Forcepoint Trusted Mail System

Enabling the secure, multi-level, policy-enforced exchange of email and attachments from a single inbox

Defense departments and ministries, intelligence communities, and civilian agencies are realizing cost savings and collaboration by moving data to shared networks in the cloud and controlling access to that data based on a user's identity, role, and "need to know." This move toward common IT architectures and infrastructure is required in order to meet the longer term goal of enabling authorized users to securely access their data, email, and applications from any device anywhere.

Key Benefits

- Increases productivity by providing "single inbox" capability across multiple email domains
- Utilizes proven, U.S. UCDSMO Baseline-listed, certified, and accredited Trusted Gateway System guard technology for content inspection and security policy enforcement
- Commercial-Off-The-Shelf (COTS) solution
- Supports inspection of email content, attachments, and headers, as well as nested messages
- Provides easy administration by integrating with existing email gateways across the enterprise

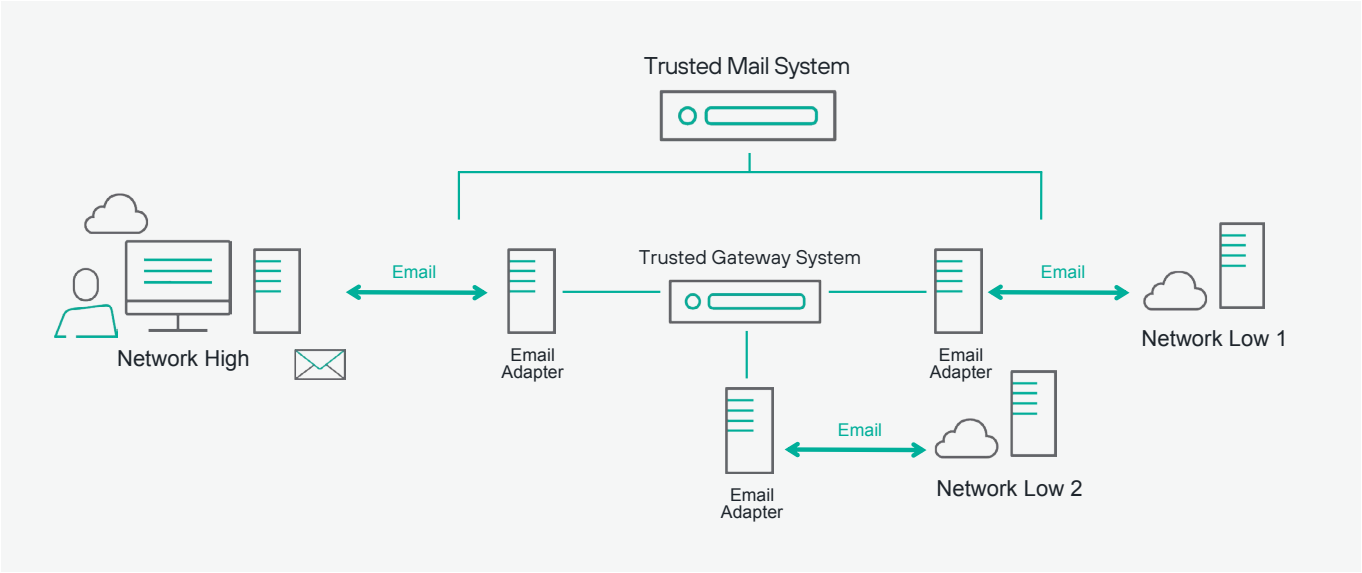
Forcepoint's secure information sharing solutions provide the ability to securely and effectively access multiple virtualized desktops within private clouds or expand their reach by connecting to remote community clouds, while also being able to securely transfer data between them. This secure connectivity fosters heightened information sharing within and between agencies and coalition partners.

Forcepoint Trusted Mail System addresses the specific need for the secure transfer of email and attachments between multiple security levels and different networks.

Forcepoint Trusted Mail System

Forcepoint Trusted Mail System is a Commercial-Off-The-Shelf (COTS) highly secure solution that enables the policy-enforced exchange of emails and attachments between users on different networks, eliminating the need to switch between email systems at multiple levels. Forcepoint Trusted Mail System provides a "single inbox" that consolidates email residing on various networks at the highest level, making it less likely that important and mission-sensitive email communications are overlooked. Users are able to read, forward, and respond to any email message that they receive regardless of the security level, but any emails generated will originate from the security level at which the single inbox resides (normally the highest security level). Email messages received from different security levels can be color coded within Microsoft Outlook using a set of simple client-based rules.

Forcepoint Trusted Mail System Architecture



Forcepoint Trusted Mail System leverages the widely deployed, accredited, and U.S. Unified Cross Domain Services Management Office (UCDSMO) Baseline-listed Forcepoint Trusted Gateway System as the secure transfer guard component. Forcepoint Trusted Gateway System ensures that malicious data is not transferred between networks and that sensitive data is not inadvertently or intentionally leaked. With Forcepoint Trusted Mail System, the guard inspects and sanitizes all email content, including messages, headers, and attachments.

In addition to the Forcepoint Trusted Gateway System transfer guard, Forcepoint Trusted Mail System includes specialized adapters, residing within each security domain. These adapters are responsible for receiving email destined for a different domain, and consolidating that into a package which is then submitted to the guard for review. The adapters perform pre-screening on all email content prior to submitting the package to the guard, to enforce controls on attachment size and type, and number of attachments, as well as blocking emails from configured lists of senders and recipients (blacklists). This pre-screening process is also used to obfuscate selected header fields (names, email addresses, and IP addresses) and remove potential vulnerabilities in email headers.

Forcepoint Trusted Gateway System performs deep content inspection filtering of email messages, attachments, and nested content (including multi-part MIME) which includes:

- → File type identification
- → Virus scanning
- → Dirty word search
- → Analysis of Microsoft Office documents via Purifile
- → PDF transformation and sanitization
- → Image transformation

Forcepoint Trusted Mail System ensures that status and error message information from the recipient's domain are correlated to the original email sent from the sender's domain. This is especially helpful for administrators when troubleshooting email errors. For additional security, Forcepoint Trusted Mail System provides complete end-to-end auditing of all events through the system for comprehensive security monitoring and post-event forensics.

Ease of Administration

Forcepoint Trusted Mail System provides seamless interoperability with existing IT and email infrastructures. Forcepoint Trusted Mail System supports common email clients such as, but not limited to, Outlook, Thunderbird, and Eudora.

Minimal user configuration is required for easy integration into the enterprise environment. Users continue to send and receive email without any disruption to their normal email activity, so no additional training is required.

Administrators can easily export audit and log data to be correlated and managed by external management systems. System error notifications are integrated with legacy network management tools to provide administrators a consolidated view.

Security

Communications between the inbound adapter and the guard is encrypted using transport layer security (TLS) and authenticated using either username/password or certificates. The communication between the guard and the output adapter is encrypted using Secure File Transfer Program (SFTP) with username/password authentication. Individual user access to the mail adapters can be restricted using a configurable list of email addresses on the inbound adapter. The configurable list can be used to enforce an inclusive set of users (e.g. those allowed to send), or an exclusive list of users (e.g. those restricted from sending).

Certification and Accreditation (C&A)

Forcepoint Trusted Mail System utilizes the certified and accredited Forcepoint Trusted Gateway System as the transfer guard between email adapters to provide a secure boundary between different classification levels. Forcepoint Trusted Gateway System is on the US UCDSMO Baseline list of approved cross-domain solutions and is widely deployed in operational systems around the world. Forcepoint Trusted Gateway System is engineered to satisfy cross-domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) certification and accreditation processes.

Conclusion

Forcepoint secure information sharing solutions are designed to enable secure access and transfer of sensitive information for government, intelligence community, civilian, and corporate entities in the U.S. and around the globe, including 5 Eyes nations and NATO member countries. Forcepoint's secure information sharing solutions continue to strike the right balance between information protection and information sharing—a vital component to enterprise security.

Internal Reference #IIS2014-095 [Trusted-Mail-System-Datasheet-US-EN] 16Jun2020