

Intrusion Prevention System

This feature enables Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) for branch offices on Cisco SD-WAN. It is delivered using a virtual image on Cisco IOS XE SD-WAN devices. This feature uses the Snort engine to provide IPS and IDS functionalities.

Snort is an open source network IPS that performs real-time traffic analysis and generates alerts when threats are detected on IP networks. It can also perform protocol analysis, content searching or matching, and detect a variety of attacks and probes (such as buffer overflows).

- Overview of Intrusion Prevention System, on page 1
- Cisco SD-WAN IPS Solution, on page 2
- Configure and Apply IPS or IDS, on page 2
- Modify an Intrusion Prevention or Detection Policy, on page 6
- Delete an Intrusion Prevention or Detection Policy, on page 6
- Monitor Intrusion Prevention Policy, on page 7
- Update IPS Signatures, on page 9

Overview of Intrusion Prevention System

The IPS feature works in the network intrusion detection and prevention mode that provides IPS or IDS functionalities. In the network intrusion detection and prevention mode, the engine performs the following actions:

- Monitors network traffic and analyzes against a defined rule set.
- Performs attack classification.
- Invokes actions against matched rules.

Based on your requirements, you can enable Snort either in IPS or IDS mode. In IDS mode, the engine inspects the traffic and reports alerts, but does not take any action to prevent attacks. In IPS mode, in addition to intrusion detection, actions are taken to prevent attacks.

IPS the traffic and reports events to vManage or an external log server (if configured). External third-party monitoring tools, which supports Snort logs, can be used for log collection and analysis.

Cisco SD-WAN IPS Solution

The Snort IPS solution consists of the following entities:

- Snort sensor: Monitors the traffic to detect anomalies based on the configured security policies (that includes signatures, statistics, protocol analysis, and so on) and sends alert messages to the Alert/Reporting server. The Snort sensor is deployed as a security virtual image on the router.
- Signature store: Hosts the Cisco Talos signature packages that are updated periodically. vManage
 periodically downloads signature packages to the Snort sensors. You can modify the time interval to
 check for and down signature updates in Administration > Settings > IPS Signature Update.
- Alert/Reporting server: Receives alert events from the Snort sensor. Alert events generated by the Snort sensor can either be sent to vManage or an external syslog server or to both vManage and an external syslog server. vManage events can be viewed in **Monitor** > **Events**. No external log servers are bundled with the IPS solution.

Configure and Apply IPS or IDS

To configure and apply IPS or IDS to a Cisco IOS XE SD-WAN device, do the following:

- Before you Begin
- Configure Intrusion Prevention or Detection
- Apply a Security Policy to a Device

Before you Begin

Before you apply an IPS/IDS, URL Filtering, or Advanced Malware Protection policy for the first time, you must Upload the Cisco Security Virtual Image to vManage.

Configure Intrusion Prevention or Detection

To configure Intrusion Prevention or Detection through a security policy, use the vManage security configuration wizard:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

=	cisco vManag	▲ 0	🏓 🕹 engg 🕶
55	Dashboard	IATION SECURITY	E Custom Options +
	Monitor >	with Pholicy	00
٠	Configuration >	Search Optione 🗸	Total Rows: 1
	Devices	Description Use Case Devices Attached Device Templates Updated By Last Updated	-
	Carthorna	UCY Security Policy Direct Internet Access 3 2 admin 17 Sep 20	18 11:49:04 PM IST ++++
	Network Design		
	Templates		
	Policies		
	Security		
	Cloud onRamp for SeeS		
	Cloud onRamp		
	Network Hub		
٩	Tools >		
•	Maintenance >		8
#1	Administration		888
			5,

- 2. Click Add Security Policy. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
- 3. In Add Security Policy, select a scenario that supports intrusion prevention (Compliance, Direct Cloud Access, Direct Internet Access, or Custom).
- 4. Click **Proceed** to add an Intrusion Prevention policy in the wizard.
- 5. In the Add Security Policy wizard, click Next until the Intrusion Prevention screen is displayed.

=	cisco VManaj	çe
55	Dashboard	CONFIGURATION Security > Add Security Policy
	Monitor >	Several
٠	Configuration	
	Certificates	
	Network Design	
	Templates	
	Policies	
	Security	Prevent and act against malicious and hostile attacks by configuring Signature set and Inspection mode.
	Cloud onRamp for SaaS	O Add Intrusion Prevention Policy +
	Cloud onRamp	
	Network Hub	
٩	Tools >	
*	Maintenance >	
	Administration >	
63	vAnalytics >	
		BACK Next CANOB.

- 6. Click the Add Intrusion Prevention Policy drop-down and choose Create New to create a new Intrusion Prevention policy. The Intrusion Prevention Policy Rule Configuration wizard appears.
- 7. Click on **Target VPNs** to add the required number of target service VPNs in the Add Target VPNs wizard.
- 8. Enter a policy name in the **Policy Name** field.
- **9.** Choose a signature set that defines rules for evaluating traffic from the **Signature Set** drop-down. The following options are available. Connectivity provides the least restrictions and the highest performance. Security provides the most restrictions but can affect system performance.
 - Balanced: Designed to provide protection without a significant effect on system performance.

This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 9. It also blocks CVEs published in the last two years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

• Connectivity: Designed to be less restrictive and provide better performance by imposing fewer rules.

This signature set blocks vulnerabilities with a CVSS score of 10 and CVEs published in the last two years.

Security: Designed to provide more protection than Balanced but with an impact on performance.

This signature set blocks vulnerabilities with a CVSS score that is greater than or equal to 8. It also blocks CVEs published in the last three years and that have the following rule categories: Malware CNC, Exploit Kits, SQL Injection, blocked list, and App Detect Rules.

- **10.** Choose mode of operation from the Inspection Mode drop-down. The following options are available:
 - Detection: Select this option for intrusion detection mode
 - Protection: Select this option for intrusion protection mode
- 11. (Optional) From the Advanced tab, choose one or more existing IPS signature lists or create new ones as needed from the Signature Whitelist drop-down.

Selecting an IPS signature list allows the designated IPS signatures to pass through.

To create a new signature list, click **New Signature List** at the bottom of the drop-down. In the IPS Signature List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only). In the IPS Signature field, enter signatures in the format *Generator ID: Signature ID*, separated with commas. You also can use the Import button to add a list from an accessible storage location. Click **Save** when you are finished.

You also can create or manage IPS Signature lists by selecting the **Configuration** > **Security** tab in the left side panel, choosing **Lists** from the **Custom Options** drop-down at the top right of the page, and then selecting **Signatures** in the left panel.

To remove an IPS Signature list from the **Signature Whitelist** field, click the **X** next to the list name in the field.

- 12. (Optional) Choose an alert level for syslogs from the Alert Log Level drop-down. The options are:
 - Emergency
 - Alert
 - Critical
 - Error
 - Warning
 - Notice
 - Info
 - Debug

You must configure the address of the external log server in the Policy Summary page.

- 13. Click Save Intrusion Prevention Policy to add an Intrusion Prevention policy.
- 14. Click Next until the Policy Summary page is displayed
- 15. Enter Security Policy Name and Security Policy Description in the respective fields.
- **16.** If you set an alert level when configuring the Intrusion Prevention policy, in the Additional Policy Settings section, you must specify the following:
 - External Syslog Server VPN: The syslog server should be reachable from this VPN.
 - Server IP: IP address of the server.
 - Failure Mode: Open or Close
- 17. Click Save Policy to configure the Security policy.
- **18.** You can edit the existing Intrusion Prevention policy by clicking on **Custom Options** in the right-side panel of the **vManage** > **Configuration** > **Security** wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. In vManage, select the Configuration > Templates screen.

≡	Cisco vManag	e				
	Dashboard	CONFIGURATION TEM	IPLATES			
	Monitor >	Device Feature				
٠	Configuration 🗸	Create Template +				
	Devices	CLI Template		Search Options 🗸		
	Certificates	Name	Description	Туре	Device Model	Feature To
	Certificates					
	Network Design					No d
	Templates					
	Policies					
	Security					
	Cloud onRamo for SaaS					

- 2. In the Device tab, from the Create Template drop-down, select From Feature Template.
- 3. From the Device Model drop-down, select one of the IOS XE SD-WAN devices.
- 4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

CONFIGURATION 18M	PLATER			
Basic Information	Transport & Management VPN	Service WW	Additional Templates	
	The constrained of the second			
**	carlobs gas sped	•		Additional VPN Templates
-	cartoliv-gar-ped	•		Additional VPN Templates
-	ow toll-ger up d	*		Additional VPN Templates
Additional Template				
harmar	Choose .			
whey	Owner.			
NUMP	Owner-	-		
ecurity Policy	epella, annump, defeuit, partop	-		
Container Profile 1	Participation of a state of a state of the state of the			

- 5. From the Security Policy drop-down, select the name of the policy you configured in the previous procedure.
- 6. Click Create to apply the security policy to a device.

Modify an Intrusion Prevention or Detection Policy

To modify a intrusion prevention or detection policy, do the following:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

=	cisco vMana	ge .						٠	Ċ.	•	0	engg •
=	Dashboard	CONFIGURATION SEC	URITY							= 0	lustom Opti	ons +
	Monitor >	Add Security Policy										90
٠	Configuration >	۹,		Search Options 🐱							Total	Rows: 1
	Devices	Name	Description	Use Case	Devices Atlached	Device Templates	Updated By		Last Upda	led .		
	Certificates	SECURITY-POLICY	Security Policy	Direct internet Access	3	2	admin		17 Sep 20	18 11:49:041	PM IST	***
	Network Cestion											
	Territory											
	Templates											
	Policies											
	Security											
	Cloud onRamp for SeeS											
	Cloud onRamp											
	Network Hub											
٩	Tools >											
•	Maintenance >											8
-	Administration											000

- 2. In the Security screen, click the Custom Options drop-down and select Intrusion Prevention.
- 3. For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.
- 4. Modify the policy as required and click Save Intrusion Prevention Policy.

Delete an Intrusion Prevention or Detection Policy

To delete an intrusion prevention or detection policy, you must first detach the policy from the security policy:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

=	cisco vManage	• .						● D # 0	engg •
=	Dashboard	CONFIGURATION SECU	RITY					Custom Op	ions +
	Monitor >	Add Security Policy							90
٠	Configuration >	٩	-	with Options 🗸				Tuta	Rows: 1
	Devices	Name .	Description	Use Case	Devices Atlached	Device Templates	Updated By	Last Updated	_
	Certificates	appointmodel	second Pointy	Denter indentes Accesso	,	1	autoria.	17 002 2010 11/00/04 PM 101	
	Network Design								
	Templates								
	Policies								
	Security								
	Cloud onRamp for SeaS								
	Cloud onRamp								
	Network Hub								
٩	Tools >								
٠	Maintenance >								8
-	Administration								988
.6	, ·								96

- 2. Detach the IPS or IDS policy from the security policy as follows:
 - **a.** For the security policy that contains the IPS or IDS policy, click the **More Actions** icon to the far right of the policy and select **Edit**.

The Policy Summary page is displayed.

- b. Click the Intrusion Prevention tab.
- c. For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Detach**.
- d. Click Save Policy Changes.
- **3.** Delete the IPS or IDS policy as follows:
 - a. In the Security screen, click the Custom Options drop-down and select Intrusion Prevention.
 - **b.** For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Delete**.

A dialog box is displayed.

c. Click OK.

Monitor Intrusion Prevention Policy

You can monitor the Intrusion Prevention System (IPS) signature violations by severity and by count using the following steps.

To monitor the Signatures of IPS Configuration on IOS XE SD-WAN device:

1. From the Monitor > Network screen, select a device.

Cisco vManaj	E4										•	o 🎣	• mgg
		ex.											
 Auritur 👻	WAN - Edge Netwo	ork Hub Clusters											
Geography													000
Network	Device Group Al	· Q		Search Op	Rone 🛩								Total Rows: 6
	Hostname												
	O VINANASE	5.1.5.3	vManage	19049e90-9074-47ca-84c9-14799	0	reachable	500		4	18.4.1-5	28 Nov 2018 5 51:00 PM IST	"No proups"	23.3.37
Events	O VEMART	1.1.1.2	vSmart	4c25abb1 eax3-4345-b33a e6da07.	0	reachable	100		7	18.4.1-5	28 Nov 2018 6:54:00 PM IST	'No prosps'	23.3.37
	@ VBOND	5.5.5.2	vEripe Cloud (ville	1ao48747-0902-4e26-bc7a-0240e	•	reachable	100			18.4.1-5	28 Nov 2018 6:52:00 PM IST	"No groups"	20.007
	Cary-CSR	1.1.1.8	CSR3000+	CSR 99510x55-x565-450x 81424.	0	reachable	200	4	3	16.10.65	28 Nov 2018 10:20:00 PM IST	"No groups"	'U.U'
	O Durham CSR	1.1.1.6	CI981000w	CSR-c34127v1-415c-465e568272	0	reachable	290	4	3	16.10.65	28 Nov 2018 10:20:00 PM IST	"No groups"	20.0.01
	O Relation COR	1.1.1.4	C1981000w	CSR-(574)440-4407-4154-9903-a	0	reachable	190	4	3	16.10.65	28 Nov 2018 9:51.00 PM IST	'No prosps'	20.03
configuration >													

2. In the left panel, under Security Monitoring, select Intrusion Prevention tab. The Intrusion Prevention wizard displays.



3. Click By Severity or By Count to designate how you want to display intrusion prevention information.

Cisco vManage	<u>Q</u> [50	rch vManage				🦊 🖬 🤤 John (
Salest Device wetter 1 373 16	Security Monitoring: Intrusion Prevention	In Standard Device	todal action temporal v			
Sectorne man (172.16		te to, site to harne Dence h	NOCE. YEDGE ASKTOUT A			
vm16 « 172.16.255.26	Intrusion Prevention Displaying Intrusion Prevention Sy	rstern (IPS) signatures by severity and b	ay count			
Dashboard						
Application	•			F Rev	al Time 1h 🚮 6h 129	24h 7days Custom
DPI						
Flows	50					
Interface	20 CO	-				
WAN Performance					_	
Circuit Health (TLOC)	erc1-dent33	arc1-dear1	well-deat!	arob-dent3	arc11-dest12	sec11-dest10
Tunnel Health						
Security Monitoring	٩			Search Options 🖌		
Firewall						
Intrusion Prevention	Source	Destination	VPN	Viol	ation Count	
URL Filtering	sec 1	dest33	VPN 10	45		
Umbrella DNS Re-direct	src1	dest1	VPN 101	32		
	sec 3	dest1	VPN 23	12		
Control Connections	src6	dest3	VPN 1	09		
Hardware Health	src11	dest12	VPN 12	09		
Events	src11	dest10	VPN 10	45		
ACL Logs	src20	dest1	VPN 101	32		
Deal Time	src52	dest3	VPN 23	12		

Update IPS Signatures

IPS uses Cisco Talos signatures to monitor the network. Cisco recommends following this procedure to download the latest signatures.



Note

te To download the signatures, vManage requires access to the following domains using port 443:

- api.cisco.com
- cloudsso.cisco.com
- dl.cisco.com
- dl1.cisco.com
- dl2.cisco.com
- dl3.cisco.com
- In Cisco vManage, select the Administration > Settings tab in the left side panel to configure IPS Signature Update.
- 2. Click on Edit to Enable/Disable and provide your Cisco.com Username and Password details to save the Policy details as shown in the following screenshot.

ADMINISTRATION SETTINGS	Real of		
Call Home	Deadord	View Auto	-
Data Stream	Station	View 1 644	
Tenancy Mode	Tingle Server	View 1 Calif	
Statistics Configuration	Collection statevall 30 networks	Ven 1 Colt	
Maintenance Window	Net Colligent	t con	
Identity Provider Settings	Deabled	View 1 Perce	
Statistics Database Configuration	Maximum Available Space: 343.7218-98	Vote 1 mile	
Google Map API Key	Mage AM Key AludiyATP+2:dr78e45c5-delay005py/hr198	View 2 KdR	
Software Install Timeout	Culter, stare Interval 60 minutes	view 3 auto	
IPS Signature Update			
Control Deveload Control Deveload	N		368856