APACHE 2.2 UNIX
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW

Version 1, Release 9

27 October 2017

Developed by DISA for the DoD

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Apache 2.2 Web Server Security Technical Implementation Guide (STIG) is a published document that can be used to improve the security posture of a Department of Defense (DoD) web server and its associated web sites. This document is meant for use in conjunction with the Enclave, Network Infrastructure, Application Security and Development, and other appropriate operating system (OS) STIGs. Guidance for deployment of web servers within the DoD intranet and the Demilitarized Zone (DMZ) will be governed by the appropriate Network Infrastructure STIG provided by DISA.

The web server must be configured to protect classified, unclassified, and/or restricted data such as Personally Identifiable Information (PII), as well as data approved for public release.

Immediate risks inherent to this role are external attacks and accidental exposure. Although security controls and infrastructure devices (such as firewalls, intrusion detection systems, and baseline integrity checking tools) offer some defense against malicious activity, security for web servers is best achieved through implementing a comprehensive defense-in-depth strategy. This strategy should include, but is not limited to, server configuration to prevent system compromise; operational procedures for posting data to avoid accidental exposure; proper placement of the server within the network infrastructure; and the allowance or denial of Ports, Protocols, and Services (PPS) used to access the web server.

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 provides 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.

1.3 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   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.

1.5   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 configuration 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 percent 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.

1.6   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 the 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. WEB SERVER AND SITE REQUIREMENTS

2.1   Open Source Software

Since Apache is open source software (OSS), it is subject to the controls placed on OSS used within the DoD. In many cases vendors embed Apache httpd server as part of their application suite. In these instances, it's the vendors' responsibility to ensure that their software (including Apache) is properly updated and patched. This responsibility should include compliance with IAVMs as well as any other vulnerability. The following link provides additional policy guidance on the use of OSS in the DoD domain:

http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx

It is always recommended with all web server installations that sample files, source code, default HTML, and sample scripts be removed. Additionally, in the case of Apache many of the modules that are supplied in the distribution are not necessary and in some cases may be vulnerable in certain circumstances. It is highly recommended that unused Apache modules be removed, or not included in the compiled application.

2.2   Assumptions

The STIG requires that the covered directives be explicitly set in the configuration files. This avoids the risk that changes to the application defaults will leave the web server vulnerable.

Further standardization provides an explicit security standard to follow. If sites cannot meet these requirements they should follow the processes in place to account for the risk (POAM, DRA, etc.).

The Apache STIGs support a standard installation where the installation files were downloaded from the Apache Software Foundation httpd project website; no recompiling of the source code was done; and the software is installed in the default directories (for Unix /usr/local/apache2x/; Windows Server 2003\2008 on 2.0 [Drive Letter]:\Program Files\Apache Group\apache2x; Windows Server 2003\2008 on 2.2 [Drive Letter]:\Program Files\apache2x\).

The Apache STIG checks don't specifically address the Include directive. However, you should check for the existence of any uncommented (i.e., no "#") Include directives within the httpd.conf. If active Include directives are found, Include files or directories are used. The entry after the Include directive statement indicates the location of other configuration information.

Navigate to the location(s) specified in the Include statement(s), and review each file for every directive required in the guidance.

The Apache STIGs discourage the use of .htaccess files. .htaccess files are discouraged since the ability to centrally manage an Apache server is lost when they're enabled. Additionally, their functionality can be accomplished via other methods. If you decide to use .htaccess files,

the following could be used as a process for determining their location when reviewing the server:

- Open the httpd.conf file and any included files with a text editor, such as Notepad or VI, to see if there are enabled .htaccess files. Within the httpd.conf and included files search for the following uncommented (i.e., enabled) directive: AllowOverride. If any enabled AllowOverride directive is not followed by "None", this indicates .htaccess files are used. The .htaccess files that are enabled are enforced in the directory specified by the "Directory" directive preceding the AllowOverride directive.

If .htaccess files are found it's recommended to review them against all applicable Directives (i.e., O p t i o n s , etc.) as describe at the Apache Software Foundation website.

The STIG checks don't specifically address additional, or multiples of, CGI and DocumentRoot directories. However, you should check for the existence of additional directories. Each entry after an uncommented ScriptAlias, Alias and ScriptAliasMatch directive indicates a CGI directory. All checks against the CGI directories should be applied to each directory. Each entry after an uncommented DocumentRoot directive indicates a DocumentRoot (Web Content Home) directory and all checks against the DocumentRoot directory should be applied to each directory.

Additionally, in the case of Apache, certain modules included in the distribution may be unnecessary and may add additional unnecessary vulnerability to the system. Where feasible it is h i g h l y recommended that Apache be compiled with only the necessary or core modules included. Dynamically loaded modules are often enabled as part of a distribution and are unnecessary, which may add additional vulnerabilities to the system. Dynamically loaded modules that are not n e c e s s a r y should be commented out in the configuration to eliminate additional risk.

2.3   Web Server and Site Definition

A web server is an automated information system that manages one or more web sites by passing or serving up web pages to an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer. This document is only applicable to web servers and sites.


2.4   Web Policy - Applicable to All Web Servers and Sites

Web policy requirements are applicable to all web servers and sites. Review Web Policy checks for all web servers or sites (classified or unclassified) that are used to process, transmit, store, or connect to DoD information or enclave resources. These checks should be reviewed before web server- and web site-specific technology checks are implemented. These policies are listed in the Vulnerability Management System (VMS) under the Non-Computing assets, Web Policy asset posture. The reviewer should create one non-computing asset for policy checks, one computing asset for a web server review, and one computing asset for each web site hosted on the reviewed web server.

2.5   Web Server and Site Topology

Web server and sites operating within an enclave are segregated as one of many hardening initiatives that can be used. The approach, to meet this initiative, is to quarantine public-facing applications and to protect them. Additionally, protections are built into the architecture to   segregate restricted and unrestricted applications from private applications. The figure below provides a visual representation of a typical Enclave.

Figure 2-1: Typical Enclave Network
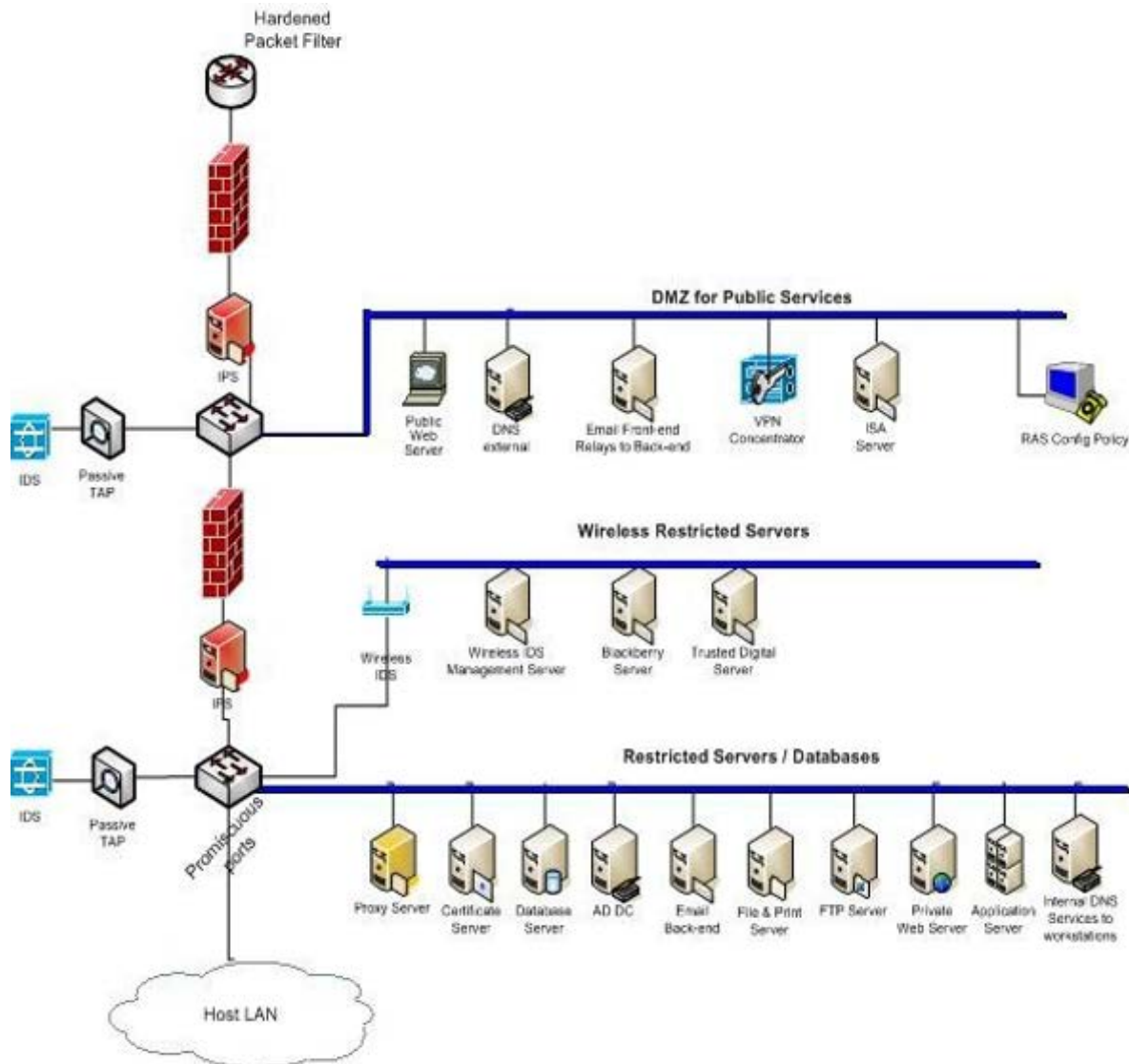
2.6   Roles

The roles of the SA and the web administrator or web master are generally understood but are often used interchangeably. The SA is responsible for the OS, while the web

administrator or web master usually manages the web site or sites. In some cases, the SA is also the web administrator/web master which is why guidance tends to be written in a certain fashion. The application development group should refer to the supporting organization for the application when application issues arise from meeting Apache STIG requirements. This guidance does not cover every unique application and configuration.