NETFORMX®

Guide

Addressing Enterprise Customer Security Concerns

August 2021

Summary / Keywords

Netformx provides the ability to discover via SNMP and Command Line Interface (CLI) inspection to analyze customer networks in order to provide accurate analysis of the infrastructure including equipment lifecycle, security alerts and contract validation. Analysis for Cisco equipment uses the online Cisco Discovery Services / Cisco Smart Advisor (CSA/CDS) systems to create end-customer consumable network assessment reports. Network discovery capabilities are accessible for users of Netformx DesignXpert®, Netformx Discovery™, and the Netformx Standalone Collection Engine.

When considering network discovery and analysis, enterprise customers have expressed some concerns related to the protection of their network performance and sensitive information during and after the assessment process. This document addresses the common concerns when using Netformx and Cisco[1].

Content / Solution

Security Concerns in Network Assessment

Network assessment consists of two processes that can be run separately.

- The systems engineer (user) configures the Netformx Discovery (ND) engine to access and 'walk' the existing network infrastructure by configuring the ND application with applicable SNMP, Telnet \SSH and other protocol definitions including CLI login credentials.
- Once the discovery SNMP walk completes, the user imports the results back into DesignXpert and uploads the raw data pulled from the responding Cisco SNMP devices to Cisco's CSA/CDS servers[1] for additional analysis.

This document lists and addresses common issues raised by users regarding their security concerns while performing the SNMP walk and network assessment provided by Cisco. These issues are listed by the order of steps in the network assessment process.

1. **Discovering the network**
    a. User must provide login credentials to gain access to network devices (CLI login and SNMP community string / login).
    b. ND, even when accessing data with privileged access (CLI enable password or SNMP read/write permission), never changes any settings on any network device.
    c. ND offers various ways to define the network for discovery, including whitelists and blacklists of devices.
    d. ND gives the user full control on the number of outstanding queries. Reducing this number will slow the discovery process but gain less load on the network and vice versa.

2. **Storing the discovery data**
    a. All the collected data is kept in the Netformx Project files stored on the host system connected to the networking infrastructure, issuing, and controlling all SNMP & other protocol commands.

3. **Access to CDS/CSA**
    a. Access to CDS/CSA is strictly controlled by Cisco (via CCW credentials) and is required only to upload the transactional data and download the analyzed output.
    b. Access to the customer related details is restricted to the user associated with the ND and tied to their CCW ID.

[1] Cisco CSA/CDS does not support analysis and reporting on Cisco Meraki products.

c. During ND, there is no need for the discovery host to be connected to the Internet.
d. Access to and from CDS/CSA is secured using 128-bit HTTPS encrypted protocol.

4. **Data sent to Cisco (analysis request)**
   a. The end-customer and user can agree (and configure limitations) to further restrict the upload from including:
      i. IP Address details
      ii. Third-party (non-Cisco) devices
   b. Sensitive information like device login information is not sent to Cisco.
   c. A unique Transaction ID (TID) is generated for every upload to Cisco.

5. **Storing the analysis data**
   a. Once Cisco completes their analysis, the data downloads to the host that sent the analysis request.
   b. The downloaded data is stored in the project file.
   c. The user may elect to purge the data from the Cisco server. In such case, the user will not be able to re-analyze the data without uploading it again.

Communication protocols used during Discovery

SNMP	Main discovery protocol, used for all SNMP enabled devices.	Read only access.
Telnet	CLI querying used mainly for collecting information required for CDS/CSA. Can also be used to retrieve Cisco configuration files.	Some information like Cisco configuration files needs enable access. User needs to provide the credentials.
SSH	Secured CLI, used for same purposes as Telnet.	
ICMP	Ping is used to determine the active IP addresses.	The use of ping is controllable via advanced settings.
HTTP	Used to query configuration for Cisco IP phones.	Depends on an option set by the user.
HTTPS	1.Access to Meraki.com 2. Communication protocol used during upload to and download from Cisco.	CDS/CSA integration uses 128-bit encrypted HTTPS communication services.

Bandwidth & Performance

ND bandwidth consumption is affected by the following factors:

- **Amount of information being collected:** Determined by the size of the network, the type of devices being discovered, and scope of the configured ND.
- **Discovery speed:** The more concurrent outstanding requests allowed, the more network bandwidth consumed.

ND Performance is sensitive to the discovery settings. Therefore, make sure your settings are as efficient as possible:

- Avoid use of Ping in networks where ICMP is not permitted.
- When using multiple login credentials / community strings sort them smartly. Locate the most common credentials on the top of the list and so on.

- When using IP range / subnet to discover, make sure you make the minimal required definition. If sections of these ranges are not populated, exclude them from range definition.
- Do not collect information you are not going to use; any information collected requires time and takes additional bandwidth to collect. For example: IP Phone discovery, Name resolution, Configuration files, etc.

If you have further questions, contact support@netformx.com.