DRAGOS
SAFEGUARDING CIVILIZATION

OT Network Traffic Validation Steps for Dragos Sensors

A GUIDE FOR CISCO ENVIRONMENTS

To ensure that a Cisco SPAN (Switched Port Analyzer) has been configured correctly to capture operational technology (OT) traffic prior to connecting your Dragos Sensors, consider these recommendations. This process includes packet capture and analysis, configuration review, and topology diagram reviews.

1. Open Change Control Tickets

Objective: Ensure all change control processes are followed and ensure that your environment will not be adversely impacted by any of the sample commands, they are not customized for your environment and are supplied as examples only.

ACTION

- [ ] Prior to making any changes to your production environment, create and seek approval for any required change management processes.

WARNING: Review official Cisco documentation and consult your network administrator to validate any commands you issue to your network fabric. The commands supplied in the following sections are provided as examples only

2. Review Network Topology Diagrams

Objective: Understand the network layout and identify the correct source and destination ports for the SPAN configuration.

ACTION

- [ ] Verify topology diagrams to locate OT devices, their connectivity, and typical communication flows.
- [ ] Identify the switch ports connected to the OT devices that need monitoring.
- [ ] Ensure that the identified SPAN sessions in the section below encompass the devices identified above.

3. Verify SPAN Configuration in Running Config

Objective: Ensure the SPAN session is correctly configured on the switch.

COMMANDS

- [ ] Connect to the switch via SSH or console.
- [ ] Enter privileged EXEC mode: `enable`
- [ ] Display the current SPAN configuration:
  `show running-config | include monitor session`
- [ ] Check the output for the correct source and destination interfaces. For example:
  ```
  monitor session 1 source interface Gi1/0/12
  monitor session 1 destination interface Gi1/0/2
  ```

4. Validate SPAN Session Settings

Objective: Confirm that the correct interfaces are selected and the SPAN is operational.

COMMANDS

- [ ] Verify SPAN session details: `show monitor session 1`
- [ ] Ensure the output includes the correct source and destination ports, and confirm the session is active.

5. Perform Packet Capture and Analysis

Objective: Capture and analyze packets to confirm the correct traffic is being mirrored.

Tools: Wireshark or a similar packet analysis tool.

ACTION

- [ ] Connect a laptop with Wireshark to the destination port of the SPAN session.
- [ ] Start a packet capture session in Wireshark.
- [ ] Generate or wait for OT traffic from the source port.
- [ ] Analyze the captured packets in Wireshark to ensure they are from the OT devices and that all expected traffic types are being captured.
- [ ] Verify that the capture contains ARP traffic and layer 2 traffic

6. Test and Verify Traffic Capture

Objective: Confirm the completeness and accuracy of the captured traffic.

COMMANDS

- [ ] Generate test traffic on the source port (e.g., by pinging, leveraging native vendor tools to communicate with your OT assets such as AccSELerator or ControlLogix), consult your Dragos SA for more detailed instructions or guidance.
- [ ] Check Wireshark or packet capture tool for this specific test traffic.
- [ ] Ensure that all expected traffic is being captured without loss, retransmissions, or errors.

7. Adjust SPAN Configuration if Necessary

Objective: Fine-tune the SPAN settings to capture all required traffic.

ACTION

- [ ] If the desired traffic is not captured (especially the traffic you generated in step 5 above), verify the source and destination interfaces again.
- [ ] Adjust the SPAN session if needed:

```
configure terminal
no monitor session 1
monitor session 1 source interface Gi1/0/1
monitor session 1 destination interface Gi1/0/2
end
```

8. Document and Report Findings

Objective: Maintain accurate records of the SPAN configuration and findings.

ACTION

- [ ] Document the SPAN session configuration, including source and destination ports.
- [ ] Record the results of the packet capture and analysis.
- [ ] Note any adjustments made and their outcomes.
- [ ] Share the documentation with relevant stakeholders.
- [ ] Share your findings with your Dragos SA/FO team.
- [ ] Close any applicable change control tickets you opened in step 1.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us