NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE

Commercial Solutions for Classified (CSFC) Multi-Site Virtual Private Network Capability Package

Version 0.8
March 14, 2012

This page left intentionally blank

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The Commercial Solutions for Classified (CSFC) program within IAD utilizes 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.

IAD is delivering a generic Multi-Site Virtual Private Network Capability Package to meet the demand for wired data in transit solutions utilizing a secure sharing suite (S3) of algorithms [NSA Suite B]. These algorithms, known as Suite B algorithms, are used to protect classified data using layers of COTS products. This Capability Package takes lessons learned from three proof-of-concept demonstrations that had implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

2. PURPOSE OF THIS DOCUMENT

This Capability Package provides a reference architecture and configuration information that would allow customers to select COTS products from the appropriate lists of NSA-approved products (called CSFC canisters) for their Multi-Site VPN solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. These solutions eliminate the overhead expenses that are imposed by Controlled Cryptographic Item (CCI) controls.

Customers who want to use a variant of the solution detailed in this Capability Package must contact NSA to determine ways to obtain NSA approval. Additional information about the CSFC process will be available on the CSFC web page www.nsa.gov/csfc.

3. DESCRIPTION OF THE MULTI-SITE VPN SOLUTION

The Multi-Site VPN solution addresses the need to protect classified information as it travels between enclaves of the same classification level across either an untrusted network or a network of a different classification level. As seen in Figure 1, there are two sets of VPN devices creating two independent Internet Protocol Security (IPsec) tunnels between the sites. The VPN devices closest to the trusted enclave (Site A or Site B, in the figure) are referred to as the Inner VPN devices. Likewise, the VPN devices closest to the untrusted network (i.e., farthest from the trusted enclaves) are referred to as the Outer VPN devices.

The following terms are used throughout this document:

- Red network – the network behind the Inner VPN device.
- Gray network – the network between the Inner and Outer VPN devices. This is broken down into two sub-networks, as follows:
    - Gray management network – the part of the Gray network that contains the management functions to run the Outer layer, including the Outer tunnel CA and the Outer VPN device admin/audit server functions.
    - Gray data network – the part of the Gray network that sends data between the Inner and Outer VPN devices.
- Black network – the network connecting the Outer VPN devices.

The figure shows data as it traverses the network. Red data exists in the network behind the Inner VPN device; this data is encrypted by the Inner IPsec VPN device and sent to the Outer VPN device (this tunnel is depicted in gray). That encrypted data is then encrypted once again, this time by the Outer VPN device and sent across the Black network (the second tunnel shown in black). This ensures that classified information is protected with two layers of encryption as it travels over the Black network each layer providing both confidentiality and integrity for the data.

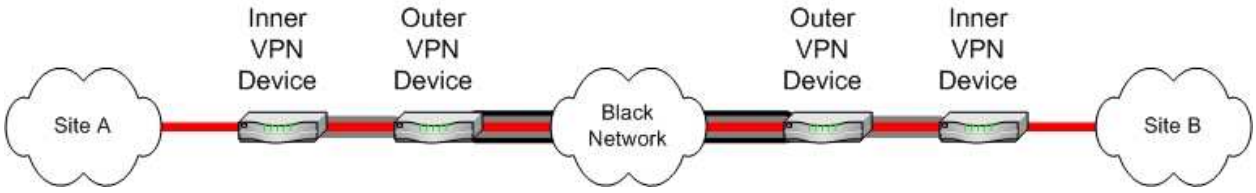

Figure 1. Two IPsec Tunnels Protect Data across a Black Network

This solution provides mutual device authentication during the tunnel setup, but does not provide any end user authentication for traffic going through the tunnels. Any required end user authentication must be provided separately and will not be considered as a part of this solution.

Throughout this document, when we discuss IP traffic, it can either be IPv4 or IPv6, unless otherwise specified. In addition, the Red, Gray and Black networks can run either version and each network is independent from the others in making that decision. Public standards conformant Layer 2 control protocols such as ARP are allowed as necessary to ensure the operational usability of the network. This Capability Package is agnostic with respect to Layer 2; specifically it does not require Ethernet. Public standards conformant Layer 3 control protocols such as ICMP may be allowed based on local DAA policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast

messages and IGMP may also be allowed depending on local DAA policy. Multicast messages received on external interfaces of the Outer VPN device shall be dropped and may be logged.

3.1 INTEROPERABILITY

The current version of the Multi-Site VPN Solution achieves interoperability between sites by having similar standards-based configurations at both ends of each layer of the solution. Commercial products currently do not allow for generic interoperability between any two approved products. It is an IAD goal to create and realize adoption of IPsec implementation standards that will allow for this generic interoperability. When widespread adoption of these standards has been achieved, a new version of the Multi-Site VPN Capability Package that requires these standards will be released.

3.2 ARCHITECTURE

There are two main types of multi-site architectures that were considered in developing this Capability Package—an architecture for Multiple Independent sites and an architecture with a Central Management Site. Fundamentally, either Multi-Site VPN solution architecture consists of two IPsec VPN devices at each site that respectively generate the Inner and Outer IPsec tunnels, providing two independent layers of encryption between the sites (see Figure 1). Fundamental network architecture components, such as DNS and NTP, are not shown in the figures or explicitly discussed in this document. These components should be located on the inside network (Gray network for the Outer VPN device and Red network for the Inner VPN device).

3.2.1 ARCHITECTURE FOR MULTIPLE INDEPENDENT SITES

In the architecture with multiple independent sites, each site performs the administration of its own VPN devices and has the option of using CAs that they control (see Figure 2). In this case, the sites need to agree on the VPN devices to ensure interoperability. In addition, the two VPN devices at each site need to have the signing certificate and revocation information for the corresponding CAs used by the other sites in the system installed. This architecture requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. This model has the advantage of allowing communication between larger organizations that have a need to share information while maintaining independence.

Note that while Figure 2 depicts two independent sites, this solution can scale to include numerous sites with each additional site having the same architecture as Site B.

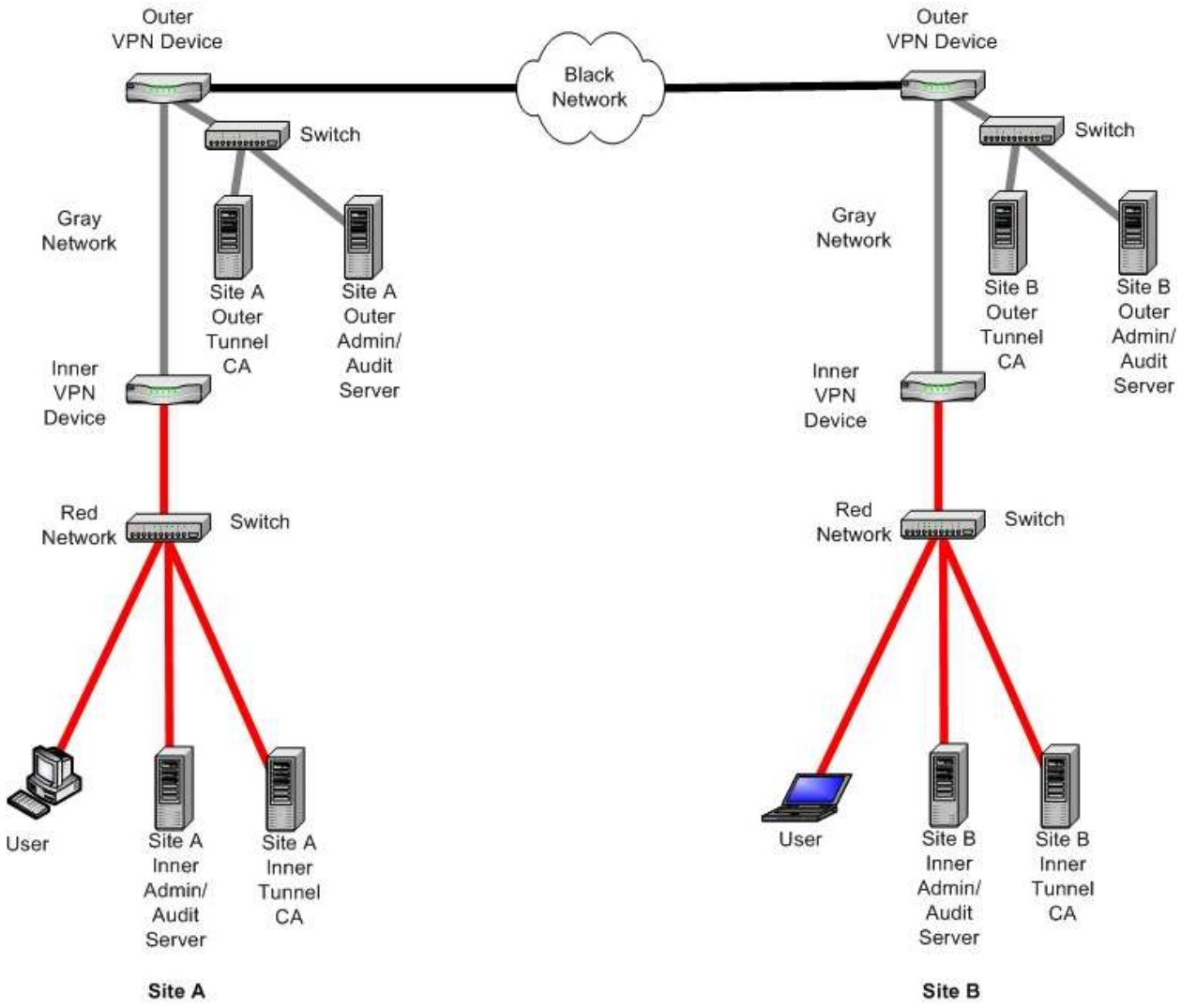

Figure 2. VPN Architecture for Multiple Independent Sites

3.2.2 ARCHITECTURE WITH A CENTRAL MANAGEMENT SITE

In the architecture with a central management site, a single site administers and performs keying for all the various sites included in the solution. Figure 3 provides an example of this architecture, where Site A is the central management site and Site B is one of potentially many other sites in the network. In this case, because the administration is done by one group of Security Administrators and CA Administrators, they can ensure interoperability of each site as sites are added and can manage just two CAs, one on the Red network for all the Inner VPN devices and one on the Gray management network for all the Outer VPN devices. This model makes it easier to add sites because of the centralized administration.

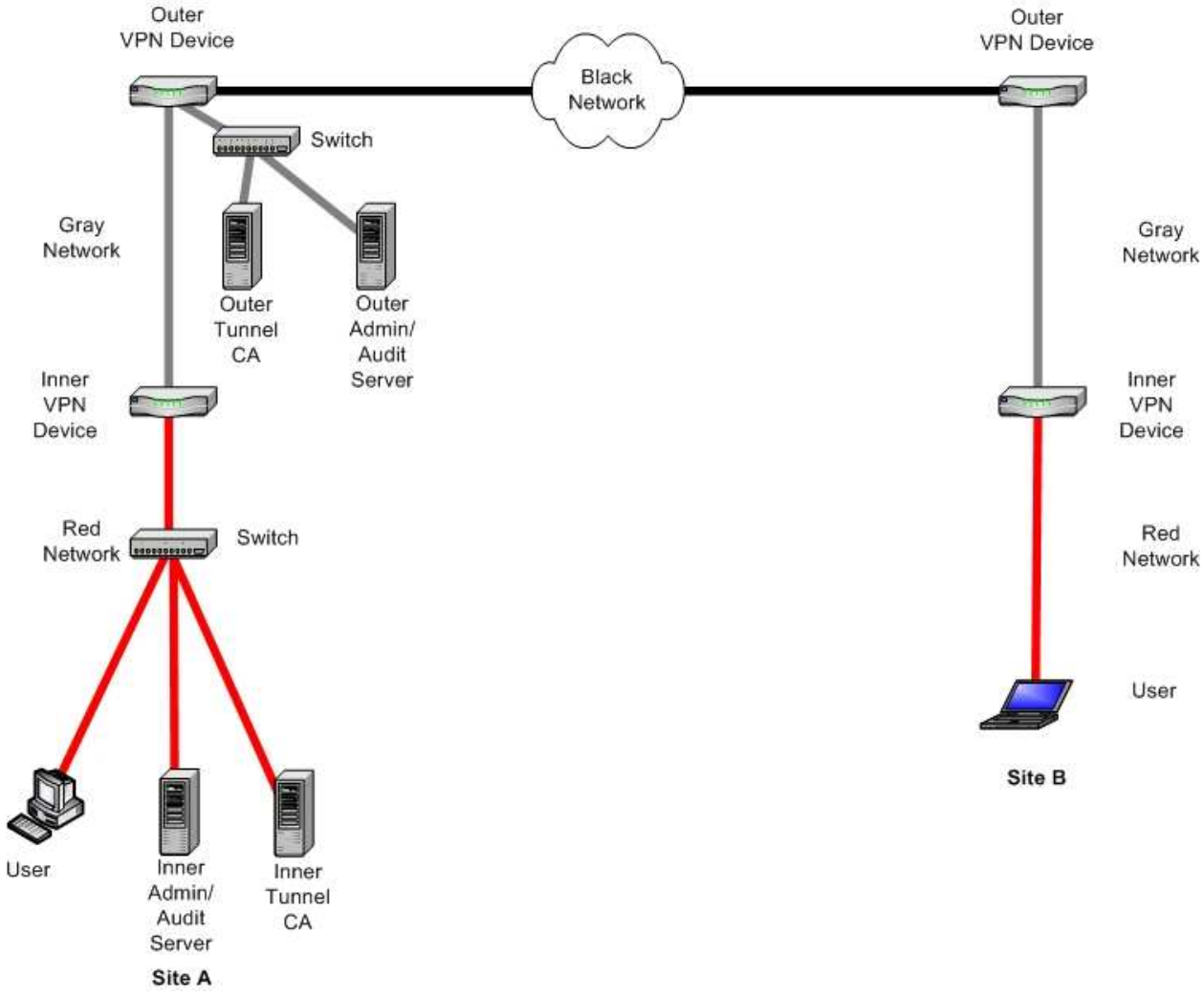

Figure 3. Multi-Site VPN Architecture with a Central Management Site

Note that while Figure 3 depicts two independent sites, this solution can scale to include numerous sites with each additional site having the same architecture as Site B.

4. SOLUTION COMPONENTS

The Multi-Site VPN solution consists of two IPsec VPN devices at each site, with each generating an IPsec tunnel, providing two layers of encryption between sites (see Figure 1). In addition to the VPN devices, mandatory aspects of the solution include administration devices and Certificate Authorities (CA) for key management using Public Key Infrastructure (PKI). Each component is described below. The descriptions include information about the security provided by the components as evidence for why they are deemed mandatory for the solution. Overall System Security is discussed in Section 6.

Additional components are discussed in Section 4.5 that can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution and, therefore, will not have configuration or security requirements placed on them.

4.1 OUTER VPN DEVICE

Authentication of a peer VPN device, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules are all aspects fundamental to the security provided by a VPN device.

The Outer VPN device located at the edge of the private network generates an IPsec tunnel, which provides device authentication and confidentiality and integrity of information traversing the unsecure/untrusted Black network. VPNs offer a decreased risk of exposure of information in transit since any information that traverses the Black network is placed in a secure tunnel that provides an authenticated and encrypted path between two sites.

Although the Outer VPN device is a perimeter VPN device and thus more exposed to external attacks, the VPN device is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flow which helps mitigate Denial of Service (DoS) attacks and prevent resource exhaustion. This solution does not require that the Outer VPN device terminate all VPNs on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 8.4.

There is some data that will originate from the Outer VPN device (such as logging and audit data, which will potentially be sent to the Gray Management network at another site) that will only go through a single IPsec tunnel. This is the only exception to having two layers of encryption for data going over the Black network and is considered acceptable given the intelligence value of that information.

4.2 INNER VPN DEVICE

Similar to the Outer VPN device, the Inner VPN device provides authentication of a peer VPN device, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules. Unlike the Outer VPN device, however, the Inner VPN device is not a perimeter VPN device and, therefore, not as exposed to external attacks, but it is more exposed to an internal attack.

The Inner VPN offers a decreased risk of exposure for data-in-transit by providing an encrypted tunnel between two sites. Along with the Outer VPN, this results in a solution with two layers of IPsec providing protection for the data-in-transit. Any single layer using Suite B algorithms should be strong enough for such a Multi-Site VPN solution. However, a single layer may be prone to vulnerabilities introduced accidentally through implementation or operator error, or intentionally by an adversary leading to compromise of sensitive information. The addition of multiple layers reduces the likelihood that such a vulnerability can be exploited to attack the full solution, particularly if the layers exhibit suitable independence.

If the Outer VPN is compromised or fails in some way, the Inner VPN can still provide the needed security for the data. In addition, the Inner VPN device can indicate that a failure of the Outer VPN device has occurred. Through the use of its internal filtering capability, the Inner VPN device is capable of protecting the network from unknown traffic by logging information about the packets received. This will indicate that the Outer VPN device has been breached or misconfigured to permit traffic to pass through to the Inner VPN device that is not allowed.

4.3 CERTIFICATE AUTHORITIES

The CA issues digital certificates for the VPN devices in this solution. These certificates are used for authentication in establishing the IPsec tunnels between the sites. Given the architecture of the solution, there are distinct CAs for the Inner and Outer VPNs. The CA providing certificates for the Inner VPN is located on the Red network, and the CA providing certificates for the Outer VPN is located on the Gray management network. This provides the key management separation required for two independent layers of encryption.

4.4 ADMINISTRATION DEVICES

Each VPN device shall also have an administration platform on the appropriate network that allows for maintaining, monitoring, and controlling all security functionality for the particular VPN device. This administration device shall also allow for logging and configuration management, as well as reviewing audit logs. Given the architecture of the solution, there are distinct administration networks for the Inner and Outer VPN devices. The administration devices for the Inner VPN are located on the Red network, and the administration devices for the Outer VPN are located on the Gray management network, which shall not be directly connected

to the Black or Red networks. This provides the separation necessary for two independent layers and supports the requirement for separate roles for each site.

4.5 OTHER COMPONENTS

There are two additional components that could be utilized within this solution to potentially reduce the overall risk of the solution. First, if the Multi-Site VPN solution attaches directly behind an existing router from a site that connects to the Black network, then from the Multi-Site VPN solution perspective, the existing router is considered part of the Black network infrastructure, though it provides some level of filtering and attack detection for the solution. Second, a more comprehensive Intrusion Detection System (IDS) could be used if additional assurance is desired. A comprehensive IDS system could increase the difficulty of a rogue actor performing activities with the networks. However, it should be noted that any IDS on the Gray data network needs to be dedicated to monitoring that network and not interconnected with an IDS on the Red (or Black) network.

5. KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner. In this solution, the only certificates necessary are for the device authentication certificates on each of the two VPN devices at each site.

No single CA can provide keys to both the Inner and Outer VPN devices, also called edge devices in PKI terminology, to reduce the impact of a vulnerability in a single CA. The CA for the Outer VPN devices shall be located in the Gray management network, connected to an Outer VPN device. Since the Gray management network is a small local network, a locally run CA will usually need to be stood up to key the Outer VPN devices, requiring that a CA product be selected from the NSA-approved CSFC canister for the Outer tunnel PKI. In addition, a Certificate Policy (CP)/Certification Practice Statement (CPS) document shall be tailored from a reference CP/CPS document available from the CSFC website, for this CA product and for the specific network environment. Then it is the Designated Approving Authority's (DAA) responsibility to approve the use of this CA.

The CA for the Inner VPN devices shall be located on the Red network, which allows for use of existing enterprise CAs already operational on the Red network, as required in Section 8.8.2 of this Capability Package. The Inner tunnel CA will be the enterprise CA already running on the Red network, which is acceptable for this solution; no additional approval is necessary for use of this CA. For example, a solution may utilize an enterprise CA (such as a CNSS-approved CA, which follows CNSSI 1300 under the NSS PKI Root CA), to issue certificates to the Inner VPN device.

Each VPN device shall have at least one CA signing certificate, which is used by the VPN device to authenticate other VPN devices in the solution and is sometimes referred to as a Trust Anchor.

For the architecture with a Central Management site, there will be only one CA signing certificate in each VPN device. For the architecture with Multiple Independent sites, one CA signing certificate shall be installed in each Inner VPN device for each Inner Tunnel CA utilized in the system. Similarly, one CA signing certificate shall be installed in each Outer VPN device for each Outer Tunnel CA utilized in the system.

Each VPN device will contain a private key that corresponds to a certificate issued by its CA, a CA signing certificate(s) as described above, and revocation information. The private key may be locally generated and shall be adequately protected. Both Inner and Outer tunnel PKIs shall utilize ECDSA signatures within X.509 certificates. The algorithms and elliptic curves that are approved for use in this Multi-Site VPN solution are found in Table 2 (see Section 8.1).

The Multi-Site VPN Solution described here requires certificates to establish the secure tunnels between VPN devices. Without certificates, the network cannot function. Thus, an out-of-band method shall be used to issue the initial certificates to the VPN devices. Future rekeying, however, should take place over the network through this solution prior to the current key's expiration. Certificate revocation information shall be updated at the same time that the device is rekeyed, and as directed by the DAA in the case of potential compromise.

6. OVERALL SYSTEM SECURITY

This section details how the required components work together to provide overall security in the solution. Figure 4 shows the security boundary of the Multi-Site VPN solution in blue.

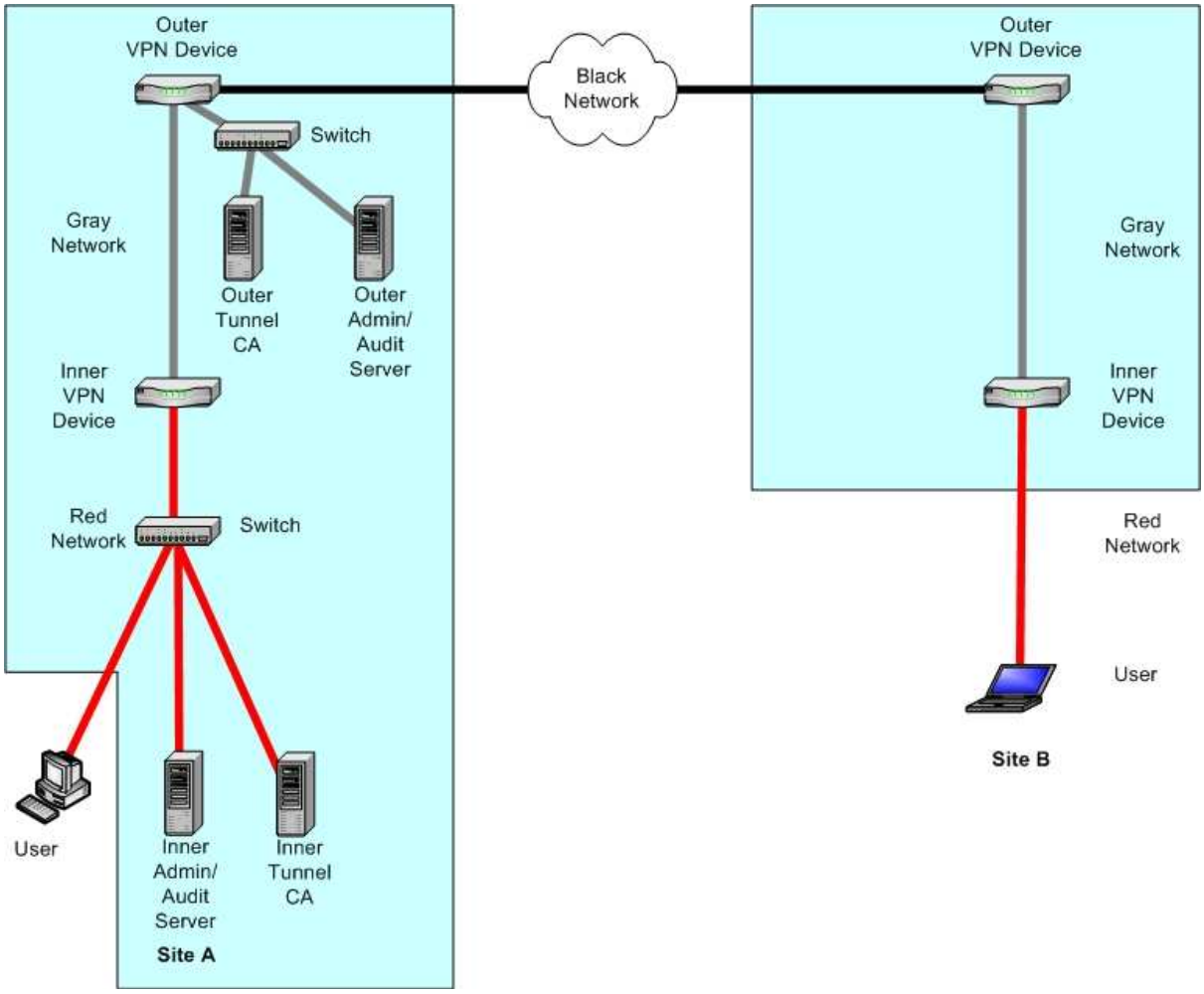

Figure 4. Security Boundary (Central Management Example)

An assessment of security was conducted on the overall architecture of the solution based on the Multi-Site VPN Capability Package while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data.

6.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the network without changing the state of the system. Threat actions include collecting or monitoring traffic (e.g., traffic analysis or sniffing the network) that is passing through a network in order to gain useful information through data analysis.

The security against a passive attack targeting the data in transit between the two sites is provided by the layered IPsec tunnels. To mitigate passive attacks, two layers of Suite B encryption, AES, is employed to provide confidentiality in each tunnel. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The two VPN devices that are used to set up the tunnels must be independent in a number of ways (see Section 7). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to get through both tunnels.

6.2 EXTERNAL (ACTIVE) THREATS

This threat refers to outsiders gaining unauthorized access to a system or network or exfiltration of sensitive Red network data. Threat actions include introducing viruses, malware, or worms with intentions to compromise the network or exfiltrate data or to analyze the architecture of the network or system for future attacks. DoS or Distributed DoS (DDoS) attacks compromise availability of the system, ceasing secure communication between sites. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

6.2.1 ROGUE TRAFFIC

One method for detecting rogue traffic from an external attack as it tries to get through one or both VPN devices is by having the port filtering native to each VPN device enabled and configured to audit and log any traffic that is not of the format described in the configuration (see Section 8). It is required that the port filtering will be set up to block any traffic not coming from or going to an IP address on the network at the other site, traffic not contained in IP packets other than control plane protocols needed for network operation and approved by DAA policy, and traffic going to unexpected ports. This will allow the Auditor(s) and/or the Security Administrator(s) to detect whether the Outer VPN device has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of a misconfigured Outer VPN device.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on the Red and Gray management networks to ensure that the VPN device configurations are not changed without the knowledge of the Security Administrator. The Auditor also ensures through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of VPN device misconfigurations.

6.2.2 Malware and Untrusted Updates

The administration devices and CAs for the Red network shall be distinct from the administration devices and CAs for the Gray network. This separation will minimize the potential of malware on a single device impacting both the Inner and Outer tunnels.

Each individual component of this solution has the capability to perform trusted updates through verification of a signature or hash to ensure that the update is from a reliable source, such as signed by the vendor. This mitigates threats of malicious users trying to push updates or code patches that affect the security of the component (and therefore system). The source of all updates and patches should be verified before installation occurs.

6.2.3 Denial of Service

DoS attack risks cannot be completely mitigated. The solution requires dropping all packets that are not IKE, ESP, or approved control plane protocol traffic on the appropriate interfaces, which significantly reduces the potential of flooding attacks. For customers that require more protection against these attacks, one option is the use of an optional perimeter router. This moves the responsibility to protect against a DoS attack away from this solution and back to a router that is already an established part of the customer's network. Other mitigations are acceptable and up to the DAA to approve their use.

6.2.4 Social Engineering

It is left up to the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in this section and already discussed.

6.3 Insider Threats

An authorized or cleared person or group of people with access–physical or logical–to the network or system may act maliciously or negligently resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the equipment, dishonest employees, or those that have the means and desire to gain escalated privileges on the network.

Threat actions include insertion or omission of data entries that result in loss of data integrity, unintentional access to an unauthorized system or network, unwillingly or unknowingly executing a virus or malware, intentionally exposing the network and systems to viruses or malware, cross contaminating a system or network with data from a higher classification to a lower classification (e.g., Secret data to Unclassified network or system), or malicious or unintentional exfiltration of classified data. Typically, the threat from insiders has the potential to

cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 10). In addition, logging and auditing of security critical functionality (see Section 8.7) is required. Finally, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. In scenarios that need additional assurance, an optional IDS could be deployed on the Gray network to help identify whether there is a failure, misconfiguration, or attack on the Inner or Outer VPN devices.

6.4 SUPPLY CHAIN THREATS

This threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the Multi-Site VPN Solution. This threat is hard to identify and test for and is increasingly harder to prevent or protect against since vendors build products using subcontracts with other companies to make certain parts of components, and it often is hard to tell where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, or at a warehouse or in storage.

There are doctrinal requirements placed on Implementers and System Integrators of these solutions to minimize the threat of supply chain attacks (see Section 9).

6.5 ADDITIONAL MITIGATION INFORMATION

Traffic to the Inner VPN device, including administration of the Inner VPN device at Site B is protected by two IPsec tunnels across the Black Network (see Figure 3). In the Central Management Architecture, similar traffic from the Gray management network administration devices would be protected by a single IPsec tunnel across the Black Network. As such, another approved encryption method from the IPsec VPN Client Protection Profile (SSH, IPsec, or TLS) shall be utilized for all traffic from the Gray management network administration device to a port on the Outer VPN device at Site B. The keys to authenticate the administration device shall be at a minimum self-generated RSA/DSA keypairs, using NIST recommendations for digital signature use beyond 2013 [SP 800-131A], but also could be ECDSA keypairs using elliptic curves given in Table 2.

To avoid potential implementation weaknesses, solutions need to be regularly patched in accordance with local policy and Information Assurance Vulnerability Alerts (IAVA) recommendations, thus minimizing the risks from newly discovered component vulnerabilities present in the solution. Product selection rules dictate methods for maximizing the independence between layers of the solution, which is done in part so that new vulnerabilities usually affect only one of the two layers. Only components included in applicable NSA-approved CSFC canisters shall be used in implementing the Multi-Site VPN solution (see Section 7).

The VPN devices will automatically perform health checks on security critical components (such as the cryptographic algorithms) during power-on self tests. By ensuring that these algorithms are not modified, the expected strength of the Suite B cryptography should be present in the solution while in use. The layering of solutions reduces the risk of single component failure breaking the security of the entire solution. However, a single component failure is likely to result in a DoS condition. One assumption underlying this solution is that loss of availability is considered a low risk because in a DoS condition, no data has been compromised, and the problem should be noticed immediately. If availability is critical for the customer, network engineering can support further DoS protection.

7. GUIDELINES FOR SELECTING COMPONENT PRODUCTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

PS1: Vendor Diversity – The Inner and Outer VPN devices shall come from different vendors. One vendor cannot be a subsidiary of the other.

PS2: Hardware Platform Diversity – The Inner and Outer VPN devices shall be run on separate physical hardware platforms.

PS3: Operating System (OS) Diversity – The Inner and Outer VPN devices shall not utilize the same OS for critical IA security functionality. Differences between Service Packs (SP) or version numbers for a particular vendor's OS do not provide adequate diversity.

It would also be beneficial when to ensure that the IPsec cryptographic libraries being used to establish the VPN tunnel are unique. In some cases, it may not be possible to know which library is used in the VPN devices, but if that information is available, then the two VPN devices should use different cryptographic libraries.

The products that are approved for use in this solution are listed on the IAD/CSFC website. No single product shall be used to protect classified information alone. The only approved methods for using COTS products to protect classified information follow the requirements outlined in a

Capability Package. Products shall be selected for the Multi-Site VPN solution from the canisters given in the following table.

Table 1. Canisters for the Multi-Site VPN Components

Component	Canister
Inner VPN device	IPsec VPN Gateway
Outer VPN device	IPsec VPN Gateway
Outer Tunnel Certificate Authority	Certificate Authority

Note that the Inner Tunnel CA is not included in Table 1. This CA is not selected from a canister because it is the CA that is already part of the customer's enterprise keying solution on the Red network.

8. CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components of the Multi-Site VPN solution.

8.1 CONFIGURATION REQUIREMENTS FOR BOTH VPN DEVICES

CR1: The proposals offered in the course of establishing the IKE Security Association (SA) and the ESP SA for the Inner and Outer Tunnels shall be configured to offer algorithm suite(s) containing only Suite B algorithms (see Table 2 or www.nsa.gov). As such, algorithm suites containing non-Suite B algorithms or parameters shall be removed from the list of algorithms offered during negotiation.

Table 2. Approved Suite B Algorithms

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	
Confidentiality (Encryption)	AES-128	AES-256	FIPS PUB 197
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3
Key Exchange/ Establishment	ECDH over the curve P-256 (DH Group 19)	ECDH over the curve P-384 (DH Group 20)	NIST SP 800-56A IETF RFC 6379 Suite B Cryptographic Suites for IPsec (IKEv2)
Integrity (Hashing)	SHA-256	SHA-384	FIPS PUB 180-3
Can protect	Up to Secret	Up to Top Secret	

CR2: The VPN device shall be configured to restrict the IP address range for the network administration device to the smallest range possible.

CR3: Default accounts, passwords, community strings, and other default access control mechanisms for the administration of the VPN devices shall be changed or eliminated.

CR4: The default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN devices shall not be used for establishing SAs and removed if possible.

CR5: A unique device certificate shall be loaded onto each VPN device along with the corresponding CA (signing) certificate. The device certificate shall be used for device authentication during IKE. The private key shall be stored on the VPN device and shall not be accessible through any of the router interfaces.

CR6: The VPN devices shall be configured so that the only approved physical paths leaving the Red network are through a Multi-Site VPN solution in accordance with this Capability Package or via an approved NSA-certified device (such as a HAIPE)[1].

CR7: Each VPN device shall be configured to audit and log when unauthorized access attempts and/or privilege escalation occur or are identified (see Section 8.7).

[1]In some cases, the customer will need to communicate with other sites that have NSA-certified Government off-the-Shelf (GOTS) equipment. In particular, it is okay for a given site to have both an egress path via an NSA-certified device and an egress path via a layered COTS solution conforming to this Capability Package. This will allow a site to communicate with remote sites that use either solution.

CR8: The time of day on each VPN device shall be synched with the Administration device and CA on the corresponding (Red or Gray) network. This is necessary to ensure that certificates are accepted by the VPN device and to ensure adherence to the validity period of the certificate.

CR9: The external interface of each VPN device shall drop all packets that use IP options (e.g., if the first byte is not 0x45 for IPv4, then the packet shall be dropped and may be audited).

CR10: The use of at least one outer interface loopback address is recommended. When present, the VPN device's loopback address shall be used as the source address for management functions. This is advantageous instead of handling the numerous physical interface addresses.

CR11: Passwords for administrative access shall be stored encrypted in the VPN device's configuration.

8.2 Additional Requirements for the Inner VPN Device

IR1: The Inner VPN device shall use the following protocols and algorithms for creating all VPN tunnels. Algorithms shall be selected from within a single Algorithm Suite column in Table 2.

- IKEv1 key exchange in Main Mode on Phase 1 or IKEv2 key exchange using the Diffie-Hellman Group 19 or 20
- Certificates based on the NIST P-256 or P-384 Elliptic Curve
- SHA-256 or SHA-384 for a hash function
- AES-128 or AES-256 in Cipher Block Chaining for IKE encryption
- Transport mode for IPsec using AES-128 or AES-256 with Cipher Block Chaining or Galois Counter Mode for ESP encryption
- IKE SA lifetime set to 24 hours
- ESP SA lifetime set to 8 hours
- No Perfect Forward Secrecy

IR2: The packet size for packets leaving the external interface of the Inner VPN device should be configured to keep the packets from being fragmented and impacting performance.

8.3 Additional Requirements for the Outer VPN device

OR1: The Outer VPN device shall use the following protocols and algorithms for creating all VPN tunnels. Algorithms shall be selected from within a single Algorithm Suite column in Table 2.

- IKEv1 key exchange in Main Mode on Phase 1 or IKEv2 key exchange using the Diffie-Hellman Group 19 or 20
- Certificates based on the NIST P-256 or P-384 Elliptic Curve
- SHA-256 or SHA-384 for a hash function
- AES-128 or AES-256 in Cipher Block Chaining for IKE encryption
- Tunnel mode for IPsec using AES-128 or AES-256 with Cipher Block Chaining or Galois Counter Mode for ESP encryption
- IKE SA lifetime set to 24 hours
- ESP SA lifetime set to 8 hours
- No Perfect Forward Secrecy

OR2: All traffic originating in the Red or Gray networks going out the external interface on the Outer VPN device shall be encrypted using an approved protocol.

8.4 Port Filtering Requirements for Both VPN Devices

PF1: For all interfaces connected to the Gray or Black networks, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols approved by policy are allowed. All other data shall be blocked and may be audited.

PF2: Any service or feature that allows the VPN device to call home to a site (such as maintained by the manufacturer) shall be disabled.

PF3: Outer VPN devices shall block all data (by ports and IP addresses) on their Gray Management network interface that is not necessary for the management of Outer VPN devices.

8.5 Configuration Change Detection Requirements

CM1: A baseline configuration for all Inner and Outer VPN devices shall be maintained by the System Administrator and the Auditor.

CM2: An automated process shall ensure that configuration changes are logged. This log entry shall include the specific changes to the configurations.

8.6 Requirements for VPN Device Administration

RA1: Inner and Outer VPN device administration management shall be performed from a VPN administration device (either on the Gray management network for the Outer VPN device or on the Red network for the Inner VPN device) as follows:

Remotely using the SSH protocol as specified in RFCs 4252-4254, the IPsec protocol as specified in RFCs 2409, 4302, 4303, 4307, 4308, 5996, and 6379, or the TLS protocol as specified in RFCs 5246 and 6460. The SSH, IPsec, or TLS data, as with all data, shall also be protected by the IPsec VPNs. In the case of the Outer VPN device, the SSH, IPsec, or TLS data will only be protected by one IPsec VPN tunnel that is also part of the double tunnel between the Red networks. Additional information about key sizes and options for using these protocols is available at [NSA Suite B].

RA2: The Admin workstations shall be dedicated for the purposes given in Section 4.4 and properly configured according to local policy and U.S. Government guidance (e.g., Defense Information Systems Agency (DISA) gold disk, NSA guidelines). Adequate procedures shall exist for handling, storage, and lifecycle support. Antivirus software shall be running on all Admin workstations.

8.7 Auditing Requirements

AU1: At a minimum, the following set of auditable events shall be monitored and logged by the VPN devices on a continuous basis:

- All modifications to the audit configuration and all actions performed on the audit log (off-loading, deletion, etc.).
- All actions involving identification and authentication.
- Attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.
- All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges.
- Any changes to the baseline configuration of a product.
- Certificate operations including generation, loading, or revoking of certificates.
- Changes to time.

- Receipt of unexpected data on any interface to the Gray data or management networks.
- All built-in self-test results, which may indicate failures in cryptographic functionality.

AU2: The set of auditable events specified in the CPS shall be monitored and logged within the outer-tunnel CAs used for edge devices on a continuous basis when in use.

AU3: The following information shall be recorded for each audit event:

- Date and time of the event
- Identifier for the event
- Type of event
- Success or failure of event to include failure code, when available
- Subject identity
- Source address for network based events
- User and role identification for role based events

8.8 KEY MANAGEMENT REQUIREMENTS

8.8.1 PKI REQUIREMENTS FOR BOTH EDGE DEVICES

KM1: The key sizes and algorithms used for the Inner and Outer VPN devices shall be as specified in Table 2 of this Multi-Site VPN Capability Package.

KM2: The CA shall be located on separate networks (specifically, the Red and Gray management networks). A separate CA shall support the Inner and Outer VPN, such that certificates are not generated by a single common CA.

KM3: Both the Inner and Outer tunnel CAs shall operate under a CPS that is formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.

KM4: Both Inner and Outer tunnel CAs shall utilize ECDSA signatures within X.509 certificates.

8.8.2 INNER TUNNEL PKI REQUIREMENTS

KM5: The Inner tunnel CA shall assert a registered Object Identifier (OID) to all of its Edge Devices.

KM6: The Inner tunnel CA shall be an approved Enterprise CA located on the Red network that is approved to issue certificates to Edge devices (such as one that follows CNSSI 1300 under the NSS PKI Root CA).

KM7: Inner tunnel Edge Devices shall only trust an Inner tunnel CA used within the solution.

8.8.3 OUTER TUNNEL PKI REQUIREMENTS

KM8: The Outer tunnel CA shall be chosen from the CSFC CA canister of NSA-approved CA devices. The DAA will need to approve the use of this CA, which will require a CP and CPS (see KM3) [CP/CPS reference document].

KM9: Outer tunnel Edge Devices shall only trust an Outer tunnel CA used within the solution.

KM10: All Outer tunnel CAs used for Edge Devices are subject to audit requirements against the CPS as defined in KM3.

KM11: The Outer tunnel CA shall only issue certificates to the Outer tunnel Edge Devices or to support its own operations.

KM12: All Outer tunnel keys/certificates for Edge Devices shall be used for authentication (i.e., signature only). Edge Device keys shall not be escrowed.

KM13: Certificate revocation information shall be made available by posting the data to a repository or service that is available for the Edge Devices.

KM14: The CA workstation used for the Outer tunnel shall be dedicated for this purpose and properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines). Adequate procedures shall exist for handling, storage, and lifecycle support. Antivirus software shall be running on all CAs.

KM15: The Outer tunnel CAs shall have a limited name space to issue certificates. Names shall be unique.

KM16: The Outer tunnel key validity period shall not exceed 14 months. New certificates may be issued as needed in accordance with local policy.

KM17: The VPN devices shall be initially keyed within a physical environment certified to protect the highest classification level of the Multi-Site VPN solution network. Rekeying shall be done over the Multi-Site VPN solution network prior to expiration of keys. The certification revocation information shall be updated at the same time as the device is

rekeyed. If rekeying is not completed prior to expiration of keys, they will need to be rekeyed through the same process as initial keying.

9. POLICY FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

P1: All components of the solution shall be physically protected as classified devices, classified at the level of the network in the solution with the highest classification. Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the components.

P2: All components of the solution shall be disposed of as classified devices, unless declassified using DAA-authorized procedures.

P3: Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.

P4: Solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation as determined by NSA.

P5: The DAA will ensure that a compliance audit shall be conducted every 3 years against the latest version of the Multi-Site VPN Capability Package, and the results shall be provided to the DAA. In addition, when a new version of the Multi-Site VPN Capability Package is published by NSA, the DAA shall ensure compliance against this new Capability Package within 6 months.

P6: Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months (see Section 11.3).

P7: Audit log data for security critical events (see Auditing requirements in Section 8.7) shall be handled according to the following requirements:

1. Audit logs shall be reviewed by the Auditor at least quarterly (or more frequently if required by the local DAA) to look for unauthorized access.
2. Audit log data shall be maintained for a minimum of 1 year.
3. During the quarterly review of the audit data, the amount of storage remaining for audit events shall be assessed in order to ensure that adequate memory space is available to continue recording new audit events.
4. Audit data shall be frequently offloaded to a backup storage medium in order to facilitate compliance with requirements 2 and 3 above.

P8: A set of procedures shall be developed to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.

P9: A procedure shall be developed for ensuring continuity of operations for the auditing capability. This plan shall include each of the following as a minimum:

- A mechanism or method for determining when the audit log is reaching its maximum storage capacity.
- A mechanism or method for off-loading audit log data for long term storage.
- A mechanism or method for responding to an overflow of audit log data within a product.
- A mechanism or method for ensuring that the audit log can be maintained during power events.

P10: Passwords – Strong passwords shall be used that comply with the requirements of the local security authority.

P11: Patching of components – It is expected that security critical patches (such as IAVAs) shall be made to all components in the solution. Local policy shall dictate how the Security Administrator will install patches on the Red, Gray, and Black networks.

P12: TEMPEST – The Multi-Site VPN solution does not provide any TEMPEST protections, thus any TEMPEST requirements shall be met through the facility's environment, which shall comply with local TEMPEST policy.

Additional policy can be found in Section 10 below.

10. ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are defined below, along with doctrinal requirements for these roles.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the Multi-Site VPN solution within a single site. Security Administrator duties include but are not limited to:

1) Ensuring that the latest software patches and updates, to include IAVAs, are applied to each product.

2) Documenting and reporting security-related incidents to the appropriate authorities.

3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.

4) Ensuring that the implemented Multi-Site VPN solution remains compliant with the latest version of this Capability Package.

Certificate Authority Administrator (CAA) – The CAA shall be responsible for maintaining, monitoring, and controlling all security functions for the CA products. CAA duties include but are not limited to:

1) Administering the CA, including authentication of all devices requesting certificates.

2) Maintaining and updating the Certificate Revocation List.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and CAA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the wired Multi-Site VPN solution. The role of Auditor and Security Administrator shall not be performed by the same individual. Auditor duties include but are not limited to:

1) Reviewing, managing, controlling, and maintaining security audit log data.

2) Documenting and reporting security related incidents to the appropriate authorities.

3) The Auditor will only be authorized access to the Outer and Inner admin components.

Solution Integrator – In certain cases, an external integrator may be hired to implement a Multi-Site VPN solution based on this Capability Package. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.

2) Configuring the Multi-Site VPN solution in accordance with this Capability Package.

Additional policies related to the personnel that perform these roles in a Multi-Site VPN Solution are as follows:

P13: The Security Administrator, CAAs, Auditor, and all Solution Integrators shall be cleared to the highest level of data protected by the Multi-Site VPN solution.

P14: When a previously established CA is utilized in the solution, the CAA already in place may also support this solution provided they meet D13.

P15: The Security Administrator, CAA, and Auditor roles shall be performed by different people.

P16: All Security Administrators, CAAs, and Auditors shall be meet local information assurance training requirements.

P17: The CAA(s) for the Red network shall be different from the CAA(s) for the Gray management network.

11. INFORMATION TO SUPPORT DAA

This section details items that likely will be necessary for the customer to obtain approval from the system DAA. The customer and DAA have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved Capability Package.
- The customer has a testing team develop a Test Plan and perform testing of the Multi-Site VPN solution, see Sections 11.1 and 12.
- The customer has system certification and accreditation performed utilizing the risk assessment information referenced in Section 11.2.
- The customer provides the results from system certification and accreditation to the DAA for use in making an approval decision.
- The customer registers the solution with NSA and reregisters yearly to validate its continued use as detailed in Section 11.3.
- The DAA will ensure that a compliance audit shall be conducted every 3 years against the latest version of the Multi-Site VPN Capability Package, and the results shall be provided to the DAA.
- The DAA will ensure that certificate revocation information is updated on all the VPN devices in the solution in the case of a compromise.
- The DAA will ensure that any Layer 2 or Layer 3 control plane protocols that are utilized in the solution are necessary for the operation of the network and that local policy supports their use.

The system DAA maintains configuration control of the approved solution implementation over the lifecycle of the solution. Additionally, the DAA shall ensure that the solution remains properly configured, with all required security updates installed.

11.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a Multi-Site VPN solution. This T&E will be a critical part of the

approval process for the DAA, providing a robust body of evidence that shows compliance with this Capability Package.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the Multi-Site VPN solution. The entire solution, to include each component described in Section 4, is addressed by this test plan.

1) Set up the baseline network architecture and configure all components.

2) Document the baseline network architecture configuration. Include product model and serial numbers, and software version numbers as a minimum.

3) Develop a Test Plan for the specific implementation utilizing the test objectives from Section 12. Any additional requirements imposed by the local DAA should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this Capability Package.

4) Perform testing utilizing the test plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.

5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the DAA for approval of the solution.

The following testing requirements have been developed to ensure that the Multi-Site VPN solution functions properly and meets the configuration requirements from Section 8. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

TR1: Ensure end-to-end communication between end users at each site.

TR2: Verify ability to manage all VPN devices in the solution.

TR3: Document the physical layout of the Multi-Site VPN solution implementation.

11.2 RISK ASSESSMENT

The risk assessment of the Multi-Site VPN solution presented in this Capability Package focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Contact NSA/IAD to request this document, or visit the SIPRNet CSFC site for information. The process for obtaining the risk assessment is available on the SIPRNet CSFC

website. The DAA shall be provided a copy of the NSA risk assessment for their consideration in approving the use of the solution.

11.3 REGISTRATION OF SOLUTIONS

All customers using this solution to protect information on National Security Systems shall register their solution with NSA. This registration will allow NSA to track where Multi-Site VPN solutions are instantiated and to provide DAAs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components approved for those solutions. The process for registering solutions will be provided on the IAD/CSFC websites on the Internet at www.nsa.gov/csfc and on SIPRNet.

12. TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure that they have properly configured the solution. These tests shall also be used to provide evidence to the DAA regarding compliance of the solution with this Capability Package.

Note that the details of the procedures are left up to the final developer of the test plan.

12.1 PRODUCT SELECTION

This section contains a procedure to verify that the Inner and Outer VPN devices were selected to ensure independence in several important features.

Requirements being tested: PS1, PS2, PS3, PS4

Procedure Description:

1) For each VPN device, perform the following:

    a) Inspect that the Inner and Outer VPN devices came from different manufactures. (PS1)

    b) Inspect that the Inner and Outer VPN devices are running on separate hardware platforms. (PS2)

    c) Inspect that the Inner and Outer VPN devices are running differing Operating Systems. (PS3)

    d) Inspect that the Outer VPN device is a hardware VPN device. (PS4)

Expected Result:

The results of the inspection should reveal that the VPN devices conform to the Multi-Site VPN CP; results are pass/fail.

12.2 PHYSICAL LAYOUT OF SOLUTION

This section contains a procedure to create an accurate record of the physical components composing the Multi-Site VPN solution (including workstations, VPN devices, CA, and wiring). The test will also ensure that the physical implementation of the Multi-Site VPN solution matches one of the architectures given in the Multi-Site VPN Capability Package.

Requirements being tested: CR6, TR3

Procedure Description:

1) Record all physical connections between the components in the Multi-Site VPN solution, including interfaces used on the VPN devices, connections used on workstations, and wiring. (TR3)

2) Compare this record with the architectures given in the Multi-Site VPN Capability Package and ensure what is implemented matches one of the architectures. (TR3)

3) Ensure that there are no wires connected to the solution that are not included in this Capability Package, which may allow for traffic to leave the Red or Gray network in a manner that does not go through the Multi-Site VPN solution (or an NSA-certified IP encryptor). (CR6)

Expected Result:

For Step 2, the record compiled in Step 1 should match either the Central Management or Multiple Independent Site architecture given in this Capability Package. For Step 3, there should be no extraneous wiring allowing data to leave the Red or Gray networks besides through the Multi-Site VPN solution (or an NSA-certified IP encryptor).

12.3 VPN DEVICE CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all the VPN devices in the Multi-Site VPN solution follow the requirements given in this Capability Package.

Requirements being tested: CR1 through CR11, IR1, IR2, OR1, OR2, RA1, RA2, KM7, KM9, PF2

Procedure Description:

1) For each VPN device in the solution, perform the following:

    a) Obtain the current configuration for the VPN device.

b) Verify that a device certificate from a CA included in the Multi-Site VPN solution is listed in the configuration for authentication. Also ensure the corresponding CA signing certificate and certificate revocation information are on the VPN device. (CR5)

c) Verify that the requirements CR2 through CR4, CR6 through CR11, and PF2 are configured properly.

2) For each Inner VPN device in the solution, use the configuration from 1a and perform the following:

a) Verify that the cryptographic algorithms, key sizes, and SA timeframes match what is given in Table 2 and IR1. (CR1, IR1)

b) Verify that IR2 has been configured.

c) Verify that all CA signing certificates used in the solution are from Inner tunnel CAs. (KM7)

3) For each Outer VPN device in the solution, use the configuration from 1a and perform the following.

a) Verify that the cryptographic algorithms, key sizes, and SA timeframes match what is given in Table 2 and OR1. (CR1, OR1)

b) Verify that OR2 has been configured.

c) Verify that all CA signing certificates used in the solution are from Outer tunnel CAs. (KM9)

4) For each device that administers a VPN device in the Multi-Site VPN solution, verify that requirements RA1 and RA2 are configured properly.

Expected Result:

For Steps 1-3, all VPN devices should be configured properly based upon the requirements in Section 8. For Step 4, all VPN device administration devices should be configured properly based upon the requirements of Section 8.6 of this Capability Package.

12.4 CA CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all of the CAs used within the Multi-Site VPN solution follow the requirements given in this Capability Package.

Requirements being tested: KM1 through KM6, KM8, KM10 through KM17

Procedure Description:

1) Verify that requirements KM1, KM2, and KM4 are met by both CAs.

2) Verify that the Inner tunnel CA is operating under a CPS. (KM3)

3) Verify that the Inner tunnel CA meets requirements KM5 and KM6.

4) Verify that the Outer tunnel CA has both a CP and CPS that it operates under. (KM3, KM8)

5) Verify that requirements KM10 through KM16 are met by the Outer Tunnel CA.

6) Verify that the VPN devices were keyed in a manner consistent with KM17. Ensure that there is certificate revocation information and CA signing certificate on each VPN device. Verify that there is a procedure in place for rekeying the VPN devices remotely.

Expected Result:

For Steps 1-6, all VPN devices should meet the requirements being tested from Section 8.8 of this Capability Package.

12.5 VPN DEVICE ADMINISTRATION

This section contains a procedure for ensuring that the Security Administrator can log directly into all VPN devices that they are administering using their credentials and that they cannot log into any VPN device with default username and passwords. In addition, this test ensures that the Security Administrator can successfully administer all VPN devices using the method determined in the implementation of the Multi-Site VPN solution.

Requirements being tested: CR3, TR2, AU1

Procedure Description:

1) Connect the appropriate VPN device administration workstation directly to each VPN device using a console cable. (CR3)

   a) Attempt to log into the VPN device using the default user name and password for the VPN device. Verify that a log file is created that indicates a failure to authenticate. (AU1)

   b) Attempt to log into the VPN device using a valid user name and password (this user name and password may be specifically created for testing and should be removed or changed prior to the solution going live). Verify that a log file is created that indicates a successful authentication. (AU1)

2) Log into each VPN device using the procedures determined in the customer's specific implementation of the solution. This includes using the appropriate protocols as detailed in RA1. (TR2)

   a) Obtain the VPN device configuration from the VPN device.

   b) Create a new entry for the access control list.

   c) Obtain again the VPN device configuration.

   d) Remove the entry created in b) from the access control list.

Expected Result:

In Step 1a, the default user name and password should be denied access to the VPN device. In Step 1b, the valid user name and password should allow the tester access to the VPN device. In Step 2, the procedures should allow access to the VPN device, and the change made in 2b should be found as the only difference between the device configurations in 2a and 2c.

12.6 SOLUTION FUNCTIONALITY

This section contains a procedure for ensuring that end user data traverses the solution to end users on Red networks at all other sites in the solution.

Requirements being tested: TR1

Procedure Description:

1) Log onto the User machine on the Red network at one site in the solution (call it Site A).

2) Complete the following steps to establish the double tunnel to a red User machine at each other site in the solution. (TR1)

   a) Determine the IP address for the red User machine at the other site.

   b) From a command window on the User machine at Site A, type "ping <ip address>". Note that in many cases, the standard timeout for the ping request will be less than the time needed to establish the double tunnel. In that case, you can change the default timeout using the following command "ping –W 7 <ip address>," which would give a default timeout of 7 seconds. Note that if ping is disabled at an endpoint, an alternate connection protocol may be used to ensure connectivity.

3) Repeat Steps 1 and 2 for each of the remaining sites in the solution.

Expected Result:

All ping commands will successfully receive packets of data from each site pinged. In cases where the results of the ping command are always "Request Timed Out", that indicates a problem in the tunnels between those two sites. Additional diagnosis will be required to determine the cause of that lack of connectivity.

12.7 APPROPRIATE PACKETS TRAVERSING THE SOLUTION

This section contains a procedure for ensuring that data traversing the Gray and Black networks is protected via encryption and that no plaintext data is seen from the sites. This procedure includes verification that data traveling between the Inner and Outer VPN devices is limited to ESP and UDP. These tests also ensure static IP address filters on the VPN devices are handling packets appropriately based on IP address.

Requirements being tested: PF1, PF3

Procedure Description:

1) Once the solution is configured as defined in this Capability Package, set up a packet analyzer on the network and begin capturing traffic crossing the VPN devices' interfaces. During the captures, regular actions from each site should be performed so that traffic simulates expected usage of the solution.

    a) For traffic at the external interface of the Outer VPN: (PF1)

        i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN devices shall be encrypted. Verify that no plaintext information is visible in the data portion of these packets.

        ii) Verify that plaintext data seen in the data portion of packets at this interface has a source address that differs from any VPN device in the solution. This is Black network traffic that does not originate from the VPN solution.

    b) For traffic at the external interface of the Inner VPN: (PF1)

        i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN devices shall be encrypted. Verify that no plaintext information is visible in the data portion of these packets. (Any plaintext data seen in the data portion at this interface will indicate a problem.)

        ii) Identify the packet types seen in the capture. The only traffic at this interface will be ESP or UDP.

    c) For traffic at the internal interface from the Gray data network of the Outer VPN: (PF1)

i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN devices shall be encrypted. Verify that no plaintext information is visible in the data portion of these packets. (Any plaintext data seen in the data portion at this interface will indicate a problem.)

ii) Identify the packet types seen in the capture. The only traffic at this interface will be ESP or UDP.

d) For traffic at the internal interface from the Gray management network of the Outer VPN: (PF3)

i) Given correct configuration, all data seen in the captured packets that originate at one of the solutions' VPN devices shall be encrypted. Verify that no plaintext information is visible in the data portion of these packets. (Some information such as Audit may be in plaintext here depending on your configuration. All security critical information should be encrypted.)

ii) Identify the packet types seen in the capture. The only traffic at this interface will be that necessary to manage the Outer VPN devices.

2) When testing is complete, remove packet analyzer from the network.

Expected Result:

Any traffic on the Gray data network will be encrypted and filtered so that only ESP and UDP packets are allowed provided that the Multi-Site VPN solution is configured properly. The traffic at the external interface of the Outer VPN device that originates from this solution will also be encrypted and limited to ESP and UDP. All tests above involve utilization of a packet analyzer and inspection of packets captured. All results are expected to be pass/fail.

12.8 SECURITY ASSOCIATION LIFETIMES

This section contains a procedure for ensuring SAs expire as given in IR1 and OR1: IKE SA lifetime is 24 hours; ESP SA lifetime is 8 hours.

Requirements being tested: IR1, OR1

Procedure Description:

1) Identify the Security Parameter Index (SPI) for the established SAs for each VPN tunnel. Note: SPIs are used as a connection identifier; these are unique identifiers of an SA.

a) SPIs are sent in the header of an IKE or ESP message; ESP messages contain only the recipient's SPI; IKE messages include both the sender and recipient SPIs.

b) Some VPN devices allow an administrator to query for current/active SAs. This query will provide information regarding the endpoints and the unique identifier for the SA.

2) Allow the network to run, as usual, for just over 8 hours.

   a) Check that the SPIs for the ESP SAs have changed (from those seen in Step 1).

3) Allow the network to run, as usual, for just over 24 hours (16 hours after Step 2).

   a) Check that the SPIs for the IKE SAs have changed (from those seen in Step 1).

   b) Alternatively, if the connection has been inactive for some time, the connection may be terminated; this would result in the IKE SA being removed. This is also an acceptable action at lifetime expiration.

Expected Result:

Configured SA lifetimes shall be maintained. When rekeyed (or reinitialized), a new SA identifier is created; verification of a new ID indicates the SA/key lifetime is upheld. All results are expected to be pass/fail.

12.9 USE OF CERTIFICATES FROM UNTRUSTED CAS

This section contains a procedure to ensure that only certificates from trusted CAs are accepted.

Requirements being tested: KM7, KM9, AU1

Procedure Description:

1) Ensure that the solution is in its default setting and that the VPN connections are established when the proper certificates (see Section 5) are used to authenticate the VPN devices.

2) Install alternate certificates on the VPN devices, not generated by the approved CAs, and configure the solution so that one of the VPN devices uses this certificate for authentication. (Note that an alternate way to perform this testing is to install a certificate without its CA Signing Certificate, so that the trust anchor is not identifiable.)

   a) Verify that an entry to the Audit log has been created due to certificate loading. (AU1)

   b) Start the VPN connections using the new configuration.

   c) Verify that the connection is not successful; end-to-end communication is not provided because the devices will fail to authenticate. Verify that failures are logged in the audit data.

d) Repeat this test for each VPN device; only 1 VPN device should offer the non-approved CA certificate per connection.

3) When testing is complete, remove the alternate certificates and return the configuration to its proper settings. Verify that an entry to the Audit log has been created due to certificate deletion. (AU1)

Expected Result:

Authentication will not occur when the VPN devices cannot identify the trust anchor of the certificates, provided the solution is configured correctly. All results are expected to be pass/fail.

12.10 CONFIGURATION CHANGE DETECTION

This section contains a procedure to ensure that changes made to any of the VPN device configurations are detected by the Configuration Change Detection tool.

Requirements being tested: CM1, CM2, AU1

Procedure Description:

1) The following steps shall be done for each of the VPN devices within the solution.

   a) Log into the VPN device.

   b) Compare the current version of the VPN device configuration with the stored baseline and ensure that the current version matches the stored configuration. (CM1)

   c) Make a change to the configuration, preferably something that is not fundamental to the security of the Multi-Site VPN solution.

   d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from c) are recorded. (AU1, CM2)

Expected Result:

The baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change.

12.11 AUDIT

This section contains procedures for ensuring that audit events are detected, that the proper information is logged for each event, and that there is a procedure detailed in the CPS documentation for auditing each CA device.

Requirements being tested: AU1, AU2, AU3, CR10

Procedure Description:

1) Examples for testing the ability of each VPN device to audit and log audit events specified in AU1 are given below. Additional tests for the events in AU1 are included in appropriate tests in other areas within this testing section. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with AU3.

    a) All actions performed by a user with super privileges (auditor, administrator, etc.) and any escalation of user privileges.

        i) Log in as an administrator to the VPN device.

        ii) Perform a variety of administrator actions on the VPN device.

        iii) Verify that a log entry was created for each action taken in Step ii that required super-user privileges.

        iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.

        v) Repeat the above with the Auditor role.

    b) Changes to time

        i) Log in as an administrator to the VPN device.

        ii) Modify the system time on the VPN device by at least 1 hour.

        iii) Verify that a log entry was created due to the change in system time.

        iv) Revert the system time back to the accurate time of day.

    c) All built-in self-test results, which may indicate failures in cryptographic functionality

        i) Completely power down the VPN device.

        ii) Power the VPN device back up so that the automatic self-tests are run.

        iii) Verify that a log entry was created due to running the self-tests.

2) Verify that the VPN device's loopback address is used as the source address for all audit log entries. (CR10)

3) Verify that there is a procedure detailed in the CPS documentation for auditing each CA device within the solution. (AU2).

Expected Result:

For Step 1, all occurrences of auditable events given in AU1 should generate an entry in the audit log including all the information given in AU3. For Step 2, the source address should be the VPN device's loopback address. For Step 3, there should be a procedure for auditing the CA devices in the solution that is outlined in the CPS document.

12.12 POLICY

This section contains a procedure to ensure that there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the Multi-Site VPN solution. It also ensures that the personnel in place to manage and administer this solution follow the guidelines given in the Capability Package.

Requirements being tested: P1 through P17

Procedure Description:

1) Verify that the procedures given in P1, P2, P3, P7, P8, P9, P10, P11, and P12 were/are followed and/or are currently in place.

2) Verify that the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (P4)

3) Verify that the solution owner and DAA are aware that a compliance audit will be conducted every 3 years. (P5)

4) Verify that the solution owner and DAA are aware that when new versions of the Multi-Site VPN Capability Package are published by NSA, they will have 6 months to move into compliance with this new version. (P5)

5) Verify that the solution owner and DAA are aware that they shall provide updated solution information to NSA on a yearly basis. (P6)

6) Verify that the personnel requirements given in P13 through P17 are met by the personnel supporting this implementation of the Multi-Site VPN solution.

Expected Result:

For 1-6, all of these policies and procedures have been followed or are in place.

APPENDIX A. GLOSSARY OF TERMS

Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance – A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. Certification by designated technical personnel of the extent to which design and implementation of the system meet specified technical requirement for achieving adequate data security.

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Audit log – A chronological record of the audit events that have been deemed critical to security. The audit log can be used to identify potentially malicious activity that may further identify the source of an attack, as well as potential vulnerabilities where additional countermeasures or corrective action are required.

Availability – Assurance that the system and its associated assets are accessible and protected against denial or service attacks, as well as available when the user needs them and in the form needed by the user.

Black box testing – Testing the functionality of a component of the solution, such that testing is limited to the subset of functionality that is available from the external interfaces of the box during its normal operational configuration without any additional privileges (such as given to the Security Administrator or Auditor).

Capability Package – The set of guidance provided by NSA that describes recommended approaches to composing COTS devices to protect classified information for a particular class of security problem. This package will point to potential products that can be utilized as part of this solution.

Certification – The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements.

Certification and Accreditation (C&A) – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating

as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

Certificate Authority (CA) – An authority trusted by one or more users to create and assign certificates. [ISO9594-8]

Certificate Policy (CP) – A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Confidentiality – Assurance that the data stored in, processed by, or transmitted by the system are protected against unauthorized disclosure and confidence in that only the appropriate set of individuals or organizations would be provided the information.

Designated Approving Authority (DAA) – The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSS Instruction 4009]

Edge Device – Another term for VPN device as described in this Capability Package, frequently used in Key Management requirements.

External Interface – The interface on a VPN device that connects to the outer network (i.e., the Gray network on the Inner VPN device or the Black network on the Outer VPN device).

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

Gray Box testing – The ability to test functionality within a component of the solution, such that full management privileges are granted (i.e., knowing passwords for security administrator and Auditor and access to the capabilities associated with those privileges). In addition, the use of any and all testing equipment and/or testing software used inside and outside the developed solution is available.

Internal Interface – The interface on a VPN device that connects to the inner network (i.e., the Gray network on the Outer VPN device or the Red network on the Inner VPN device).

May – This word means that an item is truly optional. Some customers may choose to include the item in their Multi-Site VPN solution while others may not.

Protection Profile – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates.

Shall – This word means that the definition is an absolute requirement of this Capability Package.

Should – This word means that there may exist valid reasons in particular circumstances to ignore a particular requirement in this Capability Package, but the full implications must be understood and carefully weighed before choosing a different course.

APPENDIX B. ACRONYMS

ACL	Access Control List
ARP	Address Resolution Protocol
C&A	Certification and Accreditation
CA	Certificate Authority
CAA	Certificate Authority Administrator
CCI	Controlled Cryptographic Item
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CSFC	Commercial Solutions for Classified
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DoS	Denial of Service
FIPS	Federal Information Processing Standards
GOTS	Government Off-the-Shelf
HAIPE	High Assurance Internet Protocol Encryption
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alerts
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IPsec	Internet Protocol Security
MPLS	Multi-Protocol Label Switching
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NSS	National Security Systems
OID	Object Identifier
OS	Operating System
PKI	Public Key Infrastructure
S3	Secure sharing suite
SA	Security Association
SP	Service Packs
T&E	Test and Evaluation
TLS	Transport Layer Security
VPN	Virtual Private Network

APPENDIX C. REFERENCES

CNSS 4009	*CNSS 4009, National Information Assurance (IA) Glossary Committee for National Security Systems www.cnss.gov/Assets/pdf/cnssi_4009.pdf*	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*	May 2001
FIPS 180	*Federal Information Processing Standard 180-3, Secure Hash Standard (SHS)*	October 2008
FIPS 186	*Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)*	June 2009
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf*	March 2006
IPsec VPN Client PP	*IPsec VPN Client Protection Profile. www.niap.ccevs.org/pp*	January 2012
NSA Suite B	*NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml*	November 2010
RFC 2409	*IETF RFC 2409 The Internet Key Exchange (IKE).* D. Harkins and D. Carrel.	November 1998
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force http://www.ietf.org/rfc/rfc3647.txt*	November 2003

RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol.* T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol.* T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol.* T. Ylonen and C. Lonvick.	January 2006
RFC 4302	*IETF RFC 4302 IP Authentication Header.* S. Kent	December 2005
RFC 4303	*IETF RFC 4303 IP Encapsulating Security Payload.* S. Kent	December 2005
RFC 4307	*IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).* J. Schiller	December 2005
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec.* P. Hoffman	December 2005
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.* T. Dierks and E. Rescorla.	August 2008
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2).* C. Kaufman, et. al.	September 2010
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec.* L. Law and J. Solinas.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS).* M. Salter, et.al.	January 2012
SP 800-56A	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.* E. Barker, D. Johnson, and M. Smid	March 2007
SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.* E. Barker, et. al.	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion.* L. Chen.	November 2011
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths.* E. Barker.	January 2011