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 Firewall Management Center-managed devices running Snort 3. This feature is not supported on Snort 2 devices and Firewall Device Manager-managed devices.

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 Firewall 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 **Events & Logs** > **Hosts** > **Network Map**, and then choose the required host.
- After enabling EVE for your access control policy, ensure that you have turned on logging for the access control rules within that policy to display the expected results on the EVE dashboard whenever any specific rule conditions are met. For more information on how to turn on logging, see Create and Edit Access Control Rules.
- EVE will not provide visibility or insights for encapsulated traffic.

Related Links

Configure EVE, on page 4

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** > **+ Show more** > **Advanced** > **Network Discovery**. In the Firewall Management Center, you can view the IoC event existence from:

- **Events & Logs** > **+ Show more** > **Hosts** > **Indications of Compromise**, and then **Analysis** > **Indications of Compromise**.
- **Events & Logs** > **Hosts** > **Network Map** > Choose the host that must be checked.

  You can view the process information of the session that generated the IoC on the **Connection Events** page. Click **Events & Logs** > **+ Show more** > **Connection** > **Events** to access the **Connection Events** page. Note that you must manually select the Encrypted Visibility fields and IoC field from the **Table View of Connection Events** tab.

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** > **Security 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 **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 the Secure Firewall Application Detectors site 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.

Access to view additional details on the Secure Firewall Application Detectors page is currently not available to users with non-Cisco email addresses.

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 Malware Processes Based on Threat Confidence Level** toggle button to block malicious client processes with the prefix *malware_* based on EVE's threat confidence level.

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, the **Reason** column header on the **Connection Events** page 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 Level 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 Encrypted Visibility Engine 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 **Unified Events** page.

Perform this procedure to access the connection events in the Firewall Management Center.

Procedure

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

The Encrypted Visibility Engine can identify the client process that initiated a connection and the operating system in the client, and indicate if the process contains malware or not.

Step 2 In the **Unified Events** page, explicitly enable these columns that are added for the Encrypted Visibility Engine:

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

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

Note
On 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 the Encrypted Visibility Engine. 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 the following dashboards:

Before you begin

- In an access control policy, the **Encrypted Visibility Engine (EVE)** must be enabled under **Advanced Settings**.
- To view the **Connections with Detected Process Names** and **Malicious Processes** widgets, the devices must be running Firewall Threat Defense Version 7.7 or later.

Procedure

Step 1 Go to **Insights & Reports** > **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 top client processes 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 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

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

Step 3 Choose **Encrypted Visibility Engine** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 5 Choose the **Monitor** mode or the **Protect** mode.

- Choose the **Monitor** mode to detect client applications and monitor encrypted traffic.
- Choose the **Protect** mode to monitor and block encrypted traffic based on the threat confidence level of the client processes. You can use this mode to monitor and block malicious connections at two threat confidence levels:
  - **High**: Use this level to block connections with threat confidence levels ranging from High to Very High.
  - **Very High**: Use this level to block connections with threat confidence levels that are categorized as Very High.

Step 6 Click **Save** and then deploy the access control policy.

Note
To manage exceptions, see Configure EVE Exception Rules, on page 9.

What to do next

Deploy configuration changes.

View Encrypted Visibility Engine 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 **Unified Events** page.

Perform this procedure to access the connection events in the Firewall Management Center.

Procedure

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

The Encrypted Visibility Engine can identify the client process that initiated a connection and the operating system in the client, and indicate if the process contains malware or not.

Step 2 In the **Unified Events** page, explicitly enable these columns that are added for the Encrypted Visibility Engine:

- **Encrypted Visibility Process Name**
- **Encrypted Visibility Process Confidence Score**
- **Encrypted Visibility Threat Confidence**
- **Encrypted Visibility Threat Confidence Score**

- **Detection Type**
- **EVE Process Name**
- **EVE Process Confidence Score**
- **EVE Threat Confidence**
- **EVE Threat Confidence Score**
- **Detection Type**

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

Note
On 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 the Encrypted Visibility Engine. Without application assignments to process names, the **Detection Type** column displays **AppID**, indicating that the engine that identified the client application was AppID.

Configure EVE Exception Rules

You can create an encrypted visibility engine (EVE) exception rule to ensure the continuity of trusted connections and services by bypassing the EVE's block action. You can add attributes such as process names and destination IP address to the exception rule. 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 confidence level.

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

Step 3 From the **More** drop-down arrow at the end of the packet flow line, choose **Advanced Settings**.

Step 4 Next to **Encrypted Visibility Engine (EVE)**, click **Edit** (✎).

Step 5 On the **Encrypted Visibility Engine** page, click the **Encrypted Visibility Engine (EVE)** toggle button to enable EVE.

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

Step 7 Click **Add Exception Rule** and add one or more of the following attributes.

a) Under the **Process Name** tab, enter an EVE-identified process name, and click **Add to Process** on the right side of the window.

You can add multiple process names to the same exception rule. EVE exception list based on process names works only with EVE-identified process names, which are case- and space-sensitive.

b) Under the **Network Objects** tab, perform one of the following:

- Choose one or more IP addresses from the list and add to the **Selected Networks** list.
- Under **Selected Networks**, manually enter the IP address and click the + icon to add it to the list of selected networks.

c) (Optional) In the **Comment** field available on all the tabs, you can enter a reason for adding the required attributes to the EVE exception rule.

Step 8 Click **Save** to save the EVE exception rule.

Step 9 Save and deploy the access control policy on the devices.

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

Add Exception Rule from Unified Events

Use the **Unified Events** page to add exception rules for connections that are blocked by EVE. The Firewall Management Center adds an exception rule to the **Encrypted Visibility Engine (EVE) exception list** object. Note that the exception rules added to this list are applicable for all the access control policies that have EVE enabled.

Before you begin

Exception list is supported only from threat defense Version 7.6.0 or later.

Procedure

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

Step 2 In the **Reason** column with **Encrypted Visibility Block** as the reason, click the **Ellipsis**( ) icon 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.

Configure EVE Exception Rules

You can create an encrypted visibility engine (EVE) exception rule to ensure the continuity of trusted connections and services by bypassing the EVE’s block action. You can add attributes such as process names

and destination IP address to the exception rule. 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 confidence level.

Procedure

Step 1 Choose **Policies** > **Security policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to the access control policy you want to edit.

Step 3 Choose **Encrypted Visibility Engine** from the **More** drop-down arrow at the end of the packet flow line.

Step 4 On the **Encrypted Visibility Engine** page, enable the **Encrypted Visibility Engine (EVE)** toggle button.

Step 5 Choose the **Protect** mode to monitor and block encrypted traffic based on the threat confidence level of the client processes. You can use this mode to monitor and block malicious connections at two threat confidence levels:

- **High**: Use this level to block connections with threat confidence levels ranging from High to Very High.
- **Very High**: Use this level to block connections with threat confidence levels that are categorized as Very High.

Step 6 Click **Manage exceptions** to view and add exception rules.

Step 7 On the **Encrypted Visibility Engine (EVE) Exception List** window, click **+Add Exception Rules** and add the required attributes.

a) Under the **Process Name** tab, enter an EVE-identified process name, and click **+Add** on the right side of the window.

You can add multiple process names to the same exception rule. EVE exception list based on process names works only with EVE-identified process names, which are case- and space-sensitive.

b) Under the **Network Objects** tab, perform one of the following:

- Choose one or more network objects from the **Available Networks** list and add the same to the **Selected Source Network** or **Selected Destination Network** list.
- To create a new network object, click **+Create Network Object**.
  1. Enter a **Name** and an optional **Description**.
  2. Choose the required network type - **Host, Range, Network, or FQDN**. Enter the relevant IP address if you choose **Host, Range, or Network**. If you choose **FQDN**, enter the fully Qualified Domain Name(**FQDN**) and choose the required option from the **Lookup** drop-down list.
  3. If you want to allow configuration overrides, check the **Allow overrides** checkbox.
  4. Click **Add**.

c) To create a new dynamic attribute, click **+Create Dynamic Attribute.**

1. Enter a **Name** and an optional **Description**.
2. Click **Add**. You can configure this object using Cisco Secure Dynamic Attribute Connector (CSDAC) or Management Center APIs.

d) (Optional) In the **Comment** field available on all the tabs, you can enter a reason for adding the required network objects and dynamic attributes to the EVE exception rule.

Step 8 Click **Save** and then deploy the access control policy.

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

Add Exception Rule from Unified Events

Use the **Unified Events** page to add exception rules for connections that are blocked by EVE. The Firewall Management Center adds an exception rule to the **Encrypted Visibility Engine (EVE) exception list** object. Note that the exception rules added to this list are applicable for all the access control policies that have EVE enabled.

Before you begin

Exception list is supported only from threat defense Version 7.6.0 or later.

Procedure

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

Step 2 In the **Reason** column with **Encrypted Visibility Block** as the reason, click the **Ellipsis**( ) icon 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.

Upgrade EVE Exception Rules

On Secure Firewall version 7.7 and earlier, EVE exception rules are configured for each policy separately. From Secure Firewall version 10.0.0, the EVE exception list is part of the global domain. As a result, the EVE exception rules are configured in the global domain and applied to all the policies on which EVE is enabled to block traffic.

When you are upgrading the Management Center from version 7.7 to 10.0.0, all the EVE exception rules from the leaf domains that contain leaf domain network objects are identified and stored. After the upgrade is complete:

- All EVE exception rules from global domain policies, as well as rules from leaf domain policies that reference global domain objects or inline IP addresses, are consolidated into a single global EVE exception

list. As a result, some policies may now include EVE exception rules that were not present before the upgrade.

- All policies that contain EVE exception rules are marked as out-of-date.

If the exception rules from leaf domains contain leaf domain network or dynamic objects, these rules are removed during the upgrade process. The upgrade script log file has a log of all the merged and deleted exception rules, along with the corresponding access control policy and domain from which each rule originated. The log file is located at */var/log/sf/Cisco_Secure_FW_Mgmt_Center_Upgrade10.0.0/800_post/1114_eve_rules.pl.log*.

When you deploy the configuration for the first time after the upgrade, a warning message on the Management Center lists all the deleted EVE exception rules. The warning message also states that there could be possible traffic impact if the rules are not reconfigured in the global EVE exception list. Note that the warning message appears only when you deploy the configuration for the first time after the upgrade is complete.

For Secure Firewall devices running version 7.7 and earlier that are mapped to Management Center running version 10.0.0, only **Very High** threat confidence connection events are sent to the **Security-Related Connection Events** table. For Secure Firewall devices running version 10.0.0, EVE **Blocked** and **Medium+** EVE threat confidence connection events are sent to the **Security-Related Connection Events** table.

Change Management Support during EVE Upgrade

When you upgrade the Management Center to version 10.0.0, all active change management tickets that contain access control policies on which EVE is enabled will have their EVE exception rules automatically merged with the global EVE exception list.

The merging of EVE exception rules with the global EVE exception list occurs regardless of the ticket's approval state. This ensures that no exception rules are lost during the upgrade.

EVE Ticket Preview Generation Behavior

If a change management ticket contains a policy that is locked and it contains only EVE-related modifications, such as EVE settings or exception rules, the EVE ticket preview will not be automatically regenerated after the upgrade. If the ticket contains other policy modifications in addition to EVE-related modifications, the EVE ticket preview will be generated normally.