FORCEPOINT

Datasheet

FORCEPOINT Trusted Gateway System

Secure Multi-Directional File Transfer for Segmented Networks

Forcepoint Trusted Gateway System enables safe and simultaneous multi-directional file movement between physically separated networks of varying security and classification levels.

Trusted Gateway System specializes in the transfer of unstructured files, such as Microsoft Office and PDF files, facilitating *critical information-sharing to the right people at the right time*.

The Need for Secure and Reliable File Transfer

Many global events, from terrorist attacks to cybersecurity breaches, have determined that secure file sharing between international, federal, state, and local entities is required and, in some cases, a legislated need. But doing so between varying classification levels can be inefficient, ineffective, and more importantly, insecure, with unacceptable levels of risk.

Depending on mission requirements, files 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.

Why Forcepoint Trusted Gateway System?

Forcepoint's secure information-sharing solutions have a proven track record of proactively preventing government agencies from being compromised, while fostering the secure and efficient access to and transfer of information. Trusted Gateway System solves the difficult problem of satisfying security needs while facilitating unstructured file sharing. It is designed to meet most, if not all, cross domain security best practices.

Key Benefits

- **Eliminate** sensitive file sharing inefficiencies ("sneakernet") during mission-critical activities.
- **Quickly and securely** move unstructured files between and within classification levels.
- **Inspect and sanitize** files with a R.A.I.N (Redundant filters that are Always Invoked) compliant solution.
- **Configure** file transfer workflows based on site-specific requirements and policies.
- **Comply** with the U.S. Government's Raise-the-Bar initiatives.
- **Add** functionality with Forcepoint Trusted Print Delivery and Trusted Mail System.

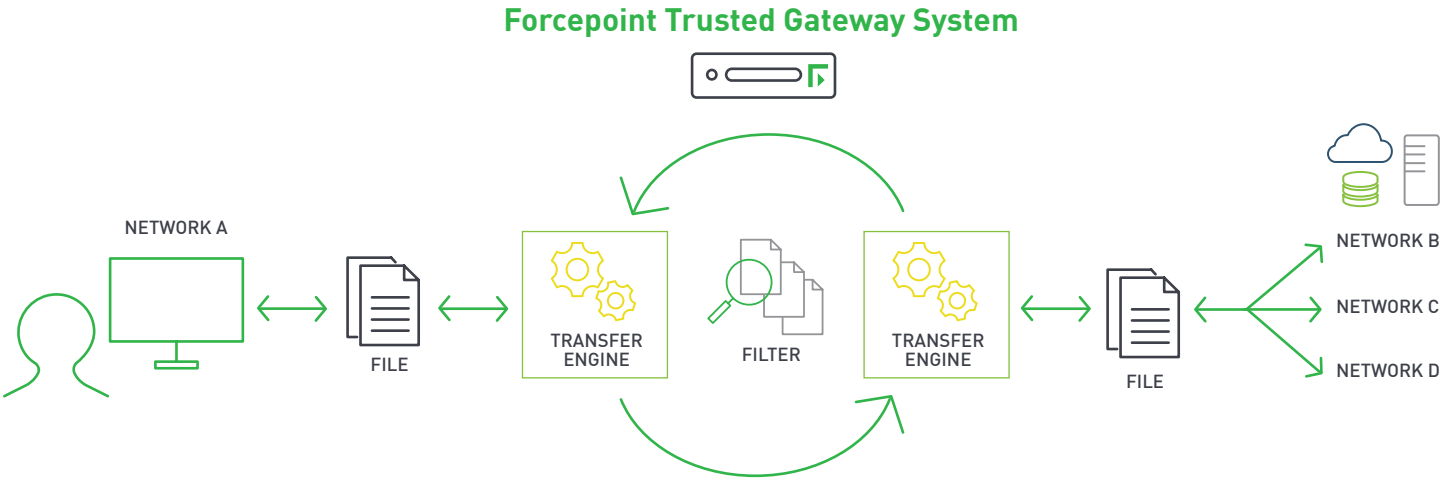

Figure 1. Forcepoint Trusted Gateway System

Configure Secure File Transfers Based on Polices and Requirements

Trusted Gateway System can be configured for different scenarios based on customer requirements and individual site security policy. Regardless of the workflows or combinations instituted, file movement can occur to and from an unlimited number of approved networks. Any-to-any classification level transfer and multiple file transfer requests are supported:

- **Two-Person Human Review/Reliable Human Review (RHR)**
  - » The Producer role is responsible for assembling and submitting transfers (or jobs).
  - » The Releaser role is responsible for review and approval (release) of the transfer.
- **Template-based Submit**
  - » A web-based interface presents users with a predefined template of the file destination and releaser information.
  - » User drags and drops files into the application to perform all configured validations.
- **Self-Release**
  - » Approved users can create a job and send it to approved destinations in one step without requiring the two-person human review process.
  - » Users must be granted the Self-Release role. Additional permission granularity is available.
- **Bulk Upload**
  - » Users have the ability to transfer large quantities of files from low- to higher-level networks, machine-to-machine.
  - » Direct file transfers are supported using Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP) from a configured network to the appropriate destination. Only configured hosts can access the input directory through SCP. All other connection attempts are denied.
  - » Users can copy/paste text or drag and drop files into the tool.
  - » 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 or email addresses at permitted classification levels.
- **Directory Transfer Service Option (DTSO)**
  - » A secure mechanism is provided to transfer directories from a low to a high network.
  - » DTSO runs on Linux and Microsoft Windows servers.
  - » This service is able to watch one or more top level, or "root," directories and transfers files placed in those directories to a high side server.

Key Features

- Operates on a Red Hat® Enterprise Linux® 64-bit operating system with Security Enhanced Linux (SELinux) components providing stringent security controls
- Resilient architectural design that meets the requirements of the "Raise the Bar" cross domain security community
- Vast amount of file types and multiple file sanitization solutions supported
- Visualization tool to set/view policy rules, configurations, and administrative status
- User-friendly web interface access to guide users through the transfer process
- Robust archive and audit management capabilities with centralized event logging
- Flexible network configurations to accommodate different environmental requirements
- Support for username/password and public key infrastructure (PKI) authentication mechanisms
- Automated bulk uploads via SCP/SFTP (low to high)
- Support for multi-channel, multi-directional file transfers with one system

Robust File Transfer Security Controls Provide Assurance

Regardless of how the transfer request is initiated, Trusted Gateway System manages the process to ensure approved file movement between secure networks and across sensitivity levels following site security policies. Trusted Gateway System provides numerous verification, inspection, sanitization, and transformation filters to safeguard file transfers. For most organizations, virus scanning will be required. Additional filtering and manual file review can be configured to meet specific requirements. Security controls include:

FILTER	FILE TYPES SUPPORTED	FILTERING CAPABILITIES
***Glasswall™**	Microsoft Office, PDF	Sanitizes Office and PDF documents. For each document type, the filter creates a new document utilizing the known good content from the input document. The filter is able to extract and import images from documents allowing embedded images to themselves be filtered (e.g. transformed). The filter also provides the export of a textual version of the document facilitating a dirty word search.
***PuriFile®**	Microsoft Office, PDF	Provides document inspection and sanitization and eases the document workflow process for Office and PDF documents.
***Aware**	bmp, png, jpg, j2k, tiff	Supports the conversion of images from one format to another and supports the stripping (reset to zero) of the least significant bit of pixel-based images. Allows support of jpeg2000 (j2k).
ImageMagick®	bmp, png, jpg, gif, tiff	Supports the conversion of images from one format to another and the stripping (reset to zero) of the least significant bit of pixel-based images.
***McAfee®**	All	Scans all file formats for the presence of virus signatures matching those in a stored virus definition list provided by McAfee.
***Sophos®**	All	Scans all file formats for the presence of virus signatures matching those in a stored virus definition list provided by Sophos.

FILTER	FILE TYPES SUPPORTED	FILTERING CAPABILITIES
XML2	XML	XML schema validation using a set of stored schema definition (XSD) files on the guard.
Xerces	XML	XML schema validation using a set of stored schema definition (XSD) files on the guard.
Archive	zip, tar, iso, gzip, cpio, bzip2	Supports the extraction of artifacts within archives.
PDF Transform	PDF	Cleanses PDF files through a format conversion process.
Dirty Word Search	All	Text search filter used for locating dirty words within any type of file. The filter supports simple text searching as well as regular expressions.
XSLT	XML	XML Stylesheet Language Transformation of XML files. Can perform validation and/or transformation of XML content based on an XML formatted stylesheet (prepared off-box). This filter enables support of Schematron-generated XSL stylesheets.
File Extension	All	Allows or blocks files based on the extension found in the file name.
File Size	All	Allows or blocks files based on file size.

*Additional cost

Administration, Monitoring, and Auditing

Trusted Gateway System administration and management is robust, easy to use, and is performed from the server by system and security administrators with the appropriate permissions.

Assessment and Authorization

Forcepoint Trusted Gateway System is engineered to comply with cross domain security requirements for processes and policies utilized by the U.S. Government in the fielding of cross domain solutions, including:

- In Process: Secret and Below Interoperability (SABI)
- Top Secret/SCI and Below Interoperability (TSABI)
- IC Directive (ICD) 503
- National Institute of Standards and Technology (NIST) 800 series Risk Management Framework (RMF)
- RMF for DoD Information Technology (IT)
- Director of Central Intelligence Directive (DCID) 6/3
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- Risk Decision Authority Criteria (RDAC)

Tested, Approved, and Validated to Secure Your Mission

For over 20 years, Forcepoint has been the global leader of cross domain and information-sharing security solutions, as evidenced by supporting the largest number of cross domain users in the world—currently over 300,000 users—and having the most approved solutions on the UCDSMO Baseline list.

CONTACT
www.forcepoint.com/contact

INTERNAL REFERENCE# FPFB-2017-0003
[DATASHEET_FORCEPOINT_TRUSTED_GATEWAY_SYSTEM_EN] 100017FED.060118