NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Enterprise Gray (EG) Implementation Requirements Annex 1.2.0

Version 1.2.0
27 March 2026

CHANGE HISTORY

Title	Version	Date	Change Summary
Enterprise Gray Implementation Requirements Annex	1.2.0	27 March 2026	• Added Purpose and Use Section • Added Legal Disclaimer Section • Added Overview Section • Reformatted document for clarity • Added Objective CNSA 2.0 Requirements
Enterprise Gray Implementation Requirements Annex	1.1.1	23 January 2023	• Corrected EG-DR-6 to have the alternative requirement of EG-DR-5
Enterprise Gray Implementation Requirements Annex	1.1	August 2021	• Product Selection Requirements added for the Gray Encryption Component and Gray Firewall • Updated reference from CSfC Key Management Requirements Annex to *CSfC Symmetric Key Management Requirements Annex* and *CSfC Key Management Requirements Annex* • Clarified use of PSKs within dynamic routing • Updated format
Enterprise Gray Implementation Requirements Annex	1.0	2 April 2019	• Reorganized and added new figures for clarity. • Added Capability Package (CP) requirements to the multiple capability package sections. • Added sections clearly describing the Gray Management and Gray Data Virtual Private Network (VPN) tunnels. • Added sections expanding dynamic routing and Virtual Routing and Forwarding (VRF). • Added a general Enterprise Gray (EG) requirements section and re-ordered the EG requirements. • Added additional requirements to Centralized Management Requirements and Scalability Requirements.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency's (NSA's) Cybersecurity Directorate (CSD) uses a series of Capability Packages (CP) to provide configurations that allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CPs are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Integrators.

Cybersecurity Solutions delivers the Enterprise Gray (EG) Implementation Requirements Annex as an enhancement to the CSfC CPs to address increasing demands from customers who desire to implement a CSfC deployment with one or more of the following characteristics which are referred to as pylons in this document:

- Ability to implement multiple Capability Packages (CPs) simultaneously
- Centralized management
- Enhanced scalability
- Enhanced site survivability

This *EG Implementation Requirements Annex* introduces guidance to help CSfC customers sustainably expand their networks across large geographic distances by leveraging their existing infrastructure and services. This annex references the CSfC *Campus Wireless Area Network (WLAN), Mobile Access (MA),* and *Multi-Site Connectivity (MSC)* Data-in-Transit CPs using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) suite, protect classified data using layers of Commercial-off-the-Shelf products. The *EG Implementation Requirements Annex, Version 1.2.0*, incorporates lessons learned from proof-of-concept demonstrations built by the National Security Agency (NSA) Information System Security Engineers (ISSEs) in a CSfC network development environment.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a NIAP-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process to determine whether such a modification will affect the component's certification.

In the case of a modification to a component, the NSA's CSfC Program Management Office (PMO) requires a statement from NIAP that the modification does not alter the certification, or the security of the component. Modifications that trigger the revalidation process include, but are not limited to, configuring the component in a manner different from its NIAP-validated configuration and configuration and modifying the Original Equipment Manufacturer's code (to include digitally signing the code).

2 PURPOSE AND USE

This Annex provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List to develop an EG solution and then properly configure those products to achieve a level of assurance sufficient for a solution used to protect classified Data-in-Transit (DIT). Throughout this document, requirements imposed on the EG implementation are identified by a label consisting of the prefix "EG," a two-letter category, and a sequence number (e.g., EG-GR-11). To successfully implement a solution based on this Annex, all Threshold (T) requirements, or the corresponding Objective (O) requirements, must be implemented as described in Section 10.1.

Customers who want to use this Annex must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Capability-Packages/).

The *CSfC EG Annex Version 1.2.0*, when approved by the Deputy National Manager (D/NM) for National Security Systems (NSS), will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required to account for technology development, new security issues, and new use cases. Solutions designed using this Annex must be registered with NSA/CSD. Once registered, a signed CSD Approval Letter will be sent validating that the EG solution is registered as a CSfC solution validated to meet the requirements of the latest EG Annex and is approved to protect classified information. Any solution designed according to this Annex may be used for one year and must then be revalidated against the most current published version of this Annex. Top Secret Solutions will be considered on a case-by-case basis. Customers are encouraged to engage their Client Advocate or the CSfC Program Management Office team early in the process to ensure the solutions are properly scoped, vetted, and that the customers have an understanding of risks and available mitigations.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/CSS Client Advocate and the Enterprise Gray Annex maintenance team at CSFC_EG_Team@nsa.gov. EG solutions must comply with the Committee on National Security Systems (CNSS) policies and instructions. Any conflicts identified between this Annex and NSS or local policy should be provided to the EG Maintenance team. If a conflict arises between NSS, local policy, and this Annex, NSS and/or local policy should be followed until a time when the EG Maintenance team rectifies the conflict.

3 LEGAL DISCLAIMER

This Annex is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Annex, even if advised of the possibility of such damage.

The user of this Annex agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees,

court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Annex is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

4 DESCRIPTION OF ENTERPRISE GRAY PYLONS

The Enterprise Gray Annex is a series of capabilities which can be implemented to augment the CSfC Data-in-Transit (DiT) solutions. These capabilities are referred to as pylons within this document. The implementation of these pylons is optional within CSfC solutions but allow for the following capabilities to be added to the CSfC solutions.

4.1 MULTIPLE CPS

The first of the pylons allows for the different DiT solutions to coexist and reuse the same physical equipment. An example of this is for the Outer Encryption Component to act as both a Outer IPsec VPN for Mobile Access (MA) CP and act as the WLAN Access System for Campus WLAN CP at the same time. For more information on this capability see Section 6.

4.2 CENTRALIZED MANAGEMENT

The second of these pylons is Centralized Management that allows for the individual Gray Networks of desperate CSfC sites to be connected together to form the Enterprise Gray Networks. The Enterprise Gray Network is made up of two logically separate networks: the Gray Management Network and the Gray Data Network. Connecting the Gray Management Networks together allows for the sharing of the management resources and allows for centralized management of the Gray Components. Connecting the Gray Data Networks allows for the sharing of Gray Data Services such as DNS and allows for access of Inner Encryption Components hosted at other sites. The Enterprise Gray Network is protected by two layers of encryption with the first layer being provided by the Outer Encryption Component and the second layer is provided by a Gray Encryption Component. For more information on this pylon see Section 7.

4.3 SCALABILITY

The third capability is Scalability that allows for the use of dynamic routing to be used on the Gray Encryption Component. Centralized Management is required for this pylon to be deployed within a CSfC solution. The use of dynamic routing is limited to only the Gray Encryption Component and additional mitigations are required for the use of dynamic routing. For more information see Section 8.

4.4 SITE SURVIVABILITY

Authorizing Officials (AOs) implementing Enterprise Gray Solution guidance may deem site survivability optional for some remote sites depending on the mission of the organization. If site survivability is not a requirement and there is a loss of connectivity, then the remote site will fail closed. In the event of loss

of connectivity, Campus WLAN, MA, and MSC solutions will not have access to offsite classified resources. For more information see Section 9.

5 ENTERPRISE GRAY COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black Network are protected by at least two layers of encryption, implemented using an Outer Internet Protocol security (IPsec) VPN tunnel and an Inner layer of IPsec, TLS, or SRTP encryption. Mandatory aspects of the solution infrastructure also include administration workstations, IDS/IPS, SIEM, firewalls, and CAs for key management using PKI. Each infrastructure component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Components List and configured per NIAP configuration guidance in accordance with the Product Selection requirements of this Annex. This section also provides details on additional components that can be added to the solution to help reduce the overall risk. However, where indicated in the text, these are not considered mandatory components for the security of the solution; therefore, this Annex does not place configuration requirements on those optional components.

5.1 OUTER FIREWALL

The Outer Firewall is located at the edge of the MA or MSC solution infrastructure and connected to the Black Transport Network. The external interface of the Outer Firewall only permits IPsec, Internet Key Exchange (IKE), Media Access Control Security (MACsec), and/or Encapsulating Security Payload (ESP) traffic with a destination address of the Outer VPN Gateway. The internal interface of the Outer Firewall only permits IPsec, MACsec, IKE, and ESP traffic with a source address of the Outer VPN Gateway and any necessary control plane traffic. The Outer Firewall, selected from the CSfC Components List, must be physically separate from the Outer VPN Gateway. For more information on the implementation and requirements of the Outer Firewall see *Mobile Access CP* or *Multi-Site Connectivity CP*.

5.2 OUTER ENCRYPTION COMPONENT

The Outer Encryption Component, located between the Outer Firewall, if present, and Gray Firewall, is capable of establishing encrypted tunnels using WPA3, IPsec, or MACsec. The Component serves as a peer gateway to other Outer Encryption Components of CSfC Solutions while also providing device authentication and ensuring the confidentiality and integrity of data transiting untrusted networks. If the Outer Encryption Component is used for Campus WLAN, then it is considered part of the WLAN Access System, which is composed of Access Point(s) and a WLAN Controller capable of initiating and terminating multiple cryptographic tunnels to and from numerous Access Points. For Campus WLAN Solutions, it is important to note that depending on the vendor, the Black/Gray boundary may either be at the Access Point or the WLAN Controller. The Outer Encryption Component also provides the outer layer of encryption protecting Gray and Red Services as they traverse untrusted networks. The Outer Encryption Component must not perform dynamic routing. The Outer Encryption Component reduces the risk of exposure of information in transit across a Black Network, since the data is placed in a secure tunnel that provides an authenticated and encrypted path between two or more sites. The Outer Encryption Component must be an IPsec VPN Gateway, WLAN Access System or MACsec Device selected

from the CSfC Components List and must be physically separate component. The Outer Encryption Component is a key component in the Centralized Management capability and thus additional requirements are levied on the Outer Encryption Component when this capability is used for more information see Section 7. For more information on the implementation and requirements of the Outer Encryption Component see *Mobile Access CP, Campus WLAN CP* or *Multi-Site Connectivity CP.*

If the Outer Encryption Component is considered a shared outer device, it also has the responsibility of filtering traffic on its Gray Network interface to prohibit Inner Encryption Components of different levels of classification from sending traffic between different levels.

5.3 GRAY FIREWALL

The Gray Firewall is located between the Outer Encryption Component and Inner encryption components. Within the *Mobile Access CP* and *Campus WLAN CP* the Gray Firewall filters and restricts EUD traffic to authorized Gray Services such as DNS and the Inner Encryption Component. As shown in Figure 1, the Gray Firewall must filter all traffic routed to two or more Inner Encryption Components of different classification ensuring that the separate Inner Encryption Component cannot communicate with each other. The Gray Firewall is a Firewall selected from the CSfC Components List, must be physically separate from the Outer VPN Gateway and Inner Encryption Components. The Gray Firewall may act as the Gray Encryption Component for the Centralized Management capability for more detail on this capability refer to Section 7. For more information on the implementation and requirements of the Gray Firewall see *Mobile Access CP, Campus WLAN CP* or *Multi-Site Connectivity CP*.

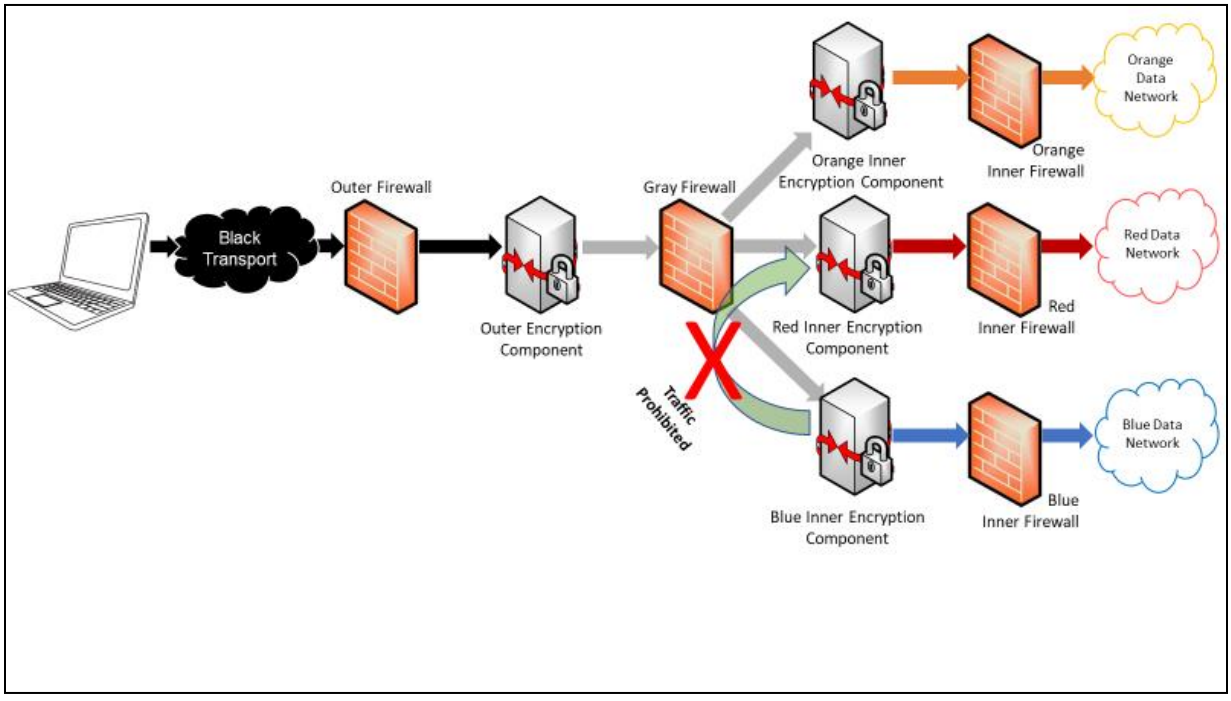

Figure 1. Multiple Inner Classification Prohibited Traffic

5.4 GRAY ADMINISTRATION WORKSTATION

The Gray Administration workstation maintains, monitors, and controls all security functionality of the Gray Network Components across one or more CSfC Solutions. This workstation must only be used for logging, configuration, and management of Gray Network Components. The Gray Administration workstation must not be used to provision solution components, or as an enrollment or registration authority for a CA. The Gray Administration workstation must not be used to administer the Inner VPN Gateway or any Red Management Services. The Gray Administration workstation may be virtualized as described within the *Multi-Site Connectivity CP* and must be physically protected as if classified to the same level as the highest classification Red Network it supports.

5.5 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT

The Gray Security Information and Event Management (SIEM) server collects and analyzes log data from all Gray Components. Log data must be encrypted between the originating components and the Gray SIEM with Secure Shell version 2 (SSHv2), TLS, or IPsec to maintain confidentiality and integrity of this data. For more information and requirements for deploying continuous monitoring see *CSfC Continuous Monitoring Requirements Annex*.

5.6 GRAY AUTHENTICATION SERVERS

Two separate Gray authentication servers are required for Solution Networks. The authentication system used to connect EUDs and client devices must use a separate authentication system, different from the authentication system used for EG administrator workstation authentication.

The authentication server for the EUDs must perform mutual authentication with EUDs by using the Outer Encryption Component as an Extensible Authentication Protocol (EAP) pass-through device. As shown in Figure 2, the Gray Management authentication server is also required for the centralized management of Gray Services between the Management Site and Remote Sites.

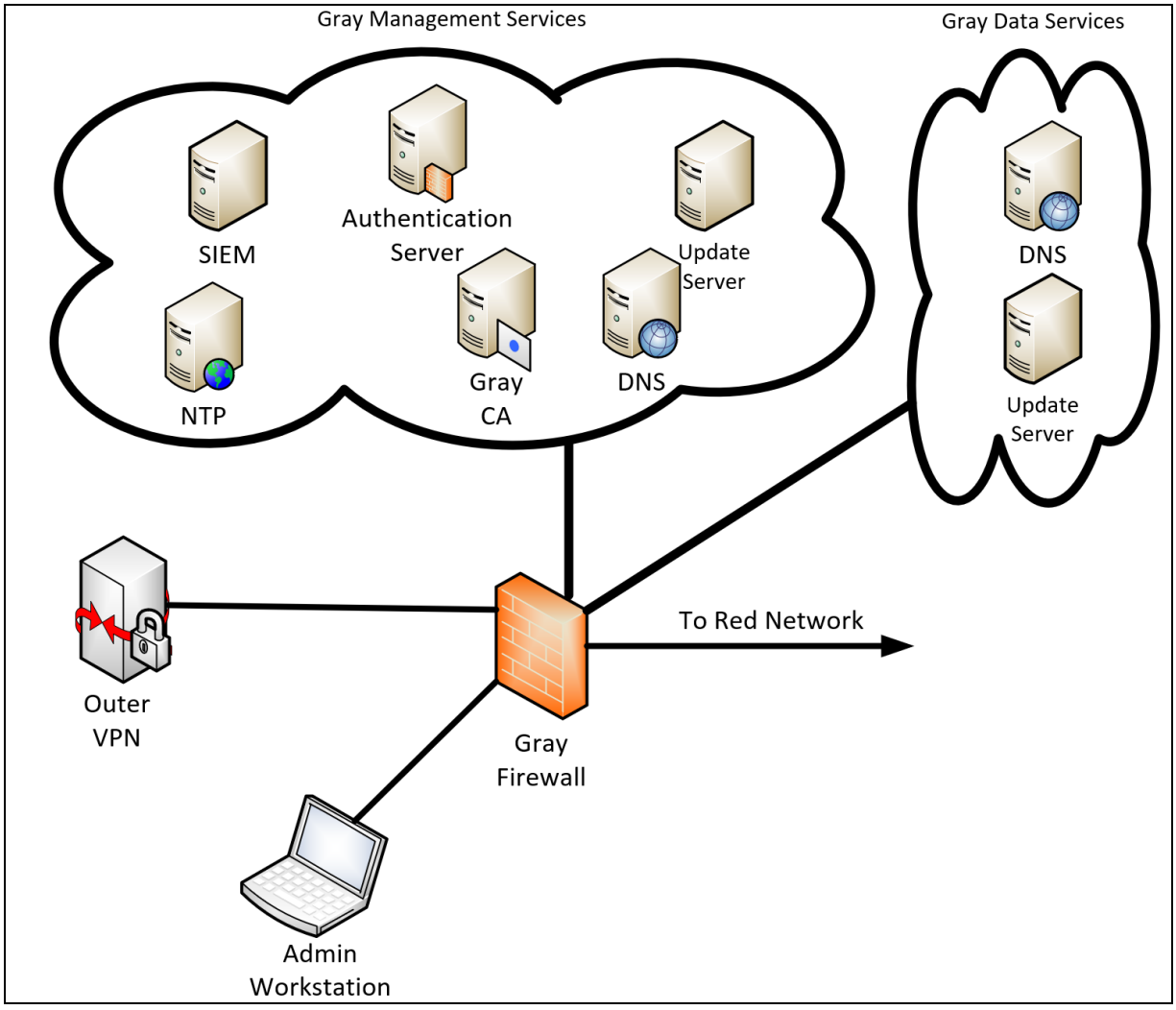

Figure 2. Gray Management and Data Services

5.7 GRAY DOMAIN NAME SYSTEM

The Gray Domain Name System (DNS) is a control plane service responsible for name resolution to Internet Protocol (IP) addresses within the Gray Network for both management and data. The DNS servers for the Data and Management Networks must be separate systems. The Gray Management DNS servers can be connected to each other in a hierarchical structure with the main site hosting the root (authoritative) DNS zone, which updates the other DNS servers throughout the EG Network. The use of Domain Name System Security (DNSSEC) is recommended to ensure the integrity of DNS query responses.

If static IP addresses are not used to connect to an Inner Encryption Component, the Data DNS is required to perform name resolution for both EUDs and site-to-site connection to ensure the correct Inner Encryption Component is connected. The Gray Data DNS server should not communicate with any other DNS servers and, therefore, must be an authoritative DNS repository.

5.8 GRAY NETWORK TIME PROTOCOL

Gray Network Time Protocol (NTP) being deployed within the Gray Management network performs all time synchronization, which is important for timestamps used for certificates and event logging within the Gray Network. NTP uses a hierarchical ranking of time sources for synchronization called strata. For example, stratum zero (0) devices are high-precision time sources such as atomic clocks. Stratum one (1) are computers that have been synchronized within microseconds to a directly connected stratum 0-time source. Stratum two (2) are computers synchronized and directly connected to a stratum 1-time source, and so on. NTPv3 is recommended to ensure that the time service of the Enterprise Gray network is Secure.

5.9 SOFTWARE AND FIRMWARE SIGNING

As part of the requirement laid out in NSM-10, the CSfC Program will be adding Software and Firmware Signing requirements for all components listed on the CSfC Components List. As of now this is an objective security feature but the implementation timeline for these requirements will be the same as the CNSA 2.0 timeline in CSfC. These timelines are subject to change depending on market acceptance, vendor and customer feedback for these new requirements.

There are three acceptable algorithms for software and firmware digital signatures, which are all included as part of the CNSA 2.0 cipher suites. These algorithms are enumerated within Table 1 and only one of the algorithms will be required to meet this requirement.

Table 1. CNSA 2.0 Algorithms for Software and Firmware Signing

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.
ML-DSA	Asymmetric algorithm for digital signatures	FIPS 204	Category 5 parameter, ML-DSA87.

6 MULTIPLE CAPABILITY PACKAGES

The CSfC EG Annex provides cost effective techniques to deploy all three Data-in-Transit CPs at the same time by using centralized certificate and Virtual Private Network (VPN) management. Selecting equipment with the ability to collapse into components for multi-use allows customers to deploy multiple CPs simultaneously. For instance, a customer might use their Outer Encryption Component as both the WLAN Access System as described in the *Campus WLAN CP* and the Outer VPN Gateway as allowed by the *Mobile Access CP*, provided the network device is on the CSfC components List to serve both functions. Note that the additional requirement for a multi-use Outer Encryption Component

within the MA, MSC, and WLAN CPs drastically reduces the number of potential Outer VPN Components that can be used and must be considered during design of the system. EG Solution Networks must be controlled and managed as classified and all Gray Network Components must be physically protected at the same level as the highest classification level of a connected Red Network Enclave. Each of these components are described in more detail in Section 5.

6.1 CAPABILITY PACKAGE REQUIREMENTS

The CSfC EG Annex allows for multiple CP instances to coexist on the same equipment. For such deployments the highest level of protection must be applied to the Solution Network(s). When using the same equipment for multiple CPs the most stringent security requirements throughout all the CPs must be used. Such as if a CSfC customer plans to combine WLAN and MA Solutions into a single EG Network, then a Black Firewall must be used outside of the Outer Encryption Component, as required by the MA CP. Figure 3 shows an example of a single EG Solution, designed around the requirements of the MA, MSC, and WLAN CPs, using the same equipment to secure two separate sites.

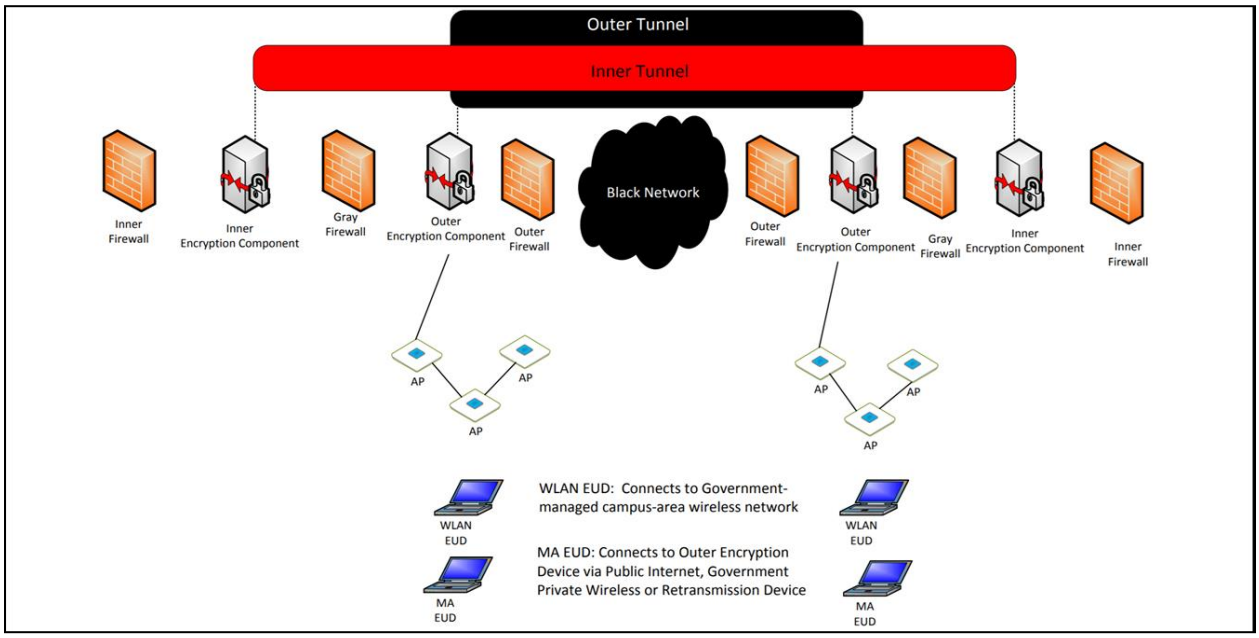

Figure 3. Deploying Multiple CPs Using the Same Components

All risks associated with the CPs being integrated together applies to the EG Solution and must be considered by the Authorizing Official (AO) for their decision on the acceptable amount of risk. Architecture changes may be used to aid in mitigating the risk of integrating CPs together. For example, customers may deploy logically separate MA and WLAN instances on the Outer Encryption Component, provided they use separate interfaces to connect to the Inner Encryption Component.

7 CENTRALIZED MANAGEMENT

The administration of components is key to providing centralized Gray Management Services. Although Gray Management Services are composed of several components, those described below have specific

roles essential to the security of the solution. Each component is accessible only through the Gray Firewall/Encryption Component and is physically protected as a classified device. Interconnecting two or more solutions using EG, allows flexibility in the placement of some components. EG allows the Gray Firewall to also serve as the Gray Encryption Component, and in doing so, extends the Gray Management and Gray Data Networks between multiple sites. This configuration allows for remote administration of Gray Management Services from a centralized location.

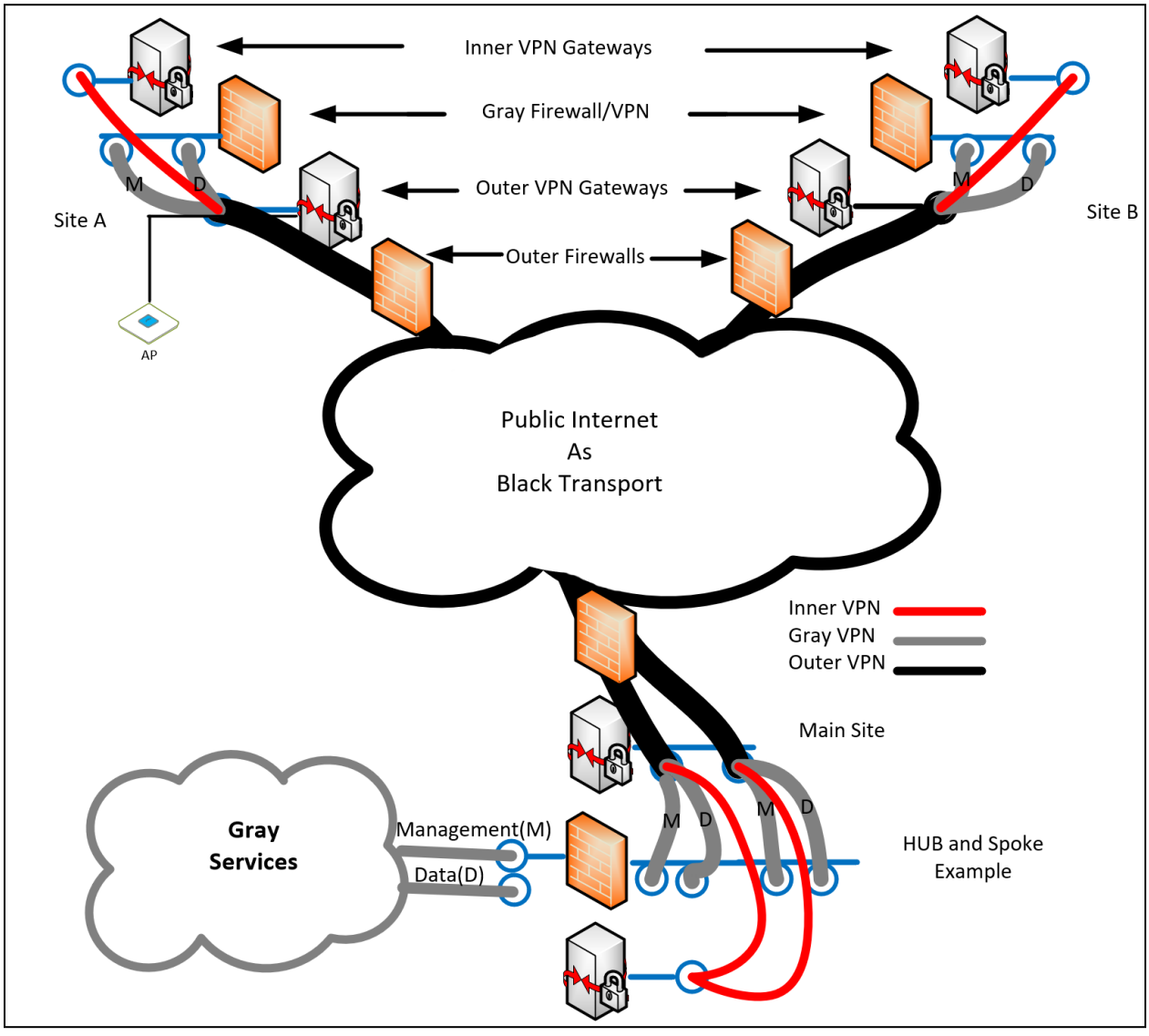

Figure 4. Two Sites ("A" and "B") Using Gray Services Hosted at a Main Site

Generally, the Gray Services area of a CSfC Solution is singly encrypted and under the control of the solution owner or a trusted third party; however, when extending Gray Services to another site over an untrusted network, two independent layers of encryption must be used to protect both Management and Data traffic. The Gray Firewall/Encryption Component at each site provides an inner layer of encryption and the Outer Encryption Component provides a second, outer layer of encryption to protect traffic between sites. As shown in Figure 4, a hypothetical Main Site's Gray Firewall/Encryption

Component can operate four VPN tunnels simultaneously: Management and Data tunnels to Site A, and Management and Data tunnels servicing Site B. The Management tunnels create a single Management plane for EG. The Data tunnels create a single Data plane for EG.

Both the Outer Encryption Component and Gray Firewall/Encryption Components must use digital certificates issued by the same Outer Certificate Authority (CA) for authentication; however, if the AO desires additional security they should create a separate CA or use Pre-Shared Key (PSK) authentication for the Gray Firewall/Encryption Components. For more information on the usage of certificates see *CSfC Key Management Requirements Annex* and for the usage of PSKs see *CSfC Symmetric Key Management Requirements Annex.* The implementing AO may require additional components for encryption separate from the Gray Firewall to reduce risk to the Solution Network(s). EG Solutions can connect the Gray Management Networks of different sites to each other, allowing for remote management, monitoring, and configuration of Gray Management Components. End User Devices (EUDs) are prohibited from connecting to the Gray Management Network to service the network as administration workstations.

7.1 OUTER ENCRYPTION COMPONENT

The Outer Encryption Component, located between the Outer Firewall, if present, and Gray Firewall, is capable of establishing encrypted tunnels using WPA3, IPsec, or MACsec. When the Centralized Management pylon is used the Outer Encryption Component must be configured to form a site-to-site tunnel with at least one other Outer Encryption Component at another site as described within *MSC CP*. This allows for the Outer Encryption Component to also provide the outer layer of encryption protecting Gray Data and Management tunnels as they traverse untrusted networks to the remote site.

7.1.1 CNSA 2.0 IPSEC

As part of the CNSA 2.0 migration, the VPN Gateways and VPN Clients will have to implement CNSA 2.0-compliant key establishment and digital signatures. As of now, this is an objective design feature but will be required in the future for the VPN Gateways and VPN Clients. The CNSA Suite 2.0 is relevant to the choice of cryptography employed in IPsec and especially affects the Internet Key Exchange Protocol Version 2 (IKEv2) key establishment construction, requiring support for several new RFCs. NSA has worked with industry to develop an implementation profile, CNSA Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile*).

The draft profile (*draft-guthrie-cnsa2-ipsec-profile*) specifies the use of the CNSA 2.0-compliant algorithms ML-KEM-1024 [FIPS203] for key establishment and ML-DSA-87 [FIPS204] for digital signatures within IPsec. It describes the use of RFCs that are required in order to support the large ML-KEM-1024 public key and ciphertext sizes, including:

- RFC 7383 IKEv2 Message Fragmentation
- RFC 9242 Intermediate Key Exchanges in IKEv2
- RFC 9370 Multiple Key Exchanges in IKEv2
- draft-ietf-ipsecme-ikev2-pqc-auth Signature Authentication in the IKEv2 using PQC

- RFC 9881 Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

- draft-ietf-ipsecme-ikev2-mlkem Post-quantum Key Exchange with ML-KEM in the IKEv2

These additional RFCs facilitate the use of ML-KEM-1024 without causing IP-level fragmentation, which can cause operational challenges and prevent the establishment of a connection. In particular, if ML-KEM-1024 were used in the initial IKEv2 Security Association (SA) key exchange (IKE_SA_INIT), the sizes of its public key and ciphertext would cause the initiator and responder messages to exceed the typical path Maximum Transmission Unit (MTU) and necessitate IP-level fragmentation. In order to prevent this issue, the solution leveraged first performs a CNSA 1.0-compliant key establishment that does not exceed PMTU and subsequently performs an additional key establishment using a newly-defined exchange called Intermediate Exchange (IKE_INTERMEDIATE). IKE_INTERMEDIATE exchanges can circumvent IP-level fragmentation by using IKEv2-level fragmentation, which does not incur the same operational issues. The specifications of which this solution is comprised work as follows:

RFC 7383 IKEv2 Fragmentation: Describes a way to prevent IP fragmentation of large encrypted IKEv2 messages by fragmenting at the IKEv2 layer. This allows IKEv2 messages to traverse network devices that do not allow IP fragments to pass through.

RFC 9242 Intermediate Key Exchanges: These IKE_INTERMEDIATE exchanges can be used for transferring large amounts of data in the process of IKEv2 SA establishment. An Intermediate Exchange makes it possible to use the existing IKE fragmentation mechanism (that cannot be used in the initial IKEv2 exchange (IKE_SA_INT)); helping to avoid IP fragmentation of large IKE messages if they need to be sent before IKEv2 SA is established.

RFC 9370 Multiple Key Exchanges: Allows multiple key exchanges to take place while computing a quantum-resistant shared secret during an IKEv2 SA setup. The initial IKEv2 key exchange (IKE_SA_INIT) messages do not have any inherent fragmentation support within IKE. Additional key exchanges are performed using IKEv2 intermediate key exchange (IKE_INTERMEDIATE) messages that follow the initial key exchange (IKE_SA_INIT). This allows the standard IKE fragmentation mechanisms (which cannot be used in IKE_SA_INIT) to be available for the potentially large key exchange messages with post-quantum algorithm data.

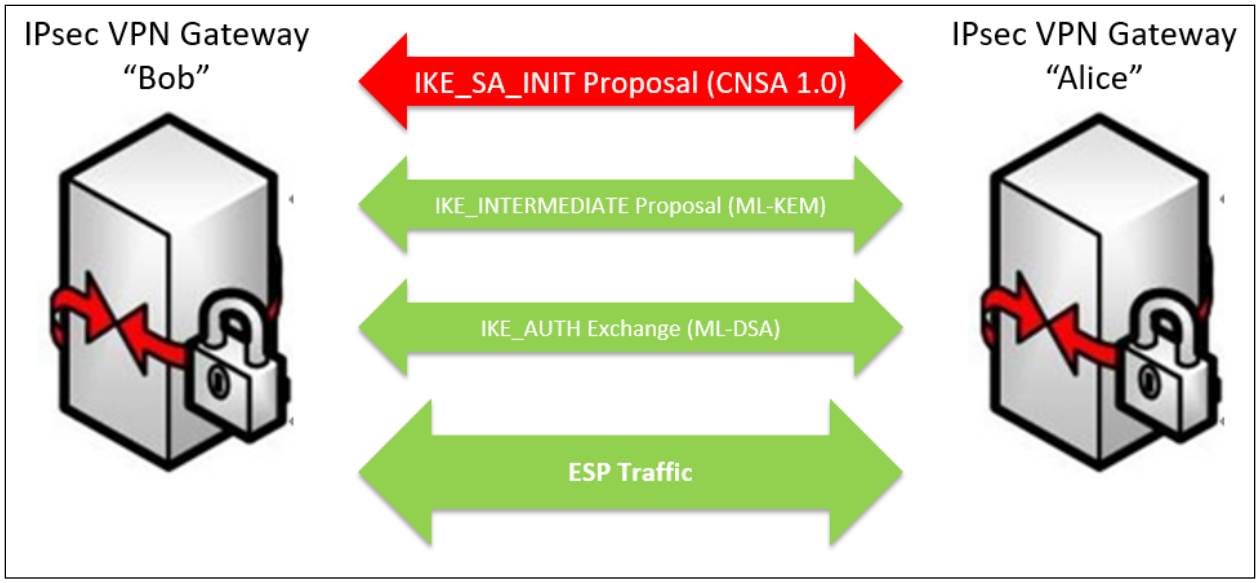

Figure 5. CNSA 2.0 IKEv2 Exchanges

As detailed in Figure 5, RFC 9370 enables peers to perform multiple key exchanges. The key-establishment algorithm used in the Initial IKE SA (IKE_SA_INIT) exchange must be constrained enough in size as to not induce IP fragmentation. The ML-KEM-1024 public key and ciphertext sizes are too large for this initial exchange and thus the IKE_SA_INIT exchange must use a CNSA 1.0-compliant key establishment algorithm. A subsequent Intermediate IKE (IKE_INTERMEDIATE) exchange (as specified in RFC 9242) is then used to perform an ML-KEM key establishment. This second exchange, encrypted using keys established by IKE_SA_INIT, can leverage the IKEv2-level fragmentation mechanism specified in RFC 7383.

7.2 GRAY FIREWALL/ENCRYPTION COMPONENT

The Gray Firewall/Encryption Component is located between the Outer and Inner Encryption Components and provides packet filtering for, and access to, Gray Management and Data Services. The Gray Firewall/Encryption Component is needed for centralized management when sharing Gray Services between sites over an untrusted network. As shown in Figure 1, the Gray Firewall/Encryption Component must filter all traffic routed to two or more Inner Encryption Components of different classification ensuring that the separate Inner Encryption Component cannot communicate with each other. The Gray Firewall/Encryption Component provides the inner layer of encryption for the protection of Gray Services as their Management and Data traffic traverses the Black Network. As shown in Figure 2, the Gray Management and Data traffic must be encrypted using IPsec, or MACsec before being routed through the Outer Encryption Component to another site's Gray Firewall/Encryption Components. When the Gray Firewall is used as the Gray Encryption Component it must be chosen from the CSfC Components list for Traffic Filtering Firewalls, and either MACsec Device or IPsec VPN Gateway. The Outer Certificate Authority digitally signs the Gray Firewall's certificate. The implementing AO may select an additional component from the CSfC components list to serve as an Encryption Component for Gray Management and Data traffic, or use a Type 1 Encryption Device.

7.2.1 GRAY MANAGEMENT VPN

The tunnel referred to as the Gray Management VPN connects multiple Gray Management Networks together to create the Enterprise Gray Network. This Gray Management VPN is located between two or more Gray Firewalls/Encryption Components in either a star or mesh network configuration (see Section 7). The Gray Management VPN allows for remote management of Gray Management Networks, other Gray Components, and resources shared between local and remote Gray Management Networks. The Gray Management VPN uses the same CA as the Outer Encryption Component and Gray Management Network, but if the AO desires to have more security they can either create a separate CA, or they can implement PSK authentication.

7.2.2 GRAY DATA VPN

The tunnel that connects the Gray Data Networks together in order for client devices to connect through the Outer Encryption Component to the Inner Encryption Component can connect to another site's Inner Encryption Component. This follows the same requirements as the Gray Management VPN and has the same options. It is most useful for a multi-site enterprise with multiple inner enclaves so that all such enclaves can be reached from any site in the enterprise. This is an optional capability of Enterprise Gray and should only be implemented if needed. The Gray Data VPN uses the same CA as the Outer Encryption Component and Gray Management Network, but if the AO desires to have more security they can either create a separate CA, or they can implement PSK authentication.

7.3 SHARED MANAGEMENT SERVICES

An additional capability of the Centralized Management pylon is sharing management services between sites. These shared management services can include CM capabilities, Key Generation Solutions (KGS), CAs, and other management services. This sharing of management services allows for these services to either be centralized on a single site for remote sites to leverage or can be distributed throughout multiple sites. This allows for a remote site to rely on the other sites for their management services and will not require them to deploy these services locally. When relying on other sites for management services the AO must have operations plan to address how these sites will react when connectivity is lost to the sites supplying its management services. For more information on site survivability see Section 9.

8 SCALABILITY

When deploying a CSfC EG Solution, the scaling of the central management and shared data planes for a large enterprise requires constant work to maintain and update static routing tables. To mitigate this situation, dynamic routing protocols are allowed, but only between the Gray Firewall/Encryption Component. Dynamic routing is only allowed on Gray Data VPN interfaces, and Gray Management VPN interfaces, to allow the shared data plane and EG Network to expand. To help isolate Gray Management VPNs, and Gray Data VPNs, Virtual Routing and Forwarding (VRF) must be used on the Gray Firewall to ensure the use of two, logically separate, routing tables along with the firewall filtering. VRFs may also be deployed on a Gray Firewall servicing a traditional statically routed network for additional protection and security of the Gray Management and Data networks.

8.1 DYNAMIC ROUTING

The ability to scale to multiple centrally managed sites, and use dynamic routing, allows customers more flexibility in how they plan for continuity of operations. This annex introduces dynamic routing for the first time in a CSfC Solution. If the AO decides to use a separate Gray Encryption Component, then dynamic routing must be implemented on it instead of the Gray Firewall. Dynamic routing must only be used on the Gray Firewall/Encryption Component to propagate routing information through the Gray Firewall/Encryption Component to share Gray Management and Gray Data services at multiple sites. If dynamic routing protocols are used, mutual authentication must occur between a solutions network's Gray Firewalls/Encryption Components at all sites, separate from the authentication for the VPN tunnels.

The following dynamic routing protocols may be used by the Gray Firewall/Encryption Component to support Enterprise Gray VPNs:

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System to Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- Routing Information Protocol, version 2 (RIPv2)

8.1.1 DYNAMIC ROUTING PROTOCOL SECURITY

Dynamic routing protocol security is dependent on both the protocol itself, and the different implementations by vendors; thus, care must be taken when selecting a device to perform dynamic routing. Dynamic routing protocols are powerful tools for network administration, and are vulnerable to attacks, misconfiguration, and misuse by administrators. Care and consideration must be used when implementing dynamic routing into a CSfC Solution.

Dynamic routing protocols support peer authentication, which allows for all unauthenticated messages to be dropped. This ensures all devices performing dynamic routing are mutually authenticated and routing updates can be trusted. The dynamic routing protocols authenticate each peer with either a PSK that may be specific to each set of network device peers, or across the entire routing domain. Different network device vendors support different levels of security within each routing protocol. Network devices are required to use the peer message authentication feature within the Enterprise Gray Firewall/Encryption Component when performing dynamic routing. Furthermore, the implementation of dynamic routing protocols must support peer authentication using at a minimum, a network PSK or ideally, a PSK per each device with a key length of at least 256 bits. A hashing-based verification must be used for this peer authentication and at minimum must support MD5 and should support SHA-256 or better.

Dynamic routing protocol implementations also support a form of route filtering which may be used to deny a subset of routes from being advertised to other devices on the network and prevent the devices

from accepting unauthorized routes. Within the CSfC Solution the Gray Firewall/Encryption Component must use route filtering to only accept the minimum routes necessary for the Enterprise Gray Network. All other routes must be rejected. The route filtering policies must not use overly large subnets or route summarization and should be limited to allowing the smallest subset of networks. In addition, the routes being advertised over the Gray Management VPN tunnels must be limited to routes about the local Gray Management Network and known remote Gray Management Networks. Also, the same is true for advertisements on the Gray Data VPN tunnels with the advertisements only sharing the local Gray Data network and other Gray Data Networks. The routes for the Gray Data Networks must not be advertised to the Gray Management Networks and Gray Management routes must not be advertised to the Gray Data Networks. The devices performing dynamic routing must disable dynamic routing on all other interfaces of the router and ensure that routes not part of the Gray Management or Data networks are not being advertised.

8.2 VIRTUAL ROUTING AND FORWARDING (VRF)

When using dynamic routing protocols, data and management traffic must be separated using VRF on the Gray Firewall to further enhance the security beyond firewall filtering. VRFs are not required outside of dynamic routing but can greatly increase the security posture within traditional static routing networks. Each interface will be assigned to a VRF that is specifically allowed to interact with its respective network plane (Data Plane or Management Plane). In some cases, the implementer may need to import or export routes to establish a VPN tunnel on an interface outside of its respective VRF. The primary use case of importing and exporting routes between VRFs is to allow for the importing of the routes destined for the Outer Encryption Component. The Data and Management VRF would send IPsec or MACsec traffic to the Outer Encryption Component to travel over its encrypted tunnel. Figure 6 shows how Data and Management VRFs interact with the Outer Encryption Component. A single VRF may be used to allow routing between Data lines and Gray Data VPN allowing for routing between the sites if the Gray Data VPN is used. A separate VRF should be used for the local Gray Management Network allowing for separation and for connecting the Gray Firewall/Encryption Component to the local Gray Management Network.

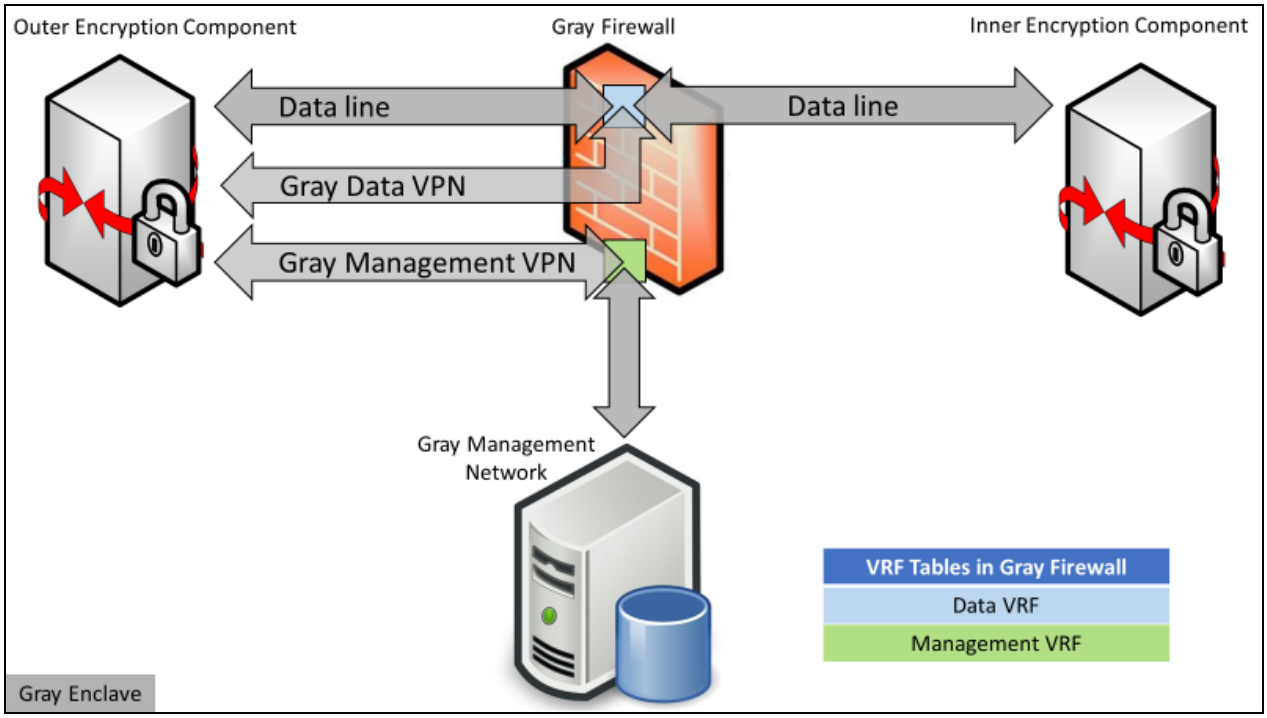

Figure 6. Dynamic Routing

8.3 AUTHORIZED PORTS, PROTOCOLS, AND INTERNET PROTOCOL ADDRESSES

8.3.1 BLACK NETWORK

As shown in Figure 7, IKE and IPsec are the only protocols authorized for bi-directional traffic flow between the Outer Encryption Component and the Outer Firewall. A default route may be used at the Outer Firewall and the Outer Encryption Component for egress traffic to the Internet. Hypertext Transfer Protocol Secure (HTTPS) is not authorized for profile download on the Black Network.

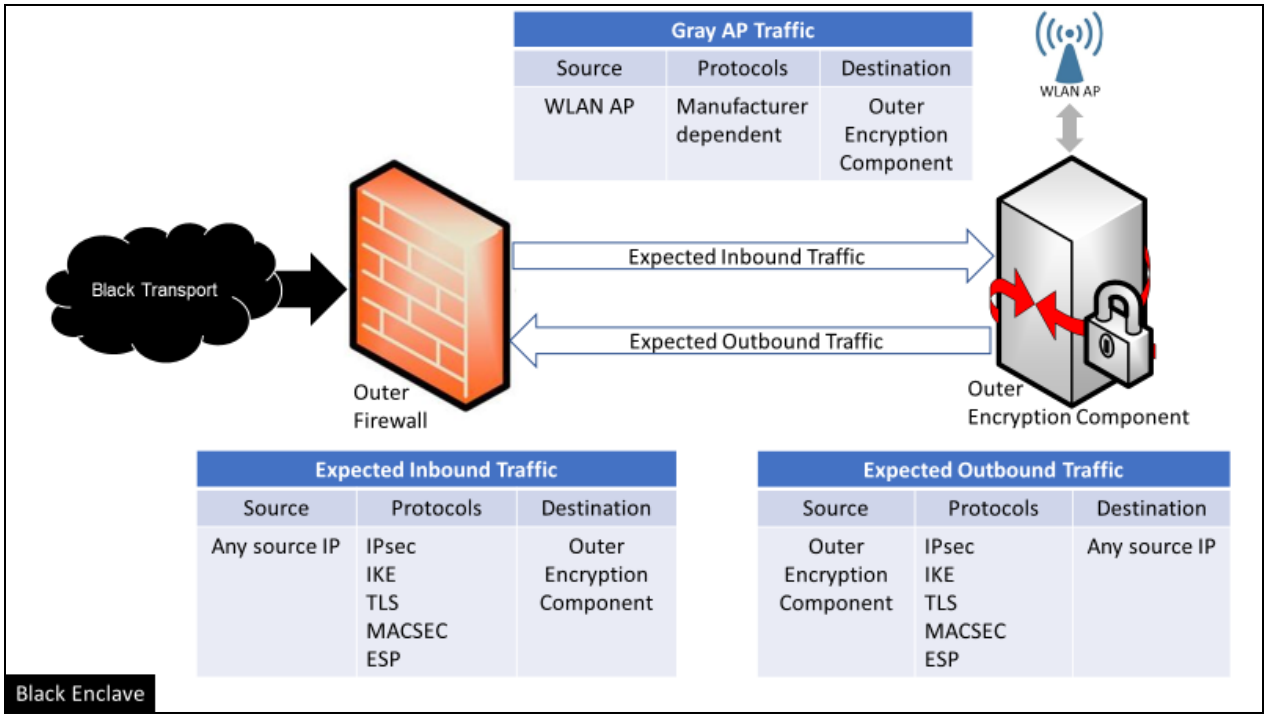

Figure 7. Authorized Protocols on Black Network

8.3.2 GRAY NETWORK

Between the Outer Encryption Component and the Gray Firewall/Encryption Component, traffic must be separated into Data Line, Gray Data VPN, and Gray Management VPN. Authorized Management traffic includes Hypertext Transfer Protocol (HTTP), HTTPS, DNS, Secure Shell (SSH), and authentication, accounting, and update services. Management traffic is designed to control networking and server services. Authorized Data traffic includes DNS, IKE, IPsec, TLS, MACsec, and update services. The Outer Encryption Component and Gray Firewall/Encryption Component may only receive Data traffic for the purpose of domain name resolution and security updates, then traverse to any Inner Encryption Component of the same classification level. Authorized VPN traffic is IKE and IPsec and it traverses to the Gray Firewall/Encryption Component to provide Gray VPN services and to Inner VPN Gateways that support MSC. From the Gray Firewall/Encryption Component to the Inner Encryption Component, traffic is separated into Data and VPN (see Figure 8).

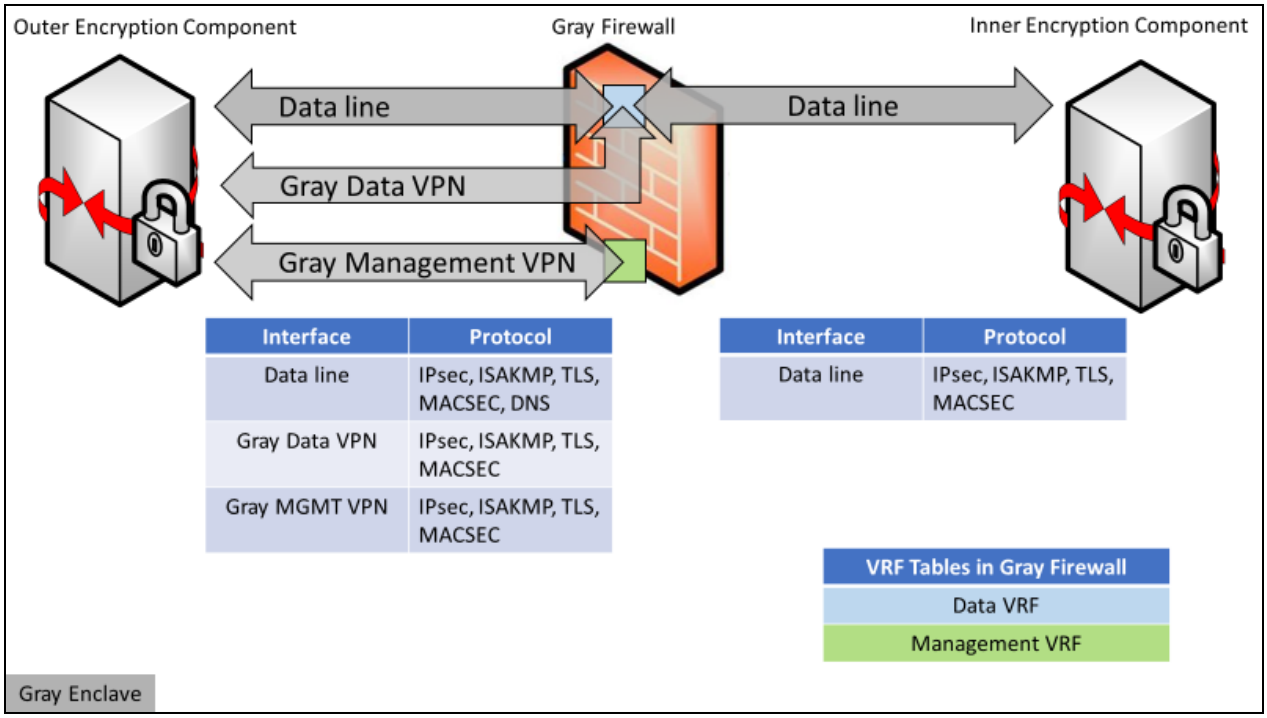

Figure 8. Authorized Protocols on Gray Network

9 SITE SURVIVABILITY

AOs implementing Enterprise Gray Solution guidance may deem site survivability optional for some remote sites depending on the mission of the organization. If site survivability is not a requirement and there is a loss of connectivity, then the remote site will fail closed. In the event of loss of connectivity, Campus WLAN, MA, and MSC solutions will not have access to offsite classified resources.

If the implementing organization requires site survivability, then redundant equipment is required for remote sites to maintain connectivity, thereby ensuring access to classified resources. Should a loss of connectivity to the centrally managed site occur, then access to resources will be impacted. However, to survive such an event, the remote site requires resources to authenticate users, provide name resolution, certificate revocation list lookups, time synchronization, and centralized log collection. Site survivability only applies to the Gray Management Services, it does not include any Inner Services, or data. An AO or Security Officer may deem that redundancy is required in the Red Data plane, but such a scenario is outside the scope of this annex.

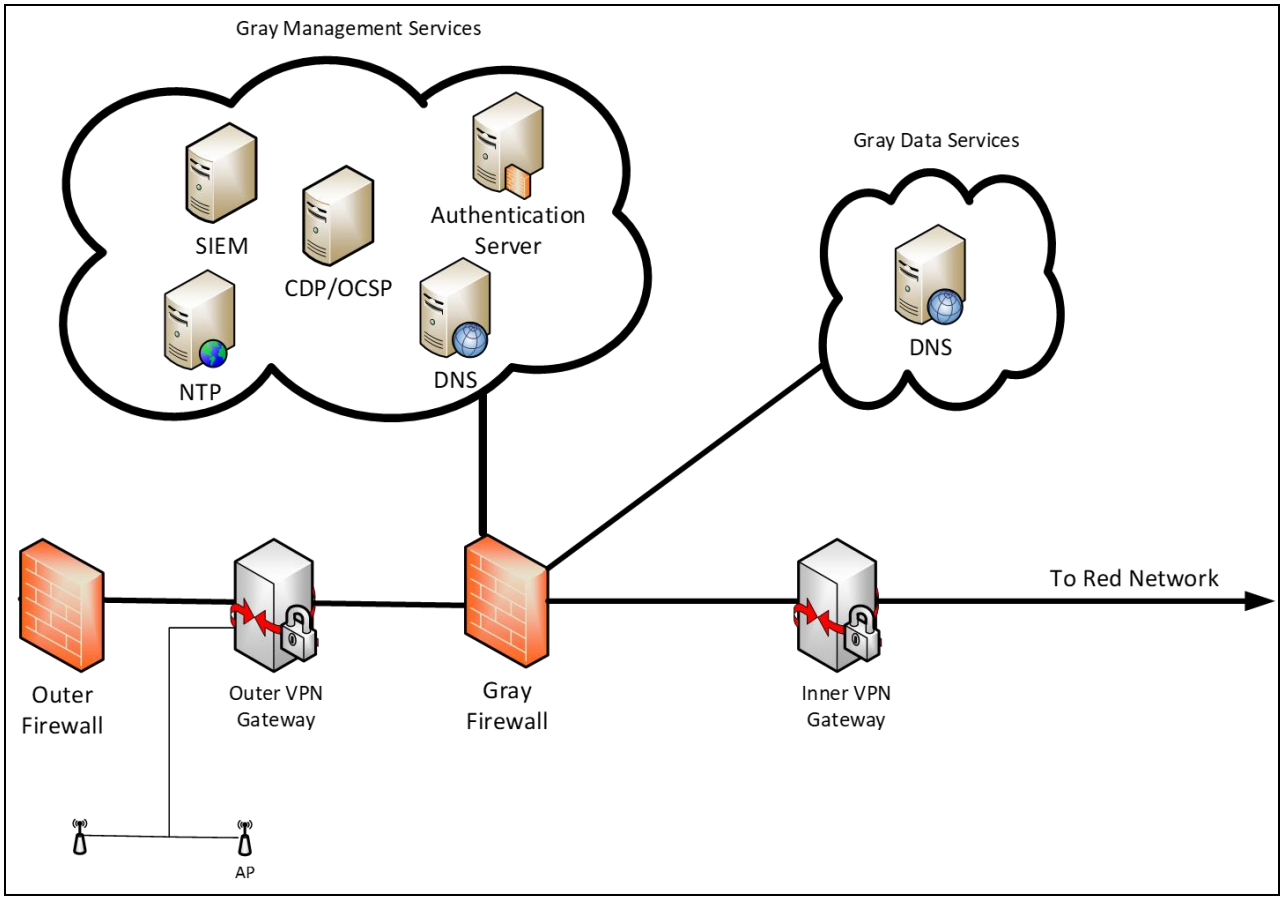

Figure 9. Minimum Services Needed for Site Survivability

10 REQUIREMENTS OVERVIEW

Sections 10 through 10.8, specify requirements necessary for the implementation of an EG Solution compliant with this annex. Interconnecting CSfC Solutions must also follow the requirements of the CPs being implemented, (e.g., MA, MSC, and WLAN).

Guidance provided in this annex allows solution owners the flexibility to implement a variety of designs for interconnecting two or more CPs that share a common Gray Network. Although most requirements apply to all CSfC Solutions, some requirements only apply to implementations whose high-level designs incorporate certain features, as noted in Table 2.

Table 2. Capability Designators

Capability Package	Designator	Description
Multiple CPs	All	Requirements pertinent to all CPs. This CSfC Annex comprises all three data-in-transit CPs and describes how to protect classified data in transit while interconnecting scalable and centrally manageable solutions simultaneously across geographically large distances by leveraging existing infrastructure and services.
Mobile Access	MA	Requirements pertinent to the MA CP only. This CP describes how to protect classified data (including voice and video traffic) in MA solutions transiting Private Cellular Networks and Government Private Wi-Fi networks.
Multi-Site Connectivity	MSC	Requirements pertinent to the MSC CP only. This CP describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with IPsec.
Campus WLAN	WLAN	Requirements pertinent to the Campus WLAN CP only. This CP describes how to protect classified data (including voice and video traffic) in a WLAN solution transiting Government Private Wi-Fi networks.

10.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

In some cases, multiple versions of a requirement may exist within this annex. Such alternative versions of a requirement are designated as being either a Threshold requirement, or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimally acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

When separate Threshold and Objective versions of a requirement exist, the Objective requirement provides more security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible, owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Optional" in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold/Objective" column indicates that the Threshold equals the Objective (T=O).

Requirements listed as Objective in this annex may become Threshold requirements in future guidance. Solution owners are encouraged to implement Objective requirements whenever possible to facilitate compliance with future guidance.

10.2 REQUIREMENTS DESIGNATORS

Each requirement in this annex is identified by a label consisting of the prefix "EG", a two-letter category, and a sequence number (e.g., EG-FW-7). The Gray Firewall/Encryption Component and General Requirements are listed together in Tables 8 through 13. Each table represents a core capability of the *Enterprise Gray Implementation Requirements Annex*.

Table 3. Requirements Digraph

Digraph	Description	Section	Table
FW	General Enterprise Gray Requirements	Sections 10.3, 10.5	Tables 8, 10
DR	Scalability Requirements	10.6	Tables 11
AR	Site Survivability Requirements	Sections 10.3-10.7	Tables 8-12
PS	Product Selection Requirements	Sections 10.3-10.5	Tables 8, 10
TR	Testing Requirements	10.8	Table 13

Table 4. CNSA 2.0 Algorithms for Software and Firmware Signing

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels
ML-DSA	Asymmetric algorithm for digital signatures	FIPS 204	Category 5 parameter, ML-DSA87

Table 5. Gray Firewall/Encryption Component: Approved CNSA 1.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 7296 IETF RFC 9206
Authentication (Digital Signature)	Rivest Shamir Adelman (RSA) 3072 or Elliptic Curve Digital Signature Algorithm over the curve P-384 with SHA-384	FIPS PUB 186-5 IETF RFC 4754 IETF RFC 7427 IETF RFC 7296 IETF RFC 9206
Key Exchange/Establishment	Elliptic Curve Diffie-Hellman over the curve P-384 (Diffie-Hellman (DH) Group 20) or DH with prime modulus of 3072 bits (group 15) or 4096 bits (group 16)	NIST SP 800-56A IETF RFC 3526 IETF RFC 5903 IETF RFC 7296 IETF RFC 9206
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6234 IETF RFC 9206

Table 6. Approved CNSA 2.0 Algorithms for IPsec

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256-GCM	FIPS PUB 197
Authentication (Digital Signature)	ML-DSA-87	FIPS 204
Key Establishment	ML-KEM-1024	FIPS 203
Integrity (Hashing)	SHA-384 or SHA-512	FIPS PUB 180-4 IETF RFC 6234

Table 7. MACsec Encryption (Approved Algorithms)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Galois Counter Mode (GCM)- AES-256 GCM-AES-XPN-256	FIPS PUB 197 IEEE 802.1AEbn-2018 IEEE
Key Wrap	AES Key Wrap	IETF RFC 3394

10.3 General Enterprise Gray Requirements

Table 8 identifies the requirements for all CSfC solutions deploying the Enterprise Gray Solution.

Table 8. General Enterprise Gray Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-1	The Gray Firewall must only accept management traffic on the physical ports connected to the Gray Management Network and/or EG Network.	T=O		All
EG-FW-2	The Gray Firewall must only permit packets whose source and destination IP addresses match the external interfaces of the Encryption Components supporting the Red Network and EG Network of the same classification level and internal interface of the Encryption Components CSfC Solution.	T=O		All
EG-FW-3	The Gray Firewall's outward interface must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O		All
EG-FW-4	The Gray Firewall must deny all traffic on the outward interface that is not explicitly allowed.	T=O		All
EG-FW-5	The Gray Firewall must block all traffic routed to and between two or more Inner VPN Gateways of different classification levels.	T=O		All
EG-FW-6	Remote administration of the Gray Firewall from the Gray Management Network and EG Networks must only use SSHv2, IPsec, or TLS.	T=O		All
EG-FW-7	The Gray Firewall must permit IKE, IPsec, or TLS traffic between EUDs and Encryption Components.	T=O		MA, WLAN
EG-FW-8	The Gray Firewall must allow HTTP traffic between the Authentication Server and the Gray CDP or OCSP Responder.	T	EG-FW-9 and EG-FW-10	All
EG-FW-9	The Gray Firewall/Encryption Component must allow HTTP traffic between the Authentication Server and the Gray CDP or OCSP Responder.	O	EG-FW-8	All
EG-FW-10	The Gray Firewall must allow HTTP responses from the Gray CDP or OCSP Responder to the Authentication Server that contains a well-formed CRL per IETF	O	EG-FW-8	All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	RFC 5280 or OCSP Response per RFC 6960 and block all other HTTP responses.			
EG-FW-11	The Gray Firewall's inward interface must block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O		All
EG-FW-12	The Gray Firewall's inward interface must deny all traffic that is not explicitly allowed.	T=O		All
EG-FW-13	The Gray Firewall must allow control plane traffic between the Outer Encryption Component, Gray Firewall, Gray Management Network, and EG Network (e.g., NTP, Dynamic Host Configuration Protocol, and DNS).	T=O		All
EG-FW-14	A Gray Firewall, Outer Encryption Component, and Gray Encryption Component must be administered from a workstation designated for managing Gray Components which resides on the local Gray Management or EG Network.	T=O		All
EG-FW-15	Remote administration of all Gray components must be done using SSHv2, IPsec, or TLS with the appropriate CNSA suite for the highest classification of the solution. Encryption provided by the EG Network does not fulfill this requirement.	T=O		All
EG-AR-1	All Gray Management Services and Enterprise Gray Services must go through a firewall to access and communicate with the Outer Encryption Component, Gray Firewall, and Gray Encryption Component.	T=O		All
EG-AR-2	The time servers that serve network time to Gray Management and Red Management must use a secure protocol to maintain the authenticity and integrity of the network time to clients.	O		All
EG-AR-3	The DNS servers used on the Gray Data, Gray Management, and Red Management Networks must use DNSSEC to secure and	O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	maintain the authenticity and integrity of the domain record to clients.			
EG-AR-4	The Outer Encryption Component must be configured to not route between the inner interfaces if there is more than one.	T=O		All
EG-AR-5	The authentication service that authenticates EG and/or Gray Management administrators must be separate from the EUD and Encryption Components.	T=O		All
EG-PS-1	The Gray Firewall must be chosen from the list of Traffic Filtering Firewalls on the CSfC Components List.	T=O		All
EG-AR-25	The Gray Management Network must be used exclusively for all management of the Outer Encryption Component, Gray Firewall, Gray Encryption Component, if present, and Solution Components within the Gray Network.	T=O		All
EG-AR-26	All solution components (Firewalls, WLAN Access Systems, VPN Gateways, Authentication Servers, and EUDs) must use software and firmware signing algorithms in Table 4.	O	Optional	All

10.4 Multiple CP Requirements

Table 9 identifies the requirements for CSfC solutions deploying the Enterprise Gray's pylon to allow for the same solution components to service multiple DiT CPs. For example, allow for a Campus WLAN CP solution to also act as a MA CP solution with the same equipment.

Table 9. Multiple CP Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-6	Inherit all security requirements of the CPs that are being integrated together. If the CPs have different requirements accept the one with the higher security posture.	T=O		All
EG-AR-7	An Outer Firewall is required between the Outer Encryption Component and the Black Network.	T=O		MA/MSC

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-8	The Outer Firewall must not have a physical or logical connection to the Gray Management Network or EG Management Network.	T=O		MA/MSC
EG-AR-9	EUDs provisioned for an MA solution must only be used for an MA solution, and not used to access any resources other than the Red Network it communicates with via two layers of encryption.	T=O		MA
EG-AR-10	EUDs provisioned for a Campus WLAN solution must only be used for a WLAN solution and not used to access any resources other than the Red Network it communicates with via two layers of encryption.	T=O		WLAN

10.5 Centralized Management Requirements

Table 10 identifies the requirements for CSfC solutions deploying the Enterprise Gray's pylon to allow for Centralized Management of remote Gray Management Networks and allows for sharing of the Gray Data Network across sites.

Table 10. Centralized Management Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-16	The Gray Firewall must be used as the Inner Encryption Component for the EG Network.	T	EG-FW-17	All
EG-FW-17	If the AO deems it necessary, a separate Gray Encryption Component must be used to service the EG Network.	O	EG-FW-16	All
EG-FW-18	The Gray Encryption Component and Outer Encryption Components must either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC criteria for implementation independence.	T=O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-FW-19	The Gray Firewall/Encryption Component at each site provides the inner layer of encryption and the Outer Encryption Component provides the outer layer of encryption to protect Gray Management traffic between sites.	T=O		All
EG-FW-20	The Gray Firewall/Encryption Component must not permit split-tunneling.	T=O		All
EG-FW-21	The Gray Firewall/Encryption Component must use Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (i.e. Generic Routing Encapsulation), authorized TLS deployment, or MACsec.	T=O		All
EG-FW-22	The Gray Firewall/Encryption Component must meet all CSfC requirements for an Encryption Component.	T=O		All
EG-FW-23	The Gray Firewall/Encryption Component must form a Gray Management VPN tunnel with other Gray Firewall/Encryption Components that allows routing between their Gray Management Networks forming the EG Network.	T=O		All
EG-FW-24	If the AO deems necessary, then the Gray Firewall/Encryption Component may form a Gray Data VPN tunnel between itself and other Gray Firewall/Encryption Components allowing for routing to happen between Gray Data Networks.	O	Optional	All
EG-FW-25	The packet size for packets leaving the external interface of the Gray Firewall/Encryption Component must be configured to keep the packets from being fragmented and impacting performance. This requires proper configuration of the Maximum Transmission Unit (MTU) for IPv4 or Path MTU (PMTU) for IPv6 and should consider the Outer VPN Gateway MTU/PMTU values for achievement.	T=O		All
EG-AR-11	Two independent layers of CSfC approved encryption must be used when extending	T=O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	Gray Services to other site(s) over an untrusted network.			
EG-AR-12	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.	-	-	All
EG-AR-13	Requirement has been relocated to the *CSfC Key Management Requirements Annex*.	-	-	All
EG-AR-14	Requirement has been relocated to the *CSfC Symmetric Key Management Requirements Annex.*	-	-	All
EG-AR-15	EUDs provisioned for MA and Campus WLAN solutions must not be used to connect to the Gray Firewall/Encryption Component.	T=O		MA, WLAN
EG-PS-2	The Gray Encryption Component must be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O	EG-PS-3	All
EG-PS-3	The Gray Encryption Component must be chosen from the list of MACsec Ethernet Encryptions on the CSfC Components List.	T=O	EG-PS-2	All
EG-FW-26	The VPN Components must use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 5.	T	EG-FW-27, EG-FW-28, and EG-FW-29	All
EG-FW-27	All IPsec connections must use IETF standards compliant with IKE implementations as specified in Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile)* including RFC 9370, RFC 9242 and RFC 7383.	O	EG-FW-26	All
EG-FW-28	All IPsec connections must use multiple key exchanges with an initial IKEv2 SA key exchange and an intermediate IKEv2 key exchange:	O	EG-FW-26	All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	• IKE_SA_INIT: The IKEv2 SA key exchange performed in IKE_SA_INIT must use a CNSA 1.0 key establishment algorithm (as specified in Table 5) • IKE_INTERMEDIATE: The IKEv2 SA key establishment performed in the IKE_INTERMEDIATE exchange must use ML-KEM-1024 (as specified in Table 6)			
EG-FW-29	The VPN Components must use algorithms from the algorithm suite in Table 6 for all IPsec VPN tunnels, with the exception of the IKE_SA_INIT exchange.	O	EG-FW-26	All

10.6 SCALABILITY REQUIREMENTS

Table 11 identifies the requirements for CSfC solutions deploying the Enterprise Gray's pylon to allow for dynamic routing and scalability on the Gray Encryption Component/Gray Firewall.

Table 11. Scalability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-DR-1	Dynamic routing is only allowed on the Gray Firewall/Encryption Component, no other devices on the network can perform dynamic routing.	T=O		All
EG-DR-2	If dynamic routing protocols are used, then dynamic routing peer authentication must be performed between the Gray Firewalls/Encryption Components running dynamic routing.	T=O		All
EG-DR-3	If dynamic routing protocols are used, dynamic routing peer authentication used by the network devices must use an MD5 hashing algorithm.	T	EG-DR-4	All
EG-DR-4	If dynamic routing protocols are used, dynamic routing peer authentication used by the network devices must use a SHA-256 hashing algorithm or greater.	O	EG-DR-3	All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-DR-5	If dynamic routing protocols are used, all network devices participating in dynamic routing message authentication must use a strong PSK with at least 256-bits of entropy for the entire network (Group Keys).	T	EG-DR-6	All
EG-DR-6	If dynamic routing protocols are used, all network devices participating in dynamic routing message authentication must use a strong PSK with at least 256-bits of entropy for every network device (Point-to-point Pre-Shared Keys).	O	EG-DR-5	All
EG-DR-7	If dynamic routing protocols are used, all network devices participating in dynamic routing must only share necessary routing information about the local Gray Management Network and other Gray Management Networks to devices servicing the Gray Management VPN tunnels.	T=O		All
EG-DR-8	If dynamic routing protocols are used, all network devices participating in dynamic routing must only share necessary routing information about the local Gray Data Network and other Gray Data Networks to devices servicing the Gray Data VPN tunnels.	T=O		All
EG-DR-9	If dynamic routing protocols are used, all network devices performing dynamic routing must use route filtering on both inbound and outbound routes stopping unauthorized routes from being received or shared and by default all routes must be blocked.	T=O		All
EG-DR-10	If dynamic routing protocols are used, the network devices performing dynamic routing must disable dynamic routing on all interfaces except the interfaces serving the Gray Management VPN tunnel and the Gray Data VPN tunnel.	T=O		All
EG-DR-11	If dynamic routing protocols are used, routes must not be shared between the Gray Management and Data Tunnels.	T=O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-DR-12	If dynamic routing protocols are used, routes being shared and filtered must be the most specific routes possible.	T=O		All
EG-AR-16	If dynamic routing protocols are used, then two VRFs must be used to separate Data and Management traffic.	T=O		All
EG-AR-17	Two VRFs must be used to separate Data and Management traffic.	O	Optional	All
EG-AR-18	If VRFs are used, the Management VRFs must only contain routing information about the local Gray Management network and remote Gray Management networks.	T=O		All
EG-AR-19	If VRFs are used, the Data VRFs must only contain routing information about the local Gray Data network and remote Gray Data networks.	T=O		All
EG-AR-20	If VRFs are used, the routes cannot be exported or imported between the data and management routing instances.	T=O		All
EG-AR-21	If VRFs are used, they are allowed to import routes from an outside routing instance as long as they do not allow sharing of non-authorized routes.	T=O		All
EG-AR-22	If dynamic routing protocols are used, implementers must use one of the following: Routing Information Protocol (RIPv2), OSPF, EIGRP, BGP, or IS-IS.	T=O		All
EG-AR-25	The VPN Components must use protocols and algorithms for creating all VPN tunnels selected from an Algorithm Suite in Table 5 that are approved to protect the highest classification level of the Red Network data.	T	EG-AR-26, EG-AR-27, and EG-AR-28	All
EG-AR-26	All IPsec connections must use IETF standards compliant with IKE implementations as specified in Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec (*draft-guthrie-cnsa2-ipsec-profile)* including RFC 9370, RFC 9242 and RFC 7383.	O	EG-AR-25	All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-27	All IPsec connections must use multiple key exchanges with an initial IKEv2 SA key exchange and an intermediate IKEv2 key exchange: • IKE_SA_INIT: The IKEv2 SA key exchange performed in IKE_SA_INIT must use a CNSA 1.0 key establishment algorithm (as specified in Table 5) • IKE_INTERMEDIATE: The IKEv2 SA key establishment performed in the IKE_INTERMEDIATE exchange must use ML-KEM-1024 (as specified in Table 6)	O	EG-AR-25	All
EG-AR-28	The VPN Components must use algorithms from the algorithm suite in Table 6 for all IPsec VPN tunnels, with the exception of the IKE_SA_INIT exchange.	O	EG-AR-25	All

10.7 SITE SURVIVABILITY REQUIREMENTS

Table 12 identifies the requirements for the site survivability pylon which allows for solutions deploying the Centralized Management pylon to have redundant management services between different sites.

Table 12. Site Survivability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-AR-23	Should a loss of connection occur, a local implementer must use an authorized authentication service to authenticate EUDs and Encryption Components.	T=O		All
EG-AR-24	If the implementing organization requires site survivability, implementers must use a Gray Data DNS on the remote site(s) that mirrors the DNS on the main site. This allows for EUDs and site-to-site interfaces to connect to the proper Inner Encryption Component.	T=O		All

10.8 TESTING REQUIREMENTS

Table 13. Testing Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
EG-TR-0	The organization implementing the annex must perform all tests listed in EG Testing Annex and maintain artifacts of the testing results.	T=O		All

APPENDIX A. ACRONYMS

Acronym	Meaning
AO	Authorizing Official
AR	Additional Requirements
BGP	Border Gateway Protocol
CA	Certificate Authority
CDP	Certificate Revocation List (CRL) Distribution Point
CNSA	Commercial National Security Algorithm
CP	Capability Package
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
DNS	Domain Name System
DNSSEC	Domain Name System Security
DR	Dynamic Routing
EG	Enterprise Gray
EIGRP	Enhanced Interior Gateway Routing Protocol
FW	Firewall
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IS-IS	Intermediate System to Intermediate System
LMS	Leighton-Micali Signature
MA	Mobile Access
MACsec	Media Access Control Security
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
ML-DSA	Module-Lattice-Based Digital Signature
MSC	Multi-Site Connectivity
MTU	Maximum Transmission Unit
NSA	National Security Agency
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OSPF	Open Shortest Path First
PMTU	Path Maximum Transmission Unit
PSK	Pre-Shared Key
RIPv2	Routing Information Protocol, version 2
SIEM	Security Information and Event Management
SSH	Secure Shell
SSHv2	Secure Shell, version 2
TLS	Transport Layer Security
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WLAN	Wireless Local Area Network

Acronym	Meaning
XMSS	Xtended Merkle Signature Scheme

APPENDIX B. REFERENCES

CNSSI 1200	CNSS Instruction No. 1200, *National Information Assurance Instruction for Space Systems Used to Support National Security Missions,* May 7, 2014.	7 May 2014
CNSSI 1253	CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems,* March 27, 2014.	27 March 2014
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	February 2019
CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.*	March 2022
CNSSP 7	CNSS Policy No. 7, *Policy on the Use of Commercial Solutions to Protect National Security Systems,* December 9, 2015.	December 2015
CNSSP 8	CNSS Policy No. 8, *Policy Governing the Release and Transfer of U.S. Government Cryptologic National Security Systems Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations,* August 2012.	August 2012
CNSSP 11	CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Technology Products,* June 10, 2013.	February 2025
CNSSP 15	*CNSS Policy (CNSSP) Number 15, Use of Public Standards for Secure Information Sharing*	October 2016
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing (CNSA 2.0)*	February 2025
CNSSP 22	CNSS Policy No. 22*, Policy on Information Assurance Risk Management for National Security Systems,* August 2016.	August 2016
CNSSD 500	CNSS Directive No. 500, *Information Assurance (IA) Education, Training and Awareness,* August 2006.	August 2006
CNSSD 502	CNSS Directive No. 502, *National Directive on Security of National Security Systems,* December 16, 2004.	16 December 2004
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	February 2025
CSfC Campus WLAN CP	Commercial Solutions for Classified (CSfC): *Campus Wireless Local Area Network (WLAN) Capability Package (CP), v3.2.0*	March 2026
CSfC CM Annex	*CSfC Continuous Monitoring Annex, v1.1.0*	March 2023
CSfC Mobile Access MA CP	Commercial Solutions for Classified (CSfC): *Mobile Access Capability Package (CP), v2.8.0*	March 2026
CSfC KM Req. Annex	*CSfC Key Management Requirements Annex, v3.0.0*	March 2026

CSfC Symmetric KM Req. Annex	*CSfC Symmetric Key Management Requirements Annex, v3.0.0*	March 2026
FIPS 140-3	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication*	March 2019
FIPS 180-4	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186-5	*Federal Information Processing Standard 186-5, Digital Signature Standard (DSS)*	February 2023
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	May 2023
FIPS 201-2	*Federal Information Processing Standard 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors*	August 2015
FIPS 203	*Module-Lattice-Based Key-Encapsulation Mechanism Standard*	August 13, 2024
FIPS 204	*Module-Lattice-Based Digital Signature Standard*	August 13, 2024
IPsec VPN Client PP	*Virtual Private Network PP-Module for VPN Client*, Version 2.3	August 2021
ISO 09594-8	*Iso9594-8 Information Technology-Open Systems Interconnection-The Directory – Part 8: Public-key and attribute certificate frameworks*	March 2013
Commercial National Security Algorithm Suite	*NSA Guidance on Encryption Algorithms*	December 2015
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	November 2003
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
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 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	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 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 8391	*XMSS: eXtended Merkle Signature Scheme*	May 2018
RFC 8784	*Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*	June 2020
NIST SP 800-37 Rev. 2	National Institute of Standards and Technology (NIST SP) 800-37 Rev. 2*, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 2018.	December 2018
SP 800-53	*NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations*.	December 2020
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019

SP 800-56C	*NIST Special Publication 800-56C Rev. 2, Recommendation for Key Derivation Methods in Key-Establishment Schemes*. L. Chen.	August 2020
NIST SP 800-111	National Institute of Standards Special Publication (NIST SP) 800-111, *Guide to Storage Encryption Technologies for End User Devices,* November 2007.	November 2007
NIST SP 800-131A	*NIST Special Publication 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths*. E. Barker.	March 2019
NIST SP 800-137	National Institute of Standards and Technology Special Publication (NIST SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011.	September 2011
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines*. D. Cooper, et. al.	April 2011
NIST SP 800-208	*Recommendation for Stateful Hash-Based Signature Schemes*	October 2020
RFC 9370	Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)	May 2023
RFC 9242	Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)	May 2022
RFC 7383	Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation	November 2014
RFC 9190	EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3	February 2022