Engineering
Simplicity

Day One+

Juniper Cloud Workload Protection

IN THIS GUIDE

Step 1: Begin

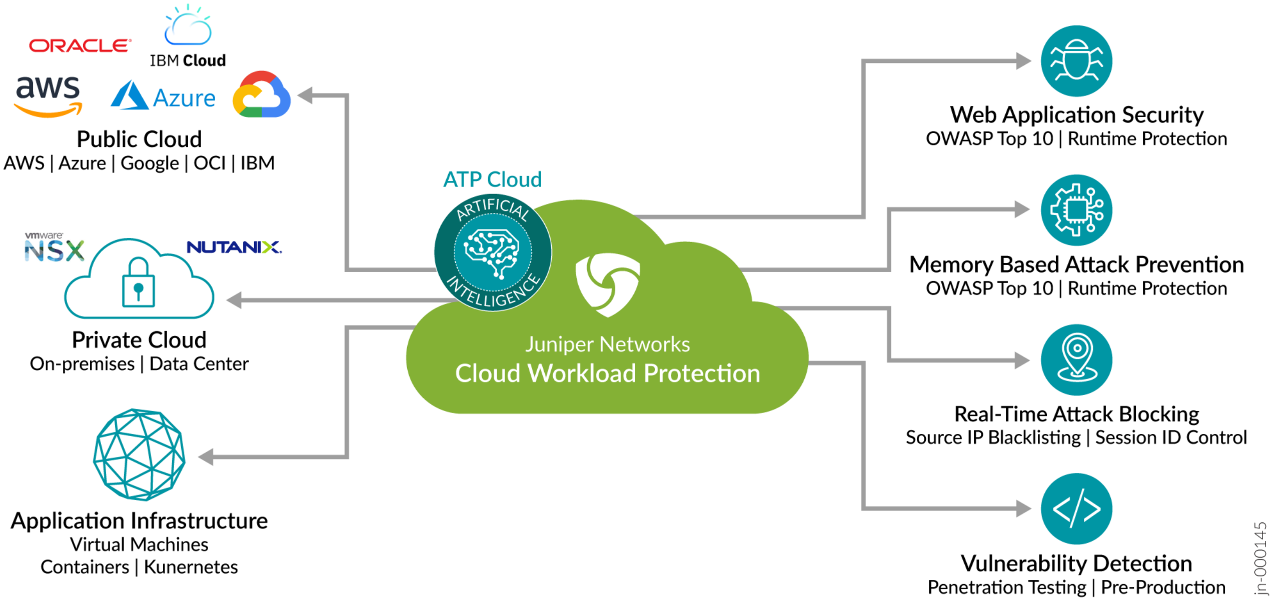
IN THIS SECTION

In this guide, we provide a simple, three-step path to quickly set up Juniper Cloud Workload Protection. Once Juniper Cloud Workload Protection is up and running, you'll learn how to enable runtime protection to protect your application workload.

Meet Juniper Cloud Workload Protection

Juniper Cloud Workload Protection provides visibility and security controls across your cloud infrastructure and applications using a single console. It automatically defends application workloads in any cloud or on-premises environment against attempts to exploit application vulnerabilities and zero day exploits. Whether applications are in production or pre-production, Juniper Cloud Workload Protection provides an effective defense to stop active exploits in their tracks as well as find vulnerabilities before they become liabilities.

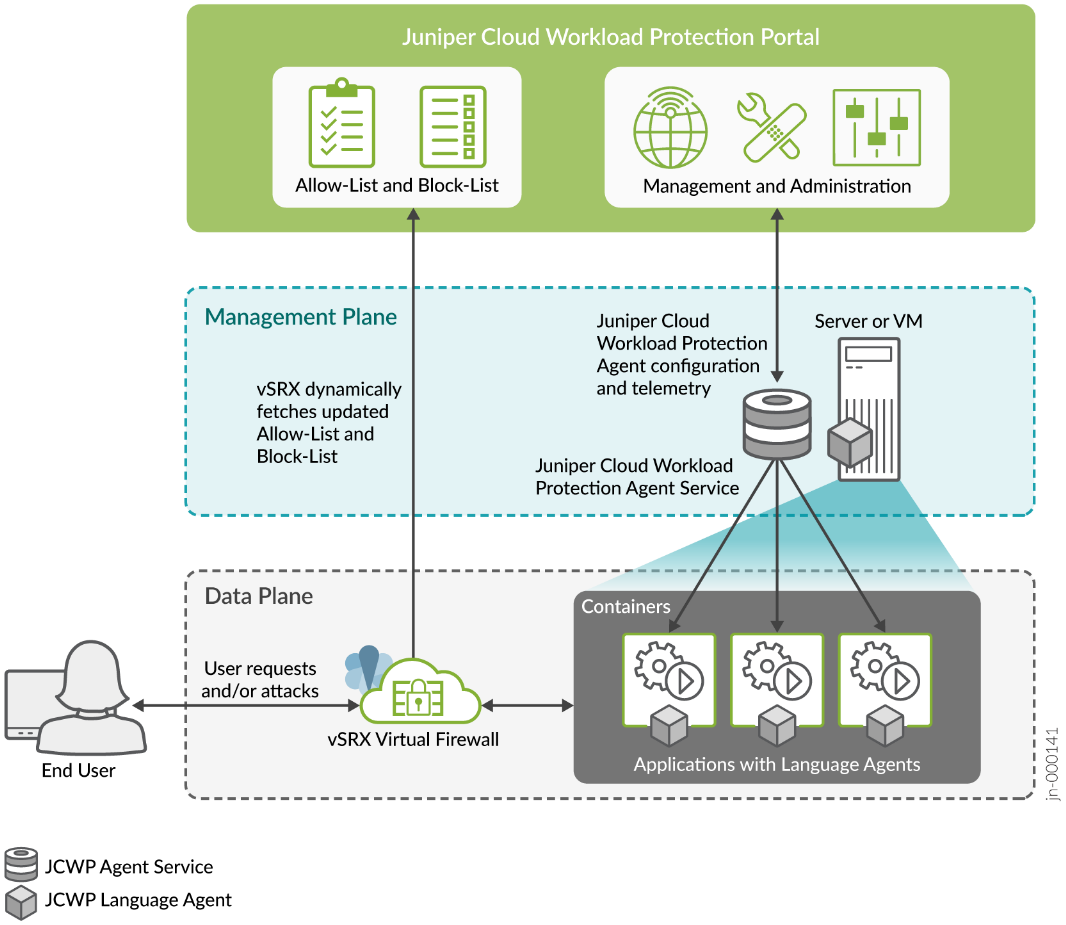
You can deploy Juniper Cloud Workload Protection in public cloud, on-premises, or in hybrid environments to protect web applications, containerized workloads, and Kubernetes. This ensures that production applications always have a safety net against exploits, keeping business-critical services connected and resilient no matter where they are.


ORACLE
IBM Cloud
aws
Azure
Public Cloud
AWS | Azure | Google | OCI | IBM
vmware NSX
NUTANIX
Private Cloud
On-premises | Data Center
Application Infrastructure
Virtual Machines
Containers | Kunernetes
ATP Cloud
ARTIFICIAL INTELLIGENCE
Juniper Networks
Cloud Workload Protection
Web Application Security
OWASP Top 10 | Runtime Protection
Memory Based Attack Prevention
OWASP Top 10 | Runtime Protection
Real-Time Attack Blocking
Source IP Blacklisting | Session ID Control
Vulnerability Detection
Penetration Testing | Pre-Production
jn-000145

Here are the key components of Juniper Cloud Workload Protection:

- Juniper Cloud Workload Protection portal: Available as Software as a Service (SaaS). You can access the portal to manage attacks, vulnerabilities, applications, containers, reports, policies, accounts and so on.

- Juniper Cloud Workload Protection agent: Available as downloadable agents to provide runtime application self-protection (RASP) or interactive application security testing (IAST) to your applications. You can deploy the agent in your environment to secure your hosts (VMs, containers, and serverless functions) on the cloud or on-premises deployments.


Juniper Cloud Workload Protection Portal
Allow-List and Block-List
Management and Administration
Management Plane
vSRX dynamically fetches updated Allow-List and Block-List
Juniper Cloud Workload Protection Agent configuration and telemetry
Server or VM
Juniper Cloud Workload Protection Agent Service
Data Plane
Containers
User requests and/or attacks
vSRX Virtual Firewall
End User
Applications with Language Agents
jn-000141
JCWP Agent Service
JCWP Language Agent

Juniper Cloud Workload Protection agent service runs in a separate container and communicates with the Juniper Cloud Workload Protection portal to receive policies and report activities. When you launch a server/VM/container/ application, the Juniper Cloud Workload Protection agents apply the policy to provide protection. A vSRX instance placed between the Internet and the protected applications receives dynamic-address feeds from the portal to block attackers.

Get Ready

In this example, you'll need the following resources to setup and use Juniper Cloud Workload Protection:

- A valid Juniper Cloud Workload Protection license
- Linux OS- Ubuntu 18.04
- Docker Engine- 18.09.1 or later versions
- Hardware requirements:
  - Juniper Cloud Workload Protection agents (RASP mode)—Linux machine with 500 MB to 2 GB RAM, two vCPUs, and a (minimum) 5 GB hard drive

  - Juniper Cloud Workload Protection agents (IAST mode)—Linux machine with 2 GB to 8 GB RAM (depending on the load), two vCPUs, and a (minimum) 5 GB hard drive

  For additional options supported, see "Software and Hardware Requirements" on page 18 for details.

- vSRX instance with Junos OS Release 19.4R1 or later

- Juniper Cloud Workload Protection agent and vSRX needs to connect to https://juniper.k2io.net/ on ports 80 and 443.

Activate Your Juniper Networks Cloud Workload Protection License

First things, first. You'll need to get a valid license before you can using start using your Juniper Cloud Workload protection.

Use the following instructions to obtain the appropriate license key for your Juniper Networks Cloud Workload Protection.

1. Create a user account with Juniper Networks. To access Juniper Cloud Workload Protection, you need an approved user account with Juniper Networks. If you don't already have one, create an account through the User Registration Portal.

   Once you create a Juniper Networks user account, it might take a couple of hours to get the compliance approval Retrieve your software serial number.

2. Retrieve your software serial number. The software serial number is a unique 14-digit number that Juniper Networks uses to identify your Juniper Networks software installation (or purchased capacity). You can find this number in the software serial number certificate attached to the email sent when you ordered your Juniper Networks service. Store the software serial number in a safe place as you might need it to identify your installation when contacting Juniper Networks for support.

3. Request your licensed software.

   Open an admin service request (case) using our Service Request Manager on the Juniper Customer Support Center (CSC) and enter the following information. Or call Customer Care.

   - Subject Line: Juniper Cloud Workload Protection Software Request

   - Description:

     - Sales order number

     - Software product SKU

     - Serial Number/SSRN (software serial number in your license fulfillment email). If available, attach the software serial number certificate (PDF) to the admin service request.

     - Email address for the primary admin account. This email address can be the same as the Juniper user account or a different email address. Ensure that the incoming email from outside your organization is allowed.

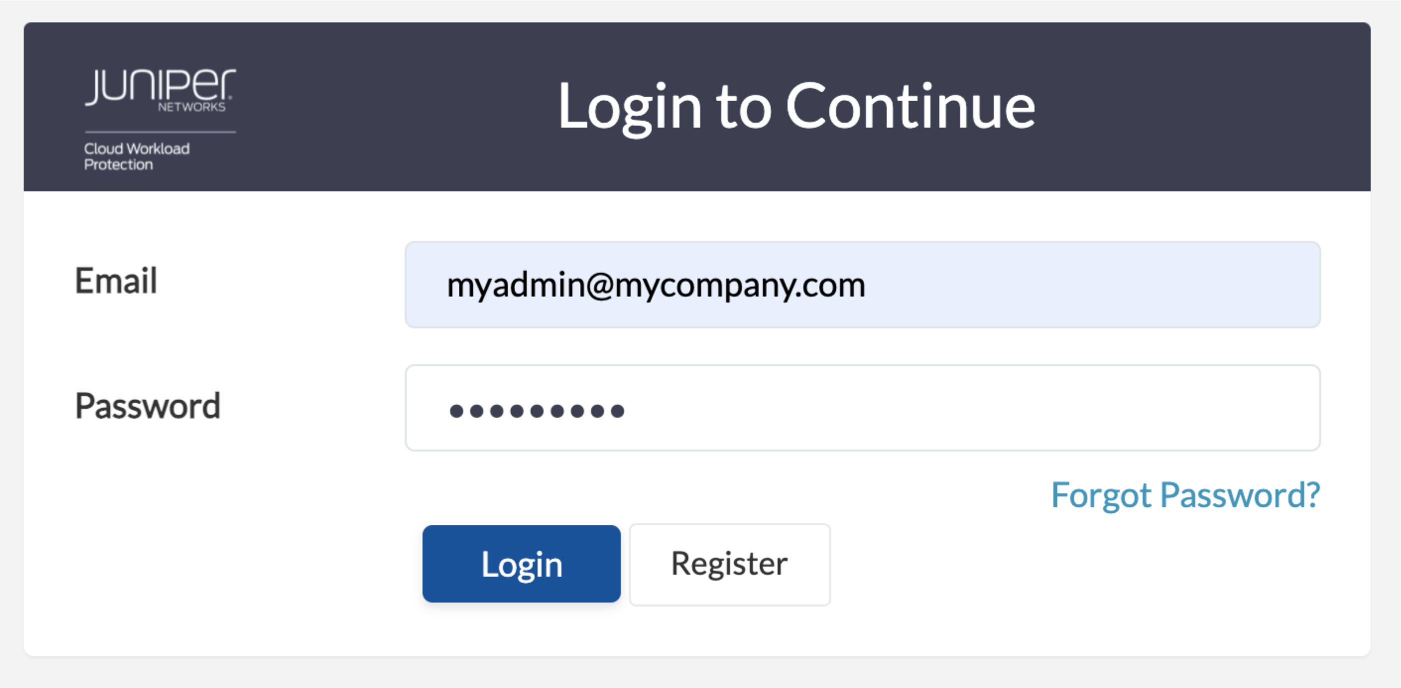
Temporary log in details are emailed automatically once your account is set up. Once your service request is processed, you'll receive an email with your account information. Your product is automatically licensed.

Access Juniper Cloud Workload Protection Portal

Here's how to access Juniper Cloud Workload Protection portal:

1. Go to Juniper Cloud Workload Protection.

2. Enter your log in details. Use the log in information you received in the email to sign into your account for the first time.



Email myadmin@mycompany.com

Password ●●●●●●●●●

Click **Login** to continue. Upon successful authentication, you'll be directed to the Juniper Cloud Workload Protection dashboard.

Next, let's install the required Juniper Cloud Workload Protection agents.

Step 2: Up and Running

IN THIS SECTION

Juniper Cloud Workload Protection agents inspect your web applications at runtime to automatically detect known and unknown vulnerabilities. In this section, we show you how to install agents, protect your web applications, view attacks, and remediate vulnerabilities in your test environment or block attacks in your production environment.

Install Juniper Cloud Workload Protection Agents

IN THIS SECTION

You can install Juniper Cloud Workload Protection agents in two separate environments:

- For applications in pre-production or development phase, use Juniper Cloud Workload Protection agents for interactive application security testing (IAST) to find vulnerabilities during the development phase. IAST scans the network for vulnerabilities, and detects and reports exploits. IAST works with third-party code and custom code to pinpoint the location of the vulnerable code at every stage.

- For applications in the production phase, use Juniper Cloud Workload Protection agents for runtime protection. Realtime attack protection detects and reports active exploits against your application without using a signature. You can automatically block attacks to secure your applications without additional software updates or manual intervention.

Install Juniper Cloud Workload Protection Agents for Vulnerability Detection

Juniper Cloud Workload Protection agents integrate with your CI/CD pipeline to find vulnerabilities. The agents provide information on the vulnerability, how it could be exploited, and how to fix it in your applications. This helps developers understand the severity of a vulnerability as well as how to remediate it at the source.

Here's how to install vulnerability detection agents on node/VM/EC2 in Docker environment:

1. Log in to the Juniper Cloud Workload Protection portal.

2. Navigate to **Installation**.

3. Select the **VM/Node Installation** option.

4. Set the following options:

   - Version: Select the latest available version (1.10.23).

   - Installation mode: **Docker**.

   - Policy Group Name: **IAST**.

   Be sure you use the proper settings for these parameters as they determine which agent installation files are downloaded.

5. Follow the instructions on the screen and download the zip file for VM installation on your Docker host.

6. Unzip the downloaded file on your host.

```
unzip vm-all.zip
```

7. Navigate to the extracted **k2install** directory.

```
cd k2install
```

8. Install the Juniper Cloud Workload Protection agents. In this example, we'll use the `prevent-web` option (default option).

```
bash k2install.sh -i prevent-web
```

9. Verify that the `prevent-web` agent is running on the host system.

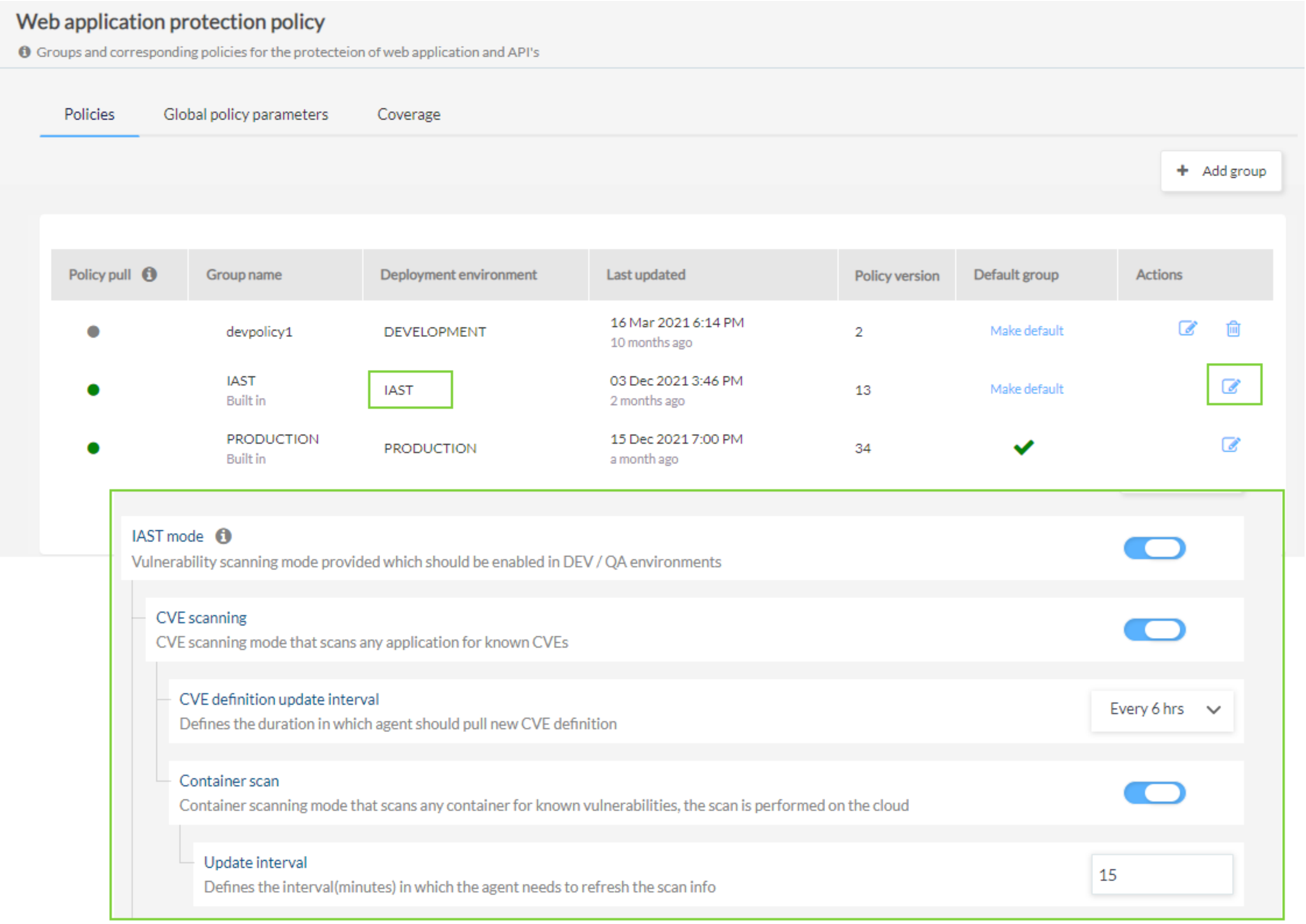
```
$ docker ps | grep -w "k2agent"
c77da5d434c5 k2cyber/k2-agent-v1:1.10.23 "/bin/bash -c '/usr/…" 3 minutes ago Up 3 minutes k2agent"
```

10. Click **Finish** to return to the main menu.

After you run the script, Juniper Cloud Workload Protection creates a policy.

To view the IAST policy, navigate to **Policy** > **Web applications** > **Policies** in the Juniper Cloud Workload Protection portal.

Select the **IAST** deployment environment and click the Edit/show policies actions icon to see policy details.



Web application protection policy

Groups and corresponding policies for the protecteion of web application and API's

Policy pull	Group name	Deployment environment	Last updated	Policy version	Default group	Actions
●	devpolicy1	DEVELOPMENT	16 Mar 2021 6:14 PM 10 months ago	2	Make default	
●	IAST Built in	IAST	03 Dec 2021 3:46 PM 2 months ago	13	Make default	
●	PRODUCTION Built in	PRODUCTION	15 Dec 2021 7:00 PM a month ago	34	✓	

IAST mode
Vulnerability scanning mode provided which should be enabled in DEV / QA environments

CVE scanning
CVE scanning mode that scans any application for known CVEs

CVE definition update interval
Defines the duration in which agent should pull new CVE definition
Every 6 hrs

Container scan
Container scanning mode that scans any container for known vulnerabilities, the scan is performed on the cloud

Update interval
Defines the interval(minutes) in which the agent needs to refresh the scan info
15

Install Juniper Cloud Workload Protection Agents for Runtime Protection

Here's how to install Juniper Cloud Workload Protection agents on Node/VM/EC2 in a Docker container:

1. Log in to the Juniper Cloud Workload Protection portal.
2. Navigate to **Installation**.
3. Select the **VM/Node Installation** option.
4. Set the following options:
   - Version: Select the latest available version (1.10.23).

- Installation mode: **Docker**.
- Policy Group Name: **PRODUCTION**.

Be sure you use the proper settings for these parameters as they determine which agent installation files are downloaded.

5. Follow the instructions on the screen and download the zip file for VM installation on your Docker host.

6. Unzip the downloaded file on your host.

```
unzip vm-all.zip
```

7. Navigate to the extracted **k2install** directory.

```
cd k2install
```

8. Install the Juniper Cloud Workload Protection agents. In this example, we'll use the `prevent-web` option (default option).

```
bash k2install.sh -i prevent-web
```

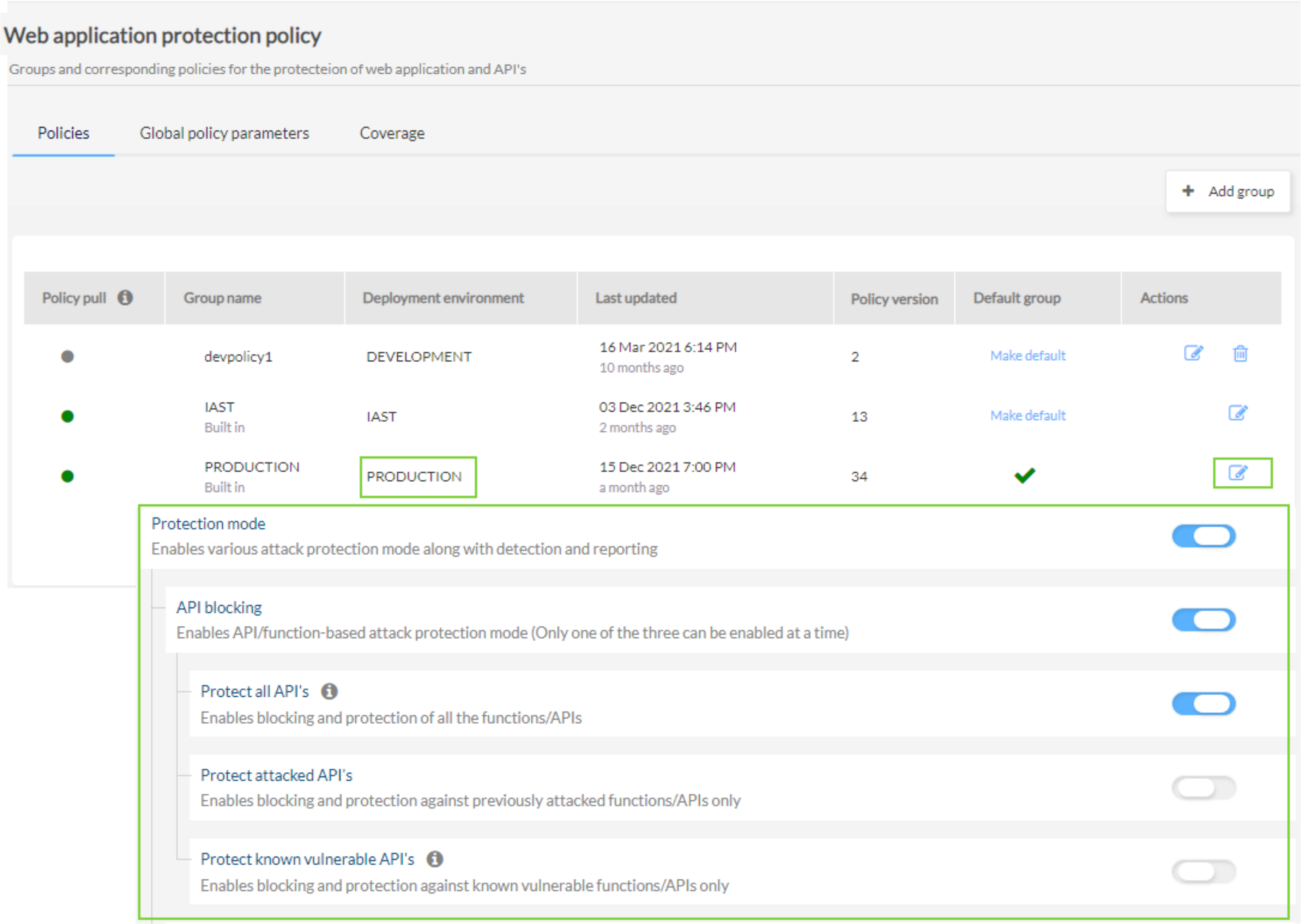
9. Verify that the `prevent-web` agent is running on the host system.

```
$ docker ps | grep -w "k2agent"
c77da5d434c5 k2cyber/k2-agent-v1:1.10.23 "/bin/bash -c '/usr/…" 3 minutes ago Up 3 minutes k2agent"
```

10. Click **Finish** to return to the main menu.

To view the production policy, navigate to **Policy** > **Web applications** > **Policies** in the Juniper Cloud Workload Protection portal.

Select the **PRODUCTION** deployment environment and click the Edit/show policies actions icon to see policy details.



Web application protection policy

Groups and corresponding policies for the protecteion of web application and API's

Policies | Global policy parameters | Coverage

+ Add group

Policy pull	Group name	Deployment environment	Last updated	Policy version	Default group	Actions
●	devpolicy1	DEVELOPMENT	16 Mar 2021 6:14 PM 10 months ago	2	Make default	
●	IAST Built in	IAST	03 Dec 2021 3:46 PM 2 months ago	13	Make default	
●	PRODUCTION Built in	PRODUCTION	15 Dec 2021 7:00 PM a month ago	34	✓	

Protection mode: On
Enables various attack protection mode along with detection and reporting

API blocking: On
Enables API/function-based attack protection mode (Only one of the three can be enabled at a time)

Protect all API's: On
Enables blocking and protection of all the functions/APIs

Protect attacked API's: Off
Enables blocking and protection against previously attacked functions/APIs only

Protect known vulnerable API's: Off
Enables blocking and protection against known vulnerable functions/APIs only

Now you're ready to launch your applications with a language agent to protect your web applications and API.

Protect Web Applications and APIs

Juniper Cloud Workload Protection uses:

- RASP mode to stop hackers' attempts to compromise web applications and data
- IAST mode to identify and manage security risks associated with vulnerabilities discovered in running web applications.

To enable RASP mode or IAST mode, you'll need to launch your application with a Juniper Cloud Workload Protection agent communication language on both servers you used for applications in pre-production (IAST) and applications in production (RASP).

Select type such as Java, Node.js, PHP, or Ruby and follow the instructions on the screen to attach the language agent.

Here's how to install and attach a Java Language Agent with your Java application hosted on your virtual machine. You can also select other environments such as Kubernetes, AWS ECS, AWS Fargate, and Windows.

1. Locate the Java ACL in one of the following locations (LANGUAGE_COLLECTORS_HOME):

- For root-user: **/opt/k2-ic**
- For non-root users: **${HOME}/k2-ic** where **${HOME}** points to the home directory of the Linux user.
- For a shareable-directory **[sharable-directory]/k2-ic**. The shareable-directory is available in the **env.properties** file when you install the agent.

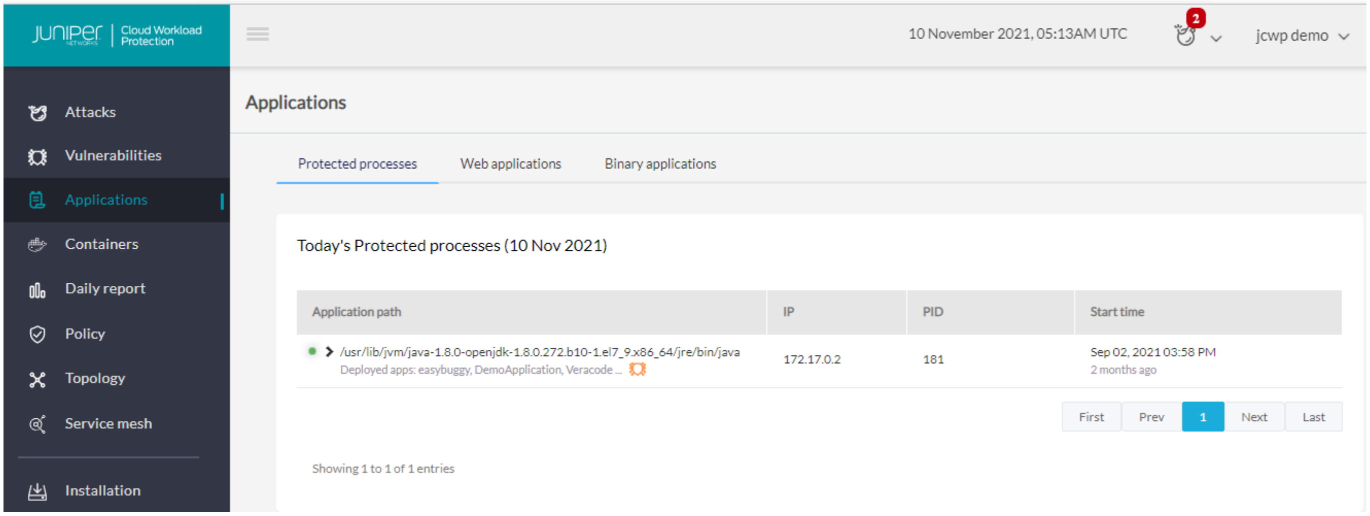
For any containerized Java web application (Docker/K8s), the host path LANGUAGE_COLLECTORS_HOME is available at **/opt/k2-ic** inside the container with option `z`.

2. Attach the Java ACL to the Java application by adding the following command to JVM arguments.

```
-javaagent:/opt/k2-ic/K2-JavaAgent-1.0.0-jar-with-dependencies.jar
```

If you're using Java 9 or above, add the **java.sql** module to your environment file by adding a JVM argument (`--add-modules java.sql`) to your application startup script.

3. Verify that the application is protected. In the Juniper Cloud Workload Protection portal, navigate to **Applications** on the left-side navigation bar and click the **Protected processes** tab.



Today's Protected processes (10 Nov 2021)

Application path	IP	PID	Start time
/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.272.b10-1.el7_9.x86_64/jre/bin/java Deployed apps: easybuggy, DemoApplication, Veracode ...	172.17.0.2	181	Sep 02, 2021 03:58 PM 2 months ago

Showing 1 to 1 of 1 entries

Click the down arrow symbol next to the application path to view details for the protected application. You can identify protected applications by their host name or container name. The details confirm that your application is successfully registered and protected with Juniper Cloud Workload Protection.

Run the Sample Exploits Script

To verify that your configuration is working, run a sample test. We've provided a script in the **\k2install\demo_scripts\** installation folder on your host.

Run the **run_script.sh** script to generate exploitable vulnerabilities. When you run the script, the script launches the application in your environment and subsequently launches the attack. Juniper Cloud Workload Protection immediately detects these attacks, so that you can verify everything is working properly.

You can run this script across Java, Node.JSand NGINX web server, all running as docker containers.

Use one of the following commands to run an exploit applicable to your setup:

```
bash run_script.sh sql-injection JAVA
bash run_script.sh verademo JAVA
bash run_script.sh forkexec JAVA
bash run_script.sh struts-cve-2017-5638 JAVA
bash run_script.sh easybuggy JAVA
bash run_script.sh spiracle JAVA
bash run_script.sh java-sec-code JAVA
bash run_script.sh tomcat-cve-2017-12617 JAVA
bash run_script.sh nginx BINARY
bash run_script.sh dnsmasq BINARY
bash run_script.sh node-demo-app sqli NODE.JS
bash run_script.sh node-demo-app rce NODE.JS
bash run_script.sh node-demo-app rci NODE.JS
bash run_script.sh node-demo-app ssrf NODE.JS
bash run_script.sh node-demo-app file-access NODE.JS"
bash run_script.sh node-demo-app nosqli NODE.JS
```

The script fetches the relevant Docker container from the Internet, launches it on some local ports (8091 or 9090 by default) and returns the following message:

```
APPLICATION SETUP IS READY FOR ATTACK!
```

Press any key to continue. The script launches a local attack from the container, and displays one of the following messages:

- If you're running the script for a pre-production server (IAST), then the script returns the following message:

  ```
  ATTACK SUCCESSFUL
  ```

  Juniper Cloud Workload Protection detects the attack but does not block it.

- If you're running the script for a production server (RASP), then the script returns the following message:

  ```
  K2 has detected an attack !
  ```

  Juniper Cloud Workload Protection portal also reports detected and blocked attacks. You can see the detected attacks in the Juniper Cloud Workload Protection portal under the **Attacks** tab.

Runtime Protection through vSRX Virtual Firewall

You can setup runtime protection through a vSRX virtual firewall to efficiently block intruders with Juniper Cloud Workload Protection. As a first step, you'll need to integrate your vSRX instance with Juniper Cloud Workload Protection.

Juniper Cloud Workload Protection identifies threat sources by their IP address, and groups those addresses into a dynamic-address group in two separate feeds: one feed for allowed IP addresses, and one feed for blocked IP addresses (attacker's IP addresses). The vSRX instance uses these two feeds to create dynamic address entries in security policies to prevent intruders from accessing protected resources.

When you integrate a vSRX instance with Juniper Cloud Workload Protection, the portal provides a validated configuration for your vSRX instance. You can copy the configuration to your firewall and then modify it to match your policy configuration.

1. Go to **Settings > Firewall Integration**. The page displays the list of firewalls, feeds, the allowlist and the blocklist.

2. Click **+** on the right side of the page to add a new firewall configuration.

3. Enter the following details in the Firewall Configuration window:

   - **Firewall**: vSRX

   - **SNAT Enabled**: False

   - **Policy configuration**: False. When you select False, Juniper Cloud Workload Protection does not push the configuration to the vSRX instance; it displays a configuration that you can apply on your vSRX instance to adapt to the current environment.

   - **Firewall IP**: IP address of your vSRX instance

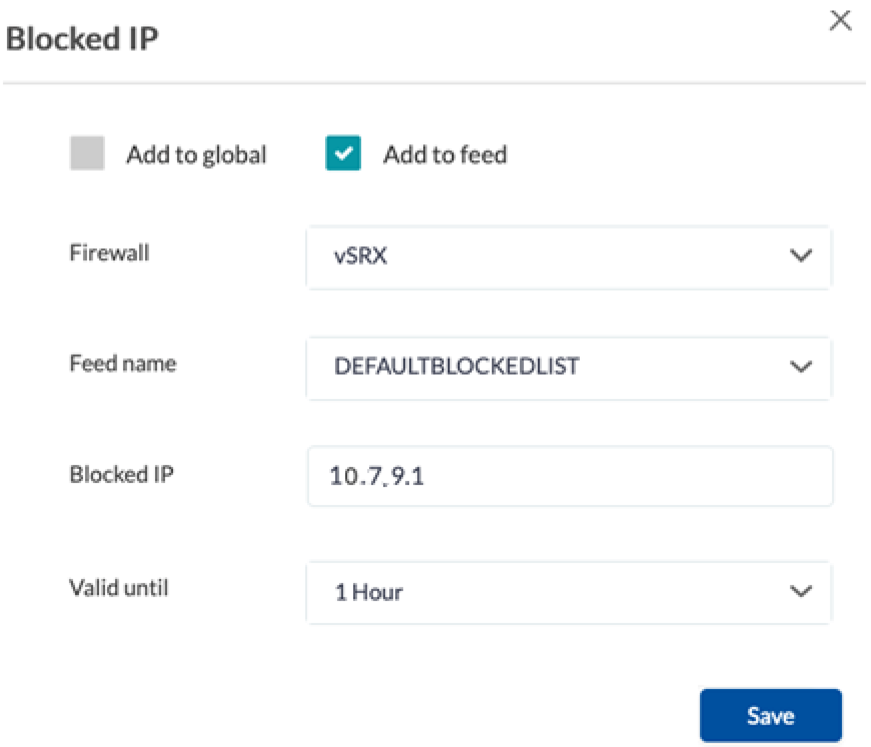
   - **Blocked list feed**: Select the blocked IP address list if you want to block IP addresses manually and automatically. Use the Blocked list tab to create a list of manually blocked IP addresses.

   - **Allowed list feed**: Select the allowed IP address list if you want to allow IP addresses manually and automatically. Use the Allowed list tab to create a list of manually allowed IP addresses.

   - **Update Interval**: Select 30 seconds. This is the time period at which the vSRX collects the information from Juniper Cloud Workload Protection.

4. Enter **Create** to save the details.

5. Select the Blocked list tab and enter the IP addresses you want to block manually. Enter the following details:



Blocked IP

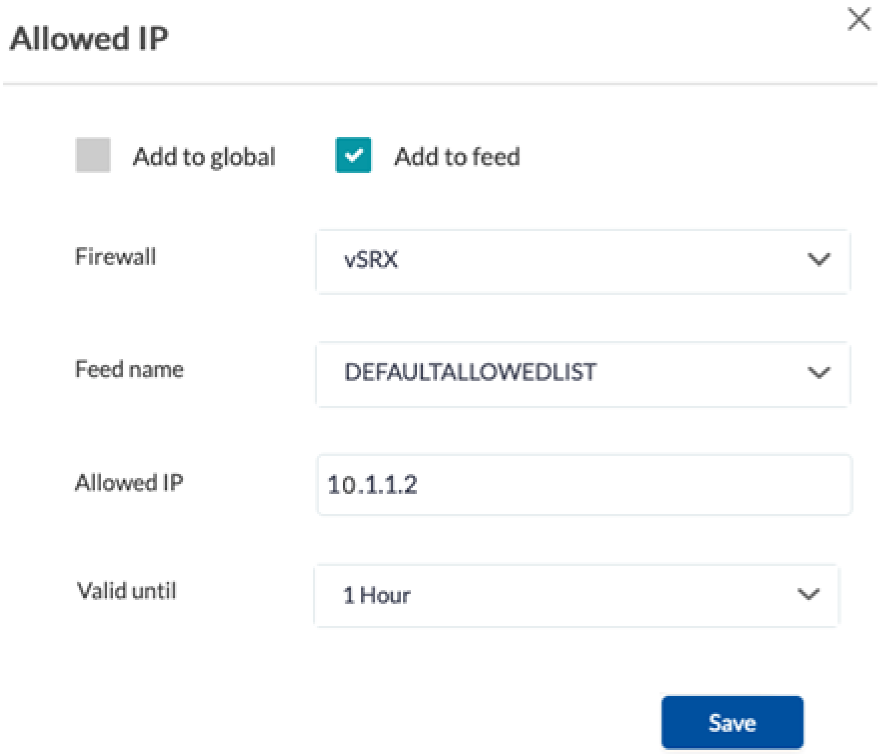
☐ Add to global ☑ Add to feed

Firewall	vSRX
Feed name	DEFAULTBLOCKEDLIST
Blocked IP	10.7.9.1
Valid until	1 Hour

- **Firewall**: Select the type of firewall from the drop-down list.
- **Feed name:** Select the feed name from the list.
- **Blocked IP**: Enter the IP address you want to block.
- **Valid until**: Select the duration for the validity of the blocked IP address.

6. Enter **Save** to save the details. Juniper Cloud Workload Protection adds blocked IP address entries automatically based on RASP detections.

7. Select the Allowed list tab and enter the following details:



Allowed IP

□ Add to global ☑ Add to feed

Firewall: vSRX

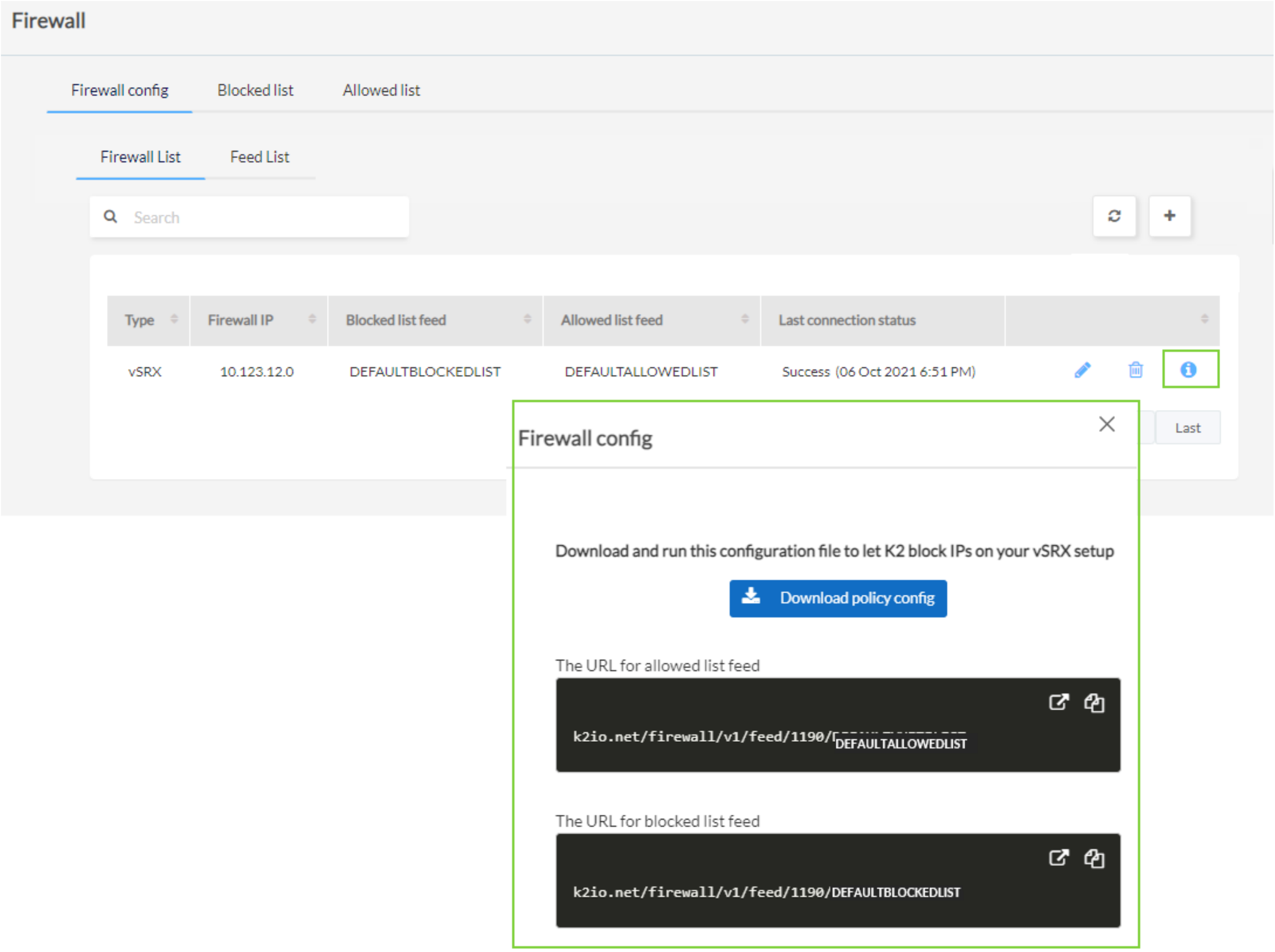
Feed name: DEFAULTALLOWEDLIST

Allowed IP: 10.1.1.2

Valid until: 1 Hour

- **Firewall**: Select the type of firewall from the list.
- **Feed name**: Select the feed name from the list.
- **Allowed IP**: Enter the IP address you want to allow.
- **Valid until**: Select the duration for the validity of the allowed IP address.

8. Enter **Save** to save the details.
9. Click **View configuration**. The Firewall Configuration window shows feed names for allowed and blocked IP address lists.



Type	Firewall IP	Blocked list feed	Allowed list feed	Last connection status
vSRX	10.123.12.0	DEFAULTBLOCKEDLIST	DEFAULTALLOWEDLIST	Success (06 Oct 2021 6:51 PM)

Download and run this configuration file to let K2 block IPs on your vSRX setup

The URL for allowed list feed

```
k2io.net/firewall/v1/feed/1190/DEFAULTALLOWEDLIST
```

The URL for blocked list feed

```
k2io.net/firewall/v1/feed/1190/DEFAULTBLOCKEDLIST
```

10. Click the **Download policy configuration** option to download the configuration template file on your host machine. You'll need to edit the configuration as per your requirements before applying it on your vSRX instance manually.

11. You can also view the details of blocked IP addresses on your vSRX instance. An attack triggers a dynamic-address entry on the vSRX instance. Use the `show security dynamic-address` command to view the dynamic-address entry.

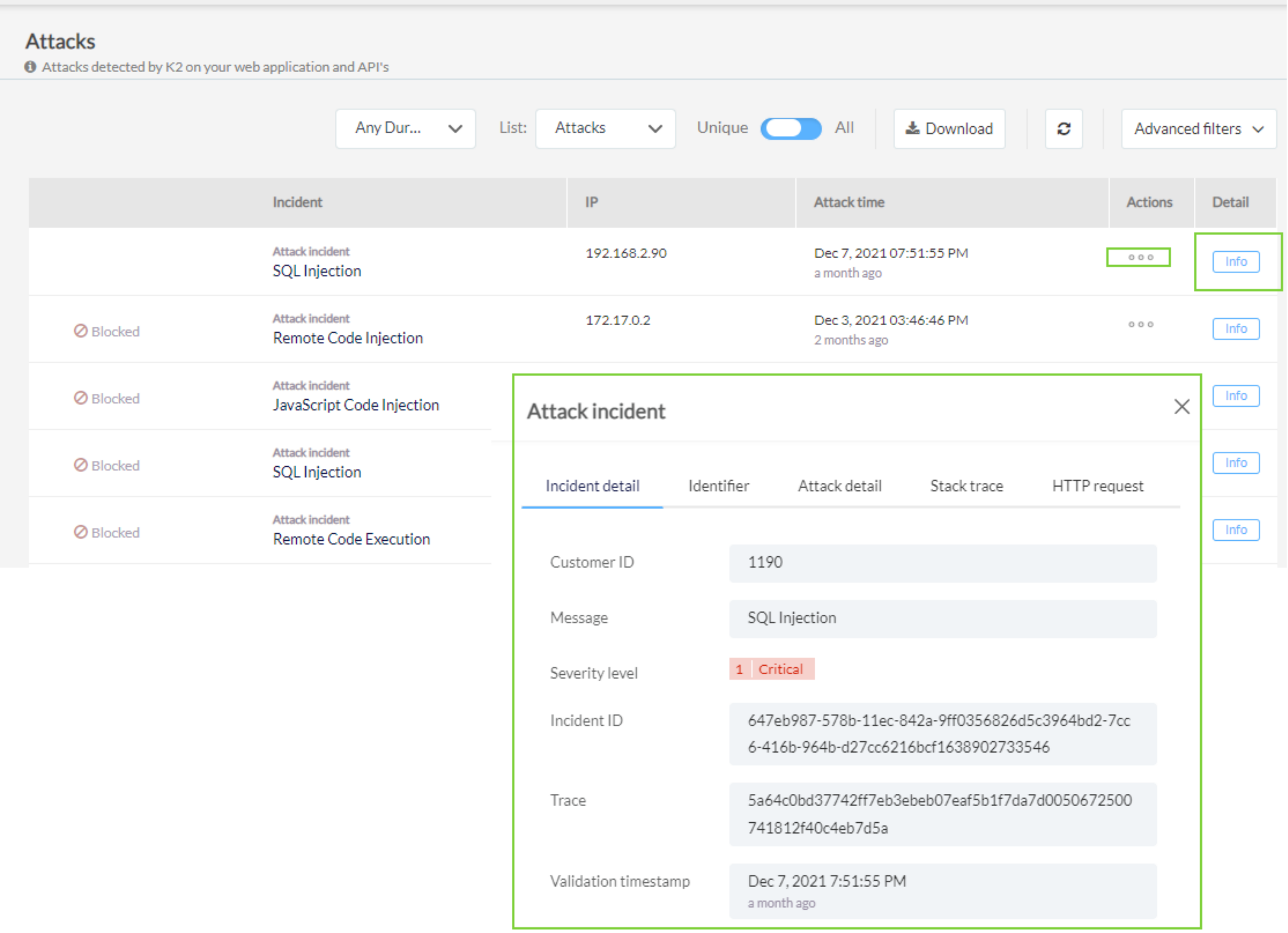
```
user@vSRX-host> show security dynamic-address
No.     IP-start          IP-end            Feed                        Address
1       10.7.9.1          10.7.9.1          DEFAULTALLOWEDLIST          DEFAULTALLOWEDLIST
2       10.1.1.2          10.1.1.2          DEFAULTBLOCKEDLIST          DEFAULTBLOCKEDLIST

Instance default Total number of matching entries: 2
Instance geoip   Total number of matching entries: 0
Instance advanced-anti-malware Total number of matching entries: 0
```

The output shows that the allowed list and the blocked list are added as dynamic-address entries on the vSRX instance. In the output, the existing entries of IP address 10.7.9.1 (allowed list) and 10.1.1.2 (blocked list) are samples.

TIP: You can integrate Juniper Cloud Workload Protection with both physical and virtual SRX Series routers. As a best practice, setup the integration at all connection points within your data center or cloud environment. Integration can include other vSRX instances on non-produced applications such as those that run on bare metal servers, SRX Series firewalls running at the edge or perimeter of your network, and as connectors to other data centers or cloud environments.

View Attacks

You can view the details of attacks that are blocked by Juniper Cloud Workload Protection using the **Attacks** option on navigation bar. The **Attacks** page displays the incident name, IP address of the intruder, attack time, and details of the attack.



Attacks

Attacks detected by K2 on your web application and API's

	Incident	IP	Attack time	Actions	Detail
	Attack incident SQL Injection	192.168.2.90	Dec 7, 2021 07:51:55 PM a month ago	○○○	Info
⊘ Blocked	Attack incident Remote Code Injection	172.17.0.2	Dec 3, 2021 03:46:46 PM 2 months ago	○○○	Info
⊘ Blocked	Attack incident JavaScript Code Injection				Info
⊘ Blocked	Attack incident SQL Injection				Info
⊘ Blocked	Attack incident Remote Code Execution				Info

Attack incident

Customer ID	1190
Message	SQL Injection
Severity level	1 Critical
Incident ID	647eb987-578b-11ec-842a-9ff0356826d5c3964bd2-7cc6-416b-964b-d27cc6216bcf1638902733546
Trace	5a64c0bd37742ff7eb3ebeb07eaf5b1f7da7d0050672500741812f40c4eb7d5a
Validation timestamp	Dec 7, 2021 7:51:55 PM a month ago

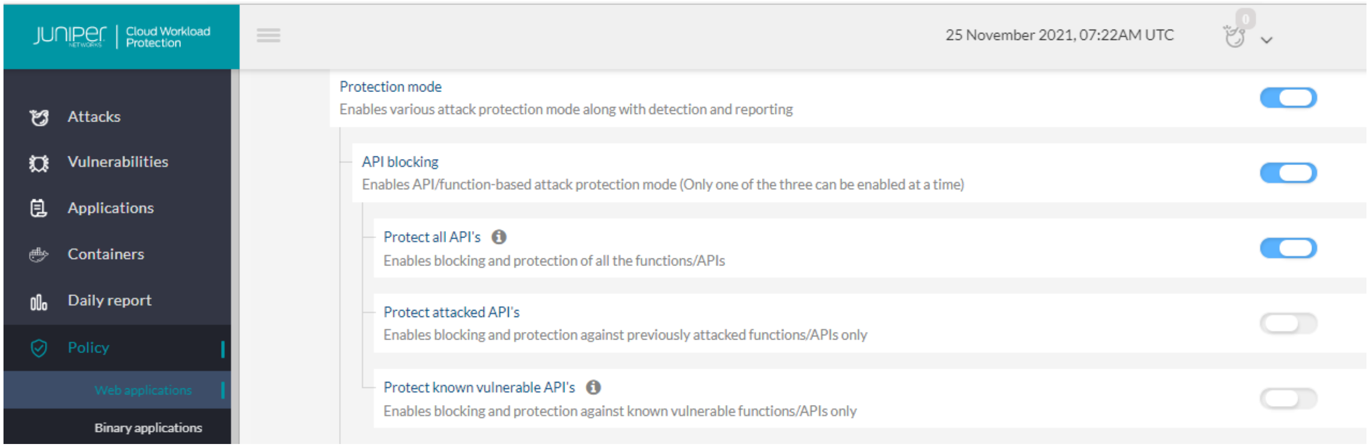
When an attack occurs, the most recent attack appears on the top of the page. Click **Actions** to block the attack or mark as not an attack. Click **Detail** to gather more details on the attack.

Block Malicious API Calls and Intruders' IP Addresses

You can block malicious API calls from attackers and block intruders' IP addresses with Juniper Cloud Workload Protection.

Here's how to configure policies for vulnerability detection and runtime protection:

1. Go to **Policy> Web application**.
2. Click the edit button for your PRODUCTION policy (default policy). You'll see three sections at the top: Agent Config, Agent Policies, and Global Policy Parameters.
3. Click the **Agent Policies** tab. Scroll to the **Protection mode**.



Protection mode
Enables various attack protection mode along with detection and reporting

API blocking
Enables API/function-based attack protection mode (Only one of the three can be enabled at a time)

Protect all API's
Enables blocking and protection of all the functions/APIs

Protect attacked API's
Enables blocking and protection against previously attacked functions/APIs only

Protect known vulnerable API's
Enables blocking and protection against known vulnerable functions/APIs only

4. Enable the following three options to enable attack protection mode along with detection and reporting:
   - Protection Mode
   - API blocking
   - Protect all API's

Now you're all set with Juniper Cloud Workload Protection!

Step 3: Keep Going

IN THIS SECTION

What's Next?

Here are some things you might want to configure next for Juniper Cloud Workload Protection.

If you want to	Then
Find more in-depth information about installing and configuring vSRX Virtual Firewall	See vSRX Documentation
Check out blog posts about Juniper Cloud Workload Protection	See Connecting and Protecting Applications within a Zero Trust Data Center Architecture with Juniper Cloud Workload Protection
Configure Intrusion Detection and Prevention (IDP)	In the *Intrusion Detection and Prevention User Guide*, see IDP Policies
Learn how to configure the IDP SSL Inspection feature on your SRX Series device	In the *Intrusion Detection and Prevention User Guide*, see IDP SSL Inspection
Configure screen options on your SRX Series device	In the *Attack Detection and Prevention User Guide for Security Devices*, see Screens Options for Attack Detection and Prevention

General Information

Here are some excellent resources that will help you take your Juniper Cloud Workload Protection knowledge to the next level:

If you want to	Then
Find product information for Juniper Cloud Workload Protection	See the Juniper Cloud Workload Protection Datasheet
See all documentation available for Juniper Cloud Workload Protection	Check out Product Documentation

Learn With Videos

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS.

If you want to	Then
Learn about how Juniper Cloud Workload Protection and the vSRX work together to defend cloud workload	Watch the Juniper Cloud Workload Protection Demonstration
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies	See Learning with Juniper on Juniper Networks main YouTube page
View a list of the many free technical trainings we offer at Juniper	Visit the Getting Started page on the Juniper Learning Portal

Additional Information

Juniper Cloud Workload Protection supports following software and hardware system requirements.

Supported Linux OS Versions

Operating Systems	Version
Ubuntu	• 16.04 • 18.04 • 19.04 • 20.04

(Continued)

Operating Systems	Version
CentOS	• 7 4. • 7.2.1511 • 7.3.1611 • 7.4.1708 • 7.5.1804 • 7.6.1810
RHEL	• 7.6 • 7.7 • 7.8 • 8.1
Fedora	• 27 • 28 • 29 • 30

Container Support

Juniper Cloud Workload Protection works with bare metal, VMs, with or without containers, and with Kubernetes.

Docker

Docker versions 18.06 and above are supported.

Language Support- Java Builds

JDK Build	JDK Version	Static Attachment	Dynamic Attachment
Oracle JDK	1.8.0.222	Yes	Yes

(Continued)

JDK Build	JDK Version	Static Attachment	Dynamic Attachment
OpenJDK	1.8.0.222	Yes	Yes
Adopt OpenJDK	1.8.0.222	Yes	Yes
RedHat OpenJDK	1.8.0.222	Yes	Yes
Azul Zulu	1.8.0_222-b10	Yes	Yes
Amazon Corretto	8.222.10.1	Yes	Yes
IBM	1.8.0_211	Yes	Yes

Java Versions

Java Version (Runtime Environment) Application Build	Java 8	Java 9	Java 10	Java 11	Java 12
Java 8	Yes	Yes	Yes	Yes	Yes
Java 9	-	Yes	Yes	Yes	Yes
Java 10	-	-	Yes	Yes	Yes
Java 11	-	-	-	Yes	Yes
Java 12	-	-	-	-	Yes

Servers

Server	Supported Versions
Tomcat	• Tomcat 7 (7.0.6, 7.0.12, 7.0.19, 7.0.23, 7.0.42, 7.0.55, 7.0.76, 7.0.9) • Tomcat 8.5 (8.5.4, 8.5.9, 8.5.11, 8.5.27, 8.5.38, 8.5.41) • Tomcat 9 (9.0.1, 9.0.2, 9.0.4, 9.0.6, 9.0.7, 9.0.8, 9.0.10, 9.0.12, 9.0.13, 9.0.14, 9.0.20)
Jetty	• Jetty 9.2 (9.2.28, 9.2.22, 9.2.14, 9.2.11, 9.2.10, 9.2.3, 9.2.0) • Jetty 9.3 (9.3.27, 9.3.25, 9.3.20, 9.3.14, 9.3.11, 9.3.8, 9.3.0) • Jetty 9.4 (9.4.18, 9.4.14, 9.4.12, 9.4.11, 9.4.8, 9.4.6, 9.4.0)
IBM WebSphere Liberty	19.0.0.9 19.0.0.8 19.0.0.7 19.0.0.6 19.0.0.5 19.0.0.4 19.0.0.3
IBM WebSphere Traditional	8.5.5.1
Weblogic	• 12.1.3.0.0, 12.2.1.0.0, 12.2.1.1.0, 12.2.1.2.0, 12.2.1.3.0 (On Host) • 12.2.1.3, 12.1.3 (On Docker)
JBoss	Wildfly: 17.0.1.Final, 17.0.0.Final, 16.0.0.Final, 15.0.1.Final, 15.0.0.Final, 14.0.1.Final, 14.0.0.Final, 13.0.0.Final,12.0.0.Final, 10.1.0.Final, 10.0.0.Final, 9.0.2.Final, 9.0.1.Final, 8.2.1.Final, 9.0.0.Final, 8.2.0.Final, 8.1.0.Final Jboss EAP: eap-7.2.0, eap-7.1.0, eap-7.0.0
Adobe Experience Manager (AEM)	6.5

Frameworks

- JSP servlet
- Struts
- Struts2
- Spring Boot
- Spring MVC

Databases

- MySQL: 5.6, 5.7, 8.0
- MongoDb: 3.2.22, 3.4.24, 3.617, 4.0.17, 4.2.5
- MSSQL MS SQL 2017 server
- Oracle: 18c, 12c, 11g
- PostgreSQL: 8, 9, 10, 11
- HSQL: 1.8.0.10, 2.3.4

Node.js

- Operating System: Ubuntu, CentOS
- Databases: Mysql, PostgreSQL, Oracle, MongoDB, SQLite
- Servers/versions: NODE 8.x to Node 14.x (all version in active and maintenance LTS status)
- Frameworks: express 4.x and above, KOA and HAPI 17.x to 18.x
- Third-party: BlueBird3.x, Sequelize, mongoose, generic-pool, multer

PHP

- Operating System: Ubuntu
- Databases: MySQL
- Versions: PHP 7 and above
- Servers: Apache

Ruby

- Operating System: Ubuntu, CentOS
- Language: Ruby 2.6
- Database: SQLite 3, Mysql2, AuroraDB, Postgres
- Frameworks: Rails v.6.0, Sinatra
- Deployments: Host Mode, Container Mode, EKS, ECS
- Ruby Interpreter: MRI

Application Server Support

Web Application Server	Mode
Puma	• Multi-threaded Mode • Cluster Mode
Phusion Passenger	• Standalone mode (with Nginx) • Nginx Mode+ Passenger (use ruby as like mod_php) • Dynamic scaling of Ruby Application Process • Static pool of Ruby Application Process • Direct Spawn Method & Smart Spawn Method
Apache+Passenger	• Dynamic scaling of Ruby Application Process • Static pool of Ruby Application Process
Unicorn	• Niginx+Unicorn • Unicorn(no reverse proxy)

Cloud Support

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Hardware Requirements

- Juniper Cloud Workload Protection agents (RASP mode)—Linux machine with 500MB to 2GB RAM, 2 vCPUs and 5 GB HD minimum
- Juniper Cloud Workload Protection agents (IAST mode)—Linux machine with 2GB to 8GB RAM (depending on load), 2 vCPUs and 5 GB HD minimum

Agent and vSRX Connectivity Requirements

Use ports 80 and 443 to connect Juniper Cloud Workload Protection portal www.juniper.k2io.net.