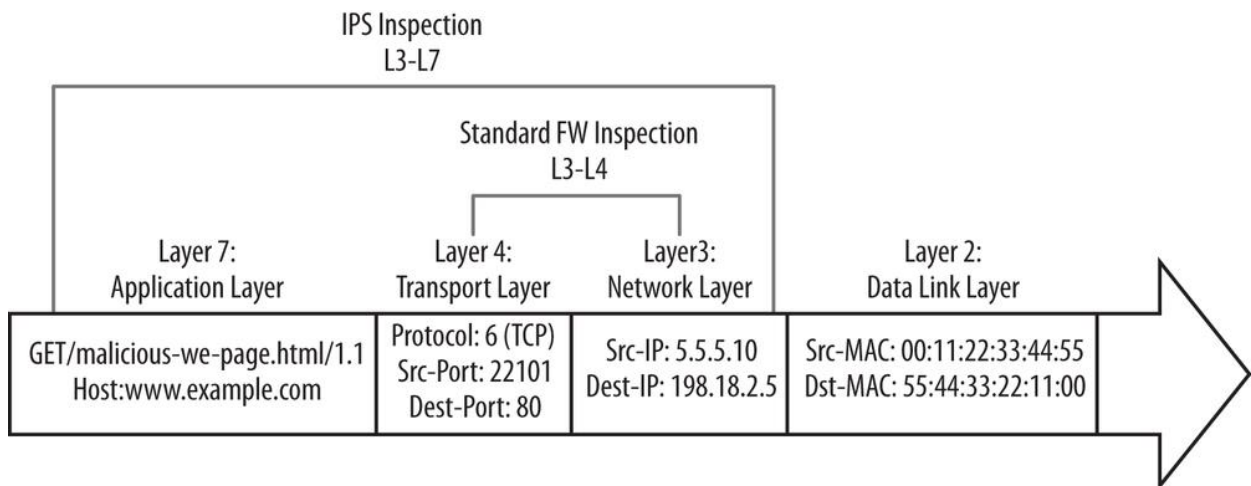


INTRUSION DETECTION AND PREVENTION ON IBM CLOUD

Traditional firewalls might not detect some malicious traffic, for these types of attacks, the solution is to use IDP. Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents on the vSRX platform.



IDP Protection Mechanism: Live Attack Database

Juniper networks maintains a database of attack signatures to use with the IDP feature. With a valid license, users can retrieve updates manually by running a CLI command, or automatically by configuring a JunOS security policy to update its database at regular intervals.

The full package download includes various policy templates. These policy templates offer protection against a variety of common attacks. Once you install these templates, you can customize them to fit the traffic patterns of a particular network.

IDP Policy Framework

Policy drives the IDP attack detection engine. IDP policy enables selective enforcement of various IDP attack detection and prevention techniques on network traffic passing through the IDP engine.

Users can write very granular rules to match a section of traffic based on zones, networks, and applications. Users can then apply specific attack prevention techniques on that traffic and take active or passive preventive actions.

Figure 2 illustrates the structural view of an IDP policy. An IDP policy can consist of an intrusion prevention system (IPS) rule base. A rule base is a collection of rules. Rules contain a collection of configuration objects and are similar in structure to security policy because they are configuration objects to create match conditions and resulting actions. Once you create IDP policy, the action of security policy applies it. Although many IDP policies might exist within the configuration, only one IDP policy is active.

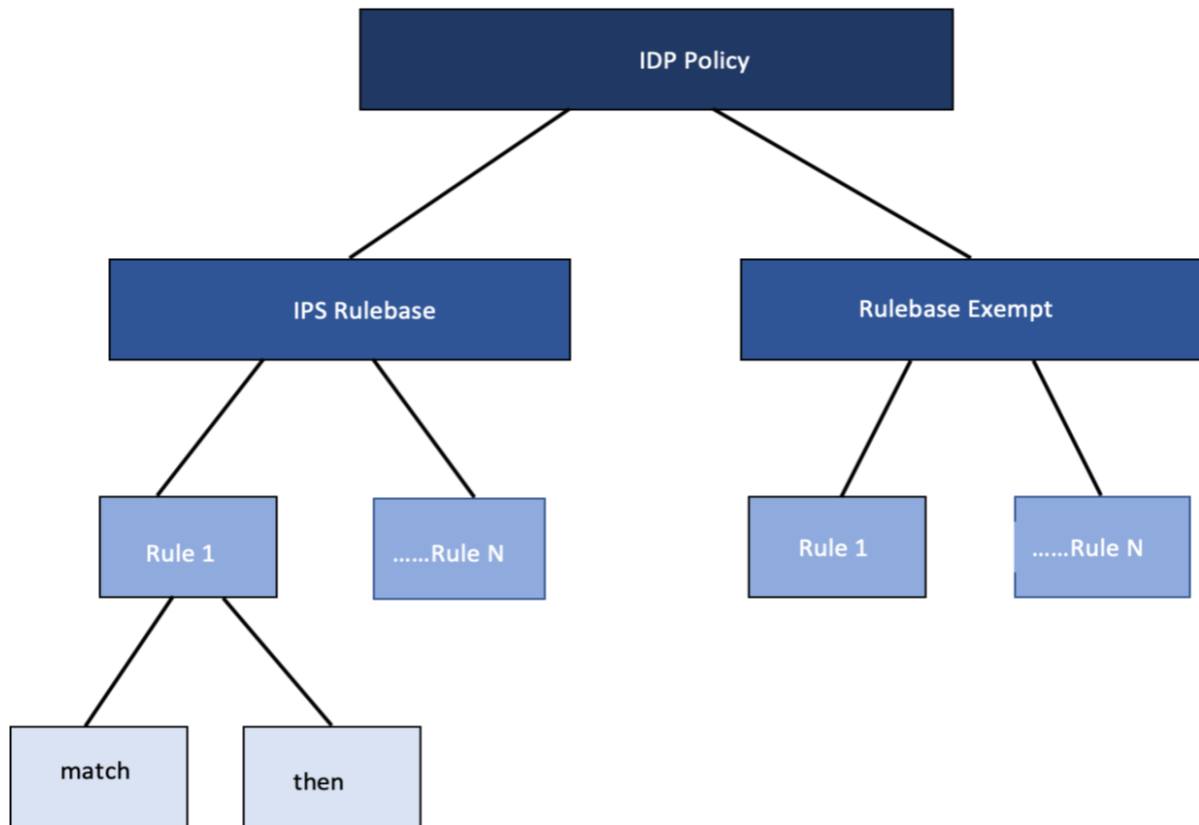


Figure 2

IDP Policy

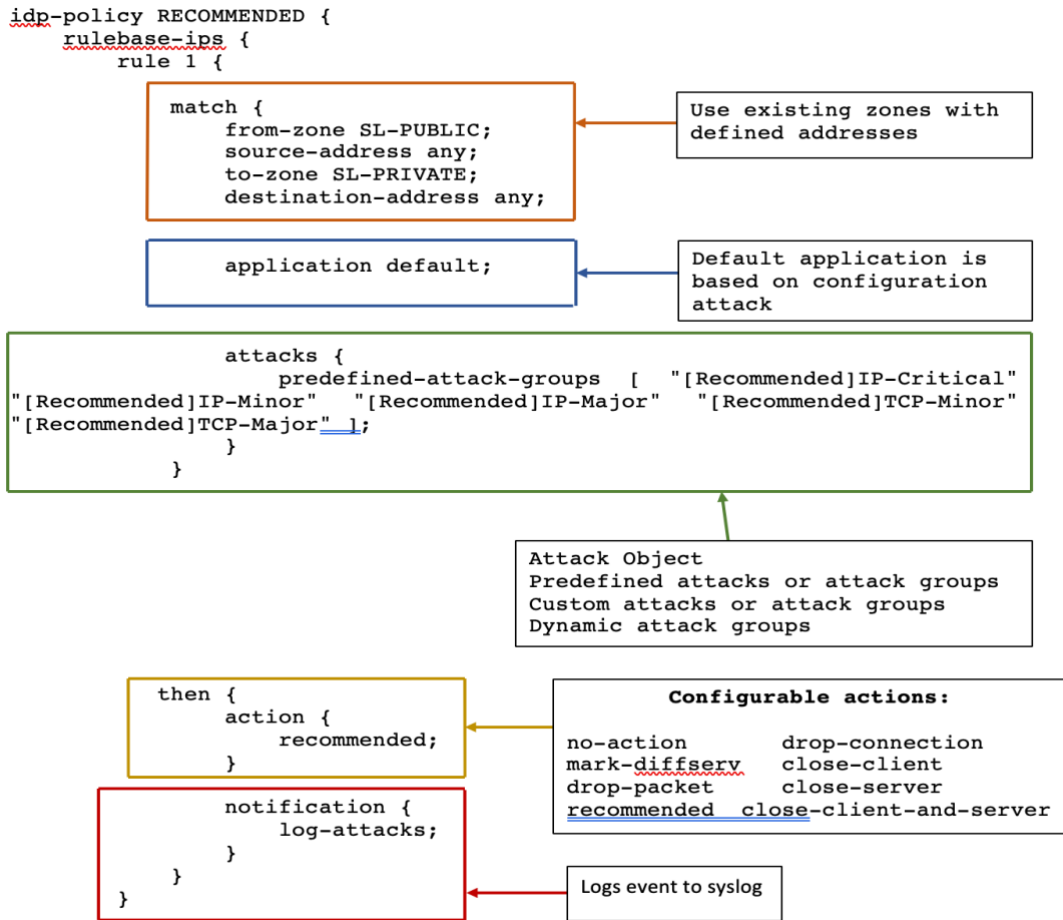


Figure 3

Figure 3 (above) shows an IDP policy configured with name RECOMMENDED. The 'rule 1' is an IPS rule base with matching conditions. In this case, the rule matches from zone SL-PUBLIC with any source address to zone SL-PRIVATE and any destination address. The rule also matches on an application type default. When we select this application type, the software bases application matches on the attack or attack group objects. The JunOS OS automatically matches on application or services settings associated with defined attack or attack group object. We can also specify a configuration application or application-set or use the "any" option.

The configuration in the figure shows a predefined attack group designed for IP and TCP attacks. Predefined attack and attack group objects are part of the signature database that can be downloaded from Juniper networks.

We can also specify custom attacks and attacks group objects or dynamic attack group objects. Custom attack and attack groups are user defined configuration. The software builds dynamic attack groups using filters that match on a particular option, such as an application.

This example defines an action *recommended*. This type of action is only applicable to IPS rule base predefined attack objects. Juniper Networks recommended action is associated with all predefined attack objects. A rule can have one of the following actions:

- **no-action:** Junos OS takes no action. (used when you only need to generate a log)
- **ignore-connection:** Junos OS stops scanning traffic for the rest of the connection.
- **mark-diffserv:** Junos OS assigns the indicated service-differentiation value to the packet then passes it on normally.
- **drop-packet:** Junos OS drops a packet before it can reach its destination - but does not close the connection.
- **recommended:** The action that Juniper networks recommended when it detects a predefined attack.
- **drop-connection:** Junos drops connection, preventing traffic for the connection from reaching its destination.
- **close-client:** Junos OS closes the connection and sends a RST packet to the client but not the server.
- **close-server:** Junos OS closes the connection and sends a RST packet to the server but not the client.
- **close-client-and-server:** Junos OS closes the connection and sends a RST packet to both client and server.

IP actions prevent repeat attacks. This rule action applies to future sessions that have the same IP action attribute of the flow on which the software detects an attack. For example, you could configure one of the IP actions in a rule to block all future HTTP sessions between two hosts if the software detects an attack on a session between hosts. Optionally you can specify a timeout value defining that the action should apply only if new sessions initiate within a specified timeout value in seconds.

IP action attributes can be used only in certain combination and list as targets in the following output:

- **destination-address: Match destination**
- **service: Match source, destination, dst-port and protocol**
- **source-address: Match source**
- **source-zone: Match source-zone**
- **source-zone-address: Match source-zone and source-address**
- **zone-service: Match source-zone, destination, dst-port, protocol**

The following are the possible IP actions:

- **ip-notify: Notify about future traffic**
- **ip-close: Close future connections**
- **ip-block: Block future connections**

```

rule 4 {
  match {
    from-zone SL-PUBLIC;
    source-address any;
    to-zone SL-PRIVATE;
    destination-address any;
    application default;
    attacks {
      predefined-attack-groups "[Recommended]UDP - All";
    }
  }
  then {
    action {
      recommended;
    }
    ip-action {
      ip-block;
      target source-address;
    }
  }
}

```

Applying the Recommended IDP policy

Starting with Junos OS Release 18.2R1, IDP policy is directly assigned in the security policy rule. This is to simplify IDP policy usage and to provide flexibility to have multiple policies active at the same time. As a part of session interest check IDP will be enabled if IDP policy is present in any of the matched rules. IDP policy is activated in security policies, by permitting the IDP policy within the application services.

```

from-zone SL-PUBLIC to-zone SL-PRIVATE {
  policy IDP_POLICY {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          idp-policy RECOMMENDED;
        }
      }
    }
  }
}

```

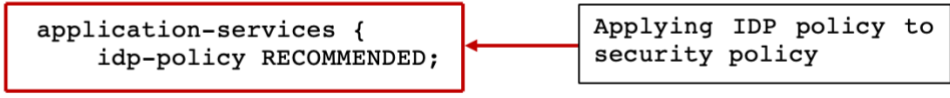


Figure 4

Activating the Recommended IDP Policy

Only one IDP policy is active on a Junos security platform at any given time. If multiple policies are configured, you can activate the required policy by the below command...

```
root@vsrx# set security idp default-policy?
```

Possible completions:

```
<default-policy>      Set active policy  
  
RECOMMENDED
```

Evaluating a Rule base

Once the RE applies an IDP policy, it pushes the policy to the data plane where the IDP policy evaluation occurs. IDP policy evaluates only the first packet of a session. If a match occurs, the software creates a set of objects and caches them within the session for use with attack detection on subsequent packets.

Junos OS evaluates IDP policies sequentially. If the session matches multiple rules, the Junos OS performs the most severe action among the rules. The order of severity is as follows:

1. Close
2. Drop
3. Diffserv
4. Ignore
5. No action

You can make an IDP rule terminal using the below command:

```
root@vsrx# set security idp idp-policy RECOMMENDED rulebase-ips rule 1  
terminal
```

When the software configures a match in a terminal rule for source, destination, zones and application it does not continue to check subsequent rules for same source, destination, and application. It does not matter whether traffic matches the attack objects in the matching rule or not. This option is useful for disregarding traffic that originates from a known trusted source. Terminal rules should appear near the top of the rule base and before other rules that would match the same traffic.

Exempt Rule base

The functionality of an exempt rule base complements an IPS rule base. You can write rules in an exempt rule base to skip detection of a set of attack in certain traffic. Carefully written rules in an exempt rule base can significantly reduce the number of false positives generated by an IPS rule base.

Note that you must configure an IPS rule base before using an exempt rule base. Rules in an exempt rule base have the same matching conditions as those of IPS rule base. The exception is that you cannot configure the application object, which means rules match all applications.

When configuring attack or attack object in an exempt rule base, note that these attacks are attacks the software should not inspect in traffic matching this rule. No actions are available for exempt rule base.

Signature Database

The signature database is one of the major components of IDP. It contains definitions of different objects show below that can be used to define IDP policy rule:

- Attack objects
- Application signature objects and
- Service objects.

The database lists the attack objects alphabetically. The names consist of attack object group name and the name of attack object. The security package downloaded also includes IDP policy templates to implement IDP policies. You can use policies as they are or customize them for your network environment. The most widely used template is called the *Recommended policy*.

Enabling firewall filters for IDP

It is important to allow TCP if firewall filters are configured, otherwise package download will fail.

```
set firewall filter <filter-name> term <term-name> from source-port 443
set firewall filter <filter-name> term <term-name> from tcp-established
set firewall filter <filter-name> term <term-name> then accept
```

Tracing IDP operations

Optionally trace option file can be set to track the download and installation status

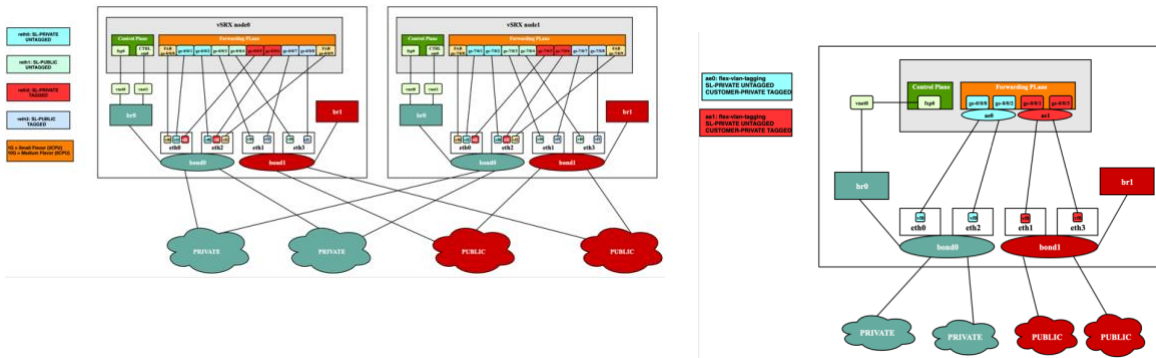
```
set security idp traceoptions file idpd
set security idp traceoptions file size 20m
set security idp traceoptions flag all
set security idp traceoptions level all
```

If your deployment of vSRX is HA, make sure the clusters is healthy.

NOTE: This document serves as a guide to introduce customers to configuring IDP on vSRX. This document is not a recommendation, nor does it cover other IDP policy templates available.

We define IDP policies and then assign it to policies. It is recommended that policies which have reference to IDP policies to be placed at the top of the policy hierarchy.

Downloading IDP Signature Database for Private & Public deployment (Online Method)



Install IDP license

1. License must be applied to both clusters if it's a HA solution

```
root@vsrx> show system license
```

License usage:

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
idp-sig	1	0	1	2019-07-18 00:00:00

2. Configure and commit the below statement on vSRX to download IDP security package.

```
root@vsrx# set security idp security-package url
https://services.netscreen.com/cgi-bin/index.cgi
```

```
root@vsrx# show security idp
```

```
security-package {
url https://services.netscreen.com/cgi-bin/index.cgi;
```

3. Download the IDP security package to JUNOS

```
root@vsrx> request security idp security-package download full-update
```

```
node0:
```

```
-----  
Will be processed in async mode. Check the status using the status checking  
CLI
```

4. Check the status of the download

```
root@vsrx> request security idp security-package download status
```

```
node0:
```

```
-----  
Done;Successfully downloaded from(https://services.netscreen.com/cgi-  
bin/index.cgi) and synchronized to backup.Version info:3181(Tue Jun 18  
11:57:00 2019 UTC, Detector=12.6.130190309)
```

5. Download the predefined policy template. Use command in step 4 to check the status

```
root@vsrx> request security idp security-package download policy-templates
```

6. IDP package will be downloaded to the below directory in JUNOS

```
root@vsrx> start shell
```

```
root@vsrx:~ # ls -l /var/db/idpd/sec-download
```

```
-rw----- 1 688 935 50927682 Jun 13 11:55 SignatureUpdate.xml  
-rw----- 1 688 935 187375 Jun 13 11:55 application_groups.xml  
-rw----- 1 688 935 603663 Jun 13 11:55 application_groups2.xml  
-rw----- 1 688 935 1401453 Jun 13 11:55 applications.xml  
-rw----- 1 688 935 11885 Jun 13 11:55 applications.xsd  
-rw----- 1 688 935 5362144 Jun 13 11:55 applications2.xml  
-rw----- 1 688 935 295670 Jun 13 11:55 contexts.xml  
-rwxr-xr-x 1 root wheel 801406 Jun 19 02:07 detector-capabilities.xml  
-rw----- 1 688 935 513668 Jun 13 11:55 filters.xml  
-rw----- 1 688 935 5071615 Jun 13 11:55 groups.xml
```

```

-r--r--r-- 1 688 935 14545 Jun 13 11:55 heuristics.bin
-r--r--r-- 1 688 935 2492688 Jun 13 11:55 libidp-detector.so.tgz.v
-r-x----- 1 688 935 4765968 Jun 13 11:55 libqmpprotocols.tgz
-rw-r--r-- 1 root wheel 83 Jun 19 02:04 manifest.xml
-rw----- 1 688 935 495 Jun 13 11:55 platforms.xml
-rw----- 1 688 935 562054 Jun 13 11:55 products.xml
-rw----- 1 688 935 14767 Jun 13 11:55 services.xml
drwxr-xr-x 2 root wheel 512 Jun 19 02:02 sub-download

```

Checkpoint:

If SignatureUpdate.xml is not found in `/var/db/idpd/sec-download/sub-download` copy it from `/var/db/idpd/sec-download`. SignatureUpdate.xml must be present in `/var/db/idpd/sec-download/sub-download`

```
root@vsrx:~ # ls -lsh /var/db/idpd/sec-download/sub-download
```

```
-rw----- 1 root wheel 50927682 Jun 19 02:02 SignatureUpdate.xml
```

7. Install the downloaded security package

```
root@vsrx> request security idp security-package install
```

```
node0:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

```
node1:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

```
root@vsrx:~ # exit
```

8. Check the status of install

```
root@vsrx> request security idp security-package install status
```

```
node0:
```

```
-----  
Done;Attack DB update : successful - [UpdateNumber=3181,ExportDate=Tue Jun 18  
11:57:00 2019 UTC,Detector=12.6.130190309]
```

```
    Updating control-plane with new detector : successful
```

```
    Updating data-plane with new attack or detector : not performed  
    due to no active policy configured.
```

```
node1:
```

```
-----  
Done;Attack DB update : successful - [UpdateNumber=3181,ExportDate=Tue Jun 18  
11:57:00 2019 UTC,Detector=12.6.130190309]
```

```
    Updating control-plane with new detector : successful
```

```
    Updating data-plane with new attack or detector : not performed  
    due to no active policy configured.
```

9. Check IDP security package version

```
root@vsrx> show security idp security-package-version
```

```
node0:
```

```
-----  
Attack database version:3291(Thu Jun 18 13:24:12 2020 UTC)
```

```
Detector version :12.6.130200415
```

```
Policy template version :3266
```

```
node1:
```

```
-----  
Attack database version:3291(Thu Jun 18 13:24:12 2020 UTC)
```

```
Detector version :12.6.130200415
```

```
Policy template version :3266
```

10. Install predefined policy templates downloaded in step 5. These policy templates serve as an example from Juniper Networks, but custom policies can be built according to customer needs.

Checkpoint:

- Step 5 should be completed for installing (step 10) and checking policy status (step 11)
- Make sure that template.xml is present in the /var/db/idpd/sec-download/sub-download

```
root@vsrx:~ # ls -lsh /var/db/idpd/sec-download/sub-download
164 -rw-r--r-- 1 root wheel 162K Jun 19 08:00 templates.xml
```

Juniper Networks provides predefined policy templates that you can use as a starting point for creating your own policies. Each template is set of rules of a specific rule-base type that you can copy and then update according to your requirements.

```
root@vsrx> request security idp security-package install policy-templates
```

```
node0:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

```
node1:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

Checkpoint:

Before you proceed with Juniper Networks template installation, make sure that templates have been downloaded by executing the command shown on step 5.

11. Check the status of policy install.

```
root@vsrx> request security idp security-package install status
```

```
node0:
```

```
-----
Done;policy-templates has been successfully updated into internal repository
(=>/var/run/scripts/commit/templates.xml)!
```

```
node1:
```

```
-----
Done;policy-templates has been successfully updated into internal repository
```

```
(=>/var/run/scripts/commit/templates.xml)!
```

12. Activate template script

```
root@vsrx# set system scripts commit file templates.xml
```

```
root@vsrx# commit
```

13. Verify policy templates

Note: The below command is a hidden command and you need to type in the full command.

```
root@vsrx# set security idp active-policy ?
```

Possible completions:

```
<active-policy>      Set active policy
```

```
Client-And-Server-Protection
```

```
Client-And-Server-Protection-1G
```

```
Client-Protection
```

```
Client-Protection-1G
```

```
DMZ_Services
```

```
DNS_Service
```

```
File_Server
```

```
Getting_Started
```

```
IDP_Default
```

```
RECOMMENDED
```

```
Recommended
```

```
Server-Protection
```

```
Server-Protection-1G
```

```
Web_Server
```

Automatic security package download

You can configure a Private/Public security platform to automatically download the security package

```
show security idp

security-package {
  automatic {
    start-time "2019-7-12.09:00:00 +0000";
    interval 24;
    enable;
  }
}
```


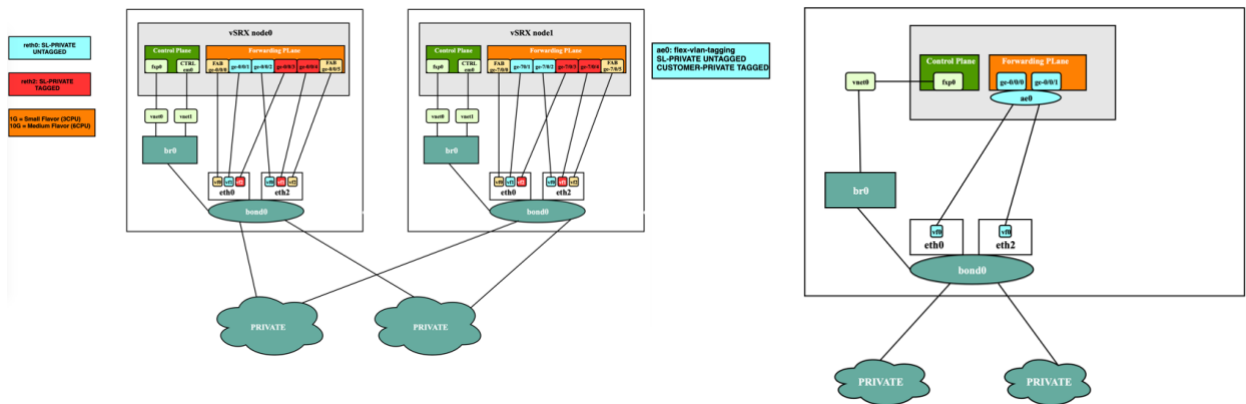


Figure 7

Downloading IDP Signature Database through offline method

Offline method is required for Private only deployments as they do not have public connection.



1. Enable Trace options

```
root@vsrx# set security idp traceoptions file idpd
root@vsrx# set security idp traceoptions file size 20m
root@vsrx# set security idp traceoptions flag all
root@vsrx# set security idp traceoptions level all
root@vsrx# commit
```

2. After committing the configuration in step 1 execute the below command

```
root@vsrx> request security idp security-package download full-update
```

This command is to get the correct download URL constructed in the idpd file. Since the vSRX does not expect to have an Internet connection, the command will give a failure status in the CLI, which is expected.

3. After step 2, get the URL of security package in `/var/log/idpd` file

You can search the URL with help of below operational command


```
{primary:node0}
root@vsrx> show log idpd | match SecPackage
```

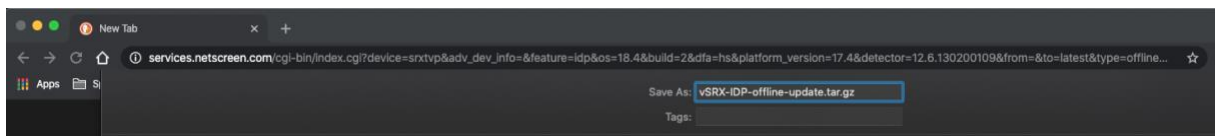
Sample URL from the `"/var/log/idpd"` log:

```
Mar 10 22:07:19 [idp_secpack_download_handler]: URL sent to get the
SecPackage is: https://services.netscreen.com/cgi-
bin/index.cgi?device=srxtp&adv_dev_info=&feature=idp&os=18.4&build=2&dfa=hs&
platform_version=17.4&detector=12.6.130200109&from=&to=latest&type=update&sn=
&release=10
```

4. Copy the above URL and change the "type" parameter value to "offline" as shown below

```
https://services.netscreen.com/cgi-
bin/index.cgi?device=srxtp&adv_dev_info=&feature=idp&os=18.4&build=2&dfa=hs&
platform_version=17.4&detector=12.6.130200109&from=&to=latest&type=offline&sn=
&release=10
```

5. Browse the URL using IE/Firefox/Chrome: It will download `offline-update.tar.gz` file.



6. Transfer the downloaded security package to vSRX. In the case of HA deployments, the package will be transferred to the node which is acting as primary for RG0.

```
% scp vSRX-IDP-offline-update.tar.gz root@<ip>:/var/tmp
```

7. Install IDP license
License must be applied to both clusters if it's an HA solution.

```
root@vsrx> show system license
```

```
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
idp-sig	1	0	1	2019-07-18 00:00:00

8. Download the IDP security package to JUNOS

```
root@vsrx> request security idp security-package offline-download package-
path /var/tmp/vSRX-IDP-offline-update.tar.gz
```

9. Check the status of download

```
root@vsrx> request security idp security-package offline-download status
```

```
Done;Signature package offline download Successful.
```

10. IDP package will be downloaded to the below directory in JUNOS

```
root@vsrx> start shell
```

```
root@vsrx:~ # ls -l /var/db/idpd/sec-download
```

```
-rw----- 1 688 935 50927682 Jun 13 11:55 SignatureUpdate.xml
-rw----- 1 688 935 187375 Jun 13 11:55 application_groups.xml
-rw----- 1 688 935 603663 Jun 13 11:55 application_groups2.xml
-rw----- 1 688 935 1401453 Jun 13 11:55 applications.xml
-rw----- 1 688 935 11885 Jun 13 11:55 applications.xsd
-rw----- 1 688 935 5362144 Jun 13 11:55 applications2.xml
-rw----- 1 688 935 295670 Jun 13 11:55 contexts.xml
-rwxr-xr-x 1 root wheel 801406 Jun 19 02:07 detector-capabilities.xml
-rw----- 1 688 935 513668 Jun 13 11:55 filters.xml
```

```

-rw----- 1 688 935 5071615 Jun 13 11:55 groups.xml
-r--r--r-- 1 688 935 14545 Jun 13 11:55 heuristics.bin
-r--r--r-- 1 688 935 2492688 Jun 13 11:55 libidp-detector.so.tgz.v
-r-x----- 1 688 935 4765968 Jun 13 11:55 libqmprotocols.tgz
-rw-r--r-- 1 root wheel 83 Jun 19 02:04 manifest.xml
-rw----- 1 688 935 495 Jun 13 11:55 platforms.xml
-rw----- 1 688 935 562054 Jun 13 11:55 products.xml
-rw----- 1 688 935 14767 Jun 13 11:55 services.xml
drwxr-xr-x 2 root wheel 512 Jun 19 02:02 sub-download

```

Checkpoint:

If SignatureUpdate.xml is not found in /var/db/idpd/sec-download/sub-download copy it from /var/db/idpd/sec-download. SignatureUpdate.xml must be present in /var/db/idpd/sec-download/sub-download

```
root@vsrx:~ # ls -lsh /var/db/idpd/sec-download/sub-download
```

```
-rw----- 1 root wheel 50927682 Jun 19 02:02 SignatureUpdate.xml
```

11. Install IDP security package

```
root@vsrx> request security idp security-package install
```

Will be processed in async mode. Check the status using the status checking CLI

12. Check the status of install

```
root@vsrx> request security idp security-package install status
```

```
Done;Attack DB update : successful - [UpdateNumber=3180,ExportDate=Thu Jun 13
11:55:28 2019 UTC,Detector=12.6.130190309]
```

```
Updating control-plane with new detector : successful
```

```
Updating data-plane with new attack or detector : not performed due to
no active policy configured.
```

13. Optionally install predefined policy-templates downloaded earlier.

Juniper Networks provides predefined policy templates that you can use as a starting point for creating your own policies. Each template is set of rules of a specific rule-base type that you can copy and then update according to your requirements.

```
root@vsrx> request security idp security-package install policy-templates
```

```
node0:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

```
node1:
```

```
-----
Will be processed in async mode. Check the status using the status checking
CLI
```

14. Check the status of install

```
root@vsrx> request security idp security-package install status
```

```
Done;policy-templates has been successfully updated into internal repository  
(=>/var/run/scripts/commit/templates.xsl)!
```

15. Check the version of security package

```
root@vsrx> show security idp security-package-version
```

```
Attack database version:3180(Thu Jun 13 11:55:28 2019 UTC)  
Detector version :12.6.130190309  
Policy template version :3180
```

At this stage vSRX is IDP ready, specific IDP policy needs to be configured to analyze traffic for signs of possible incidents, violations, or imminent threats. See Appendix for sample IDP policy configuration.

Monitoring IDP Policies

```
root@vsrx> show security policies policy-name <policy-name> detail
```

```
root@vsrx> show security idp status
```

```
root@vsrx> show security idp counters
```

```
root@vsrx> show security idp memory
```

Appendix

IDP Recommended Policy Configuration

```
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match from-zone SL-PUBLIC
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match source-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match to-zone SL-PRIVATE
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match destination-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match application default
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match attacks predefined-attack-
groups "[Recommended]IP-Critical"
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match attacks predefined-attack-
groups "[Recommended]IP-Minor"
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match attacks predefined-attack-
groups "[Recommended]IP-Major"
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match attacks predefined-attack-
groups "[Recommended]TCP-Minor"
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 match attacks predefined-attack-
groups "[Recommended]TCP-Major"
set security idp idp-policy RECOMMENDED rulebase-ips rule 1 then action recommended
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match from-zone SL-PUBLIC
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match source-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match to-zone SL-PRIVATE
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match destination-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match application default
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match attacks predefined-attack-
groups "[Recommended]ICMP-Major"
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 match attacks predefined-attack-
groups "[Recommended]ICMP-Minor"
set security idp idp-policy RECOMMENDED rulebase-ips rule 2 then action recommended
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match from-zone SL-PUBLIC
```

```
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match source-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match to-zone SL-PRIVATE
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match destination-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match application default
set security idp idp-policy RECOMMENDED rulebase-ips rule 3 match attacks predefined-attack-
groups "[Recommended]Minor - SNMP"

set security idp idp-policy RECOMMENDED rulebase-ips rule 3 then action recommended

set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match from-zone SL-PUBLIC
set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match source-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match to-zone SL-PRIVATE
set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match destination-address any
set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match application default
set security idp idp-policy RECOMMENDED rulebase-ips rule 4 match attacks predefined-attack-
groups "[Recommended]UDP - All"

set security idp idp-policy RECOMMENDED rulebase-ips rule 4 then action recommended
```

```
idp-policy RECOMMENDED {
  rulebase-ips {
    rule 1 {
      match {
        from-zone SL-PUBLIC;
        source-address any;
        to-zone SL-PRIVATE;
        destination-address any;
        application default;
        attacks {
          predefined-attack-groups [ "[Recommended]IP-Critical"
"[Recommended]IP-Minor" "[Recommended]IP-Major" "[Recommended]TCP-Minor" "[Recommended]TCP-Major"
];
        }
      }
      then {
        action {
          recommended;
        }
      }
    }
    rule 2 {
      match {
        from-zone SL-PUBLIC;
        source-address any;
        to-zone SL-PRIVATE;
        destination-address any;
        application default;
        attacks {
          predefined-attack-groups [ "[Recommended]ICMP-Major"
"[Recommended]ICMP-Minor" ];
        }
      }
      then {
        action {
          recommended;
        }
      }
    }
  }
}
```


FAQ

- **What is signature database**

The signature database is one of the major components of Intrusion Detection and Prevention (IDP). It contains definitions of different objects, such as attack objects, application signatures objects, and service objects—that are used in defining IDP policy rules.

- **Where is Juniper's IDP signature database hosted**

IDP Signature database is hosted in Public cloud.

- **How often are the Signature database updated?**

Juniper has a dedicated team for Signatures and Publishes update to its signature database approximately once in every 2 weeks.

- **How is Standalone deployment different from HA deployment?**

Download and installation of security packages for Standalone and HA is similar.

For HA deployment, license must be applied on both the nodes of cluster. Downloading IDP Security package and installation is performed on primary node only.

- **Can the signature be auto updated?**

Yes, auto update can be performed for deployment which has internet access. Please refer to the below link

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-signature-database.html#id-example-updating-the-signature-database-automatically

- **What goes in new signature database update?**

As a response to new vulnerabilities, Juniper Networks periodically provides a file containing attack database updates on the Juniper website. You can download this file to protect your network from new threats.

- **How can I search the signature database?**

You can use our searchable database of IPS signatures and Application signatures to help protect your environment. These signature pages will give you visibility into the vulnerabilities covered, their CVE numbers, their CVSS scores and our recommendation for deployment.

<https://threatlabs.juniper.net/home/search/#/list/ips>

- **How can I get started with IPS using J-Web?**

Check the following YouTube videos where Juniper guides you step by step on how to set up IPS.

Installing IPS Signatures with J-Web

https://www.youtube.com/watch?v=vplzNsA5h-U&feature=emb_title

Using IPS Templates with J-Web

https://www.youtube.com/watch?v=lnOn9RE9rBo&feature=emb_title

To learn more about Intrusion Detection and Prevention [Click here](#) to download the User Guide or visit the Juniper documentation site at https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-overview.html