -----
---------       --------   ---------------      --------   -----
----

1      IPSec-To-Linux:Internal         IPSec-To-Linux
10.10.101.0/24       0:0        10.14.100.0/24       0:0
ESP tunl [no-pfs][AES128][SH
A256] 3600-sec 0-kb

Show IPSec tunnel config: Total 1 tunnels found.
```

Show and Troubleshooting Commads

Ubuntu-StronSwan Troubleshooting commands:

```
ipsec status
ipsec statusall
ipsec restart
ipsec up <connection name>

tcpdump -i any -nn icmp or esp or udp port 500 or udp port 4500
and " host 172.16.25.254 or host 95.177.166.177 or host
10.10.101.100"
```

```
tcpdump -ttttnnvvS -i any -nn icmp or esp or udp port 500 or udp
port 4500


tail -f /var/log/secure
tail -f var/log/daemon.log
tail -f/var/log/auth.log
tail -f /var/log/messages
```

Palo Alto VM- Troubleshooting commands:

```
debug ike gateway WU-GW-Environment1 on debug

debug ike global on debug
less mp-log ikemgr.log
tail follow yes  mp-log ikemgr.log
debug ike pcap on
view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap
ikemgr.pcap
debug ike pcap off
 show running tunnel flow tunnel-id 2
```

Phase 2 Debug:

```
debug ike tunnel <Tunnel-Name - and Id> on debug
tail follow yes mp-log ikemgr.log
```

IPsec Detailed Status and Results

Site-A IPsec XFRM Policies and States

```
root@ipsec-test1-site-a-ubuntu1:~# sudo ip xfrm policy
src 10.14.100.0/24 dst 10.10.101.0/24
        dir out priority 375423
        tmpl src 172.16.25.254 dst 95.177.166.177
                proto esp spi 0xce31a8c8 reqid 5 mode tunnel
src 10.10.101.0/24 dst 10.14.100.0/24
        dir fwd priority 375423
        tmpl src 95.177.166.177 dst 172.16.25.254
```

```
                proto esp reqid 5 mode tunnel
src 10.10.101.0/24 dst 10.14.100.0/24
        dir in priority 375423
        tmpl src 95.177.166.177 dst 172.16.25.254
                proto esp reqid 5 mode tunnel
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket in priority 0
src 0.0.0.0/0 dst 0.0.0.0/0
        socket out priority 0
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0
src ::/0 dst ::/0
        socket in priority 0
src ::/0 dst ::/0
        socket out priority 0


root@ipsec-test1-site-a-ubuntu1:~# sudo ip xfrm state

src 172.16.25.254 dst 95.177.166.177
        proto esp spi 0xce31a8c8 reqid 5 mode tunnel
        replay-window 0 flag af-unspec
        auth-trunc hmac(sha256)
0x2aa0377c2eecd05d931876b5c224504e82b8389254cfe2406901cc2bd403a9
2b 128
        enc cbc(aes) 0x2eede602001ed71f5bd018ca60b8c401
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x0, oseq 0x2, bitmap
0x00000000
src 95.177.166.177 dst 172.16.25.254
        proto esp spi 0xc2283ccb reqid 5 mode tunnel
        replay-window 32 flag af-unspec
```

```
        auth-trunc hmac(sha256)
0x9d7678d0b7a32b6052b15de7e5bfe93cf5256e7f74df2191db52ee876b0651
91 128
        enc cbc(aes) 0x699024cc18b32526b8b30434e1a7c3c0
        encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
        anti-replay context: seq 0x2, oseq 0x0, bitmap
0x00000003
```

Site-B IPsec XFRM Policies and States

```
admin@PA-VM> show vpn flow name IPSec-To-Linux:Internal

tunnel  IPSec-To-Linux:Internal
        id:                     1
        type:                   IPSec
        gateway id:             1
        local ip:               172.16.16.250
        peer ip:                95.177.168.28
        inner interface:        tunnel.1
        outer interface:        ethernet1/1
        state:                  active
        session:                2003
        tunnel mtu:             1416
        soft lifetime:          3505
        hard lifetime:          3600
        lifetime remain:        1273 sec
        lifesize remain:        N/A
        latest rekey:           2327 seconds ago
        monitor:                off
          monitor packets seen: 0
          monitor packets reply:0
        en/decap context:       2
        local spi:              C322893F
        remote spi:             C38F7B99
        key type:               auto key
        protocol:               ESP/UDP[4500->4500]
        auth algorithm:         SHA256
        enc  algorithm:         AES128
        proxy-id:
          local ip:             10.10.101.0/24
```

```
          remote ip:            10.14.100.0/24
          protocol:             0
          local port:           0
          remote port:          0
        anti replay check:      yes
        copy tos:               no
        authentication errors:  0
        decryption errors:      0
        inner packet warnings:  0
        replay packets:         0
        packets received
          when lifetime expired:0
          when lifesize expired:0
        sending sequence:       700
        receive sequence:       700
        encap packets:          700
        decap packets:          700
        encap bytes:            89600
        decap bytes:            89600
        key acquire requests:   0
        owner state:            0
        owner cpuid:            s1dp0
        ownership:              1


admin@PA-VM> show running tunnel flow name IPSec-To-
Linux:Internal

tunnel  IPSec-To-Linux:Internal
        id:                     1
        type:                   IPSec
        gateway id:             1
        local ip:               172.16.16.250
        peer ip:                95.177.168.28
        inner interface:        tunnel.1
        outer interface:        ethernet1/1
        state:                  active
        session:                2003
        tunnel mtu:             1416
```

```
soft lifetime:          3505
hard lifetime:          3600
lifetime remain:        1321 sec
lifesize remain:        N/A
latest rekey:           2279 seconds ago
monitor:                off
  monitor packets seen: 0
  monitor packets reply:0
en/decap context:       2
local spi:              C322893F
remote spi:             C38F7B99
key type:               auto key
protocol:               ESP/UDP[4500->4500]
auth algorithm:         SHA256
enc  algorithm:         AES128
proxy-id:
  local ip:             10.10.101.0/24
  remote ip:            10.14.100.0/24
  protocol:             0
  local port:           0
  remote port:          0
anti replay check:      yes
copy tos:               no
authentication errors:  0
decryption errors:      0
inner packet warnings:  0
replay packets:         0
packets received
  when lifetime expired:0
  when lifesize expired:0
sending sequence:       652
receive sequence:       652
encap packets:          652
decap packets:          652
encap bytes:            83456
decap bytes:            83456
key acquire requests:   0
owner state:            0
owner cpuid:            s1dp0
ownership:              1
```

Site-A IPsec status all

root@ipsec-test1-site-a-ubuntu1:~# ipsec statusall

Status of IKE charon daemon (strongSwan 5.6.2, Linux 4.15.0-64-generic, x86_64):

uptime: 97 minutes, since Sep 21 19:13:37 2019

malloc: sbrk 2568192, mmap 0, used 916480, free 1651712

worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 20

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:

172.16.25.254

10.14.100.254

Connections:

Site-A-To-PaloAlto1: 172.16.25.254...95.177.219.205 IKEv1 Aggressive

Site-A-To-PaloAlto1:   local: [95.177.168.28] uses pre-shared key authentication

Site-A-To-PaloAlto1:   remote: [95.177.219.205] uses pre-shared key authentication

Site-A-To-PaloAlto1:   child: 10.14.100.0/24 === 10.10.100.254/32 TUNNEL

Site-A-To-PaloAlto[6]: ESTABLISHED 37 minutes ago, 172.16.25.254[95.177.168.28]...95.177.166.177[95.177.166.177]

Site-A-To-PaloAlto[6]: IKEv1 SPIs: d67471cef8fb481a_i* 049471ff2498725a_r, pre-shared key reauthentication in 7 hours

Site-A-To-PaloAlto[6]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048

Site-A-To-PaloAlto{8}: INSTALLED, TUNNEL, reqid 5, ESP in UDP SPIs: c2283ccb_i ce31a8c8_o

Site-A-To-PaloAlto{8}: AES_CBC_128/HMAC_SHA2_256_128, 168 bytes_i (2 pkts, 2223s ago), 168 bytes_o (2 pkts, 2223s ago), rekeying in 10 minutes

Site-A-To-PaloAlto{8}:   10.14.100.0/24 === 10.10.101.0/24

Site-B IPsec status all

N/A

Packet Captures and Traces

Test Connectivity from a client in Site-A to another client in Site-B resides behind Palo Alto FW

1- Ping traceroute & show ip route test:

```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 02:04:c1:0c:47:ee brd ff:ff:ff:ff:ff:ff
    inet 10.14.100.100/24 brd 10.14.100.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::4:c1ff:fe0c:47ee/64 scope link
       valid_lft forever preferred_lft forever
$ traceroute 10.10.101.100
traceroute to 10.10.101.100 (10.10.101.100), 30 hops max, 46 byte packets
 1  10.14.100.254 (10.14.100.254)  1.149 ms  0.988 ms  0.872 ms
 2  *  *  *
 3  10.10.101.100 (10.10.101.100)  3.913 ms  63.488 ms  7.560 ms
$ ip r
default via 10.14.100.254 dev eth0
10.14.100.0/24 dev eth0  src 10.14.100.100
$ ping 10.10.101.100
PING 10.10.101.100 (10.10.101.100): 56 data bytes
64 bytes from 10.10.101.100: seq=0 ttl=62 time=7.946 ms
^C
--- 10.10.101.100 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.946/7.946/7.946 ms
$
```

2- Palo Alto Traffic monitor

(addr.src in 10.14.100.100) and (addr.dst in 10.10.101.100)

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	09/21 09:25:05	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	0	ping	allow	Temp-Allow-Any	aged-out	196
	09/21 09:17:07	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33443	insufficient-data	allow	Temp-Allow-Any	aged-out	148
	09/21 09:17:07	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33442	insufficient-data	allow	Temp-Allow-Any	aged-out	148
	09/21 09:16:37	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33441	insufficient-data	allow	Temp-Allow-Any	aged-out	148
	09/21 09:16:12	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33440	traceroute	allow	Temp-Allow-Any	aged-out	60
	09/21 09:16:07	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33439	traceroute	allow	Temp-Allow-Any	aged-out	60
	09/21 09:16:02	end	IPSec-Using-Internet-Interface	PRD-LAB-DMZ-VLAN101	10.14.100.100		10.10.101.100	33438	traceroute	allow	Temp-Allow-Any	aged-out	60

Test Connectivity from a client behind Site-B-Palo Ato to another client in Site-A

1- Ping, Traceroute, show route test

Connected (encrypted) to: QEMU (instance-00014dee)

```
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 02:e7:a3:29:fb:5c brd ff:ff:ff:ff:ff:ff
    inet 10.10.101.100/24 brd 10.10.101.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::e7:a3ff:fe29:fb5c/64 scope link
       valid_lft forever preferred_lft forever
$ traceroute 10.14.100.100
traceroute to 10.14.100.100 (10.14.100.100), 30 hops max, 46 byte packets
 1  *  *  *
 2  10.14.100.254 (10.14.100.254)  2.104 ms  1.789 ms  1.241 ms
 3  10.14.100.100 (10.14.100.100)  2.203 ms  2.595 ms  3.622 ms
$ ip r
default via 10.10.101.250 dev eth0
10.10.101.0/24 dev eth0  src 10.10.101.100
$ ping 10.14.100.100
PING 10.14.100.100 (10.14.100.100): 56 data bytes
64 bytes from 10.14.100.100: seq=0 ttl=62 time=29.760 ms
64 bytes from 10.14.100.100: seq=1 ttl=62 time=2.240 ms
^C
--- 10.14.100.100 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 2.240/16.000/29.760 ms
$
```

2- Palo Alto Traffic monitor

(addr.src in 10.10.101.100) and (addr.dst in 10.14.100.100)

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
09/21 09:00:27	end	PRD-LAB-DMZ-VLAN101	IPSec-Using-Internet-Interface	10.10.101.100		10.14.100.100	0	ping	allow	Temp-Allow-Any	aged-out	784
09/21 09:00:11	end	PRD-LAB-DMZ-VLAN101	IPSec-Using-Internet-Interface	10.10.101.100		10.14.100.100	0	ping	allow	Temp-Allow-Any	aged-out	588
09/21 08:59:56	end	PRD-LAB-DMZ-VLAN101	IPSec-Using-Internet-Interface	10.10.101.100		10.14.100.100	33436	traceroute	allow	Temp-Allow-Any	aged-out	60
09/21 08:59:51	end	PRD-LAB-DMZ-VLAN101	IPSec-Using-Internet-Interface	10.10.101.100		10.14.100.100	33435	traceroute	allow	Temp-Allow-Any	aged-out	60

Site-A Packet captures

```
root@ipsec-test1-site-a-ubuntu1:~# tcpdump -i any -nn icmp or esp or udp port 500
or udp port 4500 and " host 172.16.25.254 or host 95.177.166.177 or host
10.10.101.100"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
20:55:34.610077 IP 95.177.163.23.4500 > 172.16.25.254.4500: isakmp-nat-keep-alive
20:55:36.058763 IP 172.16.25.254.500 > 95.177.192.154.500: isakmp: parent_sa
ikev2_init[I]
20:55:36.073439 IP 95.177.192.154 > 172.16.25.254: ICMP host 95.177.192.154
unreachable - admin prohibited, length 370
20:55:40.018446 IP 172.16.25.254.500 > 95.177.166.177.500: isakmp: phase 1 I agg
20:55:40.032488 IP 95.177.166.177.500 > 172.16.25.254.500: isakmp: phase 1 R agg
20:55:40.039932 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 1 I agg[E]
20:55:40.041004 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I oakley-quick[E]
20:55:40.041910 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R oakley-quick[E]
20:55:40.044776 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I oakley-quick[E]
20:55:40.594010 IP 172.16.25.254.4500 > 95.177.163.23.4500: NONESP-encap: isakmp:
child_sa  inf2[I]
20:55:40.594796 IP 95.177.163.23.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
child_sa  inf2
20:55:40.594824 IP 95.177.163.23.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
child_sa  inf2[R]
20:55:40.595760 IP 172.16.25.254.4500 > 95.177.163.23.4500: NONESP-encap: isakmp:
child_sa  inf2[IR]
20:55:43.704312 IP 172.16.25.254.4500 > 95.177.219.205.4500: isakmp-nat-keep-alive
20:55:49.019974 IP 172.16.25.254.500 > 95.177.192.154.500: isakmp: parent_sa
ikev2_init[I]
20:55:49.034360 IP 95.177.192.154 > 172.16.25.254: ICMP host 95.177.192.154
unreachable - admin prohibited, length 370
20:55:50.040427 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:55:50.041888 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:00.040744 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:56:00.041713 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:03.704584 IP 172.16.25.254.4500 > 95.177.219.205.4500: isakmp-nat-keep-alive
20:56:04.601976 IP 172.16.25.254.4500 > 95.177.163.23.4500: isakmp-nat-keep-alive
20:56:04.610922 IP 95.177.163.23.4500 > 172.16.25.254.4500: isakmp-nat-keep-alive
```

```
20:56:10.041001 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:56:10.041854 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:10.594669 IP 172.16.25.254.4500 > 95.177.163.23.4500: NONESP-encap: isakmp:
child_sa  inf2[I]
20:56:10.595432 IP 95.177.163.23.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
child_sa  inf2
20:56:10.595449 IP 95.177.163.23.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
child_sa  inf2[R]
20:56:10.595774 IP 172.16.25.254.4500 > 95.177.163.23.4500: NONESP-encap: isakmp:
child_sa  inf2[IR]
20:56:12.348035 IP 172.16.25.254.500 > 95.177.192.154.500: isakmp: parent_sa
ikev2_init[I]
20:56:12.362353 IP 95.177.192.154 > 172.16.25.254: ICMP host 95.177.192.154
unreachable - admin prohibited, length 370
20:56:20.041113 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:56:20.041935 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:23.704982 IP 172.16.25.254.4500 > 95.177.219.205.4500: isakmp-nat-keep-alive
20:56:30.041383 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:56:30.042102 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:34.602496 IP 172.16.25.254.4500 > 95.177.163.23.4500: isakmp-nat-keep-alive
20:56:34.611636 IP 95.177.163.23.4500 > 172.16.25.254.4500: isakmp-nat-keep-alive
20:56:40.041632 IP 172.16.25.254.4500 > 95.177.166.177.4500: NONESP-encap: isakmp:
phase 2/others I inf[E]
20:56:40.042333 IP 95.177.166.177.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
phase 2/others R inf[E]
20:56:40.594674 IP 172.16.25.254.4500 > 95.177.163.23.4500: NONESP-encap: isakmp:
child_sa  inf2[I]
20:56:40.595499 IP 95.177.163.23.4500 > 172.16.25.254.4500: NONESP-encap: isakmp:
child_sa  inf2[R]
20:56:43.705293 IP 172.16.25.254.4500 > 95.177.219.205.4500: isakmp-nat-keep-alive
20:56:47.416761 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x1), length 136
20:56:47.416761 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
0, length 64
20:56:47.416901 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
0, length 64
20:56:47.419053 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
0, length 64
20:56:47.419095 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x1), length 136
20:56:48.416673 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x2), length 136
```

```
20:56:48.416673 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
1, length 64
20:56:48.416782 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
1, length 64
20:56:48.417202 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
1, length 64
20:56:48.417234 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x2), length 136
20:56:49.418965 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x3), length 136
20:56:49.418965 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
2, length 64
20:56:49.419043 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
2, length 64
20:56:49.419516 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
2, length 64
20:56:49.419547 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x3), length 136
20:56:50.416689 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x4), length 136
20:56:50.416689 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
3, length 64
20:56:50.416863 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
3, length 64
20:56:50.417189 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
3, length 64
20:56:50.417254 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x4), length 136
20:56:51.416677 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x5), length 136
20:56:51.416677 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
4, length 64
20:56:51.416804 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
4, length 64
20:56:51.417159 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
4, length 64
20:56:51.417191 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x5), length 136
20:56:52.417021 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x6), length 136
20:56:52.417021 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
5, length 64
20:56:52.417140 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
5, length 64
20:56:52.417476 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
5, length 64
20:56:52.417513 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x6), length 136
```

```
20:56:53.417133 IP 95.177.166.177.4500 > 172.16.25.254.4500: UDP-encap:
ESP(spi=0xccdfbcce,seq=0x7), length 136
20:56:53.417133 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
6, length 64
20:56:53.417261 IP 10.10.101.100 > 10.14.100.100: ICMP echo request, id 47105, seq
6, length 64
20:56:53.417575 IP 10.14.100.100 > 10.10.101.100: ICMP echo reply, id 47105, seq
6, length 64
20:56:53.417617 IP 172.16.25.254.4500 > 95.177.166.177.4500: UDP-encap:
ESP(spi=0xebd2c54f,seq=0x7), length 136
```