Security Architecture of the CSPC System

Basic CSPC Security

The CPSC system allows for the configuration of the polling functionality. A device can be removed from the polling list. Protocol policies can be set such that only a certain protocol such as ssh or telnet will be used in the polling. It is also possible to reduce the number of threads and throttle the polling traffic.

All configuration and device collection information is stored in the local SQL database. The collected data is not stored encrypted, but there is a robust set of masking operations such that any portion of a device collection can be masked before insertion into the database or upload to Cisco.

All passwords and SNMP community strings are store encrypted in the database with AES-256 encryption. Device passwords are stored encrypted as well. The CSPC system has a mechanism to schedule regular backups. The backup files are encrypted AES256 before they are stored. All application code is stored on the system encrypted with AES-256. A custom classloader has been written which decrypts and loads the encrypted application classes into memory upon system initialization. There are different AES keys for database records, application code and backups respectively. Device passwords are never uploaded to Cisco

If the system is compromised a new CSPC image can be installed on the appliance and the entire system can be reconstituted to its original state from the encrypted backups.

Users authenticate through two roles. Administrators can configure and manage the system while helpdesk users can perform view only operations.

All application code is deployed to an operating system image that is hardened per NSA recommendations.

CSPC Transport Security

Data is encrypted using AES128 bit key. This key is generated per client registration. Both transport end points are authenticated to an LDAP server with a username and password. Once both end-points log in, both end points are checked for authorization to transfer information back and forth.When an end point wants to transfer a file an XMPP connection over SSL or HTTPS over SSL connection is established. During this SSL handshake, client certificates are used for authentication.

CSPC Backend Security Operations

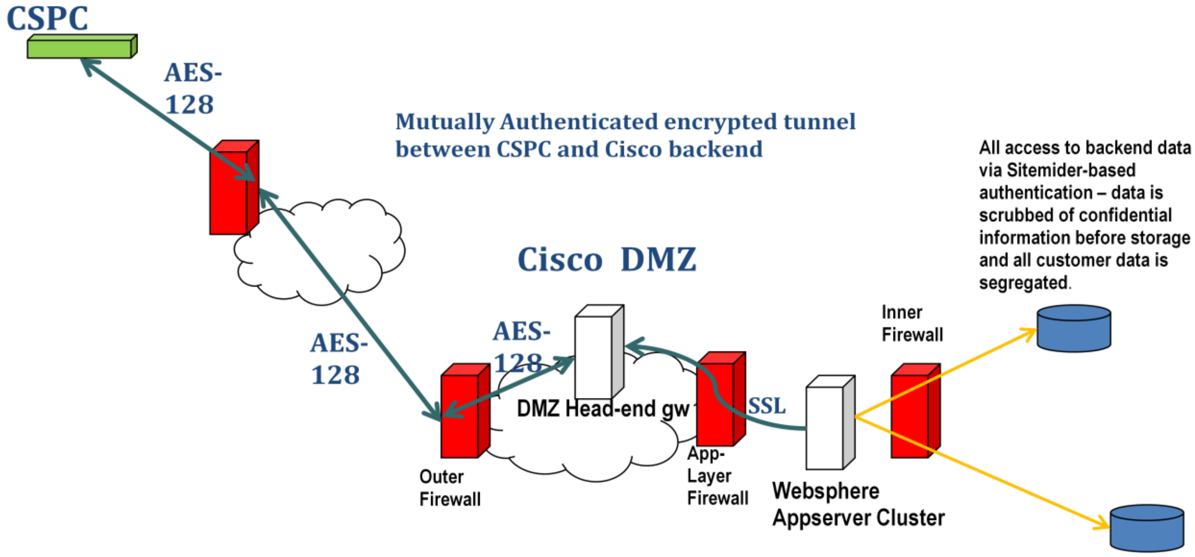
The collected data is not encrypted in the backend databases. It is, however, protected with strict authentication and access control measures. The database is secured using a role based security model implemented natively via Oracle application schema grants and privileges and a robust audit logging configuration. Application level access to the data is protected via a single sign-on mechanism that is well accepted in the industry.

The following programs have access to the information collected and processed by CSPC:

- NLS
- Inventory and Reporting
- Smart Call Home
- Smart Enabler
- MACD
- SNAS

A small subset of developers have view only roles to the data for debugging purposes. Local trusted DBAs generally have full access, but mainly for maintenance and tuning purposes. Sales people do not have direct access to the collection data. They can view certain aspects of it only through pre-generated reports

Fig1 CSPC Backend Operations



Mutually Authenticated encrypted tunnel between CSPC and Cisco backend

All access to backend data is via Sitemider-based authentication – data is scrubbed of confidential information before storage and all customer data is segregated.

Traffic between Cisco DMZ and the Wesphere Appservers on the internal secure network is via JMS running over mutually authenticated SSL. There is never data stored in the DMZ. The Websphere Cluster retrieves the messages from the JMS queue.

The databases are backed up via hot backup daily and cold backup once per week. Profiled information is stored in the databases for up to one year. Raw unprofiled data is purged after 6 months

Port Uses in CSPC

Port	Type	CSPC Module	Description	Purpose
TCP/5222	Outbound to Internet	Connectivity	• Outgoing TCP/5222 open. Auto-fallback to BOSH if outgoing TCP/5222 is not open • Allow incoming packets that match outgoing packets' address/port information • Out of customer network	To connect to Cisco/partner backend
TCP/443	Outbound to internet	Connectivity	• Follow standard https procedures. No special treatment for BOSH. • Outgoing TCP/443 open (requests) • Allow incoming packets that match outgoing packets' address/port information • Out of customer network	To connect to cisco/partner backend aggregator services
TCP/22	Inbound from LAN	Remote GUI client and Local Shell Access for CLI use	For CSPC GUI client • Used when CSPC GUI port is not accessible via customer firewall • Used if customer allows SSH port forwarding mechanism • SSH inbound connection to be opened on CSPC box if customer wants to control CSPC server using CSPC GUI client remotely For NOS Server Local Management • If CSPC GUI access is not possible, we need shell access to get into CSPC box and use it with CLI • Till customer local jump box • Local to customer network	To use SSH port forwarding for remote GUI access To access shell for local CSPC server management
TCP/42605	Inbound from LAN	CSPC GUI client port	• Need access from internal box in customer network if client is installed on a different box • Local to customer network	To use CSPC GUI client from remote box inside customer network
ICMP/SSH/TELNET /SNMP/HTTP(S) Application Ports	Outbound to LAN	CSPC Protocol Layer for command execution	• All these TCP and UDP based ports are used in CSPC protocol layer to access devices • Local to customer network	To execute OIDs and CLI commands on cisco devices To execute SOAP and HTTP requests on cisco devices
TFTP	Inbound to LAN	CSPC protocol layer	• To run tftp server in CSPC to execute tftp bases tasks on devices	To execute tftp CLI commands or config collection using SNMP on devices