Router & Switch Security Standard

Applies To:	All	Policy Number:	ITS-0041
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope

This standard describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the University.

Purpose

All routers and switches connected to the University production networks are affected. This document is broken in to two sections: Baseline routers and switches, and Perimeter routers and switches. All routers and switches will be configured to the baseline standard, perimeter devices have additional required controls.

Standard

Baseline:

1. No local user accounts are configured on the router. Routers must use RADIUS for all user authentication.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
    1. IP directed broadcasts
    2. TCP small services
    3. UDP small services
    4. All web services running on router
    5. Switch interfaces set with “dynamic” port negotiation
4. Use SNMPv3 and MD5 hashing.
5. All routing updates shall be done using secure routing updates.
6. Access control lists are to be added and modified as business needs arise.
7. A primary and backup point of contact must be provided for each router and switch on the University’s networks.
8. Each router must have the following statement posted in clear view:
   "This computer and network are provided for use by authorized members of the University of Detroit Mercy community. Use of this computer and network are subject to all applicable University policies,

including Information Technology Services policies. Any use of this computer or network constitutes acknowledgment that the user is subject to all applicable policies. Any other use is prohibited. Users of any networked system, including this computer, should be aware that due to the nature of electronic communications, any information conveyed via a computer or a network may not be private. Sensitive communications should be encrypted or communicated via an alternative method."

9. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.
10. Synchronize all clocks through the use of NTP.
11. An audit and logging strategy, based on the ITS Log Management Standard, must be utilized.
12. Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).

Perimeter:

1. Disallow the following:
    1. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses or the University public IP space
    2. Block IP packets that have the same source and destination
    3. Outgoing packets at the router sourced with invalid addresses, such as RFC1918 addresses
    4. All source routing
    5. CDP on Internet connected interfaces
    6. IP directed-broadcast
2. Implement black hole routing, or null routing
3. Disable network auto-loading via TFTP

History and Updates

July 1, 2016: Initial Policy