White Paper

Data Collection and Analysis: Get End-to-End Security with Cisco Connected Analytics for Network Deployment

Cisco® Connected Analytics for Network Deployment (CAND) is Cisco hosted, subscription-based software that analyzes service requests and network deployment data. It provides information about devices, software, and technology configurations. CAND provides visualizations and actionable recommendations that focus on network planning and optimization.

What You Will Learn

This document provides information on the security processes that CAND implements. It covers:

- Configuration collection
- Communication with the Cisco data center
- Processing the uploaded data
- Reporting on the CAND portal

Cisco CAND Overview

CAND is a software product in the Cisco Connected Analytics portfolio.

CAND serves both enterprises and service providers. The product uniquely analyzes device data along with Cisco service request data to pinpoint opportunities to standardize device configurations. Based on this analysis, CAND provides actionable recommendations to help optimize your IT network by promoting network resilience and readiness to support complex business services.

CAND provides the following benefits:

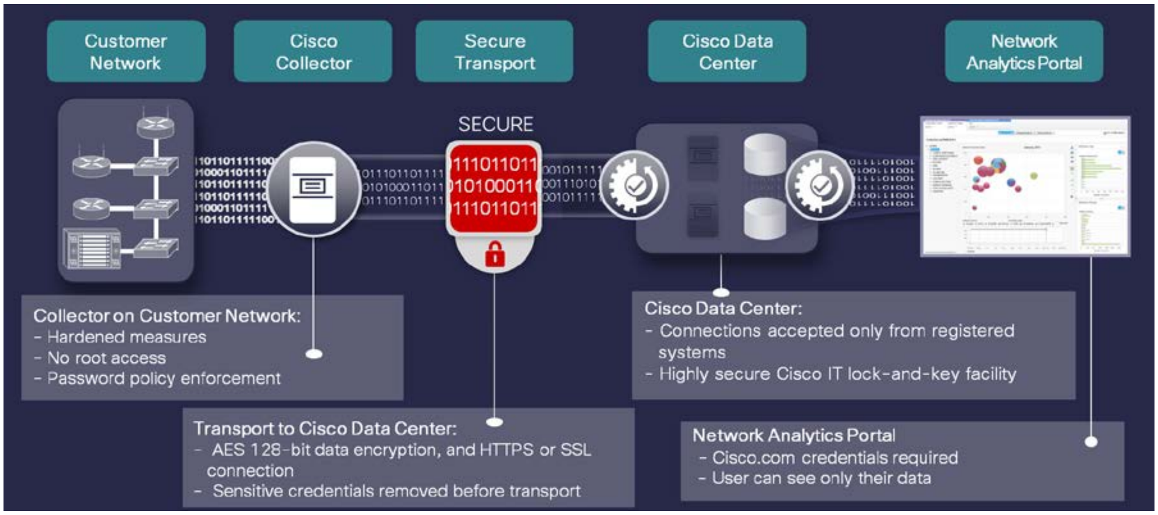
- Rapid transformation of network and service request data into visuals pinpointing where corrective action is needed
- Actionable insights and help in establishing a stable and controlled network baseline
- Greater efficiencies and lower cost and risk through rapid identification of weaknesses in network deployments
- Prioritized corrective actions, helping network personnel focus on the devices most correlated with undesirable service call trends
- Highly resilient network ready for strategic business services, such as big data, collaboration services, and IP video

These benefits help you make better and faster decisions that can reduce operational costs while improving IT support for business requirements.

CAND Security Architecture

CAND provides an end-to-end highly secure architecture for your network deployment data. The security functionality addresses all aspects, including collection, transmission, processing, storage, and viewing (see Figure 1).

Figure 1. End-to-End Security in Cisco CAND



Collector on Customer Network:
- Hardened measures
- No root access
- Password policy enforcement

Cisco Data Center:
- Connections accepted only from registered systems
- Highly secure Cisco IT lock-and-key facility

Transport to Cisco Data Center:
- AES 128-bit data encryption, and HTTPS or SSL connection
- Sensitive credentials removed before transport

Network Analytics Portal
- Cisco.com credentials required
- User can see only their data

This white paper outlines the following important security functionalities of CAND:

- Securing the collector and the data
- Providing highly secure connectivity and data transmission to the Cisco data center
- Storing data at the Cisco data center
- Controlling access to the portal data and offline reports

Securing the Collector and the Data

Collector Security

CAND uses a collector placed in your network to uniquely identify Cisco devices and collect configuration details. It uses the CentOS distribution of the Linux operating system. Hardening measures are applied to the collector during configuration. Hardening procedures include, but are not limited to, the following:

- All application code is deployed to an operating system image that is hardened per industry-standard recommendations.
- No unsecured or nonessential accounts, ports, applications, or services are enabled.
- A firewall is installed and configured with a default set of rules tailored for the collector.
- Collector configuration auditing and logging for troubleshooting and monitoring are enabled.
- Privileged (root) access to the collector is restricted to administrator usage, with a limited and hardened command shell environment.
- Users authenticate through role-based access. For example, some users can be granted access to configure and manage the system while other users may perform view-only operations.
- Collector administration functions are accessed through a highly secure web UI that uses industry-standard HTTPS for secure communications.

Access to the Collector

The collector has an administrative shell that is accessible through a local console or, if enabled, a secure shell (SSH). The interface is a command-line shell interface that allows the administrator to perform basic tasks such as IP address assignment and any operating-system-related tasks. Creating and managing discovery and collection jobs is performed through a web UI. The web UI is accessible through the HTTPS protocol to enforce security.

Collector password policy requires passwords to be a minimum of nine characters in length, containing uppercase and lowercase letters, numbers, or special characters. They cannot form any known English-language words or likely words. In addition, Cisco recommends changing the password for a nonprivileged account used to log in to the collector, as well as the privileged password, every 180 days.

Collector Logging and Monitoring

All security-sensitive events occurring on the collector are logged locally. Self-monitoring is used to examine the state of the collector at certain points in time and to provide alerts on security-sensitive events. Such events include but are not limited to:

- Unsuccessful login attempts
- Secure connectivity or cryptographic processing errors
- Policy configuration changes
- Status changes of collector subsystems, such as the local database and file system
- Data access from collector user accounts

- Transmission of information to the Cisco data center

Discovery and Collection

Device discovery can be controlled using several methods. You can choose different protocols for discovery, such as the Address Resolution Protocol (ARP), Link Layer Discovery Protocol (LLDP), Border Gateway Protocol (BGP), and others. The output from the command-line interface (CLI) commands in Table 1 must be collected for data processing. It is critical that the proper collector configuration is put in place to collect this data for CAND analysis.

Table 1. Mandatory CLI Commands for CAND

CLI Commands
show diag
show module
show running-config
show version

Device Simple Network Management Protocol (SNMP) read-only credentials and Telnet or Secure Shell (SSH) protocol credentials are required to perform a valid collection. This information is entered on, or imported to, the collector and used in the collection process.

Collection functionality can be configured. Policies can be set such that only a certain protocol such as SSH or Telnet is used during the collection. CAND data collection places a very light load on the network, and you can also reduce the number of threads and throttle the collection traffic if network performance is a concern. For more information on the collector discovery process, please refer to the CSPC Overview.

Data Storage on the Collector

All collected inventory and device collection information is stored in a local structured query language (SQL) database on the collector, not as part of the general file system. The collected device data is not encrypted. However, any portion of a device collection can be masked before it is inserted into the database or uploaded to Cisco.

All passwords and SNMP community strings are encrypted in the database with 256-bit AES encryption. There are different AES keys for database records, application codes, and backups. Device credentials are never transmitted to Cisco.

The collector can be configured to store data for the most recent 20 collection jobs. The default value configuration is for 5 data collections to be archived.

Communication Between the Collector and Cisco Products on Your Network

A Cisco collector gathers data from supported Cisco devices using a variety of protocols (see Table 2).

SNMP

The Cisco collector uses SNMP read-only access to poll the devices in the network and collect device details.

SSH

The Cisco collector supports SSH-based CLI access to network devices. SSH provides a highly secure form of remote access to network devices by encrypting all traffic, including passwords, between the collector and devices on the network. The collector supports SSH versions 1.5 and 2.0. Cisco recommends using this method for CLI access instead of less secure Telnet-based sessions.

Table 2. Port Usage in the Collector

Port	Description	Inbound	Outbound
22 TCP	SSH	For shell access to the collector for administration tasks	To execute CLI commands on devices
23 TCP	Telnet		To execute CLI commands on devices
53 TCP/UDP	Domain Name Service (DNS)		To connect to the DNS server
69 UDP	Trivial File Transfer Protocol (TFTP)	To connect the collector TFTP service listener	To connect to TFTP service on devices
80 TCP	HTTP service		To access the HTTP port on devices like Cisco Unified Communications Manager, IP phones or to connect to Cisco DMZ service for data uploads
161 UDP	SNMP ports		For SNMP queries on devices
443 TCP	SSL connection		For HTTPS connections to uploaded data
514 UDP	Syslog ports	To receive syslog messages from devices	To send messages to any outside syslog server
1098 TCP/UDP	Java remote method invocation (RMI) activation		To establish an initial connection to Java RMI service
1099 TCP/UDP	Java RMI ports		To connect to external Java RMI service for external API services
3306 TCP/UDP	MySQL database ports		To connect to database service outside a collector box, if configured
42605 TCP	Collector GUI or XML port	To use the collector GUI client from a remote box inside your network.	To connect to Collector GUI or XML API port
8001/8443 TCP	Collector Web UI Port	To access the collector web UI	To connect to Collector web UI port to connect
ICMP/IP	ICMP Ping		To discover and troubleshoot devices

Telnet

The Cisco collector uses Telnet to collect data for device configuration. Privileged-mode access is required for CAND. Cisco recommends the use of a TACACS+ server that stores usernames and passwords to authenticate access to network devices. This type of access allows you to limit the types of commands that the collector can execute on the devices by appropriate configuration of the TACACS+ server. The recommended authentication method for the CLI is to use a TACACS+ server allowing all show commands needed.

Internet Control Message Protocol (ICMP)

The collector uses ICMP Ping messages as a method of discovering Cisco devices and monitoring device and network availability.

Secure Connectivity and Data Transmission to the Cisco Data Center

Data Transport Security

The connection for transferring data is always initiated from the collector to the Cisco upload server in the Cisco data center. At no point will the Cisco upload servers attempt to establish incoming connections to the collector in your network. The collector does not accept incoming connections from external sources. Cisco recommends that all collectors be placed behind existing firewalls within your network to further reinforce this policy.

All sensitive device passwords and credentials—such as SNMP strings and encoded enable passwords—are masked in the associated device configurations so they are not visible during transport. Administrators are also able to specify specific devices or data strings to be excluded from the uploaded data file prior to transport.

Uploaded CAND files are encrypted and transferred over the public Internet to the Cisco data center. The transferred data is encrypted at the application layer using a public key infrastructure (PKI)-based 128-bit AES key that is generated per data upload. When an endpoint wants to transfer a file, an HTTPS-over-SSL connection is established. During this SSL handshake, client certificates are used for authentication. The HTTPS-over-SSL transfer encrypts data at the transport layer using a 2048-bit PKI-based system. This is in addition to the AES-128 encryption that the collector software performs at the application layer.

The data encryption has the following characteristics:

- A 128-bit AES key is generated dynamically for every data upload to encrypt the transferred data.
- The AES key itself is also encrypted with the public key generated by Cisco.
- In addition, every collector installation includes a pre-generated public and private key pair that is common for all collectors.
- The encrypted data plus the encrypted 128-bit AES key is signed using the private key that is pre-generated during installation to form the digital signature.

Data Authentication

In addition to the password-based authentication with the Cisco upload servers, each collector is assigned a unique, randomly generated digital certificate. This digital certificate, registered and stored at the Cisco data center in highly secure conditions, is used to validate the authenticity of the data after arrival. Data transfers from clients with unregistered or nonexistent certificates are permanently deleted on detection and never decrypted or transferred further.

Key Composition

The public and private keys used to encrypt the HTTPS session keys are 2048 bits in length. AES-128 bit encryption is used at the application layer. The transport layer security (TLS) session key is 56 bits in length and is used in stream mode. As described in the previous section, the data is encrypted three times using three different keys.

Key Management

PKI key exchange for application-layer encryption is done dynamically during the upload. Trusted third-party external servers keep an up-to-date copy of both the public key used for application-layer encryption and the public key used for the SSL session setup. The collector supports all TLS protocols, and a symmetric key is exchanged through encryption with PKI for a timed duration of the session.

Upload Integrity

A message digest 5 (MD5) checksum is calculated from the uploaded data and is encrypted in the final package using the private key of the client. The MD5 value for a file is a 128-bit value very similar to a standard checksum. The additional length dramatically reduces the possibility of a different or corrupted file having the same MD5 value. The calculated MD5 value of the encrypted data before it is transferred is compared with the MD5 value of the data once it has arrived at the Cisco data center to verify authenticity.

Data Upload Servers

Cisco maintains hosts in its highly secure DMZ to receive uploaded encrypted files. These hosts do not store the keys necessary to decrypt information and transport data to its final destination behind the Cisco firewall only when the integrity of the data file is verified.

Data Storage at the Cisco Data Center

Data Storage

Cisco is committed to protecting the privacy and confidentiality of the data it stores. To help ensure this, the following steps are taken:

- The CAND environment that processes your data is located behind the Cisco firewall and on a highly secure switched segment of the network.
- The installation process for all Cisco IT machines follows a rigorous standard of security; this includes the application of hardening scripts to protect these machines.
- The machines are kept in a lock-and-key facility where access is restricted to Cisco IT administrators.
- Cisco intrusion detection systems are deployed throughout the corporate network and the restricted network on which the data is stored.
- The uploaded network information is uncompressed and decrypted only on Cisco production machines inside the Cisco firewalls.

The data is protected with strict authentication and access control measures within the Cisco firewall. The database is secured using a role-based security model implemented natively through Oracle application schema grants and privileges and a robust audit logging configuration. Application-level access to the data is protected through a single sign-on mechanism that is well accepted in the industry.

All access to data center data is through CA SiteMinder-based authentication. Confidential information, such as community strings and passwords, is removed before storage. Data is stored according to Cisco corporate IT best practices and data protection and retention policies.

Storage Policies

Raw uploaded data is archived per Cisco enterprise retention policies. The raw data is converted, processed, and stored in the data center database from which the portal reports are generated. Once the data is processed and analyzed, it is made available for display in the portal.

Cisco Processes to Verify and Audit the Security of Its Systems

Cisco uses a combination of static analysis during major releases and regular vulnerability testing. Products and services undergo security risk analysis, security standards compliance testing, and vulnerability scans. Any issues discovered by these processes are reported, and corrective action is handled through the standard Cisco Defect and Enhancements Tracking System (CDETS).

Controlling Access to the Portal Data and Offline Reports

CAND Portal Security

The CAND portal allows you to review processed information about your network inventories and contract information. Your company's data is logically segregated from data from all other companies in the portal. The portal has the following security mechanisms in place:

- Unique, authorized Cisco.com ID and password, linked to the entitled company of the user
- Customer administration of user access to your CAND portal
- Server-authenticated SSLv3
- Secured session management with expiration
- Hierarchical role-based access control
- Logging and monitoring of failed logins, invalid resource access attempts, and similar events

Your designated administrator controls access to the CAND portal. The administrator can register new users and unregister an existing user (for example, someone who leaves the company or changes job responsibility).

Conclusion

CAND provides a highly secure end-to-end architecture for the collection, processing, and transmission of your network deployment data to the Cisco data center and CAND portal. There you can access comprehensive reports that provide actionable insight into your Cisco network deployment.

Cisco takes the security of your data seriously. If you need further details about CAND and how we implement our security architecture, contact your Cisco sales representative or your Cisco authorized partner. They will be happy to set up a meeting to discuss your questions and provide details about your specific situation.

For More Information

Visit CAND on Cisco.com or email the CAND team.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 10/14