



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.

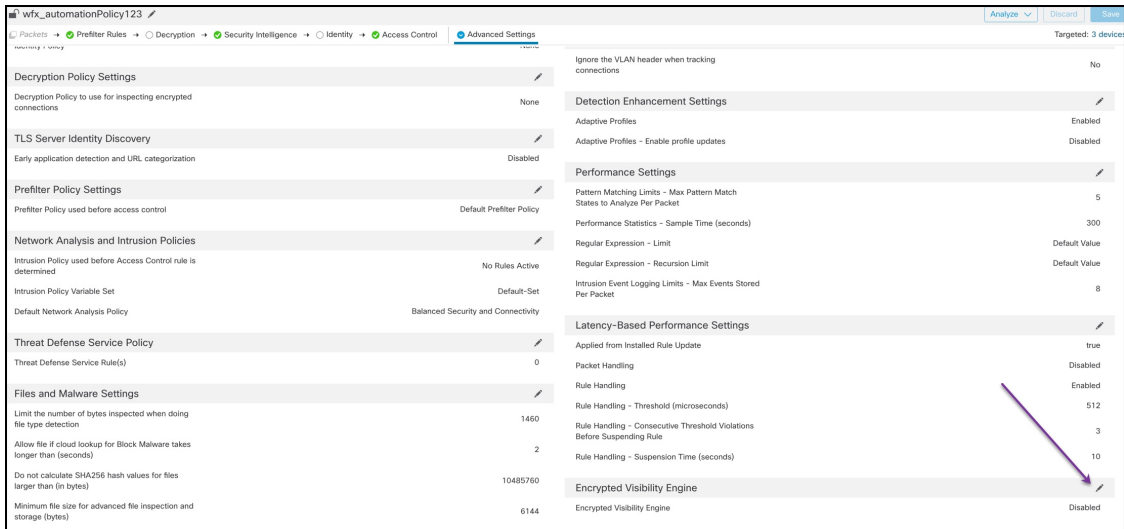
High-Level Workflow

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** (✎) 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** (✎) next to **Encrypted Visibility Engine**.



Step 5
Step 6

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

Encrypted Visibility Engine ?

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. [Learn more](#)

Recommended Settings v

- [Enable](#) automatic updates for future Cisco Vulnerability Database (VDB) releases.
- [Enable](#) Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

i Customize your threshold for blocking traffic based on the EVE scores.

i **Advanced Mode** - Block

Very Low Low Medium High Very High

Revert to Defaults Cancel OK

- Note** By default, the threshold at which malware is blocked is 99 percent, which means:
- If EVE detects the traffic to be malware with 99 percent confidence or higher, EVE blocks the traffic.
 - If EVE detects the traffic to be malware with less than 99 percent confidence, EVE takes no action.

Step 7 Use the slider to adjust the threshold for blocking based on EVE threat confidence. This ranges from **Very Low** to **Very High**. In this example, the slider is set to **Very High**.

Encrypted Visibility Engine ?

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. [Learn more](#)

Recommended Settings v

- [Enable](#) automatic updates for future Cisco Vulnerability Database (VDB) releases.
- [Enable](#) Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

i Customize your threshold for blocking traffic based on the EVE scores.

i **Advanced Mode**

— Block

Very Low Low Medium High Very High

Revert to Defaults
Cancel
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 Visibility Engine ?

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. [Learn more](#)

Recommended Settings v

- [Enable](#) automatic updates for future Cisco Vulnerability Database (VDB) releases.
- [Enable](#) Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

i Customize your threshold for blocking traffic based on the EVE scores.

i **Advanced Mode** **Block From**

0 25 50 75 100

Revert to Defaults
Cancel
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**.

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 3 The 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.

Time	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			tls/(0303)(130213031:	90%	test_malware	Very High	90%
2023-01-10 14:22:28			tls/(0303)(130213031:	90%	test_malware	Very High	90%
2023-01-10 14:22:25			tls/(0303)(130213031:	90%	test_malware	Very High	90%
2023-01-10 14:14:13			tls/(0303)(130213031:	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](#)