**PCI Switch Configuration Document (Juniper / Cisco)**
***[Team Name]***

[Company Name]

Confidential

# PCI Access Switch Configuration Guideline

*This text is to be used and followed when configuring a new Juniper/Cisco switch for PCI environment running the latest version of JUNOS/Cisco supported by the switch model in use.*
*The intended audience is only for [Team Name] personnel.*

Please follow the guidelines in this document when configuring a switch for PCI environment.
For every step that is completed, please tick the box in the last column. Once done, please fill out your information and have your manager or supervisor sign the document.

## Access Switch Configuration (Juniper/Cisco)

| Item No. | Description of Task | Done |
|---|---|---|
| 1 | Change default management VLAN0 to VLAN249 called mmamgmt. Make last 2 ports (47, 48) and any uplinks members of mmamgmt VLAN. | ☐ |
| 2 | Enable only HTTPs and SSH via management ports. Disable all unsecured protocols such as HTTP, Telnet, SNMP v1, etc. | ☐ |
| 3 | Identify the port roles for each port in use. Roles include VOIP, Desktop, Switch, Router, WAP, etc. | ☐ |
| 4 | Disable LLDP-MED/CDP on all access ports except uplinks and management ports including OAB management port. | ☐ |
| 5 | Disable PoE on all ports except those that need it and set PoE priority to HIGH and max power to 15.4 Watts | ☐ |
| 6 | Enable DHCP snooping for DHCP client ports | ☐ |
| 7 | Enable 802.1x if required and configure profile to authenticate against RADIUS | ☐ |
| 8 | Disable ability to reset to factory default from LCD | ☐ |
| 9 | If using SNMP, use SNMP v2 or higher to send traps only to internal SNMP via secure link or channel. Configure SNMP as follow:<br><br>SNMPv2 or higher with Read-Only community string called "mma-snmp-private" preferably on separate monitoring VLAN<br><br>Create and send these traps to designated targets only:<br><br>**snmp-access:** authentication, remote operations, startup, configuration<br>**snmp-data:** link, routing, VRRP event<br>**romon:** RMON alarm<br>**physical:** Chassis | ☐ |
| 10 | Specify the domain name for switch | ☐ |
| 11 | Configure Split-Permission model for switch authentication as follows:<br><br>1. Remotely Authenticate users against AD via RADIUS.<br>2. Upon failures, authenticate locally | ☐ |

**PCI Switch Configuration Document (Juniper / Cisco)**
***[Team Name]***

[Company Name]

Confidential

| | | |
|---|---|---|
| | **Local Users** - Create following local users on the switch<br><br>**JUNOS Only - Do not use root unless absolutely necessary!!!** | |
| 12 | Time & NTP<br>Configure local clock as following:<br><br>Runtime: ntp.inernalsource.com (Primary)<br>ntp.externalsource.com (Secondary)<br>Boot & Runtime: UTC | ☐ |
| 13 | Create a rescue configuration which should be set to default configuration. | ☐ |
| 14 | Create and display a Message of the Day (MoD) banner that notifies anyone who connects to a switch that it is for authorized use only and any use of it will be monitored.<br>**Example:**<br>This is an official computer system and is the property of the ORGANIZATION. It is for authorized users only. Unauthorized users are prohibited. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system may be subject to one or more of the following actions: interception, monitoring, recording, auditing, inspection and disclosing to security personnel and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to these actions. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By accessing this system you indicate your awareness of and consent to these terms and conditions of use. Discontinue access immediately if you do not agree to the conditions stated in this notice. | ☐ |
| 15 | If possible, Configure and Layer 3 built-in out of band management port *(JUNOS only)* | ☐ |
| 16 | Disable any unnecessary services such as bootp server, finger, proxy-arp, etc. | ☐ |
| 17 | Scheduled remote configuration backups whenever changes are made to existing configuration. | ☐ |

| | |
|---|---|
| **Switch IP** | |
| **Engineer** | |
| **Date Completed** | |
| **Manager's Signature / Initials** | |