FORCEPOINT
POWERED BY Raytheon

Datasheet

High Speed Guard™

AUTOMATED, HIGH-PERFORMANCE DATA TRANSFER

FEATURES AND BENEFITS

- **Sustains** the industry's fastest transfer rates of more than 9Gb/s on 10Gb networks
- **Included** in the US UCDSMO Baseline for SABI and TSABI environments
- **Customer configurable** for simplified management and maintenance
- **Enables** real-time video streaming while providing unparalleled control and auditing
- **Supports** multiple application protocols and adaptability for custom interfaces
- **Provides** highly customizable data validation rules for maximum flexibility
- **Supports** complex web services

RAPID DATA TRANSFER TO FACILITATE SECURE INFORMATION SHARING

As governments, agencies, and the private sector focus on the need to collaborate and share critical information, protecting and improving how that information is distributed between various domains becomes paramount. Our customers' most sensitive intelligence must often be sanitized and made accessible to various services, agencies, forces, and coalitions as quickly as possible. At the same time, data from a wide variety of sources must be transferred to protected enclaves for processing and analysis. The sharing and movement of this data are essential to the rapid, accurate, and precise execution of our customers' missions. Unfortunately, the persistent threat of cyber-attack, penetration, and data loss requires that only the most secure methods are utilized to allow information sharing and transfer. Forcepoint™ consistently enables customer mission success while maintaining the highest standards of security.

HIGH SPEED

Forcepoint™ High Speed Guard™ is an integral part of many authorized systems enabling highly complex, bi-directional, automated data transfers between multiple domains (see Figure 1 next page).

High Speed Guard supports large enterprise systems with comparatively low administration costs, making it the ideal choice for large scale deployments that require rapid, automated data transfer. High Speed Guard has demonstrated the fastest bi-directional transfer rates of any guard technology. A typical High Speed Guard deployment is able to sustain transfer rates of more than 9 gigabits per second (Gb/s) on a commodity server, running the Red Hat® Enterprise Linux® operating system with a custom Security Enhanced Linux (SELinux) policy.

High Speed Guard is included on the United States Unified Cross Domain Services Management Office (UCDSMO) Baseline list as an accredited and operational transfer solution. Because it is an operationally accredited system, the Assessment and Authorization (A&A) process is streamlined for individual installations.

High Speed Guard supports a wide variety of data transfer scenarios through the use of flexible transfer mechanisms and extensive data support. These include web services, real-time Moving Pictures Experts Group (MPEG2) video, transfer imagery of multiple formats, imagery metadata files, inter-system messaging,

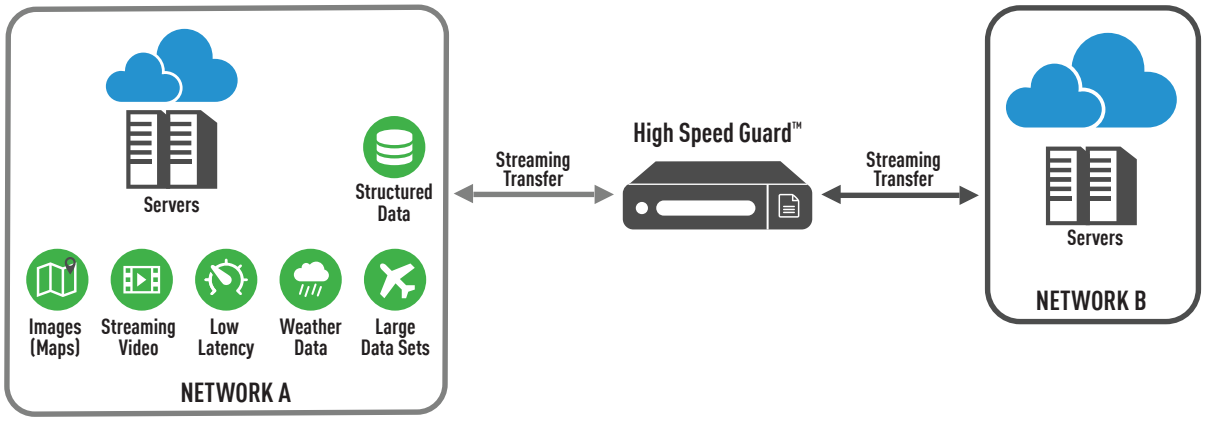

Figure 1: High Speed Guard™ Architecture

Ground Moving Target Indicator (GMTI) data, and a wide variety of proprietary data formats.

A Flexible Approach

High Speed Guard is highly flexible in its secure approach to multi-directional data movement through the inclusion of numerous transfer mechanisms and a wide array of inspection capabilities that, together, form robust security policies.

SECURITY POLICY ENFORCEMENT

High Speed Guard's Rule Engine provides a consistent policy enforcement capability across all transfer mechanisms. Instead of pre-packaged point-and-click policies, the Rule Engine supports full customization of inspection capabilities enabling the creation of complex security policies. This allows specific inspections and constraints for each deployment rather than generic controls based on file type. Almost any security policy can be expressed through the Rule Engine's user-configurable interface language. This allows new data formats to be added without product modification.

Transfer Mechanisms

The High Speed Guard transfer mechanisms provide a variety of fixed security protections and secure transfer methods. Forcepoint works with each customer to determine which mechanism(s) best supports their requirements. Many customers utilize multiple transfer mechanisms on a single system to reduce the size and cost of the solution (Figure 2).

Any combination of transfer mechanisms can be used to provide multiple flows through a single system. Each flow is independently managed without affecting other operational flows. Providing separate security policies and configurations permits the broadest applicability possible.

STREAMING VIDEO

High Speed Guard provides unparalleled control and auditing of MPEG Transport Stream streaming video, supporting multiple formats like MPEG-2, MPEG-4, and H.264 encodings along with STANAG 4609 (North Atlantic Treaty Organization (NATO) Standardization Agreement) compliant data. The built-in MPEG capability ensures that all data received is properly formatted and can process multiplexed streams individually. High Speed Guard extracts, audits, and validates the key length value (KLV) metadata within the MPEG stream, for example, classification and release caveats. Designed for flexibility, the Streaming Video transfer mechanism supports both unicast and multicast transfers and can send each input to multiple destinations across multiple networks.

SERVICE-ORIENTED ARCHITECTURE (SOA) WEB SERVICES

Utilizing Hypertext Transfer Protocol (HTTP), with or without Secure Socket Layer (SSL), High Speed Guard has built-in support for web services. Ideally suited for SOAP over HTTP services, High Speed Guard supports complete inspection of all HTTP headers and a full suite of parsing capabilities for the HTTP payload. This mechanism also provides extensive support for data sanitization and re-write, enabling the guard to deliver data that is different than what was transferred. The SOA Web Services transfer mechanism automatically parses and validates Multipurpose Internet Mail Extensions (MIME) segments and natively supports SOAP with Attachment (SWA) services for optimized data transmission.

ADAPTABLE LIGHTWEIGHT MESSAGING

The Adaptable Lightweight Messaging transfer mechanism gives High Speed Guard the flexibility to support almost any standard or custom messaging protocol, while still providing extensive security controls on all transmissions. High Speed Guard supports almost any UDP or TCP based protocol with or without SSL. Many customers utilize this capability for the cross domain transfer of custom protocols. High Speed Guard, using adaptable lightweight messaging, has demonstrated the transfer of GMTI/STANAG 4607 and Cursor On Target (COT) broadcasts, as well as high performance Java Messaging Services (JMS). Current JMS demonstrations show the capability to transfer over 4,000 messages per second through a single guard with additional untapped performance. Messaging

latency can be as low as single-digit milliseconds or lower, providing exceptional support to low tolerance systems.

HIGH PERFORMANCE TRANSFER

High Speed Guard supports the Joint Architecture Study Data Transfer Protocol (JAS/DTP), which is specifically designed and implemented for the highest possible data transfer performance. JAS/DTP is jointly defined by the National Geospatial-Intelligence Agency (NGA) and their mission partners to provide standardized high performance data dissemination across a wide variety of networks and systems. High Speed Guard supports repeatable transfer rates of over 9Gb/s when using this protocol. This protocol provides exceptional support where a standard file transfer protocol (FTP)-style data delivery would be appropriate but requires higher performance.

CROSS DOMAIN SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Cross Domain SNMP provides the means to extend network management across domains of different sensitivity levels. With this capability, enterprise network status can be received by a controlling domain.

ULTRA HIGH DATA RATE USER DATAGRAM PROTOCOL (UDP)

The Ultra High Data Rate UDP mechanism provides enterprises with a unique messaging capability that has achieved transfer rates of 96,000 messages per second with 1200 byte messages, without any packet loss.

AUTOMATED SECURE TRANSFER (AST)

The AST mechanism provides a standard file "drop box" transfer capability that allows High Speed Guard to monitor external file servers for files to transfer. Using AST, High Speed Guard can monitor and re-create subdirectories, monitor multiple source directories, and transfer to multiple destinations across multiple domains. A unique feature of AST is the ability to send files that fail validation to a specific destination. For example, failed files could be automatically redirected to Forcepoint's Human Review Manager tool within High Speed Guard or to another guard such as Forcepoint's Trusted Gateway System™. High Speed Guard may also redirect failed files to a problem or trouble queue on the source system for further review. AST supports both Secure Copy (SCP) and FTP transfers.

Administration and Management

High Speed Guard architecture divides administrative tasks from critical data transfer tasks on separate hardware platforms. This separation permits the guard to be highly minimized and locked down, while administrators have complete access to the Administration Server for performing functions such as backup, restoration, configuration, logging, auditing, real-time alerting, and administrator account management. A single Administration Server supports ten or more guards depending on the deployment. Consolidated logging and real-time alerting for the enterprise can be managed from a central area. The Administration Server itself can be accessed directly or remotely, depending on customer configuration requirements.

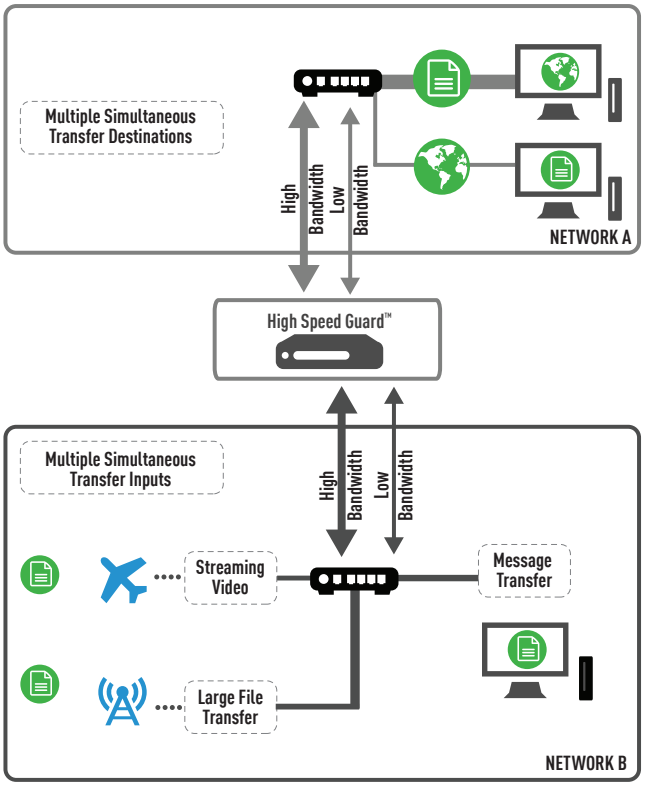

FIG 2: High Speed Guard™ Simultaneous Transfer Support

LOGGING AND AUDITING

High Speed Guard is deployed with an audit configuration that meets standard requirements across the cross domain community. Each deployment is enhanced with auditing specific to the data flows and security policies for that deployment. This unique auditing is driven by the Rule Engine, permitting the security policy to send any data deemed appropriate to the audit trail at any time. High Speed Guard supports local and remote log consolidation of the standard operating system syslog, binary auditing, and data transfer logging. All log and audit data is actively collected, parsed and reduced for immediate administrator notification of security events.

SYSTEM INTEGRITY

High Speed Guard uses various mechanisms for file system integrity checking and local configuration monitoring. Integrity validation can occur at any interval as specified by customer policy, typically twice a day. Integrity failures result in a full server halt or service termination (i.e., transfer mechanisms are stopped), depending on customer policy.

CONFIGURATION MANAGEMENT

The High Speed Guard Administration Server contains built-in configuration management functionality. The configuration management

system preserves a controlled baseline of all High Speed Guard configurations. System modifications are tracked through the configuration manager which runs in a dedicated area on the server. Use of configuration management enforces the maintenance of prior configuration versions and ensures strict adherence to two-person integrity controls.

Assessment & Authorization (A&A)

High Speed Guard is engineered to satisfy cross domain security requirements for Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) A&A processes. High Speed Guard is deployed worldwide and is part of systems authorized under Department of Defense (DoD) Risk Management Framework (RMF) IT, ICD 503, and National Institute of Standards & Technology 800-53 and 8500.2 security controls.

Conclusion

Forcepoint's cross domain 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 cross domain solutions to strike the right balance between information protection and information sharing—a vital component to national security.

High Speed Guard is a secure transfer solution that solves the difficult problem of satisfying security needs while enhancing information sharing. High Speed Guard provides the automated, high-performance transfer of information securely between and within classification levels. High Speed Guard is designed to satisfy the information assurance accrediting community requirements and to mitigate potential leaks and risks. All Forcepoint's cross domain solutions have been designed to meet or exceed extensive and rigorous security A&A testing by multiple agencies, organizations and services 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 A&A processes.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #FPFB-2017-0001 [DATASHEET_HIGH_SPEED_GUARD_EN] 100023FED.011517