MICROSOFT EXCHANGE SERVER 2010 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 6

22 January 2016

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 2
1.4 STIG Distribution 2
1.5 SRG Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 3
1.8 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Security Assessment Information 4
2.2 Exchange Management Shell 4
2.3 Pre-review Procedure 4
2.3.1 Email Domain Security Plan 4
2.3.2 Email Domain Servers and Settings 5
2.4 SRR Method 5

3. CONCEPTS AND TERMINOLOGY CONVENTIONS {OPTIONAL} 6

3.1 Introduction 6
3.2 Exchange Server Roles 9
3.2.1 Mailbox Server 9
3.2.2 Client Access Server 9
3.2.3 Hub Transport Server 9
3.2.4 Edge Transport Server 9
3.2.5 Unified Messaging Server 10
3.2.6 Email Services Policy STIG 10
3.3 Email Data Overview 10
3.4 Message Access Path 10
3.5 Message Transport Path 11

4. REFERENCE DOCUMENTS 13

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2
Table 4-1: Reference Documents..... 13

LIST OF FIGURES

Page

Figure 3-1: Microsoft Exchange 2010 Architecture Overview 8
Figure 3-2: Message Access Path 11
Figure 3-3: Message Transport Path 12

1. INTRODUCTION

1.1 Executive Summary

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks, as addressed in the technology section. These requirements are designed to assist System Managers (SMs), Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls.

Email systems are composed of multiple products and services working together to enable transport and delivery of messages to users. This overview gives technology-specific background and information specific to Microsoft Exchange email servers. Included also are security review considerations to prepare for periodic assessments.

The associated Security Technical Implementation Guide (STIG) provides security policy and configuration requirements for the Microsoft Exchange Server 2010 application. There are five roles within the Microsoft Exchange Server 2010 architecture: Mailbox Server, Client Access Server, Hub Transport Server, Edge Transport Server, and Unified Messaging Server.

Currently there are STIGS for four of the five roles available for the Microsoft Exchange Server architecture: Mailbox Server STIG, Client Access Server STIG, Hub Transport Server STIG, and Edge Transport Server STIG. There is no STIG for the Unified Messaging Server.

An Email Services Policy STIG is also available that governs DoD installations that are non-technical directives and must be part of every Exchange security review.

The Microsoft Exchange Server 2010 Server STIGs and Email Services Policy STIG can be referenced on the IASE (Information Assurance Support Environment) website at the following URL: http://iase.disa.mil/stigs/app-security/app-servers/Pages/index.aspx

There are five STIGS available for Microsoft Exchange Server 2010:

- Exchange 2010 Mailbox Server STIG
- Exchange 2010 Client Access Server STIG
- Exchange 2010 Hub Transport Server STIG
- Exchange 2010 Edge Transport Server STIG
- Email Services Policy STIG

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.

1.3 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 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 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 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.

1.7 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.

1.8 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. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The Microsoft Exchange Server 2010 Security Readiness Review (SRR) ensures the site has properly provisioned and implemented the application and it is being managed in a way that is secure, efficient, and effective. The STIG identifies vulnerabilities that undermine security, in that they have the potential to affect the confidentiality, integrity, or availability of email services. The items reviewed are based on standards and practices published by the DoD, their contractors, and other security guidance entities, following guidance published in the Department of Defense Instruction (DoDI) 8500.2 and National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 security controls.

Defense Information Systems Agency (DISA) has assigned a level of urgency to each finding based on Chief Information Officer (CIO) established criteria for Certification and Accreditation (C&A). All findings are based on regulations and guidelines. All findings require correction by the host organization.

2.2 Exchange Management Shell

The Exchange Management Shell, built on the Windows Power Shell technology, provides a powerful command-line interface for Microsoft Exchange Server 2010 that enables automation of administrative tasks. With the Shell, you can manage most aspects of Exchange. Several checks and fixes in the STIG are only available through the use of the cmdlets.

Open the Exchange Management Shell and use the following steps:

Click Start >> All Programs >> Microsoft Exchange Server 2010
Click Exchange Management Shell

Note: The Windows Power Shell is also used to perform several Operating System (OS) and Internet Information Services (IIS)/Client Access (CA) checks.

2.3 Pre-review Procedure

2.3.1 Email Domain Security Plan

It is a best practice and a DoD requirement for systems to have a documented security plan. Because there are additional, unique system attributes that pertain to email applications, a separate plan-within-a-plan is recommended and is referred to as the Email Domain Security Plan (EDSP). Email domains are entities whose configurations not only affect internal system behaviors but also affect interaction between email domains. Settings such as certificate names for authentication, mailbox size quotas, or partner domain interaction can be unique for sites. Also, depending on domain size and network type, certain tuning parameters must be set optimally to ensure reliable message throughput.

The Exchange STIG requires that these values be deliberately set and documented to confirm the system is configured as engineered. Obtaining the email system configuration specifics as identified in the EDSP will aid the reviewer in comparing values set to values documented.

The National Institute of Standards and Technology Special Publications in the 800 series are of general interest to the computer security community. This series reports on ITL's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. The NIST 800 series Special Publications can be referenced at: http://csrc.nist.gov/publications/PubsSPs.html.

NIST publication SP800-53, which is publicly available, is entitled "Security and Privacy Controls for Federal Information Systems and Organizations". The SP800-53 provides information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

NIST publication SP800-18, which is publicly available, is entitled "Guide for Developing Security Plans for Federal Information Systems". The SP800-18 provides both guidelines and a template for security plan creation and can serve as a base for development.

2.3.2 Email Domain Servers and Settings

The following commands will provide the exchange environment information that will be needed to perform a review. The reviewer will be able to determine the roles of each server that is configured to perform and determine if servers are providing multiple roles. The exchange environment could consist of two servers or as many as twenty in a large enterprise. The commands can be piped to a text file for reference during the review.

```
Get-ExchangeServer | Format-List Name, ServerRole Get-MailboxServer | Format-List Name, Identity
Get-TransportConfig | Format-List
```

To pipe the results to a file use the following command:

```
Get-TransportConfig | Format-List > c:\temp\filename.txt
```

Note: The cmdlets are not case sensitive. They may be entered in uppercase, lowercase, or any combination of both to return results. The commands are written to make the command more intuitive by using uppercase and lowercase characters.

2.4 SRR Method

To perform a successful SRR, this document and accompanying STIGs' data provide the methods to assess vulnerabilities on deployed Microsoft Exchange Servers. The review process is manual.

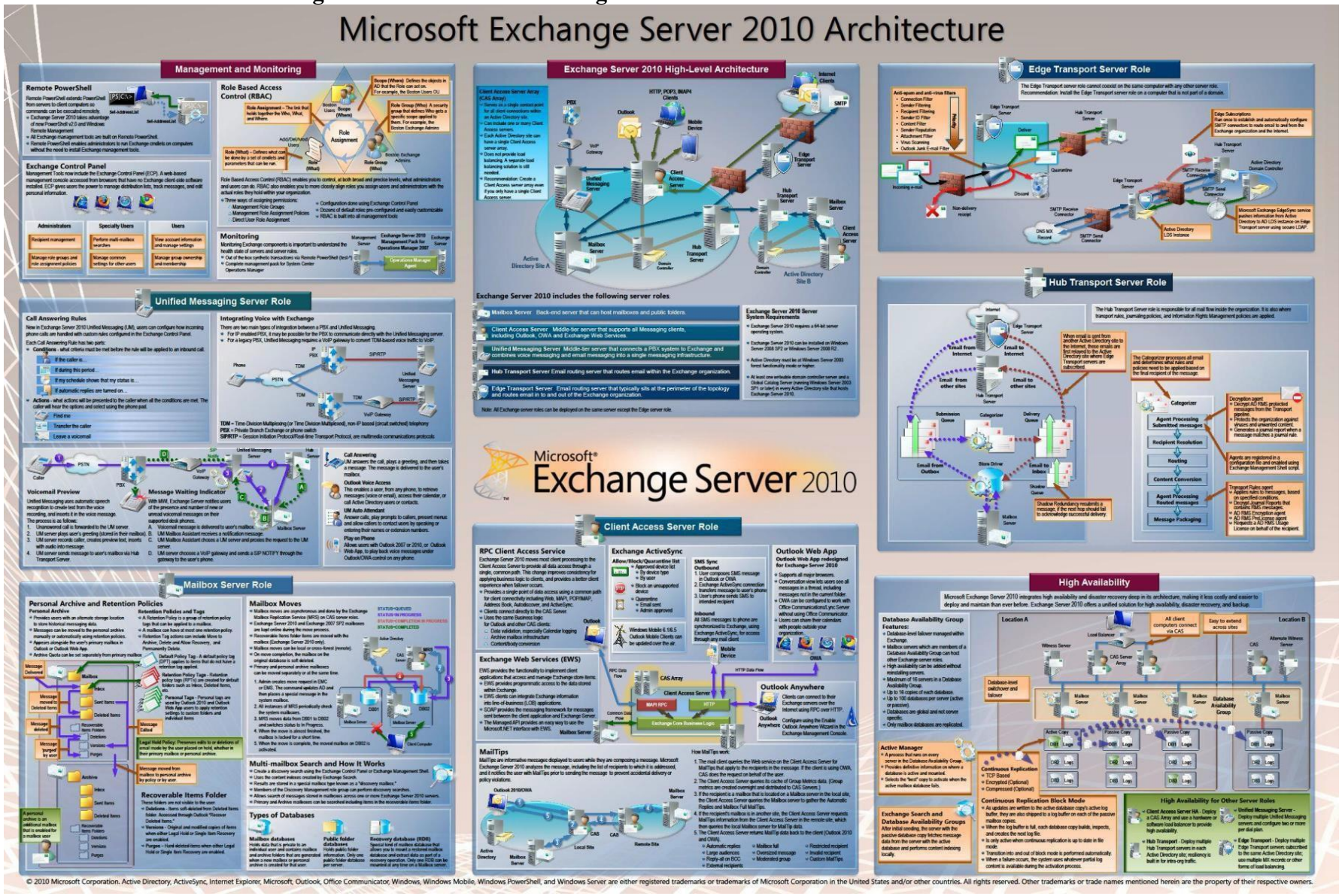
3. CONCEPTS AND TERMINOLOGY CONVENTIONS {OPTIONAL}

3.1 Introduction

Microsoft Exchange Server 2010 is a 64-bit email application currently licensed and distributed to the DoD by the Microsoft Corporation. Microsoft Exchange Server 2010 is compatible with Microsoft Windows 2008 Server SP2 or newer.

The Microsoft Exchange Server 2010 STIG was created using a Windows 2008 R2 Domain controller with three member servers running the Mailbox, Client Access, and Hub roles. A standalone Windows 2008R2 Server with the Edge Transport role installed was also included in the infrastructure.

Figure 3-1: Microsoft Exchange 2010 Architecture Overview



3.2 Exchange Server Roles

3.2.1 Mailbox Server

The Mailbox Server role hosts mailboxes and advanced scheduling services for Microsoft Office Outlook and Microsoft Outlook Web App users. In addition, Mailbox servers may also host public folders, if desired. In all, the Mailbox Server role provides a foundation for workflow, document sharing, and other forms of collaboration. The Mailbox Server STIG must be reviewed on each Mailbox Server in the Exchange environment.

3.2.2 Client Access Server

The Client Access Server role is the initial point of contact for end users seeking email access. Applications such as Outlook Web App (OWA), Outlook Anywhere (OA), and Outlook, as well as mobile technologies servers and public folders requests, are processed through the Client Access Server. Commercial mobile devices (CMD) communicate with the Client Access Server through protocols such as Exchange ActiveSync (EAS) to provide email services.

Current CMD policy (DoD CIO memo dated 6 Apr 2011) requires mobile devices to communicate using Mobile Email Management (MEM) servers that act as intermediaries between the email server and the CMDs. The Client Access Server also depends on Microsoft IIS web services, which must be reviewed prior to performing the Client Access Server review.

3.2.3 Hub Transport Server

The Hub Transport Server role handles all mail flow to and from Mailbox Servers. Among its capabilities are transport rules behaviors, some SPAM and sanitization capabilities, and secure message transport to the message batch "next hop". Messages outbound toward the Internet are relayed by the Hub Transport Server to the Edge Transport Server role at the perimeter network, before they are sent to another email domain. Inbound messages received by the Edge Transport Server role are passed to the Hub Transport Server for routing to another Hub Transport Server or to a destination Mailbox Server. The Hub Transport Server guidance must be reviewed in each environment that hosts a Mailbox Server role.

3.2.4 Edge Transport Server

The Edge Transport Server role is deployed in an organization's perimeter network. Designed to minimize the attack surface, the Edge Transport Server role handles all Internet-facing mail flow, providing SMTP relay and smart host services for the Exchange organization.

The Edge Transport Server role, as the first point of contact for inbound message batches, performs tasks such as Sender Authentication, SPAM evaluation, enabling attachment stripping policies, archiving filtered messages, logging activity results, and alerting administrators to findings. The Exchange Edge Transport Server guidance must be used when Microsoft Exchange 2010 is deployed in the Edge Transport Server role.

3.2.5 Unified Messaging Server

The Unified Messaging Server role combines voice messaging and email for users, which can be accessed from the telephone and the computer. Unified Messaging integrates Exchange Server 2010 with the telephony network in the organization and brings the features found in Unified Messaging to the core of the Exchange Server product line.

The Exchange Server 2010 STIG does not address the Unified Messaging Server role.

3.2.6 Email Services Policy STIG

Policies that govern DoD installations are non-technical directives that must be part of every Exchange security review. Included are items such as performing regular conformance reviews, backups, and role-based assignment separation. Policies contribute to best practices for security in depth and continuity of operations.

Policies review is required for every email domain, regardless of the deployed email services product.

3.3 Email Data Overview

Email data travels on two paths. One is the message transport path, which primarily uses Simple Mail Transfer Protocol (SMTP) and moves messages from one domain (the sending domain) location to another (the receiving domain). Process steps for email messages as they traverse the message transport path include domain identification, session encryption and authentication, message sanitization for SPAM and virus content, and message delivery to identified recipients.

The other path is the "message access" path, which enables users to reach their delivered messages or create new messages. It is typical for sites to offer more than one message access path for users to access messages, as users often travel off-site or require multiple devices that are email enabled. Message access paths include via Microsoft Outlook client, Outlook Web App (OWA), Outlook Anywhere, and Active Sync (mobile devices).

Email threats include SPAM and SPOOFED content, often inserted at an unsecured point in the message transport path. Inbound email often contains PHISHING and PHARMING attacks, forged messages, embedded malware, or may be signed with a counterfeit certificate, all created for the purpose of compromising email recipients' systems or data. Appropriate security measures that prevent unsecured insertion points in the message transport path are essential in preventing most SPAM. Other measures include processes to evaluate sending domains, message content, or attachment composition. Each of these results can then be used to "score" and possibly filter suspicious messages if they appear to be a potential problem for the recipient.

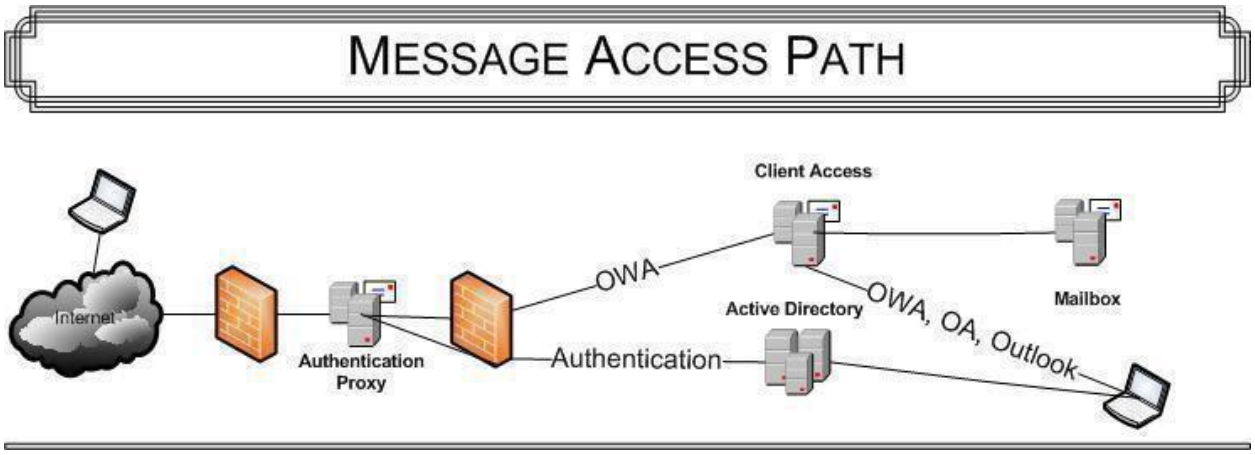
3.4 Message Access Path

There are a number of network paths that enable end users to access messages on mailbox servers. For local users inside enclave environments, LANs provide the most direct access for

desktops provided they are configured with Outlook and CAC authentication hardware and software. Off-site users may also have access to Virtual Private Network (VPN) connectivity, which enables use of Outlook from off-site locations. For sites offering Outlook Web App (OWA), off-site users may elect to access email messages using browsers (such as Microsoft Internet Explorer [IE] 8.0) with an Internet connection.

All client requests for message access use HTTP to attach to the Client Access server. The CA server then issues Remote Procedure Calls (RPC) to the user mailboxes. Use of OWA from remote locations, such as the public Internet, must use TLS but authenticate and off-load encryption prior to entering the enclave, to enable traffic inspection. The proxy server can then impersonate the requestor for the remainder of the access request.

Figure 3-2: Message Access Path



3.5 Message Transport Path

Message transport primarily uses Simple Mail Transfer Protocol (SMTP). SMTP was not created with security in mind; therefore, all security precautions are add-ons that aid with confidentiality and integrity protection while en route to their destinations. While being transported, messages are relayed from server to server, sometimes crossing unsecured networks, such as the public Internet. It is in such environments that messages can be trapped, modified, copied, or subject to other mischief during unsecured SMTP message transfer.

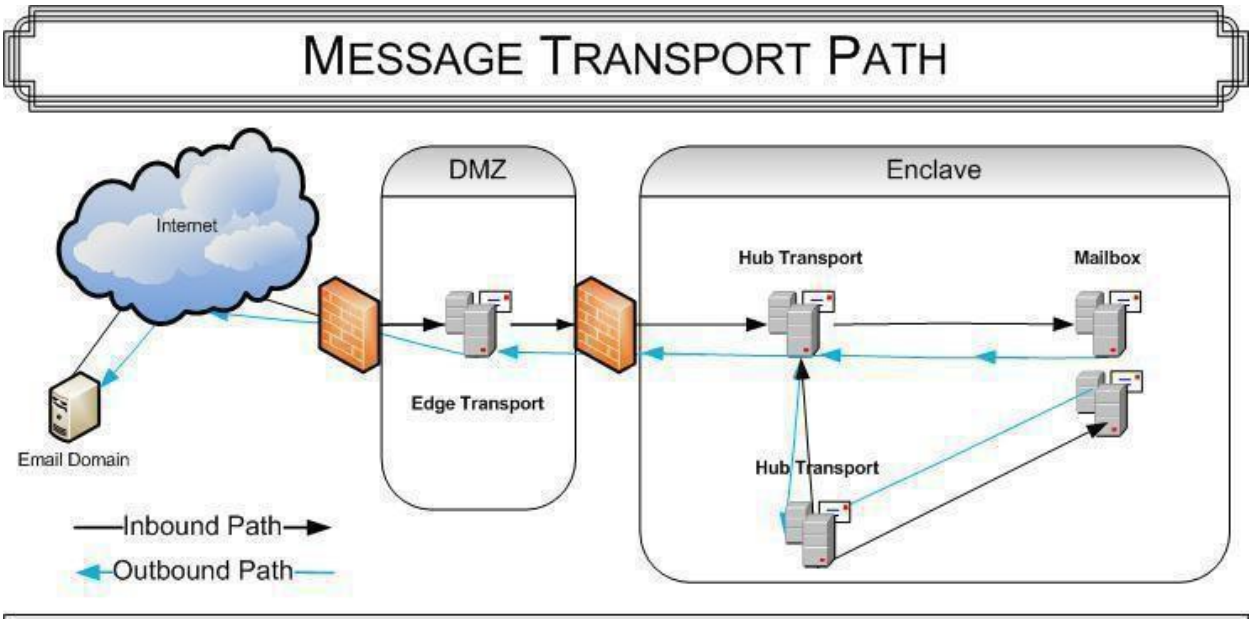
It has become a tenet of email message delivery that all message hand-offs be managed using authenticated connections and TLS encryption using server certificates. By eliminating unsecured transport connections, the risk of SPAM insertion is significantly reduced.

Because email domains must interact with other domains originating across unsecured networks, it is critical that a robust Edge Transport server role be deployed as the first point of contact for inbound message delivery requests. By using a number of techniques, an Edge server's tasks examine and evaluate attributes of the source domain, the message envelope, and rate for SPAM and malware potential. Careful examination of inbound messages helps protect the enclave from Internet-sourced threats. Similarly, outbound message scanning helps protect the domain from

reputation damage by ensuring domain-based threats are thwarted before being transported to remote email domains.

Once admitted to the email environment, messages are handed to a Hub transport server, whose role is similar to that of a traffic manager. The Hub transport server directs messages to users' mailbox servers, where they can be accessed by email-enabled domain users.

Figure 3-3: Message Transport Path



4. REFERENCE DOCUMENTS

The following table enumerates the documents and resources referenced:

Table 4-1: Reference Documents

Date	Document Description	Source
2010	Microsoft Exchange Server 2010 Best Practices	Microsoft Press
January 2012	Microsoft Exchange Server 2010: Help	technet.microsoft.com
Current Version	Windows 2008 R2 STIG	iase.disa.mil
March 2012	Microsoft Exchange 2010 Security Guide	technet.microsoft.com
April 2013	SP 800 -53 Security and Privacy Controls in the Federal Information Systems and Organizations	http://csrc.nist.gov/publications/PubsSPs.html
February 2006	SP 800 -18 Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/PubsSPs.html