Switch Port Security

Standard ID
IOT-CS-SEC-113

Published Date
7/28/2008

Effective Date
7/28/2008

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
11.0 Protective Technology (PR.PT)
   11.4 PR.PT-4
   11.4.1 Network Protection

Purpose
The information below sets the requirements configuration of network switch ports on the state network.

Scope
IOT Supported Entities

Statement
Below are the requirements for switch port security:

Port Security

1. The standard switch port will be configured with port security to allow only one MAC address. Wireless access points, unauthorized switches, or other devices using more than one MAC address will cause the port to be shut down. Operator intervention will be required to reactivate the port.
2. Switch ports configured for IP phones will be configured to allow two MAC addresses. If more than two MAC addresses are detected, the port will be restricted to the first two connected MAC addresses. Phone service should continue but operator intervention will be required to reactivate the port after documenting event.
3. Each switch port will be configured with BPDU (bridge protocol data unit) Guard to prevent unknown LAN Switches from being connected. If a switch is detected, the port will be shut down; operator intervention will be required to reactivate the port.
4. Unused switch ports will be placed in a NULL vlan and can be activated by following the appropriate IOT procedure.

Management Security

1. Where practicable, each device will be configured for SSH2 remote console login and TELNET will be disabled.
2. Access Lists will be employed to control remote console and SNMP access.
3. Remote Access to devices will be centrally controlled using TACACS (Terminal Access Controller Access-Control System) and Active Directory authentication. Logins will be recorded and commands will be logged for each device.

Exceptions to the above requirements should be kept to a minimum and only made when there is a significant negative impact on business operations. Wired and wireless connectivity solutions are available that do not compromise security or increase the cost of
support. Exceptions granted will fall into one of the categories below:

**Temporary:**

Situations where agencies have an immediate, unexpected circumstance arise and port security restrictions need to be temporarily relaxed. These exceptions should be one-time only with recurring needs addressed going forward by appropriate wired or wireless connectivity solutions.

**Short-term:**

Circumstances where the implementation of port security standards impacts ongoing business activities. In such cases, agencies will be granted relaxed port security for a brief period of time while a long-term solution is selected (wired or wireless). Agencies should have their long-term connectivity solution implemented within 30 days.

**Roles**

IOT Personnel

**Responsibilities**

IOT shall configure network configurations in accordance with this Standard.

**Management Commitment**

Management is responsible for confirming configurations are in accordance with this Standard.

**Coordination Among Organizational Entities**

Agencies shall coordinate with IOT where necessary to have temporary or short-term exceptions, on an approved case-by-case basis.

**Compliance**

Policy enforced by device configuration. Regular audit of device logs for anomalies.

**Exceptions**

Exceptions will be handled on a case by case basis by the Network team via ticket. For extended exception requests, all exceptions must be approved through the State CISO.