Encrypted Visibility Engine

Encrypted Visibility Engine (EVE) is used to identify client applications and processes utilizing TLS encryption. It enables visibility and allows administrators to take actions and enforce policy within their environments. The EVE technology can also be used to identify and stop malware.

Overview of Encrypted Visibility Engine

The encrypted visibility engine (EVE) is used to provide more visibility into the encrypted sessions without the need to decrypt them. These insights into encrypted sessions are obtained by Cisco's open-source library that is packaged in Cisco's vulnerability database (VDB). The library fingerprints and analyzes incoming encrypted sessions and matches it against a set of known fingerprints. This database of known fingerprints is also available in the Cisco VDB.

Note The encrypted visibility engine feature is supported only on management center-managed devices running Snort 3. This feature is not supported on Snort 2 devices, device manager-managed devices, or CDO.

Some of the important features of EVE are the following:

- You can take access control policy actions on the traffic using information derived from EVE.
- The VDB included in Cisco Secure Firewall has the ability to assign applications to some processes detected by EVE with a high confidence value. Alternatively, you can create custom application detectors to:
  - Map EVE-detected processes to new user-defined applications.
  - Override the built-in value of process confidence that is used to assign applications to EVE-detected processes.

See the **Configuring Custom Application Detectors** and **Specifying EVE Process Assignments** sections in the **Application Detection** chapter of the Cisco Secure Firewall Management Center Device Configuration Guide.

- EVE can detect the operating system type and version of the client that created a Client Hello packet in the encrypted traffic.
- EVE supports fingerprinting and analysis of Quick UDP Internet Connections (QUIC) traffic too. The server name from the Client Hello packet is displayed in the URL field of the **Connection Events** page.

Attention To use EVE on management center, you must have a valid IPS license on your device. In the absence of a IPS license, the policy displays a warning and deployment is not allowed.

Note EVE can detect the operating system type and version of SSL sessions. Normal usage of the operating system, such as running applications and package management software, can trigger OS detection. To view client OS detection, in addition to enabling the EVE toggle button, you must enable **Hosts** under **Policies** > **Network Discovery**. To view a list of possible operating systems on the host IP address, click **Analysis** > **Hosts** > **Network Map**, and then choose the required host.

Related Links

Configure EVE, on page 3

Configure EVE Exception Rules, on page 6

How EVE Works

The Encrypted Visibility Engine (EVE) inspects the Client Hello portion of the TLS handshake to identify client processes. The Client Hello is the initial data packet that is sent to the server. This gives a good indication of the client process on the host. This fingerprint, combined with other data such as destination IP address, provides the basis for EVE’s application identification. By identifying specific application fingerprints in the TLS session establishment, the system can identify the client process and take appropriate action (allow/block).

EVE can identify over 5,000 client processes. The system maps a number of these processes to client applications for use as criteria in access control rules. This gives the system the ability to identify and control these applications without enabling TLS decryption. By using fingerprints of known malicious processes, EVE technology can also be used to identify and block encrypted malicious traffic without outbound decryption.

Through machine learning (ML) technology, Cisco processes over one billion TLS fingerprints and over 10000 malware samples daily to create and update EVE fingerprints. These updates are then delivered to customers using Cisco Vulnerability Database (VDB) package.

If EVE does not recognize a fingerprint, it identifies client application and estimates the threat score of the first flow using the destination details, such as IP address, port, and server name. At this point, the status of the fingerprints are randomized and the status can be viewed in the debug logs. For subsequent flows with the same fingerprint, EVE skips reanalysis and marks the fingerprint status as unlabeled. If you intend to block traffic based on EVE's Low or Very Low score thresholds, the initial flow is blocked. However, future flows will be allowed once the application's fingerprint is cached.

Indications of Compromise Events

The host's Indications of Compromise (IoC) events for encrypted visibility engine detection allows you to check connection events with a very high malware confidence level, as reported by EVE. IoC events are triggered for encrypted sessions generated from a host using a malicious client. You can view information, such as IP address, MAC address, and OS information of the malicious host, and the timestamp of the suspicious activity.

A session with Encrypted Visibility Threat Confidence score 'Very High' as seen in connection events genreates an IoC event. You must enable **Hosts** from **Policies** > **Network Discovery**. In the management center, you can view the IoC event existence from:

- **Analysis** > **Indications of Compromise**.
- **Analysis** > **Network Map** > **Indications of Compromise** > Choose the host that must be checked.

  You can view the process information of the session that generated the IoC from:

  Analysis > **Connection Events** > **Table View of Connection Events** > **IoC** column. Note that you must manually select the Encrypted Visbility fields and IoC field.

QUIC Fingerprinting in EVE

Snort can identify client applications in Quick UDP Internet Connections (QUIC sessions) based on EVE. QUIC fingerprinting can:

- Detect applications over QUIC without enabling decryption.
- Identify malware without enabling decryption.
- Detect service applications. You can assign access control rules based on the service detected over the QUIC protocol.

Configure EVE

Procedure

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 In the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 6 **Use EVE for Application Detection**—This toggle button is enabled by default, which means that EVE is allowed to assign client applications to processes.

EVE's fingerprint information is added in the **Encrypted Visibility Fingerprint** column header of the connection events or unified events. For further analysis of the EVE data collected, you can right-click the fingerprint information to open a dropdown menu. In the menu, click **View Encrypted Visibility Engine Process Analysis** to go to appid.cisco.com and view details, such as the fingerprint, VDB version, and so on. Different rows with the same fingerprint string and potential process names associated with them and their prevalence are displayed. Prevalence indicates the frequency of a process associated with a particular fingerprint in the data collection system. You can choose the process names and click **Submit Request** to give feedback about any discrepancy in EVE's process detection. For example, you can submit requests if the process name that is detected does not match with the traffic that is being sent or if the process name is not detected at all for a particular fingerprint.

If you disable the **Use EVE for Application Detection** toggle button:

- AppID-identified clients are assigned to processes and you can see the EVE process and score, but there is no mapping of EVE-detected processes to applications and no action is taken. You can see the details of the events under **Connection Events** or **Unified Events**. To see the difference in connection events (with and without application assignment), see the **Client Application** column header.
- The **Encrypted Visibility Fingerprint** field in the connection events or unified events is empty.

Step 7 Enable the **Block Traffic Based on EVE Score** toggle button to block traffic based on EVE's threat confidence score. Any incoming traffic that is a potential threat is blocked by default.

The default block threshold is 99 percent, which means:

- If EVE detects the traffic to be malware with 99 percent confidence or more, the traffic is blocked.
- If EVE detects the traffic to be malware with less than 99 percent confidence, EVE takes no action.

Note If EVE has blocked the traffic, in the **Connection Events** page, the **Reason** column header displays **Encrypted Visiblity Block**.

Step 8 Use the slider to adjust the threshold for blocking based on EVE's threat confidence, which ranges from **Very Low** to **Very High**.

Step 9 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 block threshold is 99 percent.

Caution We recommend that you do not set a threshold below 50 percent to ensure optimal performance.

Step 10 Click **OK**.

Step 11 Click **Save**.

What to do next

Deploy configuration changes.

View EVE Events

After enabling the **Encrypted Visibility Engine** and deploying your access control policy, you can start sending live traffic through your system. You can view the logged connection events in the **Connection Events** page. To access the connection events, in the management center:

Procedure

Step 1 Click **Analysis** > **Connections** > **Events**.

Step 2 Click the **Table View of Connection Events** tab.

You can also view the connection event fields in the **Unified Events** viewer, which is under the **Analysis** menu.

Encrypted Visibility Engine can identify the client process that initiated a connection, the OS on the client, and if the process contains malware or not.

Step 3 In the **Connection Events** page, view the following columns that are added for Encrypted Visibility Engine. Note that you must explicitly enable the mentioned columns.

- Encrypted Visibility Process Name
- Encrypted Visibility Process Confidence Score
- Encrypted Visibility Threat Confidence
- Encrypted Visibility Threat Confidence Score
- Detection Type

For information about these fields, see the section **Connection and Security Intelligence Event Fields** in the **Connection and Security-Related Connection Events** chapter of the Cisco Secure Firewall Management Center Administration Guide.

Note In the **Connection Events** page, if processes are assigned applications, the **Detection Type** column displays **Encrypted Visibility Engine** indicating that the client application was identified by EVE. Without application assignments to process names, the **Detection Type** column displays **AppID** indicating that the engine that identified the client application was AppID.

View EVE Dashboard

You can view the EVE analysis information in two dashboards. To access the dashboards:

Procedure

Step 1 Under **Overview** > **Dashboards**, click **Dashboard**.

Step 2 In the **Summary Dashboard** window, click the **switch dashboard** link and choose **Application Statistics** from the dropdown box.

Step 3 Choose the **Encrypted Visibility Engine** tab to view the following two dashboards:

- **Top Encrypted Visibility Engine Discovered Processes**—Displays the top TLS process names being used in your network and the connection count. You can click the process name in the table to see the filtered view of the **Connection Events** page, which is filtered by the process name.

- **Connections by Encrypted Visibility Engine Threat Confidence**—Displays the connections by the confidence levels (Very High, Very Low, and so on). You can click the Threat confidence level in the table to see the filtered view of the **Connection Events** page, which is filtered by the confidence level.

Configure EVE Exception Rules

You can create an encrypted visibility engine (EVE) exception list to ensure the continuity of connections and services when EVE’s block feature is enabled. It allows you to bypass EVE’s verdict for blocking a connection, based on the process names and destination IP address attributes. For example, you may want to bypass EVE's block verdict for trusted networks. All the connections in the bypassed networks are exempted from EVE’s block verdict based on the threat score.

Procedure

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 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 6 Enable the **Block Traffic Based on EVE Score** toggle button to block traffic based on EVE's threat confidence score.

Step 7 Click **Add Exception Rule** to create exception rules based on the destination network, EVE's process names, or both.

Step 8 In the **Add EVE Exception Rule** page, click the **Network Objects** tab and choose the required network objects from the list.

Step 9 Click **>** to add your chosen network objects to **Selected Networks** on the right side of the window.

You can also use the **Manually Enter IP** field to manually enter the destination IP address and add it to the list of selected networks.

Step 10 (Optional) In the **Comment** field, you can enter a comment for adding the exception rule.

Step 11 Click the **Process Name** tab.

Step 12 In the **Process Name** field, enter an EVE-identified process name.

Note EVE exception based on process names works only with EVE-identified process names, which are case- and space-sensitive.

Step 13 Click **Add to Process** on the right side of the window.

You can add multiple process names to the same exception rule.

Step 14 Click **Save**.

Step 15 Click **OK**.

Step 16 Save and deploy your policy.

Note When a connection matches an exception rule, it bypasses the EVE's block verdict. You can view EVE's action in the **Unified Events** viewer. The **Reason** column header displays **EVE Exempted** for identification of such EVE-bypassed traffic.

Add Exception Rule from Unified Events

You can use the **Unified Events** window to add exception rules for connections that are blocked by EVE.

Procedure

Step 1 Click **Analysis** > **Unified Events**.

Step 2 In the **Reason** column with **Encrypted Visibility Block** as the reason, click the ellipsis icon (three vertical dots) inside the cell.

Step 3 Choose **Add EVE Exception Rule** from the drop-down list.

Step 4 In the **Encrypted Visibility Engine** window that is displayed, the rule is automatically added to the bottom of the exception list. You can review and make changes to the added rule before saving and deploying the configuration.

Event Enrichment

Context enrichment for MITRE ATT&CK occurs from the Talos taxonomy and the encrypted visibility engine (EVE). Both Talos and EVE enrichments are communicated using the Talos taxonomy. EVE enrichment works when EVE is enabled. For more information about enabling EVE, see Configure EVE, on page 3.

On the **Connection Events** page, you can view the following column headers that are added as part of enriched eventing content. You must explicitly enable these columns.

- **MITRE ATT&CK**
- **Other Enrichment**

For information about these fields, see the section Connection and Security Intelligence Event Fields in the Connection and Security-Related Connection Events chapter of the Cisco Secure Firewall Management Center Administration Guide, 7.6.