LAYER 2 SWITCH
SECURITY REQUIREMENTS GUIDE (SRG)
TECHNOLOGY OVERVIEW

Version 1, Release 0.1

20 July 2015

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

1.1 Executive Summary

Layer 2 switches are deployed at the access layer in enclave, data center, enterprise, and campus area networks to provide high-speed connectivity between end stations. Ethernet switching has played one of the most fundamental and essential roles in moving data reliably, efficiently, and securely across Local Area Networks (LANs). Applying best practice security measures to the upper layers does not benefit the network if Layer 2 is compromised. Attacks at the data link layer can cause traffic black holes, network outages, non-optimized forwarding, and redirection of traffic. Fortunately, features available on these critical network devices provide effective measures to protect the network traffic flow and the devices themselves. This Layer 2 Switch Security Requirements Guide (SRG) provides the guidelines and requirements for implementing security measures for Layer 2 Ethernet switches that will enable network operations to minimize the risk of a network outage or compromise.

1.1.1 Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

This Layer 2 Switch SRG is based on the Network. This Layer 2 Switch SRG contains general check and fix information that can be utilized for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

SRG Hierarchy example:

Application SRG
|__Database SRG
* |__MS SQL Server 2005 STIG*

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology

family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

1.1.2   SRG Naming Standards

In an effort to establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs the following applies:

{Core SRG value}-{*Technology SRG*}-{5- or *6-digit numeric sequence number*}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-NET-000001-VVSM-00001
SRG-OS-000001-UNIX-000001

Checks/Fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

1.2   Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include, but is not limited to: Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 SRG and STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of

environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7   Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. ASSESSMENT CONSIDERATIONS

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DoD systems, based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

3.   CONCEPTS AND TERMINOLOGY CONVENTIONS

A Layer 2 switch is a multiport bridge that learns about the Media Access Control (MAC) addresses of the connecting station on each of its switch ports. The learning of the MAC addresses for both ingress and egress frames to and from the attached stations enables the switch to create the Content Addressable Memory (CAM) table, commonly referred to as the MAC address table. Hence, the forwarding path of any received frame is determined by the MAC address table.

Unlearned unicast as well as broadcast and multicast packets are forwarded out to all switch ports belonging to the same broadcast domain. Bridging technology provides segmentation of LANs at the Layer 2 level into Virtual LANs (VLANs) thereby limiting the scope of broadcast domains. Internet Group Management Protocol (IGMP) snooping can help mitigate the flooding of IP multicast packets over a Layer 2 switched network by identifying which set of switch ports a packet is to be flooded on, that is, those switch ports whose attached host has subscribed to specific multicast groups.

A Layer 2 Ethernet-switched network can consist of many interconnected switches using both access and trunk links. An access link is carrying traffic for a single VLAN while a trunk link will carry traffic for multiple VLANs with each frame encapsulated via 802.1q VLAN tag. If there are redundant links connecting the switches, a loop can exist when all switch ports are in the forwarding mode. Hence, a packet with an unknown destination will cause a broadcast storm as the packet continues to loop infinitely. Spanning Tree Protocol (STP) prevents loops by blocking redundant paths and ensuring that only one active path exists between every two switches in the network. STP uses Bridge Protocol Data Units (BPDUs) that traverse the broadcast domain to identify which ports need to be blocked. The forwarding topology of the switched network is calculated and based on the STP root bridge position.

4. GENERAL SECURITY REQUIREMENTS

The network Layer 2 infrastructure provides the means to transfer data between network entities with interoperability and interconnectivity to the layers above. However, if the data-link layer is compromised, the layers above will also be compromised and not be aware of it. Security is only as strong as your weakest link and Layer 2 can be a very weak link. Hence, it is imperative to implement all applicable security measures that will mitigate the risks associated with attacks on the Layer 2 infrastructure.

Attacks such as VLAN hopping and Address Resolution Protocol (ARP) spoofing will enable an attacker to redirect or intercept traffic. Either of these compromises will provide the attacker an opportunity to hijack a session or launch a Denial of Service (DoS) attack. A compromise of the VLAN Trunking Protocol (VTP) can result in the deletion of all VLANs within the entire VTP domain. LAN floods (e.g., ping, UDP, MAC, etc.), broadcast storms, and CAM overflow attacks can completely cripple the network infrastructure.

The vulnerabilities created by the few minor flaws found in the STP can lead to an unstable topology that will disrupt service or can even result in a DoS. The attack vector for the STP is to alter the election of the root bridge creating suboptimal forwarding, enable a rogue switch to become the root bridge, or to hold the network in a constant state of reelecting the root bridge. The measures that can be taken to prevent these attacks should become a standard for basic security in LAN environments.

It can be difficult to protect against network misuse and attacks launched from hosts connected to the LAN. It is well known that the majority of compromises do occur internally. Hence, access to the network must only be provided to trusted personnel and hosts. Network access control measures using both port security and 802.1x authentication can aid in reducing the risk of an internal breach of the network.

Bandwidth capacity must be managed in order to provide preferential treatment for delay-sensitive and jitter-sensitive applications; thereby providing the necessary bandwidth during periods of congestion. A trusted boundary provides the ability to trust Quality of Service (QoS) priority settings for packets sent from an IP phone and disable the trust setting at the switch port if the phone is removed; thereby preventing malicious users from overriding QoS policies enabling them to abuse bandwidth resources.