FORCEPOINT
POWERED BY Raytheon

Datasheet

FORCEPOINT High Speed Guard

INDUSTRIAL CONTROL SYSTEMS

Secure, Automated, High-Performance Data Transfer.

Protecting Industrial Control Systems

Supervisory Control and Data Acquisition (SCADA) systems are more vulnerable to attack than ever before. With the introduction of modern network protocols into SCADA architectures, cyberattack vectors have increased dramatically. Isolating the SCADA network is impractical – information still must be shared with other organizations and control centers. Mechanisms used to share information must support a broad range of protocols, such as the Inter-Control Center Communications Protocol (ICCP), Distributed Network Protocol (DNP3) and International Electrotechnical Commission's (IEC) 61850, to ensure maximum flexibility for future growth and transition.

Forcepoint High Speed Guard provides just the solution. High Speed Guard is a militarygrade solution in widespread use throughout the United States Department of Defense (DoD) and Intelligence Community (IC). This state-ofthe-art solution automatically and securely moves data between physically separated networks. High Speed Guard allows the SCADA controlled local area network (LAN) to be completely isolated from routable protocol communication (as defined in North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP-002-4), thus providing unmatched protection to the SCADA system.

High Speed Guard

High Speed Guard is a DoD and (IC) accredited software solution that enables highly complex, uni-directional or bi-directional, automated data transfers between multiple physically segregated networks. High Speed Guard supports diverse systems' communication with comparatively low administration costs, making it the ideal choice for production-critical systems that require rapid, automated data transfer. High Speed Guard has demonstrated the fastest throughput and lowest latency transfer rates of any guard or diode technology. A typical High Speed Guard deployment is able to sustain transfer rates of more than 9 gigabits per second (Gb/s) and latencies below 10 milliseconds (ms) on commodity hardware, running a hardened Red Hat® Enterprise Linux® operating system with a strict Security-Enhanced Linux (SELinux) policy.

Key Benefits

- **Serves as the primary barrier in the electronic security perimeter (ESP) of a distributed control system (DCS)**
- **Readily compatible with SCADA protocols**
- **Low Latency for control systems**
- **Broad flexibility for multiple uses in one installation**
- **Customer configurable for simplified management and maintenance**
- **Highly customizable for precise control of data flow**

SCADA Protocol Support

High Speed Guard can be readily integrated to secure and validate common SCADA related protocols such as DNP3, IEC 61850, ICCP, and Multimedia Messaging Service (MMS). Additionally, its data transfer capabilities meet or exceed the low latency requirements of DNP3 and IEC 61850.

High Speed Guard in Action

Deploying High Speed Guard in a SCADA environment provides unprecedented protection for this critical cyber asset. No longer will communication traverse the SCADA controlled network segment to the Field Device LAN or the corporate network without intense scrutiny. Using High Speed Guard's trusted operating system protections and network separation combined with rigorous protocol enforcement and content inspection, every message (ICCP, IEC 61850, DNP3, etc.) can be inspected. Furthermore, one High Speed Guard can have several data flows with different protocols. The adjacent diagram shows the High Speed Guard deployed in a generic SCADA environment.

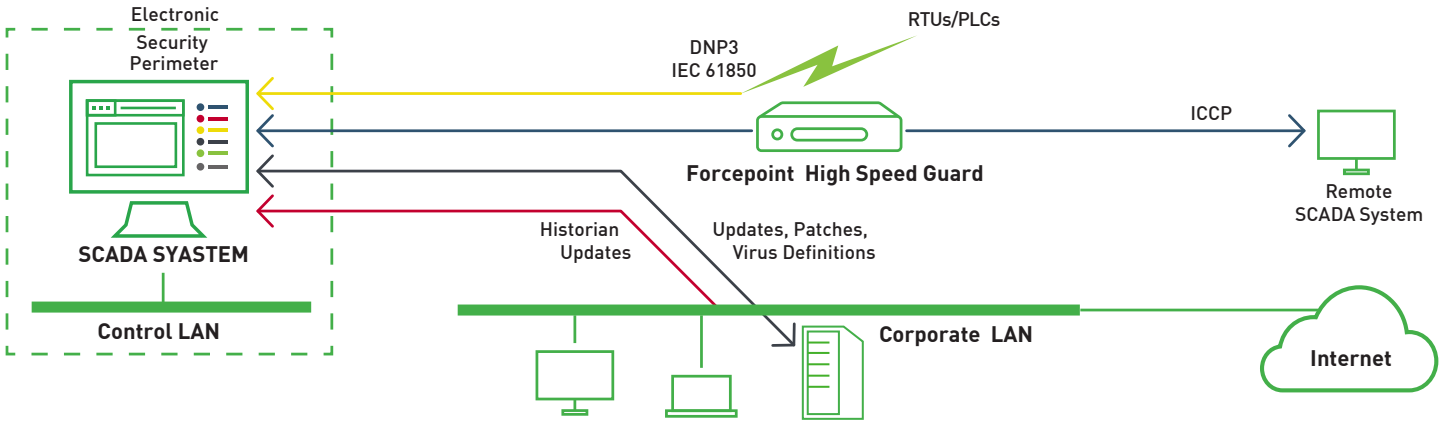
High Speed Guard Rule Engine

Unlike a firewall, High Speed Guard validates the correctness of a protocol as well as the content at the application layer. It does not forward or route packets; it inspects application level data. The Rule Engine supports full customization of inspection capabilities enabling the creation of complex security policies. This allows specific inspections and constraints for each protocol. Almost any security policy can be expressed through the Rule Engine's programming language.

Conclusion

With hundreds of government customers and more than a decade and a half of success, Forcepoint is the global leader in secure data transfer solutions. The company's products have a proven track record of proactively preventing organizations from being compromised, while fostering the secure transfer of information across network boundaries. This allows Forcepoint solutions to strike the right balance between Critical Cyber Asset protection and information transfer.

High Speed Guard has a distinguished history of satisfying the information assurance community requirements and mitigating security risks. All Forcepoint solutions have been designed to meet or exceed extensive and rigorous security certification and accreditation testing by multiple US government 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 which strengthens the Electronic Security Perimeter of Critical Cyber Assets as part of the US Critical Infrastructure.



CONTACT
www.forcepoint.com/contact

INTERNAL REFERENCE #FPFB-2017-0027
[DS_FP_HIGH_SPEED_GUARD_ICS_EN] 100024FED.082017