# Introduction



# Overview

This guide explains how to configure Cisco Security Analytics and Logging (On Premises) to store your Firewall event data for increased storage at a larger retention period. By deploying Cisco Secure Network Analytics (formerly Stealthwatch) appliances, and integrating them with your Firewall deployment, you can export your event data to a Secure Network Analytics appliance.

You can then:

- Store events on the Firepower Management Center (FMC) and events on the Secure Network Analytics deployment.
- Specify this remote data source to view these events in the FMC.
- Review your event data from the Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) Web App UI using the Event Viewer.
- Cross-launch from the FMC UI to the Event Viewer to view additional context on the information from which you cross-launched.

**Note** If you want to store Firewall event data in the Cisco cloud, as opposed to on-premises, see the Cisco Security Analytics and Logging (SaaS) documentation for more information.

## Supported Event Types

- FTD Security Events
  - Connection
  - Intrusion
  - File and Malware
- FTD Data Plane Events (Multi-node deployment only)

- ASA Events (Multi-node deployment only)

# Concepts and Architecture

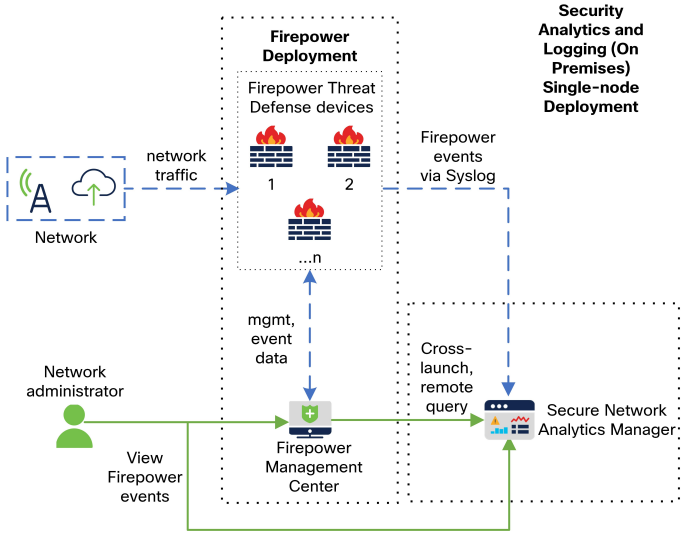
In a Security Analytics and Logging (OnPrem) deployment, you can use a Secure Network Analytics appliance to store data from another Cisco product deployment, such as a Firepower appliance deployment. In the case of the Firepower deployment, you can export your Firepower Security Events and data plane events from your Firepower Threat Defense devices managed by a Firepower Management Center to a Manager to store that information. In the Security Analytics and Logging (OnPrem) app v3.0.0, we added the ability to export events from your ASA devices via syslog to a Manager.

You have two options for Secure Network Analytics deployment:

- Single-node - Deploy a standalone Manager to receive and store events, and from which you can review and query events
- Multi-node - Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Cisco Secure Network Analytics Data Store (containing 3 Cisco Secure Network Analytics Data Nodes) to store events, and a Manager from which you can review and query events

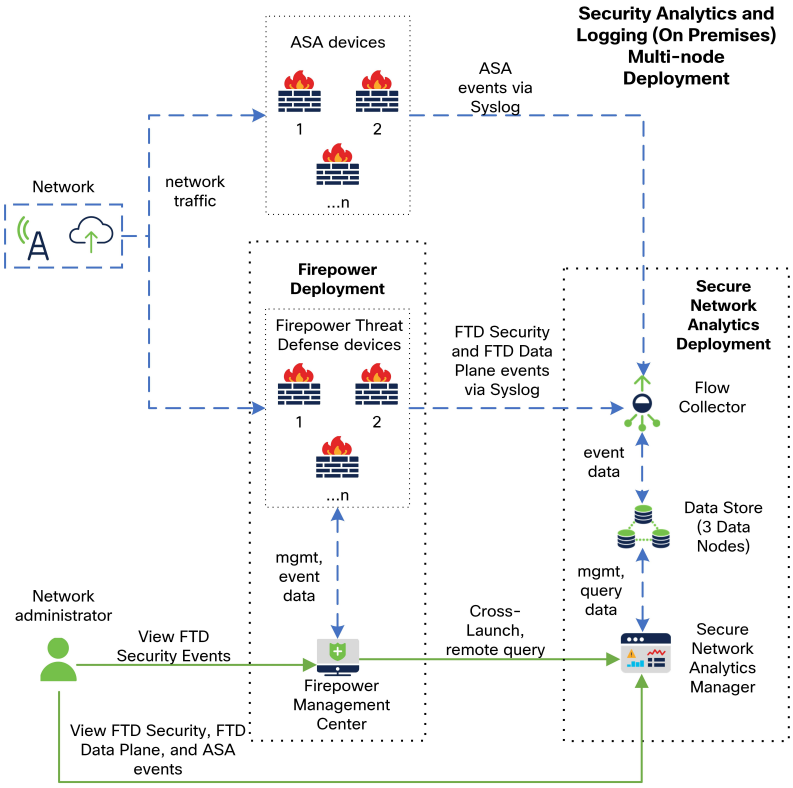
**Note** We support installing the app on an Manager as a standalone appliance (Single-node), or an Manager that manages a Flow Collector and 3 Data Nodes (Multi-node). You cannot install the app on an Manager if it manages one or more Flow Collectors without managing 3 Data Nodes. See Troubleshooting for more information.

See the following diagram for an example of a Single-node deployment with a Manager:




In this deployment, the Firepower Threat Defense devices send Firepower events to the Manager, and the Manager stores these events. From the Firepower Management Center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the Firepower Management Center.

See the following diagram for an example of a Multi-node deployment with a Manager, 3 Data Nodes, and a Flow Collector:




In this deployment, the Firepower Threat Defense and ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store (3 Data Nodes) for storage. From the Firepower Management Center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the Firepower Management Center.