

# In Focus

## Junos Space Security Director and Policy Enforcer

#### IN THIS GUIDE

- About This In Focus Guide | 1
- Use Case 1: Configure IPS Policy in a Firewall Policy | 2
- Use Case 2: Import a Firewall Policy that Has IPS Policy Configured | 11
- Use Case 3: Configure Certificate-Based Authentication in Policy Enforcer | 19

## **About This In Focus Guide**

Use cases	Use this guide to quickly learn about important use cases of Junos Space Security Director and Policy Enforcer.			
	In addition to this guide, you can find detailed information about concepts and configuration in the Junos Space Security Director documentation and Policy Enforcer documentation.			
Audience Network operators and administrators				
Knowledge level	General familiarity with networking fundamentals and data center architectures.			
Supported web browsers	Junos Space Security Director and Policy Enforcer are best viewed on the following web browsers:			
	• Mozilla Firefox			
	Google Chrome			
	Microsoft Internet Explorer 11			

## **Use Case 1: Configure IPS Policy in a Firewall Policy**

#### SUMMARY

An intrusion prevention system (IPS) policy enables you to selectively enforce various attack detection and prevention techniques on the network traffic passing through an IPS-enabled device. In this section, you'll learn how to create an IPS policy and then assign the IPS policy to a firewall policy rule that is assigned to a device running Junos OS Release 18.2 or later.

#### IN THIS SECTION

•	Benefits   2
•	Before You Begin   3
•	Overview   3
•	Create an IPS Policy   4
•	Assign the IPS Policy to a Firewall Policy Rule   6
•	Verify the IPS Policy Assignment to Firewall Policy   9
•	CLI Configuration   9

## **Benefits**

- Assign a different IPS policy to each firewall policy rule.
- IPS policy matches are handled within the standard or unified firewall policy to which the IPS policy is assigned.
- Simplifies application-based security policy management at Layer 7.
- Provides greater control and extensibility to manage dynamic applications traffic.

## **Before You Begin**

- Install Junos Space Security Director and Log Collector. See Junos Space Security Director Installation and Upgrade Guide.
- Ensure that IPS is enabled on the SRX Series device.
- Ensure that the SRX Series device runs Junos OS Release 18.2 or later.

#### NOTE:

- Although this use case has been specifically validated against Junos Space Security Director Release 19.3 and an SRX Series device running Junos OS Release 18.2, you can use Junos OS Release 18.2 or later.
- Only mandatory fields and other required fields are included in the procedures in this use case.

## Overview

Starting in Junos Space Security Director Release 19.3, you cannot assign devices running Junos OS Release 18.2 and later to an IPS policy from the IPS Policies page. You'll need to assign an IPS policy to a firewall policy rule for devices running Junos OS Release 18.2 and later. The CLI configuration for the IPS policy is generated along with the standard or unified firewall policy to which the IPS policy is assigned. When an IPS policy is configured in a firewall policy, the traffic that matches the specified criteria is checked against the IPS rule bases. This type of configuration can be used to monitor traffic to and from the secure area of an internal network as an added security measure for confidential communications.

In the following topology, we have an enterprise local area network behind a Layer 2 switch. The switch is connected to an SRX Series firewall that has IPS enabled and inspects all the traffic traveling in and out of the network. The SRX Series device can be in any form: hardware, virtual, or containerized.



## **Create an IPS Policy**

Let's first create an IPS policy that we will then configure on an SRX Series device running Junos OS Release 18.2:

1. Select Configure > IPS Policy > Policies.

The IPS Policies page is displayed.

2. Click the + icon.

The Create IPS Policy page is displayed.

*		Configu	re / IPS Policy / Policies			Q Unifie	ed_IPS 🗸 🗸	Δ ⊑ ⑤ ?
×	Eirowall Bolicy	IPS	Policies @					
	Standard Policies		Create IPS Policy @	)				□   Q T.
1	Devices Schedules Profiles		Name* ⑦ Description ⑦	IPS_Policy		У	Modified By	Domain
*	Templates Environment		Policy Options				super	Global/Unified_IPS
٢	Application Firewall > SSL Profiles		Policy Templates ⑦		Select		super	Global/Unified_IPS Global/Unified_IPS
	IPS Policy ~ Policies Devices		Туре*	Group Policy     Evice Pelicy			super super	Global/Unified_IPS Global/Unified_IPS Global/Unified_IPS
	Templates	> P0 6 iter	Device Selection					
	UTM Policy >			Clear All				
	Threat Prevention					Cancel OK		
	Shared Objects >	~						

3. Enter the following IPS policy name: IPS\_Policy

A policy name can have a maximum of 255 characters, and can include alphanumeric characters, spaces, and periods.

4. Select the Policy Type as **Device Policy**.

**NOTE:** You can also select the group policy option. You can assign either a group policy or a device-specific policy to the firewall policy.

5. Do not select any device from the list.

**NOTE:** Only the devices running Junos OS Release 18.1 and earlier are listed. To configure an IPS policy on devices running Junos OS Release 18.2 or later, you'll need to assign an IPS policy (without device assignment) to a firewall policy rule. The IPS policy is updated with firewall policy update.

6. Click OK.

The created IPS Policy (IPS\_Policy) is displayed on the IPS Policies page.

## Assign the IPS Policy to a Firewall Policy Rule

Now let's assign the created IPS policy to a firewall policy rule:

1. Select Configure > Firewall Policy > Standard Policies.

The Standard Policies page is displayed.

2. Click the + icon.

The Create Firewall Policy page is displayed.

:		Configure / Firewall Policy / Standard Policies	Q Unified_IPS ∨ Ω ⊑ S ?
	Firewall Policy	Standard Policies @	
	Standard Policies	Create Firewall Policy 🗇	
	Unified Policies		g 🗸 🛛 More 🧹   🕂 🖉   🍳 🏹 -
	Devices	General Information	
	Schedules	Name* ② Firewall_Policy	y Modified By Domain
37	Profiles	> Pr Description ③	
~	Templates	Y DI	
	Environment		super Global/Unified_JPS
	User Firewall Manag >	Policy Options	super Global/Unified IPS
	Application Firewall >		super Global/I Ini5ed IPS
	IPS Policy	Select an option V Clear All	Olevel Alexandro
	Policies		Giobal/United_IPS
	Devices	Pr     Type* ⑦     Group Policy     Oroup Policy     Device Policy	
	Signatures	4 ite	
	Templates	Device Selection	
	NAT Policy >	Device ⑦ vsrx-18.2	
	UTM Policy	Clear All	
	Application Policy B		
	Threat Prevention >	Cance	
	IPSec VPN		
	Shared Objects >		

- 3. Enter the following firewall policy name: Firewall\_Policy
- 4. Select the Policy Type as **Device Policy**.

When you select the device policy option, the firewall policy is created for each device. If you select the group policy option, the firewall policy is shared with multiple devices.

5. Select the vsrx-18.2 device.

All the devices that are discovered by Junos Space Security Director are listed in the drop-down. To know more about device discovery in Junos Space Security Director, see Create Device Discovery Profiles in Security Director.

NOTE: The device that you select must be running Junos OS Release 18.2 or later.

6. Click **OK** to create the firewall policy.

The firewall policy that you created (Firewall\_Policy) is displayed on the Standard Policies page.

7. Click Add Rule for the Firewall\_Policy policy to add rules.

The Create Rule page is displayed.

8. On the General tab, enter the following rule name: Firewall\_Policy\_Rule

:		Configur	e / Firewall Policy / Standard Policies					(	Q Unified	d_IPS	~ <u> </u>	s ?
×	Firewall Policy ~ Standard Policies Unified Policies	Fire	Create Rule @	Destination	Advanced Security	Rule Options	Rule Analysis	Rule Placement		+ / 11   2	л <sup>и</sup> К	7.1
	Devices Schedules		General Information						ID	) End User Pro	file	Des
*	Templates	*	Rule Name* ⑦ Description ⑦	Firewall_Policy_Rule					- 1			
٢	User Firewall Manag >											,
	SSL Profiles > IPS Policy > Policies											
	Devices Signatures											
	NAT Policy											
	Application Policy B Threat Prevention											
	IPSec VPN > Shared Objects >		Cancel						Next			

- 9. Click Next until you reach the Advanced Security tab.
- 10. On the Advanced Security tab:
  - a. Select **Permit** from the Action drop-down list.
  - b. Select the value IPS\_Policy from the IPS Policy drop-down list.

**NOTE:** Starting in Junos Space Security Director Release 20.1R1 V1 hot patch, you can assign a group IPS policy that is not assigned to any device to a firewall policy.

		Configure	/ Firewall Policy / Standard Policies					Q	Unified_IPS	~ A 5	s ?
×	Firewall Policy ~ Standard Policies Unified Policies	Fire	Create Rule ⑦ General Source	Destination	Advanced Security	Rule Options	Rule Analysis	-O Rule Placement	(+ / m)	<sup>یہ</sup> م <sup>ی</sup> د م	7-1
	Devices Schedules Profiles	~	Advanced Security Rule Action						ID End User	Profile	Des
*	Templates Environment User Firewall Manag	~	Action ⑦	Permit	```	*					>
0	Application Firewall > SSL Profiles >		App Firewall ②	Supported in Junos OS version 18.2 version and later, use dy	Clear n 18.1 and lower. For Jun mamic application of Unit	NI Add New 15 ed					
	Policies Devices		SSL Proxy ① IPS ⑦	Select an option	Clear Clear	NI Add Forward Proxy	Add Revense Proxy				
	Signatures Templates NAT Policy		IPS Policy 🕖	Supported in Junos OS version IPS_Policy Supported in Junos OS version	n 18.1 and lower Clear . n 18.2 and later	Alf					
	UTM Policy > Application Policy B Threat Prevention >		UTM 💮	Select an option	<ul> <li>Clear</li> <li>Clear</li> </ul>	NI Add New					
	IPSec VPN > Shared Objects >		Cancel					Back No	ext		

11. Click Next until you reach the Rule Placement tab, and click Finish.

You can view the IPS policy details in the firewall policy configuration summary.

8	Í	Configure / Firewall Policy / Standard Policies	Q Unified_IPS ∨ Ω ⊑ s ?
×	Firewall Policy ~	Fir Create Rule 0	
$\odot$	Unified Policies	Summary	
	Devices	Review the summary of configuration changes.	
	Schedules	General Information Edit	ID End User Profile Des
(mail	Profiles	Name Firewall_Policy_Rule	
*	Templates	Identify Traffic Source Edit	
ē	Environment	Address Any	
	User Firewall Manag >	Identify Traffic Destination	2
۲	Application Firewall >	Address Any	
	SSL Profiles >	Service Any	
	IPS Policy 🗸 🗸	Advanced Security Edit	
	Policies	IPS Off	
	Devices	IPS_Policy IPS_Policy	
	Signatures	Action PERMIT	
	Templates	Rule Options Edit	
	NAT Policy >	Profile Inherited from policy	
	UTM Policy >	Rule Analysis	
	Application Policy B	Edit	
	Threat Prevention >	Rule Placement Edit	~
	IPSec VPN >	Cancel Back	ox
	Shared Objects >		

12. Click **OK** to create the rule.

The rule is displayed on the Firewall\_Policy/Rules page.

13. Click **Save** to save the rule.

Similar to Firewall\_Policy\_Rule, we have created another rule Firewall\_Policy\_Rule2.

## Verify the IPS Policy Assignment to Firewall Policy

#### Purpose

Let's verify that the firewall policy that you created includes the IPS policy that you created (IPS\_Policy).

#### Action

1. Select Configure > Firewall Policy > Standard Policies.

The Standard Policies page is displayed.

2. Click the rules for the firewall policy named (Firewall\_Policy).

The Firewall\_Policy/Rules page is displayed. In the Advanced Security column, the IPS policy named **IPS\_Policy** is displayed for both the rules that you created (**Firewall\_Policy\_Rule** and **Firewall\_Policy\_Rule2**).

٠			Configure / Firew	vall Policy /	Standard Po	licies				Q unif	ied_JPS ✓ 众 0	s ?
×	irewall Policy Standard Policies	~	Firewa	II_Po	licy /	Rules	Currently editing this	policy				
∞	Unified Policies							Save Discard Publis	h Update Shared Obj	ects ~ More ~	+ / 1 12 2 2 9	<b>∀</b> • :
53	Devices											
	Schedules			Seq.	Hit Co.	Bula Marra	Est Toos	Sec. Address	Darit Topo	Dest Address	Advanced Exterior	Empire
-	Profiles				HILLO.	Null Name	arc. zone	art. Aduress	Dest. 2019	Dest. Address	Advanced security	SHIVILL
3.1	Templates		ZONE (0	Rule)								
e e	invironment		V GLOBAL	(2 Rules)								
e •	Jser Firewall Management	>	0									
A	Application Firewall Policy	>	0 +	1	<u> </u>	Firewall_Policy_Rule	-	Any		Any	IPS PIPS_Policy	Ary
© _ s	SL Profiles	>	<b>2</b> •	2	NA	Firewall_Policy_Rule2	2 -	Any		Any	IPS PIPS_Policy	Arty
	PS Policy	>	4									•
N	NAT Policy	>										
	JTM Policy	>										
A	Application Policy Based Routing											
т	Threat Prevention	>										
	PSec VPN	>										
s	ihared Objects	>										
0	Thange Management	>										
6	Suided Setup	>										
		~										

## **CLI** Configuration

You'll see that the IPS\_Policy policy is assigned to the Firewall\_Policy\_Rule and Firewall\_Policy\_Rule2 rules.

##Security Firewall Policy: global ##

set security policies global policy Firewall\_Policy\_Rule match application any

set security policies global policy Firewall\_Policy\_Rule match destination-address any

set security policies global policy Firewall\_Policy\_Rule match source-address any

set security policies global policy Firewall\_Policy\_Rule then permit application-services idp-policy IPS\_Policy

set security policies global policy Firewall\_Policy\_Rule2 match application any

set security policies global policy Firewall\_Policy\_Rule2 match destination-address any

set security policies global policy Firewall\_Policy\_Rule2 match source-address any

set security policies global policy Firewall\_Policy\_Rule2 then permit application-services idp-policy IPS\_Policy

#### ##IDP Configurations##

set security idp idp-policy IPS\_Policy rulebase-ips rule Device-1 match application default

set security idp idp-policy IPS\_Policy rulebase-ips rule Device-1 match attacks predefined-attack-groups "Additional Web Services - Info"

set security idp idp-policy IPS\_Policy rulebase-ips rule Device-1 match from-zone any

set security idp idp-policy IPS\_Policy rulebase-ips rule Device-1 match to-zone any

set security idp idp-policy IPS\_Policy rulebase-ips rule Device-1 then action recommended

#### WHAT'S NEXT

To learn more about IPS features, see Junos Space Security Director User Guide.

# Use Case 2: Import a Firewall Policy that Has IPS Policy Configured

#### SUMMARY

An intrusion prevention system (IPS) policy enables you to selectively enforce various attack detection and prevention techniques on the network traffic passing through an IPS-enabled device. In this section, you'll learn how to import a device running Junos OS Release 18.2 (that has a firewall policy with an IPS policy configured) to Junos Space Security Director. You'll see that the assigned IPS policy is imported along with the firewall policy.

#### IN THIS SECTION

Director | 16

•	Benefits   11
•	Before You Begin   12
•	Overview   12
•	Import a Firewall Policy   13
•	CLI Configuration   15
•	Verify the Imported Configuration in Security

## **Benefits**

- Each imported firewall policy rule can have a different IPS policy assigned.
- Simplifies application-based security policy management at Layer 7.
- Provides greater control and extensibility to manage dynamic applications traffic.

## **Before You Begin**

- Install Junos Space Security Director and Log Collector. See Junos Space Security Director Installation and Upgrade Guide.
- Ensure that IPS is enabled on the SRX Series device.
- Ensure that the SRX Series device runs Junos OS Release 18.2 or later.

#### NOTE:

- Although this use case has been specifically validated against Junos Space Security Director Release 19.3 and an SRX Series device running Junos OS Release 18.2, you can use Junos OS Release 18.2 or later.
- Only mandatory fields and other required fields are included in the procedures in this use case.

## Overview

Starting in Junos Space Security Director Release 19.3, when you import a firewall policy from an SRX Series device running Junos OS Release 18.2 or later, the IPS policy that is assigned to the firewall policy is also imported. The imported device is assigned to the firewall policy, and is displayed on the firewall policies page. The imported device is not displayed on the IPS Policies page.

In the following topology, we have an enterprise local area network behind a Layer 2 switch. The switch is connected to an SRX Series firewall that has IPS enabled and inspects all the traffic traveling in and out of the network. The SRX Series device can be in any form: hardware, virtual, or containerized.



## Import a Firewall Policy

Let's import a firewall policy from an SRX Series device running Junos OS Release 18.2:

1. Select **Devices > Security Devices**.

The Security Devices page is displayed.

2. Select the vsrx-18.2 device, and click Import.

The Import Configuration page is displayed.

							O Unified_IPS	
alle		Devices / Security De	vices				۹	· □ · □ · □ · □ · □ · □ · □ · □ · □ · □
$\times$	Security Devices	Import Con	figuration ®					
$\odot$	Device Discovery	•	•					
~	Secure Fabric >	Manageo Services		I CE Resolution				letwork More V V V I
	Licenses	<ul> <li>For devices with.</li> </ul>	lunos OS Release 18.2 and late	r. IPS policy is auto	imported along v	ith the assigned Firewall Policy.		1 Status Connection Status
Land		For devices with	lunos OS Release 18.2 and late	r, Deprecated App	Fw configuration v	vill not be imported.		sed - Unverifi 🛦 up
*		1 selected						sed - Unverifi 🔺 un
								>
0		Name Name		Rules	Errors	Summary		Display 50 🗸
~		✓ Firewall Poli	cy					
		vsrx-18.2		1	0			
		✓ NAT Policy						
		vsrx-18.2		2	0			
		2 items						
		Concel					Ne	
		Concd					12	

3. Select the firewall policy vsrx-18.2 (the IPS policy is assigned to this firewall policy).

#### 4. Click Next.

A summary of the configuration changes to be imported is displayed.

*		Devices / Security Devices		Q Unified	JJPS	✓ △ □ S ?
	Security Devices	Import Configuration ®				
	Device Discovery Secure Fabric >	Summary Review the summary of configuration changes.				
	Licenses	Managed Services Firewall Policy Rules	Firewall Policy JPS Policy Edit			ietwork More -   Q T :
		IPS Policy Rules Error Summary Object Conflicts	1			sed - Unverifi 🛦 up
		Object Connects Object Creation list Object Modification list	0 1 0		1	sed - Unverifi 🛦 up
		Report Click OK to complete.	SummaryReport.zip			Display 50 🗸
		Cancel		Back	ox	

5. Click **OK** to import the device configuration.

The Job Details page is displayed. The IPS policy (IPS-Policy-1) is imported along with the firewall policy (vsrx-18.2).

Security Devices Device Discovery	e Job Details @	
Device Discovery	Job Details ©	
Secure Fabric > Licenses	1 b     Job Type:     Import     Job State:       Job ID:     1608930     Percent Comp       Job Name:     Import-16089300     Scheduled State       User:     Super     Actual State       Device Assigned Policies varx-18.2 (Finewall Policy)     Image: State	blete: 100% art Time: Wed, 12 Aug 2020 15:45:19 IST Wed, 12 Aug 2020 15:45:58 IST Wed, 12 Aug 2020 15:45:58 IST Wed, 12 Aug 2020 15:45:58 IST Credentials Based - Unverifi∟ ▲ up Credentials Based - Unverifi∟ ▲ up Credentials Based - Unverifi∟ ▲ up
	Task Name Status Details	
	Importing IPS Policy IPS-Policy 1 Success Finished at Wed,	12 Aug 2020 15:45:53 IST
	Importing Firewall Policy *vsrx-18.2* Success Finished at Wed, [Deprecated AppFW Config if any in Device will not be imported]	12 Aug 2020 15:45:58 IST
	Generating Report Success Finished at Wed,	12 Aug 2020 15:45:58 IST
	3 Rows	
	Importing Firewall Policy *vsrc 18.2* Success Finished at Wed, [Deprecated AppFW Config if any in Device will not be imported] Generating Report Success Finished at Wed, <b>3</b> Rows	12 Aug 2020 15:45:58 IST 12 Aug 2020 15:45:58 IST

#### 6. Click OK.

The imported policies are displayed on the IPS Policies page and also in the firewall policy rule.

## **CLI Configuration**

Here is the CLI configuration from the vsrx-18.2 device: set security idp idp-policy IPS-Policy-1 rulebase-ips rule rule1 match from-zone any set security idp idp-policy IPS-Policy-1 rulebase-ips rule rule1 match to-zone any set security idp idp-policy IPS-Policy-1 rulebase-ips rule rule1 match application default set security idp idp-policy IPS-Policy-1 rulebase-ips rule rule1 match attacks predefined-attacks ICMP:INFO:ECHO-REPLY set security idp idp-policy IPS-Policy-1 rulebase-ips rule rule1 then action recommended set security policies global policy rule-one match source-address any set security policies global policy rule-one match application any set security policies global policy rule-one then permit application-services idp-policy IPS-Policy-1

## Verify the Imported Configuration in Security Director

#### Purpose

Let's verify that the device is assigned to the imported firewall policy. You'll see that the device is not assigned to the imported IPS policy on the IPS Policies page.

#### Action

1. Select Configure > IPS Policy > Policies.

The device is not displayed for the imported IPS policy on the IPS Policies page.

			Configure / IPS	Policy / Po	olicies						Q	Unified_IP	S	~ 0	ĘS	?
	Firewall Policy	~	IFSFU	incre:	<b>5</b> 0											
۵	Unified Policies									Publish	Update	Locking ~	More -	/ 6	9 7	7.
	Devices	- 1														
	Schedules			Seq.	Name		Rules	Devices	Publish State	Last Modified	c	reated By	Modified By	Do	main	
×	Profiles		> POLICIES	APPLIED BE	EFORE 'DEVICE SPECI	IFIC POLICIES' (	0 policy)									
~	Templates	- 1		PECIFIC POL	ICIES (1 policy)											
	Environment				IPS-Policy-1		1		Not Published	Wed Aug 12,2020 3:45 PM	si	iper	super	Gk	bal/Unified_	IPS
۲	Application Firewall	;	> POLICIES	APPLIED AF	FTER 'DEVICE SPECIF	IC POLICIES' (0)	policy)									
	SSL Profiles	>	1 items													
	IPS Policy	~	_													
	Policies	- 1														
	Devices	- 1														
	Signatures	- 1														
	Templates	- 1														
	NAT Policy	>														
	UTM Policy	>														
	Application Policy B	- 1														
	Threat Prevention	>														
	IPSec VPN	>														
	Shared Objects	>														
	Change Management	>	~													

2. Select Configure > Firewall Policy > Standard Policies.

The imported firewall policy (**vsrx-18.2**) and the assigned device (**vsrx-18.2**) are displayed on the Standard Policies page.

* *	Firewall Policy 🗸	Configure / Frewall Policy / Standard Policies Q Unified_JPS ∨ Δ 𝔅 S ? Standard Policies ⑦
8	Unified Policies Devices	Publish Update Global Options Looking V More V + 🖉 🔍 🖓 🗸
-	Schedules Profiles	Seq. Name     Rules     Devices     Publish State     Last Modified     Created By     Modified By     Domain
*	Templates	POLICIES APPLIED BEFORE 'DEVICE SPECIFIC POLICIES' (0 policy)
	Environment User Firewall Manag >	vsn-18.2 1 vsn-18.2 Not Published Wed Aug 12,2020 3:45 PM super super Global/Unified_IPS
۲	Application Firewall >	> POLICIES APPLIED AFTER 'DEVICE SPECIFIC POLICIES' (0 policy)
	SSL Profiles	1 kons
	IPS Policy ~ Policies	
	Devices	
	Signatures	
	Templates	
	NAT Policy >	
	UTM Policy >	
	Application Policy B	
	Threat Prevention >	
	IPSec VPN >	
	Shared Objects >	

3. Click the rules for the vsrx-18.2 firewall policy.

On the firewall policy rules (vsrx-18.2/Rules) page, you'll see the imported IPS policy (IPS-Policy-1) in the Advanced Security column.

	Devices	~	Configure / Fire	mail Policy	Standard Pe	Acies							Q Unified	UPS	~		2
	Schedules			0.21	Dulas												
$\times$	Profiles		VSFX-1	8.27	Rules	Edited 2 minut	e(s) ago										
~	Templates																
<u>د</u>	Secure Web Prony	- 84								Publish	Update Sh	ared Objects 👒	More -	+ / 8	1 2 2	* Q <b>Q</b> .	÷.
⊠	Environment																
-	User Firewall Manag 3	>		Seq.	HILCO	Rule Name	Adva	nced Security	Src. Zone	Sec	Address	5	rc. Expression		User ID	End Use	r Profi
21	Application Firewall 3	>	× 20NE (	0 Rufe)													
×.	SSL Profiles	>		L (1 Rule)													
	IPS Policy	-	10		2.0		-				~						
~	Policies				-	rule-one	IPS P	20CY			× Any						
۳	Devices						IPS PC	JUEY: IPS-Policy	-1								
	Signatures																
	Templates.																
	NAT Policy 2	>															
	UTM Policy 2	>															
	Application Policy B																
	Threat Prevention	>															
	IPSec VPN	, I															
	Insights 3	>															
	Shared Objects	>															
	Change Management	>															
	Guided Setup	>															
		- 11															

**NOTE:** If a device runs Junos OS Release 18.2 or later and has deprecated active-idp policy CLI, Junos Space Security Director imports the IPS policy and assigns it to all firewall policy rules with IPS ON.

#### WHAT'S NEXT

To learn more about IPS features, see Junos Space Security Director User Guide.

# Use Case 3: Configure Certificate-Based Authentication in Policy Enforcer

#### SUMMARY

Users typically gain access to resources from an application or system on the basis of their username and password. You can also use certificates to authenticate and authorize sessions among various servers and users. Only one authentication mode is supported at a time and all users are authenticated using the selected authentication mode. In this use case, you'll learn how to configure certificate-based authentication for a Policy Enforcer user.

#### IN THIS SECTION

Benefits   20
Before You Begin   20
Overview   20
Generate SSL certificates   21
Upload the CA Certificate   24
Upload the User Certificate   25
Upload X.509 Certificate File in Policy Enforcer   26
Configure the Web Browser Settings   27
Change the User Authentication Mode to Certificate-Based Authentication Mode   <b>29</b>
Verify the Certificate-Based Authentication Mode   30
Troubleshoot Authentication Issues   31

## Benefits

Certificate-based authentication over a Secure Sockets Layer (SSL) connection is the most secure type of authentication.

## **Before You Begin**

- Install Junos Space Security Director. See Junos Space Security Director Installation and Upgrade Guide.
- Install and configure Policy Enforcer virtual machine, see Policy Enforcer Installation Overview.
- Generate X.509 certificates, and make sure that the user certificates are available on your local machine. See "Generate SSL certificates" on page 21.

NOTE: Only mandatory fields and other required fields are included in the procedures in this use case.

## Overview

Starting in Policy Enforcer Release 20.1R1, you can enable certificate-based authentication for the Policy Enforcer user.

The following topology shows Policy Enforcer configured in Junos Space Security Director. The user can configure certificate-based authentication mode and use certificates to gain access to the application.



### **Generate SSL certificates**

#### IN THIS SECTION

- Generate a CA certificate | 21
- Generate Client SSL certificates | 22
- Copy the Certificates from the Linux Server to Your Local Machine | 24

Let's learn how to generate a certification authority (CA) certificate, generate a client certificate and a private key for the SSL client, and then convert the client certificate and private key to Personal Information Exchange-pkcs#12 format for use by web browsers.

#### Generate a CA certificate

- 1. Log in to the Linux server.
- 2. Run the following command:

openssl req -newkey rsa:4096 -keyform PEM -keyout ca.key -x509 -days 3650 -outform PEM -out ca.cer

3. Enter the PEM passphrase, for example: 1234.

You'll need this passphrase while you generate client certificates.

- 4. Enter the following details, for example:
  - Country Name: IN
  - State or Province name: KAR
  - Locality Name: BAN
  - Organization Name: Juniper
  - Organization Unit Name: space
  - Common Name: space\_user

The certificate is issued by this name.

• Email Address: example@juniper.com

ot@nm-apps-ip26 ~]# openssl req -newkey rsa:4096 -keyform PEM -keyout ca.key x509 -days 3650 -outform PEM -out ca.cer enerating a 4096 bit RSA private key writing new private key to 'ca.key' Inter PEM pass phrase: Verifying - Enter PEM pass phrase: (ou are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. or some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [XX]:IN State or Province Name (full name) []]KAR Locality Name (eg, city) [Default City]:BAN Organization Name (eg, company) [Default Company Ltd]: Juniper Organizational Unit Name (eg, section) []:space ommon Name (eg, your name or your server's hostname) []:space\_user mail Address []:example@juniper.com root@nm-apps-ip26 ~]#

#### The CA certificate is generated.

-rw-r--r-- 1 root root 2094 Jan 29 00:11 ca.cer -rw-r--r-- 1 root root 3394 Jan 29 00:11 ca.key

#### **Generate Client SSL certificates**

- 1. Log in to the Linux server.
- Run the following command to generate a private key for the SSL client, for example: client1.key.
   openssl genrsa -out client1.key 4096
- 3. Run the following command to generate the certificate request, for example: client1.req.

#### openssl req -new -key client1.key -out client1.req

- 4. Enter the following details for client1, for example:
  - Country Name: IN
  - State or Province name: KAR
  - Locality Name: BAN
  - Organization Name: Juniper
  - Organization Unit Name: space
  - Common Name: space\_user1

The certificate is issued by this name.

- Email Address: example1@juniper.com
- 5. Enter the challenge password, for example: **12345**.

6. Run the following command to issue the client certificate using the certificate request and the CA key, for example: client1.cer.

openssl x509 -req -in client1.req -CA ca.cer -CAkey ca.key -set\_serial 101 -extensions client1 -days 365 -outform PEM -out client1.cer

- 7. Enter the passphrase for the ca.key as **1234**. This must be the same passphrase that you provided while creating the CA certificate in Step 3.
- 8. Run the following command to convert the client certificate and private key to pkcs#12 format for use by web browsers, for example: **client1.p12** (Personal Information Exchange file type).

#### openssl pkcs12 -export -inkey client1.key -in client1.cer -out client1.p12

9. Enter the export password, for example **123456**.

You'll need this password to import the certificate to the web browser.

The following certificates are generated:

AL 11 AL AL				OF THE R		· · · · ·	CONTRACT NOT	
-rw-rr	root	root	2094		29	00:11	ca.cer	
-rw-rr	root	root	3394	Jan	29	00:11	ca.key	
-rw-rr	root	root	1968	Jan	29	00:16	client1.cer	
-rw-rr	root	root	3243	Jan	29	00:14	client1.key	
-rw-rr	root	root	4165	Jan	29	00:17	client1.p12	
-rw-rr	root	root	1813	Jan	29	00:16	client1.req	I

Similarly, generate client2.cer, client2.key, and client2.p12 certificates with the following details, for example:

- Country Name: IN
- State or Province name: KAR
- Locality Name: BAN
- Organization Name: Juniper
- Organization Unit Name: space
- Common Name: space\_user2

The certificate is issued by this name.

• Email Address: example2@juniper.com

**NOTE:** In this example, we will use the generated **client1** certificates for the Junos Space user (**user1**) and **client2** certificates for the Policy Enforcer user (**pe\_user**).

#### Copy the Certificates from the Linux Server to Your Local Machine

- Log in to the WinSCP client to copy the certificates that you generated from the Linux server to your local machine.
   You can use any file transfer protocol client.
- 2. Select the file protocol as **SFTP**.
- 3. Enter the hostname of the Linux server, username, and password, and click Login.
- 4. Select the certificate files that you generated in the Linux server, and copy the files to the preferred location on your local machine.

## Upload the CA Certificate

Let's upload the CA certificate or the root certificate to verify user certificates. The private key of the root certificate is used to sign the user certificates, which then inherits the trustworthiness of the root certificate.

To upload a CA certificate:

- 1. Log in to Junos Space Network Management Platform.
- 2. Select Administration > CA/CRL Certificates.

The CA CRL Certificates page is displayed.

3. Click the arrow next to the + icon, and select X.509 CA Certificate.

The Upload X.509 CA Certificate File page is displayed.

4. Browse the X.509 CA certificate file (for example: **ca.cer**) from your local machine that you generated in "Generate SSL certificates" on page 21.

Applications	Administration > CA/CRL Certificates					
Network Management Platform		CA/CRL C				
Devices     Devices		<b>⊙</b> •⊖				
B CLI Configlets		Disting	juished Name	Certification Type	Expiration Time	
Images and Scripts     Reports		Upload X	.509 CA Certificate			
Network Monitoring     Configuration Files		X.509	CA Certificate File:	ca.cer	Browse	
B Jobs			_			
Audit Logs			Up	cancel		
Administration  Fabric						
<ul> <li>Database Backup and Restore</li> <li>Licenses</li> </ul>						
Applications     Snace Troubleshooting						
Platform Certificate						
- Authentication Servers						

#### 5. Click Upload.

A success message is displayed after you upload the valid certificate. You can view the CA certificate details on the CA/CRL Certificates page.

## Upload the User Certificate

Let's upload user certificates to authenticate the Junos Space user by using certificate-based authentication. You need to upload the corresponding certificate for each user for the Junos Space server to authenticate the user. To create a user in Junos Space Network Management Platform, see Create Users in Junos Space Network Management Platform.

To upload the user certificate for an existing user, for example user1:

- 1. Log in to Junos Space Network Management Platform.
- 2. Select Role Based Access Control > User Accounts.

The User Accounts page is displayed.

3. Right-click the Junos Space user, for example: user1, and select Modify User.

The Modify User page for user1 is displayed.

- 4. In the X509 Cert File field, browse the X.509 certificate file (for example: **client1.cer**) from your local machine that you generated in "Generate SSL certificates" on page 21.
- 5. Click Upload.

A success message is displayed.

## Upload X.509 Certificate File in Policy Enforcer

After you configure Policy Enforcer, a new user called pe\_user is created. You must add X.509 certificate for the pe\_user for seamless certificate-based authentication. Policy Enforcer authenticates with Junos Space Security Director and Junos Space Network Management Platform using certificates in the certificate-based authentication mode.

1. Log in to Junos Space Security Director.

#### 2. Select Administration > Policy Enforcer > Settings.

The Settings page is displayed.

#### 3. Enable Certificate Based Authentication.

This provides seamless operation when Junos Space Network Management Platform user switches to certificate-based authentication mode.

		Administration / Policy Enforcer / \$	ettings		
My Profile		Settings ©			
Users & Roles	>	The Policy Enforcer Space AP	N user (pe. user) password is currently valid. It will	expire	t on 1970-01-01.
Logging Management	>				
Monitor Settings		The Policy Enforcer is active			
Signature Database		It is configured with version	2000.01		
License Management	>				
Policy Enforcer	$\sim$	IP Address*	10.26Re34%		
Settings Connectors		Username*	admin		
Backup and restore		Password*			
NSM Migration		If you are planning to use certificate	based authentication later, enable the following to	iggle I	button to upload certificate and key for Policy Enforcer.
Policy Sync Settings		Certificate Based Authen ③			
Insights Management	>	X509Certificate File (2)	client2.cer		Browse
		X509Certificate Key File 🕐	client2.key		Browse
		ATP Cloud Configuration 🕐	ATP Cloud/JATP with Juniper Connected Sec	~	
		Configure polling timers to discover	hasts in your network		
		Poll Network wide endpo * 🕐	24	÷	hours
		Poll Site wide endpoints* 🕐	5	÷	mins
		Enablie purge to delete old feeds da	ta. You can set the purge History to determine how	v man	ry days of feeds history to be stored in Policy Enforcer.
		Enable Feeds Purge 🕐	0		
			OK Reset		

- 4. Browse the X509 certificate file, for example: **client2.cer**, and X509 certificate key file, for example: **client2.key** that you generated in "Generate SSL certificates" on page 21.
- 5. Click OK.

After uploading the certificates on the Settings Page, navigate to Junos Space Network Management Platform, select **User > Role Based Access control > User Accounts**. Right-click the pe\_user, and select **Modify User**. Here, you can view

#### the certificate details uploaded for the pe\_user.

Applications 帐	Role Based Access Control > User Acc	ounts > Modify User	
Network Management Platform	Modify User: pe_user		
B Devices	General		
Device Templates			
CLI Configlets	Login ID:	pe_user	
Images and Scripts	First Name:	Policy	
Reports	Last Name:	Falseer	
Network Monitoring	Cast Name.	Enforcer	
Configuration Files	Email:		
😠 Jobs		Use global settings	
Role Based Access Control	Maximum concurrent UI sessions:	5	0
-User Accounts	Automatic logout after inactivity:	Vise Global Settings	-
Roles	rate logot and locally.		~
Domains		0	
-Remote Profiles			
-API ACCESS PIDILES	Image File:	Browse	
Liser Groups			
P Audit Loos		Upload	
Administration			
	Cert Subject Name:	EMAILADDRESS=example2@juniper.com, CN=space_user2, OU=Sj	
		<	
		Stree .	
		Clear	
	X509 Cert File:	Browse	
		Upload	

## Configure the Web Browser Settings

You must import the Personal Information Exchange-pkcs#12 file type certificate uploaded to the Junos Space user (**user1**) on all the supported web browser settings page. In this example, let's upload the **client1.p12** on Google Chrome to enable certificate-based authentication.

1. Open the Google Chrome web browser.

NOTE: You can use any supported web browser.

- 2. Click on the ellipsis icon on the top-right corner of the web browser, and select Settings.
- 3. Select Security and Privacy.

The Security and Privacy page is displayed.

4. Select Security.

The Security page is displayed.

5. Select Manage Certificates.

The Certificates page is displayed.

#### 6. Click Import.

The Certificate Import Wizard is displayed.

7.	Browse the personal	information	file type, for	r example: <b>client1.p12</b> .	
----	---------------------	-------------	----------------	---------------------------------	--

<ul> <li>Ertificate Import Wizard</li> </ul>	
File to Import	
Specify the file you want to import.	
<u>F</u> ile name:	
C:\Users\Desktop\Cert1\dient1.p12	Browse
Note: More than one certificate can be stored in a single f	ile in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 Cer	tificates (.P7B)
Microsoft Serialized Certificate Store (.SST)	
	Next

You must select the personal information file type of the same certificate that you selected for the Junos Space Network Management Platform user (**user1**) as in "Upload the User Certificate" on page 25.

- 8. Click Next.
- 9. Enter the password for the private key as **123456**. You must use the same password that you provided in Step 9 while creating the client1 certificates.
- 10. Browse the location to store the certificate.

A summary of certificate details is displayed.

11. Click Finish.

 $\times$ 

A pop-up is displayed confirming the import of new private exchange key.

#### 12. Click OK.

A success message is displayed and the certificate is added to your web browser settings.

Certificates							×
Intended pu	urpose:	<all></all>					~
Personal	Other Peop	le Inte	rmediate Certifica	tion Authorities	Tru	isted Root Ce	ertification 1
Issued	To re_user1	I: Sj	ssued By pace_user	Expirat 1/29/2	io 023	Friendly Na <none></none>	me
Import	. Exp	ort	Remove				Advanced
Certificate	e intended p	urposes					View
							VIEW
							Close

## Change the User Authentication Mode to Certificate-Based Authentication Mode

Now let's change the authentication mode from password-based to complete certificate-based for users to get authenticated on the basis of their certificates.

- 1. Log in to Junos Space Network Management Platform.
- 2. Select Administration > Application.
- 3. Right-click Network Management Platform, and select Modify Application Settings.

The Modify Network Management Platform Settings page is displayed.

4. Select User.

The User page is displayed.

5. Select the Use X509 Certificate Complete Certificate option as the authentication mode.



The Change Summary page is displayed.

6. Click Confirm to enable the certificate-based authentication.

When you change the authentication mode, all existing user sessions, except that of the current administrator who is changing the authentication mode, are automatically terminated and the users are forced to log out.

## Verify the Certificate-Based Authentication Mode

#### Purpose

Let's verify that you can log in to Junos Space Network Management Platform using certificates.

#### Action

1. Access the Junos Space Network Management Platform application.

The following pop-up is displayed.

ciect a certificate			
elect a certificate to authe	nticate yourself to 10.2000000	745	
Subject	Issuer	Serial	
space_user1	space_user	65	
Certificate information		ок	Cancel

2. Click OK.

The Security Page is displayed.

3. Click Allow.

The user1 is logged in to the Junos Space Network Management application without providing any username and password.

## **Troubleshoot Authentication Issues**

#### Problem

Description: You must follow all the steps in the previous sections to enable certificate-based authentication. However, if you are restricted from logging in by using certificate-based authentication mode, then you can change the authentication mode to password-based from the CLI.

#### Solution

To change the authentication mode to password-based authentication from the CLI:

- 1. Log in to the CLI of the Junos Space server VIP node.
- 2. Navigate to the following directory: /var/www/cgi-bin.
- 3. Type the following command:

#### ./setSpaceAuthMode password-based

The authentication mode is changed to password-based, and you can login with the username and password.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2022 Juniper Networks, Inc. All rights reserved. .