FORCEPOINT
POWERED BY Raytheon

Datasheet

Trusted Gateway System™

SECURE MULTI-DIRECTIONAL DATA TRANSFER

FEATURES AND BENEFITS

- **Included** in the US UCDSMO Baseline list
- **User-friendly** web interface guides users through each transfer
  - Enforcing Reliable (two-person) Human Review when configured
  - Minimizes the need for extensive training and support
- **Quick** Release and Quick Submit features for simplified self-release transfers
- **Ability** to create templates containing frequently used data allows users to create jobs with a single click
- **Support** for multi-channel, multi-directional transfers with one system
- **Support** for username/ password and public key infrastructure (PKI) authentication mechanisms
- **Expandable** functionality with Trusted Print Delivery™ and Trusted Mail System™ adapters

SECURE INFORMATION SHARING DATA TRANSFER

Many global events from terrorist attacks to cybersecurity breaches have identified that secure information sharing between international, federal, state, local, tribal, and private sector entities is a recognized and, in some cases, legislated need. In light of this, the term "need to know" has been replaced with "need to share" or "responsibility to provide." Secure information exchange, collaboration, and data sharing are goals we must attain to protect national and international security interests, but they have not been easy to achieve.

Frequently, information stored on a proprietary or sensitive network must be transferred to a shared or less sensitive, less controlled network for use by another agency or organization. This sensitive data may be a single document or an entire directory containing imagery, maps, multiple documents, and databases that must be moved quickly and securely to prevent viruses, network intrusions, and data leakage. Critical data must be transferred between and across networks to the right people at the right time, keeping it secure and protecting against its unintended or malicious distribution.

By deploying a secure transfer system to enforce role-based access, workflow tasks, and secure file management and controls, agencies and organizations can efficiently ensure the quick and secure sharing of information.

TRUSTED GATEWAY SYSTEM™

Trusted Gateway System™, a Commercial-Off-The-Shelf (COTS) transfer solution, provides exceptional builtin manual review and automatic validations, such as virus scanning, file type verification, dirty word search, and deep content inspection. Trusted Gateway System enables safe and simultaneous data movement between networks typically at different sensitivity levels. The solution can be operated in a single server configuration that provides the physical connections to multiple networks, maintaining network separation and enforcing customer-configured transfer policies. The server, or guard, runs on Red Hat® Enterprise Linux® 64-bit systems with Security Enhanced Linux (SELinux) components providing stringent security controls (Figure 1).

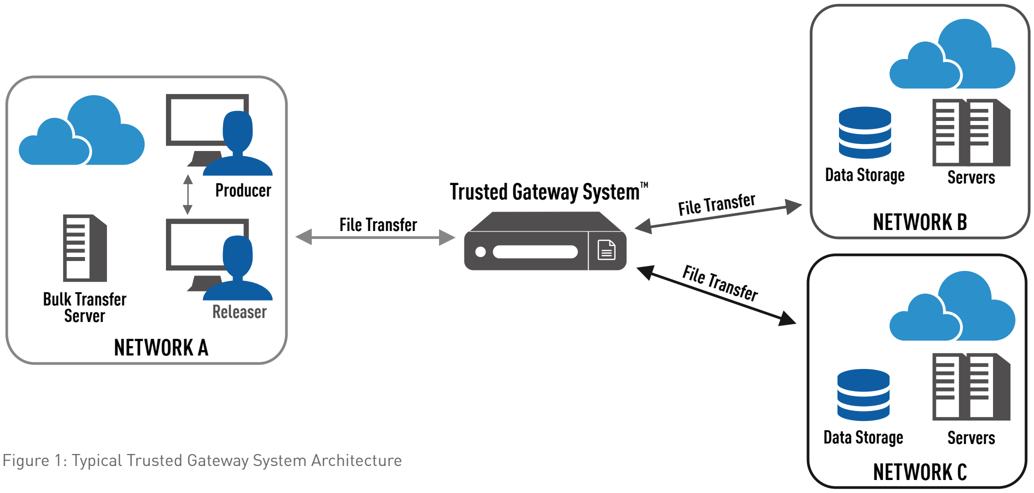


Figure 1: Typical Trusted Gateway System Architecture

SECURE TRANSFER WORKFLOWS

Trusted Gateway System can be configured for different usage scenarios based on customer requirements: Two-person Human Review, Self-Release, Quick Submit, Quick Release, Bulk Upload, and Directory Transfer Service Option. Each option is described in more detail below.

Individual site security policy determines which workflows can be used. Regardless of the workflows or combinations instituted, data movement can occur to and from an unlimited number of approved classified networks. File transfer occurs by data push or email distribution. Any-to-any classification level transfer and multiple file transfer requests are supported.

TWO PERSON HUMAN REVIEW

The two-person review and release process (Reliable Human Review (RHR)) is typically used when moving data to a less sensitive network (high-to-low classification transfers). When configured for this process Trusted Gateway System enforces the use of two standard roles, Producer and Releaser, for job creation and transfer. This workflow requires that the person responsible for assembling and submitting transfers is assigned the Producer role, and that the person responsible for review and approval (release) of the transfer is assigned the Releaser role. Releasers must also open each file in the job and accept any dirty word search results before the job can be approved for release to the designated network(s). A standard workflow is depicted in Figure 2.

SELF-RELEASE

Self-Release allows approved users to create a job and send it to approved destinations (after passing all validations) in one step without requiring the two-person human review process. Self-Release users must be granted to the Self-Release role. Additional permission granularity can be achieved by limiting Self-Release to specific destinations. For example, Jane may be authorized to approve her own file transfers when releasing to Network A; however, when moving files to Network B she must specify the appropriate Releaser.

QUICK SUBMIT

Quick Submit is part of the Trusted Gateway System web-based interface and can be used with or without the full workflow. When the user logs in, the application destination and releaser information is pre-defined through templates established by an administrator. The user drags and drops files into the application for Trusted Gateway System to perform all configured validations. Files that pass validation are transferred to a releaser (if configured) or to the destination (high side). If any of the configured validations fail, the user is alerted and the transfer is not permitted.

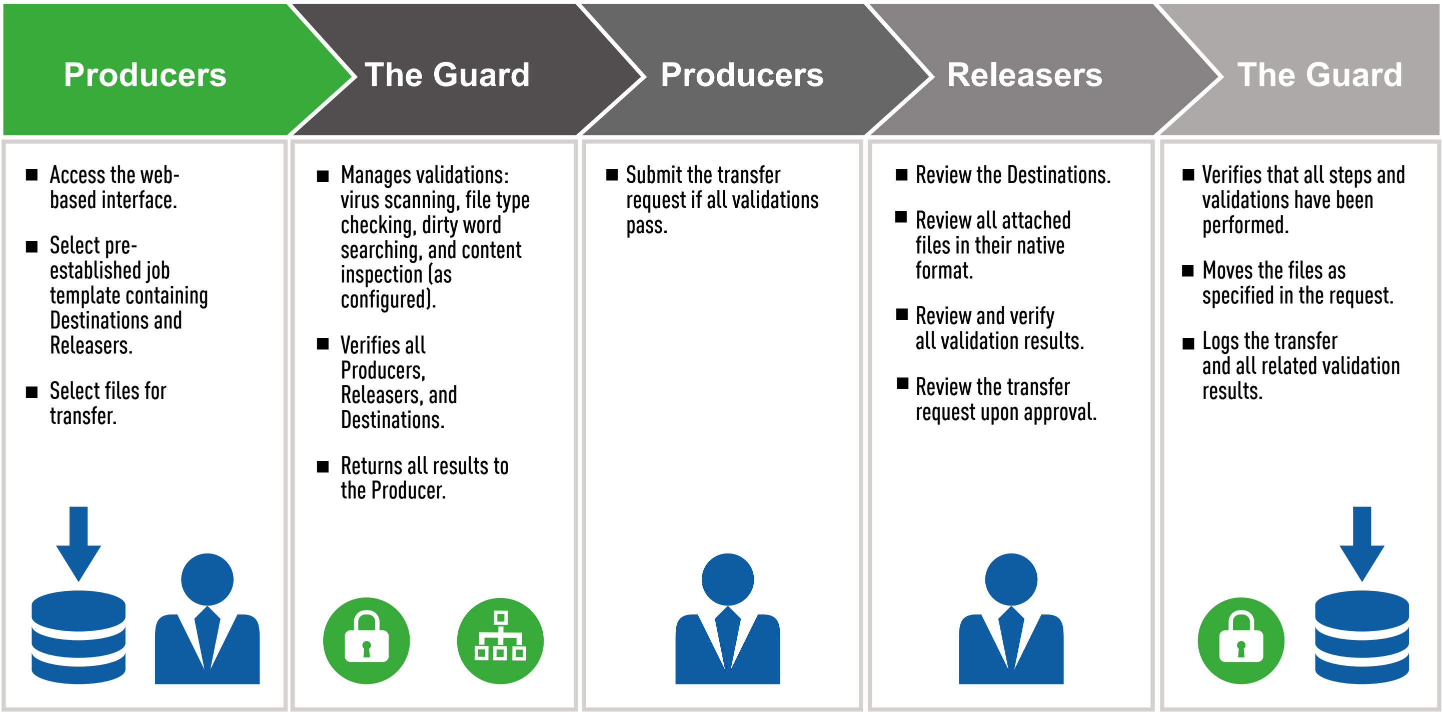
QUICK RELEASE

Quick Release is a secure instant messaging tool that rapidly transfers information through Trusted Gateway System to configured networks (destinations). Quick Release installs on a user's Microsoft® Windows® system (enabled when permitted by site security policy).

Quick Release can send text or files through Trusted Gateway System to selected networks. The user can copy/paste text or drag and drop files into the tool. When Trusted Gateway System receives the information, it conducts file validation, dirty word searching, and virus scanning. Text or files that pass validation are delivered directly through extensible messaging and presence protocol (XMPP) before the information is permitted to pass to the network destination. The Quick Release option is disabled by default.

BULK UPLOAD

Bulk upload is generally used when transferring large quantities of files from low to higher level networks. The



Producers

- Access the web-based interface.
- Select pre-established job template containing Destinations and Releasers.
- Select files for transfer.

The Guard

- Manages validations: virus scanning, file type checking, dirty word searching, and content inspection (as configured).
- Verifies all Producers, Releasers, and Destinations.
- Returns all results to the Producer.

Producers

- Submit the transfer request if all validations pass.

Releasers

- Review the Destinations.
- Review all attached files in their native format.
- Review and verify all validation results.
- Review the transfer request upon approval.

The Guard

- Verifies that all steps and validations have been performed.
- Moves the files as specified in the request.
- Logs the transfer and all related validation results.

Figure 2: Two Person Human Review Workflow

destinations can be customized to meet specific site policies and procedures.

The Bulk Upload transfer mechanism supports direct file transfers, using Secure Copy Protocol (SCP), from a configured network to the appropriate destination. For security reasons, only configured hosts can access the input directory through SCP. All other connection attempts are denied. An optional service can be included on a Microsoft® Windows® system (2000 or later) allowing users to maintain local input directories. This service monitors the local folder and automatically copies the file for processing. A right-click shortcut allows users to send files to defined destinations, which can be secure file transfer protocol (SFTP) servers, FTP servers, or email addresses at permitted classification levels.

DIRECTORY TRANSFER SERVICE (DTSO)

Directory Transfer Service Option (DTSO) runs on Microsoft® Windows® and Linux® networks and servers. DTSO provides a secure mechanism to transfer directories from a lower labeled network through the Trusted Gateway System to a higher labeled network. The DTSO provides a service that is able to watch one or more top level, or "root," directories and transfers files placed in those directories through the Trusted Gateway System to a high side server.

FILE TRANSFER SECURITY CONTROLS

Regardless of how the transfer request is initiated, Trusted Gateway System manages the process to ensure approved file movement between secure networks and across classification levels following site security policies. By default, all files are required to pass two controls prior to movement, virus scanning and file typing. Dirty word search, content inspection, and manual file review can be configured to meet specific requirements.

VIRUS SCANNING

The third-party virus scanning engine can be customized, and a site can elect to exclude certain trusted file types from virus scanning to enhance performance.

FILE TYPE VERIFICATION

The different varieties of file type checking are extension matching, XML validation, Forcepoint™ signature algorithm, and third party algorithm, all of which are configurable. File verification signatures can be customized to accommodate unique file types, configured by both source and destination policies and XML files can be validated against site-specific schemas.

DIRTY WORD SEARCH

Trusted Gateway System checks files for sensitive or "dirty" words that should not be released to other networks. This control also allows the designation of "clean" words, which are common words that contain dirty words. For example, the word "secretary" contains the embedded word "secret" but it is considered a false positive and can be ignored. System administrators can create and customize a master list of dirty and clean words, as well as lists that are used with specific source and destination network pairs. Once these lists and transfer pair rules are configured, each file uploaded to the guard is searched against the list for matches. If dirty words are found, the user is given the option to acknowledge and allow the word.

The user's acceptance of each dirty word is recorded and stored in an auditable database. All dirty words must be acknowledged before the transfer containing the flagged file can be submitted for release. All actions and overrides are stored.

CONTENT INSPECTION

When Trusted Gateway System is configured for content inspection, files such as Microsoft Office and portable document format (PDF) are scanned to identify and remove a wide range of hidden or embedded data and metadata. This option provides added prevention against inadvertent or malicious disclosure of sensitive or proprietary information when documents are released.

Administration and Management

Trusted Gateway System administration and management are performed by a system administrator, with the appropriate permissions from the server or remotely through the Remote Access Console (RAC).

USER ACCESS ADMINISTRATION CONTROLS

User access and authorization controls (username, password, Public Key Infrastructure (PKI) X.509 digital certificates, clearance level, and group management) are configured and managed within the server or tied into a pre- existing Microsoft Active Directory® server or Lightweight Directory Access Protocol (LDAP) directory server on the high-side network. Utilizing a pre-existing LDAP or Active Directory server eliminates the need to manage user accounts on the server, thus reducing the administrative overhead. System administrators can create and manage end users directly from the server or through an easy to use web-based application for basic account maintenance.

AUDITING

The Trusted Gateway System Auditor role grants permission for job review and status report creation from the web interface based on specified criteria. For example, Auditors can generate reports detailing when the dirty word search has been overridden for all files transferred in the last week. Auditors can export reports in CSV, Excel®, and XML formats. Additionally, the server generates application logs and the operating system collects detailed audit records to track use and activity. This log and audit data can also be pushed to a centralized enterprise storage location.

REMOTE ACCESS (RAC)

RAC is used to centrally manage and access Protection Level 4 (PL4)-capable servers over a secure connection. RAC provides scalable remote access that can be utilized from any authorized location on the network where the servers reside. RAC uses Keyboard, Video, Mouse (KVM)-over- IP capabilities that enable an authorized user "console" access as if he or she were seated at the attached device.

CERTIFICATION AND ACCREDITATION (C&A)

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) C&A processes. Trusted Gateway System is identified on the US Unified Cross Domain Services Management Office (UCDSMO) Baseline list as an approved transfer solution.

CONCLUSION

Forcepoint's secure information sharing solutions have a proven track record of proactively preventing government and commercial organizations from being compromised, while fostering the secure access and transfer of information. This allows Forcepoint's solutions to strike the right balance between information protection and information sharing — a vital component to national security. Trusted Gateway System is a secure transfer solution that solves the difficult problem of satisfying security needs while enhancing information sharing. It provides the ability to quickly and securely move data between and within classification levels and is designed to satisfy the information assurance accrediting community requirements, eliminate potential leaks and risks, and provide users with an easy to use workflow application. All Forcepoint secure information sharing solutions have been designed to meet or exceed extensive and rigorous security C&A testing for simultaneous connections to various networks at different security levels. Forcepoint offers an experienced professional services team to guide customers through the technical implementation and C&A processes.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2014-104 [DATASHEET_TRUSTED_GATEWAY_SYSTEM_EN] 100017FED.032516