Leveraging DTECH Products in a VPN CSfC Solution

Abstract

> The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off - the - Shelf (COTS) products. The Capability Packages are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators. (https://www.nsa.gov/ia/programs/csfc_program/)

This paper provides an example utilization of DTECH's commercial off the shelf (COTS) products being utilized to implement a CSfC Virtual Private Network (VPN) Capability Package. The CSfC VPN Capability Package describes a CSfC system that meets the demand for using commercial products to protect data in transit. The VPN Capability Package Version 3.0 enables customers to implement VPNs between two or more sites and VPNs between fixed sites and End User Devices (EUDs).

References:

- https://www.nsa.gov/ia/_files/VPN_CP_3_0.pdf
- www.DTECHlabs.com

1 Introduction

The M3-SE Product Family consists of modular interlocking set of components that share a power supply.

The M3-EXT Product Family consists of modular interlocking set of components with a modular UPS/power design.

The NSA CSfC VPN Capability Package v3.2 defines the architecture and requirements necessary to field a VPN CSfC Solution. CSfC Solutions must use certain products from the NSA's CSfC Components list. Even though DTECH's M3-SE products don't appear directly on the CSfC Components list, DTECH M3-SE products embed CSfC components or can be used to host software that is a CSfC Approved Component.

2 VPN Architecture and Components

2.1 VPN Capability Package Overview

The following Architecture diagram is sourced from the VPN Capability Package document.

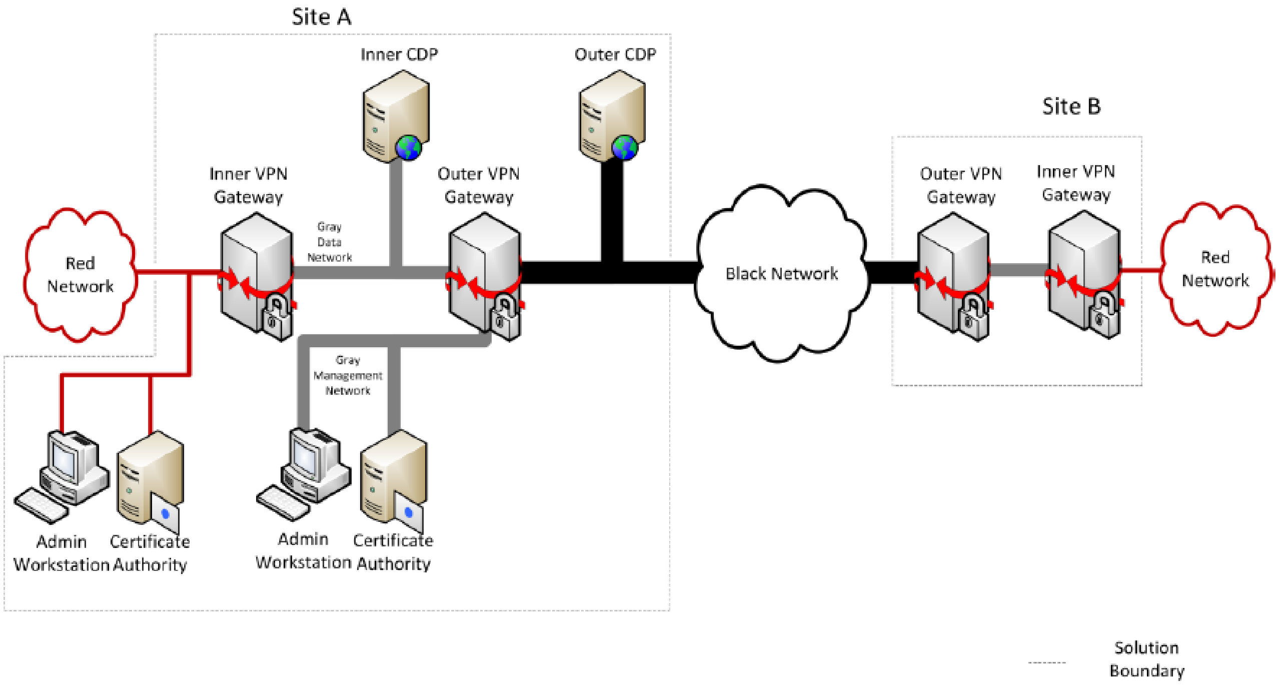

Figure 1: Two Layers of Encryption Protected Data across an Untrusted Network

In the VPN architecture, see Figure 1, the VPN Gateways are all similar devices, however the inner and outer gateways may not be sourced from the same baseline/manufacturer. The 2 layers of cryptographic services are provided using IPsec in the specific modes permitted by the Capability Package. The CRL Distribution Points (CDPs) are servers that make the Certificate Authorities list of known bad certificates available for retrieval by the VPN Gateways. Certificate Authorities are the servers that create, revoke and otherwise maintain the list of certificates used within the solution. Admin Workstations are computers that are used exclusively for managing the CA, VPN Gateway, CDP, and any other solution infrastructure asset. Other optional network assets not shown in Figure 1 include standalone firewalls, System Information and Event Management (SIEM) software and Intrusion Detection System/Intrusion Prevention System (IDS/IPS).

Note that the scope of what is contained within the solution's boundary for a given site can range in size/count dependent on if the site is providing supporting services (CDP, CA, Admin Workstations). Typically the scenario is that multiple remote sites are only "participant" or remote nodes in the VPN, while a single or only a few sites are the centralized management nodes providing CA, CDP, and Admin Workstations. There is nothing in the Capability Package that prohibits remote nodes from directly connecting with one another, however depending on VPN configuration the VPNs will likely require access to the CDP in order to establish any VPN. Therefore while the management VPN node is not in the remote-to-remote traffic path it may be required to be present to support remote-to-remote VPN session establishment.

In this Capability Package it is envisioned that the red networks are provided for individual devices through multiple subnets of machines. The architecture can even be extended for use with multiple classification levels through the addition of more Inner VPN Gateways as seen in Figure 2.

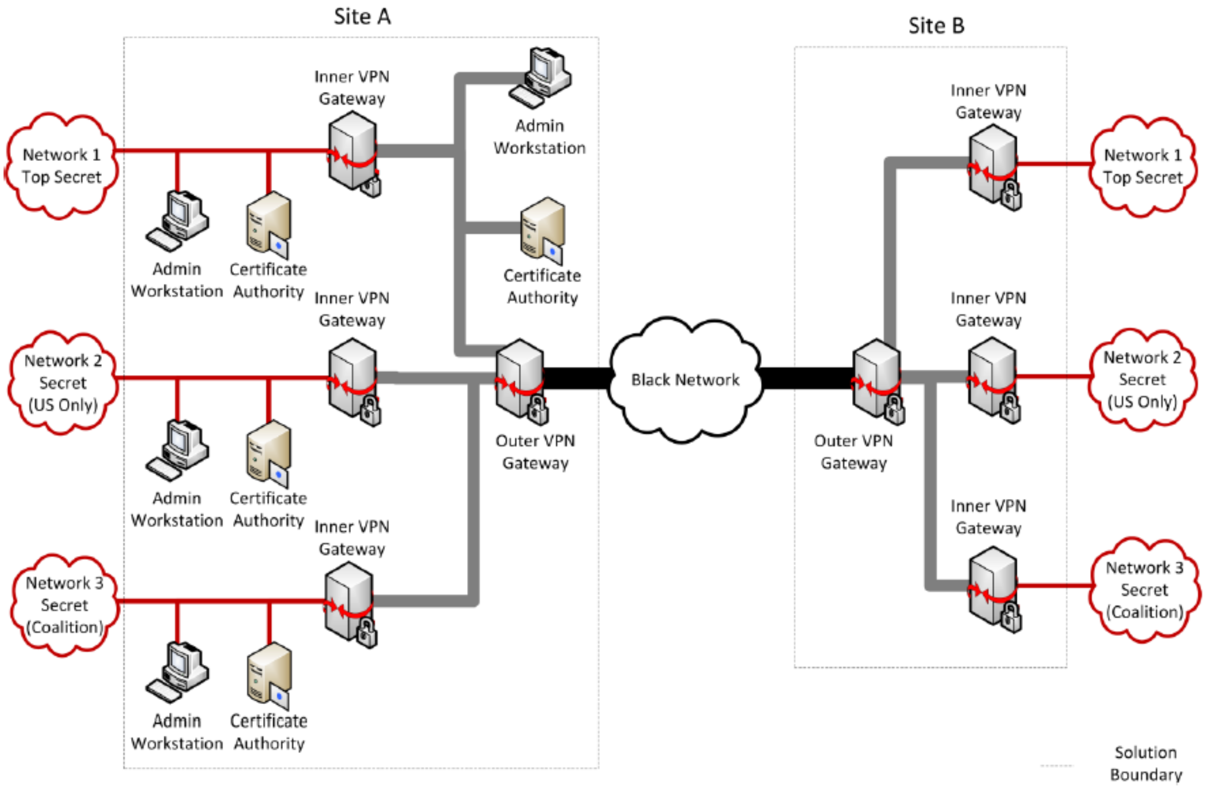

Figure 2: CSfC VPN Solution with Multiple Classification Levels

2.2 The DTECH M3-SE Products as VPN Solutions

As shown in Section 2.1 above, VPN solutions generally fall under two categories of nodes/sites/solutions: remote and central management. For the purposes of this paper the M3-SE product line is used as an example, however the component roles prescribed within the VPN Capability Package map to many different DTECH products. The M3-SE product line is a small form factor rugged family of stackable interlocking modules that share a common power supply and integrated UPS battery backup. M3-SE products are ideal for rapid deployment or high mobility systems. An example of how to use DTECH M3-SE products to achieve each type of VPN node is shown in the following subsections.

2.2.1 M3-SE Products as a Central Management VPN Node

An example VPN management node solution built from DTECH M3-SE components is shown below in Table 1. This solution includes many optional components including the CDP, SIEM, and IDS/IPS.

Table 1: DTECH M3-SE CSfC VPN Capability Functional to Physical Mapping – Central Management Site

Function	M3C4G Model	CSfC Component
Outer CDP	M3-SE-APP3	Windows Server 2012 R2 (as CDP server)
Outer VPN Gateway w/ Gray Firewall function	M3-SE-SVR3Q	Aruba VMC VM
Gray CA, Gray SIEM, Gray IPS/IDS, Gray Admin Workstation	M3-SE-SVR3	Windows Server 2012 R2 (with SIEM software, IDS/IPS software, CA software, and as a workstation)
Inner VPN w/ Red Firewall function	M3-SE3	Cisco ESR 5915
Red CA, Red SIEM, Red IPS/IDS, Red Admin Workstation, Red content server/services	M3-SE-SVR3Q	Windows Server 2012 R2 VM (with SIEM software, IDS/IPS software, CA software, and as a workstation), Windows Server 2012 R2 VM (as content server)

In practice, a group of equipment like what is depicted above could be split into 2 stacks with independent power supplies to extend UPS life and create a cleaner red/black boundary. The resulting system would look like what is depicted below in Figure 3.

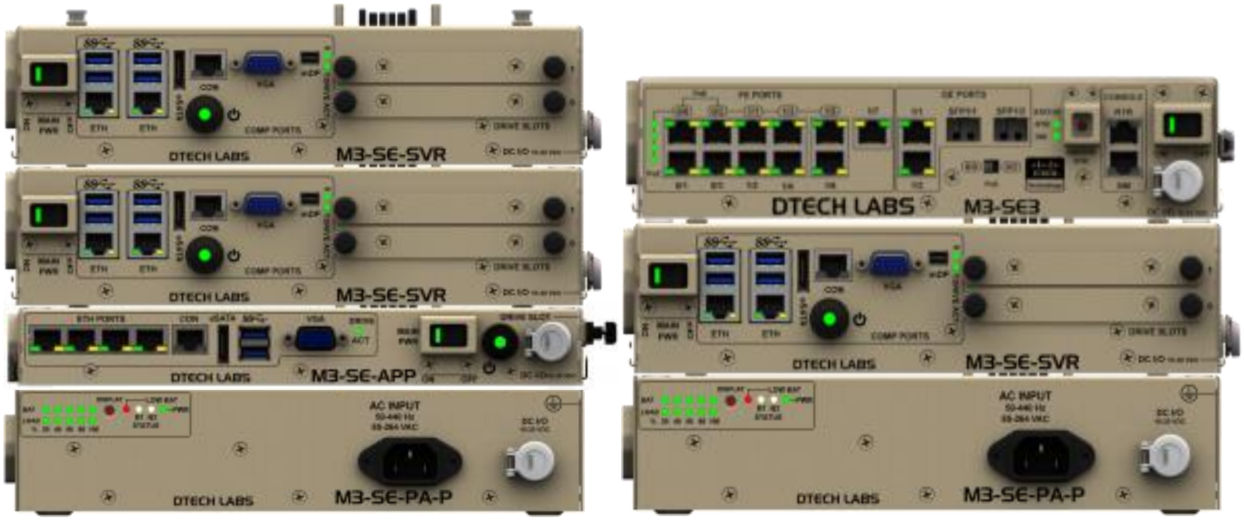

Figure 3: DTECH Example M3-SE VPN Management Node Gray Network (left) and Red Network (right)

This example stack up is easily modified to add more compute power for applications or mission specific interfaces. The inclusion of additional M3-SE modules can provide E&M ports for LMR integration, telephony ports, MANET radio, switches, bulk storage, and/or more computers/servers.

2.2.2 M3-SE Products as a Remote VPN Node

An example VPN remote node solution built from DTECH M3-SE components is shown below in Table 2.

Table 2: DTECH M3-SE CSfC VPN Capability Functional to Physical Mapping – Remote Site

Function	M3C4G Model	CSfC Component
Outer VPN Gateway w/ Gray Firewall function	M3-SE-SVR3Q	Aruba VMC VM
Inner VPN w/ Red Firewall function	M3-SE3	Cisco ESR 5915

In practice, a group of equipment like what is depicted above in Table 2 could be used on a single UPS power supply. The resulting system would look like what is depicted below in Figure 4.

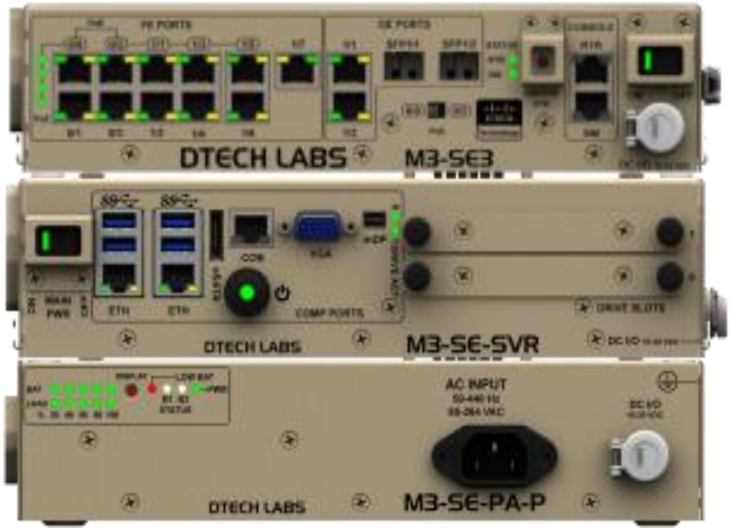

Figure 4: DTECH Example M3-SE VPN Remote Node

Just as in the Gray Network example stack, the mix of capabilities is easily modified to add more compute power for applications or the number and type of ports/interfaces. The inclusion of additional M3-SE modules can provide E&M ports for LMR integration, telephony ports, MANET radios, Ethernet ports, cellular radios, bulk storage, and/or more computers/servers.

2.2.3 M3-EXT Products as a Remote VPN Node

An example VPN remote node solution built from DTECH M3-EXT components is shown below in Table 3.

Table 3: DTECH M3-EXT CSfC VPN Capability Functional to Physical Mapping – Remote Site

Function	M3-EXT Model	CSfC Component
Outer VPN Gateway w/ Gray Firewall function	M3-EXT-COMP1	Aruba VMC VM
Inner VPN w/ Red Firewall function	M3-EXT	Cisco ESR 5915

The resulting system would look like what is depicted below in Figure 5. Note that the pictured system also includes a MANET radio module within the M3-EXT in-board expansion bay.

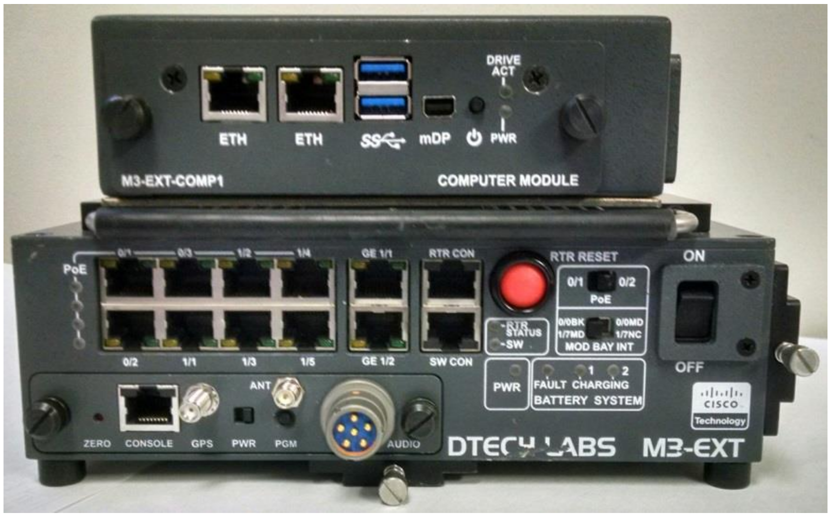

Figure 5: DTECH Example M3-EXT VPN Remote Node

Just as in the Gray Network example stack, the mix of capabilities is easily modified to add more compute power for applications or the number and type of ports/interfaces. The inclusion of additional M3-EXT modules can provide E&M ports for LMR integration, MANET radios, Ethernet ports, cellular radios and Wi-Fi, and/or more computers/servers.

3 Conclusion

The CSfC VPN Capability Package provides government users with a set of instructions and guidance on how to go about properly using commercial products to field classified services. The DTECH M3-SE product line provide an industry leading combination of small size and rugged design that meets the requirements of government users in even the most challenging of conditions. When composing CSfC solutions to meet the NSA published CSfC Capabilities Packages DTECH products can be effectively used either directly or as host platforms across the entire spectrum of CSfC components. In those cases where DTECH equipment is already fielded or in use, modifying those systems to provide a CSfC solution would require only minimal modification or reconfiguration.

4 Points of Contact:

Nick Podolak
Senior Principal Software Engineer
CUBIC | DTECH LABS
nicholas.podolak@DTECHlabs.com
http://www.DTECHlabs.com/

Or contact an account manager at sales@DTECHlabs.com . They may assist in getting any questions answered or support needed regarding DTECH products used for CSfC or any other requirements you may have.