World Wide Technology

COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) - TELEWORK ACCESS TO CLASSIFIED DESKTOPS

BACKGROUND

A Department of Defense (DoD) global combatant command has a requirement for Secret Internet Protocol Router Network (SIPRNet). The requested solution will support ~1500 key personnel as they continue critical mission operations through the COVID-19 national emergency. WWT rapidly responded with a team to provide an initial solution to the DoD customer.

PROPOSED SOLUTION

This solution will enable a DoD customer SIPRNet user to work remotely while securely accessing and creating classified information. Most of the hardware is located on military facilities, with minimal hardware and software at a user's location. This solution meets the National Security Agency's (NSA) guidelines for CSfC. WWT's solution provides a functional workspace during quarantined situations and a secure method for working with classified data in a non-secure facility. The NSA's CSfC requires a dual encryption encapsulated connection for the purpose of transmitting classified data over an unclassified network.

WWT's solution provides a dual-hardware tunnel option as a preliminary/budgetary design. This design includes two virtual private network (VPN) routers and a Dell/Wyse Thin Client with docking station at each teleworker location. Per the CSfC's guidelines, the two VPN routers are products from discrete manufacturers. The VPN routers and the Dell Wyse clients can be centrally managed. Our forward-looking solution allows for future modifications such as removing one of the hardware tunnels and replacing it with a software tunnel.

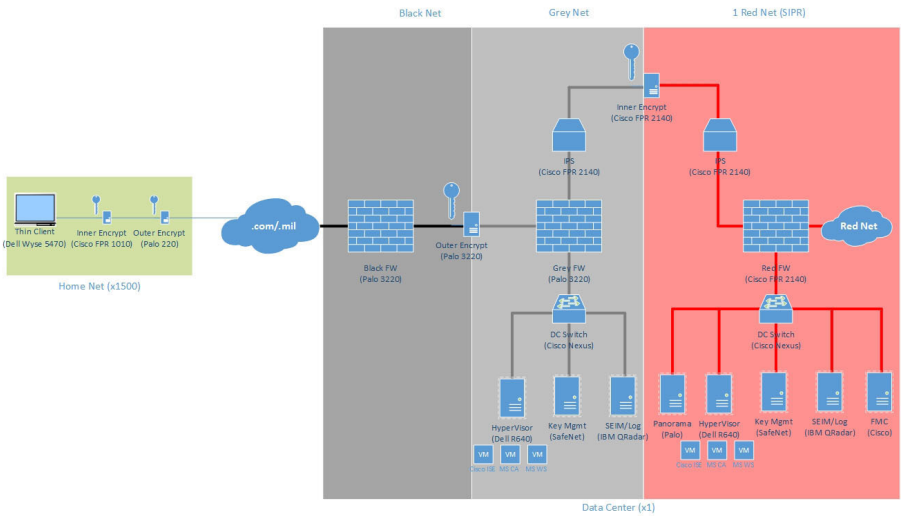

Figure 1: High Level Design Topology Diagram

GET STARTED TODAY

WWT is an NSA Certified Trusted Integrator on the Commercial Solutions for Classified program. WWT has deep experience designing and implementing solutions for customers that exceed CSfC guidelines and standards. Ask your WWT salesperson about WWT's CSfC knowledge and solutions. Let WWT help you design your next-generation remote access solution today.

ABOUT WWT

World Wide Technology (WWT) is a technology solution provider with more than USD 11 billion in annual revenue that provides innovative technology and supply chain solutions to large public and private organizations around the globe. While most companies talk about delivering business and technology outcomes, WWT does it. Based in St. Louis, WWT employs more than 6,000 people and operates over 4 million square feet of warehousing, distribution and integration space at its Integration Centers around the world.

World Wide Technology
1 World Wide Way
St. Louis, MO 63146

wwt.com/federal

PRODUCT OVERVIEW

Endpoint User Device(s) (EUD): Wyse 5470 Thin Clients with docking stations – These laptop-like thin clients meet the CSfC's requirements of no local persistent storage to eliminate the need for further CSfC data at rest (DAR) encryption requirements. Additionally, this allows the end user device to only be considered classified when connected to the VPN with a virtual desktop infrastructure (VDI) session open. Disconnected and powered off end user devices revert to an unclassified state per DISA guidelines. The 5470 also utilizes VMware's wide area network (WAN) and graphics-friendly Blast Extreme protocol. The included docking stations allow teleworkers to attach additional monitors for higher-resolution applications. The Dell Wyse 5470 Thin Clients attaches to the Cisco Firepower 1010 end user tunnel device at the users telework location.

Home IPSEC Router (Outer Tunnel): Palo Alto 220 – This end user tunnel device provides Internet Protocol Security (IPSEC) encryption and serves as the outer CSfC tunnel. The Palo Alto 220 is a small office/home office, small form factor device that requires minimal desktop space. The Palo Alto 220 attaches to a user's "Internet Provider" and the Cisco Firepower 1010 end user tunnel device.

Home IPSEC Router (Inner Tunnel): Cisco Firepower 1010 - This end user tunnel device provides IPSEC encryption and serves as the inner CSfC tunnel. The Cisco Firepower 1010 is a small office/home office, small form factor device that requires desktop space. The Cisco Firepower 1010 attaches to the Palo Alto 220 and the Dell Wyse 5470 Thin Client.

Firewalls (Black/Grey/Red): Palo Alto 3220 – The Palo Alto 3220 serves as the Next-Generation Firewall (NGFW) for the Black and Grey Networks. The Cisco Firepower 2140 serves as the NGFW for the Red Network. The NGFW meets CSfC filtering requirements.

Data Center IPSEC Router (Outer Tunnel): Palo Alto 3220 – The Palo Alto 3220 serves as the Data Center facing outer IPSEC tunnel. This device serves as the IPSEC hub and terminates all the end user Palo Alto 200 devices.

Data Center IPSEC Router (Inner Tunnel): Cisco Firepower 2140 - The Cisco Firepower 2140 (ASA) serves as the Data Center-facing inner IPSEC tunnel. This device serves as the IPSEC hub and terminates all the end user Firepower 1010 devices.

Data Center Management:

- Two Dell R640 rack mount servers running VMWare vSphere act as Grey and Red network hypervisors for virtualized CA servers, virtualized authentication servers and virtualized management workstation(s).
- Two Cisco Firepower 2140 IPS devices serve as intrusion prevention security appliances for the Grey and Red networks.
- Two SafeNet key management servers for the Grey and Red networks.
- Two IBM QRADAR for Red and Grey network security incident and event management (SIEM) and logging servers.
- Two Cisco Nexus switches provide network management server connectivity for the Grey and Red networks.

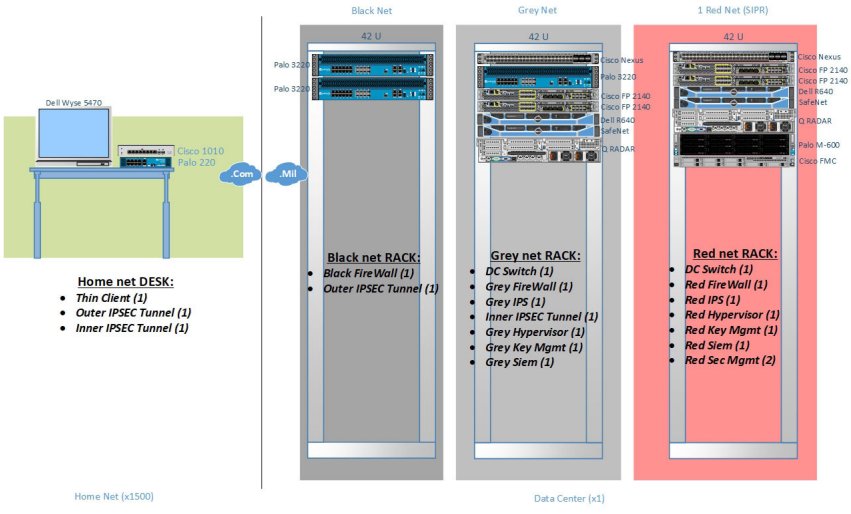

Figure 2: Rack Diagram

World Wide Technology