HardwareWall® (HWW)
Cross Domain Solution

May 20, 2021

Problem Statement:

Mission Operations require a broad set of supporting data to plan and execute a given mission. This data often originates from different sources on disparate networks of varying security classifications (such as NIPR, SIPR, JWICS, NATO and coalition partner enclaves on BICES). As the sensitivity of an operation increases, so does the required degree of separation between the supporting networks in order to maintain information security. For example, space-based missions require cloud cover and collision avoidance data, airborne missions require weather, situational awareness, and electronic order of battle (EOB) data, and maritime missions require ocean current and state information, where various networks host this data separately from the Mission Operations network. Further, disconnected and disparate networks are likely to host collection requirements and the recipients of this collected data. Moving the supporting data and disseminating collected mission data between these networks can be a challenging factor in successful Mission Operations.

HWW Background:

HardwareWall (HWW) is a cross-domain solution (CDS) that provides the secure and efficient transfer of data with physical separation, virus protection, and enforcement of data handling policy between otherwise disconnected networks operating in multiple security domains, e.g. unclassified (U), secret (S), and top secret (TS). HWW supports bidirectional transfer of file-based and streaming data in a wide variety of formats. The dynamic HWW rules engine extends to support additional formats.

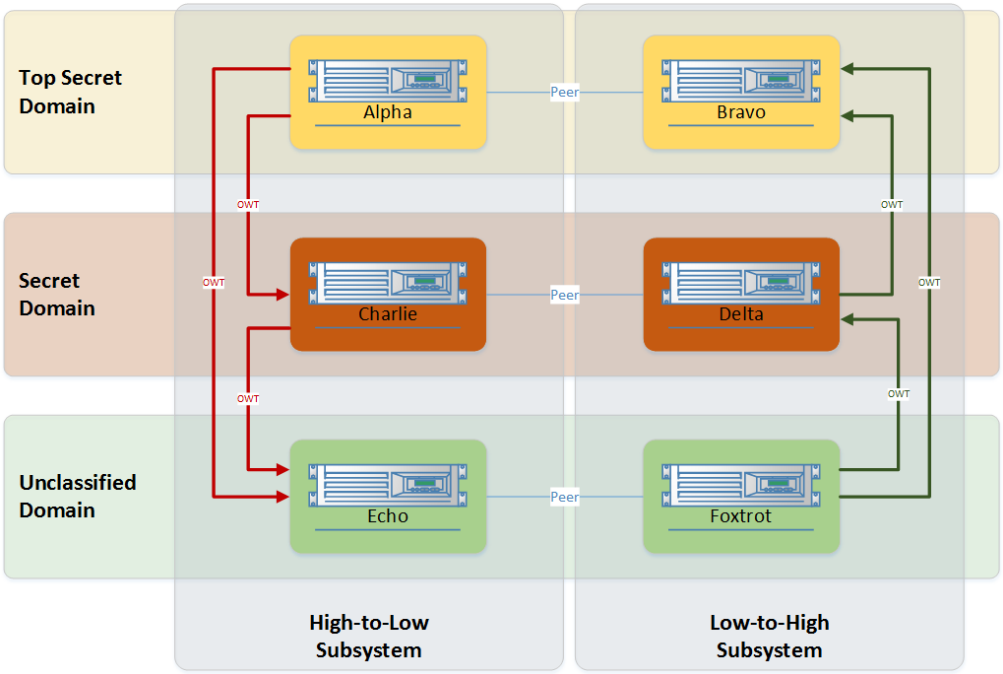

Figure 1: HWW Notional System Architecture

In its full three-domain configuration, both the modular HWW server system, as well as a single 1U or 2U HWW tactical system, consist of two directional subsystems with six servers: three servers for the low-to-high subsystem and three servers for high-to-low subsystem. Each directional subsystem hosts a single server in each security domain. The optional peer connection between the directional subsystems in each domain facilitates log file rotation to a specified domain, status notification for data delivery acknowledgement, health status of each node, and virus definition updates.

Low-to-High File Transfer of Mission Support Data:

Mission Operations require the transfer of file-based and streaming support data to the operational network on a regular basis, i.e. weather data, raster data such as maps and imagery, and administrative files such as briefings, documents, and spreadsheets. This sort of data typically originates on networks operating at a lower classification than the operational network. As a result, physical separation and anti-virus protection are of primary importance and the data handling policy enforcement tends to be more basic. If the data originates from a trusted source, the data handling policy enforcement may simply check the file's particular type rather than inspecting the value of specific metadata fields.

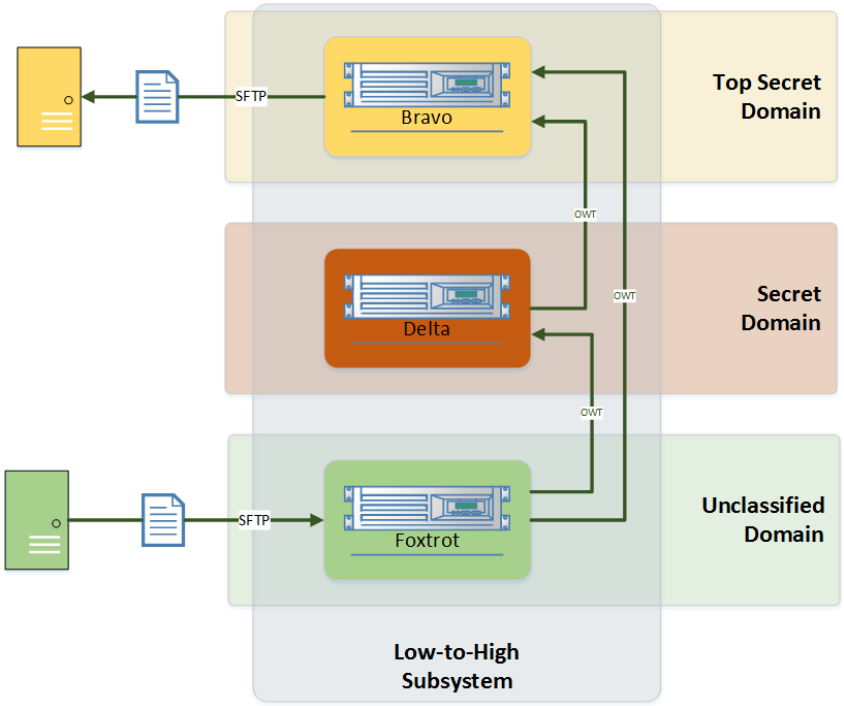

Figure 2: Low-to-High File Transfer Example

In the scenario shown in Figure 2, the HWW low-to-high subsystem receives data from a specific host (not shown) via a secure file transfer protocol (SFTP). Once transferred, HWW scans the file for viruses and applies rules prior to transferring the data to a designated storage location on the operational network. All data is virus scanned and ruleset checked once per domain. For example, if data were to pass from the U domain to the S domain then to the TS domain, HWW would check that data three times prior to reaching its final destination. The system configured to send data to HWW on the low side can send data in an automated fashion or via an ad-hoc user request. The orchestration of the transfer to HWW is outside the system boundary for the HWW system so it provides maximum flexibility for the organization. Implementations include automated polling of an incoming directory to transfer mission support data from a trusted source (or a well-audited user directed transfer) to automate organizational data-transfer duties.

Low-to-High Streaming of Data:

Streaming data can also be required to provide Mission Operations users with a comprehensive common operational picture. Track data from sources such as the Automatic Dependent Surveillance Broadcast (ADS-B), the Automatic Identification Service (AIS), and many of the Department of Defense (DoD) tactical data feeds are delivered as network streams. HWW provides a

mechanism to receive this data on the low-side network and transfer it to the operational network.

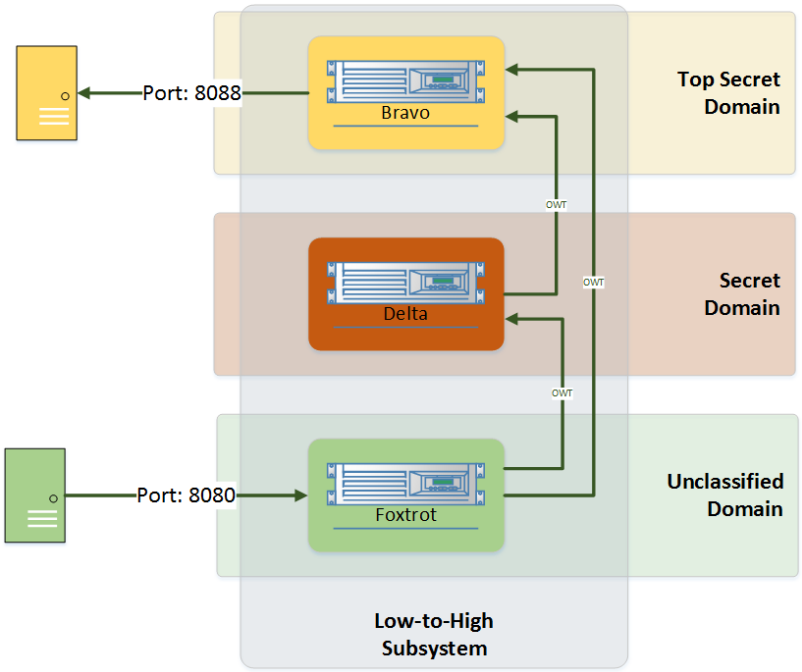

Figure 3: Low-to-High Streaming Example

HWW receives data from a specific server on a specific port (Figure 3). HWW inspects the received packets from the low-side server via the rules engine in real-time. Like low-to-high file transfer, low-to-high streaming transfer maintains physical separation of the networks as its primary focus. If the source of the data is from a trusted system, there exists a reduced need for rigorous packet inspection. On the operational network, the HWW system rebroadcasts the packets on a designated port to the consuming clients. HWW streaming support is designed to minimize latency and supports data transfer rates on par with the fastest guards in the industry. HWW supports encrypted network traffic by acting as a proxy for such connections.

Low-to-High File Transfer in Support of Software Development:

The ability to develop software in an unclassified environment offers considerable benefit for an organization or unit. Unclassified software development promotes re-use of code across programs, encourages information sharing between vendors, facilitates the adoption of interface standards, and reduces the overall cost of security accreditation by eliminating the need to accredit sophisticated and rapidly changing development environments. Unfortunately, the transfer of code and compiled software from the unclassified network to a classified

integration network represents a huge barrier to the benefit of all these things. Establishing a file-based transfer though HWW allows for agile development and deployment of customer software required to support ISR Mission Operations.

High-to-Low Dissemination of File-based Mission Data:

Data handling policy enforcement is much more rigorous in high-to-low transfers than it is in low-to-high transfers. Where low-to-high transfers are almost exclusively concerned with file integrity, high-to-low transfer must inspect the content of the transferred files to ensure the protection of data from unauthorized disclosure.

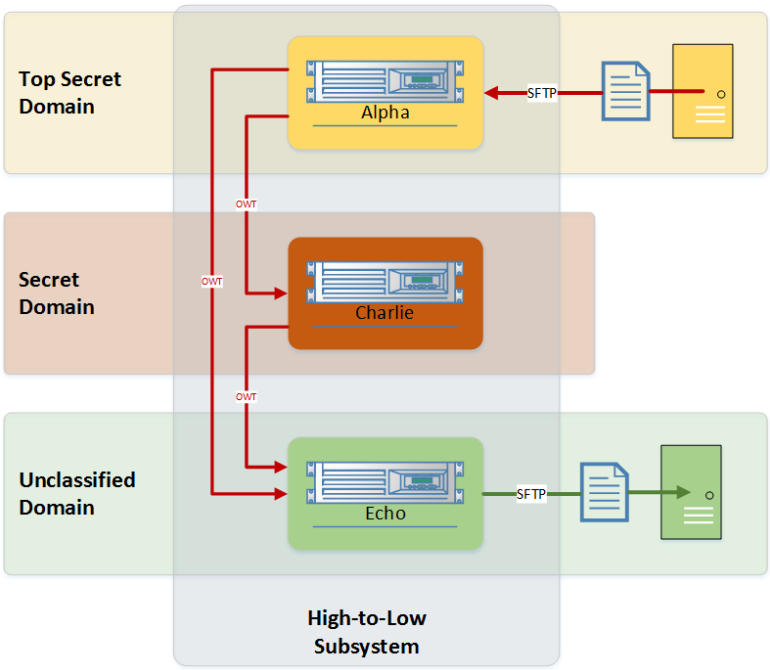

Figure 4: High-to-Low File Transfer Example

In a high-to-low transfer scenario, the HWW rules engine inspects the content of specific fields in a given file. Inspection rules indicate the specific position of the data in the file and the logic specific to the release of the data based on designated values. HWW includes a library of rules relevant to Mission Operations, which include rules that read metadata in National Imagery Transmission Format (NITF) data and Moving Picture Experts Group (MPEG) video with embedded Key-Length-Value (KLV) video files. In addition to the existing library of rules, customized rules can support new formats or security policy without the need to release software. Many current HWW customers become proficient in authoring their own rules, with trusted Boeing HWW Integrators available to assist if needed.

Often, the unit or organization responsible for Mission Operations does not have direct configuration control on the lower classification networks as they are commonly owned by peer programs or the enterprise. This is an important distinction when planning a high-to-low transfer as there needs to be a designated server to receive transferred data on the lower classification network. If the Mission Operations team does not control the receiving network there will be additional coordination required.

High-to-Low Dissemination of Streaming Mission Data:

Just as HWW supports low-to-high streaming transfer, it can also support high-to-low streaming (Figure 5). Similar to file transfers, rules inspect the content of data packets streaming through a HWW instance. For example, this feature supports the transfer of vehicle telemetry data and sensor data such as streaming video or signal information.

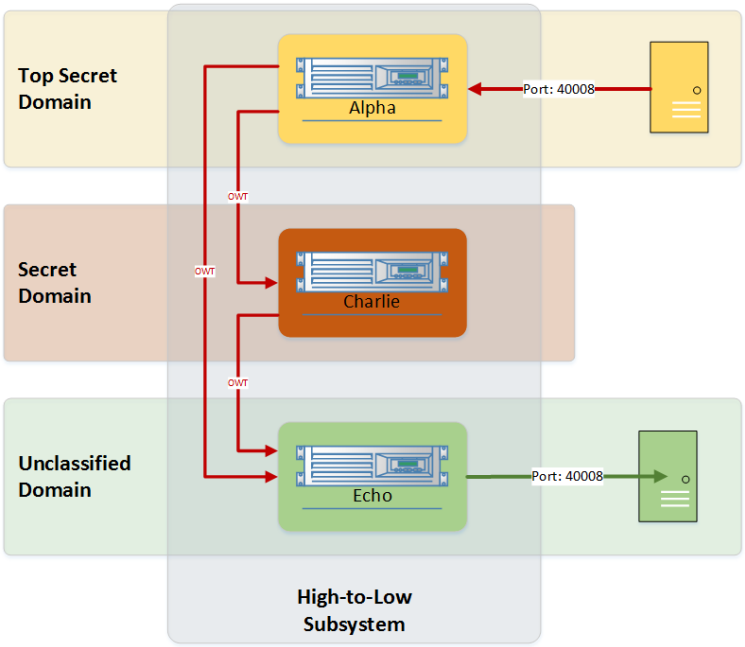

Figure 5: High-to-Low Streaming Example

Boeing Cross Domain History:

Boeing HWW has deployed hundreds of Cross Domain Systems over its 20+ year history with continuous A&A efforts. Boeing HWW has enjoyed success at each step of the ever-evolving cross domain security requirements from operating system requirements (Trusted Solaris 8 to Red Hat Linux 7.x, to RHEL

8.x on the horizon) to accreditation requirements (DCID 6/3 and DIACAP to ICD503/RMF and NCDSMO's Raise-The-Bar).

HWW Cross Domain Solution has been accredited across the DoD and IC in PL-3, PL-4, and PL-5 configurations. The first TS ←→ U system was accredited in 2003, and HWW continues to support U, S, and TS configurations in a modular enterprise system or a single tactical unit.

HWW has been independently tested within the CDS market and the results consistently show HWW to be the easiest for users to manage, including ruleset changes or additions, configuration changes, and installation and integration efforts. In a specific test for MTBF, the HWW enterprise system was the only CDS to run without interruption for the entire length of the study. HWW throughput speed has also consistently ranked as the fastest with specific data types and data validation requirements in both enterprise systems and tactical units.

HWW Full training support is provided for the users, and a variety of support contracts are available if Boeing is the preferred support path. HWW has yet to require an FTE for any of its deployments.

Contracting Address:

The Boeing Company
12701 Fair Lake Cir STE 700
Fairfax, VA 22033-4907
Cage Code 2R708
DUNS Number 96281393
Large Business

Sales Contract:

SalesAMS@Boeing.com
1-888-775-4390