# 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 Secure Firewall Management Center and events on the Secure Network Analytics deployment.
- Specify this remote data source to view these events in the management center.
- 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 management center 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.

## 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. In the case of the Secure Firewall deployment, you can export your Security Events and data plane events from your Secure Firewall Threat Defense devices managed by the management center to a Manager to store that information.

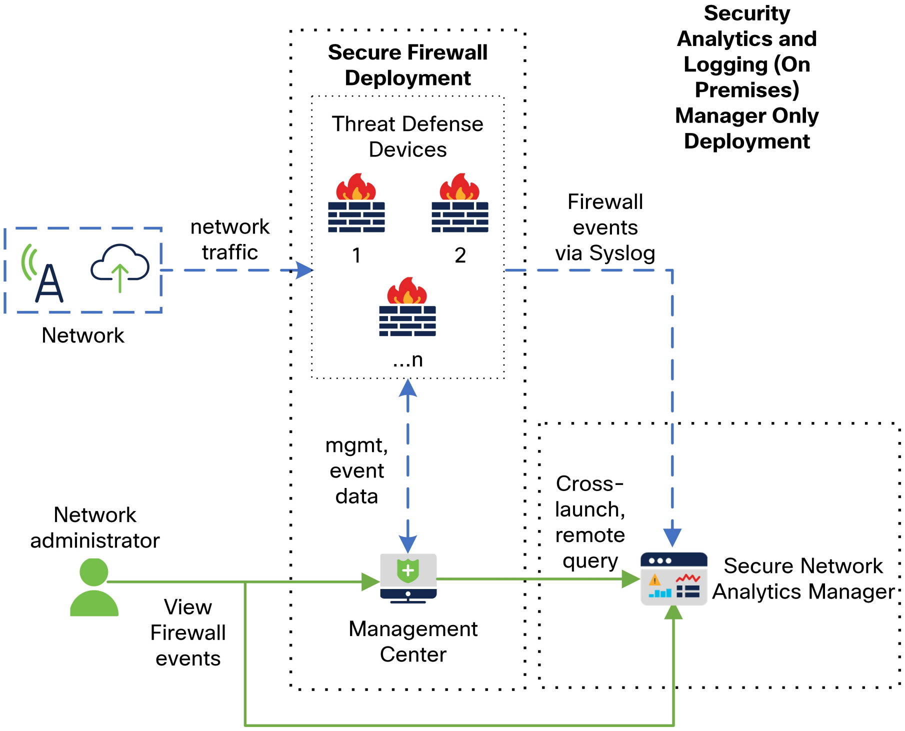
You have two options for Secure Network Analytics deployment:

- Manager only - Deploy a standalone Manager to receive and store events, and from which you can review and query events

- Data Store - Deploy Cisco Secure Network Analytics Flow Collectors (up to 5) to receive events, a Cisco Secure Network Analytics Data Store containing 1, 3, or more (in sets of 3) Cisco Secure Network Analytics Data Nodes to store events, and a Manager from which you can review and query events

### Manager Only

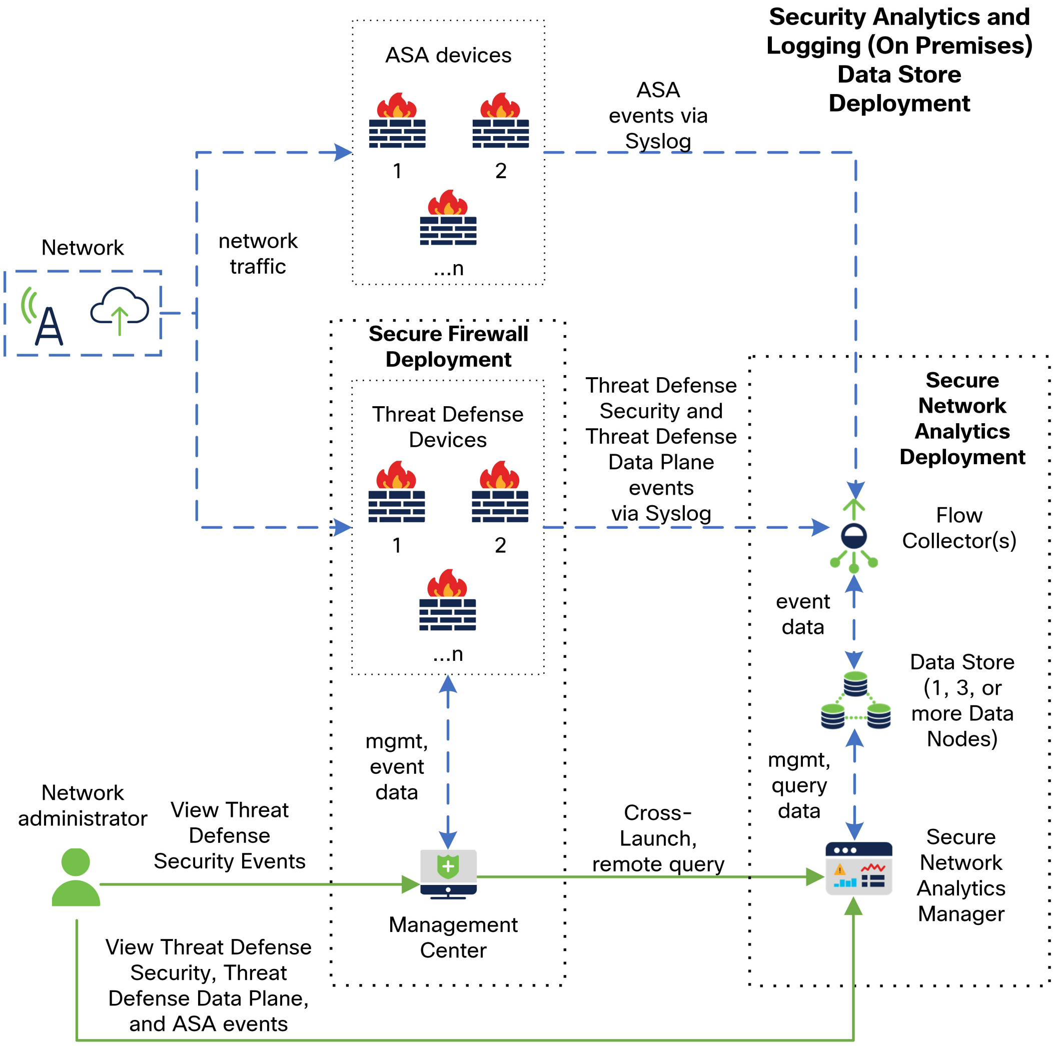
See the following diagram for an example of a Manager only deployment:


Secure Firewall Deployment
Security Analytics and Logging (On Premises) Manager Only Deployment
Threat Defense Devices
1
2
...n
network traffic
Network
Firewall events via Syslog
mgmt, event data
Network administrator
View Firewall events
Management Center
Cross-launch, remote query
Secure Network Analytics Manager

In this deployment, the threat defense devices send Secure Firewall events to the Manager, and the Manager stores these events. From the 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 management center.

### Data Store

See the following diagram for an example of a Data Store deployment with a Manager, Data Nodes, and Flow Collector(s):


Security Analytics and Logging (On Premises) Data Store Deployment
ASA devices
1
2
...n
ASA events via Syslog
Network
network traffic
Secure Firewall Deployment
Threat Defense Devices
1
2
...n
Threat Defense Security and Threat Defense Data Plane events via Syslog
Secure Network Analytics Deployment
Flow Collector(s)
event data
Data Store (1, 3, or more Data Nodes)
mgmt, event data
mgmt, query data
Network administrator
View Threat Defense Security Events
Cross-Launch, remote query
Secure Network Analytics Manager
Management Center
View Threat Defense Security, Threat Defense Data Plane, and ASA events

In this deployment, the threat defense and Secure Firewall ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store for storage. From the 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 management center.

## Supported Event Types

- Threat Defense Security events
  - Connection
  - Intrusion
  - File and Malware
- Threat Defense Data Plane events (Data Store deployment only)
- ASA events (Data Store deployment only)