

# Troubleshooting Checklist Outline

## 1. Check connectivity from SRX to Sky ATP cloud

### a. Verify DNS

- i. Default public DNS servers on JUNOS (OpenDNS) do not always resolve Sky ATP & AWS hostnames properly, change to 8.8.8.8 (Google DNS) or another DNS provider

- 1. In JUNOS shell, execute:

```
show configuration | display set | match name-server
```

### 2. Sample output:

```
root@srx-5800-02> show configuration | display set | match
name-server
set groups global system name-server 8.8.8.8
```

- ii. Verify DNS can resolve Sky ATP servers to an IP address:

US - [amer.sky.junipersecurity.net](#) & [srxapi.us-west-2.sky.junipersecurity.net](#)

EU - [euapac.sky.junipersecurity.net](#) & [srxapi.eu-west-1.sky.junipersecurity.net](#)

Enrollment - [ca.junipersecurity.net](#) & [va.junipersecurity.net](#)

- 1. In JUNOS shell, execute:

dig <FQDN> for each server above to verify DNS can resolve hostname properly, for example:

```
dig srxapi.us-west-2.sky.junipersecurity.net
```

### 2. Sample Output

```

root@srx-3400-05% dig srxapi.us-west-2.sky.junipersecurity.net
; <<>> DiG 9.6.-ESV-R11 <<>>
srxapi.us-west-2.sky.junipersecurity.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60938
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4,
ADDITIONAL: 3
;; QUESTION SECTION:
srxapi.us-west-2.sky.junipersecurity.net. IN A
;; ANSWER SECTION:
srxapi.us-west-2.sky.junipersecurity.net. 29 IN A 54.69.49.66
srxapi.us-west-2.sky.junipersecurity.net. 29 IN A 52.39.119.162
;; AUTHORITY SECTION:
junipersecurity.net. 103073 IN NS ns-1208.awsdns-23.org.
junipersecurity.net. 103073 IN NS ns-1905.awsdns-46.co.uk.
junipersecurity.net. 103073 IN NS ns-5.awsdns-00.com.
junipersecurity.net. 103073 IN NS ns-1009.awsdns-62.net.
;; ADDITIONAL SECTION:
ns-5.awsdns-00.com. 38100 IN A 205.251.192.5
ns-1208.awsdns-23.org. 38099 IN A 205.251.196.184
ns-1905.awsdns-46.co.uk. 38101 IN A 205.251.199.113
;; Query time: 28 msec
;; SERVER: 192.168.5.68#53(192.168.5.68)
;; WHEN: Thu Jun 16 16:35:08 PDT 2016
;; MSG SIZE rcvd: 274

```

b. Verify Routing from RE and also PFE (data-plane)

i. Verify there is a valid route to Sky ATP cloud servers:

US - [amer.sky.junipersecurity.net](#) & [srxapi.us-west-2.sky.junipersecurity.net](#)

EU - [euapac.sky.junipersecurity.net](#) & [srxapi.eu-west-1.sky.junipersecurity.net](#)

Enrollment - [ca.junipersecurity.net](#) & [va.junipersecurity.net](#)

1. In JUNOS shell execute:

ping <FQDN> for each server above to test routing, for example:

```
ping ca.junipersecurity.net
```

2. Sample Output

```

root@srx-3400-05% ping ca.junipersecurity.net
PING ca-1583073466.us-west-2.elb.amazonaws.com (54.149.141.235):
56 data bytes
ping: sendto: No route to host
ping: sendto: No route to host
^C
--- ca-1583073466.us-west-2.elb.amazonaws.com ping statistics
---
2 packets transmitted, 0 packets received, 100% packet loss

```

Note in this example output, there is not a valid route to Sky ATP cloud.

ii. Verify the route to Sky ATP cloud servers is through the PFE

1. In JUNOS CLI execute:

show route <FQDN>

## 2. Sample Output

```
root@argon-srx550-06> show route ca.junipersecurity.net
inet.0: 25 destinations, 25 routes (24 active, 0 holddown,
1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 1d 00:11:55
                   > to 19.255.254.1 via ge-0/0/5.0
```

Note in this sample output, the route to Sky ATP is through PFE interface and not fxp0 or mgmt interface on RE

## c. Verify connectivity

### i. Check connectivity to device servers

US - [srxapi.us-west-2.sky.junipersecurity.net](#) port 443

EU - [srxapi.eu-west-1.sky.junipersecurity.net](#) port 443

#### 1. In JUNOS shell execute:

telnet <FQDN> for the above servers, for example:

```
telnet srxapi.eu-west-1.sky.junipersecurity.net 443
```

## 2. Sample output:

```
root@srx-3400-05% telnet
srxapi.eu-west-1.sky.junipersecurity.net 443
Trying 52.18.17.219...
telnet: connect to address 52.18.17.219: No route to host
Trying 54.171.18.197...
telnet: connect to address 54.171.18.197: No route to host
telnet: Unable to connect to remote host
```

Note in this example output, the telnet failed. If it had worked, it would have looked like:

```
• root@srx-3400-05% telnet
srxapi.eu-west-1.sky.junipersecurity.net 443
Trying 54.148.88.83...
Connected to srxapi.eu-west-1.sky.junipersecurity.net
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Note the "Connected" line.

### ii. For aamw-ca daemon, verify connectivity to [ca.junipersecurity.net](#) port 8080

#### 1. In JUNOS shell, execute:

```
root@srx-3400-05% cd /var/tmp
root@srx-3400-05% fetch
http://ca.junipersecurity.net:8080/ejbca/publicweb/apply/scep/SRX/pkiclient.exe
```

This will download a file from the CA server  
Note: Some firewalls can block this URL because it contains '.exe'  
It is normal to receive an HTTP 400 Message

- iii. For aamw-secintel-ca, aamw-cloud-ca daemons, verify connectivity to [va.junipersecurity.net](http://va.junipersecurity.net) port 80
1. In JUNOS shell, execute:

```
root@srx-3400-05% cd /var/tmp
root@srx-3400-05% fetch
http://va.junipersecurity.net/ca/SecInteljunipersecuritynetCA.pem
root@srx-3400-05% fetch
http://va.junipersecurity.net/ca/SecInteljunipersecuritynetsubCAforCloud.pem
```

- d. Check for packet loss
- i. Check for packet loss to Sky ATP device servers [srxapi.us-west-2.sky.junipersecurity.net](http://srxapi.us-west-2.sky.junipersecurity.net) or [srxapi.eu-west-1.sky.junipersecurity.net](http://srxapi.eu-west-1.sky.junipersecurity.net)
  1. In JUNOS shell, execute:

```
root@srx-3400-05% mtr srxapi.us-west-2.sky.junipersecurity.net
```

- e. Check MTU
- i. Check Path MTU Discovery
  1. In JUNOS CLI, execute:

```
root@srx-5800-01> ping connect.us-west-2.sky.junipersecurity.net
size 9001 do-not-fragment
```

This is not always reliable method. The problem is not all gateway upstream of your SRX will respond to ping or send ICMP control codes, so they will not advertise their MTU.

As another method, you can use the same ping command and adjust the payload size to see what will go through your upstream ISP:

```
root@srx-5800-01> ping connect.us-west-2.sky.junipersecurity.net
size 1472 do-not-fragment
root@srx-5800-01> ping connect.us-west-2.sky.junipersecurity.net
size 1460 do-not-fragment
root@srx-5800-01> ping connect.us-west-2.sky.junipersecurity.net
size 1450 do-not-fragment
```

- ii. Check Interface MTU and confirm it is set to 1500 or smaller
1. In JUNOS CLI, execute:

```
root@srx-3400-05> show configuration | display set | match mtu
set interfaces ge-0/0/0 mtu 9000
set interfaces ge-0/0/1 mtu 9000
```

Large MTU is currently not supported by JUNOS Sky ATP, please reduce MTU interface size to default 1500. Several customers reported that interface MTU 1450 works for most VLAN and MPLS tagged traffic.

f. Check Latency (more than 10 secs)

i. [Check latency to Sky ATP device servers](#)

[srxapi.us-west-2.sky.junipersecurity.net](#) or [srxapi.eu-west-1.sky.junipersecurity.net](#) to see over 10 seconds

1. In JUNOS shell, execute:

```
traceroute srxapi.us-west-2.sky.junipersecurity.net
```

2. Sample Output

```
root@srx-3400-05> traceroute
srxapi.us-west-2.sky.junipersecurity.net
traceroute: Warning: srxapi.us-west-2.sky.junipersecurity.net
has multiple addresses; using 54.149.92.60
traceroute to srxapi.us-west-2.sky.junipersecurity.net
(54.149.92.60), 64 hops max, 52 byte packets
 1 cns-vpn-gw.jnpr.net (10.200.200.200) 11.449 ms 18.983 ms
 10.446 ms
 2 172.29.160.66 (172.29.160.66) 10.439 ms 12.599 ms 11.367 ms
 3 jpsvl-egress-fw1.jnpr.net (172.29.130.132) 8.731 ms 9.809 ms
 9.963 ms
 4 66.129.239.2 (66.129.239.2) 29.961 ms 15.360 ms 13.332 ms
 ^C
```

Note none of the gateways took more than 10 seconds.

g. Check for Errors in logs

i. [View logs to see if there any errors during on boarding process](#)

1. In JUNOS shell, execute:

```
root@srx-3400-05> show log op-script.log
```

ii. [Enable traceoptions to see if there are errors](#)

1. In JUNOS shell, execute:

```
edit
set services advanced-anti-malware traceoptions flag daemon
set services advanced-anti-malware traceoptions flag connection
commit
```

Then check trace log for errors

2. Customer Portal Checks

a. Verify device has been added to Realm and have a current (not expired) op url

- b. Verify not using illegal characters in Realm Name or Hostname
- c. Before transferring Device from one Realm to another, dis-enroll and remove the device from the old Realm before enrolling to a new Realm

