Cheatography

HPE Switch (Aruba/Procurve) Hardening Cheat Sheet

by Gorgonopsid via cheatography.com/19293/cs/2348/

Passwords

password all

Enable SSH

configure terminal

crypto key generate ssh

ip ssh

no telnet

Time Servers

sntp server x.x.x.x	alternatively: sntp server priority 1 x.x.x.x

sntp unicast

sntp 720

timesync sntp

Logging and other services depend on accurate timestamping, Procurve can use standard NTP sources and Windows DCs

TFTP, SFTP & SCP

ip ssh filetransfer	enable sftp & scp

no tftp server

no tftp client

Management VLAN

management-vlan x	can be either VLAN number or name

ip authorized-manager x.x.x.x mask x.x.x.x operator/manager

Locks down the Management functions of the switch, allowing access from the nominated VLAN only, it also Disables routing to the management VLAN

Syslog

logging x.x.x.x

Enable SSL

crypto key generate certificate 1024	Generates RSA cert
crypto host generate self-signed	fill in the requested details to generate your certificate
web-m ssl	enables https
no web-m pla	disables plaintext

Banner

banner motd #

WARNING!!! This system is solely for the use of authorized users for official purposes. You have no expectation of privacy in its use and to ensure that the system is functioning properly, individuals using this computer system are subject to having all of their activities monitored and recorded by system personnel. Use of this system evidences an express consent to such monitoring and agreement that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. #

Stack Management

no stack

Removes the remote possibility that someone will bring another Procurve into your office and take command of your device.

SNMPv3

snmpv3 enable

snmpv3 user USERNAME auth md5 AUTHPASSWORD priv des PRIVPASSWORD

snmpv3 group operatorauth user USERNAME sec-model ver3

no snmpv3 user initial

snmpv3 only	disables snmp v1 & 2c

RADIUS

radius-server host x.x.x.x key Super$ecretRadiusK3y

aaa authentication X login radius local	X can be console, telnet, ssh or web

aaa authentication X enable radius local

aaa authentication num-attempts N

aaa authentication login privilege-mode	optional to allow operator or manager access as per RADIUS response

Options configure switch to contact RADIUS for logon to switch console or webinterface, and optionally via enable to use L15/Manager commands.
If no RADIUS server is contactable, switch will fall back to using local authentication table

Physical Security

no front-panel-security password-clear

no front-panel-security factory-reset

Somewhat dangerous commands if you forget the local password

By **Gorgonopsid**
cheatography.com/gorgonopsid/

Published 17th July, 2014.
Last updated 23rd May, 2018.
Page 1 of 1.