FMC Correlation Policy Allow List Events Require Network Discovery Policy to be Enabled

Contents

Issue

When configuring correlation policies with allow lists on Cisco Secure Firewall Management Center (FMC), it is important to note that **Allow List Events** and **Allow List Violations** are not generated unless the **Network Discovery Policy** is configured for the **Target Network** IP. Without this configuration, no events appear under **Analysis > Correlation > Allow List Events** and **Analysis > Correlation > Allow List Violations**.

During laboratory testing, these behaviors were observed:

- Correlation events are generated correctly for the configured target network.
- No **Allow List Events** or **Allow List Violations** are generated when the **Target Network** host becomes non-compliant.

Environment

- Cisco Firepower Threat Defense (FTD) managed by Secure Firewall Management Center (FMC)
- Correlation policy configured with allow list targeting specific IP addresses
- Allow list configured to permit a specific web application, application, or protocol

Resolution

After extensive lab testing and consultation with the development team, it was confirmed that **Network Discovery** policy must be enabled as a prerequisite for **Allow List Events** and **Allow List Violations** to be generated.

The resolution involves these steps:

Step 1: Enable Network Discovery Policy

Navigate to **Policies > Network Discovery** in the FMC interface and create a rule if none exists.

Step 2: Configure Network Discovery Rule

Configure the network discovery rule with the appropriate source network settings:

- Specify the source network as your internal network range.
- Alternatively, use all networks (0.0.0.0/0) if monitoring all traffic sources.
- Ensure the rule covers the networks from which you are expecting to generate **Allow List Events**.

Step 3: Activate Correlation Policy Rules

Verify that the correlation policy rules are active and not in a disabled state.

Step 4: Verify Allow List Event Generation

After enabling network discovery and activating the correlation policy rules:

1.- Access websites from the configured Target Network using a browser(making the host as non-compliant).

2.- Monitor **Analysis > Correlation > Allow List Events** and **Analysis > Correlation > Allow List Violations** for event generation.

3.- Verify that events are populated when host is going non-compliant.

Laboratory testing confirmed that once **Network Discovery** is enabled, **Allow List Events** and the **Allow List Violations** are successfully generated for a non-compliant host.

Cause

The root cause is that **Network Discovery Policy** is a mandatory prerequisite for generating **Allow List Events** in **FMC Correlation Policies**. Without an active **Network Discovery Policy**, the system cannot properly evaluate host compliance against configured **Allow List**, resulting in no **Allow List Events** being generated when the **Target Network** host becomes non-compliant.

Related Content

- Cisco FMC Correlation Compliance Lists Documentation
- Cisco Technical Support & Downloads