

Addressing Security Concerns Regarding a Network Discovery with neteXpose DNA

Deploying the Cisco Discovery Services (CDS) or the neteXpose Knowledge Base Server (KBS) Approach

1 Introduction

Every network assessment using neteXpose DNA consists of two main phases:

- Discovery for data collection
- Analysis and data evaluation to create reports and network maps.

The following paragraphs describe the security methods and measurements provided by the DNA software. The process is summarized in the following table.

neteXpose DNA NETWORK ASSESSMENT PHASES	NETEXPOSE DNA SECURITY METHODS AND PROCEDURES
Discovery	
Discovery station	Local or remote; Customer PC or Partner PC USB stick solution
Discovery range, protocols, methods	SNMP v1, SNMPv2c, SNMPv3, SSH, Telnet; WMI Community string, Username/Password, MD5 or SHA, DSA or RSA Multi-protocol scan, Ping scan
Network device access	Credentials depending on setup
Discovery data storage	SQL database and XML file on the DNA station
Discovery data access	User ID and password
Discovery Data Analysis	
Discovery data analysis only	Discovery data, asset reports and network maps are stored on the DNA station; no data will leave the DNA station
Discovery data plus external data analysis Using the neteXpose Knowledge Base Server	Discovery data is correlated with product lifecycle data on the DNA station locally. Then the EOX reports are created on the DNA station. All reports made locally, all data, reports and maps are stored on the SQL DB and/or on XML file of the DNA station. All files are open and accessible. No external connections are needed.
Discovery data plus external data analysis Using the Cisco Discovery Services (CDS) API	Discovery data is stored on the DNA station Only the discovery data from selected Cisco devices is transferred to Cisco using the CDS XML SOAP API (all XML data can be reviewed prior to upload)

2 Discovery Phase

2.1 Local or Remote Discovery

Using neteXpose DNA the discovery can be performed on the customer site or remotely.

2.2 DNA Station

The neteXpose DNA software can be installed on any PC or laptop either supplied by the Service Partner or the Customer.

2.3 Discovery Range and Discovery Depth

The discovery range and the discovery depth can be fully controlled by the user. The user needs to provide the information which network or subnet he wants to discover. The discovery range will be defined by one or more IP addresses or by one or more address ranges. It is also possible to exclude one or more IP addresses or address ranges from the discovery. In addition the user can define, if he wants to discover SNMP devices only, SNMP plus WMI devices, devices plus topology. After completion of the discovery process the user can also delete data from the SQL database based on IP address, subnet, device type or individual host name.

2.4 Discovery Methods and Protocols

Dependent on the discovery setup, the following discovery methods are used:

- Multi-protocol Scan: every IP address of the subnet will be tested with Ping, SNMP as well as WMI/NetBIOS if the option "MS Windows Inventory" is chosen.
- Ping Scan: IP addresses are pinged only.
- IP range: similar to the Multi-Protocol Scan; it limits the test to a specific IP range.

2.5 Login Credentials

Dependent on the discovery setup, the following credentials are supported by neteXpose DNA to get access to the device information. The credentials must be provided by the customer.

Model	Level	Authentication	Encryption	What happens
SNMP v1	noAuthNoPriv	Community String (read only)	No	Uses community string match for authentication
SNMP v2c	noAuthNoPriv	Community String (read only)	No	Uses community string match for authentication
SNMP v3	noAuthNoPriv	Username	No	Uses username match for authentication
SNMP v3	AuthNoPriv	MD5 or SHA	No	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm
SNMP v3	AuthPriv	MD5 or SHA	DES	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm Provides DES-56 bit encryption in addition to the authentication based on the CBC-DES (DES-56) standard
SSH/Telnet		Username/password	DSA (SSH) RSA (SSH)	Uses a secure channel to exchange data between two devices including encryption

2.6 Discovery Data Storage

The discovery data is stored in the SQL database, as well as in XML format in the XML folder on the DNA station. All data can be viewed and analyzed by the user.

2.7 Remote Discovery

If a discovery is executed remotely, the Service Provider needs to provide the security elements for the discovery data transmission between the customer site and the central DNA station on the Service Provider's site, e.g. via VPN or Firewall configuration.

3 Discovery Data Analysis

For data analysis and evaluation, neteXpose differentiates between discovery data only analysis and discovery data plus external data correlation. For example using device information to get end of life information.

3.1 Discovery Data Only Analysis

The discovery data is processed to asset reports and network maps using the integrated DNA Reporting and Visualisation Tools. In this case all discovery information, including reports and maps are kept on the DNA station and controlled by the user, performing the analysis.

3.2 Discovery Data Plus External Data Analysis

For additional analysis such as product lifecycle information analysis, external data need to be added to the discovery data. This is accomplished in two different ways:

3.2.1 DNA Knowledge Base Server (KBS)

To correlate data from external sources with the discovery data, neteXpose uses its own knowledge base.

Product lifecycle data from different vendors is provided by the neteXpose Knowledge Base Server.

The local DNA server updates its knowledge base via user request. All updates to and from the KBS are generic hardware and software details, e.g. chassis type, OS version, etc. No specific configuration data, e.g. serial number, hostname, IPs etc. is needed.

After the discovery the device data is correlated locally and the DNA VAI interface provides Cisco and other manufacturers reports based on the correlate KBS data.

The product lifecycle analysis on the Cisco devices can be sent to Cisco by the Cisco Partner in accordance with the customer, if the **Cisco Discovery Services (CDS) API** cannot be used for some reason.

3.2.2 Cisco Discovery Services (CDS) API

Using the CDS API, only the data on selected discovered Cisco devices is transferred to the Cisco Backend System. The transfer is accomplished by the Cisco Partner using his Cisco Login (Level 3) access the Backend System including HTTPS encrypted protocol and other security measurements provided by Cisco.

Please note:

- Only the discovered Cisco asset data is transferred.
- No customer sensitive data such as IP addresses or hostnames is transferred unless specifically specified for SSH (e.g. show conf command).
- No information on discovered devices from other vendors is transferred.

When the analysis is finished, the data will be sent back from the Cisco Backend System to the DNA station. The downloaded data is stored in the related customer data base on the DNA station. The final Cisco CDS Services and Analysis Reports will be automatically created on the DNA station. The DNA discovery database as well as the received Cisco data analysis can be deleted at any time. If the user deletes all data, a new discovery and a new update is necessary for a consecutive analysis.

4 Additional Security Aspects

For customers not allowing any external DNA station to be connected to the customer network neteXpose offers the following solutions:

1. The DNA software can be installed on any customer PC. All discovery data is kept on that customer PC. If the customer decides for the Cisco CDS API analysis approach, only the Cisco-related part of the discovery data is transferred to Cisco. If the customer decides for the neteXpose Knowledge Base Server approach, no data will leave the customer's PC. The product lifecycle analysis is executed on the DNA PC and can be handed over to Cisco in the form of spreadsheets and other off-line documents.
2. DNAonUSB, a self-running discovery software application on an USB stick. No discovery application and no data need to be installed or stored on any PC. The USB is connected to a customer PC, and the discovery data will be directly transferred to the Partner's Backend System (via a secure VPN connection) where all further analysis is done.

4.1 What happens to the data after the discovery?

All data is stored locally and reports are created from the locally stored data. All data is visible on the customer PC or Server. If the discovery is performed on a Customer's PC the customer is responsible for the data.

If the discovery is performed on a Partner's PC or Partner's Backend server the following approaches are supported:

1. After the discovery all data (SQL DB and XML files) can be deleted. In this case a new discovery including setup and analysis is necessary for a scan repetition.
2. After the discovery all data (SQL DB and XML files) can be de-installed from the DNA station and put aside in a secure environment (customer or partner environment). They can be re-installed before a successive discovery to allow the same setup and to use the same product identification number (UOID) to get comparisons between different scans.
3. All data (SQL DB and XML files) can be stored in a multi-tenant security environment of the Cisco Service Partner.
4. It is also possible to delete a single database file after the discovery and analysis process. It is up to the customer to decide if he wants to store the files for a later re-discovery including reports creation.