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

Registration #

Solution Name:

Date Submitted

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 Approval for release

LIST OF TABLES

Table 1. General Enterprise Gray Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	
EG-FW-12	The Gray Firewall's inward interface must deny all traffic that is not explicitly allowed.	T=O		All	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	O		All	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
	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	

Table 2. Multiple CP Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	

Table 3. Centralized Management Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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	
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	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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 of the Gray Management and Gray Data VPN Tunnels.	T	EG-AR-11 or EG-AR-12	All	
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	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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 4. Scalability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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		All	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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 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	T=O		All	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
	outbound routes stopping unauthorized routes from being received or shared and by default all routes must be blocked.				
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 local Gray Data network and remote Gray Data networks.	T=O		All	

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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 5. Site Survivability Requirements

Req #	Requirement Description	Threshold/ Objective	Alternative	Capability Package	Compliance (Explain how your solution meets the requirement)
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

Acronym	Meaning
SSHv2	Secure Shell, version 2
TLS	Transport Layer Security
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WLAN	Wireless Local Area Network