

Block Traffic Based on the EVE Threat Confidence Score

- About Encrypted Visibility Engine, on page 1
- Benefits, on page 1
- Sample Business Scenario, on page 1
- Prerequisites, on page 2
- High-Level Workflow, on page 2
- Configure Block Thresholds in EVE, on page 2
- Additional References, on page 6

About Encrypted Visibility Engine

You can use the Encrypted Visibility Engine (EVE) to identify client applications and processes using Transport Layer Security (TLS) encryption. EVE provides more visibility into the encrypted sessions without decryption. Based on EVE's findings, administrators can enforce policy actions on the traffic within their environments. You can also use the EVE to identify and stop malware.

Benefits

Administrators can leverage and adjust EVE's threat score to block malicious encrypted traffic. If the probability that the incoming traffic is malicious, then based on the threat score, you can configure EVE to block the connection.

Sample Business Scenario

A large corporate network uses Snort 3 as its primary intrusion detection and prevention system. In a rapidly evolving threat landscape, adoption of robust network security measures is necessary and important. The security team uses EVE to enhance encrypted traffic inspection without the need to implement full man-in-the-middle (MITM) decryption. The EVE technology uses fingerprints of known malicious processes to identify and stop malware. Network administrators must have the flexibility to configure EVE's block traffic thresholds to block potentially malicious connections, which are based on their configured block thresholds.

Prerequisites

- You must be running management center 7.4.0 or later, and the managed threat defense must also be 7.4.0 or later.
- Ensure that you have a valid Intrusion Prevention System (IPS) license and Snort 3 is the detection engine.

High-Level Workflow

- 1. EVE analyzes the incoming traffic and gives a verdict on the probability of incoming traffic being malware or not.
- 2. If EVE detects incoming traffic to be malware with a certain level of confidence, you can configure EVE to block that traffic.
- **3.** The packets are first checked for malware probability or threat score, and the threat score is compared with the block threshold that you have set.
- 4. If the threat score is higher than the configured threshold, EVE blocks the traffic.
- 5. If the threat score is lesser than the configured threshold, EVE takes no action.

Configure Block Thresholds in EVE

This procedure shows how to block potentially malicious traffic, based on the EVE threat confidence score of 90 percent or higher.

- Step 1 Choose Policies > Access Control.
- **Step 2** Click **Edit** (*I*) next to the access control policy you want to edit.
- Step 3 Choose Advanced Settings from the More drop-down arrow at the end of the packet flow line.
- **Step 4** Click **Edit** (*I*) next to **Encrypted Visibility Engine**.

wfx_automationPolicy123			Analyze 🗸 Discard Sav
Packets O Prefiter Rules O Decryption O Security Intelligence O Identity O Access Contr	rol O Advanced Settings		Targeted: 3 devic
normaly i oney		Ignore the VLAN header when tracking	No
Decryption Policy Settings	1	connections	NO
Decryption Policy to use for inspecting encrypted connections	None	Detection Enhancement Settings	/
		Adaptive Profiles	Enabled
TLS Server Identity Discovery	/	Adaptive Profiles - Enable profile updates	Disabled
Early application detection and URL categorization	Disabled		
		Performance Settings	1
Prefilter Policy Settings	/	Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet	5
Prefilter Policy used before access control	Default Prefilter Policy		
		Performance Statistics - Sample Time (seconds)	300
Network Analysis and Intrusion Policies	/	Regular Expression - Limit	Default Value
Intrusion Policy used before Access Control rule is determined	No Rules Active	Regular Expression - Recursion Limit	Default Value
Intrusion Policy Variable Set	Default-Set	Intrusion Event Logging Limits - Max Events Stored Per Packet	8
Default Network Analysis Policy Balan	nced Security and Connectivity		
		Latency-Based Performance Settings	1
Threat Defense Service Policy	/	Applied from Installed Rule Update	true
Threat Defense Service Rule(s)	0	Packet Handling	Disabled
Files and Malware Settings	/	Rule Handling	Enabled
Limit the number of bytes inspected when doing		Rule Handling - Threshold (microseconds)	512
file type detection	1460	Rule Handling - Consecutive Threshold Violations Before Suspending Rule	3
Allow file if cloud lookup for Block Malware takes longer than (seconds)	2	Rule Handling - Suspension Time (seconds)	10
Do not calculate SHA256 hash values for files larger than (in bytes)	10485760	Encrypted Visibility Engine	×,
Minimum file size for advanced file inspection and storage (bytes)	6144	Encrypted Visibility Engine	Disabled

Step 5In the Encrypted Visibility Engine page, enable the Encrypted Visibility Engine (EVE) toggle button.Step 6Enable the Block Traffic Based on EVE Score toggle button. Any incoming traffic that is a potential threat is blocked
by default.

Encrypted V	isibility Engin	е		0
This encrypted sessions without	ut decrypting the	EVE) uses machine m. To use this featu	0 1	vide insights into the encrypted a valid IPS license and feature
support is only Recommend	for Snort 3 devic	es. Learn more		~
 Enable autom 		uture Cisco Vulnera <.	ability Database	(VDB) releases.
Encrypted Vi	sibility Engine	(EVE)		
	r Application I assign client app	Detection Detections to process	ses.	
 Customiz 		/E Score for blocking traffic b	pased on the EV	
Adva	nced Mode			- Block
Very Low	Low	Medium	High	Very High
Revert to De	faults			Cancel OK

Note	2	<i>.</i>	reshold at which		1		n means: higher, EVE blocks th
					-		fidence, EVE takes no
			reshold for blocki he slider is set to	-	EVE threat co	onfidence. Thi	s ranges from Very Lo
End	crypted Visi	bility Engi	ne				0
Ab	out Encrypte	ed Visibility	Engine				
ses	sions without o	lecrypting the	(EVE) uses machine em. To use this featu ces. Learn more	• •	•		
Red	Recommended Settings						
	able automationable Cisco Suc		future Cisco Vulnera rk.	ability Database	(VDB) release	·S.	
Enc	crypted Visik	oility Engine	e (EVE)				
U	lse EVE for A	pplication	Detection				
А	llow EVE to as	sign client ap	plications to proces	ses.			
В	lock Traffic	Based on E	VE Score				
	Customize y	our threshold	for blocking traffic b	based on the E	/E scores.		
	Advance	ed Mode				- Block	
	Very Low	Low	Medium	High	Very Hig	Jh	
F	Revert to Defau	lts			Ca	ancel OK	

- **Step 8** For further granular control, enable the **Advanced Mode** toggle button. Now, you can assign a specific EVE Threat Confidence Score for blocking traffic. The default threshold is 99 percent.
- **Step 9** In this example, change the block threshold to **90** percent.
 - **Attention** As a best practice, we recommend that you do not set the block threshold to below 50 percent to ensure optimum performance.

Encrypted Vis	sibility Engine			0
This encrypted vi sessions without	, , ,	ses machine learning to pr se this feature, you require	0	,,
Recommende	d Settings			\sim
 <u>Enable</u> automat <u>Enable</u> Cisco Su 	· · · · · · · · · · · · · · · · · · ·	Sisco Vulnerability Databas	e (VDB) releases.	
Encrypted Visi	bility Engine (EVE)			
	Application Detect ssign client applicatior			
	Based on EVE Sco			
 Customize y Advance 		king traffic based on the E	Block From	90
0	25	50	75	100
Revert to Defa	ults		Canc	el OK

Step 10 Click OK.

Step 11 Click Save.

What to do next

Deploy configuration changes. See Deploy Configuration Changes.

View EVE Events

 Step 1
 To verify the block action, choose Analysis > Connections > Events. You can also view the events from the Unified Events viewer.

Step 2 If you have configured EVE to block traffic, the **Reason** field shows **Encrypted Visibility Block**.

2.	Source IP 172.16.77.1 ×	× Select						
Showing all 10 events (\$ 10) 🗜								
	Time	Action	Reason					
>	2023-01-10 14:22:33	Block	Encrypted Visibility Block					
>	2023-01-10 14:22:28	Block	Encrypted Visibility Block					
>	2023-01-10 14:22:25	Block	Encrypted Visibility Block					
>	2023-01-10 14:14:13	Block	Encrypted Visibility Block					
>	2023-01-10 14:14:10	Block	Encrypted Visibility Block					
>	2023-01-10 14:14:06	Block	Encrypted Visibility Block					
>	2023-01-10 14:12:40	Block	Encrypted Visibility Block					
>	2023-01-10 14:12:40	Allow						
>	2023-01-10 14:12:34	Block	Encrypted Visibility Block					
>	2023-01-10 14:12:34	Allow						

Step 3The following is an example of the Encrypted Visibility Process Name as test_malware, Encrypted Visibility Threat
Confidence as Very High, and Encrypted Visibility Threat Confidence Score as 90 percent.

Qx Source IP 172.16.77.1 × × Select × Refree Ø Showing all 10 events (5, 10) ± ■ Ø Source IP Ø Source IP Ø Source IP								
	Time	b Application	URL	Encrypted Visibility Fingerprint	Encrypted Visibility Process Confidence Score	Encrypted Visibility Process Name	Encrypted Visibility Threat Confidence	Encrypted Visibility Threat Confidence Score
>	2023-01-10 14:22:33			tis/(0303)(1302130313)	90%	test_malware	Very High	90%
>	2023-01-10 14:22:28			tis/(0303)(1302130313)	90%	test_malware	Very High	90%
>	2023-01-10 14:22:25	-		tis/(0303)(130213031)	90%	test_malware	Very High	90%
>	2023-01-10 14:14:13			@ tls/(0303)(1302130313	90%	test_malware	Very High	90%

Additional References

For detailed conceptual information, see the Encrypted Visibility Engine for Snort 3 chapter in this guide or the content in the following link:

Encrypted Visibility Engine