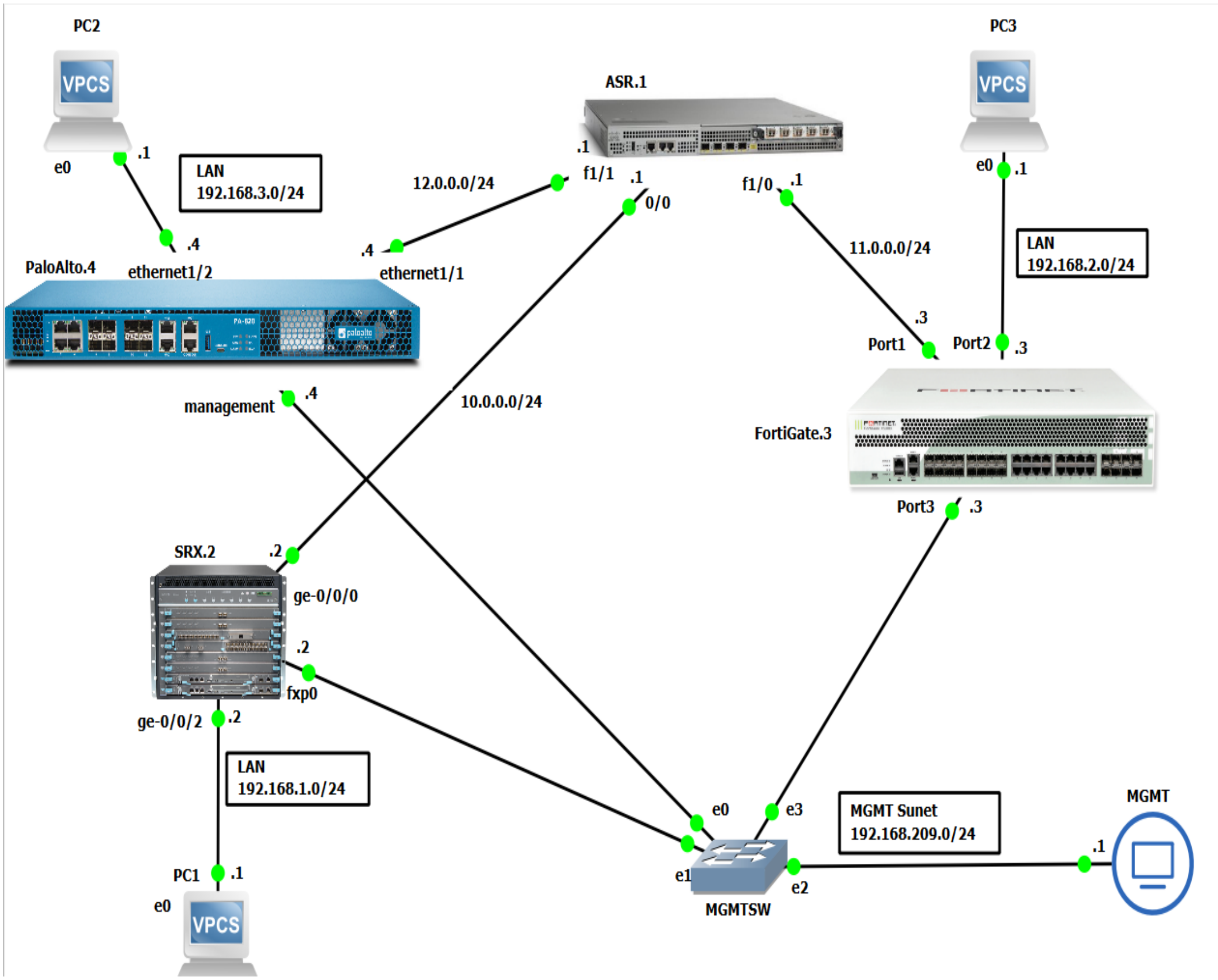
DEPI_1_ONL1_ISS8_G1e Fortinet

➢ Site-to-Site VPN between (FortiGate - Paloalto) and (FortiGate - Juniper SRX) LAB on GNS3

Student Name: Ahmed Essam Ewis
Student Number:21025550
Group: DEPI_1_ONL1_ISS8_G1e Fortinet Cybersecurity Engineer
Email: ahmed3osam7878@gmail.com

❖ Topology



DEPI_1_ONL1_ISS8_G1e Fortinet

Created by Eng/Ahmed Essam

Founder of **JTA Technology**

Contact Information:

- **YouTube Link:**

https://youtube.com/@jtatechnology?si=pH4zD-4IrmcQj2r-

- **FB Page:**

https://www.facebook.com/profile.php?id=100095716232637&mibextid=ZbWKwL

- **What's app Group:**

https://chat.whatsapp.com/CHSjiOEjv72FuCtW1wlRjO

- **Telegram Group:**

https://t.me/+pzMQo7BjQZE5MjM0

- **LinkedIn Profile:**

https://www.linkedin.com/in/ahmed-essam-8000b6207

Site-to-Site VPN between (FortiGate-Paloalto) & (FortiGate-Juniper SRX) LAB

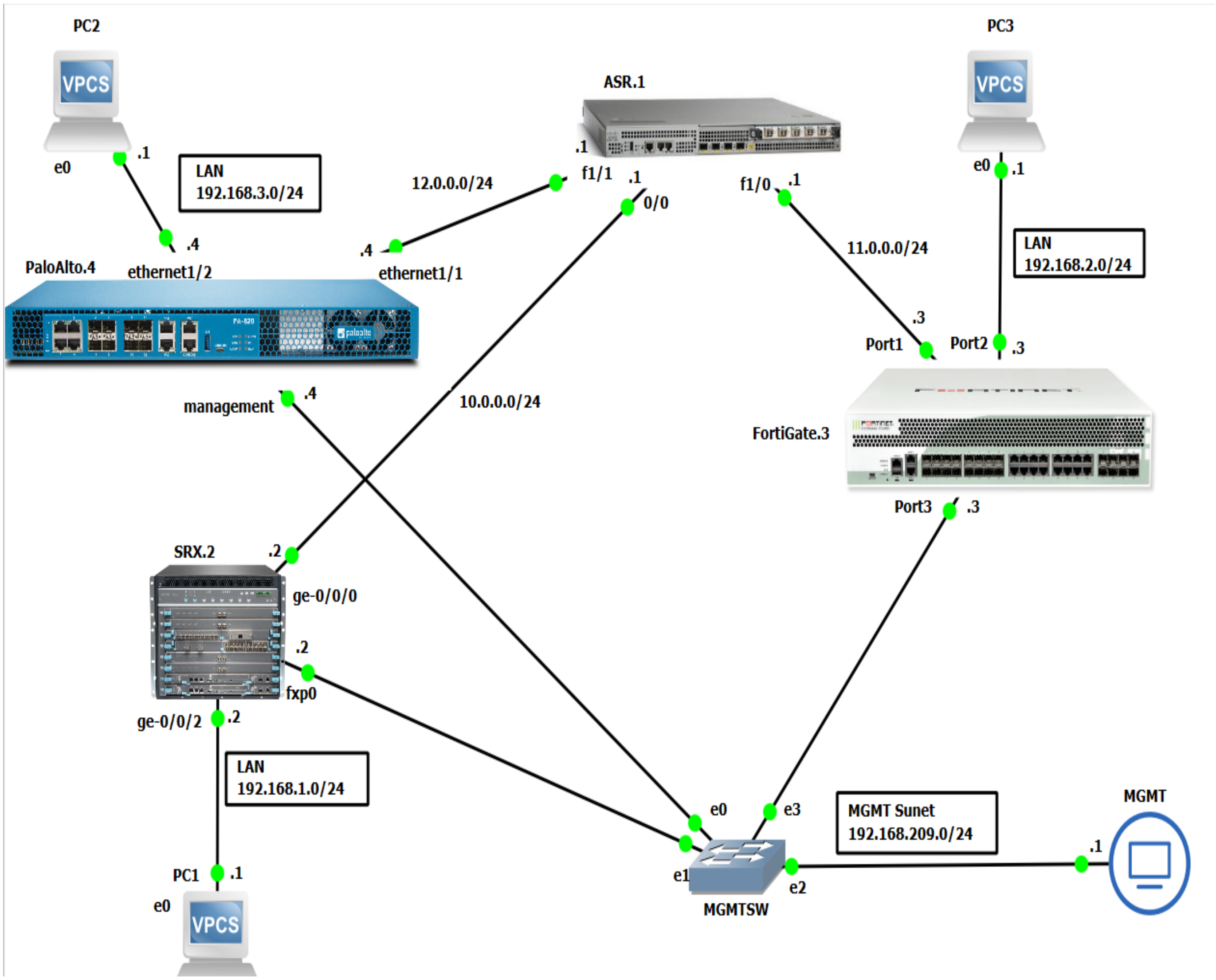
Objectives

This practical lab guide aims to provide hands-on experience in creating and verifying VPN tunnels between different firewall vendors using GNS3. Specifically, this document covers:

- **Site-to-Site VPN Configuration*:***
  - Establishing a VPN tunnel between Fortigate and Juniper SRX.
  - Configuring a VPN tunnel between Fortigate and Palo Alto Networks.
- **Cross-Vendor Configuration:**
  - Detailed steps for configuring VPN on Fortigate, Juniper SRX, and Palo Alto firewalls.
  - Verification procedures to ensure successful tunnel establishment on each device.
- **Policy and Route Management:**
  - Creation of necessary security policies and static routes for each firewall.
  - Configuration of objects and assignment of IP addresses to interfaces.
- **ISP Configuration:**
  - Setting up an ASR router as an ISP to facilitate connectivity between Fortigate, SRX, and Palo Alto firewalls.
  - Assigning appropriate IP addresses to the ASR router interfaces.

➢ **This guide will equip network professionals with the skills to implement and troubleshoot multi-vendor VPN setups, enhancing their understanding of interoperability in secure network environments.**

Topology


PC2
VPCS
e0
.1
LAN
192.168.3.0/24
.4
PaloAlto.4
ethernet1/2
12.0.0.0/24
.4
ethernet1/1
ASR.1
.1
f1/1
.1
0/0
f1/0
.1
11.0.0.0/24
PC3
VPCS
e0
.1
LAN
192.168.2.0/24
.3
Port1
Port2
.3
management
.4
10.0.0.0/24
FortiGate.3
Port3
.3
SRX.2
.2
ge-0/0/0
.2
fxp0
ge-0/0/2
.2
LAN
192.168.1.0/24
PC1
.1
e0
VPCS
e0
e3
MGMT Sunet
192.168.209.0/24
MGMT
.1
e1
e2
MGMTSW

Configuration

1. ASR Configuration

✓ interfaces Configuration

```
ASR#configure t

ASR(config)# interface FastEthernet0/0

ASR(config-if)#no shutdown

ASR(config-if)# ip address 10.0.0.1 255.255.255.0

ASR(config-if)#interface FastEthernet1/0

ASR(config-if)#ip address 11.0.0.1 255.255.255.0

ASR(config-if)#no shutdown

ASR(config-if)#interface FastEthernet1/1

ASR(config-if)#ip address 12.0.0.1 255.255.255.0

ASR(config-if)#no shutdown

ASR(config-if)#end

ASR#wr

Warning: Attempting to overwrite an NVRAM configuration previously written

by a different version of the system image.

Overwrite the previous NVRAM configuration?[confirm]

Building configuration...

[OK]
```

2. FortiGate Configuration

✓ Set Management Interface

```
FortiFirewall-VM64-KVM # config system interface

edit "port3"

    set vdom "root"

    set ip 192.168.209.3 255.255.255.0

    set allowaccess ping https ssh http telnet

    set type physical

    set alias "MGMT-Port"

  next
```

✓ interfaces Configuration

```
edit "port1"

    set vdom "root"

    set ip 11.0.0.3 255.255.255.0

    set allowaccess ping https ssh fgfm

    set type physical

    set alias "WAN-port"

  next

  edit "port2"

    set vdom "root"

    set ip 192.168.2.3 255.255.255.0

    set allowaccess ping

    set type physical

    set alias "LAN-port"

  next
```

✓ Create Tunnel Interfaces

```
edit "FG_TO_SRX"
        set vdom "root"
        set type tunnel
        set snmp-index 13
        set interface "port1"
    next
    edit "FG_TO_PA"
        set vdom "root"
        set type tunnel
        set snmp-index 14
        set interface "port1"
    next
end
```

✓ Address Objects Configuration

```
FortiFirewall-VM64-KVM # config firewall address
  edit "FG_TO_SRX_remote_subnet_1"
    set allow-routing enable
    set subnet 192.168.1.0 255.255.255.0
  next
  edit "local_subnet"
    set allow-routing enable
    set subnet 192.168.2.0 255.255.255.0
  next
  edit "FG_TO_PA_remote_subnet_1"
    set allow-routing enable
    set subnet 192.168.3.0 255.255.255.0
  next
end
```

✓ VPN Configuration

❖ IPSEC Phase1 Configuration

```
FortiFirewall-VM64-KVM # config vpn ipsec phase1-interface
  edit "FG_TO_SRX"
    set interface "port1"
    set peertype any
    set net-device disable
    set proposal des-md5
    set dhgrp 2
    set remote-gw 10.0.0.2
    set psksecret 123456
  next
  edit "FG_TO_PA"
    set interface "port1"
    set peertype any
    set net-device disable
    set proposal des-md5
    set dhgrp 2
    set remote-gw 12.0.0.4
    set psksecret Admin@123
end
```

❖ IPSEC Phase2 Configuration

```
FortiFirewall-VM64-KVM # config vpn ipsec phase2-interface
    edit "FG_TO_SRX"
        set phase1name "FG_TO_SRX"
        set proposal des-md5
        set dhgrp 2
        set src-addr-type name
        set dst-addr-type name
        set src-name "local_subnet"
        set dst-name "FG_TO_SRX_remote"
    next
    edit "FG_TO_PA"
        set phase1name "FG_TO_PA"
        set proposal des-md5
        set dhgrp 2
        set src-addr-type name
        set dst-addr-type name
        set src-name "local_subnet"
        set dst-name "FG_TO_PA_remote"
    next
end
```

✓ Static Route Configuration

```
FortiFirewall-VM64-KVM # config router static
  edit 1
    set gateway 11.0.0.1
    set device "port1"
  next
  edit 2
    set device "FG_TO_SRX"
    set dstaddr "FG_TO_SRX_remote"
  next
  edit 3
    set distance 254
    set blackhole enable
    set dstaddr "FG_TO_SRX_remote"
  next
  edit 4
    set device "FG_TO_PA"
    set dstaddr "FG_TO_PA_remote"
  next
  edit 5
    set distance 254
```

```
        set blackhole enable
        set dstaddr "FG_TO_PA_remote"
    next
end
```

✓ Security Policy Configuration

```
FortiFirewall-VM64-KVM # config firewall policy
    edit 1
        set name "vpn_FG_TO_SRX_local_0"
        set srcintf "port2"
        set dstintf "FG_TO_SRX"
        set srcaddr "local_subnet"
        set dstaddr "FG_TO_SRX_remote"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "vpn_FG_TO_SRX_remote_0"
        set srcintf "FG_TO_SRX"
        set dstintf "port2"
        set srcaddr "local_subnet"
        set dstaddr "FG_TO_SRX_local"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "vpn_FG_TO_PA_local_0"
        set srcintf "port2"
        set dstintf "FG_TO_PA"
        set srcaddr "local_subnet"
        set dstaddr "FG_TO_PA_remote"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 4
        set name "vpn_FG_TO_PA_remote_0"
        set srcintf "FG_TO_PA"
        set dstintf "port2"
        set srcaddr "FG_TO_PA_remote"
        set dstaddr "local_subnet"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

3. Paloalto Configuration

✓ Set cli config-output

```
admin@PA-VM> set cli config-output-format set
```

✓ Enter Configuration Mode

```
admin@PA-VM> configure

Entering configuration mode

[edit]
```

✓ Set Management Interface

```
admin@PA-VM# set deviceconfig system type static

admin@PA-VM# set deviceconfig system ip-address 192.168.209.4

admin@PA-VM# set deviceconfig system netmask 255.255.255.0

admin@PA-VM# set deviceconfig system default-gateway 192.168.209.1
```

✓ Interface Configuration

```
admin@PA-VM# set network interface ethernet ethernet1/1 layer3 ip 12.0.0.4/24

admin@PA-VM# set network interface ethernet ethernet1/1 layer3 interface-management-profile Ping

admin@PA-VM# set network interface ethernet ethernet1/2 layer3 ip 192.168.3.4/24

admin@PA-VM# set network interface ethernet ethernet1/2 layer3 interface-management-profile Ping
```

✓ Create Tunnel Interface

```
admin@PA-VM# set network interface tunnel units tunnel.1
```

✓ Zones Configuration

```
admin@PA-VM# set zone WAN network layer3 ethernet1/1

admin@PA-VM# set zone LAN network layer3 ethernet1/2

admin@PA-VM# set zone VPN network layer3 tunnel.1
```

✓ Create interface-management-profile (Ping)

```
admin@PA-VM# set network profiles interface-management-profile Ping ping yes

admin@PA-VM# set network profiles monitor-profile default interval 3

admin@PA-VM# set network profiles monitor-profile default threshold 5

admin@PA-VM# set network profiles monitor-profile default action wait-recover
```

✓ VPN Configuration

❖ IKE crypto-profiles Configuration

Phase 1

```
admin@PA-VM# set network ike crypto-profiles ike-crypto-profiles PA_to_FG hash md5

admin@PA-VM# set network ike crypto-profiles ike-crypto-profiles PA_to_FG dh-group group2

admin@PA-VM# set network ike crypto-profiles ike-crypto-profiles PA_to_FG encryption des

admin@PA-VM# set network ike crypto-profiles ike-crypto-profiles PA_to_FG lifetime hours 24
```

Phase 2

```
admin@PA-VM# set network ike crypto-profiles ipsec-crypto-profiles PA_to_FG_IPSEC esp authentication md5

admin@PA-VM# set network ike crypto-profiles ipsec-crypto-profiles PA_to_FG_IPSEC esp encryption des

admin@PA-VM# set network ike crypto-profiles ipsec-crypto-profiles PA_to_FG_IPSEC lifetime hours 24

admin@PA-VM# set network ike crypto-profiles ipsec-crypto-profiles PA_to_FG_IPSEC dh-group group2
```

❖ IKE Gateway Configuration

```
admin@PA-VM# set network ike gateway PA_to_FG_GW authentication pre-shared-key Key Admin@123

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol ikev1 dpd enable yes

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol ikev1 ike-crypto-profile PA_to_FG

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol ikev1 exchange-mode main

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol ikev2 dpd enable yes

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol version ikev1

admin@PA-VM# set network ike gateway PA_to_FG_GW local-address ip 12.0.0.4/24

admin@PA-VM# set network ike gateway PA_to_FG_GW local-address interface ethernet1/1

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol-common nat-traversal enable no

admin@PA-VM# set network ike gateway PA_to_FG_GW protocol-common fragmentation enable no

admin@PA-VM# set network ike gateway PA_to_FG_GW peer-address ip 11.0.0.3
```

❖ Tunnel IPSEC Configuration

```
admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel auto-key ike-gateway PA_to_FG_GW

admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel auto-key proxy-id Fortigate protocol any

admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel auto-key proxy-id Fortigate local 192.168.3.0/24

admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel auto-key proxy-id Fortigate remote 192.168.2.0/24

admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel auto-key ipsec-crypto-profile PA_to_FG_IPSEC

admin@PA-VM# set network tunnel ipsec PA_to_FG_tunnel tunnel-interface tunnel.1

admin@PA-VM# set network virtual-router default interface [ ethernet1/1 ethernet1/2 tunnel.1 ]
```

✓ Static Route Configuration

```
admin@PA-VM# set network virtual-router default routing-table ip static-route "Route to ASR" nexthop ip-address 12.0.0.1

admin@PA-VM# set network virtual-router default routing-table ip static-route "Route to ASR" interface ethernet1/1

admin@PA-VM# set network virtual-router default routing-table ip static-route "Route to ASR" metric 10

admin@PA-VM# set network virtual-router default routing-table ip static-route "Route to ASR" destination 0.0.0.0/0

admin@PA-VM# set network virtual-router default routing-table ip static-route VPN_Route interface tunnel.1

admin@PA-VM# set network virtual-router default routing-table ip static-route VPN_Route metric 10

admin@PA-VM# set network virtual-router default routing-table ip static-route VPN_Route destination 192.168.2.0/24
```

✓ Security Policy Configuration

```
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" to [ LAN VPN ]
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" from [ LAN VPN ]
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" source any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" destination any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" source-user any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" category any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" application any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" service application-default
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" source-hip any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" destination-hip any
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" action allow
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" log-start yes
admin@PA-VM# set rulebase security rules "allow Remote_to_Local" log-end yes
admin@PA-VM# set import network interface [ ethernet1/1 ethernet1/2 tunnel.1 ]
```

✓ Commit

```
admin@PA-VM# Commit
[edit]
admin@PA-VM#
```

4. Juniper SRX Configuration

✓ Enter Configuration Mode

```
root@:~ # cli

root> configure

Entering configuration mode

[edit]
```

✓ Set Root Password

```
root# set system root-authentication plain-text-password

New password:root123

Retype new password:root123
```

✓ Set Management Interface

```
root# set system services ssh

root# set system services web-management http interface fxp0.0

root# set interfaces fxp0 unit 0 family inet address 192.168.209.2/24
```

✓ Interface Configuration

```
root# set interfaces ge-0/0/0 unit 0 description "WAN Interface"

root# set interfaces ge-0/0/0 unit 0 family inet address 10.0.0.2/24

root# set interfaces ge-0/0/2 unit 0 family inet address 192.168.1.2/24
```

✓ Create Tunnel Interface

```
root# set interfaces st0 unit 20 family inet
```

✓ Zone Configuration

```
root# set security zones security-zone trust interfaces ge-0/0/2.0

root# set security zones security-zone trust interfaces st0.20

root# set security zones security-zone untrust interfaces ge-0/0/0.0

root# set security zones security-zone trust host-inbound-traffic system-services ping

root# set security zones security-zone untrust host-inbound-traffic system-services ping
```

✓ VPN Configuration

❖ IKE Proposal Configuration

```
root# set security ike proposal SRX_to_FG_ph1 authentication-method pre-shared-keys

root# set security ike proposal SRX_to_FG_ph1 dh-group group2

root# set security ike proposal SRX_to_FG_ph1 authentication-algorithm md5

root# set security ike proposal SRX_to_FG_ph1 encryption-algorithm des-cbc

root# set security ike proposal SRX_to_FG_ph1 lifetime-seconds 86400
```

❖ IKE Policy Configuration

```
root# set security ike policy SRX_TO_FG_POLICY mode main

root# set security ike policy SRX_TO_FG_POLICY proposals SRX_to_FG_ph1

root# set security ike policy SRX_TO_FG_POLICY pre-shared-key ascii-text 123456
```

❖ IKE Gateway Configuration

```
root# set security ike gateway FG_TO_FG_GW ike-policy SRX_TO_FG_POLICY

root# set security ike gateway FG_TO_FG_GW address 11.0.0.3

root# set security ike gateway FG_TO_FG_GW external-interface ge-0/0/0.0
```

❖ IPSEC Proposal Configuration

```
root# set security ipsec proposal SRX_TO_FG_ph2 protocol esp

root# set security ipsec proposal SRX_TO_FG_ph2 authentication-algorithm hmac-md5-96

root# set security ipsec proposal SRX_TO_FG_ph2 encryption-algorithm des-cbc

root# set security ipsec proposal SRX_TO_FG_ph2 lifetime-seconds 43200

root# set security ipsec policy SRX_TO_FG_POLICY perfect-forward-secrecy keys group2

root# set security ipsec policy SRX_TO_FG_POLICY proposals SRX_TO_FG_ph2
```

❖ IPSEC VPN Tunnel Configuration

```
root# set security ipsec vpn SRX_T0_FG_TUNNRL bind-interface st0.20

root# set security ipsec vpn SRX_T0_FG_TUNNRL ike gateway FG_TO_FG_GW

root# set security ipsec vpn SRX_T0_FG_TUNNRL ike ipsec-policy SRX_TO_FG_POLICY

root# set security ipsec vpn SRX_T0_FG_TUNNRL traffic-selector VPN_Subnet_SRX_FG local-ip 192.168.1.0/24

root# set security ipsec vpn SRX_T0_FG_TUNNRL traffic-selector VPN_Subnet_SRX_FG remote-ip 192.168.2.0/24

root# set security ipsec vpn SRX_T0_FG_TUNNRL establish-tunnels immediately
```

✓ Static Route Configuration

```
root# set routing-options static route 192.168.2.0/24 next-hop st0.20

root# set routing-options static route 0.0.0.0/0 next-hop 10.0.0.1
```

✓ Security Policy Configuration

```
root# set security policies from-zone untrust to-zone trust policy default-permit_31 match source-address any

root# set security policies from-zone untrust to-zone trust policy default-permit_31 match destination-address any

root# set security policies from-zone untrust to-zone trust policy default-permit_31 match application any

root# set security policies from-zone untrust to-zone trust policy default-permit_31 then permit
```

✓ Show Candidate Configuration

```
root# show | compare

[edit system]

+  root-authentication {

+      encrypted-password "$6$SFyJ159T$.x21aV0o4bxkpznUa7nvWo.dxqiXT0j6TV.B41JF9Sy.pJE0OkzngsEVDPWQaDdY7MYGaG574hZJURNHB6Ij8/"; ## SECRET-DATA

+  }
```

```
-  autoinstallation {
-      delete-upon-commit;
-      traceoptions {
-          level verbose;
-          flag {
-              all;
-          }
-      }
-  }
[edit security]
+  ike {
+      proposal SRX_to_FG_ph1 {
+          authentication-method pre-shared-keys;
+          dh-group group2;
+          authentication-algorithm md5;
+          encryption-algorithm des-cbc;
+          lifetime-seconds 86400;
+      }
+      policy SRX_TO_FG_POLICY {
+          mode main;
+          proposals SRX_to_FG_ph1;
+          pre-shared-key ascii-text "$9$S3vrM8xNdsgo7Nqm5Qn6"; ## SECRET-DATA
+      }
+      gateway FG_TO_FG_GW {
+          ike-policy SRX_TO_FG_POLICY;
+          address 11.0.0.3;
+         external-interface ge-0/0/0.0;
+     }
+ }
+ ipsec {
+     proposal SRX_TO_FG_ph2 {
+         protocol esp;
+         authentication-algorithm hmac-md5-96;
+         encryption-algorithm des-cbc;
+         lifetime-seconds 43200;
+     }
+     policy SRX_TO_FG_POLICY {
+         perfect-forward-secrecy {
+             keys group2;
+         }
+         proposals SRX_TO_FG_ph2;
+     }
+     vpn SRX_T0_FG_TUNNRL {
+         bind-interface st0.20;
+         ike {
+             gateway FG_TO_FG_GW;
+             ipsec-policy SRX_TO_FG_POLICY;
+         }
+         traffic-selector VPN_Subnet_SRX_FG {
+             local-ip 192.168.1.0/24;
+             remote-ip 192.168.2.0/24;
+         }
+       establish-tunnels immediately;
+     }
+   }
[edit security policies]
    from-zone trust to-zone untrust { ... }
+   from-zone untrust to-zone trust {
+     policy default-permit_31 {
+       match {
+         source-address any;
+         destination-address any;
+         application any;
+       }
+       then {
+         permit;
+       }
+     }
+   }
[edit security zones security-zone trust]
+   interfaces {
+     ge-0/0/2.0;
+     st0.20;
+   }
+   host-inbound-traffic {
+     system-services {
+       ping;
+     }
+    }
[edit security zones security-zone untrust]
+   interfaces {
+       ge-0/0/0.0;
+   }
[edit interfaces]
+  ge-0/0/0 {
+      unit 0 {
+          description "WAN Interface";
+          family inet {
+              address 10.0.0.2/24;
+          }
+      }
+  }
+  ge-0/0/2 {
+      unit 0 {
+          family inet {
+              address 192.168.1.2/24;
+          }
+      }
+  }
[edit interfaces fxp0 unit 0]
+    family inet {
+        address 192.168.209.2/24;
+    }
[edit interfaces]
```

```
+  st0 {
+      unit 20 {
+          family inet;
+      }
+  }
[edit]
+ routing-options {
+     static {
+         route 0.0.0.0/0 next-hop 10.0.0.1;
+         route 192.168.2.0/24 next-hop st0.20;
+     }
+ }
[edit]
root#
```

✓ Commit Check

```
root# commit check
configuration check succeeds
[edit]
```

✓ Commit

```
root# commit
commit complete
[edit]
root#
```

Verification

1) ASR Verification

```
ASR# show ip int b

Interface          IP-Address      OK? Method Status           Protocol

FastEthernet0/0        10.0.0.1       YES manual up               up

FastEthernet1/0        11.0.0.1       YES manual up               up

FastEthernet1/1        12.0.0.1       YES manual up               up
```

```
ASR# show ip route | begin Gate

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C       10.0.0.0/24 is directly connected, FastEthernet0/0

L       10.0.0.1/32 is directly connected, FastEthernet0/0

     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C       11.0.0.0/24 is directly connected, FastEthernet1/0

L       11.0.0.1/32 is directly connected, FastEthernet1/0

     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C       12.0.0.0/24 is directly connected, FastEthernet1/1

L       12.0.0.1/32 is directly connected, FastEthernet1/1
```

2) FortiGate-SRX-VPN Tunnel Verifications

✓ Check Conductivity for Two GW peers

❖ From Juniper SRX

```
root> ping 11.0.0.3

PING 11.0.0.3 (11.0.0.3): 56 data bytes

64 bytes from 11.0.0.3: icmp_seq=0 ttl=254 time=63.987 ms

64 bytes from 11.0.0.3: icmp_seq=1 ttl=254 time=39.331 ms

64 bytes from 11.0.0.3: icmp_seq=2 ttl=254 time=34.178 ms

64 bytes from 11.0.0.3: icmp_seq=3 ttl=254 time=43.236 ms

64 bytes from 11.0.0.3: icmp_seq=4 ttl=254 time=42.592 ms

64 bytes from 11.0.0.3: icmp_seq=5 ttl=254 time=35.988 ms
```

❖ From FortiGate

```
FortiFirewall-VM64-KVM # execute ping 10.0.0.2

PING 10.0.0.2 (10.0.0.2): 56 data bytes

64 bytes from 10.0.0.2: icmp_seq=0 ttl=63 time=24.8 ms

64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=21.5 ms

64 bytes from 10.0.0.2: icmp_seq=2 ttl=63 time=19.5 ms

64 bytes from 10.0.0.2: icmp_seq=3 ttl=63 time=18.3 ms

64 bytes from 10.0.0.2: icmp_seq=4 ttl=63 time=31.3 ms
```

✓ Check that the tunnels are up from two peers

❖ From Juniper SRX

```
root> show security ike security-associations

Index   State  Initiator cookie  Responder cookie  Mode        Remote Address

3529508 UP     75ce242585314860  2b495c8e121bd27d  Main        11.0.0.3
```

```
root> show security ipsec security-associations

  Total active tunnels: 1     Total Ipsec sas: 1

  ID    Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway

  <67108865 ESP:des/md5   c8e6a547 42592/ unlim -   root 500   11.0.0.3

  >67108865 ESP:des/md5   76c5f6cf 42592/ unlim -   root 500   11.0.0.3
```

```
root> show security ipsec statistics

ESP Statistics:

  Encrypted bytes:           4624

  Decrypted bytes:           2604

  Encrypted packets:           34

  Decrypted packets:           31
```

```
AH Statistics:

  Input bytes:                0

  Output bytes:                0

  Input packets:               0

  Output packets:               0

Errors:

  AH authentication failures: 0, Replay errors: 0

  ESP authentication failures: 0, ESP decryption failures: 0

  Bad headers: 0, Bad trailers: 0
```

- **From FortiGate FW**

```
FortiFirewall-VM64-KVM # get vpn ipsec tunnel summary

'FG_TO_SRX' 10.0.0.2:0  selectors(total,up): 1/1  rx(pkt,err): 34/0  tx(pkt,err): 31/2
```

```
FortiFirewall-VM64-KVM # diagnose vpn ike gateway list name FG_TO_SRX

vd: root/0

name: FG_TO_SRX

version: 1

interface: port1 3

addr: 11.0.0.3:500 -> 10.0.0.2:500

created: 937s ago

IKE SA: created 1/4  established 1/1  time 580/580/580 ms

IPsec SA: created 1/2  established 1/1  time 560/560/560 ms

  id/spi: 53 75ce242585314860/2b495c8e121bd27d

  direction: responder

  status: established 887-886s ago = 580ms

  proposal: des-md5

  key: 24bcf591eec92d3a

  lifetime/rekey: 86400/85243

  DPD sent/recv: 00000000/00000000
```

✓ Check Conductivity from PC2 to PC3 & Vice versa

❖ Ping from PC1 to PC3

```
PC1> show

NAME   IP/MASK            GATEWAY         MAC               LPORT  RHOST:PORT

PC1    192.168.1.1/24     192.168.1.2     00:50:79:66:68:00  10017  127.0.0.1:10018
```

```
PC1> ping 192.168.2.1 -t

84 bytes from 192.168.2.1 icmp_seq=1 ttl=62 time=36.871 ms

84 bytes from 192.168.2.1 icmp_seq=2 ttl=62 time=33.571 ms

84 bytes from 192.168.2.1 icmp_seq=3 ttl=62 time=31.785 ms

84 bytes from 192.168.2.1 icmp_seq=4 ttl=62 time=32.077 ms

84 bytes from 192.168.2.1 icmp_seq=5 ttl=62 time=32.367 ms
```

❖ Ping from PC3 to PC1

```
PC3> show

NAME   IP/MASK            GATEWAY         MAC               LPORT  RHOST:PORT

PC3    192.168.2.1/24     192.168.2.3     00:50:79:66:68:02  10019  127.0.0.1:10020
```

```
PC3> ping 192.168.1.1 -t

84 bytes from 192.168.1.1 icmp_seq=1 ttl=62 time=36.225 ms

84 bytes from 192.168.1.1 icmp_seq=2 ttl=62 time=49.372 ms

84 bytes from 192.168.1.1 icmp_seq=3 ttl=62 time=32.679 ms

84 bytes from 192.168.1.1 icmp_seq=4 ttl=62 time=36.183 ms

84 bytes from 192.168.1.1 icmp_seq=5 ttl=62 time=32.775 ms
```

3) FortiGate-Paloalto-VPN Tunnel Verifications

✓ Check Conductivity for Two GW peers

❖ From Paloalto

```
admin@PA-VM> ping source 12.0.0.4 host 11.0.0.3

PING 11.0.0.3 (11.0.0.3) from 12.0.0.4 : 56(84) bytes of data.

64 bytes from 11.0.0.3: icmp_seq=1 ttl=254 time=28.4 ms

64 bytes from 11.0.0.3: icmp_seq=2 ttl=254 time=25.7 ms

64 bytes from 11.0.0.3: icmp_seq=3 ttl=254 time=39.9 ms

64 bytes from 11.0.0.3: icmp_seq=4 ttl=254 time=21.8 ms

64 bytes from 11.0.0.3: icmp_seq=5 ttl=254 time=25.3 ms

64 bytes from 11.0.0.3: icmp_seq=6 ttl=254 time=18.4 ms

64 bytes from 11.0.0.3: icmp_seq=7 ttl=254 time=31.4 ms

64 bytes from 11.0.0.3: icmp_seq=8 ttl=254 time=30.6 ms

64 bytes from 11.0.0.3: icmp_seq=9 ttl=254 time=30.3 ms

64 bytes from 11.0.0.3: icmp_seq=10 ttl=254 time=29.9 ms
```

❖ From FortiGate

```
FortiFirewall-VM64-KVM # execute ping 12.0.0.4

PING 12.0.0.4 (12.0.0.4): 56 data bytes

64 bytes from 12.0.0.4: icmp_seq=0 ttl=63 time=27.9 ms

64 bytes from 12.0.0.4: icmp_seq=1 ttl=63 time=27.7 ms

64 bytes from 12.0.0.4: icmp_seq=2 ttl=63 time=27.5 ms

64 bytes from 12.0.0.4: icmp_seq=3 ttl=63 time=27.0 ms
```

✓ Check that the tunnels are up from two peers

❖ From Paloalto

```
admin@PA-VM> test vpn ike-sa

Start time: Sep.30 20:48:42

Initiate 1 IKE SA.
```

```
admin@PA-VM> test vpn ipsec-sa

Start time: Sep.30 20:48:54

Initiate 1 IPSec SA.
```

```
admin@PA-VM> show vpn flow

total tunnels configured:                    1

filter - type IPSec, state any

total IPSec tunnel configured:               1

total IPSec tunnel shown:                    1

id   name                    state   monitor local-ip          peer-ip           tunnel-i/f

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

1    PA_to_FG_tunnel:Fortigate   active  off    12.0.0.4      11.0.0.3          tunnel.1
```

```
admin@PA-VM> show vpn gateway

GwID    Name       Peer-Address/ID   Local Address/ID   Protocol   Proposals

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

1       PA_to_FG_GW   11.0.0.3       12.0.0.4           Main       [PSK][DH2][DES][MD5]86400-
sec

Show IKE gateway config: Total 1 gateways found.
```

```
admin@PA-VM> show vpn ike-sa

IKEv1 phase-1 SAs

GwID/client IP  Peer-Address        Gateway Name        Role Mode Algorithm          Established
Expiration      V  ST Xt Phase2

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

1           11.0.0.3          PA_to_FG_GW         Init Main PSK/ DH2/ DES/ MD5    Sep.30
20:48:42 Oct.01 20:48:42 v1 13 1  1

1           11.0.0.3          PA_to_FG_GW         Resp Main PSK/ DH2/ DES/ MD5    Sep.30
20:41:43 Sep.30 20:49:42 v1 13 1  1

 Show IKEv1 IKE SA: Total 1 gateways found. 2 ike sa found.

IKEv1 phase-2 SAs

Gateway Name        TnID     Tunnel              GwID/IP        Role Algorithm         SPI(in)
SPI(out) MsgID     ST Xt

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

PA_to_FG_GW         1      PA_to_FG_tunnel:Fortig 1            Init ESP/ DH2/tunl/ MD5
FF10D45F 41C0FAF4 AC9C3096 9  1

PA_to_FG_GW         1      PA_to_FG_tunnel:Fortig 1            Resp ESP/ DH2/tunl/ MD5
9D60B156 41C0FAF3 B5F6D66A 9  1

Show IKEv1 phase2 SA: Total 1 gateways found. 2 ike sa found.
```

```
admin@PA-VM> show vpn ipsec-sa

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

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

1             1      11.0.0.3          PA_to_FG_tunnel:Fortigate(PA_to_FG_GW)        ESP/DES/MD5
FF10D45F 41C0FAF4 43200/Unlimited        43149

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

```
admin@PA-VM> show vpn tunnel

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

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

1     PA_to_FG_tunnel:Fortigate     PA_to_FG_GW        192.168.3.0/24      0:0
192.168.2.0/24      0:0       ESP tunl [DH2][DES][MD5] 86400-sec 0-kb
```

From FortiGate

```
FortiFirewall-VM64-KVM # get vpn ipsec tunnel summary

'FG_TO_PA' 12.0.0.4:0  selectors(total,up): 1/1  rx(pkt,err): 330/0  tx(pkt,err): 331/2
```

```
FortiFirewall-VM64-KVM # diagnose vpn ike gateway list name FG_TO_PA

vd: root/0

name: FG_TO_PA

version: 1

interface: port1 3

addr: 11.0.0.3:500 -> 12.0.0.4:500

created: 370s ago

IKE SA: created 1/1  established 1/1  time 120/120/120 ms

IPsec SA: created 1/1  established 1/1  time 20/20/20 ms

  id/spi: 6 d4d9ba8ee1a34799/e95566b7fa344053

  direction: initiator

  status: established 370-370s ago = 120ms

  proposal: des-md5

  key: 1b349cc508e1d69c

  lifetime/rekey: 86400/85729

  DPD sent/recv: 00000000/00000000
```

✓ Check Conductivity from PC2 to PC3 & Vice versa

❖ Ping from PC2 to PC3

```
PC2> show

NAME   IP/MASK           GATEWAY         MAC              LPORT  RHOST:PORT

PC2    192.168.3.1/24    192.168.3.4     00:50:79:66:68:01  10010  127.0.0.1:10011
```

```
PC2> ping 192.168.2.1 -t

84 bytes from 192.168.2.1 icmp_seq=1 ttl=62 time=31.891 ms

84 bytes from 192.168.2.1 icmp_seq=2 ttl=62 time=31.792 ms

84 bytes from 192.168.2.1 icmp_seq=3 ttl=62 time=36.910 ms

84 bytes from 192.168.2.1 icmp_seq=4 ttl=62 time=32.584 ms

84 bytes from 192.168.2.1 icmp_seq=5 ttl=62 time=32.556 ms
```

❖ Ping from PC3 to PC2

```
PC3> show

NAME   IP/MASK           GATEWAY         MAC              LPORT  RHOST:PORT

PC3    192.168.2.1/24    192.168.2.3     00:50:79:66:68:02  10012  127.0.0.1:10013
```

```
PC3> ping 192.168.3.1 -T

84 bytes from 192.168.3.1 icmp_seq=1 ttl=62 time=31.603 ms

84 bytes from 192.168.3.1 icmp_seq=2 ttl=62 time=31.738 ms

84 bytes from 192.168.3.1 icmp_seq=3 ttl=62 time=32.090 ms

84 bytes from 192.168.3.1 icmp_seq=4 ttl=62 time=32.458 ms

84 bytes from 192.168.3.1 icmp_seq=5 ttl=62 time=32.737 ms
```

Conclusion

In this lab, we successfully configured and verified site-to-site VPN tunnels between Fortigate, Juniper SRX, and Palo Alto firewalls, demonstrating the interoperability of different vendors in a secure network environment. By establishing these connections, we enhanced our understanding of multi-vendor VPN configurations, including the intricacies of policies, static routes, and object management.

Additionally, the integration of an ASR router as an ISP highlighted the importance of proper routing and connectivity in complex network setups. The hands-on experience gained through this exercise will be invaluable for network professionals looking to implement and troubleshoot VPN solutions in real-world scenarios.

This guide serves as a foundation for further exploration into advanced configurations and troubleshooting techniques, encouraging continuous learning and adaptation in the ever-evolving field of network security.

NSE4 Course details serviced by JTA Technology

Ahmed Essam

Network Security Engineer

Fortigate Networks Firewalls

01148482530

JTA Technology

JTA Technology

Ahmed Essam