Forcepoint

Solution Brief

Forcepoint Cross Domain Suite For Tactical Deployments

Challenge

- The U.S. Department of Defense (DoD) must deploy highly mobile cross domain systems in-theater.
- Systems must be modular and rapidly configurable, meet size, weight, power, and cost (SWaP-C) requirements, and provide access to applications and data on multiple networks of varying sensitivity levels.

Solution

- Secure access to multiple domains from just one device.
- Secure, efficient data transfers between segmented networks.
- Work offline with disconnected comms, with no loss of work.

Outcome

- Secure access and transfer of data between segmented networks at speeds previously unimagined.
- End-user collaboration when and where they need to, without onerous logistical barriers.
- Reduced hardware and infrastructure costs and automated processes and reduce complexity.
- Work offline, keep smart card authentication, access applications, work with local content, sync data when connection is re-established, without losing work.

The U.S. Department of Defense (DoD) has a need to deploy highly mobile cross-domain systems in-theater. These systems must be modular and rapidly configurable, meet size, weight, power, and cost (SWaP-C) requirements, and provide access to applications and data on multiple networks of varying sensitivity levels.

Without an approved, multi-network security solution in place, accessing three different network domains requires three Type-1 encryptors and three endpoint devices, each of which can only access a single network. Users waste time going between computers to access their required networks, and each workstation requires a sizeable investment to maintain and support. This approach is highly impractical in-theater, and virtually impossible on mobile platforms with limited space.

Improving efficiency through secure multi-network access

Forcepoint Cross Domain Suite for tactical deployments is a secure multi-network access solution that solves the difficult problem of satisfying security needs while enhancing user productivity regardless of the user's physical location.

With Forcepoint Cross Domain Suite deployed in austere environments, the necessary equipment in-theater or in-vehicle can be reduced by up to two-thirds. Eliminating encryptors, network switches, and cabling reduces footprint and setup requirements, as well as cost.

→ **Trusted Thin Client (TTC)**: A cross-domain access solution for x86-based endpoints. Each endpoint simultaneously accesses all allowed networks without the need for users to switch between devices.

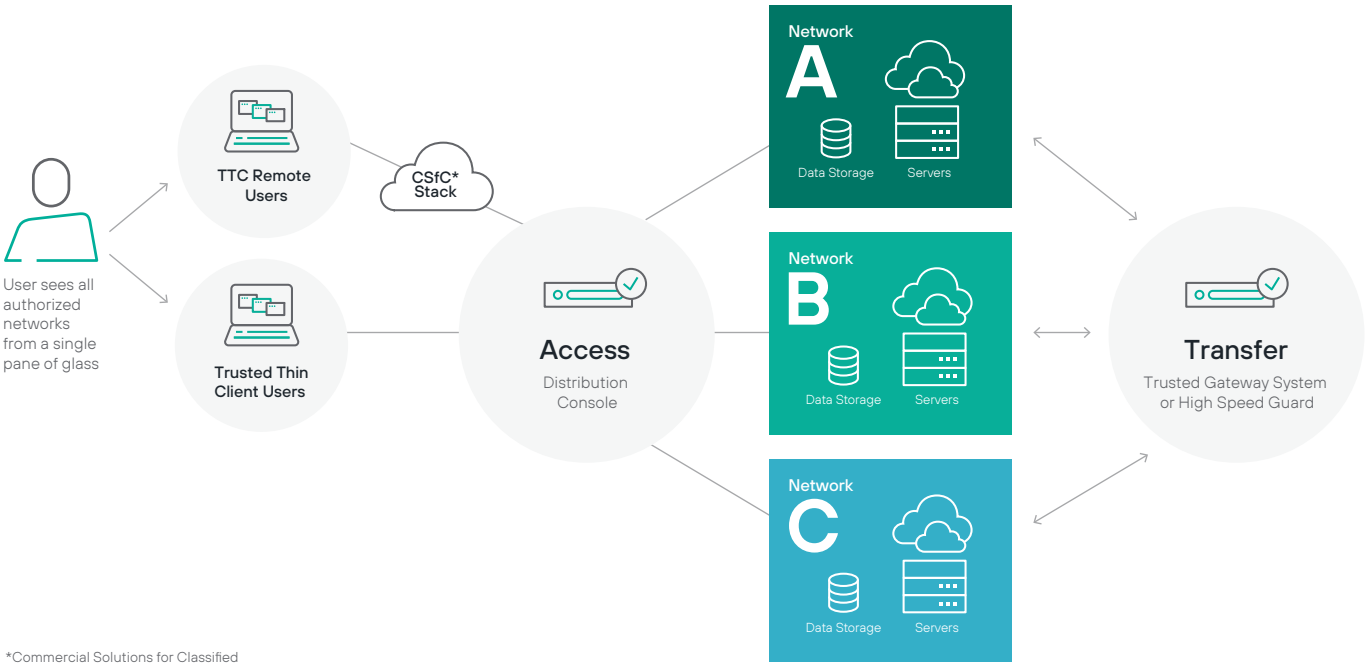
- TTC Distribution Console spanning reduces network complexity. A single endpoint across the wide-area network (WAN) or low-bandwidth networks (tactical/satellite) can span to other Distribution Console servers in different enclaves via one network drop, eliminating the need to pull network cabling.

→ **Trusted Thin Client Remote:** Extends the proven cross-domain technology of TTC for wireless endpoints or black network infrastructures using a certified Commercial Solutions for Classified Infrastructure.

→ **Trusted Gateway System:** A cross-domain unstructured file transfer solution. Unstructured file types can be moved between different classifications of networks without manual processes that require data be copied to uncontrolled external media ("Sneakernet").

→ **Forcepoint High Speed Guard:** Streams weather, map, or other structured data in real time, from machine to machine and between security levels, keeping up with the speed of operations.

MLS Access and Transfer Components:



*Commercial Solutions for Classified

TACTICAL MISSION CHALLENGE	CROSS DOMAIN FOR TACTICAL SOLUTION
Access to multiple networks requires laying and maintaining heavy network cabling with multiple network administration interfaces that are complex and difficult to maintain.	Reduce network cabling to one wire (or WiFi over CSfC) and centralize network resources and management with Trusted Thin Client and TTC Remote.
It is costly to provide temporary field locations with network drops and cabling for multiple networks.	Trusted Thin Client Distribution Console spanning allows users to connect to enclaves in geographically disparate datacenters under a single administrative management console.
Transferring Office documents (e.g., .doc, .pdf, .pptx) between security levels exposes data to additional attack vectors and exfiltration when moved with "Sneakernet."	Eliminate external media usage risks and inefficiencies with Trusted Gateway system, a secure file transfer solution.
Operating system or system patching is cumbersome and involves manual processes with file types that are sensitive to move without filtering first.	Disseminate patches between security levels with High Speed Guard, a machine-to-machine data transfer solution, without requiring downloads to external media first.
Multiple hard drives and multiple endpoints in theater increases risk of "Data-at-Rest" spillage.	No "Data-at-Rest" on user end-devices with Trusted Thin Client. For TTC Remote, the solution supports Commercial Solutions for Classified (CSfC Data At Rest) self-encrypting drives (SEDs).
Disrupted or Disconnected communications (network connection) when working at the tactical edge, can cause loss of work on an endpoint.	Enables user to keep smart card authentication, work locally on the endpoint, and upon communications reconnection, will sync up with no loss of work.

Cross Domain tactical hardware

The tactical Cross Domain Solution packages scale up and down to support large and small deployments, from 2 to 20+ users:

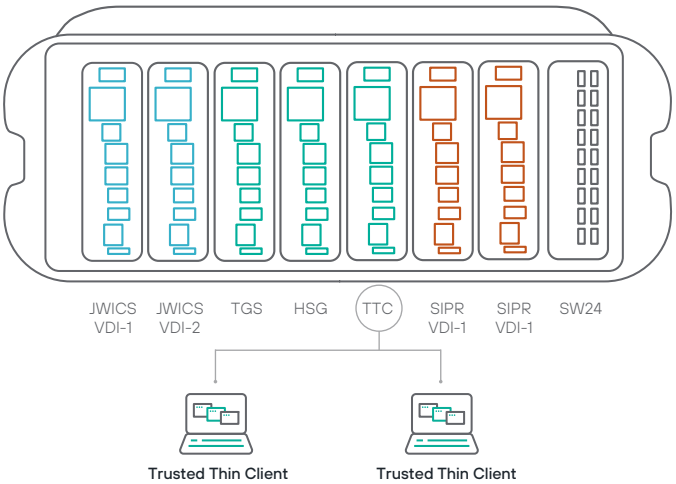
- → Can support a variety of hardware vendors.
- → Modules can combine and interoperate to create a total communications/data solution.
- → Chassis can support single- or multi-enclave configurations.
- → Minimum hardware requirements include:

HARDWARE	MINIMUM REQUIREMENTS	MEDIUM 1U[1]	MEDIUM 2U[2]
Processor Type	E5-2603 v4, 1.7GHz/15M	E5-2650 v4, 2.2GHz/30M	E5-2630 v4, 2.2GHz/25M
# of Processors	1	1	2
# of Cores	6	12	10
RAM	32GB	64GB	64GB
Expansion Slots	2 PCIe 3.0	2 PCIe 3.0	6 PCIe 3.0
Common	Hewlett Packard Enterprise® (HPE) or Dell®		
	Network: 1 Gb 331i QP Ethernet or 1 Gb Broadcom 5720 QP Ethernet		
	Drives: 2 x 300GB 10K SAS RAID 1		
	RAID: HPE Smart Array P440ar/2 Gb or PERC H730P 2 Gb		

[1]1U are Dell R630 or HPE DL360
[2]2U are Dell R730 or HPE DL380

Cross Domain tactical software

- → Multi-level Access: Trusted Thin Client (TTC) Remote; Simultaneous access up to five enclaves and <20 users support single device.
- → Transfer: Trusted Gateway System, High Speed Guard; Secure multi-directional data transfer between networks.
- → No data at-rest on user end devices. Reduced administration.
- → Reduced Garrison VDI footprint forward.
- → SABI and TSABI Certified.
- → Trusted Thin Client Remote can be part of a Commercial Solutions for Classified (CSfC) solution.



forcepoint.com/contact

[Cross-Domain-Suite-Tactical-Deployments-Solution-Brief-EN] 19Oct2021