12- Cisco Stealthwatch

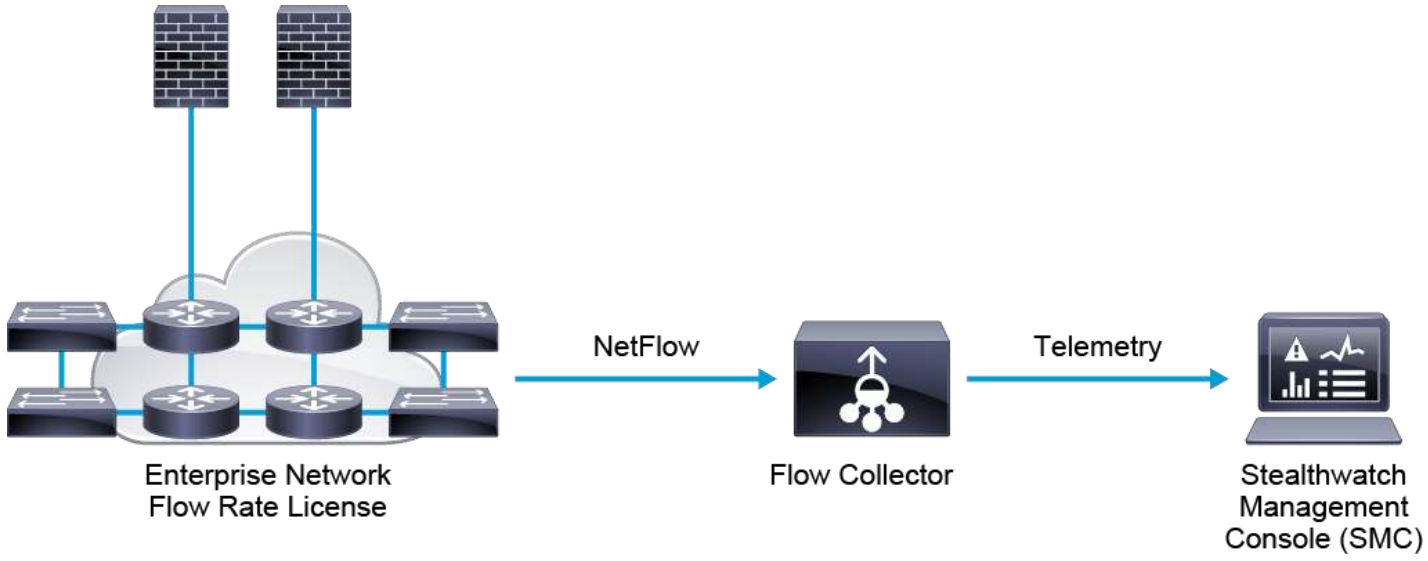
Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Introduction

- Cisco Stealthwatch Enterprise is a flow-based visibility solution that turns your entire network into a sensor.
- Instead of a handful of sensors deployed on various network segments, which directly impact network architecture options, your entire network becomes a sensor.
- This Network as a Sensor (NaaS) approach provides visibility at any infrastructure component in your network.
- Any movement – laterally or north-south – is captured in telemetry by the routers and switches that you already have, and then sent to Stealthwatch for analysis.

Introduction (cont.)

- The Cisco NaaS solution brings visibility to your entire network through a very lightweight deployment of a Stealthwatch Management Console, a FlowCollector, and a Flow Rate License.



Cisco Stealthwatch Required Components

This Stealthwatch Enterprise required components:

1. Stealthwatch Management Console:

- ✓ (physical or virtual appliance) is the Graphical User Interface (GUI)-based management console that aggregates, organizes, and presents analysis from the flow collectors via graphical representations of network traffic, user identity information, customized summary reports, and integrated security and network intelligence for drill-down analysis.
- ✓ The collection of Stealthwatch System appliances (flow collectors and other optional components) are coordinated, configured, and managed by the SMC.
- ✓ The FlowCollector stores the flow data and sends the summarized flow and alarm data to the SMC.
- ✓ The SMC then correlates this data, in real time and displays it in an easily understood graphical layout.

Cisco Stealthwatch Required Components (cont.)

This Stealthwatch Enterprise required components (cont.)

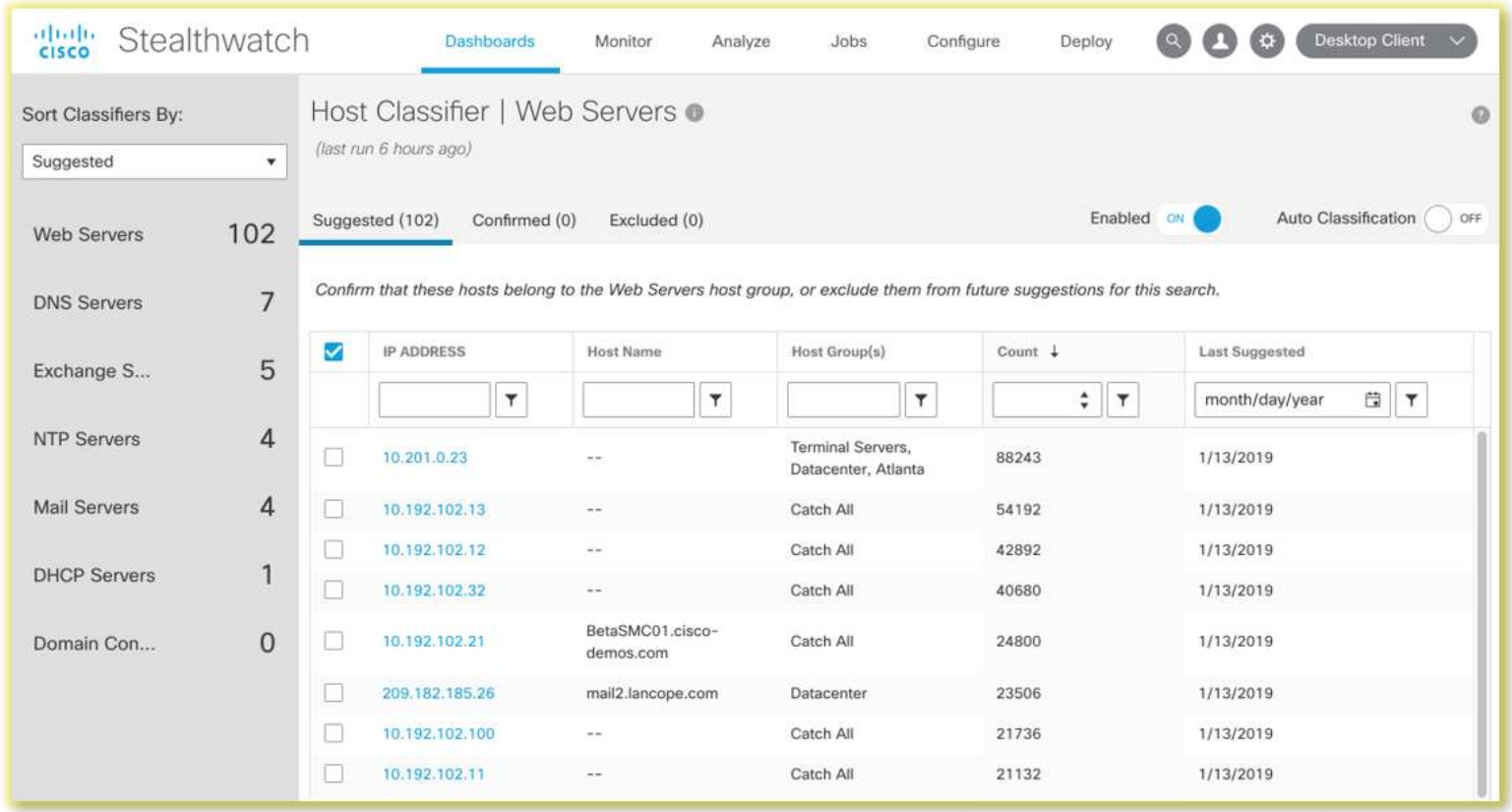
2. FlowCollector:

- ✓ (physical or virtual appliance) aggregates and normalizes the NetFlow data that is collected from network devices.
- ✓ The FlowCollector provides network visibility and security intelligence across physical and virtual environments to help improve incident response.
- ✓ Multiple FlowCollectors may be installed.
- ✓ The FlowCollector monitors, analyzes, categories, and stores information from each flow, creating a baseline of typical network activity.
- ✓ If unusual activity occurs, the FlowCollector immediately sends an alarm to the SMC with the contextual information necessary to help isolate the root cause.
- ✓ A single FC can store and analyze data from as many as 4000 flow sources at up to 240,000 flows per second (FPS).

Cisco Stealthwatch Required Components (cont.)

- Routers and switches send flow data to the FlowCollector, which parses the telemetry and sends further filtered information to the Stealthwatch Management Center.
- The flow data could be **NetFlow**, if you have Cisco routers and switches, or it could be **jFlow**, **sFlow**, or **IPFIX** if your network uses other networking equipment.
- Stealthwatch Enterprise configuration and reporting are performed at the SMC.

Cisco Stealthwatch Required Components (cont.)



Explore Cisco Stealthwatch [Lab]

Demo Lab