High Speed Guard

Automated, high-performance data transfer for any enviroment

Key Benefits

- **Sustains** the industry's fastest transfer rates of more than 9Gb/s on 10Gb networks with latencies as low as 1.3ms
- **Included** in the U.S. NCDSMO Baseline for SABI and TSABI environments since 2001 and is designed to meet current Raise-The-Bar guidelines
- **Customer-maintainable** for simplified configuration and management
- **High Speed Guard SP** implementations support tactical and mobile forces and meet SWAP-C requirements
- **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

Rapid data transfer supporting all mission types

Protecting and streamlining how data is distributed between separated networks, in any environment, is essential to efficient and secure data sharing and collaboration. 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 from austere environments for processing and analysis. The sharing and movement of this data are essential to the rapid, accurate, and precise execution of our customers' missions. The persistent threat of cyber attack, penetration, and data loss requires that only the most secure methods are used to maintain the highest standards of security.

Forcepoint High Speed Guard & High Speed Guard SP

Forcepoint High Speed Guard is an integral part of many authorized systems enabling highly complex, bi-directional, automated data transfers between multiple domains (Figure 1). Forcepoint High Speed Guard and High Speed Guard SP for special-purpose implementations support both large enterprise environments and austere environments requiring specific size, weight, power, and cost (SWAP-C) considerations with comparatively low administration overhead. Forcepoint High Speed Guard has demonstrated the fastest bi-directional transfer rates of any guard technology. A typical Forcepoint High Speed Guard deployment is able to sustain transfer rates of more than 9 gigabits per second (Gb/s) on a commodity server. The operating system is derived from the Red Hat Enterprise Linux secure operating system with Security Enhanced Linux (SELinux) modules. Forcepoint High Speed Guard is included on the United States National Cross Domain Strategy Management Office (NCDSMO) Baseline list as an accredited transfer solution. Because it is an operationally accredited system, the Assessment and Authorization (A&A) process is streamlined for individual installations.

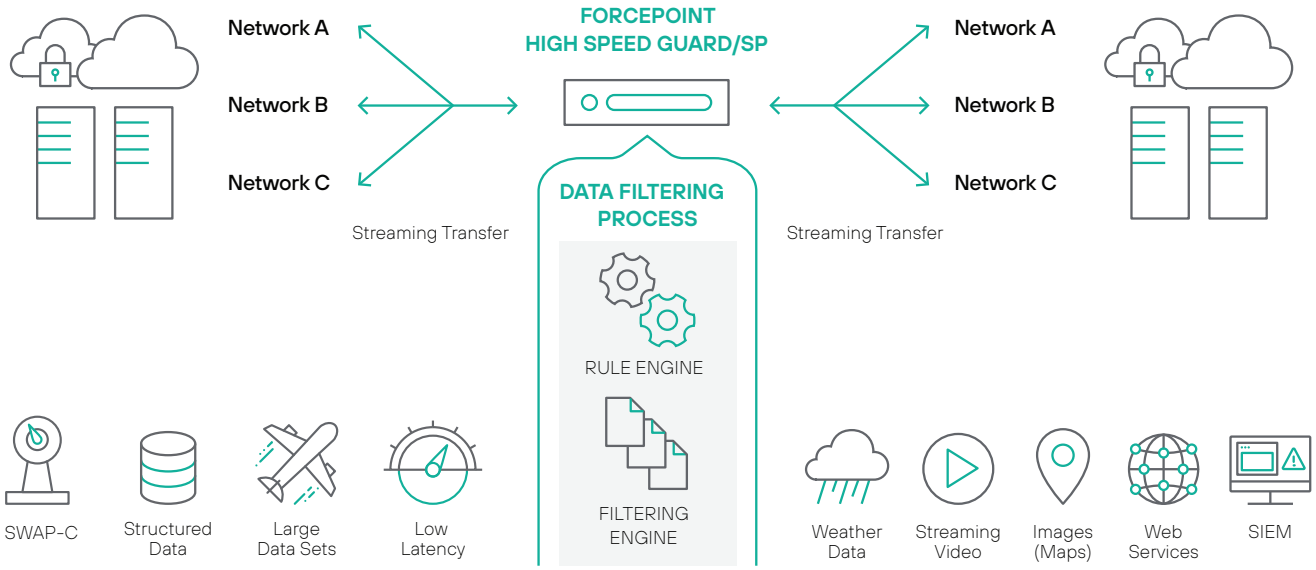

Figure 1: Forcepoint High Speed Guard Architecture

Forcepoint 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, 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

The Forcepoint High Speed Guard provides built-in redundant filtering capabilities delivered by two filtering engines: Rule Engine and the Filtering Engine. Each engine provides consistent policy enforcement across all transfer mechanisms. Instead of pre-packaged point-and-click policies, the engines support 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 engines' user-configurable interface languages. 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 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 for Ultra-High Data Rates (UDP & TCP)

High Speed Guard supports almost any UPD- or TCP-based protocol with or without SSL. Many customers utilize this capability for the cross-domain transfer of custom protocols. Customers utilizing this protocol have demonstrated the transfer of broadcasts, as well as high-performance Java Messaging Services (JMS). Messaging latency can be as low as single- digit milliseconds or lower, providing exceptional support to low tolerance systems.

High-Performance File Streaming

The Joint Architecture Study Data Transfer Protocol (JAS/DTP), which is specifically designed and implemented for the highest possible data transfer performance, 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.

Streaming Video	› Provides enhanced security controls for video › Live MPEG video transport streams
Service-Oriented Architecture (SOA) Web Services	› Standards-based interoperability through SOAP/HTTP › Cross-domain Web Services
Adaptable Lightweight Messaging for Ultra-High Data Rates (UDP & TCP)	› Custom messaging integration; easy integration into existing TCP/IP, UDP/IP systems › Supports latencies as low as 1.3ms › High-throughput UDP messaging (Xtreme rate UDP)
High-Performance File Streaming (JAS/DTP)	› Ideal for time-sensitive, large payload transfers › USG standard for product transmission
Cross-Domain SNMP	› Extending network management across domains › Supports enterprise network management from a controlling domain
Automated Secure Transfer (AST)	› Simple file drop-box interface › Secure Copy/SSH-based transfer mechanism › 1.8 TB/hr to 3 TB/hr

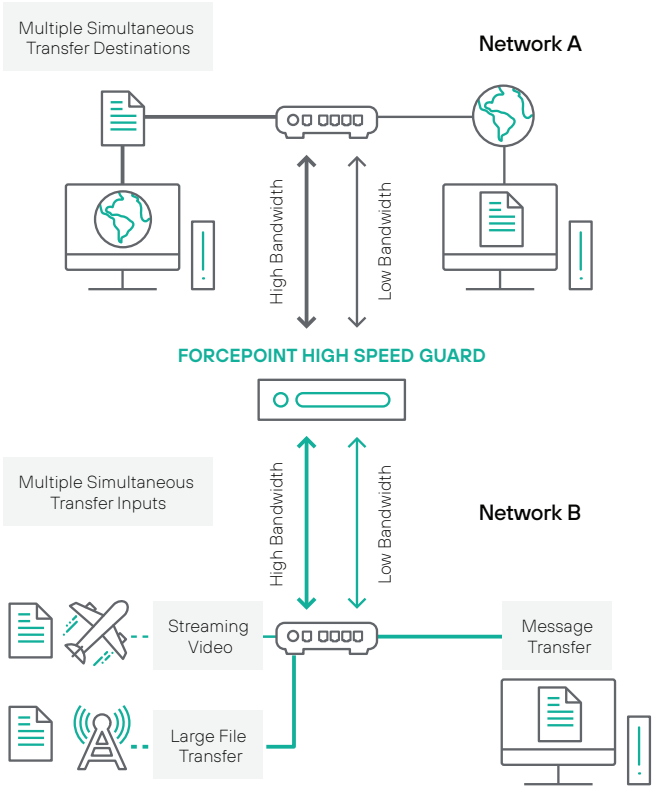

Figure 2: High-Performance file streaming

Cross-domain Simple Network Management Protocol (SNMP)

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

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 another guard such as Forcepoint 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 10 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.

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 and Filter Engines, 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 and can be sent, in real time, to a collection server.

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

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 to include meeting current NSA Raise-The-Bar guidelines. Forcepoint 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 solutions have a proven track record of proactively preventing 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.