Active Discovery overview

General principles

Active Discovery allows the sensor to send packets to the network to discover previously unseen devices and gather additional properties for known devices.

There are two different types of Active Discovery operations:

- Broadcast

    The sensor sends Broadcast packets targeting all the devices in the subnet. Devices that support the protocol will give a response back and appear in Cisco Cyber Vision.

- Unicast

    The sensor sends Unicast packets to known components and analyses the responses received.

The protocols supported for Active Discovery operations are:

- Broadcast:
    - EtherNet/IP
    - Siemens S7
    - Profinet
    - ICMPv6

- Unicast:
    - EtherNet/IP
    - SNMP

For more information about discoverable properties, refer to Active Discovery protocol details.

Design considerations

Several requirements must be met when deploying and configuring Active Discovery on a sensor:

- The sensor must have access to the required subnet:

  - For Broadcast discovery, the target subnet/VLAN must be directly accessible from the sensor, meaning the sensor must have an IP address set in this subnet.

    On IOx sensors, the AppGigabit interface must be in trunk mode, and the VLAN must be allowed on this port.

    On the Cisco IC3000, one of the interfaces must be connected to a port on the VLAN, with no span configured on this port.

  - For Unicast discovery, the target subnet/VLAN must be either directly accessible from the sensor, or the sensor must have the required gateway or route to reach the targeted devices.

- The list of nodes targeted in Unicast discovery comes from the device list of the preset which launch the discovery. A preset configured with sensors in its filter will trigger Active Discovery on these sensors. It means that only the components that have been filtered by this particular preset will be scanned.

Basic configuration workflow

To configure Active Discovery, you must perform the following steps:

- Deploy a sensor with the required configuration: IP address, VLAN, gateway or routes.

- Create an Active Discovery policy containing the protocols needed and their respective parameters.

- Create a preset with at least one sensor.

- Set the policy on the preset and set an execution time or run it once.