Juniper Networks | Engineering Simplicity

Juniper Advanced Threat Prevention Cloud

Juniper ATP Cloud Troubleshooting Guide

Published
2025-04-23

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Advanced Threat Prevention Cloud Juniper ATP Cloud Troubleshooting Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to troubleshoot some typical problems you may encounter with Juniper ATP Cloud.

1

PART

Troubleshooting Juniper Advanced Threat Prevention Cloud

CHAPTER 1

Troubleshooting Juniper Advanced Threat Prevention Cloud

IN THIS CHAPTER

Juniper ATP Cloud Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you might encounter on Juniper ATP Cloud.

Table 1 on page 3 provides a summary of the symptom or problem and recommended actions with links to the troubleshooting documentation.

Table 1: Troubleshooting Juniper ATP Cloud

Symptom or Problem	Recommended Action
SRX Series Firewall can't communicate with cloud	See "Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations" on page 4 See "Troubleshooting Juniper ATP Cloud: Checking Certificates" on page 6 See "Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status" on page 8 See request services advanced-anti-malware data-connection See request services advanced-anti-malware diagnostic
Files not being sent to cloud	See "Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations" on page 4 See "Troubleshooting Juniper ATP Cloud: Checking Certificates" on page 6 See "Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status" on page 8 See Troubleshooting Juniper Advanced Threat Prevention Cloud: Checking the application-identification License
Viewing system log messages	See "Viewing Juniper ATP Cloud System Log Messages" on page 9
Setting traceoptions	See "Configure Traceoptions " on page 10 See "View the Traceoptions Log File" on page 13 See "Turning Off Traceoptions" on page 13
Dashboard reports not displaying any data	See "Juniper ATP Cloud Dashboard Reports Not Displaying" on page 14

Troubleshooting Juniper ATP Cloud: Checking DNS and Routing Configurations

Domain name system (DNS) servers are used for resolving hostnames to IP addresses.

For redundancy, it is a best practice to configure access to multiple DNS servers. You can configure a maximum of three DNS servers. The approach is similar to the way Web browsers resolve the names of a Web site to its network address. Additionally, Junos OS enables you configure one or more domain names, which it uses to resolve hostnames that are not fully qualified (in other words, the domain name is missing). This is convenient because you can use a hostname in configuring and operating Junos OS without the need to reference the full domain name. After adding DNS server addresses and domain names to your Junos OS configuration, you can use DNS resolvable hostnames in your configuration and commands instead of IP addresses.

DNS servers are site-specific. The following presents examples of how to check your settings. Your results will be different than those shown here.

First, check the IP addresses of your DNS servers.

```
show groups global system name-server
xxx.xxx.x.68;
xxx.xxx.xx.131;
```

If you set up next-hop, make sure it points to the correct router.

```
show routing-options
static {
    route 0.0.0.0/0 next-hop xx.xxx.xxx.1;
```

```
show groups global routing-options
static {
    route xxx.xx.0.0/12 {
        next-hop xx.xxx.xx.1;
        retain;
        no-readvertise;
    }
}
```

Use ping to verify the SRX Series Firewall can communication with the cloud server. First use the `show services advanced-anti-malware status` CLI command to get the cloud server hostname.

```
show service advanced-anti-malware status
Server connection status:
  Server hostname: xxx.xxx.xxx.com
  Server port: 443
    Control Plane:
      Connection Time: 2015-12-14 00:08:10 UTC
      Connection Status: Connected
    Service Plane:
      fpc0
        Connection Active Number: 0
        Connection Failures: 0
```

Now ping the server. Note that the cloud server will not respond to ping, but you can use this command to check that the hostname can be resolved to the IP address.

```
ping xxx.xxx.xxx.com
```

If you do not get a `ping: cannot resolve` *`hostname`*`: Unknown host` message, then the hostname can be resolved.

You can also use telnet to verify the SRX Series Firewall can communicate to the cloud server. First, check the routing table to find the external route interface. In the following example, it is `ge-0/0/3.0`.

```
show route
inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 2d 17:42:53
                    > to xx.xxx.xxx.1 via ge-0/0/3.0
```

Now telnet to the cloud using port 443.

```
telnet xxx.xxx.xxx.xxx.com port 443 interface ge-0/0/3.0
Trying xx.xxx.xxx.119...
Connected to xxx.xxx.xxx.xxx.com
Escape character is '^]'
```

If telnet is successful, then your SRX Series Firewall can communicate with the cloud server.

Troubleshooting Juniper ATP Cloud: Checking Certificates

Use the `show security pki local-certificate` CLI command to check your local certificates. Ensure that you are within the certificate's valid dates. The `ssl-inspect-ca` certificate is used for SSL proxy. Show below are some examples. Your output might look different as these are dependent on your setup and location.

```
show security pki local-certificate
Certificate identifier: ssl-inspect-ca
  Issued to: www.juniper_self.net, Issued by: CN = www.juniper_self.net, OU = IT
, O = Juniper Networks, L = xxxxx, ST = xxxxx, C = IN
  Validity:
    Not before: 11-24-2015 22:33 UTC
    Not after: 11-22-2020 22:33 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-srx-cert
  Issued to: xxxx-xxxx_xxx, Issued by: C = US, O = Juniper Ne
tworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) subCA for SRX dev
ices, emailAddress = xxx@juniper.net
  Validity:
    Not before: 10-30-2015 21:56 UTC
    Not after: 01-18-2038 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

Use the `show security pki ca-certificate` command to check your CA certificates. The `argon-ca` certificate is the client certificate's CA while the `argon-secintel-ca` is the server certificate's CA. Ensure that you are within the certificate's valid dates.

```
root@host> show security pki ca-certificate
Certificate identifier: argon-ca
  Issued to: SecIntel (junipersecurity.net) subCA for SRX devices, Issued by: C
= US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.ne
t) CA, emailAddress = xxx@juniper.net
  Validity:
    Not before: 05-19-2015 22:12 UTC
    Not after: 05- 1-2045 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-secintel-ca
  Issued to: SecIntel (junipersecurity.net) CA, Issued by: C = US, O = Juniper N
etworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) CA, emailAddress
```

```
 = xxx@juniper.net
  Validity:
    Not before: 05-19-2015 03:22 UTC
    Not after: 05-16-2045 03:22 UTC
  Public key algorithm: rsaEncryption(2048 bits)
```

When you enroll an SRX Series Firewall, the ops script installs two CA certificates: one for the client and one for the server. Client-side CA certificates are associated with serial numbers. Use the `show security pki local-certificate detail` CLI command to get your device's certificate details and serial number.

```
show security pki local-certificate detail
Certificate identifier: aamw-srx-cert
  Certificate version: 3
  Serial number: xxxxxxxxxx
  Issuer:
    Organization: Juniper Networks Inc, Organizational unit: SecIntel, Country: US,
    Common name: SecIntel (junipersecurity.net) subCA for SRX devices
  Subject:
    Organization: xxxxxxxxxx, Organizational unit: SRX, Country: US,
    Common name: xxxxxxxxxx
  Subject string:
    C=US, O=xxxxxxxx, OU=SRX, CN=xxxxxxxx, emailAddress=secintel-ca@juniper.net
  Alternate subject: secintel-ca@juniper.net, fqdn empty, ip empty
  Validity:
    Not before: 11-23-2015 23:08 UTC
    Not after: 01-18-2038 15:00 UTC
```

Then use the `show security pki crl detail` CLI command to make sure your serial number is not in the Certificate Revocation List (CRL). If your serial number is listed in the CRL then that SRX Series Firewall cannot connect to the cloud server.

```
show security pki crl detail
CA profile: aamw-ca
  CRL version: V00000001
  CRL issuer: C = US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel
(junipersecurity.net) subCA for SRX devices, emailAddress = secintel-ca@juniper.net
  Effective date: 11-23-2015 23:16 UTC
  Next update: 11-24-2015 23:16 UTC
  Revocation List:
    Serial number              Revocation date
    xxxxxxxxxxxxxxxx                10-26-2015 17:43 UTC
```

```
    xxxxxxxxxxxxxxxxx               11- 3-2015 19:07 UTC
    ...
```

Troubleshooting Juniper ATP Cloud: Checking the Routing Engine Status

Use the `show services advanced-anti-malware status` CLI command to show the connection status from the control plane or routing engine.

```
show services advanced-anti-malware status
Server connection status:
  Server hostname: xxx.xxx.xxx.xxx.com
  Server port: 443
    Control Plane:
      Connection Time: 2015-12-01 08:58:02 UTC
      Connection Status: Connected
    Service Plane:
      fpc0
        Connection Active Number: 0
        Connection Failures: 0
```

If the connection fails, the CLI command will display the reason in the Connection Status field. Valid options are:

- Not connected
- Initializing
- Connecting
- Connected
- Disconnected
- Connect failed
- Client certificate not configured
- Request client certificate failed
- Request server certificate validation failed
- Server certificate validation succeeded

- Server certificate validation failed
- Server hostname lookup failed

Troubleshooting Juniper ATP Cloud: Checking the Application-Identification License

You must have a valid application-identification (AppID) license installed for the supported platforms. For the complete list of supported features and platforms, see Application Identification in Feature Explorer. Use the `show services application-identification version` CLI command to verify the applications packages have been installed. You must have version 2540 or later installed. For example:

```
show services application-identification version
Application package version: 2540
```

If you do not see the package or the package version is incorrect, use the `request services application-identification download` CLI command to download the latest application package for Junos OS AppID. For example:

```
request services application-identification download
Please use command "request services application-identification download status"  to check status
```

Then use the `request services application-identification install` CLI command to install the downloaded application signature package.

```
request services application-identification install
Please use command "request services application-identification install status"  to check status
```

Use the `show services application-identification application version` CLI command again to verify the applications packages is installed.

Viewing Juniper ATP Cloud System Log Messages

The Junos OS generates system log messages (also called syslog messages) to record events that occur on the SRX Series Firewall. Each system log message identifies the process that generated the message

and briefly describes the operation or error that occurred. Juniper ATP Cloud logs are identified with a SRX_AAWM_ACTION_LOG or SRX AAMWD entry.

The following example configures basic syslog settings.

```
set groups global system syslog user * any emergency
set groups global system syslog host log kernel info
set groups global system syslog host log any notice
set groups global system syslog host log pfe info
set groups global system syslog host log interactive-commands any
set groups global system syslog file messages kernel info
set groups global system syslog file messages any any
set groups global system syslog file messages authorization info
set groups global system syslog file messages pfe info
set groups global system syslog file messages archive world-readable
```

To view events in the CLI, enter the following command:

```
show log
```

Example Log Message

```
<14> 1 2013-12-14T16:06:59.134Z pinarello RT_AAMW - SRX_AAMW_ACTION_LOG [junos@xxx.x.x.x.x.28
http-host="www.mytest.com" file-category="executable" action="BLOCK" verdict-number="8" verdict-
source=”cloud/blacklist/whitelist” source-address="x.x.x.1" source-port="57116" destination-
address="x.x.x.1" destination-port="80" protocol-id="6" application="UNKNOWN" nested-
application="UNKNOWN" policy-name="argon_policy" username="user1" session-id-32="50000002"
source-zone-name="untrust" destination-zone-name="trust"]

http-host=www.mytest.com file-category=executable action=BLOCK verdict-number=8 verdict-
source=cloud source-address=x.x.x.1 source-port=57116 destination-address=x.x.x.1 destination-
port=80 protocol-id=6 application=UNKNOWN nested-application=UNKNOWN policy-name=argon_policy
username=user1 session-id-32=50000002 source-zone-name=untrust destination-zone-name=trust
```

Configure Traceoptions

In most cases, policy logging of the traffic being permitted and denied is sufficient to verify what Juniper ATP Cloud is doing with the SRX Series Firewall data. However, in some cases you might need more information. In these instances, you can use traceoptions to monitor traffic flow into and out of the SRX Series Firewall.

Using trace options are the equivalent of debugging tools. To debug packets as they pass through the SRX Series Firewall, you need to configure `traceoptions` and flag `basic-datapath`. This configuration will trace packets as they enter the SRX Series Firewall until they exit, giving you details of the different actions the SRX Series Firewall is taking along the way. See Debugging the Data Path in the SRX Series documentation for details.

A minimum `traceoptions` configuration must include both a target `file` and a `flag`. The target `file` determines where the trace output is recorded. The `flag` defines what type of data is collected. For more information about using `traceoptions`, see the documentation for your SRX Series Firewall.

To set the trace output file, use the `file` *`filename`* option. The following example defines the trace output file as `srx_aamw.log`:

```
edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]
set file srx_aamw.log
```

where `flag` defines what data to collect and can be one of the following values:

- `all`—Trace everything.
- `connection`—Trace connections to the server.
- `content`—Trace the content buffer management.
- `daemon`—Trace the Juniper ATP Cloud daemon.
- `identification`—Trace file identification.
- `parser`—Trace the protocol context parser.
- `plugin`—Trace the advanced anti-malware (AAMW) plug-in.
- `policy`—Trace the AAMW policy.

The following example traces connections to the SRX Series Firewall and the AAMW policy:

```
edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]set services advanced-anti-malware
traceoptions file skyatp.logset services advanced-anti-malware traceoptions file size 100M
set services advanced-anti-malware traceoptions level allset services advanced-anti-malware
traceoptions flag all
```

Before committing your `traceoption` configuration, use the `show services advanced-anti-malware` command to review your settings.

```
# show services advanced-anti-malware
url https://xxx.xxx.xxx.com;
authentication {
    tls-profile
        ...
}
traceoptions {
    file skyatp.log;
    flag all;
    ...
}

...
```

You can also configure public key infrastructure (PKI) trace options. For example:

```
set security pki traceoptions file pki.log
set security pki traceoptions flag all
```

Debug tracing on both the Routing Engine and the Packet Forwarding Engine can be enabled for SSL proxy by setting the following configuration:

```
set services ssl traceoptions file ssl.log
set services ssl traceoptions file size 100m
set services ssl traceoptions flag all
```

You can enable logs in the SSL proxy profile to get to the root cause for the drop. The following errors are some of the most common:

- Server certification validation error
- The trusted CA configuration does not match your configuration.
- System failures such as memory allocation failures
- Ciphers do not match.
- SSL versions do not match.
- SSL options are not supported.

- Root CA has expired. You need to load a new root CA.

Set flow trace options to troubleshoot traffic flowing through your SRX Series Firewall:

```
set security flow traceoptions flag all
set security flow traceoptions file flow.log size 100M
```

RELATED DOCUMENTATION

> Enabling Debugging and Tracing for SSL Proxy
>
> traceoptions (Security PKI)

View the Traceoptions Log File

Once you commit the configuration, `traceoptions` starts populating the log file with data. Use the `show log` CLI command to view the log file. For example:

```
show log srx_aamw.log
```

Use `match`, `last` and `trim` commands to make the output more readable. For more information about using these commands, see Configuring Traceoptions for Debugging and Trimming Output.

Turning Off Traceoptions

`traceoptions` is very resource-intensive. We recommend you turn off `traceoptions` when you are finished to avoid any performance impact. There are two ways to turn off `traceoptions`.

The first way is to use the `deactivate` command. This is a good option if you need to activate the trace in the future. Use the `activate` command to start capturing again.

```
deactive services advanced-anti-malware traceoptionscommit
```

The second way is to remove `traceoptions` from the configuration file using the `delete` command.

```
delete services advanced-anti-malware traceoptions
commit
```

You can remove the `traceoptions` log file with the `file delete` *filename* CLI command or clear the contents of the file with the `clear log` *filename* CLI command.

Juniper ATP Cloud Dashboard Reports Not Displaying

Juniper ATP Cloud dashboard reports require the Juniper ATP Cloud premium license for the C&C Server & Malware report. If you do not see any data in this dashboard report, make sure that you have purchased a premium license. For more information, see Software Licenses for ATP Cloud.

NOTE: Juniper ATP Cloud does not require you to install a license key onto your SRX Series Firewall. Instead, your entitlement for a specific serial number is automatically transferred to the cloud server. It might take up to 24 hours for your activation to be updated in the Juniper Advanced Threat Cloud server. For more information, see Manage the Juniper Advanced Threat Prevention Cloud License.

All reports are specific to your realm; no report currently covers trends derived from the Juniper ATP Cloud worldwide database. Data reported from files uploaded from your SRX Series Firewalls and other features make up the reports shown in your dashboard.

If you did purchase a premium license and followed the configuration steps (Quick Start) and are still not seeing data in the dashboard reports, contact Juniper Networks Technical Support.

Juniper ATP Cloud RMA Process

On occasion, because of hardware failure, a device needs to be returned for repair or replacement. For these cases, contact Juniper Networks, Inc. to obtain a Return Material Authorization (RMA) number and follow the RMA Procedure.

Once you transfer your license keys to the new device, it might take up to 24 hours for the new serial number to be registered with the Juniper ATP Cloud cloud service.

WARNING: After any serial number change on the SRX Series Firewall, a new RMA serial number needs to be re-enrolled with Juniper ATP Cloud cloud. This means that you must enroll your replacement unit as a new device. See Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal. Juniper ATP Cloud does not have an “RMA state”, and does not see these as replacement devices from a configuration or registration point of view. Data is not automatically transferred to the replacement SRX Series Firewall from the old device.

CHAPTER 2

Configuration Statements and Operational Commands

IN THIS CHAPTER

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands