Security Target for

NoSpamProxy Server

Version 14

Version 1.0, 14.11.2023

Table of Contents

Introduction

Context

This document is the Security Target (ST) description for the BSZ certification of “NoSpamProxy Server“ running on a dedicated Windows Server 2022 machine (Target of Evaluation – TOE) by the Bundesamt für Sicherheit und Informationstechnik (BSI).

It was created by Dr. Horst Joepen, external advisor to Net at Work GmbH. Technical contributions and review were done by Jan Jäschke, Product Manager NoSpamProxy at Net at Work GmbH. This document was released by Stefan Cink, Business Unit Manager NoSpamProxy at Net at Work GmbH.

Product Identification

TOE name: NoSpamProxy Server

TOE version: NoSpamProxy Server 14.0.5.62

The TOE name and version are displayed and can be checked in the NoSpamProxy Command Center (NCC) of the TOE.

The TOE version is deployed on Windows Server 2022, Build 20348.1787 released on 2023-06-13 .

Abbreviations and Acronyms

AD	Active Directory
BSI	Bundesamt für Sicherheit in der Informationstechnik
AIS	Anwendungshinweise und Interpretations zum Schema (BSZ documents by BSI)
BSZ	Beschleunigte Sicherheitszertifizierung
MMC	Microsoft Management Console
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightwight Directory Access Protocol
MTA	Mail Transfer Agent
NCC	NoSpamProxy Command Center
NSP	NoSpamProxy
IP	Internet Protocol
IT	Information Technology
PII	Personally Identifiable Information
RDP	Remote Desktop Protocol
RFC	Request for Comments (IETF Standard)
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target

TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL Safeguard	NoSpamProxy function to rewrite hyperlinks in emails
WAN	Wide Area Network
WCF	Windows Communication Foundation Security

References

RFC 8446	Transport Layer Security Protocol Version 1.3	https://datatracker.ietf.org/doc/html/rfc8446
RFC 5246	Transport Layer Security Protocol Version 1.2	https://datatracker.ietf.org/doc/html/rfc5246
RFC 8314	Use of Transport Layer Security for Email Submission and Access	https://datatracker.ietf.org/doc/html/rfc8314
RFC 5411	Lightwight Directory Access Protocol (LDAP) : The Protocol	https://datatracker.ietf.org/doc/html/rfc4511
RFC 8551	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0	https://datatracker.ietf.org/doc/html/rfc8551
RFC 7230	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	https://datatracker.ietf.org/doc/rfc7230/
RFC 5321	Simple Mail Transfer Protocol	https://datatracker.ietf.org/doc/html/rfc5321
RFC 6234	US Secure Hash Algorithms (SHA)	https://datatracker.ietf.org/doc/html/rfc6234
RFC 1851	ESP Triple DES Transform	https://datatracker.ietf.org/doc/html/rfc1851
RFC 2437	PKCS#1: RSA Cryptography Specification 2.0	https://datatracker.ietf.org/doc/html/rfc2437
IEEE 1363	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings	https://ieeexplore.ieee.org/document/891000
FIPS 197	Advanced Encryption Standard (AES)	https://csrc.nist.gov/publications/detail/fips/197/final
SP800-38A	Recommendation for Block Cipher Modes of Operation	https://csrc.nist.gov/publications/detail/sp/800-38a/final
SP800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode and GMAC	https://csrc.nist.gov/publications/detail/sp/800-38d/final
ANSI X9.62-2005	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	
RFC 4880	Open PGP Message Format	https://datatracker.ietf.org/doc/html/rfc4880

Product Description

Product Overview

NoSpamProxy is an email security software that receives and sends emails for organizations and provides state-of-the-art email security functionality. There is a total of four NoSpamProxy modules that can be combined with each other: NoSpamProxy Protection, NoSpamProxy Encryption, NoSpamProxy Large Files and NoSpamProxy Disclaimer.

The scope of the evaluation is limited to the functionality and operation on a single system. Focus of the security testing is on self-protection of the TOE against attacks.

NoSpamProxy is deployed in a company network and needs to be the first system receiving and processing incoming emails (MTA). The software communicates with external as well as an organization‘s email server via the SMTP protocol. Administrators can access NoSpamProxy via HTTP (secured via certificates) and configure it. This makes it possible to apply corporate email security policies and to all inbound and outbound emails.

S/MIME certificates and PGP keys of corporate users and external communication partners are centrally stored and managed in NoSpamProxy.

As user management is centralized in most organizations using Active Directory (AD) or other LDAP protocol-based services, AD settings are utilized by NoSpamProxy and can be used to determine which rules have to be applied to inbound or outbound emails for a single user or groups of users.

Architecture Overview

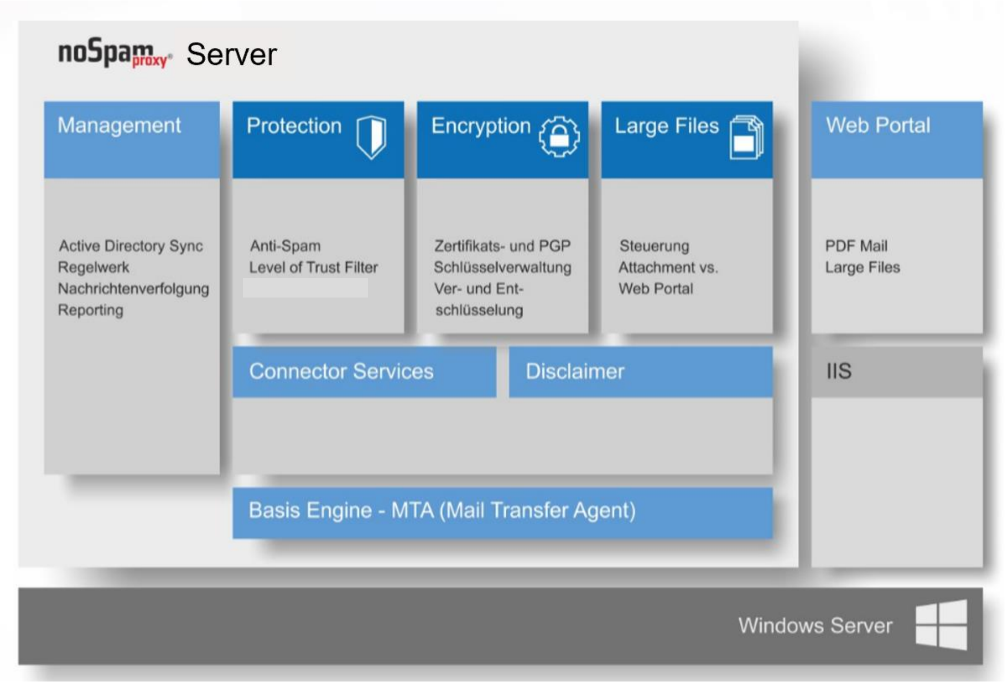

Figure: TOE Architecture Overview

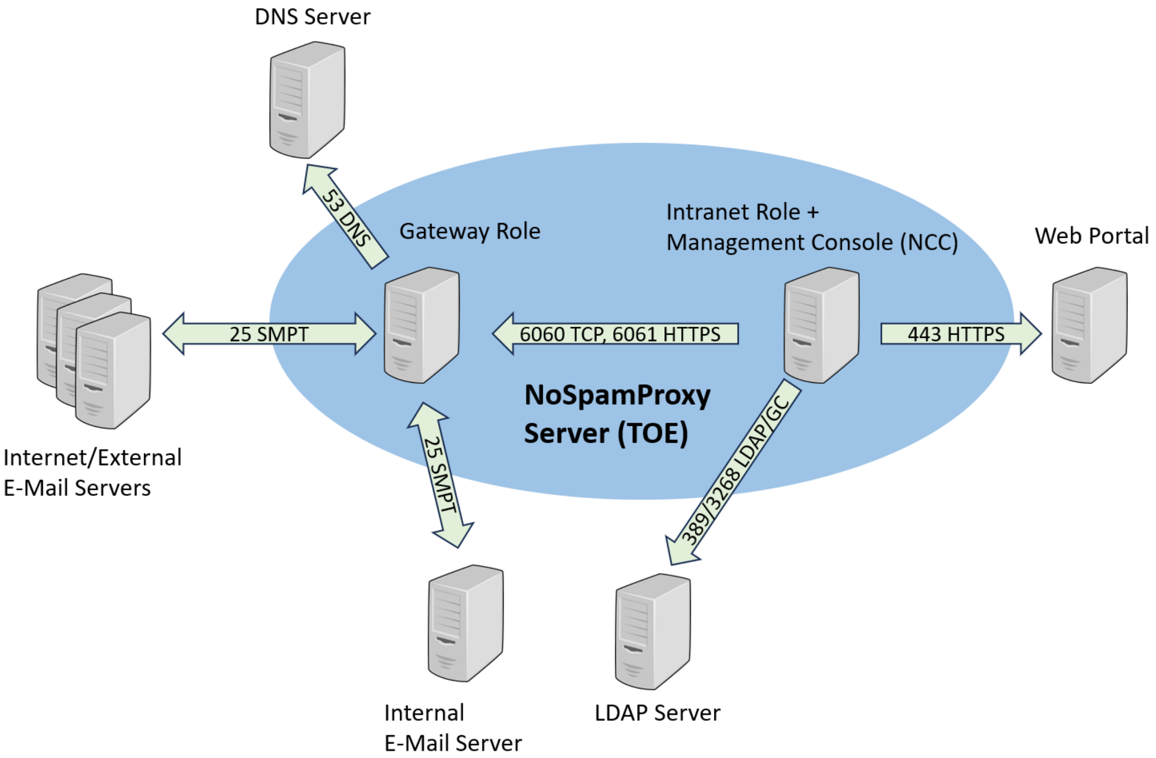

Figure: Deployment of the TOE and used communication protocols and ports

Features

Module Protection: Spam and Malware Protection

The module NoSpamProxy Protection scans inbound emails for spam and malware and rejects emails identified as spam, emails that contain malware, and emails that otherwise violate the organizations policy configured in the settings of NoSpamProxy Protection. It also scans outbound emails to prevent compromised mailboxes from distributing spam and malware using an organization’s domain. To do this, it applies a variety of scanning and filtering methods. External services are also used for this purpose but are outside the scope of this evaluation.

The reliability and quality of the spam and malware protection is critical to protect users and the organization from malware and phishing attacks. Therefore, the protection level is regularly tested by an independent organization. Results are published and can be viewed at https://www.virusbulletin.com/testing/results/recent/vbspam-email-security/netatwork-nsp . Instead, the focus of the evaluation is on self-protection as mentioned before.

Module Large Files: Secure Transfer of Large Files

The Large Files module provides a secure transfer method for files which are too large to be sent as email attachments. It uses the web server provided by the operating system (Windows Internet Information Server) for the secure upload and download of messages and files via HTTPS. The Large Files module is outside the scope of this evaluation

Module Encryption: Encryption and Decryption of Emails

The Encryption module combines the signing, encryption, and decryption of emails with centralized key management. Encryption methods supported are S/MIME, PGP, and password-protected PDF containers. NoSpamProxy stores all public keys from signed inbound emails and centrally stores all S/MIME certificates and PGP keys for entitled users in an organization. By using this internal key repository of NoSpamProxy and by connecting to publicly available and trusted public key servers, automatically encrypted communication can be achieved at a large scale with very little effort. PDF functionality of the Encryption module is outside the scope of this evaluation due to inherent limitations of PDF standard.

Module Disclaimer: Generation of Disclaimer Texts

The Disclaimer module appends or inserts so-called disclaimer texts or trailers based on Active Directory groups and other common patterns. Provided they have the necessary role, administrators can define disclaimer texts and graphic elements using a browser-based editor. Disclaimers can be applied on outbound and inbound emails.

Interfaces

The TOE supports and uses one WAN Ethernet port which is the only physical connection to access the TOE. Both the Intranet role (control) and Gateway role of NoSpamProxy are installed on the same physical or virtual Windows server and communicate internally via port 6060 (HTTP with message level security using certificates and port 6061 (HTTPS) as shown in the architectural overview in the appendix. When the module Large Files is used there is a need to also install the Web portal on the Windows server utilizing the Internet Information Server (IIS) which is part of the Windows Server operating system. All services using outbound connections are listed in the following table.

List of outbound connections (port 6061 – HTTPS)

Module	Service	Enabled by defalt	Address
Core Antispam Engine	Pattern and signature files	yes	https://av-patterns.nospamproxy.com/; nimbus.bitdefender.net
Gateway Role	Public Suffix List	yes	https://publicsuffix.org/list/public_suffix_list.dat
	Office365 tenant verification	yes	Standard Azure Cloud: https://login.windows.net German Azure Cloud: https://login.microsoftonline.de
	NoSpamProxy Services	yes	https://service.nospamproxy.de CSA: /CSAWhitelist
	32Guards	yes	https://heimdall.cloud.nospamproxy.com
	NoSpamProxy licensing	Yes	https://license.cloud.nospamproxy.com

	Freemailer; URL Safeguard allow list	Yes	https://nospamproxynaw.blob.core.windows.net/freemailer/freemailer.txt
Intranet Role	Public Suffix List	Yes	https://publicsuffix.org/list/public_suffix_list.dat
	Azure Active Directory	No	https://graph.microsoft.com https://login.microsoft.online.com
Management Console	News Feed	Yes	https://www.nospamproxy.de
	NoSpamProxy services	Yes	https://service.nospamproxy.de

Management Services

The administrator can manage the TOE using the following interfaces:

Web App Message Tracking: An HTTPS service provide a graphical user interface to manage the email flow of the organization, including locating, analyzing, releasing, and putting on hold specific emails as well as creating reports. In addition, the Disclaimer is managed using this user interface as well.

NoSpamProxy Command Center (NCC):

The command center is used to monitor the NoSpamProxy operation as well as to create and manage users and identities. The NCC provides functions for the configuration of NoSpamProxy such as send and receive connectors and filtering rules and policies. Furthermore, troubleshooting is done via the NCC which can be configured to generate logfiles, to perform automatic checks and to correct specific settings. NCC is a Web App using WCF (HTTP protocol with content encryption using the self-signed NoSpamProxy certificate) and HTTPS for secure access by administrators.

To operate NoSpamProxy in the certified configuration it must be administrated local via the NCC.

Product Usage

General Concepts

The product is an email security software that needs to be installed and configured on a Windows Server physical or virtual machine. It is designed to run in a local and secure network with state-of-the-art protection such as firewalls which allows connections to the TOE only via the specified ports. It is recommended to also use the Windows Firewall to further protect the system. The TOE automatically processes inbound and outbound emails, acting as a Mail Transport Agent (MTA). It can accept or reject emails, put emails on hold for automatic or manual release, and convert office document formats containing active content into non-hazardous PDF documents.

While administrators have access to the message tracking to manage an organization’s email flow, focus is on the fully automated processing of emails with minimum administration effort for administrators. The TOE is fully transparent to the user with support for the users’ email client, i.e., Microsoft Outlook to send and receive emails.

Usage by Administrators

There are four administrator roles: NoSpamProxy Configuration Administrator, NoSpamProxy Identities Administrator, NoSpamProxy Monitoring Administrator, and the NoSpamProxy Disclaimer Administrator. Users in the “NoSpamProxy Monitoring Administrator” group can use the Message Tracking Web App and the NCC to perform the following tasks:

- Message tracking
- Checking of email queues
- Releasing emails put on hold
- Reporting
- Checking of the event log

Users of the “NoSpamProxy Identities Administrator” group can use the NCC to perform the following tasks:

- Managing domains and users
- Managing certificates and keys
- Managing partner settings and trust levels of communication partners
- Managing public key servers
- Managing DKIM keys and trusted ARC signers

Users of the ““NoSpamProxy Configuration Administrator” group can use the NCC to perform the following tasks:

- Define filter rules
- Define encryption rules
- Configure email routing
- Define attachment filter rules
- Configure URL-Safeguard
- Configuring advanced settings
- Database management
- SSL/TLS configuration
- SMTP configuration

Users in the “Disclaimer administrator” group have access to a web interface which allows them to define so called text signatures of emails, define content elements as placeholders for name, address and phone number of a user which are to appear in the text signature. The Disclaimer administrator cannot access actual personal data.

Usage by Users

Users have no direct or indirect access to the TOE. The TOE processes emails sent or received by a user, depending on the settings and rules defined by the NoSpamProxy administrators. Disclaimer texts will be added to emails sent by users depending on the disclaimers and rules defined by the disclaimer administrators. When enabled in the TOE configuration, users can use keywords in the email subject, e.g., to instruct NoSpamProxy to encrypt specific emails.

Operating Environment

A Windows Server operating system installed on a physical or virtual machine is required. The TOE is designed to be installed in environments with physical access restrictions and trusted administrators.

Administrators can have physical access to the TOE for physical installation. They can manage the TOE using the following protocols over IPv4:

- Web App: HTTPS
- NCC: HTTPS and HTTP with message level encryption based on certificates (WCF)

Users have no physical or logical access to the TOE.

To operate NoSpamProxy in the certified configuration it must be administrated local via the NCC.

Security Perimeter

Assumptions

- **Assumption.FirstMailGateway** – The TOE is the first instance receiving emails for an organization’s email infrastructure. The TOE’s internet address must be placed in the MX record of the DNS entry for the organization’s domain. This is required to ensure that NoSpamProxy can decrypt received emails and apply all security checks to the email content or directly reject the acceptance of the email. Otherwise, an attacker could send malware contained in encrypted emails undetected, or emails violating policies or security rules can enter the organizations IT infrastructure and represent unmanageable security risks.
- **Assumption.PhysicalAccess** – There is a state-of-the-art protection of the TOE from physical access and physical access shall be limited to trusted personnel. Otherwise, an attacker could perform physical attacks against the TOE.
- **Assumption.NetworkSecurity** – the TOE is expected to be installed in a secured and local network which is protected by state-of-the-art firewall systems. Otherwise, the server on which the TOE is installed could be attacked from the Internet.
- **Assumption.AdminNoEvil** – the administrator of the TOE shall be trustworthy. Otherwise, the administrator could misconfigure the TOE not to fulfill its security services, e.g., allow emails with potentially dangerous attachments to be delivered to mailboxes of users in the organization.
- **Assumption.AdminKnowHow** – The Administrator of the TOE shall be able to configure the TOE in a way that results in a secure configuration meeting the organizations policies and security requirements. The Administrator also must be knowledgeable about potentially harmful filetypes so that he does not accidentally release a dangerous file to users.
- **Assumption.OnlyAdminUsers** – Only NoSpamProxy administrator users and NoSpamProxy admin user accounts shall be allowed on the Windows Server hosting the TOE. No non-administrator users (including users administrating other applications) shall have access rights of any kind (also no read-only access) to the Windows server hosting the TOE.
- **Assumption.SecureCredentials** – The administrator of the TOE shall be able to generate secure administrator credentials. Otherwise, the created credentials may not be strong enough to withstand an attack. The corresponding secure configuration of the Windows Server operating system should be used to enforce strong and secure credentials.

- **Assumption.SecuredWindowsServer** – There is a state-of-the-art protection of the Windows Server hosting the TOE from physical access and physical access shall be limited to trusted personnel. The administrator shall use the most recent guidelines to ensure best practice secure configuration of the Windows Server operating system on which the TOE is installed - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.html . As a result of the hardening attacks such as DNS-spoofing are prevented by the Windows server hosting the TOE.
- **Assumption.SecureAdminClient** – The administrator shall use a secure computer to manage the TOE. Otherwise, an attacker could attack the administrators' client computer, e.g., using key loggers to get access to the administrators' credentials of to the TOE's configuration.
- **Assumption.AdminSecureAssets** – The administrator shall put copies of the TOE's configuration and other valuable assets of the TOE in a secure place when storing them outside of the TOE. Otherwise, an attacker could try to read or change a copy of the TOE's configuration.
- **Assumption.SecureExternalCertificates** – External communication partners shall only use certificates or PGP keys with sufficient key lengths and recommended algorithms for encrypted email communication. This assumption is valid for all relevant certificate authorities. Administrator shall not allow import of 3rd party certificates or keys with insufficient key lengths.

Assets

The TOE protects the following assets and security properties:

- **Asset.TOE.Config** – the configuration of the TOE controls all security measures that are applied to all emails entering or leaving an organizations network and its protection therefore is essential.
- **Asset.TOE.Monitoring** – monitoring data consists of metadata allowing to analyze the communication partners and topics of an organization.
- **Asset.TOE.EmailComm** – User data and email contents consisting of all kinds of business or trade secrets, personal data and other sensitive information of an organization for which confidentiality, integrity and authenticity must be secured.
- **Asset.TOE.EncryptionKeys** – Private and Public Keys (S/MIME and PGP) are centrally stored and maintained on the TOE for an organization. Keys must be protected against attackers to maintain integrity and confidentiality.
- **Asset.TOE.PII** – personally identifiable information of users that needs to be protected. This can be information like data of birth, phone numbers, gender or confession.

Threat Model: Attackers

The following attackers of the TOE are assumed in the threat model:

- **Attacker.Employee**: User who is employee or member of the organization but who has no Administrator role
- **Attacker.Internet**: Person attacking the TOE from an untrusted network (Internet) who wants to read, misuse, or change any of the assets.

Threat Model: Threats

The following threats are expected:

- **Threat.PrivateKey.Compromise** – an attacker is getting access to the TOE database and retrieves the private keys of users in the organization.
- **Threat.PublicKey.Compromise** – an attacker is sending a modified public key for a legitimate communication partner. The TOE is storing the key and using it to encrypt a message which can be decrypted and read by the attacker.
- **Threat.MITMAttack** – an attacker could start a man in the middle attack to connect to the TOE as legitimate sending or receiving email server.
- **Threat.RelayMisuse** – an attacker could try to misuse the TOE as mail relay sending out spam or malicious emails on behalf of the organization.
- **Threat.MailDoSSecBlock** – an attacker could try to overload an organization's email infrastructure by sending high volumes of "legitimate" non-malicious emails.
- **Threat**.**ConfigMetaData.Access** – an attacker is getting access to TOE configuration, rules or meta data

Security Functions

The TOE is providing the security functions listed in the table below. In combination with security functions provided by the Windows servers hosting the TOE   requirements defined in BSI AIS B6 are met.. In case a mandatory requirement is not implemented in a security function of the TOE but is a function of the underlying Windows Server system, we refer to the corresponding assumption Assumption.SecuredWindowsServer.

Security Function	**Comment**
Sec.AdminAuth	Secure Authentication of Administrators of the TOE
Sec.SMTPAuth	Secure SMPT authentication between e-mail servers (RFC 5321)
Sec.LDAP	User administration is done via Active Directory/LDAP (RFC 5411)
Sec.MultiTenant	Strict role/rights model for Administrators to define the scope of information which can be accessed by an administrator
Sec.EmailEncryption	Content of emails can be encrypted (S/MIME 4.0 – RFC 8551, PGP – RFC 4880). Cryptographic methods used by TOE comply with requirements (see chapter "Cryptographic Specifications")
Sec.TLS	TOE enforces transport layer encryption for communication with email servers (TLS - RFC 8446). Cryptographic methods used by TOE comply with requirements (see chapter "Cryptographic Specifications").
Sec.MessageTracking	The administrator can use the message tracking to identify attack attempts via email
Sec.NSPMonitoring	The administrator will get alerts via NoSpamProxy Control Center about new email attacks and necessary configuration changes or before resource limitations are hit
Sec.MailReject	TOE will not accept and reject emails identified as Spam, malicious or otherwise not allowed due to TOE configuration
Sec.KeyPass	The administrator is forced to provide a password which is afterwards used to store all private keys encrypted in the database.
Sec.ServerLogging	TOE is writing to the Windows Security Event Log of Windows Server to provide the required auditable logging. Time stamps, events and event results are logged

Threats vs. Assets

Asset(s)	**Attacker(s)**	**Threat(s)**	**Security Function(s) / Assumption(s)**
Asset.TOE.Config	Attacker.Internet Attacker.Employee	Threat.ConfigMetaData.Access	Sec.AdminAuth Sec.LDAP Assumption.OnlyAdminUsers Assumption.SecureWindowsServer
Asset.TOE.Monitoring	Attacker.Internet Attacker.Employee	Threat.ConfigMetaData.Access	Sec.AdminAuth Sec.MultiTenant Sec.LDAP Assumption.OnlyAdminUsers Assumption.SecureWindowsServer
Asset.TOE.EmailComm	Attacker.Internet Attacker.Employee	Threat.MITMAttack	Sec.TLS Sec.EmailEncryption
Asset.TOE.EmailComm	Attacker.Internet Attacker.Employee	Threat.RelayMisuse	Sec.TLS Sec.SMTPAuth Sec.MessageTracking Sec.NSPMonitoring
Asset.TOE.EmailComm	Attacker.Internet	Threat.MailDoSSecBlock	Sec.MailReject
Asset.TOE.EncryptionKeys	Attacker.Internet	Threat.PrivateKey.Compromise	Sec.AdminAuth Sec.KeyPass Assumption.OnlyAdminUsers Assumption SecureWindowsServer
Asset.TOE.PII	Attacker.Internet	Threat.PublicKey.Compromise	Sec.TLS Sec.EmailEncryption Sec.MailReject

Limits of Evaluation

The TOE is designed to operate in a variety of scenarios and with optional services. The scope of the evaluation is limited to the core functionality and operation on a single system. Therefore, the following is not within the scope of the evaluation:

- Sandbox Array service – a connected service which can receive file attachments from the TOE via a secure connection to perform further in-depth security checks on an object.
- Distributed installation of Intranet role and one or multiple Gateway Roles on different/multiple Windows servers to provide higher service availability and performance scalability.
- PDF functionality of Encryption module due to inherent limitations of PDF standard
- Function for generation of PGP Keys
- HTTPS via Port 6061
- Large Files module
- Plugin control of the TOE from email clients (Outlook)
- ICAP server
- Email threat evaluation network 32Guards
- SMS services
- Email archive connector
- De-Mail connector
- digiSeal server