National Security Agency/
Central Security Service

CYBERSECURITY SOLUTIONS

ENTERPRISE GRAY IMPLEMENTATION REQUIREMENTS ANNEX V1.0

The guidance given in this Commercial Solutions for Classified (CSfC) Annex describes how to protect classified data in transit while interconnecting scalable and centrally manageable solutions from multiple Capability Packages simultaneously across geographically large distances by leveraging existing infrastructure and services.

Version 1.0
2 April 2019

Enterprise Gray Implementation Requirements Annex

CHANGE HISTORY

Version	Date	Change Summary
0.8	12 July 2018	• Initial draft of *CSfC Enterprise Gray Implementation Requirements Annex*. Posted for customer review and comments.
0.9	5 March 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.
1.0	2 April 2019	• Final approved version.


Enterprise Gray Implementation Requirements Annex

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

Enterprise Gray Implementation Requirements Annex

1 INTRODUCTION

Cybersecurity Solutions delivers the Enterprise Gray (EG) Implementation Requirements in this document to address increasing demands from customers who desire to implement a Commercial Solutions for Classified (CSfC) deployment with one or more of the following characteristics:

- 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 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 1.0*, 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.

This EG Annex, similar to the CSfC CPs, defines areas of a given network solution in terms of Black, Gray, and Red Network segments commensurate to the level of protection applied to the data in each respective area. Specific guidance for the CPs and these defined areas can be found at: https://www.nsa.gov/resources/everyone/csfc/capability-packages/. Customers who want to use this documentation to register two or more interconnecting CSfC Solutions must do so with NSA.

Additional information about the CSfC process is available on the CSfC web page at: https://www.nsa.gov/resources/everyone/csfc/.

Both the Registration Form and Compliance Checklist are available online at: https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml.

Please provide comments on the usability, applicability, and any shortcomings of this guidance to your NSA Client Advocate and the EG Annex maintenance team (via email) at: Enterprise_Gray_team@nsa.gov.

Solutions adhering to this guidance must also comply with the Committee on National Security Systems policies and instructions.

2 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 3.

2.1 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). 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 1 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.

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.

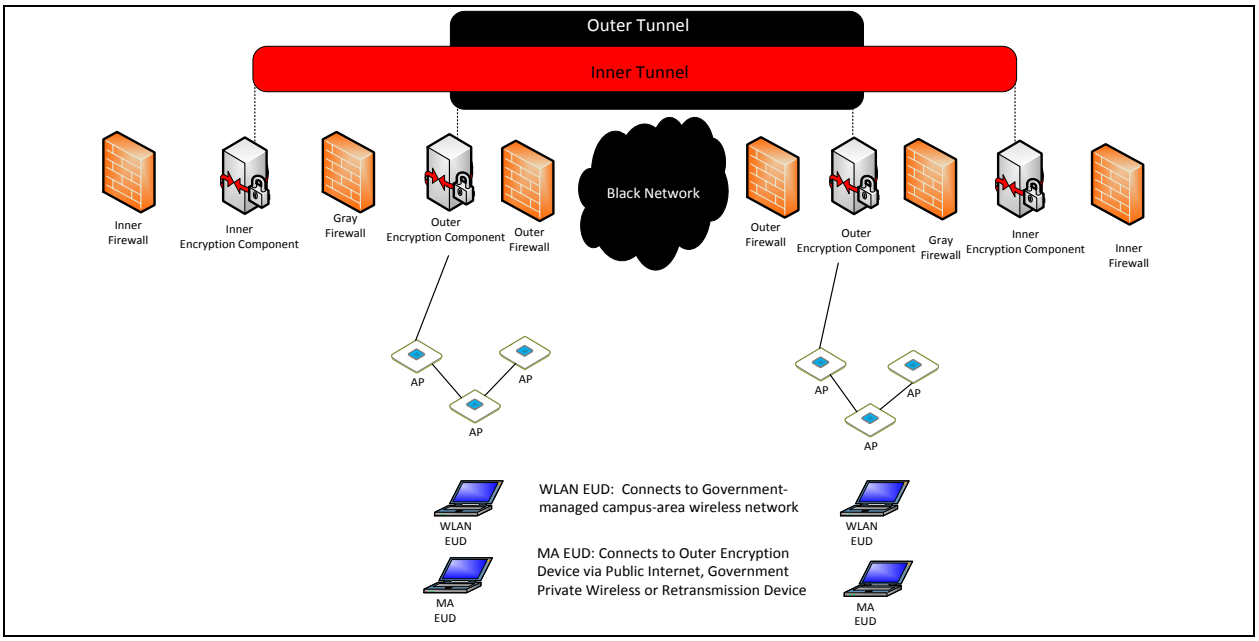

Figure 1. Deploying Multiple CPs Using the Same Components

3 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.

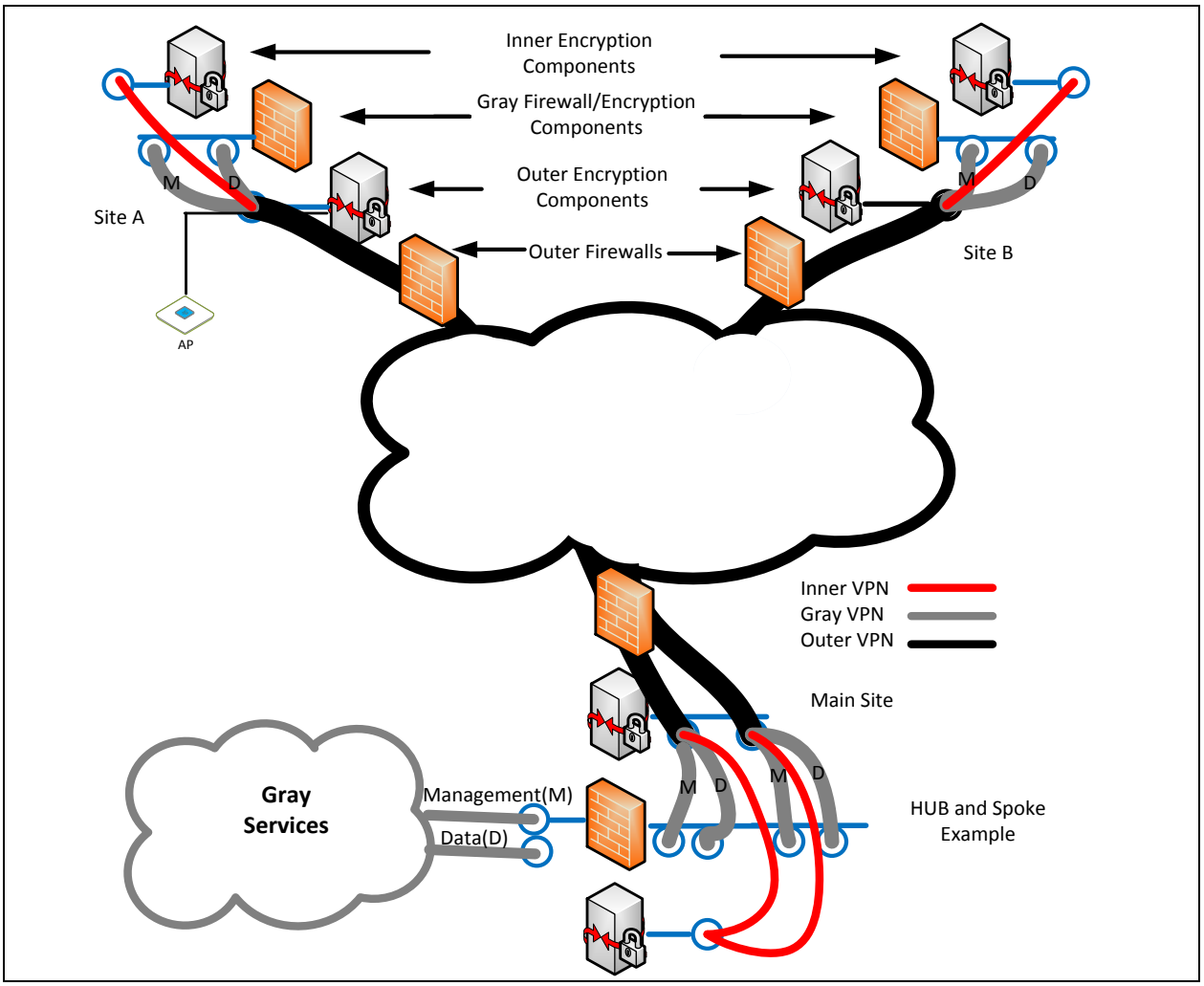

Figure 2. Two Sites ("A" and "B") Using Gray Services Hosted at a Main Site

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 2, 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. 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.

3.1 Enterprise Gray Implementation Guide Components

3.1.1 Outer Firewall

An approved Outer Firewall must be incorporated into most CSfC Solutions designed to send Management and Data traffic over an untrusted network. For customers deploying only a Campus WLAN CP Solution, an Outer Firewall is not required. The Outer Firewall must be located at the edge of all CSfC Solution infrastructures implementing the EG guidance. Both the internal and external interfaces of the Outer Firewall must only permit Internet Protocol security (IPsec), Internet Key Exchange (IKE), Transport Layer Security (TLS), Media Access Control Security (MACsec), and/or Encapsulating Security Payload (ESP) traffic, depending on the encryption method of the Outer Encryption Component, with a destination address of the Outer Encryption Component. As shown in Figure 6, the Outer Firewall and Outer Encryption Component must be physically separate devices.

3.1.2 Outer Encryption Component

The Outer Encryption Component, located between the Outer Firewall and Gray Firewall, is capable of establishing encrypted tunnels using IPsec, IKE, MACsec, and TLS. When used in an EG Solution, this 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.

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.

3.1.3 GRAY FIREWALL/ENCRYPTION COMPONENT

This annex introduces two new functions to the CSfC Program:

- The use of dynamic routing in a Solution Network (discussed in Section 4)
- A security component serving as a firewall and encryption component simultaneously

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 3, 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, MACsec, or TLS before being routed through the Outer Encryption Component to another site's Gray Firewall/Encryption Components. 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.

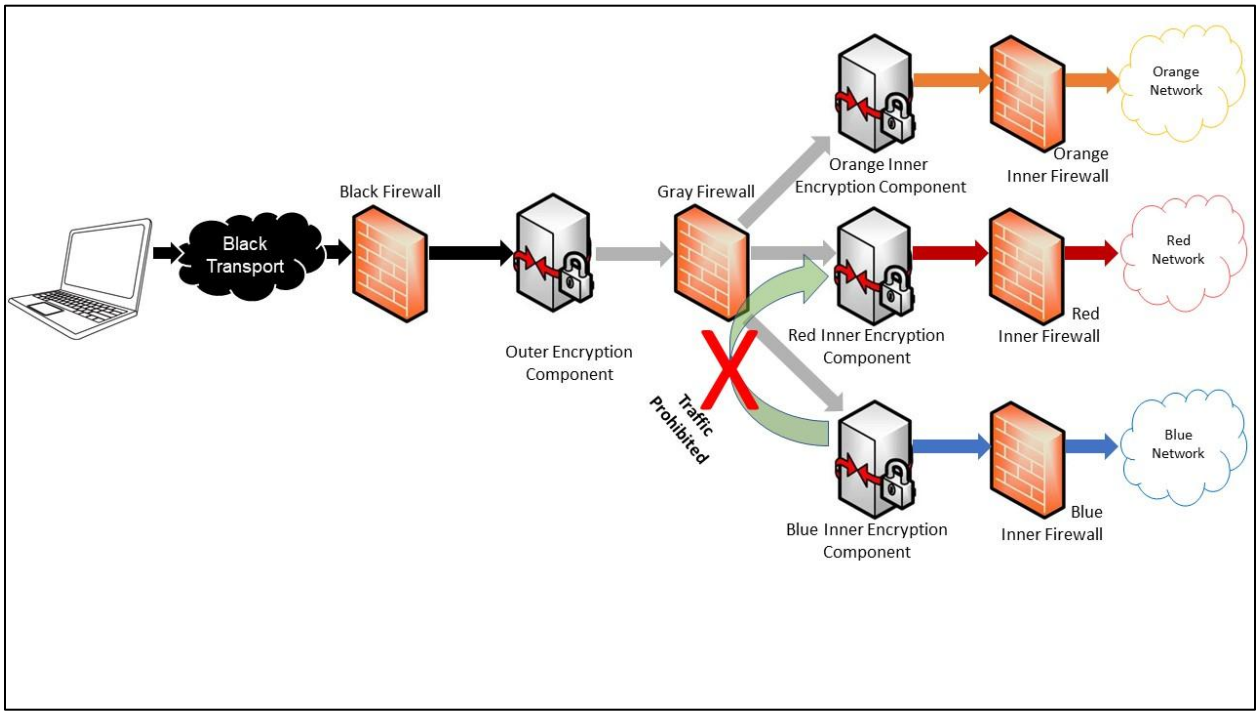

Figure 3. Multiple Inner Classification Prohibited Traffic

3.1.4 GRAY FIREWALL/ENCRYPTION COMPONENT – 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 4). 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.

3.1.5 GRAY FIREWALL/ENCRYPTION COMPONENT – 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.

3.1.6 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.

3.1.7 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.

The EG Annex provides guidance to customers deploying multiple CP solutions physically located outside of a secure government facility in tactical environments. Given an increase in accessibility, potential threats cause a need to continuously monitor network traffic and system log data within the solution infrastructure. This monitoring allows customers to detect, react to, and report any attacks against their solution in addition to detecting any configuration errors within infrastructure components. At a minimum, this annex requires alerts, events, and system logs to be sent back to a SIEM at a centralized operations center to facilitate continuous monitoring of the solution on a daily basis. This minimum review period allows customers in tactical environments to implement solutions in situations where it may not be feasible to perform real-time local monitoring and analysis. For more information and requirements for deploying continuous monitoring into a CSfC solutions see the relevant CP(s) being implemented.

3.1.8 GRAY AUTHENTICATION SERVER

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 4, the Gray Management authentication server is also required for the centralized management of Gray Services between the Management Site and Remote Sites.

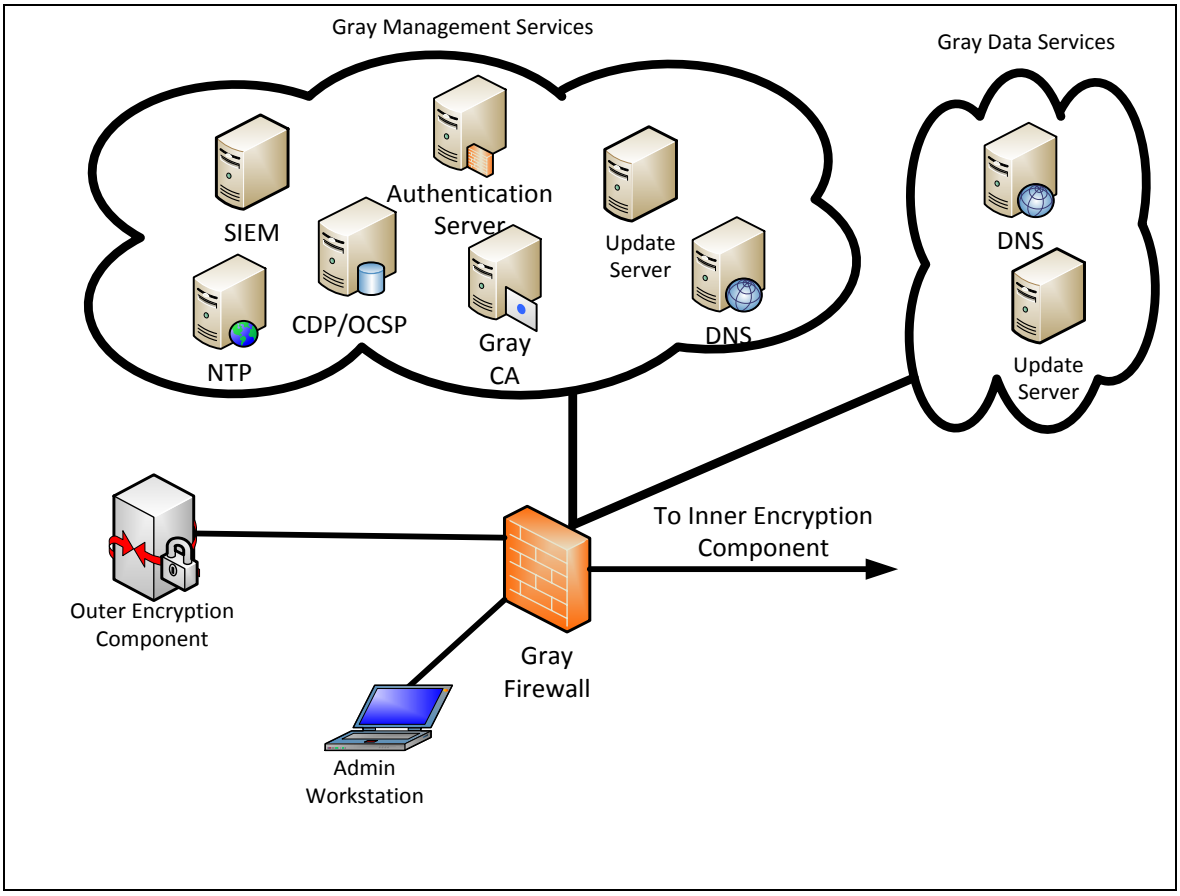

Figure 4. Gray Management and Data Services

3.1.9 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.

3.1.10 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.

3.2 GRAY CERTIFICATE AUTHORITY AND REVOCATION STATUS SERVICES

The CA for Outer and Gray Encryption Components may be located on a Gray Management Network, connected to the Encryption Components, or offline on the Red Network. A Certificate Policy and Certification Practice Statement document must be created or tailored for each CA in the Solution. It is the AO's responsibility to approve the use of a CA. If an Outer Tunnel CA is an Enterprise CA already running on the necessary Gray Management Network, then no additional approvals are necessary. It is important to note that no single CA may provide the public key to both Inner and Outer Encryption Components. Since the Gray Encryption Component that creates the secondary tunnel for Gray Services across an untrusted network resides on the Gray Network, its certificate can be signed by the Gray CA.

Each Encryption Component has at least one CA signing certificate (sometimes referred to as a Trust Anchor) to authenticate clients and other Encryption Components within the Solution. When centralized management is used, each Encryption Component has only one CA signing certificate. Otherwise, one CA signing certificate is installed on each Inner Encryption Component for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate is installed on each Outer Encryption Component for each Outer Tunnel CA used in the system.

3.3 Certificate Revocation List Distribution Point and Online Certificate Status Protocol

A Certificate Revocation List (CRL) Distribution Point (CDP) is a web server that hosts CRL files for Encryption Components to verify the validity of EUD certificates before allowing a connection to the network. A solution may use CDPs to provide CRLs to Encryption Components before those Encryption Components have established any VPN tunnels. CDPs should be placed on the network reachable from the Encryption Component's internal interface, or on the Gray Network for the Outer Encryption Component(s), and on the Red Network for the Inner Encryption Component(s).

The Online Certificate Status Protocol (OCSP) allows applications to determine the revocation state of a certificate. OCSP is more efficient than CRLs because it checks the status of a single certificate eliminating overhead for certificate checking. To avoid needless network traffic, applications should verify the signature of signed data before asking an OCSP client to check the status of certificates used to verify the data. If the signature is invalid or the application is not able to verify it, the OCSP client must not send a status request to the OCSP responder. An acceptable response is the accurate data exchanged between the application checking the status of the certificate and the server providing the status.

4 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.

4.1 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 solution 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)

4.1.1 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.

4.2 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 IKE/IPsec, TLS or MACsec traffic to the Outer Encryption Component to travel over its encrypted tunnel. Figure 5 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.

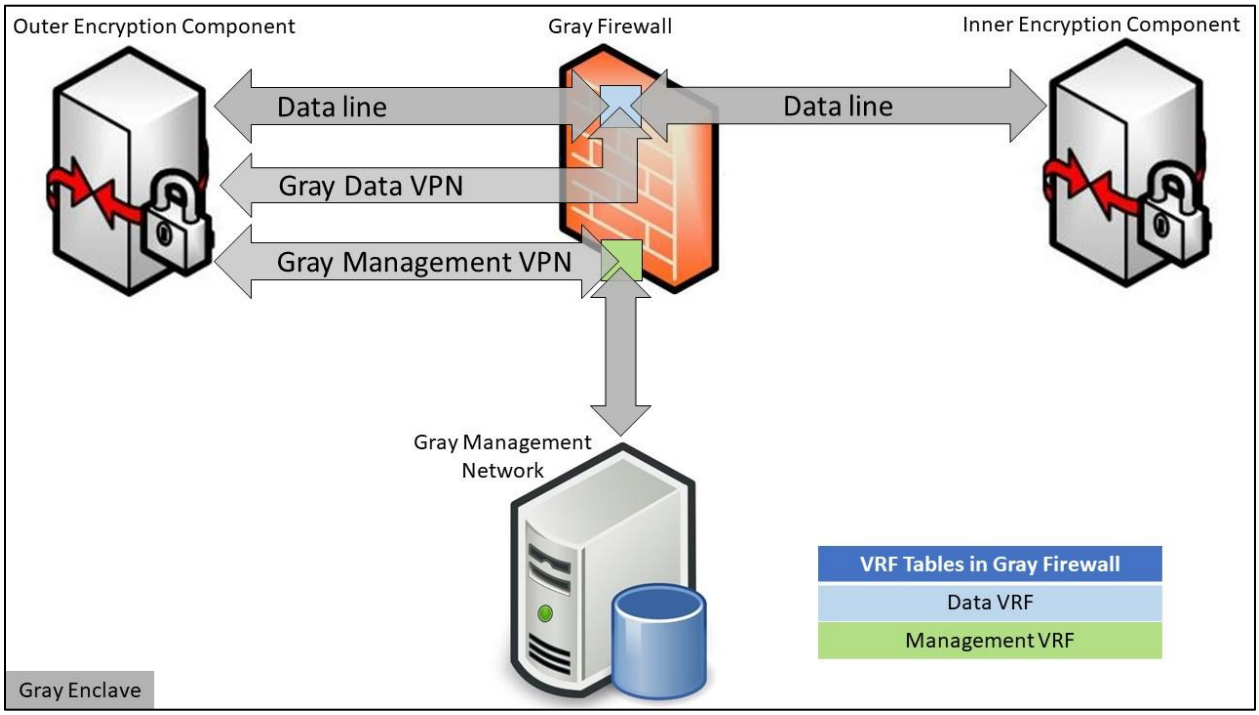

Figure 5. Dynamic Routing

4.3 AUTHORIZED PORTS, PROTOCOLS, AND INTERNET PROTOCOL ADDRESSES

4.3.1 BLACK NETWORK

As shown in Figure 6, 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.

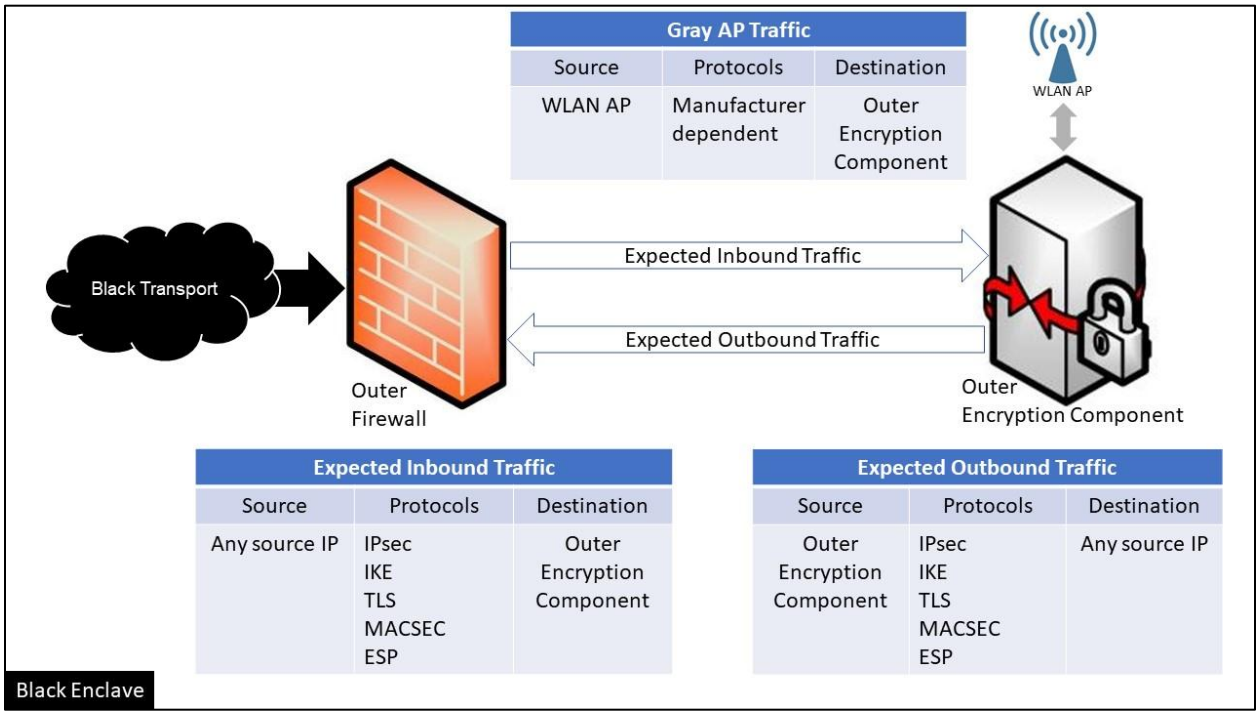

Figure 6. Authorized Protocols on Black Network

4.3.2 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 (see Figure 7). 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 7).

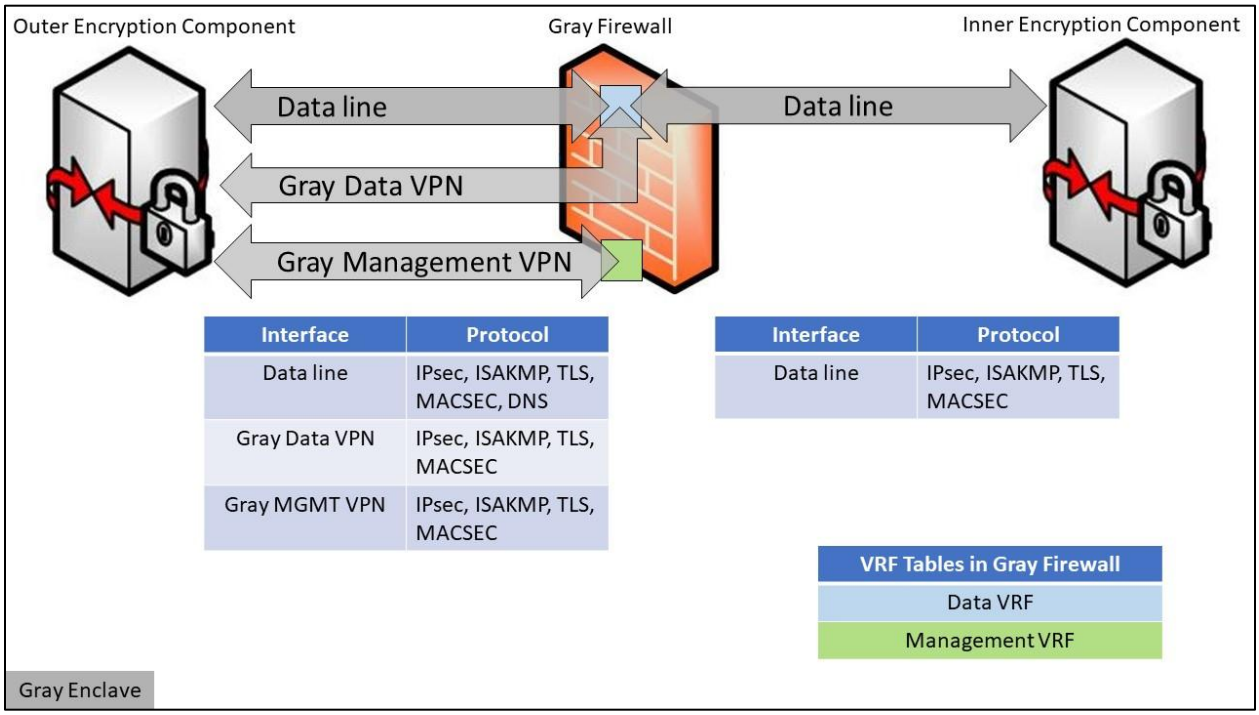

Figure 7. Authorized Protocols on Gray Network

5 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.

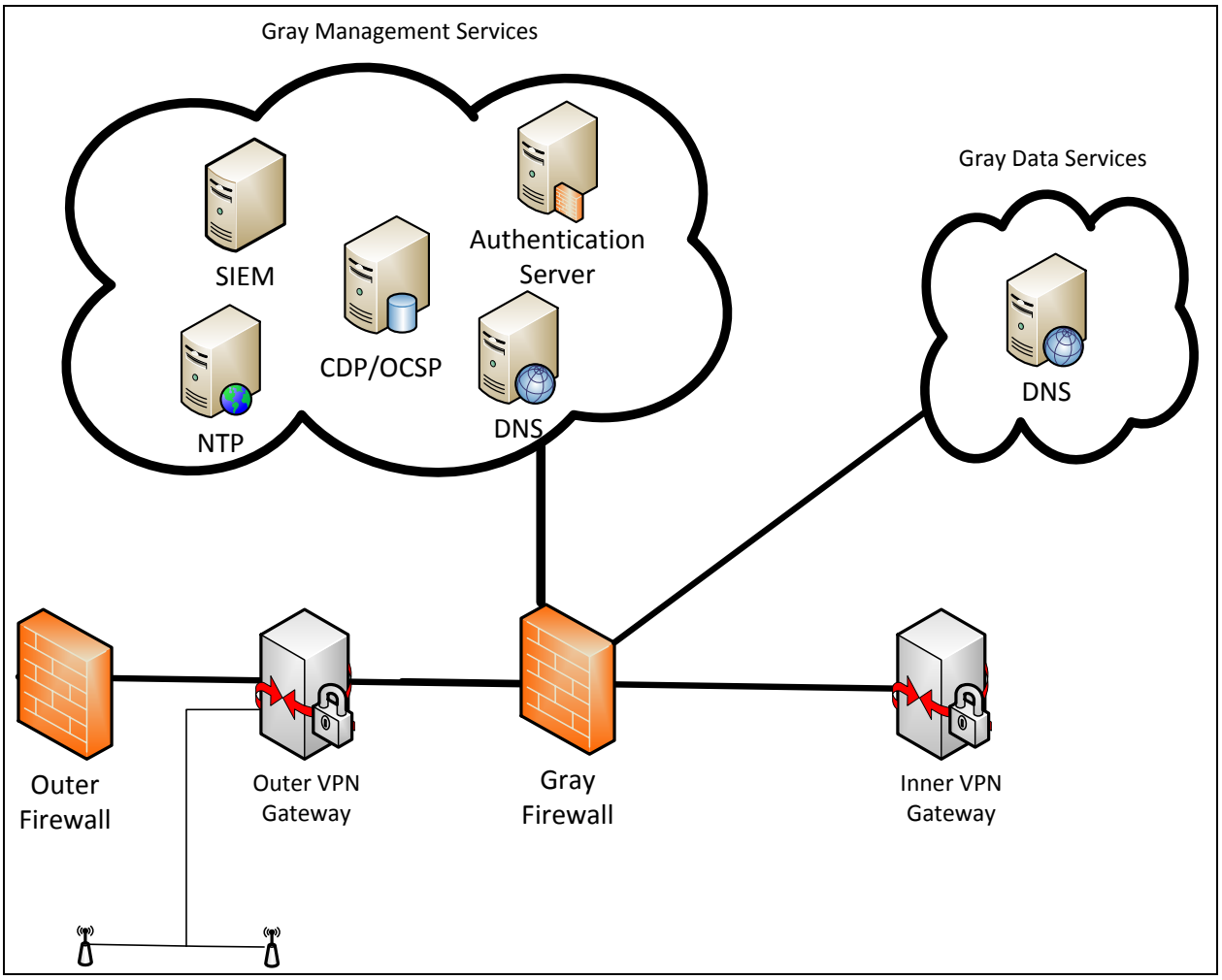

Figure 8. Minimum Services Needed for Site Survivability

6 REQUIREMENTS OVERVIEW

Sections 6.1 through 6.3, 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 1.

Table 1. 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.

6.1 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.

6.2 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 4 through 8. Each table represents a core capability of the *Enterprise Gray Implementation Requirements Annex*.

Table 2. Requirements Digraph

Digraph	Description	Section	Table
FW	Gray Firewall/Encryption Components Requirements	6.3	Tables 4-8
DR	Dynamic Routing	6.3	Tables 4-8
AR	Additional Requirements	6.3	Tables 4-8

6.3 Gray Firewall/Encryption Component and Additional Requirements

Table 3. Gray Firewall/Encryption Component IPsec Encryption (Approved Algorithms for Classified)

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	Advanced Encryption Standard (AES)-256	FIPS PUB 197 IETF RFC 6379 IETF RFC 6380

Security Service	Algorithm Suite	Specifications
Authentication (Digital Signature)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 IETF RFC 4754 IETF RFC 6380 IETF RFC 7427
Key Exchange/Establishment	ECDH over the curve P-384 Diffie Hellman (DH) Group 20 Or DH 3072	NIST SP 800-56A IETF RFC 3526 IETF RFC 5903 IETF RFC 6379 IETF RFC 6380 IETF RFC 7296
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6379 IETF RFC 6380

Table 4. 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


Enterprise Gray Implementation Requirements Annex

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
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 is authorized to only use SSHv2, IPsec, or TLS with the appropriate CNSA.	T=O		All
EG-FW-7	The Gray Firewall must permit IKE, IPsec, or TLS traffic between EUDs and Encryption Components protecting networks of the same classification level.	T=O		All
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 RFC 5280 or OCSP Response per RFC 6960 and block all other HTTP responses.	O	EG-FW-8	All
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

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
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 maintain the authenticity and integrity of the domain record to clients.	O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
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

Table 5. 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
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	T=O		WLAN

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	solution and not used to access any resources other than the Red Network it communicates with via two layers of encryption.			

Table 6. 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		All
EG-FW-18	The Gray Firewall/Encryption Component and the Outer Encryption Component must use different cryptographic libraries.	T=O		All
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 (e.g. Generic Routing Encapsulation), authorized TLS deployment, or MACsec.	T=O		All


Enterprise Gray Implementation Requirements Annex

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
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.		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 Gray Services to other site(s) over an untrusted network.	T=O		All
EG-AR-12	The Gray Firewall/Encryption Component must use the same Root CA as the Outer Encryption Component for authentication	T	EG-AR-11 or EG-AR-12	All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	of the Gray Management and Gray Data VPN Tunnels.			
EG-AR-13	The AO may deem that the Gray Firewall/Encryption Component must be a different Root CA than the Outer Encryption Component for authentication of the Gray Management and Gray Data VPN Tunnels.	O	EG-AR-10 or EG-AR-12	All
EG-AR-14	The AO may deem that the Gray Firewall/Encryption Component must use a long PSK instead of certificate based authentication for the Gray Management and Gray Data VPN tunnels. See the *CSfC Key Management Requirements Annex* for more information.	O	EG-AR-10 or EG-AR-11	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

Table 7. 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

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
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		All
EG-DR-5	If dynamic routing protocols are used, all network devices participating in dynamic routing message authentication must use a strong network PSK, which meets all requirements of the *CSfC Key Management Requirements Annex*.	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 for every network device which meets all requirements of the *CSfC Key Management Requirements Annex*.	O		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	T=O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	Networks to devices servicing the Gray Data VPN tunnels.			
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
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		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	T=O		All

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package
	local Gray Data network and remote Gray Data networks.			
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

Table 8. 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

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
MA	Mobile Access
MACsec	Media Access Control Security
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