NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Continuous Monitoring Annex 2.0.0

DRAFT 1

Version 2.0.0 DRAFT 1
16 May 2025

CHANGE HISTORY

Title	Version	Date	Change Summary
Continuous Monitoring (CM) Annex	2.0.0 DRAFT 1	16 May 2025	• Added section for Dedicated Outer VPN Use Case and Requirements • Added section for Mobile Device Management (MDM) Use Case and Requirements • Added section for Virtualized EUD (VEUD) Use Case and Requirements • Added requirements across MPs with respect to Zero Trust, Attestation, and Automation capabilities • Moved MP1 as "Optional" in Table 4 • Added figure for Virtualized EUD data flow • Updated all figures • Other administrative changes
Continuous Monitoring (CM) Annex	1.1.0	2 March 2023	• Added Campus WLAN Tactical use case to the Tactical Appendix • Added requirement for logs and Monitoring Solution to be review at least once a week
Continuous Monitoring (CM) Annex	1.0	4 August 2021	• Initial release of CSfC Continuous Monitoring Annex

DRAFT

Table of Contents

DRAFT

DRAFT

Table of Figures

DRAFT

List of Tables

DRAFT

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA) Cybersecurity Directorate (CSD) publishes guidance to empower its customers to implement secure communications solutions using independent, layered Commercial-off-the-Shelf (COTS) products. This guidance is product-neutral and describes system-level solution frameworks documenting security and configuration requirements for customers or integrators.

CSD delivers guidance for customers implementing Continuous Monitoring (CM) capabilities of CSfC data in transit and data at rest solutions using approved cryptographic algorithms, and National Information Assurance Partnership (NIAP) evaluated components.

2 PURPOSE AND USE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 defines information security continuous monitoring as, "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organization risk management decisions." With respect to CSfC solutions, CM enables the following:

- Defines a baseline set of expected system and network behavior within a CSfC solution environment
- Detects improperly configured products within solutions to achieve a level of assurance sufficient for protecting classified data in transit and data at rest
- Analyzes system activities to identify unauthorized activity within a CSfC solution network

CM is implemented as part of a holistic, risk management and defense-in-depth information security strategy integrated into CSfC architectures. Organizations designing CSfC solutions and implementing CM capabilities should leverage the information gathered from CM capabilities to take appropriate risk mitigation actions as well as make cost-effective, risk-based decisions regarding the operation of CSfC systems.

The guidance provided in the CM Annex references architecture and corresponding high-level configuration information to help customers develop a CM solution to meet CSfC CM requirements. To implement a CM solution based on this guidance, all Threshold requirements, or the corresponding Objective requirements, must be implemented as described in Section 10.

The requirements in this document supersede existing CM requirements in published CSfC Capability Packages (CP). Future CP revisions will direct customers to this annex for CM implementation.

Please provide comments on the usability, applicability, and/or shortcomings of this guidance to an NSA Client Advocate and the CM guidance maintenance team at CSfC_CM_team@nsa.gov. Solutions adhering to this guidance must also comply with Committee on National Security Systems (CNSS) policies and instructions.

DRAFT

For any additional information on Cross Domain Solutions (CDS) contact the National Cross Domain Strategy Management Office (NCDSMO) at ncdsmo@nsa.gov.

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 purpose are disclaimed. In no event must the United States (U.S.) Government is 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, 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 U.S. 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 THE CONTINUOUS MONITORING SOLUTION

This CM Annex provides guidance for collecting and analyzing network and security data to enable CM within a deployed CSfC solution. Given CSfC's multi-layered approach to encryption, failure of one or more components may result in observable network or device behavior that significantly deviates from established baselines. For example, these deviations may manifest as unexpected protocols, port usage, packet size, Internet Protocol (IP) addresses, or anomalous events observed on an End User Device (EUD).

CSfC CM capabilities are designed with a multi-layer approach to compliment the functional architecture of a CSfC solution. CSfC CM solutions provide high visibility across the monitored network, allowing analysts to validate the operational status of encryption components by observing network activity before and after encryption points and within management networks.

Eight (8) distinct Monitoring Points (MPs) are defined within the CSfC CM architecture. These MPs are positioned in strategic locations across the Black, Gray, and Red Networks (see Figures 5, 6 & 7). Each MP represents a critical point within the CSfC infrastructure where monitoring capabilities grant visibility into system and network behavior. This does not necessarily represent a physical point where monitoring will be deployed. Customers have the flexibility to deploy solutions that will meet their needs.

DRAFT

An MP may be comprised of one or more monitoring capabilities. A monitoring capability is the implementation of a specific monitoring system that feeds data to collection, analysis, and notifying systems for CSfC solutions operators (see Section 5).

4.1 Monitoring Solution Overview

The monitoring solution provides high visibility across the network, allowing analysts to validate the operational status of encryption components by observing network activity before and after encryption points, within management networks, and at eight distinct but strategic monitoring points within the CSfC architecture. The monitoring solution provides observability of networks and systems, comprised of solutions such as Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) technologies that are pivotal in strengthening security operations, collection notifications, and network analysis. The monitoring solution:

- Comprised of one or more capabilities for analyzing and aggregating network traffic, system logs, and user behavior analytics to monitor environmental behavior
- Optionally within monitoring solutions, automated response to observed behaviors may be deployed to mitigate potential threats and risks posed to the CSfC network
- A robust monitoring solution provides views into CSfC systems and networks which enable administrators to observe and monitor system health and behavior to mitigate threats, misconfigurations, anomalies, or unexpected user and device activities
- Monitoring capabilities can include systems such as network traffic analyzers to include intrusion detection and prevention systems, centralized logging and security event management
- Popular implementations of such monitoring capabilities include products such as SIEM and SOAR solutions. These products enable administrator searching, reporting, and observation, and if configured, response within a CSfC network when properly configured and tuned

Comprehensive data collection and aggregation from each MP into centralized monitoring capabilities such as SIEM systems, provide security administrators with the capability to monitor data sources from within a network. SIEM solutions present security administrators with the collective data set to monitor the security posture of the CSfC solution and report on security-relevant events within the infrastructure. These tasks are often accomplished through a defined set of automated notification capabilities and dashboards built to identify targeted information of interest.

Expanding beyond SIEM management of CM data are SOAR systems to provide more robust management and remediation for events of interest. A SOAR enables security administrators to receive notable events, manage them through a case management system to enrich event data, evaluate potential root causes of events, and conduct triage and response activities that can be manually or automated and executed through playbooks. Event management can be further automated to remove the security administrator and allow for remediation to occur based on defined evaluation rules.

In addition to technical CM implementation, broader CM success relies on the implementation of site-specific policies and procedures for managing the CM infrastructure. Security administrators should have defined roles and responsibilities to review and generate timely, meaningful analysis of the data.

DRAFT

Organizations should have defined policies and procedures for managing findings and making sound risk-based decisions during incident response/remediation. The scope of this document does not delve into these components in detail. However, customers are expected to develop their own policies and procedures in accordance with local policies and Authorizing Official (AO) guidance.

The monitoring solution must also integrate Cyber Threat Intelligence (CTI) across SIEM, endpoints, network, cloud, and on-premises sources to support analytics (i.e., malware and social engineering threats), thus improving detection, investigation, and responsiveness.

4.1.1 Security Information and Event Management (SIEM)

Security Information and Event Management, or "SIEM" systems, are designed to collect, aggregate, correlate, and analyze security event data from CSfC components. Data should be sent to the SIEM from the following sources: hardware devices, virtual machines, security appliances, and software and services running within the solution network(s). Within a CSfC solution network, a properly configured SIEM can provide near real-time support for data-driven risk management decisions via reporting dashboards and security administrator querying capability across all data sources. The term 'SIEM' covers both proprietary and open-source solutions, which can be hosted within the solution boundary or on a separate network outside the solution boundary, protected at the highest security that the solution supports. When configured correctly, this functionality presents customers with a holistic view of the status of their solution network to detect anomalies and system events that may impact performance or security posture of the environment.

CSfC customers, integrators, and solution owners standing up new, or adding to existing SIEM capabilities, can expect the following benefits:

- Increased data confidentiality, integrity, and availability
- Greater visibility of security-related network events
- Improved network resilience, despite the ever-changing cyber threat landscape
- Easier tracking of hardware and software information technology assets throughout the enterprise
- Enhanced support for organizational change management processes

SIEMs enable a 'big picture view' for observing system and network behavior and defining thresholds for reportable events. Over time as event data is collected, security administrators should be able to better identify behavioral changes which may indicate a failure of security components, misconfiguration, subversion, or attempted subversion of implemented security controls.

SIEMs should provide notification when anomalous behavior is detected. Security administrators should monitor and review monitoring dashboards on a frequency determined by the AO or relevant governing policy. Automating notifications are recommended to enable security administrators to monitor metrics operating outside of expected thresholds. Thresholds should be reviewed on a continual basis as determined by their AO to verify compliance and adjust to operational risk decisions for their organization’s baseline controls.

Results from SIEM reporting mechanisms should directly support Incident Response activities for an organization. The metrics gathered and the ability to search through historical data should enable security administrators to readily review event data.

4.1.2 Security Orchestration, Automation, and Response (SOAR)

Expanding beyond passive monitoring solutions, additional monitoring capabilities should be considered by customers to improve response of generated notifications from monitoring solutions or other similar monitoring capabilities.

SOAR platforms provide the capability to expand customer’s CM environments to a reactionary environment and provide tools for managing event evaluation, enriching events to add additional context through threat intelligence feeds or other third-party data sources and applying necessary remediation actions. These remediation actions can be manually executed or automated through the application of playbooks.

Such evaluation and remediation can be fully automated where specified for each customer environment but it is not required. Examples of remediation actions may include updating firewall policies to isolate systems on the network, forcing disconnections or requiring reauthentication of services. By automating such responses, customers should be able to swiftly react and respond to reported events in a repeatable manner to mitigate against potential external and internal threats within the CSfC environment.

Implementation of a SOAR capability within an environment should provide benefits to more efficiently triage security events, automate remediation workflows where applicable, and reduce the Security Administrator’s workload to focus on higher priority reported security events. SOAR solutions can be comprised of one or more solutions working independently or in conjunction with each other to meet an organization’s automation and case management needs.

DRAFT

4.2 Gray Management Monitoring Solution

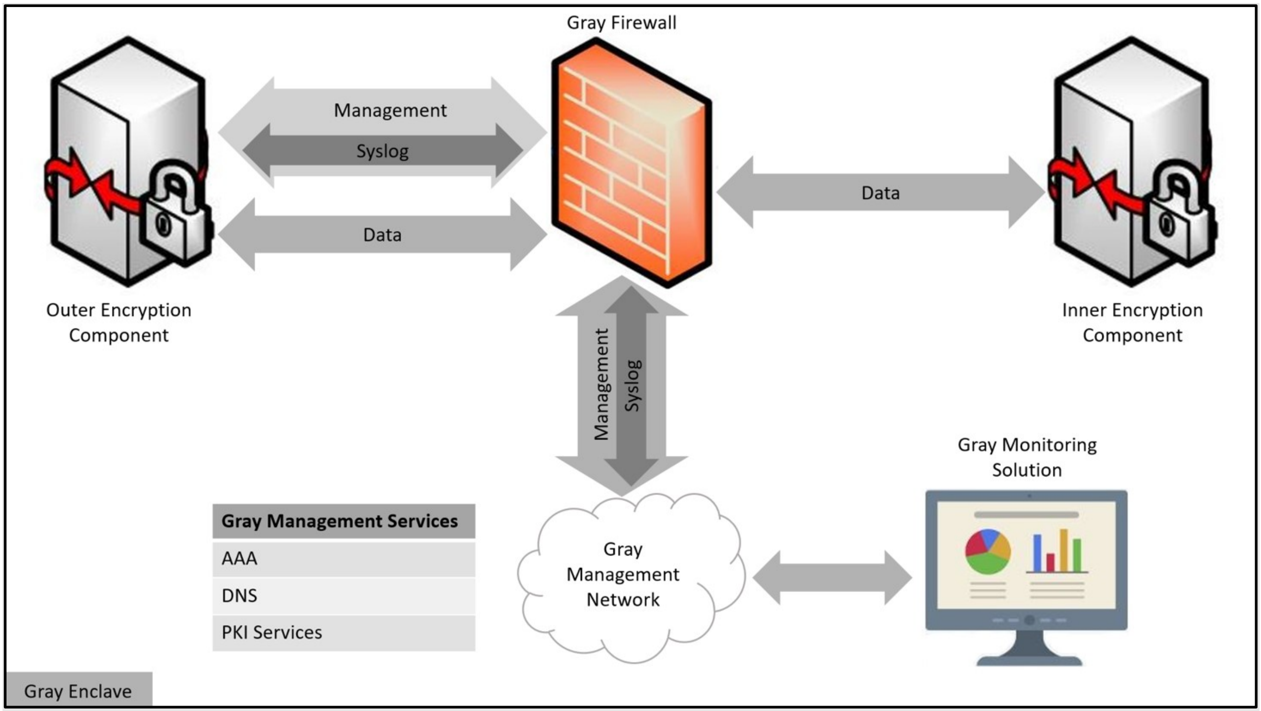


Figure 1. Gray Management Monitoring Solutions

The Gray Management monitoring solutions collect and analyze log and network monitoring data from the Outer Encryption Component, Gray Firewall, and other Gray Service components in both the Data and Management networks. Log data must be encrypted while traversing the Gray Network to maintain its confidentiality and integrity. Gray Management monitoring solution notifications must be reviewed at least once a week by a security administrator at a regular interval defined by the mission and approved by the AO or relevant governing policies.

The monitoring solution is configured to provide notifications for specific events. For example: if the Outer Encryption Component or Gray Firewall receives and drops any unexpected traffic, it could indicate a compromise of the Outer Firewall or Outer Encryption Component. A Gray Management monitoring solution may be used to aggregate log data from Black components when used in conjunction with an approved CDS (see Section 6.2). When an approved CDS is used, the data collected from Gray Network systems can be sent to the Red Network where these functions can be performed on a Red Management monitoring solution (see Section 6.3).

DRAFT

4.3 Red Management Monitoring Solution

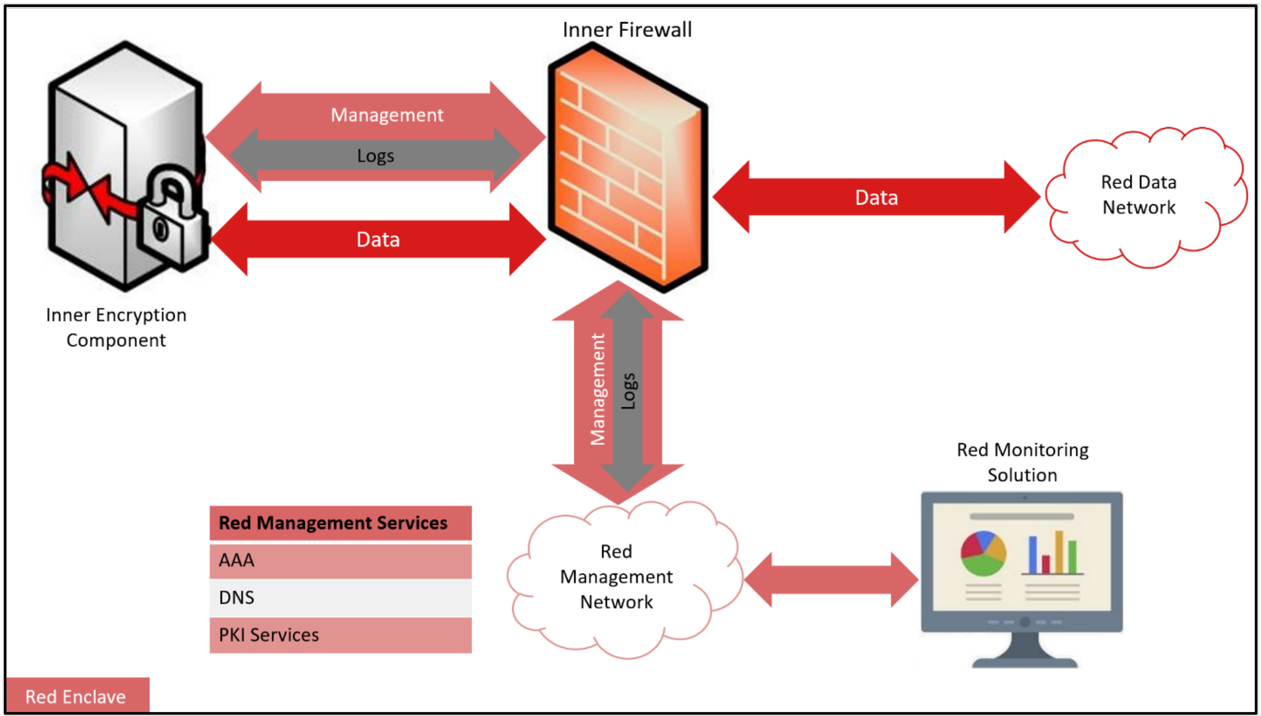


Figure 2. Red Management Monitoring Solution

DRAFT

The Red Management monitoring solution collects and analyzes log and network monitoring data from the Inner Encryption Component, Inner Firewall, and other Red Management Service components in both the Data and Management lines. Log data should be encrypted while traversing the Red Network to maintain confidentiality and integrity. Red Management monitoring solution notifications must be reviewed at least once a week by a security administrator at a regular interval defined by the mission and approved by the AO or relevant governing policies.

If available, customers are encouraged to leverage existing enterprise monitoring solutions if available within their network architecture. A Red Management monitoring solution may be used to aggregate log data from Black and/or Gray Network components when used in conjunction with an approved CDS (see Section 6.3).

4.4 Monitoring Data Sources

Data for the CM solution can be sourced from applications, networks, and security components, including but not limited to: Network Taps, network security monitoring tools such as Intrusion Detection System/Intrusion Prevention System (IDS/IPS), host-based security monitoring tools, network vulnerability scanning, system event logging, Wireless Intrusion Detection System (WIDS)/Wireless Intrusion Prevention System (WIPS), Device Health Attestation, or Integrity Verification processes. Network Monitoring Data is information about network traffic traversing the solution. This data can include full packet captures or meta-data about traffic, comprised of information gathered from Network TAPs, Port Mirrors, Network Flow, or IDS/IPS.

Table 1. Monitoring Data Sources Overview

Monitoring Data Sources	Description
Network Tap	In-line “bump in the wire” which copies all network traffic. End targets for this data are typically a data collection server or IDS/IPS to monitor for unauthorized network traffic.
Port Mirroring	Configured on network devices, port mirrors duplicate network traffic on the device to a destination on a specified network port. Provides similar functionality as a Network Tap.
Network Flow	Network protocol providing IP traffic information for monitoring purposes.
System Logging	Local system event logging functionality providing logs generated from services such as application, security, and host operating systems.
Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)	A device or software application that monitors a network or system for malicious activity or policy violations. Includes network-based Intrusion Detection System (IDS) and host-based IDS solutions.
Network Scanning	The collection of tools providing Vulnerability and Network Scanning capabilities.
WIDS/WIPS	A component or group of components that monitors the WLAN Access System wireless connects for malicious activity or policy violations.
Device Health Attestation	The process for providing a digital signature for a set of security measurements stored on a system, and then having the requester validate the signature and the set of measurements.
Integrity Verification	Methods to obtain assurance that information has not be altered in an unauthorized manner since it was created or stored.

Network Taps are standalone devices deployed within an infrastructure to copy all network traffic, known as raw network traffic, and send to another system for analysis and retention. Network Taps are most useful when integrated with an IDS/IPS to provide real time monitoring, inspection, and notification generation on unexpected or anomalous network traffic. Network tap data can be stored on a collection server or monitoring solution to maintain a history of all network activity. For customers implementing network taps, consideration may be made for a solution using Cyber One-Way Tap or an NSA evaluated diode to transmit directly to higher classification networks from these tap points. This option enables consolidation of network data without requiring the data flow to transmit through a CDS to monitoring solutions analyzing the data. Cyber One-Way Taps must be compliant with the NCDSMO document "Cyber One-Way Taps Technical Requirements" v1.0 or higher and deployed within the manner described in this document. This document can be obtained by emailing the NCDSMO at ncdsmo@nsa.gov.

Port mirroring provides a similar capability as a Network Tap. However, this functionality is deployed on network devices versus standalone devices. Network devices implementing port mirroring include both physical and virtual switching devices. A port mirror capability should direct traffic to a dedicated port mirror interface on a collection server, monitoring solution or IDS/IPS. When considering implementation of this capability, customers should assess their expected network volumes to ensure port mirroring can be reliably performed.

DRAFT

Network flow data (e.g., NetFlow, J-Flow, IPFIX, NetStream) is generated from network devices, such as routers, switches, and standalone probes. Network flow data provides characterization of network traffic flow that includes information such as IP protocols, source and destination IP addresses, source and destination ports, and traffic volume on a per-session basis. Conducting analysis of network flow data requires establishing a baseline for network behavior, updating it on a continual basis, and developing triggers for notification generation when customer-defined thresholds have been exceeded. Network flow data should be reviewed continuously to identify anomalies such as systems generating excessive amounts of traffic, devices trying to connect to improper IP addresses, and clients trying to connect to closed or undefined ports.

System logging capabilities are broad and include operating system, application and security relevant events, generated health and status notifications, and any other data generated by a system. Granularity needs of system logging may vary from customer to customer. Customers should become familiar with system logging severity levels to determine what level of logging is appropriate for their monitoring needs. To protect the confidentiality and integrity of the data, all system logging data should be encrypted with Secure Shell (SSH), Transport Layer Security (TLS), Internet Protocol Security (IPsec), Media Access Control Security (MACsec), or Datagram Transport Layer Security (DTLS) when sent to the collection server. If a component does not allow or perform the function, then it is considered compliant with the logging requirement.

EUDs can be configured with host-based solutions, often referred to as endpoint detection systems or endpoint applications. To complement system logging, endpoint detection systems allow for the collection of endpoint and network events to analyze and detect whether an anomalous activity is present. Endpoint solutions may provide local notification and technical preventative actions in the event of such anomalous activities. Where technically and programmatically feasible, customers should send relevant endpoint analytics back to a central collection system within the enterprise for correlation and analysis.

An IDS monitors network behavior or systems for malicious activity or policy violations. IDSs are implemented in one of two configurations: either they receive network traffic from a Network Tap or port mirror interface or are deployed inline on the network. IDSs should be configured to generate notifications when unknown or unexpected traffic is observed. A complementary technology to an IDS is an Intrusion Prevention Systems (IPS). An IPS carries out automated actions such as dropping malicious packets, blocking traffic, or resetting connections using signature-based and/or statistical anomaly detection in addition to the functions provided by an IDS.

Network Scanning tools encompass a suite of solutions performing Vulnerability Scanning and Network Device enumeration. These systems allow continuous scanning of systems within a network to search for known vulnerabilities, document system configurations to validate configuration compliance or identify unexpected systems connected to the network.

A WIDS monitors the behavior, infrastructure, and clients of a WLAN Access System for malicious activity or policy violations. WIDS should be configured to generate notifications when unknown or unexpected events are observed. A complementary technology to WIDSs is a WIPS. A WIPS carries out automated actions such as dropping malicious clients blocking unauthorized clients or resetting connections to the

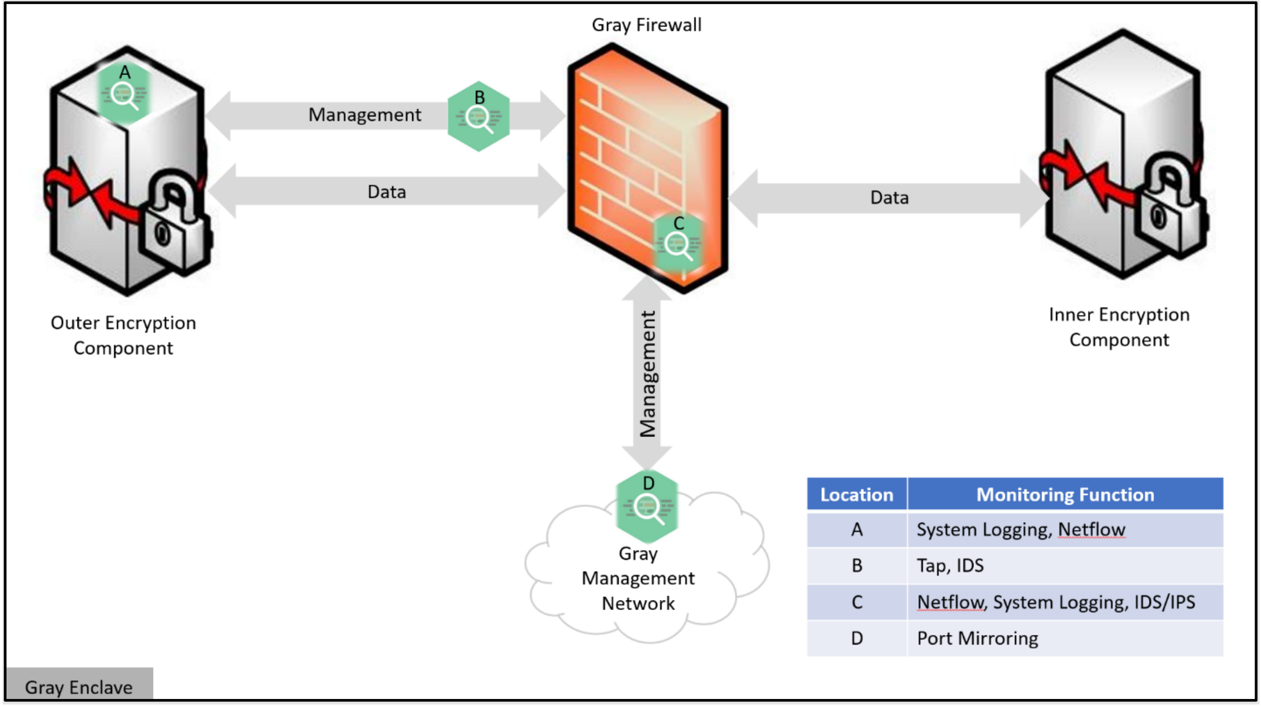
DRAFT

WLAN Access System using signature-based and/or statistical anomaly detection in addition to the functions provided by a WIDS. For more information and requirements see *CSfC WIDS/WIPS Annex*.

Device Health Attestation (DHA) provides the capability to verify the status of an EUD's hardware and firmware status. This provides assurance that the device is operating in a known and trusted state either as a requirement for certain actions or as a general periodic status check. Storage of device health credentials should be protected by appropriate hardware or software-based solutions such as a Trusted Platform Module (TPM) or Virtual TPM. Managing DHA can be accomplished through a variety of methods to include Mobile Device Management (MDM) systems and dedicated health monitoring reporting services.

Integrity Validation provides a broad set of capabilities across which CSfC implementations can leverage validation of the operating environment of a EUD or service component. Integrity checking is a vital part of the assurance process of an information system. Considerations for the use of integrity validation checks include component configuration file verification, system state verification, container validation, and evaluating virtualized component status before execution. Integrity validation can be executed as part of run-time operations or prior to the execution of critical system functionality.

Figure 3 depicts an example of the monitoring data sources that a customer may consider for placement within a CSfC network architecture to collect relevant CM data.



Location	Monitoring Function
A	System Logging, Netflow
B	Tap, IDS
C	Netflow, System Logging, IDS/IPS
D	Port Mirroring

Figure 3. Examples of Monitoring Data Sources

4.5 Dataflow Model

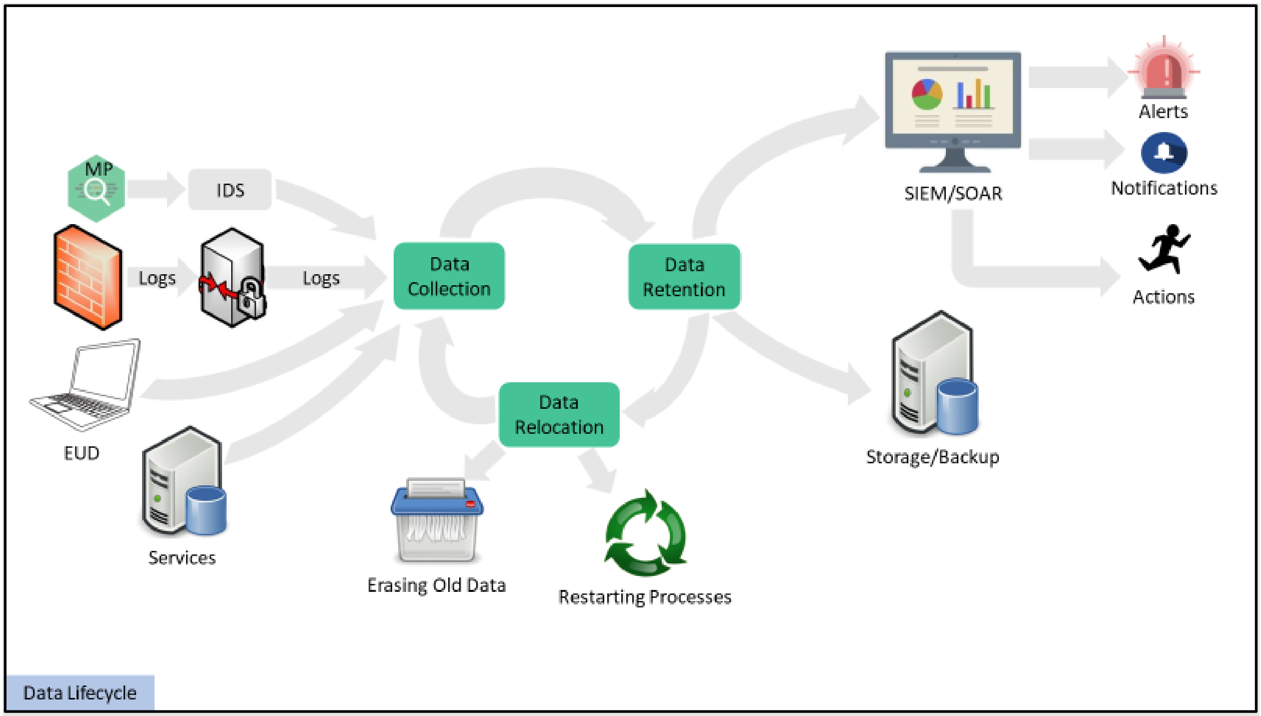


Figure 4. Data Lifecycle

The CM data lifecycle model is a process for which customers should define within their systems development, integration, and maintenance plans. This document defines the three primary activities within the CM lifecycle dataflow for integrator consideration. In addition to the below guidance, customers should consult their organization’s data governance policies for storing, maintaining, and aging off data used for monitoring purposes.

Data Collection

Collection of monitoring data within a CSfC solution takes many forms as referenced in Section 4.1. Consideration must be made to balance expected monitoring data collected against network bandwidth and available storage for monitoring data, especially for customers performing remote logging and centralized management functions. Appropriate logging levels required from network devices and services, EUDs, and other log-generating elements must be determined by customers’ requirements inclusive of meeting specified logging events as defined in the CM Requirements. Most network devices allow privileged users to configure logging facilities at different logging levels, such as ‘debug,’ ‘informational,’ and ‘warning’. Some logging levels repeat data or may prove to be overly verbose for customer needs. Superfluous information fills data storage and triggers data reallocation more frequently. Proper data hygiene is critical to maximizing available storage.

Data Retention

Data retained from collection activities should be backed up at regular intervals. Data can be aggregated in higher classification networks using an approved CDS. Data retention should be analyzed for data sent to CM collection points and local device storage. In the event network-based solutions fail, security

DRAFT

administrators must be able to fall back to local logging facilities to view event data. Retention policies must be defined in the data lifecycle plan as approved by the AO but is recommended to store logs for a minimum of one year.

Data Reallocation

A data reallocation strategy must be defined due to a limited capacity in data storage solution. To prevent processes from encountering completely full storage devices, old data should be erased at regular intervals and backed up per local data storage policies. In addition, processes should be restarted at regular intervals to flush memory, stop memory leaks, and clear temporary files. Older data that is no longer required to provide meaningful results to on-demand queries may be considered for longer term storage.

Consolidated Monitoring

The CM solution architecture is designed to maintain the separation of Black, Gray, and Red monitoring data within each security domain. Dividing monitoring data into discrete sectors presents challenges to track and correlate systems and network events across each of the domains. Also, it requires the implementation of separate infrastructure components to collect and manage monitoring data. Consolidated monitoring within CSfC is the process by which monitoring data is moved into a single environment to track and manage. This “single pane of glass” environment enables security administrators to monitor their infrastructure from a single location and reduce the monitoring footprint within the Black and Gray domains at the expense of implementations of data transfer solutions (see Section 6).

5 MONITORING POINTS

Each subsection below expands upon the intent of each MP and defines the scope of traffic transiting the MP, expected MP functionality, and types of notifications generated within each MP. MPs are a collection of one or more monitoring data sources (See Table 1). Each MP is designed to give visibility into a particular network segment and detect malicious activity or misconfigured components. Customers are required to implement MPs in accordance with Section 10.4. While all MPs are not required, customers are highly encouraged to deploy all MPs to provide the most comprehensive coverage for monitoring system and network activity across the CSfC solution.

The diagrams that follow, reference MP placement for each CSfC CP solution.

DRAFT

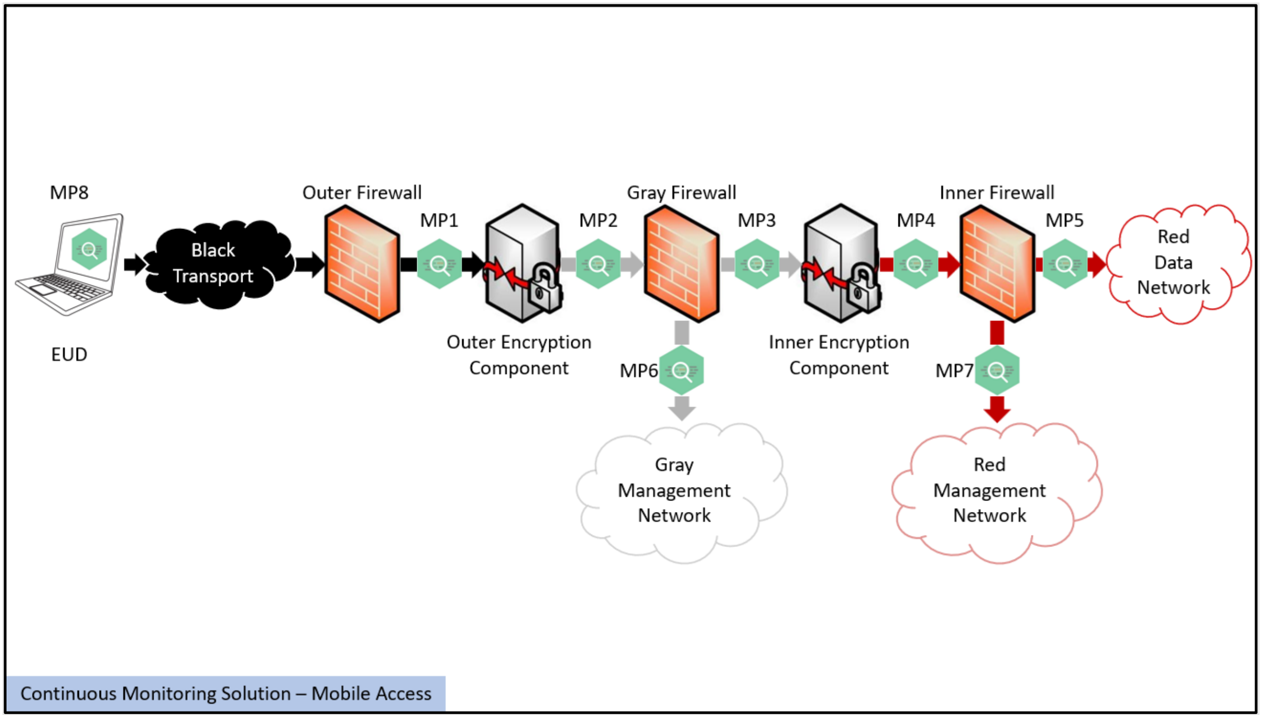


Figure 5. Continuous Monitoring Solution – Mobile Access CP

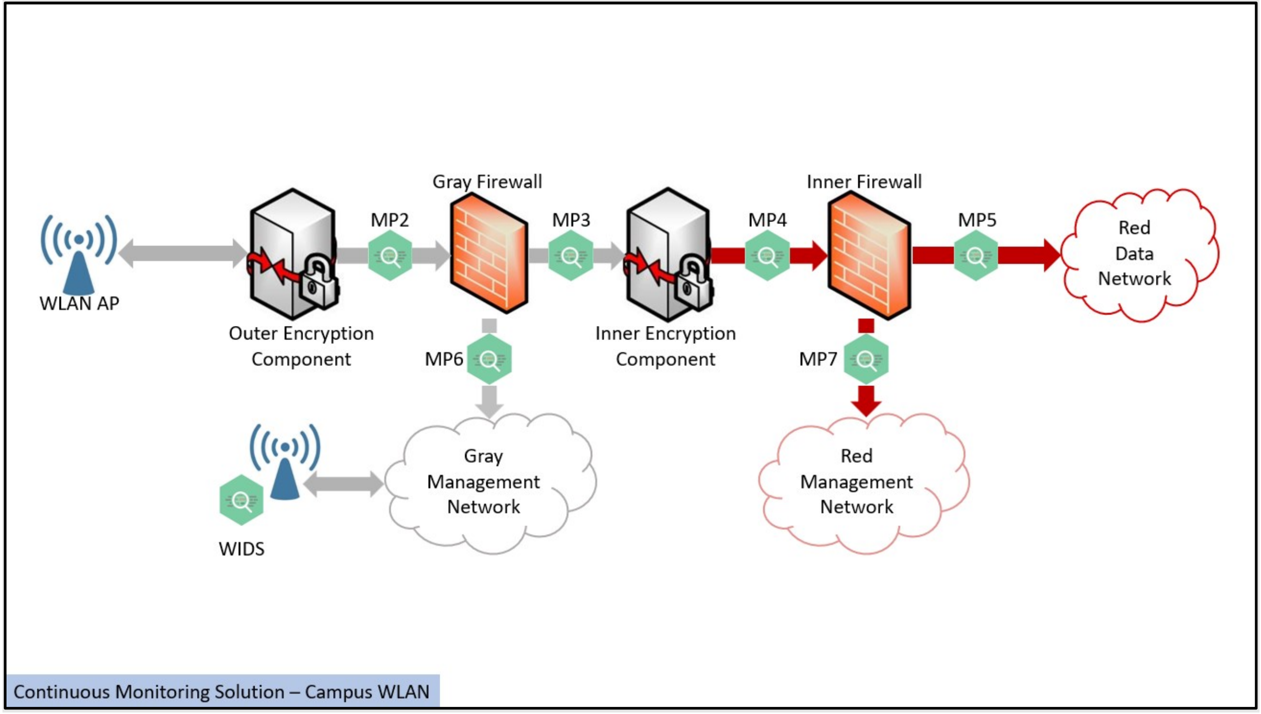


Figure 6. Continuous Monitoring Solution – Campus WLAN CP

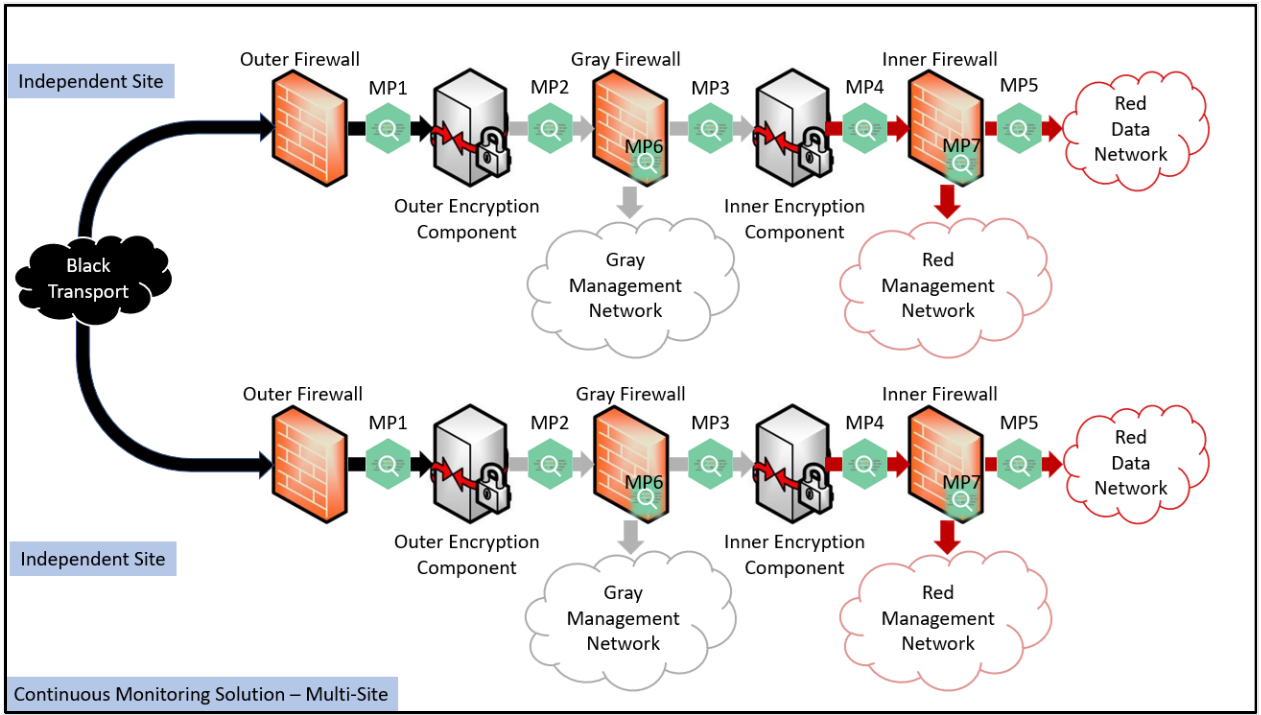


Figure 7. Continuous Monitoring Solution – Multi-Site Connectivity CP

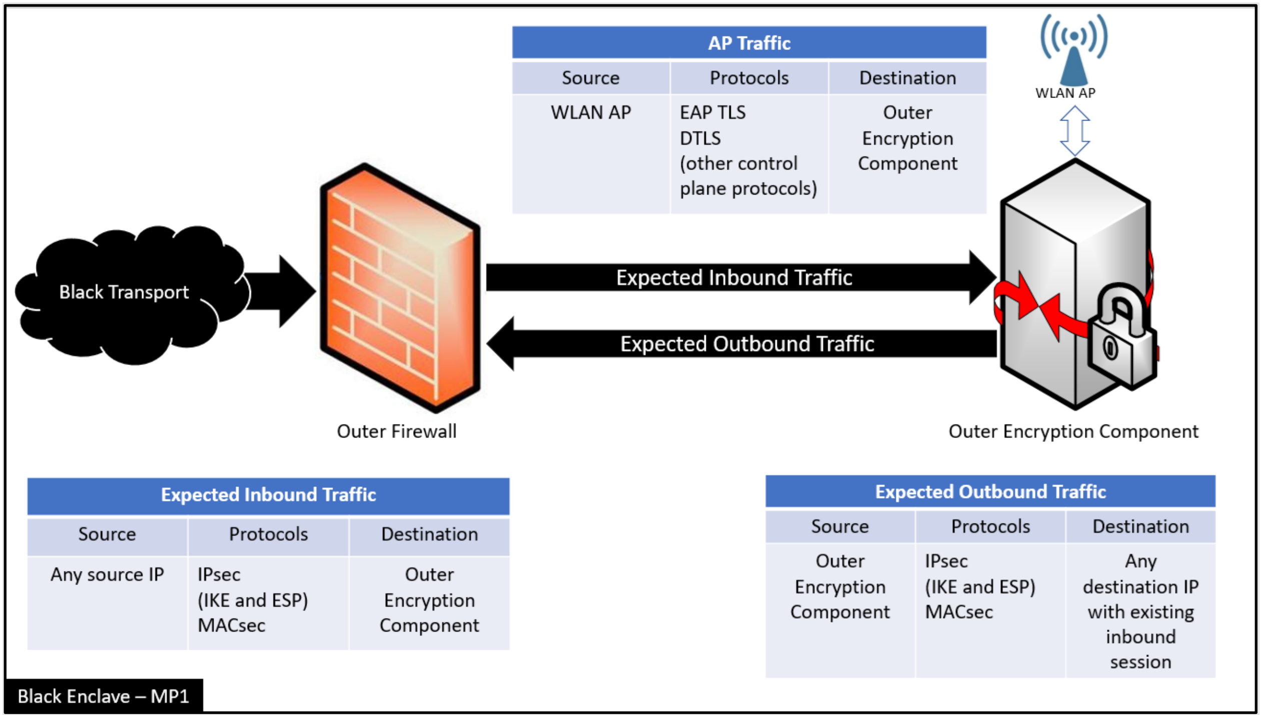
5.1 Monitoring Point 1 (MP1): Black Data Line

MP1 is located within the Black Network to monitor the data network between the Outer Firewall and Outer Encryption Component. The monitoring solution(s) should be configured to generate a notification upon detection of any traffic that should have been blocked by the Outer Firewall. These notifications may indicate a failure of the Outer Firewall's filtering functions and may be evidence of either an improper configuration, a potential compromise, or attempts to make unauthorized connections to the Outer Encryption Component(s).

The two key components within the Black Network segment are the Outer Firewall and MP1. The recommended solution receives data from both devices to the Black Network monitoring solution. In addition, network flow data from the Black Network can be collected from the Outer Firewall and sent to a Black Network collection server. The Outer Firewall may be a standalone component or if operating within an enterprise environment, a shared firewall providing services for multiple customer networks. If MP1 is implemented, then network monitoring data must be collected from the chosen monitoring solution.

Normal traffic at MP1 is well-defined. Traffic traversing the Outer Firewall to the Outer Encryption Component should be limited to ports and protocols required to support the outer encryption layer: IPsec, MACsec, and a limited number of control plane protocols as required per customer implementation. Inbound traffic should only be destined for the Outer Encryption Component IP address. All outbound traffic not matching preexisting inbound sessions should be blocked and only traffic sourced from the outer encryption IP address should be allowed.

DRAFT



AP Traffic		
Source	Protocols	Destination
WLAN AP	EAP TLS DTLS (other control plane protocols)	Outer Encryption Component

Expected Inbound Traffic		
Source	Protocols	Destination
Any source IP	IPsec (IKE and ESP) MACsec	Outer Encryption Component

Expected Outbound Traffic		
Source	Protocols	Destination
Outer Encryption Component	IPsec (IKE and ESP) MACsec	Any destination IP with existing inbound session

Figure 8. Monitoring Point 1: Black Data Line

Since nearly all traffic traversing MP1 is encrypted, network monitoring capabilities are generally limited to analyzing IP addresses, MAC Addresses, ports, protocols, and flow data. Management of MP1 components occurs within the Black Management Network or via local connections if no Black Management Network is implemented.

For customers implementing CSfC solutions operating Government owned Black Infrastructure, MP1 capabilities can optionally extend throughout the Black Network to include monitoring from the EUD to the infrastructure and throughout the entirety of the network path between client to server. Additional monitoring within the Black Infrastructure will not be considered applicable to meeting MP1 requirements but rather optional enhancements for customer assurances CSfC EUDs and Outer Encryption components are operating as expected.

Customers are encouraged to leverage existing enterprise monitoring capabilities, if available within their network architecture, to function as MP1 so long as their existing enterprise monitoring capabilities meet CSfC MP1 Requirements.

5.2 WIDS/WIPS

For Campus Wireless Local Area Network (WLAN) CP solutions, MP1 does not exist in the traditional sense as deployed in “Wired” CSfC CP in the Black Network Infrastructure. MP1 for WLAN solutions consists of Wireless WIDS capabilities within the wireless infrastructure. For more information and requirements for WIDS solutions see *CSfC WIDS/WIPS Annex*.

For MA CP solutions using the government private wireless a WIDS must be used to monitor the Wireless Access System. For more information and requirements on WIDS see *CSfC WIDS/WIPS Annex*.

DRAFT

5.3 Monitoring Point 2 (MP2): Gray Data Line

MP2 is located within the Gray Network to monitor the data network between the Outer Encryption Component and Gray Firewall.

Normal traffic at MP2 is not as narrowly defined as MP1, however a restricted set of traffic is expected. This set of traffic includes, but may not be limited to, IPsec, TLS, MACsec, data plane traffic encrypted with TLS or Secure Realtime Transport Protocol (SRTP), and customer defined control plane traffic (e.g., client Domain Name System (DNS) requests, Hypertext Transfer Protocol (HTTP) requests for Certificate Revocation List (CRL), Address Resolution Protocol (ARP), Spanning Tree Protocol (SPT). Source IP addresses from inbound client traffic should be restricted to assigned Outer Encryption IP address pools and destination IPs should be to Gray Data Network Services or Inner Encryption Components.

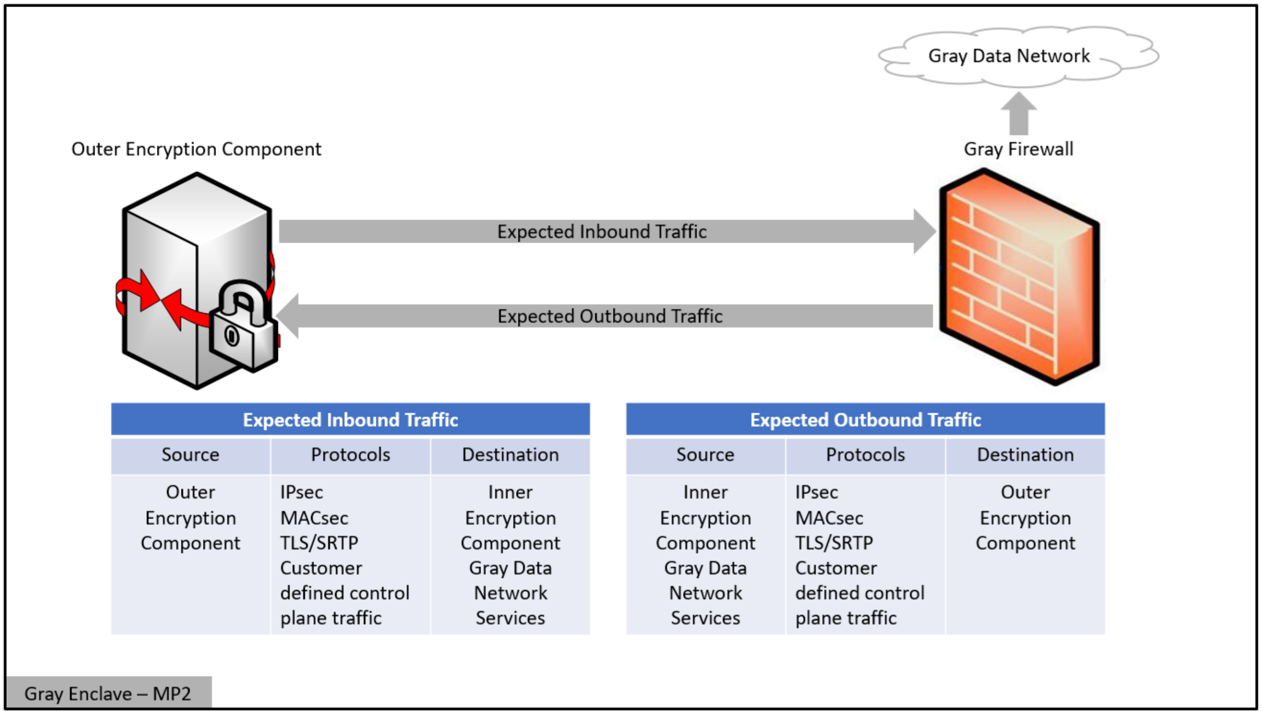
The monitoring infrastructure should be configured to generate a notification upon detection of any traffic that should have been blocked by the Outer Encryption Component or Gray Firewall. These notifications may indicate a failure of the Gray Firewall or Outer Encryption Component’s filtering functions and may be evidence of either an improper configuration or a potential compromise. All security event data must be sent to a collection server located within the Gray Management Network and may be fed into the monitoring solution.

If MP2 is implemented, network monitoring data must be collected from the chosen monitoring solution. Network flow data from the Gray Network should be collected from the Outer Encryption Component and Gray Firewall and sent to a collection server or monitoring solution in the Gray Management Network. If additional network devices are deployed between two these two components, it is recommended that network flow data be sent to the collection server or monitoring solution as well.

This method of data collection may aggregate data in such a way that MP2 and MP6 requirements may be satisfied. Customers should evaluate MP compliance when designing their monitoring architecture.

Management of MP2 occurs within the Gray Management Services Network.

DRAFT



Expected Inbound Traffic		
Source	Protocols	Destination
Outer Encryption Component	IPsec MACsec TLS/SRTP Customer defined control plane traffic	Inner Encryption Component Gray Data Network Services

Expected Outbound Traffic		
Source	Protocols	Destination
Inner Encryption Component Gray Data Network Services	IPsec MACsec TLS/SRTP Customer defined control plane traffic	Outer Encryption Component

Figure 9. Monitoring Point 2: Gray Data Line

DRAFT

5.4 Monitoring Point 3 (MP3): Gray Data Line

MP3 is located within the Gray Network to monitor the data network between the Gray Firewall and Inner Encryption Component(s).

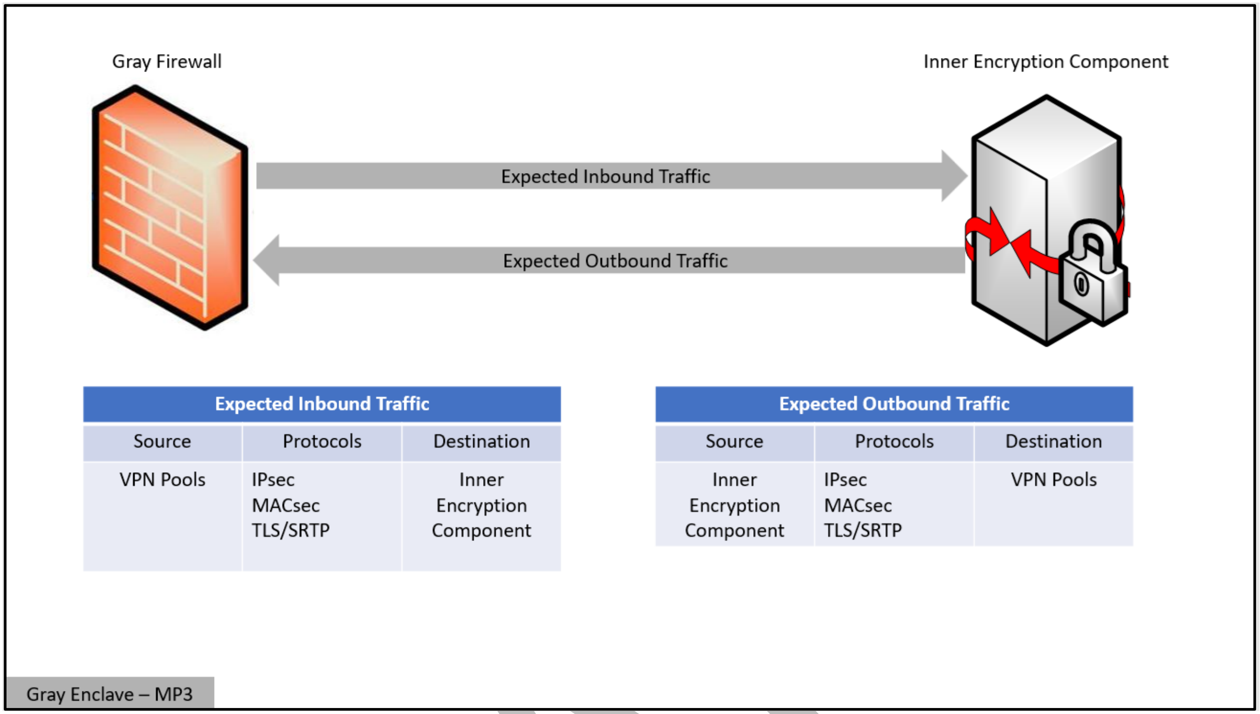
Normal traffic at MP3 should be a subset of data transiting MP2. Traffic observed at this MP should only include communications with the Inner Encryption Components. Types of traffic include IPsec, TLS, MACsec, data plane traffic encrypted with TLS or SRTP, and control plane traffic necessary for network health and management. Source IP addresses from inbound client traffic should be restricted to assigned Outer Encryption IP address pools and destination IPs should be to Inner Encryption Components.

The monitoring infrastructure should be configured to generate a notification upon detection of any traffic that should have been blocked by the Gray Firewall or sent by the Inner Encryption Component(s) that is not expected. These notifications may indicate a failure of the Gray Firewall's filtering functions and may be evidence of an improper configuration or a potential compromise of the Firewall or Inner Encryption Component. All security event data must be sent to the monitoring solution located within the Gray Management Network and may be fed into the Gray monitoring solution.

If MP3 is implemented network monitoring data must be collected from the chosen monitoring solution. Network flow data from the Gray Network should be collected from the Gray Firewall and sent to a collection server or monitoring solution in the Gray Management Services.

Nearly all traffic traversing MP3 is encrypted either with IPsec, MACsec, TLS, or SRTP, which prevents deep packet inspection of client data traffic.

Management of MP3 occurs within the Gray Management Network.



Expected Inbound Traffic		
Source	Protocols	Destination
VPN Pools	IPsec MACsec TLS/SRTP	Inner Encryption Component

Expected Outbound Traffic		
Source	Protocols	Destination
Inner Encryption Component	IPsec MACsec TLS/SRTP	VPN Pools

Figure 10. Monitoring Point 3: Gray Data Line

5.5 Monitoring Point 4 (MP4): Red Data Line

MP4 is located within the Red Network to monitor the data network between the Inner Encryption Component(s) and Inner Firewall.

Expected traffic for MP4 must be defined by the customer and should be limited to that required for end users to perform their mission. Ports, protocols, and destination IP addresses should be documented within the solutions registration package and implemented into Red Network security components to restrict traffic flow to allowed services only. Source IP addresses should be well-defined from the client IP address pool assigned by the Inner Encryption Component.

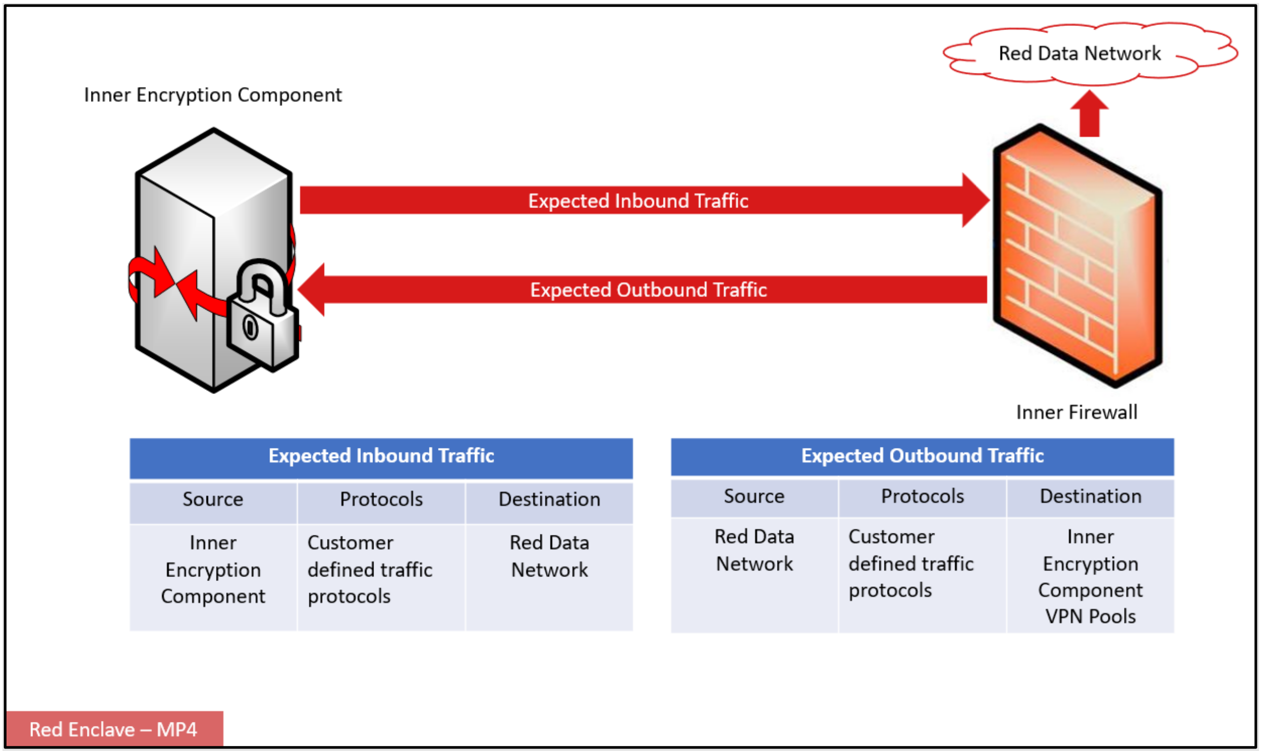
Monitoring capabilities should take into consideration the defined set of allowed traffic and develop appropriate reporting and notification mechanisms to identify anomalies within their network. The monitoring infrastructure should be configured to generate a notification upon detection of any traffic that should have been blocked by the Inner Encryption Component or the Inner Firewall. These notifications may indicate a failure of the Inner Encryption Component’s or Inner Firewall filtering functions and may be evidence of an improper configuration or a potential compromise. All security event data must be sent to the monitoring capability located within the Red Management Services Network and may be fed into the Red monitoring solution.

If MP4 is implemented network monitoring data must be collected from the chosen monitoring solution. Network flow data from the Red Network must be collected from the Inner Encryption Component and Inner Firewall and sent to a collection server or monitoring solution in the Red Management Network.

DRAFT

Deep packet inspection may be feasible for MPs deployed in the Red Network. The customer may consider deploying solutions to collect and analyze client traffic at this point in the network.

Management of the MP4 monitoring point occurs within the Red Management Services.



Expected Inbound Traffic		
Source	Protocols	Destination
Inner Encryption Component	Customer defined traffic protocols	Red Data Network

Expected Outbound Traffic		
Source	Protocols	Destination
Red Data Network	Customer defined traffic protocols	Inner Encryption Component VPN Pools

Figure 11. Monitoring Point 4: Red Data Line

5.6 Monitoring Point 5 (MP5): Red Data Line

MP5 is located within the Red Network to monitor the data network between the Inner Firewall and the Red Data network.

Expected traffic for MP5 must be defined by the customer and should be limited to those that are required for end users to perform their mission. Ports, protocols, and destination IP addresses should be documented within the solution’s registration package and implemented into Red Network security components to restrict traffic flow to allowed services only. Source IP addresses should be well-defined from the IP address pool assigned by the Inner Encryption Component.

Monitoring capabilities should consider the defined set of allowed traffic and build appropriate reporting and notification mechanisms for the security administrators to identify anomalies within their network. The monitoring infrastructure should be configured to generate a notification upon detecting any traffic that should have been blocked by the Inner Firewall or detecting unexpected traffic sent from the Red Network destined for the EUD or Inner Encryption Component. These notifications may indicate a failure of the Inner Encryption Component’s, or Inner Firewall filtering functions and may represent an improper configuration or a potential compromise. In addition, all security event data must be sent to the monitoring capability located within the Red Management Network and may be fed into the Red monitoring solution.

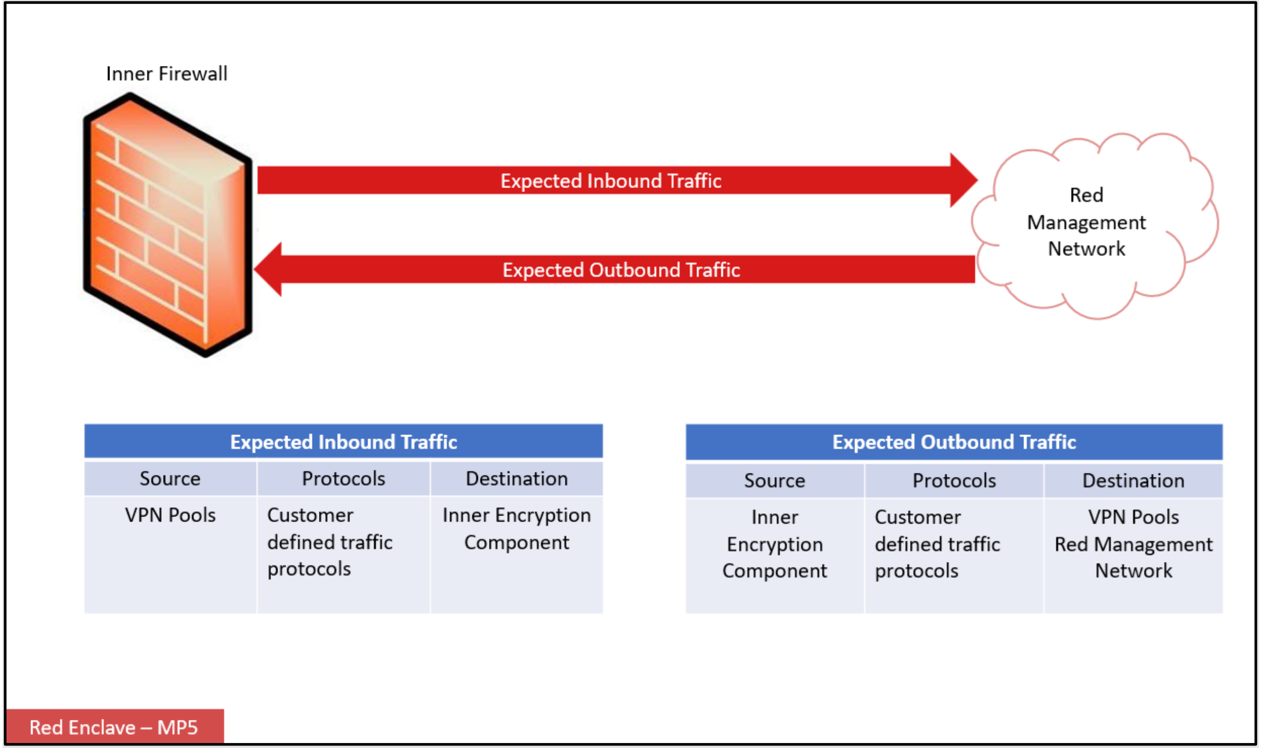
DRAFT

If MP5 is implemented, network monitoring data must be collected from the chosen monitoring solution. Network flow data from the Red Network must be collected from Inner Firewall and sent to a collection server or monitoring solution in the Red Management Network.

Deep packet inspection may be feasible for MPs deployed in the Red Network. The customer may consider deploying solutions to collect and analyze client traffic at this point in the network. Solutions such as proxies may be considered to inspect encrypted traffic at MP5 or within the Red Network. If deployed in MP5 it is recommended to configure notifications and analysis capabilities where feasible within the red monitoring capability.

Customers are encouraged to leverage existing enterprise monitoring capabilities if available within their network architecture to function as MP1 so long as their existing enterprise monitoring capabilities meet CSfC MP5 requirements.

Management of the MP5 monitoring point occurs within the Red Management Services.



Expected Inbound Traffic		
Source	Protocols	Destination
VPN Pools	Customer defined traffic protocols	Inner Encryption Component

Expected Outbound Traffic		
Source	Protocols	Destination
Inner Encryption Component	Customer defined traffic protocols	VPN Pools Red Management Network

Figure 12. Monitoring Point 5: Red Data Line

5.7 Monitoring Point 6 (MP6): Gray Management

MP6 is located within the Gray Management Network to monitor the management network deployed in the Gray Network. MP6 is required in all CSfC CM Solutions. The aggregate of data collected for MP6 must provide security administrators visibility of all network and system behavior on the Gray Management Network to meet specified MP6 requirements.

Data collected at MP6 may include but not limited to system log data, network flow data from the Outer Encryption Component and Gray Firewall, Network Tap traffic, IDS/IPS notifications, inline IDS/IPS traffic/notifications, and SPAN port or port mirroring. All traffic source and destination addresses should be within the subset of management network IP addresses. All monitoring data should be sent to the CM monitoring capability for aggregation and analysis. Gray Management Network traffic destined for the Outer Encryption Component, Gray Firewall, or other network devices (e.g., data switches) should be restricted for management access via defined protocols and ports to known IP addresses.

Monitoring capabilities in MP6 include Vulnerability Scanning Tools, Network Scanning Capabilities, and similar tools to monitor security posture and configuration compliance. Reports generated from these tools should be sent to monitoring solutions and reviewed on an AO defined interval. If existing enterprise capabilities for performing these scans are already deployed within customer sites, these solutions can be leveraged where available.

Monitoring solutions should be configured to generate notifications for non-expected traffic transiting the Gray Management Network, identify traffic that should have been blocked by the Gray Firewall, and enable security administrators to query system event log data for components connected to the Gray Management Network. Notifications generated in the Gray Management Network may indicate a failure of the Gray Firewall's filtering functions or may be evidence an improper configuration or potential compromise of the Outer Encryption Component, Gray Firewall, or Gray Management Network components.

Data Network traffic is forbidden on the Gray Management Network. Collection of EUD logs within the Gray Network must maintain separation unless transmitted using authorized data transfer mechanisms between the Data and Management networks (see Section 6).

Management of MP6 occurs from within the Gray Management Services.

DRAFT

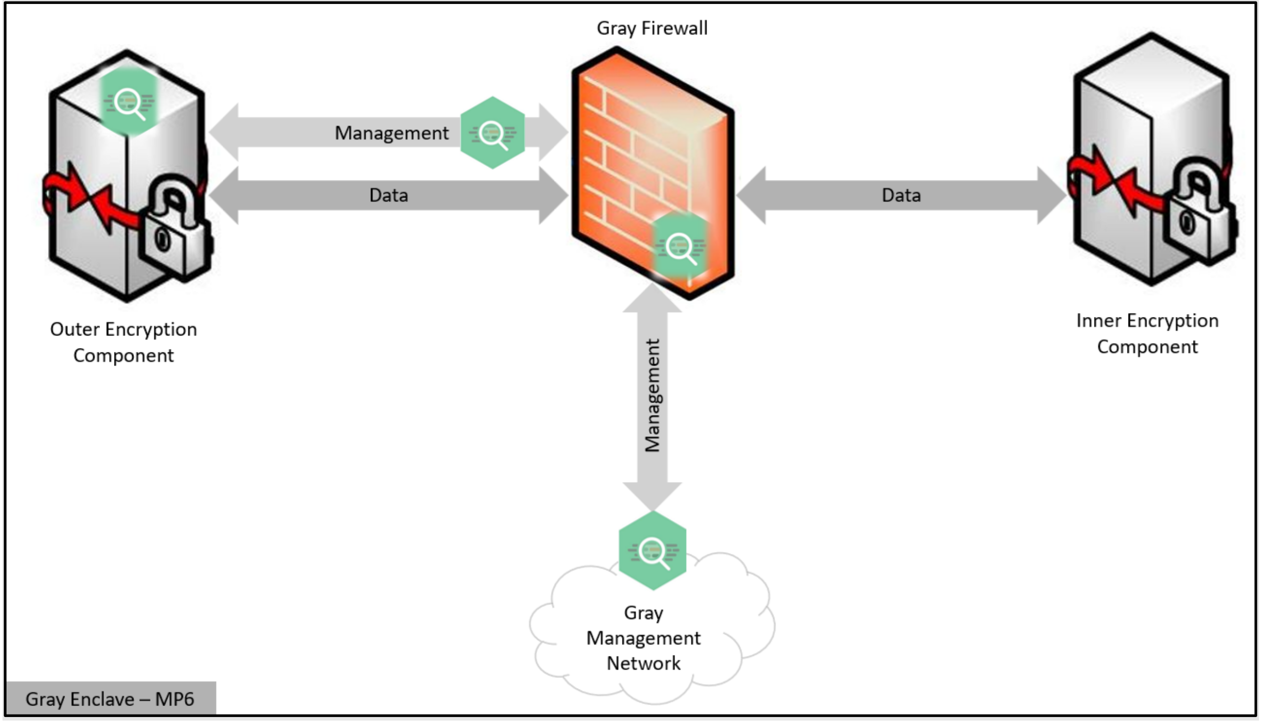


Figure 13. Monitoring Point 6: Gray Management Line

5.8 Monitoring Point 7 (MP7): Red Management

MP7 is located within the Red Management Network to monitor the management network deployed in the Red Network. MP7 is required in all CSfC CM Solutions. The aggregate of data collected for MP7 must provide security administrators visibility of all network and system behavior on the Red Management Network to meet specified MP7 requirements.

Data collected at MP7 may include but is not limited to system log data, network flow data from the Outer Encryption Component and Inner Firewall, Network Tap traffic, IDS/IPS notifications, inline IDS/IPS traffic/notifications, and SPAN port or port mirroring. All traffic source and destination addresses should be within the subset of management network IP addresses. All data should be sent to the data collection system and ultimately the monitoring solution for aggregation and analysis. If existing monitoring solutions are deployed within an existing Management Network within the Red Network, these solutions can be leveraged in place of deploying a separate solution for the CSfC monitoring solution. Red Management Network traffic destined for the Inner Encryption Component, Inner Firewall, or other network devices (e.g., data switches) should be restricted for management access via defined protocols and ports to known IP addresses.

Monitoring capabilities in MP7 include Vulnerability Scanning Tools, Network Scanning Capabilities, and similar tools to monitor security posture and configuration compliance. Reports generated from these tools should be sent to monitoring solutions and reviewed on an AO defined interval. If existing enterprise capabilities for performing these scans are already deployed within customer sites, these solutions can be leveraged where available.

Monitoring solutions should be configured to generate notifications for non-expected traffic transiting the Red Management Network, identify traffic that should have been blocked by the Inner Firewall, and enable security administrators to query system event log data for components connected to the Red Management Network. Notifications generated in the Red Management Network may indicate a failure of the Inner firewall's filtering functions or maybe evidence of an improper configuration or potential compromise of the Outer Encryption Component, Inner firewall, or Red Management Network components.

Data Network traffic is forbidden on the Red Management Network. Collection of EUD logs within the Red Network must maintain separation unless transmitted using authorized data transfer mechanisms between the Data and Management networks (see Section 6).

Management of MP7 occurs from within the Red Management Services.

DRAFT

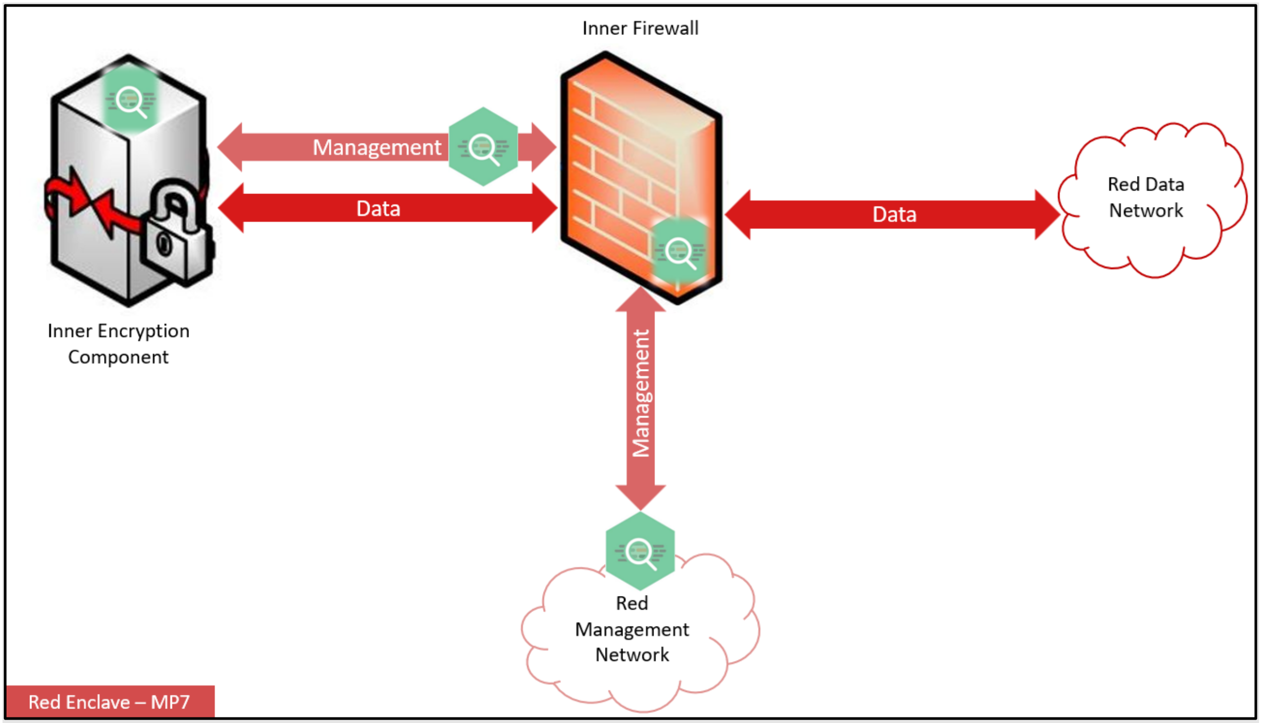


Figure 14. Monitoring Point 7: Red Management Line

5.9 Monitoring Point 8 (MP8): End User Device (EUD)

MP8 is located on the EUD and collects system, network, and application event log data from the device. Sources of EUD monitoring data include but are not limited to operating system event log data, Host Intrusion Detection System, Remote Attestation Solutions, Mobile Device Manager, Endpoint Detection and Response tools, Extended Detection and Response tools, and enterprise Data-at-Rest agents.

Implementation of MP8 capabilities is directly influenced by the EUD's form factor and system architecture designed to implement two layers of encryption. Given modern EUD solution designs, an EUD may be comprised of one or more physical, logical, or virtual layers providing Black Network transport, Gray Network access, Red Network access, and User Environment services. Considerations should be made by customers to consider the extent for which holistic event logging and monitoring within each of these layers provides the greatest visibility for device behavior to meet CM Annex requirements and add additional capabilities as so desired by the AO.

Logging from the Inner Virtual Private Network (VPN) Tunnel provides status of the VPN tunnel, software/firmware updates, hardware status, misconfigurations, and/or intrusion-related event data. Device health attestation measurements can be executed by systems operating on the inner encryption boundary or within the red network management EUD management systems to ascertain the current running state of hardware, firmware, drivers, software, or other measurements as deemed necessary by the AO. Performing these checks provides assurances against compromise of the EUD platform to erode trust that the EUD has not be altered from a good known operating state.

Data transmitted from an EUD lives in the Data Network. Customers deploying remote log collection should take this into consideration when designing monitoring architectures. Consolidating EUD log data

DRAFT

with infrastructure log data requires data transfer between the Data and Management networks (see Section 6).

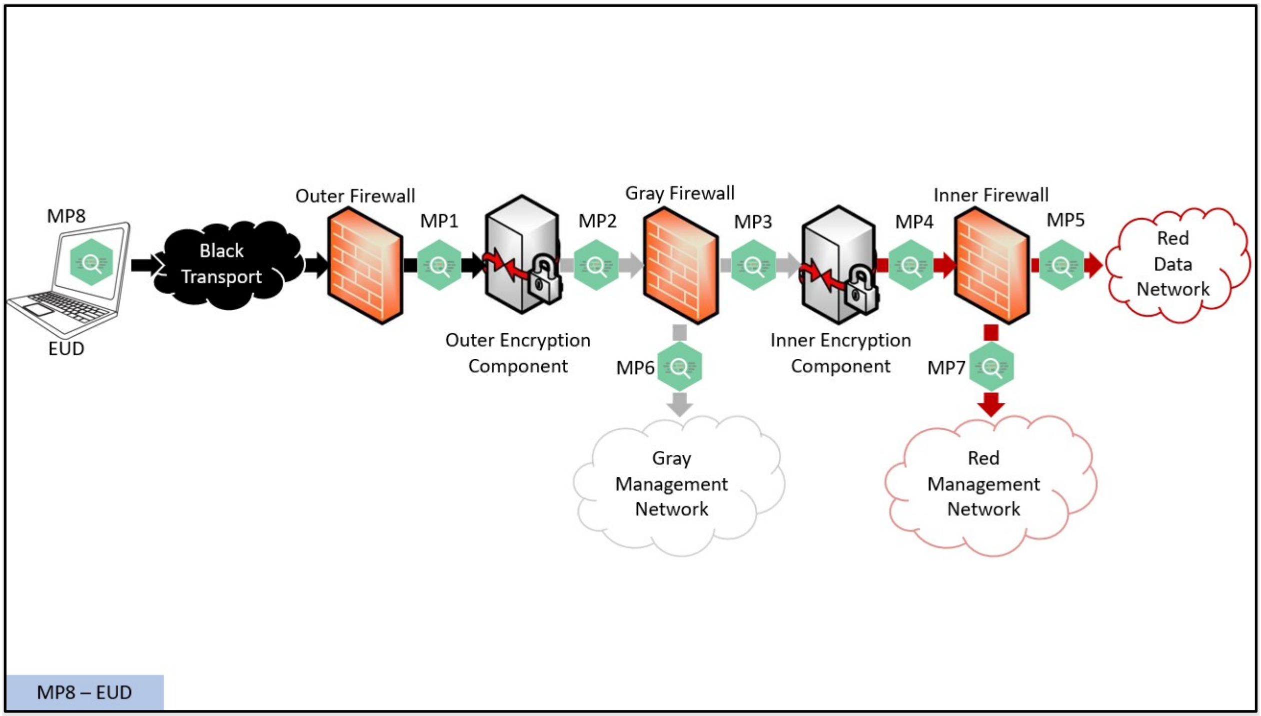


Figure 15. Monitoring Point 8: EUD

Customers must configure MP8 capabilities to send EUD log data to a Red Data Network collection server or monitoring solution. The exception to this requirement is customers who choose to deploy MP8-like monitoring requirements to service virtual machines or dedicated security components on an EUD. Only those components that can connect into the Gray Network or Red Network are authorized to send log data. The logs and notifications generated may show evidence on the EUD of either an improper configuration or a potential compromise. Managing MP8 may occur from within the Red Management Network, Red Data Network, via boundary Inner Encryption Components, or locally on EUD platforms when protected by Administrator access (see Figure 18).

DRA

5.10 Virtual Monitoring Point 8 (VMP8): Virtualized EUD (VEUD)

A Virtual EUD (VEUD) is an EUD that relies on a virtualized engine to separate out the portions of the EUD which handle Black, Gray and Red Data. VMP8 is located on a Virtualized EUD and collects system, network and application event data. Sources of VEUD monitoring data include, but are not limited to, authentication event logs, remote attestation solution, user space logs and non-user space logs in the Red and Gray Data Networks. VEUD monitoring data considers the defined set of allowed traffic and facilitates the development of appropriate reporting and notification mechanisms to identify anomalies within the Red and Gray Data Networks. The VEUD will monitor and validate the credential failures of CSfC security-relevant components. The VEUD must detect if there is any attempt to reach an unauthorized IP address, domain and/or network. The VEUD will monitor configuration changes to the security-relevant components of the virtual instance. The VEUD must monitor and validate hardware, firmware and driver component signatures. The VEUD must log the establishment and termination of VPN and TLS connections. Figure 16 shows the expected connectivity flow of a VEUD.

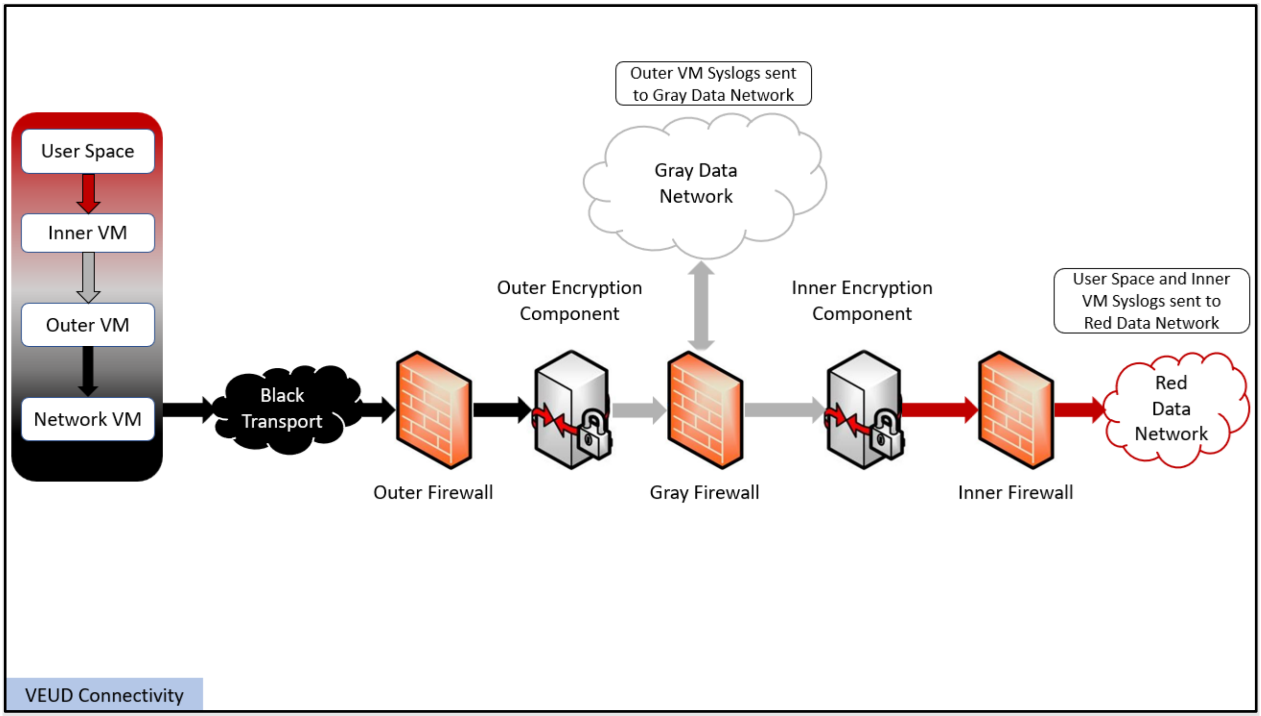

Outer VM Syslogs sent to Gray Data Network
User Space
Inner VM
Outer VM
Network VM
Gray Data Network
Outer Encryption Component
Inner Encryption Component
User Space and Inner VM Syslogs sent to Red Data Network
Black Transport
Red Data Network
Outer Firewall
Gray Firewall
Inner Firewall
VEUD Connectivity

Figure 16. Expected VEUD Connectivity

5.11 Dedicated Outer

A Dedicated Outer is a separate device that can be used as the Outer Encryption Component for an EUD. Dedicated Outers are separated into Dedicated Outer VPN and Dedicated Outer WLAN. The Dedicated Outer is included as part of the EUD and must be physically connected to the computing platform using an Ethernet or Ethernet over USB connection. The use of a physically separate VPN or WLAN as part of the EUD improves security by providing physical separation between the Computing Device and the Outer layer of encryption.

The Dedicated Outer has the capability to log events such as the establishment and termination of VPN tunnels, the establishment and termination of Wi-Fi connections, and other relevant security and configuration events.

Once generated, device logs are then forwarded to the Gray Data collection server using an existing Outer Encryption tunnel establishing a layer of encryption using SSHv2, IPsec, TLS 1.2 or later, MACsec, or DTLS.

DRAFT

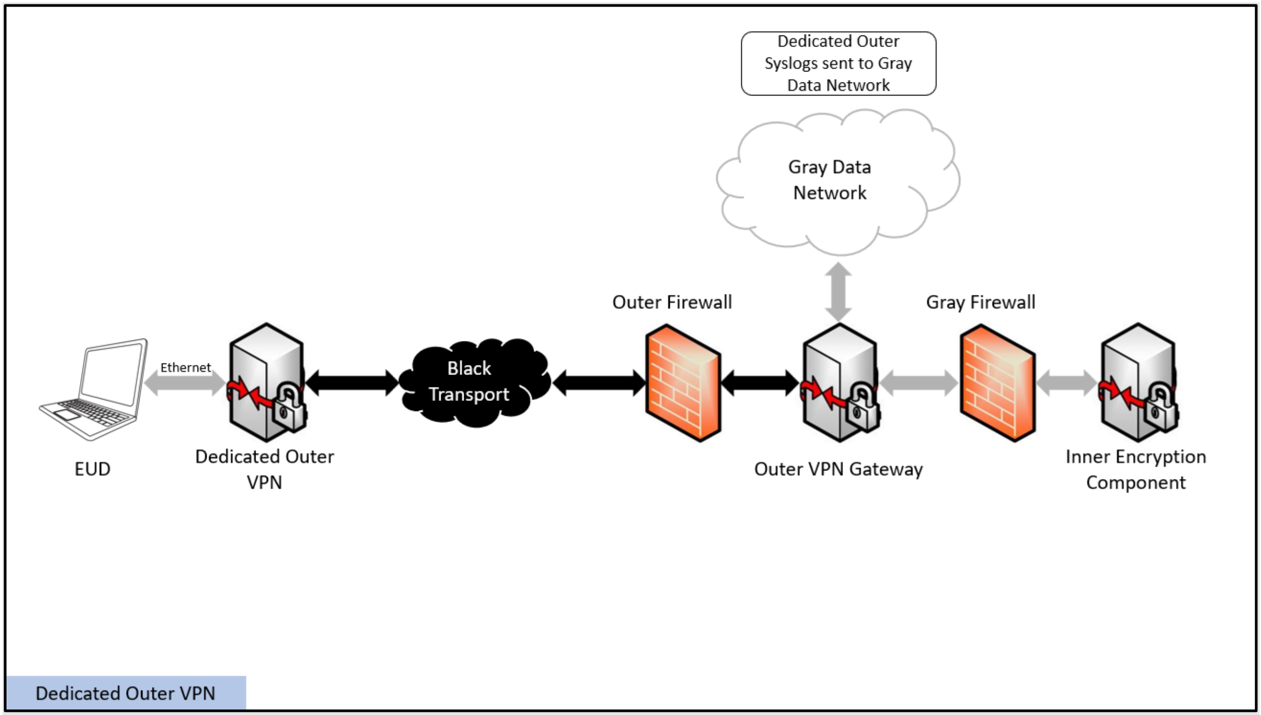


Figure 17. Dedicated Outer VPN

5.12 Mobile Device Management (MDM)

Mobile Device Management (MDM) products allow customers to apply security policies to mobile devices, such as smartphones, tablets and laptops. These policies establish an adequate security posture to permit mobile devices to process customer data and connect to customer network resources. Multiple devices are managed with a single solution and allows for visibility of those devices, protection of data containerization and device security features. These security enforcement features are being used in place of the traditional monitoring and logging features of EUDs which do not rely on an MDM.

The MDM server provides administrators with a single point of control over the customer's device fleet to ensure consistent security, configuration, compliance and software management. The MDM server collects and logs the provisioning of these enforced device-wide policies.

The MDM client (residing on the EUD device), contains its own security requirements and is loaded with an MDM agent that establishes inner encryption TLS connections back to the MDM server.

DRAFT

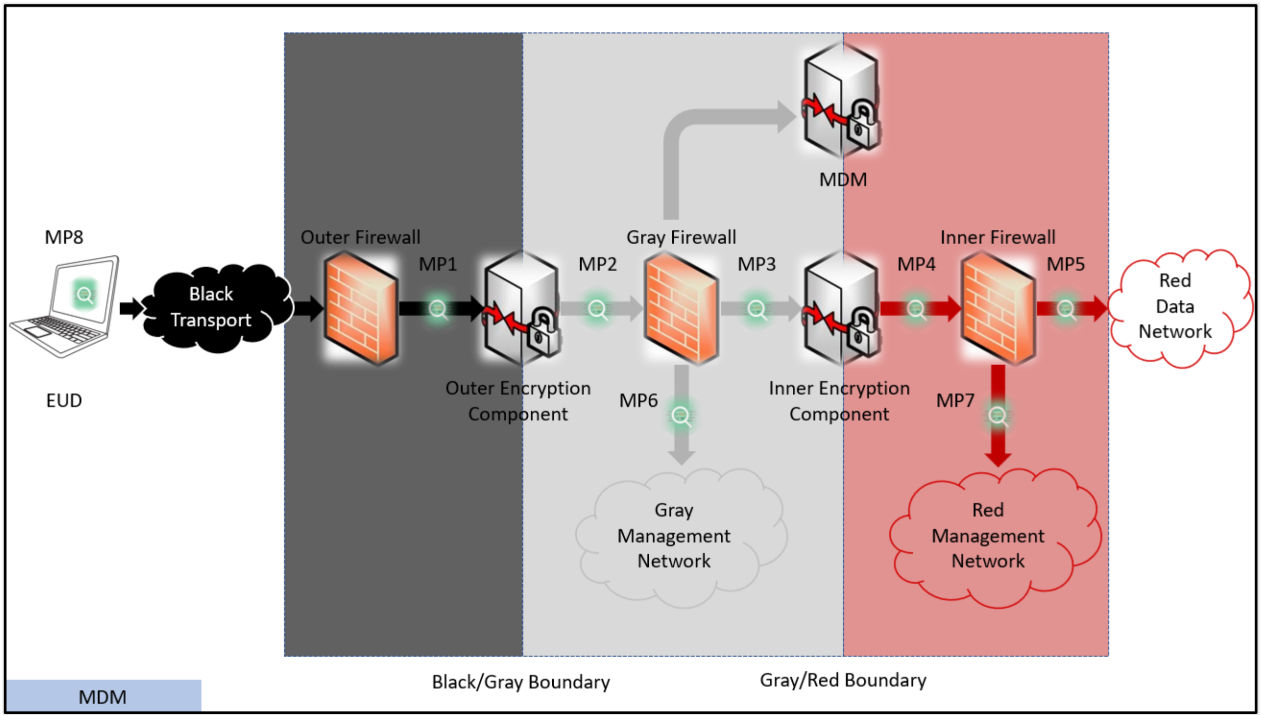


Figure 18. Mobile Device Management

5.13 Deployment of Monitoring Points Supporting Multiple-CPs

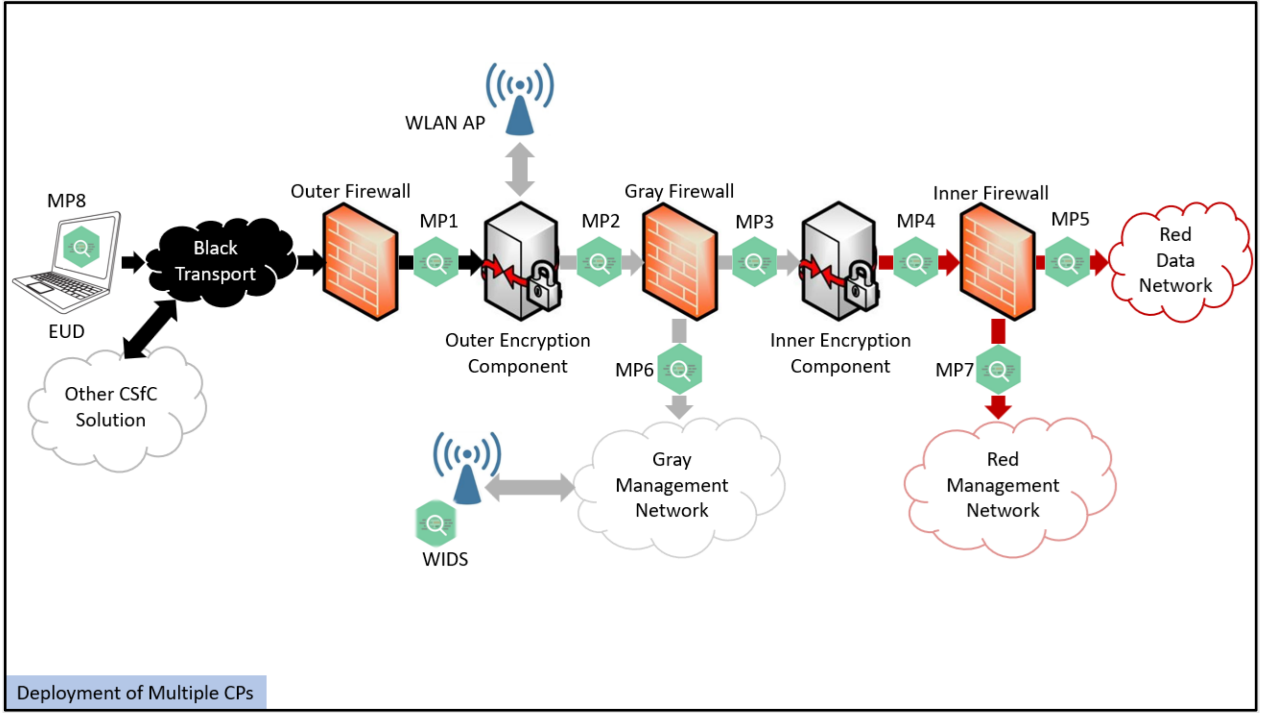


Figure 19. Deployment of Multiple CPs

For deployments of multiple CPs within the same network architecture, customers can share CM capabilities to meet applicable CM requirements. Each CSfC solution must meet the functional requirements specified in each respective CP, as well as all applicable CM requirements specified within this annex.

Customers should consider tailoring monitoring solutions with individual and combined common operating pictures of their network operations to monitor and observe network activity and systems operations for each CP implementation. Notification and reporting mechanisms should be built in to verify network segregation is enforced as defined by the customer's site requirements.

6 CONSOLIDATED MONITORING

The CM Annex allows for the implementation of CDS capabilities to transfer data from the Black and Gray Networks to either the Gray and/or Red Management Networks to co-locate monitoring event data into a single monitoring solution. Consolidated monitoring can be accomplished through the implementation of "low-to-high," one-way data transfers from the Black and Gray Networks into the Gray or Red Network through an approved CDS. Using a CDS to aggregate the data may eliminate the need for a gray monitoring solution depending on customer monitoring requirements. With all data accessible from a single monitoring solution, security administrators will no longer need to work across multiple networks to perform event detection and correlation. Additionally, a Cyber One-Way Tap or an NSA evaluated diode, as described in Section 4.4, may be used to transfer raw network traffic to higher protection levels without a CDS for ingestion into an IDS, monitoring solution or other CM capability. This use of Cyber One-Way Tap or an NSA evaluated diode is limited to only raw network capture of the solution and cannot be used for the transfer of logs or any other processed data to a higher level of protection.

Figure 20 shows an approach implementing CDS capabilities to move data between security domains within a CSfC solutions network. There is no requirement for customers to implement data transfer capabilities within their solution.

For customers deploying consolidated monitoring functionality, the requirements specified in Table 22, Multi-Site Requirements, must be met. Implementers must consider two caveats:

- Data must only be transferred in the "low-to-high" direction within a CSfC solutions network.
- Data from higher classification levels cannot pass to a lower classification level.
- Data and Management plane traffic is considered to be on separate security/administrative domains within each respective network.

Customers and integrators must adhere to all applicable data transfer policies for their organization when designing and implementing these capabilities within their CSfC solution architecture. For example, DoD customers must follow DoD Instruction (DoDI) 8540 when deploying a CDS within a CSfC solution, and if any discrepancies are found between guidance in this document and DoDI 8540 report according to the instruction found in Section 2.

DRAFT

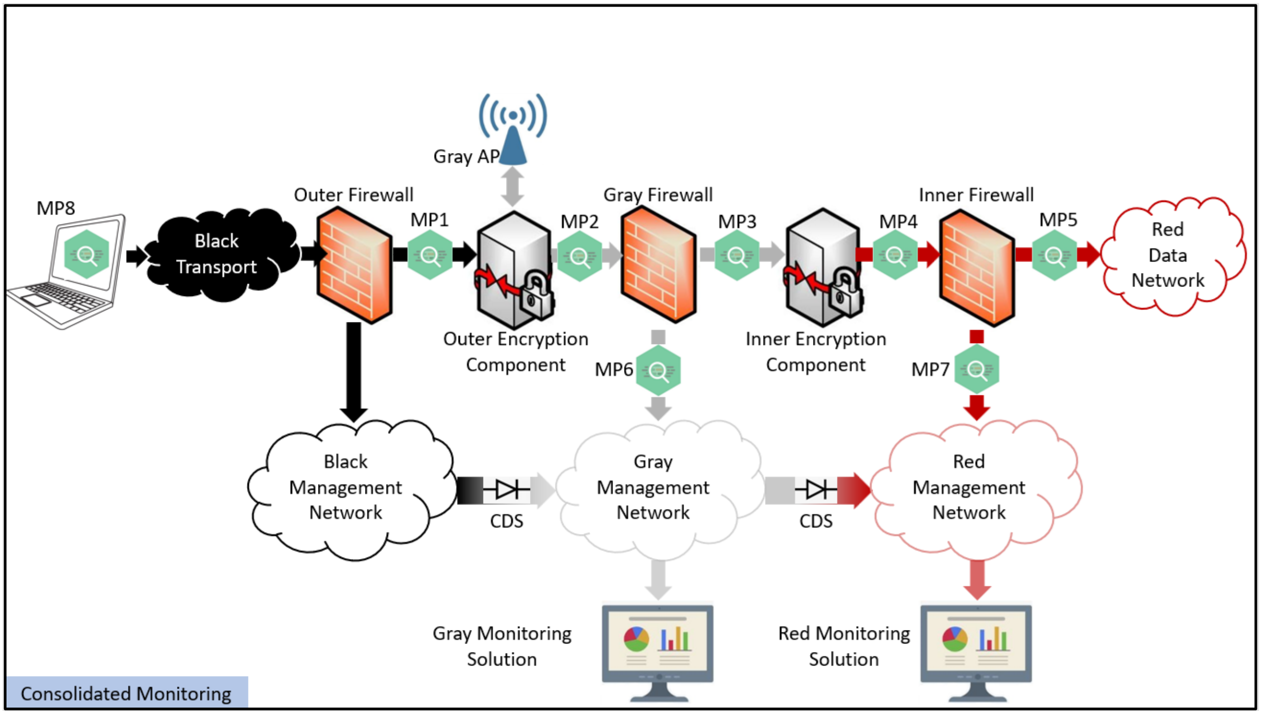


Figure 20. Consolidated Monitoring

6.1 Black Network

The Black Network is not permitted to receive data from a higher classification network such as the Gray or Red Networks. Data received from Black Network devices and stored on the Black collection server or monitoring solution in the Black Network can be forwarded to the Gray collection server or monitoring solution in the Gray Management Network, or to the Red collection server or monitoring solution in the Red Management Network through an approved CDS. In addition, Cyber One-Way Taps or an NSA evaluated diode must be used between the Black Network and the CDS.

DRAFT

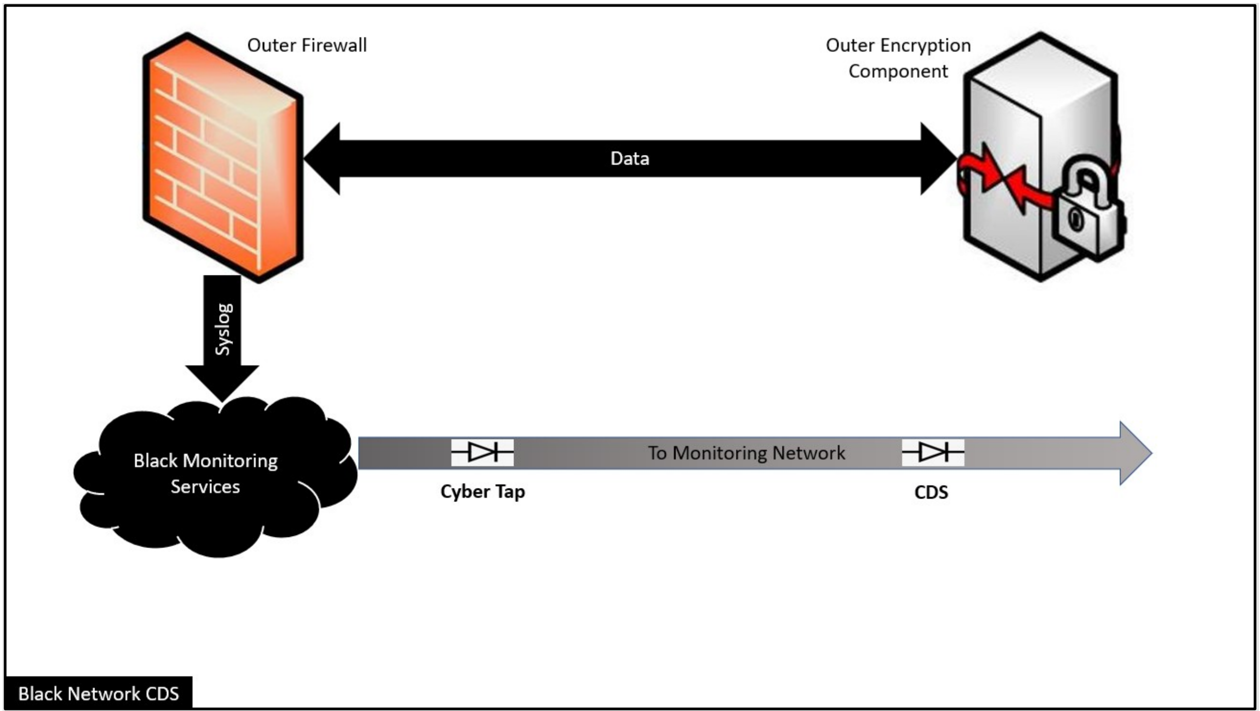


Figure 21. Black Network CDS

6.2 Gray Network

The Gray Collection Server or monitoring solution is permitted to collect data from the Black Network through an approved CDS. The recommended solution would store data from all devices in the Gray Network on a Gray data collection server or monitoring solution. If authorized by an AO, data from the Gray collection server or monitoring solution in the Gray Network can be forwarded to the Red Collection Server or monitoring solution in the Red Network through an approved CDS. In addition, Cyber One-Way Taps or an NSA evaluated diode must be used between the Gray Network and the CDS.

DRAFT

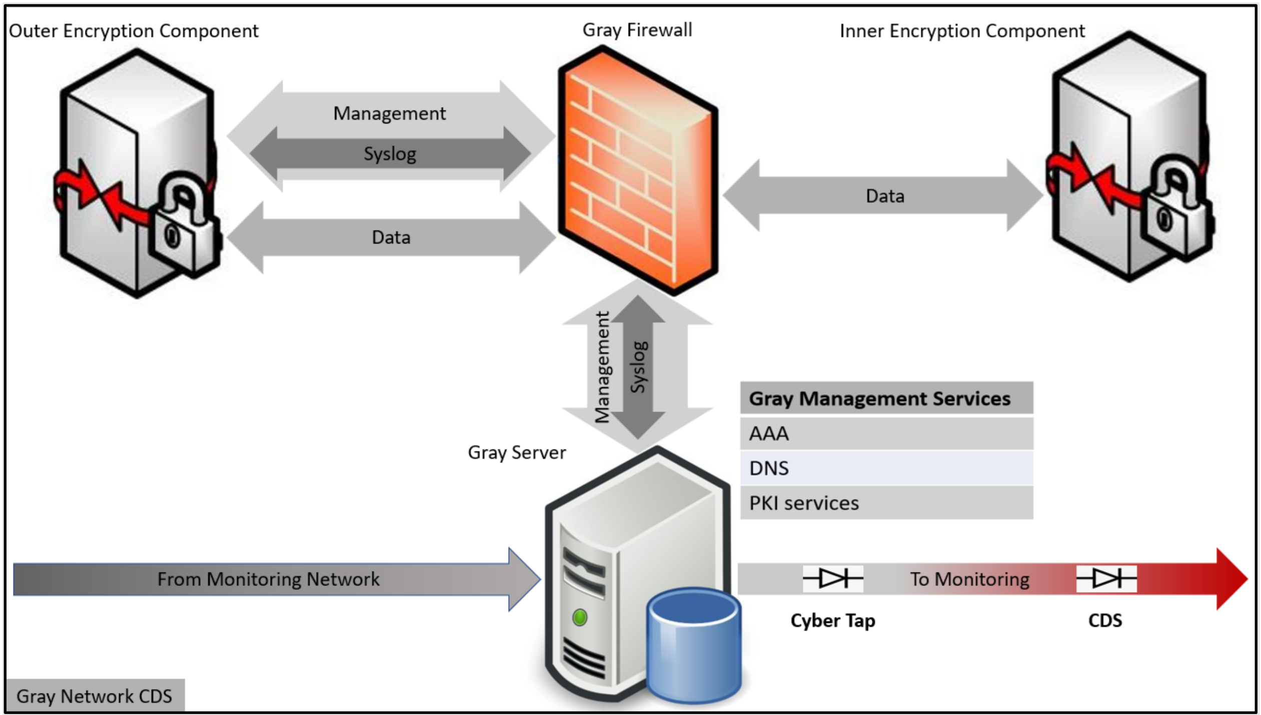


Figure 22. Gray Network CDS

6.3 Red Network

The Red Management collection server or monitoring solution is permitted to collect data from the Black and Gray Network Networks through an approved CDS. The recommended solution would store data from all devices in the Red Network on a Red Management Collection Server or monitoring solution.

DRAFT

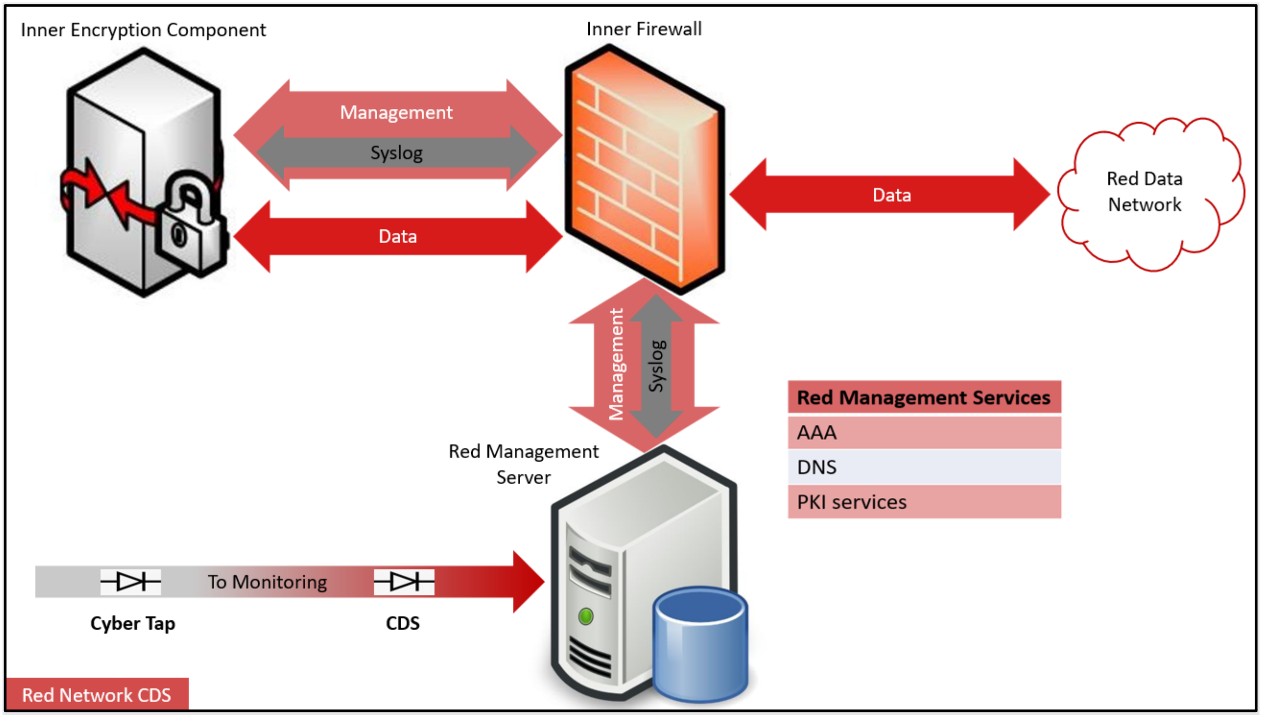


Figure 23. Red Network CDS

7 MULTIPLE INNER ENCLAVES

Customers deploying multiple Inner Enclaves to provide access to Red Networks operating at different classification levels, groups, or Inner Encryption Component types have a tailored set of CM MP requirements to implement. Regardless of the chosen CP, the CM Annex requires network traffic monitoring to occur at MP3, MP6, and MP7 for multiple Inner Enclave solutions. At a minimum, one MP in each Inner Enclave (MP4 or MP5) and one MP located in either the Black Enclave (MP1) or Gray Enclave (MP2) are also required.

Key components within each Inner Enclave may vary based on the services implemented, but must include the Inner Firewall, Inner Encryption Component, separate monitoring points, and associated Management Services. As shown in Figure 24, all security event data within each destination enclave must be sent to a collection server located within its respective enclave (e.g., Orange, Red, and Blue). Network flow data from the Inner VPN Encryption Component and/or Inner Firewall must be sent to a collection server or monitoring solution within its respective enclave. A separate monitoring solution within each Inner Enclave must be deployed to monitor each local enclave network.

When multiple Inner Enclaves are interconnected, implementation of multiple monitoring solutions and disparate collection devices may result in an increase in complexity for the CSfC CM solution. To support event correlation and provide an enterprise-wide CM capability, data from Inner Enclaves (e.g., Red, Orange, and Blue) can be forwarded to Inner Enclaves of higher classification levels, or enclaves higher in the hierarchy (Orange and Blue forwarded to Red) through an approved CDS.

DRAFT

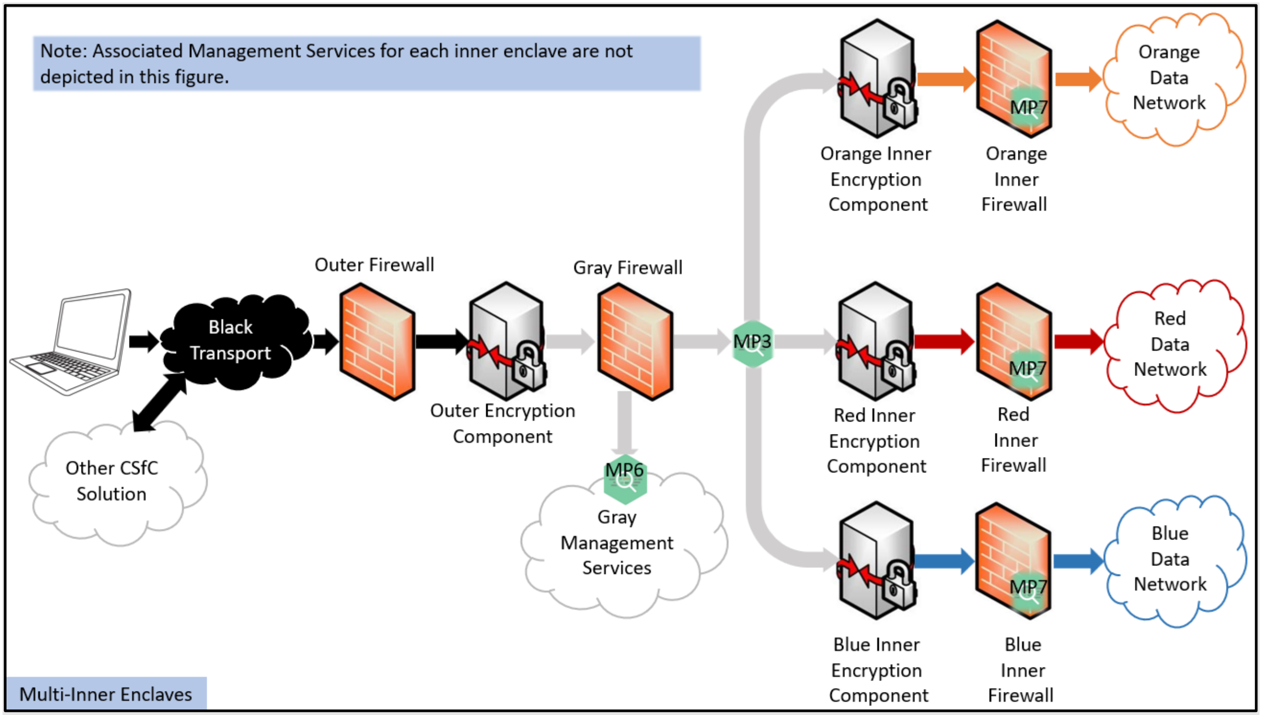


Figure 24. Multi-Inner Enclaves

DRAFT

8 MULTI-SITE ENVIRONMENTS

This section provides guidance for CM implementations of the Multi-Site Connectivity (MSC) CP. MSC solutions connect more than one CSfC solution to each other in a hub and spoke, or mesh configuration. Two monitoring design options are presented below for customers to consider in managing MSC Environments: Standalone or Centrally Managed CM configuration.

Customers may consider using a hybrid design, consisting of a standalone and centralized managed CM configuration. Customers should use configurations and data models that best meet mission needs and levels of risk acceptable to the AO.

8.1 STANDALONE CONFIGURATION

Standalone CM configurations require deploying monitoring capabilities locally within the Management Network of each site. Standalone CM configurations are typically administered on-site.

Advantages:

- Standalone CM solutions are less likely to be affected by communication outages to other sites for shared resources since they are designed to operate independently
- Local personnel have more options to respond to incidents than centrally managed solutions
- Standalone CM solutions can be tailored to fit the specific needs of CSfC sites and operations

Disadvantage:

- Customer CSfC solutions must implement requirements from the CM Annex at each site, which may take valuable resources away from local operations

8.2 CENTRALLY MONITORED SOLUTION

In Centrally Monitored Solutions, customers have one or more main sites that monitor, maintain, and administer one or more remote sites. In order to enable correlation across remote sites, the Gray Network monitoring capabilities at the remote sites must forward data to the Gray Network storage server at the main site(s). Similarly, the Red Network storage servers at the remote sites must forward data to the Red Network storage server(s) at the main site. This monitoring allows customers to detect, react to, and report any attacks against their CSfC solutions in addition to detecting any configuration errors within infrastructure components from a customer’s centralized watch floor or operations centers.

Advantages:

- Valuable local resources can focus on mission requirements, while a centralized watch floor can oversee the health and operation of remote sites. Using local personnel only when required
- Centrally Managed CM solutions are typically standardized across multiple remote sites
- A broader view of the health of remote sites in a central location or watch floor

Disadvantage:

- Centrally Managed Configuration CM solutions are likely to be affected by communication outages to other sites for shared resources like DNS, Certificate Distribution Point (CDP), or Authentication Authorization and Accounting Services

Geographically remote sites may experience low bandwidth, intermittent connectivity, or other issues that limit the transfer of data to a main site, resulting in a degraded ability to detect, report, and react to malicious activities at the remote site. In these situations, users may store logs and CM data locally for remote security administrators to review notifications from an incident when network connectivity is restored or when authorized personnel arrive to audit CM data and/or provide incident response. For networks with limited bandwidth availability, customers should consider forwarding such data during non-peak hours.

Customers should consider deploying a centrally managed monitoring solution to integrate IPS capabilities at remote sites. In the absence of having onsite administrative personnel or reliable remote management access capabilities, an IPS allows the remote site to protect itself by automatically detecting and reacting to anomalous network behavior while connectivity to a main site is degraded.

DRAFT

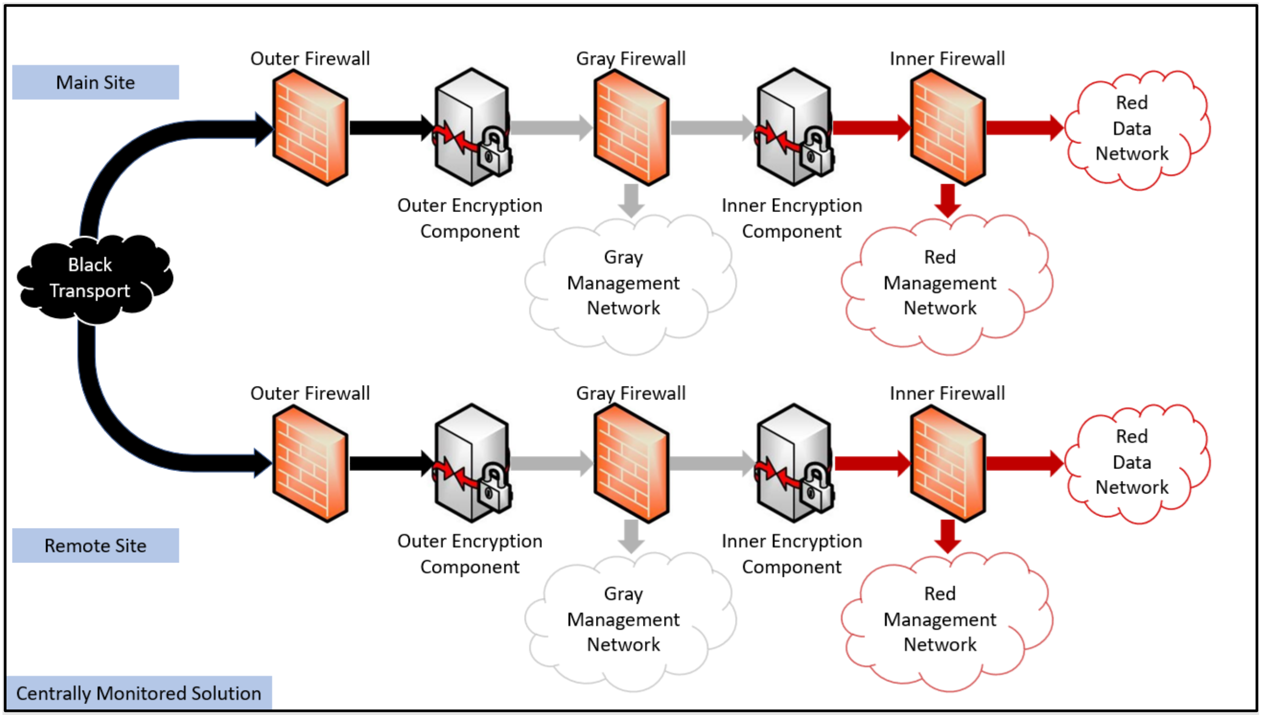


Figure 25. Centrally Monitored Solution

DRAFT

9 MONITORING IN A HIGH AVAILABILITY ENVIRONMENT

Customers scaling their CSfC solutions architecture to implement high availability requirements, such as hot or cold failover, redundancy, or load balancing, must extend the monitoring architecture to account for the increased network footprint. The following must be considered when deploying high-availability capabilities:

- Verification and monitoring of traffic transiting cross-links
- Additional bandwidth and computational power may be required to transmit data and management traffic, as well as processing within deployed monitoring solutions

No specific requirements are levied for customers deploying CM capabilities within a high availability environment. Customers must meet the intent of the requirements as defined for each respective MP and ensure all communications paths are monitored.

Customers should develop notifications within their monitoring infrastructure to detect event triggering failover conditions. Expected network behavior of the system in a ‘normal’ state and a ‘failover’ state should be defined. Customers should monitor for unexpected changes within the solution that may otherwise indicate an issue in any of the systems component’s operation or anomalous behavior within the solution’s network when in either of the previously mentioned states.

Figure 26 represents a sample high availability architecture and points within the network architecture that must be evaluated for CM capability deployment for MP2.

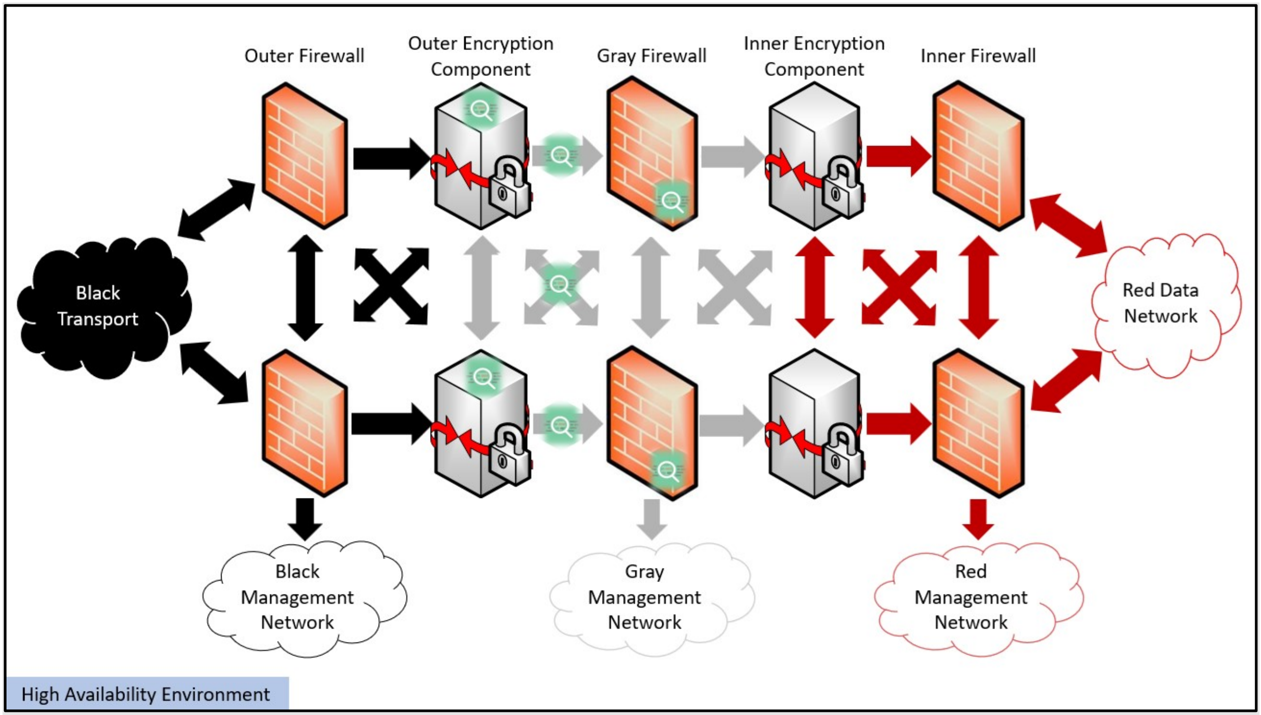


Figure 26. High Availability Environment

10 REQUIREMENTS OVERVIEW

Sections 10.4 through 10.23 specify the set of requirements for the implementation of a Continuous Monitoring solution compliant with this annex. Interconnecting CSfC solutions will follow the requirements of the CPs being deployed. Although most requirements apply to all CSfC solutions, some requirements only apply to implementations whose high-level designs implement certain features, as noted in Table 2.

10.1 CAPABILITIES

Additionally, customers should review Table 4 to identify the MPs which they intend to deploy to meet the minimum deployment requirements for CM capabilities.

Table 2. Capability Package Descriptions

Capability Package	Designator	Description
Multiple CPs	All	This *CM Annex* comprises all three data-in-transit CPs and describes how to protect classified data in transit while simultaneously interconnecting scalable and centrally manageable solutions across geographically large distances and leveraging existing infrastructure and services

DRAFT

Capability Package	Designator	Description
Mobile Access	MA	Requirements are pertinent to the *Mobile Access CP* only. This CP describes how to protect classified data (including Voice and Video) in MA solutions transiting Private Cellular Networks and Government Private Wi-Fi networks.
Campus WLAN	WLAN	Requirements are pertinent to the *Campus WLAN CP* only. This CP describes how to protect classified data (including Voice and Video) in a WLAN solution transiting Government Private Wi-Fi network.
Multi-Site Connectivity	MSC	Requirements are 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.
Enterprise Gray	EG	Requirements are pertinent to the *Enterprise Gray Implementation Requirements Annex* only. This CSfC EG Annex describes additional options for CSfC deployments and allows for centralized management of the Gray Management Network.

DRAFT

10.2 Threshold and Objective Requirements

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

- A Threshold (T) requirement specifies a feature or function that provides the minimal 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 some 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 a feasible solution, 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 that are listed as Objective in this annex may become Threshold requirements in future guidance. Solution owners are encouraged to implement Objective requirements where possible to facilitate compliance with future guidance.

10.3 Requirements Designators

Each requirement in this annex is identified by a label consisting of the prefix “CM” a two-letter category, and a sequence number (e.g., CM-MP1-3).

Table 3. Requirement Digraphs

Digraph	Description	Section	Table
MP	Monitoring Point Requirements	Section 10.5	Table 5
MP1	Monitoring Point 1 Requirements	Section 10.7	Table 6
MP2	Monitoring Point 2 Requirements	Section 10.8	Table 7
MP3	Monitoring Point 3 Requirements	Section 10.9	Table 8
MP4	Monitoring Point 4 Requirements	Section 10.10	Table 9
MP5	Monitoring Point 5 Requirements	Section 10.11	Table 10
MP6	Monitoring Point 6 Requirements	Section 10.12	Table 11
MP7	Monitoring Point 7 Requirements	Section 10.13	Table 12
MP8	Monitoring Point 8 Requirements	Section 10.14	Table 13
VMP8	Virtual Monitoring Point 8 Requirements	Section 10.15	Table 14
DO	Dedicated Outer Requirements	Section 10.16	Table 15
MDM	Mobile Device Management Requirements	Section 10.17	Table 16
LN	Logging Requirements	Section 10.18	Table 17
GR	General Requirements	Section 10.19	Table 18
SM	SIEM/SOAR Requirements	Section 10.20	Table 19
MI	Multi-Inner Enclave Requirements	Section 10.21	Table 20
MS	Multi-Site Requirements	Section 10.22	Table 21
CD	Consolidated Monitoring Requirements	Section 10.23	Table 22

10.4 Matrix of CP and Required Monitoring Points

The set of required MPs must be deployed for each CP, which at least one needs to be selected for the gray and red networks. For the two customer selected MPs, these cannot be within the same network exclusively.

Table 4. Required MP Deployments for CSfC Solutions

CP	Required	(Optional) MP in Black Network	(Required) Choose One MP in Gray Network	(Required) Choose One MP in Red Network
MA	MP6, MP7, MP8, and _*WIDS_	MP1	MP2, MP3	MP4, MP5

DRAFT

CP	Required	(Optional) MP in Black Network	(Required) Choose One MP in Gray Network	(Required) Choose One MP in Red Network
WLAN	WIDS, MP6, MP7, and MP8	N/A	MP2, MP3	MP4, MP5
MSC	MP6 and MP7	MP1	MP2, MP3	MP4, MP5

*For *MA CP* deployments using the government private wireless use case a WIDS/WIPS is required. For requirements see *CSfC WIDS/WIPS Annex.* Table 4 above denotes this use case with *WIDS.

10.5 CM Monitoring Point Requirements

Based on the CP implementation, only certain MPs from

Table 4 will apply for a customer solution. In addition, CM-MP-3 through 5, require customers to choose specific MPs to use and then only implement those requirements that relate to that MP.

Table 5. CM Monitoring Point Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP-1	Conduct network monitoring at MP6 and MP7.	All	T=O	
CM-MP-2	Conduct device monitoring at MP8.	MA	T=O	
CM-MP-3	Conduct network monitoring on at least one of the following monitoring points: MP2, or MP3.	MA, MSC	T=O	
CM-MP-4	Conduct network monitoring on at least one of the following monitoring points: MP2, or MP3.	WLAN	T=O	
CM-MP-5	Conduct network monitoring on at least one of the following monitoring points: MP4, or MP5.	All	T=O	
CM-MP-6	A WIDS must be deployed to monitor a Campus WLAN CP, and an MA CP using Government Private Wireless use case. All requirements for a WIDS are located in the *CSfC WIDS/WIPS Annex*.	MA, WLAN	T=O	

10.6 Network Monitoring Requirements

Depending on the MP chosen to implement within the solution, only apply those requirements that directly apply to the given solution. See the specific MP requirements tables for additional requirements on information that needs to be logged and notified on within the solution.

10.7 MP1 Requirements (Data Network Between Outer Firewall & Outer Encryption Component)

Only apply these requirements to the solution if MP1 is implemented.

Table 6. MP1 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP1-1	The monitoring capability must log all traffic outside expected traffic of the Outer Encryption Component	MA, MSC	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
	(i.e., non-UDP 4500 or UDP 500 for Internet Key Exchange/IPsec, or MACsec tunnel).			
CM-MP1-2	The monitoring capability must log all traffic that has a destination other than the Outer Encryption Component or Outer Firewall.	MA, MSC	T=O	
CM-MP1-3	The monitoring capability must log any unauthorized attempts to scan the Outer Encryption Component or Outer Firewall.	MA, MSC	T=O	
CM-MP1-4	The monitoring capability must log unauthorized IPs attempting to connect to Outer Encryption Components.	MA, MSC	T=O	
CM-MP1-5	The Outer Firewall must log any configuration changes.	MA, MSC	T=O	
CM-MP1-6	The Outer Firewall must log attempts to perform an unauthorized action (e.g., read, write, execute, delete) on an object.	MA, MSC	T=O	
CM-MP1-7	The Outer Firewall must log all actions performed by a user with super-user or administrator privileges.	MA, MSC	T=O	
CM-MP1-8	The Outer Firewall must log any escalation of user privileges.	MA, MSC	T=O	
CM-MP1-9	Withdrawn			
CM-MP1-10	The monitoring capability must log when system generates excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP1-11	The monitoring capability must log when system receives excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	

DRAFT

10.8 MP2 Requirements (Data Network Between Outer Encryption Component & Gray Firewall)

Only apply these requirements to the solution if MP2 is implemented.

Table 7. MP2 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP2-1	The monitoring capability must log all traffic outside expected traffic passing through the Outer Encryption Component to the Gray Firewall.	All	T=O	
CM-MP2-2	The monitoring capability must log all traffic that has a source or destination other than the EUD/Encryption Components, Outer Encryption Component, Gray Firewall/Encryption Component, Inner Encryption Component, or Gray Data services.	All	T=O	

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP2-3	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Outer Encryption Component, Gray Firewall/Encryption Component, Inner Encryption Component, or Gray Data services.	All	T=O	
CM-MP2-4	The monitoring capability must log communication between EUDs.	MA, WLAN	T=O	
CM-MP2-5	The monitoring capability must log any DNS request for any domain or name not included in the Gray Data domain.	All	T=O	
CM-MP2-6	The monitoring capability must log when a system generates an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP2-7	The monitoring capability must log when a system receives an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP2-8	The monitoring capability must create a notification when EUDs exceed AO defined operating thresholds for expected system behavior.	MA, WLAN	O	CM-MP2-9
CM-MP2-9	The monitoring capability must isolate EUDs that exceed AO defined operating behavior until device compliance remediation actions have been satisfied.	MA, WLAN	O	CM-MP2-8

10.9 MP3 Requirements (Data Network Between Gray Firewall & Inner Encryption Component)

Only apply these requirements to the solution if MP3 is implemented.

Table 8. MP3 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP3-1	The monitoring capability must log all traffic outside expected traffic passing through the Gray Firewall to the Inner Encryption Component.	All	T=O	
CM-MP3-2	The monitoring capability must log all traffic that has a source or destination other than the EUD/Encryption Components, Outer Encryption Component, Gray Firewall, or Inner Encryption Component.	All	T=O	
CM-MP3-3	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Outer Encryption Component, Gray Firewall, or Inner Encryption Component.	All	T=O	
CM-MP3-4	The monitoring capability must log communications between EUDs.	MA, WLAN	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP3-5	If the Inner Encryption Components use certificate-based authentication, the monitoring capability must log invalid or expired certificates used to attempt a connection to the Inner Encryption Component.	All	O	Optional
CM-MP3-6	The monitoring capability must log when a system generates an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP3-7	The monitoring capability must log when a system receives an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP3-8	The monitoring capability must create a notification when EUDs exceed AO defined operating thresholds for expected system behavior.	MA, WLAN	O	CM-MP3-9
CM-MP3-9	The monitoring capability must isolate EUDs that exceed AO defined operating behavior until device compliance remediation actions have been satisfied.	MA, WLAN	O	CM-MP3-8

10.10 MP4 Requirements (Data Network Between Inner Encryption Component & Inner Firewall)

Only apply these requirements to the solution if MP4 is implemented.

Table 9. MP4 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP4-1	The monitoring capability must log unusual data movement within or out of the network.	All	T=O	
CM-MP4-2	The monitoring capability must log any attempt to connect to any external domain or IP address from the Red Network.	All	T=O	
CM-MP4-3	The monitoring capability must log when a system that generates an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP4-4	The monitoring capability must log when a system that receives an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP4-5	The monitoring capability must log detection of any protocol or port outside of those specifically allowed by the Inner Firewall and/or Inner Encryption Component.	All	T=O	
CM-MP4-6	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Inner Encryption Component, Inner Firewall or Red Data Network.	All	T=O	

DRAFT

DRAFT

10.11 MP5 Requirements (Data Network After Red Firewall)

Only apply these requirements to the solution if MP5 is implemented.

Table 10. MP5 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP5-1	The monitoring capability must log unusual data movement within or out of the network.	All	T=O	
CM-MP5-2	The monitoring capability must log any attempt to connect to any external domain or IP address from the Red Network.	All	T=O	
CM-MP5-3	The monitoring capability must log when a system generates an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP5-4	The monitoring capability must log when a system receives an excessive number of short packets (e.g., a system sending over 60% of packets containing 150 or less bytes).	All	T=O	
CM-MP5-5	The monitoring capability must log the detection of any protocol or port outside of those specifically allowed by the Inner Firewall and/or Inner Encryption Component.	All	T=O	
CM-MP5-6	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Inner Encryption Component, Inner Firewall or Red Data Network.	All	T=O	

10.12 MP6 Requirements (Gray Management Network)

Applies to all CSfC solutions.

Table 11. MP6 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP6-1	The Gray Authentication services, Gray Network components and Gray Management services must log any failed login attempt.	All	T=O	
CM-MP6-2	The Gray Authentication service supporting the Gray Management services must log whenever a new user is created.	All	T=O	
CM-MP6-3	The Gray Authentication services supporting EUDs must log whenever a new EUD user is created.	MA, WLAN	T=O	
CM-MP6-4	The Gray Authentication services must log whenever a user is added or removed from a group.	All	T=O	
CM-MP6-5	The Gray Authentication services must log whenever a change is made to user or group privileges.	All	T=O	
CM-MP6-6	The Gray Authentication services must log whenever a user account attribute is changed.	All	T=O	

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP6-7	The Gray Authentication services must log whenever an authentication rule is created or modified.	All	T=O	
CM-MP6-8	The monitoring capability must log any attempt to scan the Outer Encryption Components, Gray Network components, and Gray Management services.	All	T=O	
CM-MP6-9	The monitoring capability must log if unusual traffic is detected between the Gray Management services, Gray Management workstation and/or Gray Network components.	All	T=O	
CM-MP6-10	The monitoring capability must log if a protocol outside of SSH, IPsec, or TLS is used to login into Gray Network components or Gray Management services from a dedicated Gray Management workstation or authorized Gray Management device.	All	T=O	
CM-MP6-11	The monitoring capability must log DNS queries on the Gray Management Network made to a domain or IP outside of the Gray Management Network.	All	T=O	
CM-MP6-12	The network components and Gray Management services must log when three or more invalid login attempts in a 24-hour period to any of the Gray Network component or Gray Management services.	All	T=O	
CM-MP6-13	The Gray Network components and Gray Management services must log any configuration change.	All	T=O	
CM-MP6-14	The Gray Network components and Gray Management services must log any configuration failures or errors.	All	T=O	
CM-MP6-15	If a CDP is used in the Gray Network, then the Outer and Gray Encryption Components must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	All	T=O	
CM-MP6-16	The Outer and Gray Encryption Components must log if signature validation of the CRL downloaded from a CDP fails.	All	T=O	
CM-MP6-17	The Outer and Gray Encryption Components must log establishment of an encryption tunnel.	All	T=O	
CM-MP6-18	The Outer and Gray Encryption Components must log termination of an encryption tunnel.	All	T=O	
CM-MP6-19	If using certificate-based authentication, the Outer and Gray Encryption Component must log any attempt by a client to connect using an invalid or expired certificate.	All	O	Optional
CM-MP6-20	If the Outer and Gray Encryption Components use pre-shared key authentication, the Encryption Component must log any attempt to connect using an invalid key.	All	O	Optional
CM-MP6-21	If using certificate-based authentication, the Outer and Gray Encryption Component must log the failure to download a CRL from a CDP.	All	T=O	
CM-MP6-22	If using certificate-based authentication, the Outer Encryption Component must log when different IP addresses are using the same EUD device certificate.	MA, WLAN	T=O	

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP6-23	Devices used for MACsec must log the installation of a Connective Association Key (CAK), into the MACsec Device, including all subsequent installations of new CAKs (e.g., CAK rekey).	MSC	T=O	
CM-MP6-24	MACsec Devices must log creation and updates of SAK, Secure Association Keys.	MSC	T=O	
CM-MP6-25	MACsec Devices must log administrator lockout due to excessive authentication failures.	MSC	T=O	
CM-MP6-26	All Gray Components must log administrator lockout due to excessive authentication failures.	All	T=O	
CM-MP6-27	Vulnerability scans must be conducted on the Gray Service Components within a time designated by the AO and relevant governing policies.	All	T=O	
CM-MP6-28	All Gray Management components must log integrity validation failures of defined system components (files, configurations, etc.).	All	O	Optional

889 ## 10.13 MP7 Requirements (Red Management Network)

890 Applies to all CSfC solutions.

891 Table 12. MP7 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP7-1	The Red authentication services, Red Network components and Red Management services must log any failed login attempt.	All	T=O	
CM-MP7-2	The Red Authentication service supporting the Red Management services must log whenever a new user is created.	All	T=O	
CM-MP7-3	The Red Authentication services supporting EUDs must log whenever a new EUD user is created.	MA, WLAN	T=O	
CM-MP7-4	The Red Authentication services must log whenever a user is added to a group.	All	T=O	
CM-MP7-5	The Red Authentication services must log whenever a change is made to group privileges.	All	T=O	
CM-MP7-6	The Red Authentication services must log whenever a user account attribute is changed.	All	T=O	
CM-MP7-7	The Red Authentication services must log whenever an authentication rule is created or modified.	All	T=O	
CM-MP7-8	The monitoring capability must log any attempt to scan the Inner Encryption Components, Red Network components, and Red Management services.	All	T=O	
CM-MP7-9	The monitoring capability must log if unusual traffic is detected between the Red Management services, Red Management workstation and/or Red Network components.	All	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP7-10	The monitoring capability must log if a protocol outside of SSH, IPsec, or TLS are used to login into Red Network component or Red Management services from a dedicated Red Management workstation or authorized Red Management device.	All	T=O	
CM-MP7-11	The monitoring capability must log any DNS queries on the Red Management networks made to a domain or IP outside of the Red Management Networks.	All	T=O	
CM-MP7-12	The network components and Red Management services must log when three or more invalid login attempts in a 24-hour period to any of the Red Network component or Red Management services when logging in with administrative privileges.	All	T=O	
CM-MP7-13	The Red Network components and Red Management services must log any configuration changes.	All	T=O	
CM-MP7-14	The Red Network components and Red Management services must log any configuration failures or errors.	All	T=O	
CM-MP7-15	The Inner Encryption Component must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	All	T=O	
CM-MP7-16	The Inner Encryption Components must log if signature validation of the CRL downloaded from a CDP fails.	All	T=O	
CM-MP7-17	The Inner Encryption Components must log establishment of an encryption tunnel.	All	T=O	
CM-MP7-18	The Inner Encryption Components must log termination of an encryption tunnel.	All	T=O	
CM-MP7-19	If using certificate-based authentication, the Inner Encryption Component must log any attempt by a client to connect using an invalid or expired certificate.	All	T=O	
CM-MP7-20	If the Inner Encryption Components uses key-based authentication, the Encryption Components must log if any key except the correct key is used to attempt to connect to the Encryption Component.	All	T=O	
CM-MP7-21	If certificate-based authentication is used, the Inner Encryption Component must log the failure to download a CRL from a CDP.	All	T=O	
CM-MP7-22	If certificate-based authentication is used, the Inner Encryption Component must log when different IP addresses are using the same EUD device certificate.	MA, WLAN	T=O	
CM-MP7-23	If using a TLS-Protected Servers, TLS-Protected Servers must log the failure to download a CRL from a CDP.	All	T=O	
CM-MP7-24	If using a TLS-Protected Servers, TLS-Protected Servers must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	All	T=O	
CM-MP7-25	If using a TLS-Protected Servers, TLS-Protected Servers must log if the signature validation of the CRL downloaded from a CDP fails.	All	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP7-26	If using a TLS-Protected Servers, TLS-Protected Servers must log establishment of a TLS connection.	All	T=O	
CM-MP7-27	If using a TLS-Protected Servers, TLS-Protected Servers must log termination of a TLS connection.	All	T=O	
CM-MP7-28	MACsec Devices must log the installation of a CAK into the MACsec Device, including all subsequent installations of new CAKs (i.e., CAK rekey).	MSC	T=O	
CM-MP7-29	MACsec Devices must log creation and updates of SAKs.	MSC	T=O	
CM-MP7-30	All Red Management components must log administrator lockout due to excessive authentication failures.	MSC	T=O	
CM-MP7-31	Vulnerability scans must be conducted on the Red Service Components within a time designated by the AO and relevant governing policies.	All	T=O	
CM-MP7-32	All Red Management components must log integrity validation failures of defined system components (files, configurations, etc.)	All	O	Optional

10.14 MP8 Requirements (End User Device)

Only apply these requirements to the solution if MP8 is implemented.

Table 13. MP8 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP8-1	The EUDs must generate logs and send to a collection server or monitoring solution in the Red Network.	MA, WLAN	T=O	
CM-MP8-2	Withdrawn			
CM-MP8-3	Withdrawn			
CM-MP8-4	The EUDs must log if configuration changes are made to the EUD.	MA, WLAN	T=O	
CM-MP8-5	The EUDs must log if there is any attempt by the EUD to reach an unauthorized IP addresses, domains, or networks.	MA, WLAN	T=O	
CM-MP8-6	The EUDs must log if an unauthorized application or program is installed on the EUD.	MA, WLAN	T=O	CM-SM-25
CM-MP8-7	The EUDs must log if any known malware is detected on the EUD.	MA, WLAN	T=O	
CM-MP8-8	Withdrawn			
CM-MP8-9	Withdrawn			
CM-MP8-10	Withdrawn			
CM-MP8-11	VPN Clients must log establishment of a VPN tunnel.	MA, WLAN	T=O	
CM-MP8-12	TLS Clients must log establishment of a TLS Inner Encryption tunnel.	MA	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP8-13	Encryption Component Clients must log termination of a VPN tunnel.	MA, WLAN	T=O	
CM-MP8-14	TLS Clients must log termination of a TLS Inner Encryption tunnel.	MA	T=O	
CM-MP8-15	The EUD must log signature verification and certificate validation events.	MA, WLAN	T=O	
CM-MP8-16	The EUD must log all system login attempts.	MA, WLAN	T=O	
CM-MP8-17	The EUD must log device attestation attempts and their results.	MA, WLAN	O	Optional
CM-MP8-18	EUD service VMs or Dedicated EUD Encryption Components must generate logs and send to a collection capability in their respective network.	MA, WLAN	O	Optional
CM-MP8-19	The monitoring capability or device management services must isolate EUDs with detected compliance violations (Device Health Attestation, configuration compliance, patching, unexpected applications, malware, etc.) until remediation actions have been satisfied.	MA, WLAN	O	Optional
CM-MP8-20	The EUD must be securely wiped in the event of a failed Device Health Attestation attempt.	MA, WLAN	O	CM-MP8-19
CM-MP8-21	The EUD must log integrity validation failures of defined system components (files, configurations, etc.).	MA, WLAN	O	Optional
CM-MP8-22	Log Data must be generated and stored even if a user is not actively logged in.	MA, WLAN	O	Optional
CM-MP8-23	The EUD must log establishment of a Wi-Fi connection.	WLAN	T=O	
CM-MP8-24	The EUD must log termination of a Wi-Fi connection.	WLAN	T=O	
CM-MP8-25	The EUD must log the Basic Service Set Identifier (BSSID) of the connected Wi-Fi network.	WLAN	T=O	

10.15 VMP8 Requirements Virtualized End User Device (VEUD)

Only apply these requirements to the solution if VMP8 is implemented. Solutions deploying multi-Virtual End User Device (VEUD) environments should review the following requirements and their applicability.

Table 14. VMP8 Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-VMP8-1	The VEUD must log all authentication events.	MA, WLAN	T=O	
CM-VMP8-2	The VEUD must log local and remote attestation attempts, and their results.	MA, WLAN	O	Optional
CM-VMP8-3	The VEUD must generate user space logs and forward logs to a collection server in their respective network.	MA, WLAN	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-VMP8-4	The VEUD must generate non-user space logs and send to a collection server in their respective network (Red, Gray).	MA, WLAN	T=O	
CM-VMP8-5	When malware is detected VEUDs must be isolated until remediation actions have been satisfied.	MA-WLAN	O	Optional
CM-VMP8-6	The monitoring capability or device management services must isolate VEUDs with detected compliance violations until remediation actions have been satisfied.	MA, WLAN	O	Optional
CM-VMP8-7	Each network component within a VEUD must log if there is any attempt by the VEUD to reach unauthorized IP addresses, domains, or networks.	MA, WLAN	T=O	
CM-VMP8-8	The VEUD must generate logs of configuration changes to the security relevant components of the virtual instance.	MA, WLAN	T=O	
CM-VMP8-9	The VEUD must log and validate hardware, firmware, and driver component signatures.	MA, WLAN	O	Optional
CM-VMP8-10	TLS Clients must log establishment of a TLS Inner Encryption tunnel.	MA, WLAN	T=O	
CM-VMP8-11	TLS Clients must log termination of a TLS Inner Encryption tunnel.	MA, WLAN	T=O	
CM-VMP8-12	The VEUD must log establishment of an Outer Encryption tunnel.	MA, WLAN	O	Optional
CM-VMP8-13	The VEUD must log termination of an Outer Encryption tunnel.	MA, WLAN	O	Optional

10.16 Dedicated Outer VPN Requirements

Only apply these requirements to the solution if Dedicated Outer VPN is implemented. Solutions deploying Dedicated Outer VPN for EUD environments should review the following requirements and their applicability.

Table 15. Dedicated Outer Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-DO-1	The Dedicated Outer VPN must log all authentication events.	MA, WLAN	T=O	
CM-DO-2	The Dedicated Outer VPN must log all configuration changes.	MA, WLAN	T=O	
CM-DO-3	The Dedicated Outer VPN must log any attempt to reach an unauthorized IP address, domain and/or networks.	MA	O	Optional
CM-DO-4	The Dedicated Outer VPN must log establishment of a VPN tunnel.	MA	T=O	
CM-DO-5	The Dedicated Outer VPN must log termination of a VPN tunnel.	MA	T=O	
CM-DO-6	The Dedicated Outer WLAN must log establishment of a Wi-Fi Connection.	WLAN	T=O	

DRAFT

CM-DO-7	The Dedicated Outer WLAN must log termination of a Wi-Fi Connection.	WLAN	T=O	
CM-DO-8	The Dedicated Outer WLAN must log the BSSID of the connected Wi-Fi network.	WLAN	T=O	
CM-DO-9	The Dedicated Outer VPN must log signature verification and certificate validation events.	MA, WLAN	T=O	
CM-DO-10	The Dedicated Outer VPN must forward logs to a Gray Data collection server.	MA, WLAN	T	CM-DO-11
CM-DO-11	The Dedicated Outer VPN must forward logs to the Outer Encryption Component.	MA, WLAN	T	CM-DO-10
CM-DO-12	All logs being forwarded by the Dedicated Outer VPN must be encrypted using SSHv2, IPsec, or TLS 1.2 or later, MACsec, DTLS.	MA, WLAN	T=O	
CM-DO-13	Logs received from the Dedicated Outer VPN on the Outer Encryption Component must be forwarded to the Gray Data collection server.	MA, WLAN	T=O	

10.17 Mobile Device Management Requirements

Only apply these requirements to the solution if MDM is implemented. Solutions deploying MDM should review the following requirements and their applicability.

Table 16. Mobile Device Management Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MDM-1	The MDM must collect authentication events from the EUD.	MA, WLAN	T=O	
CM-MDM-2	The MDM must log device policy changes.	MA, WLAN	T=O	
CM-MDM-3	The MDM must collect configuration changes made on the EUD.	MA, WLAN	T=O	
CM-MDM-4	The MDM must collect unauthorized network activity logs from the EUD.	MA, WLAN	T=O	
CM-MDM-5	The MDM must collect logs for establishment of VPN tunnels from the EUD.	MA, WLAN	T=O	
CM-MDM-6	The MDM must collect logs for the termination of VPN tunnels from the EUD.	MA, WLAN	T=O	
CM-MDM-7	The MDM must collect TLS Inner Encryption tunnel establishment logs from the EUD.	MA, WLAN	T=O	
CM-MDM-8	The MDM must collect TLS Inner Encryption tunnel termination logs from the EUD.	MA, WLAN	T=O	
CM-MDM-9	The MDM must collect BSSID association logs of the connected Wi-Fi network from the EUD.	MA, WLAN	T=O	
CM-MDM-10	The MDM must isolate EUDs with detected compliance violations (Device Health Attestation, configuration compliance, patching, unexpected applications, malware, etc.) until remediation actions have been satisfied.	MA, WLAN	O	Optional

DRAFT

10.18 Logging Requirements

Requirements for all network components in Black, Gray, and Red networks such as Encryption Component, Firewall, Authentication service and any additional service components supporting the CSfC solution.

Table 17. Logging Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-LN-1	Each log entry must record the date and time of the event.	All	T=O	
CM-LN-2	Each log entry must include the identifier of the event.	All	T=O	
CM-LN-3	Each log entry must record the type of event.	All	T=O	
CM-LN-4	Each log entry must record the success or failure of the event to include failure code, when available.	All	T=O	
CM-LN-5	Each log entry must record the subject identity.	All	T=O	
CM-LN-6	Each log entry must record the source address for network-based events.	All	T=O	
CM-LN-7	Each log entry must record the user and, for role-based events, role identity, where applicable.	All	T=O	
CM-LN-8	Solution Components must log all actions performed on the audit log (e.g., off-loading, deletion).	All	T=O	
CM-LN-9	Solution Components must log all actions involving identification and authentication.	All	T=O	
CM-LN-10	Solution Components must log generation, loading, and revocation of certificates.	All	T=O	
CM-LN-11	Solution Components must log changes to time.	All	T=O	
CM-LN-12	Solution Components must log when packets received on a network interface are dropped or blocked.	All	T=O	
CM-LN-13	Solution Components must log the results of built-in self-tests.	All	T=O	
CM-LN-14	All solution components must be configured with an automated service that detects all changes to configuration.	All	T=O	
CM-LN-15	Solution components must forward monitoring data to a collection server.	All	T=O	CM-MS-2
CM-LN-16	Monitoring data must be sent within a time designated by the AO and relevant governing policies.	All	O	Optional
CM-LN-17	All logs forwarded to a SIEM, or collection server must be encrypted using SSHv2, IPsec, or TLS 1.2 or later, MACsec, DTLS.	All	O	Optional
CM-LN-18	All logs must be reviewed at an interval set by the AO or set by local policy but must be done at least once a week.	All	T=O	

DRAFT

10.19 General Requirements

General requirements for Continuous Monitoring of CSfC solutions.

918

Table 18. General Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-GR-1	If network flow is used within the solution, a network flow data collector (e.g., SILK, IP Flow, and NetFlow Collector) must be installed in the Red Management Network.	All	T=O	
CM-GR-2	If network flow is used within the solution, a network flow data collector (e.g., SILK, IP Flow, and NetFlow Collector) must be installed in the Gray Management Network.	All	T=O	
CM-GR-3	A baseline for network monitoring data must be established.	All	T=O	
CM-GR-4	A baseline for network monitoring data must be updated at an interval determined by the AO or governing policy.	All	T=O	
CM-GR-5	If network flow is used within the solution, network flow data must be reviewed on an interval set by the AO or local policy but must be done at least once a week: Systems generating excessive amounts of traffic. Systems trying to connect to improper IP addresses. Systems trying to connect to closed ports on internal servers.	All	T=O	
CM-GR-6	If network flow is used within the solution, collected network flow data must be compared and analyzed against the established baseline on an interval set by the AO or set by local policy but must be don't at least once a week.	All	O	Optional
CM-GR-7	Locally run CAs must comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	All	T=O	
CM-GR-8	Locally run CAs must comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	All	T=O	
CM-GR-9	Audits and assessments for Outer and Inner CAs must be performed by personnel who are knowledgeable in CA operations, as well as Certificate Policy and Certification Practice Statement requirements and processes, respectively.	All	T=O	
CM-GR-10	Audit log data must be maintained for a time determined by the AO and relevant governing policies.	All	T=O	
CM-GR-11	The amount of storage remaining for audit events must be assessed by the Security Administrator on a basis set by the AO and relevant governing policies to ensure that adequate storage space is available to continue recording new audit events.	All	T=O	
CM-GR-12	Audit data must be backed up to an external storage medium on a basis set by the AO and relevant governing policies.	All	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-GR-13	The implementing organization must develop a set of procedures to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	All	T=O	
CM-GR-14	The implementing organization must develop a continuity of operations plan for auditing capability, which includes a mechanism or method for determining when the audit log is reaching its maximum storage capacity.	All	T=O	
CM-GR-15	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for backed up to an external long-term storage.	All	T=O	
CM-GR-16	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for responding to an overflow of audit log data within a product.	All	T=O	
CM-GR-17	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for ensuring the audit log can be maintained during power events.	All	T=O	
CM-GR-18	If a consolidating monitoring capability is implemented, an approved CDS must be used to move CM related data from the Black Network to the Gray Network, Black Network to the Red Network, and Gray Network to the Red Network.	All	T=O	
CM-GR-19	If a solution has shared network plane for multiple sites (e.g., shared Gray Management network) then a site may send its CM related data to that site instead of processing it locally.	All	O	Optional
CM-GR-20	The implementing organization must develop a defined dataflow plan for the lifecycle of the data collected in the CM process.	All	T=O	
CM-GR-21	Customers must have notification procedures in place for notifications generated by security devices, monitoring solutions, and any other analytic tools.	All	T=O	
CM-GR-22	If deploying EUDs, a baseline of system behavior of the EUD must be established.	All	T=O	
CM-GR-23	Withdrawn			
CM-GR-24	All dataflows must be monitored by CM capabilities.	All	T=O	
CM-GR-25	Key Generation Systems (KGSs) that deliver CAK Management Services for MSC Solutions must comply with audit and assessment requirements defined by the customer's operational security doctrine and enterprise KGS (if applicable).	MSC	T=O	
CM-GR-26	Audits and assessments for a KGS must be performed by personnel who are knowledgeable in the KGS's operations, audit requirements and processes.	MSC	T=O	

DRAFT

10.20 MONITOR SOLUTION REQUIREMENTS

Requirements for the Monitoring Solution supporting the CSfC solutions Continuous Monitoring capability.

Table 19. Monitoring Solution Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-SM-1	Monitoring solution components must be placed within the Gray Network unless devices are configured to push events to a Red Network monitoring solution through an approved CDS.	All	T=O	
CM-SM-2	The monitoring solution must be configured to send notifications to the Security Administrator when anomalous behavior is detected outside of organization defined thresholds.	All	T=O	
CM-SM-3	The Gray monitoring solution must receive all system logs and network monitoring data collected from the MPs within the Gray Network.	All	T	CM-SM-5
CM-SM-4	The Red monitoring solution must receive all system logs and network monitoring data collected from the MPs within red.	All	T	CM-SM-5
CM-SM-5	The Red monitoring solution must receive all system logs and network monitoring data collected from the MPs from all Gray and Red Networks.	All	O	CM-SM-3 and CM-SM4
CM-SM-6	The monitoring solutions(s) must provide notification for when devices attempt to establish a connection with the Encryption Components using incorrect or misconfigured settings.	All	T=O	
CM-SM-7	If certificate-based authentication is used for the Encryption Components, the monitoring solution(s) must maintain a table of Certificate Common Names and assigned IP addresses used for connecting to the Encryption Components.	All	T	CM-SM-8
CM-SM-8	If key-based authentication is used for the Encryption Components, the monitoring solution(s) must maintain an up-to-date table of assigned IP addresses used for connecting to the Encryption Components.	All	O	CM-SM-7
CM-SM-9	The monitoring solution(s) must provide a notification for three or more invalid login attempts in a 24-hour period to the Solution Components.	All	T=O	
CM-SM-10	The monitoring solution(s) must provide a notification of privilege escalations on Solution Components.	All	T=O	
CM-SM-11	The monitoring solution(s) must provide a notification of configuration changes to the Solution Components.	All	T=O	
CM-SM-12	The monitoring solution(s) must provide a notification of new accounts created on the Solution Components.	All	T=O	
CM-SM-13	The monitoring solution(s) must provide a notification for attempted connections to the Encryption Components that use invalid certificates or keys.	All	O	Optional

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-SM-14	The monitoring solution(s) must provide a notification of blocked traffic at the Firewalls (if present).	All	T=O	
CM-SM-15	The monitoring solution(s) must provide a notification for DNS queries other than expected domains.	All	T=O	
CM-SM-16	All monitoring solution notifications must be reviewed at an interval set by the AO or set by local policy but must be done at least once a week.	All	T=O	
CM-SM-17	The monitoring solution must log when there are a high number of anomalous EUD events compared to the baseline.	MA, WLAN	T=O	
CM-SM-18	The monitoring solution must log if calls or connections are made from an EUD in different locations within a timeframe that is not possible.	MA, WLAN	T=O	
CM-SM-19	The monitoring solution must detect when two or more simultaneous VPN connections from different IP addresses are established using the same EUD device certificate.	MA, WLAN, MSC	T=O	
CM-SM-20	The monitoring solution must detect when two or more simultaneous TLS connections from different IP addresses are established using the same EUD device certificate.	MA, WLAN	T=O	
CM-SM-21	The monitoring solution must integrate CTI.	All	O	Optional
CM-SM-22	The monitoring solution must log compliance evaluations performed for all network authorization attempts.	All	O	Optional
CM-SM-23	The monitoring solution must implement User Activity Monitoring capabilities to monitor user and system behavior for EUDs and Management Components. User Activity Monitoring should include person and non-person entities.	All	O	Optional
CM-SM-24	The monitoring solution must automate responses to AO defined notable security events.	All	O	Optional
CM-SM-25	The monitoring solution must log and notify security administrators if an unauthorized application or program is installed on the EUD.	MA, WLAN	T=O	CM-MP8-6
CM-SM-26	The monitoring solution must provide a notification if a failed attestation measurement occurs.	MA, WLAN	O	Optional

DRAFT

10.21 Multi-Inner Enclave Requirements

Only apply these requirements to the solution if multiple Inner Enclaves are implemented.

Table 20. Multi-Inner Enclave Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MI-1	Within each Inner Enclave, implement MP4 or MP5.	All	T=O	
CM-MI-2	The network monitoring components and Gray Firewall must log any attempt of the different Inners Encryption Components to connect to each other.	All	T=O	
CM-MI-3	The monitoring solution must notify when an EUD or Encryption Component is connected to two or more Inner enclaves simultaneously.	All	T=O	
CM-MI-4	The monitoring solution must notify when an EUD or Encryption Component connects to an unauthorized Inner Enclave.	All	T=O	
CM-MI-5	All security event data from key components within each Inner Enclave (e.g., Inner Firewall, Inner VPN, Monitoring Points and Management Services) must be sent to a collection server or monitoring solution located within that particular Inner Enclave.	All	T=O	
CM-MI-6	Network flow data from each Inner Enclave must be collected from the Inner VPN or Inner Firewall and sent to a collection server or monitoring solution within that particular Inner Enclave.	All	T=O	

10.22 Multi-Site Requirements

Only apply these requirements to the solution if deploying a multi-site solution with central management.

Table 21. Multi-Site Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MS-1	Multi-Site configurations using Centralized Gray Management, data from Gray Network monitoring and logging capabilities may forward its data to another site for storage, analysis and reporting.	EG	O	Optional
CM-MS-2	Multi-Site configurations using Centralized Gray Management and CM, data is forwarded to another site, local storage of logs and network monitoring data must still exist in case connection is lost to the site conducting storage, analysis and reporting.	EG	T=O	
CM-MS-3	Multi-Site configurations using Centralized Management, data from Inner/Red Network storage servers at remote sites must be forwarded to Inner/Red Network storage server(s) at the main site.	All	O	Optional

10.23 Consolidated Monitoring Requirements

Only apply these requirements to the solution if deploying consolidate monitoring capabilities.

DRAFT

Table 22. Consolidated Monitoring Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-CD-1	Data, with the exception of raw network traffic, passing from the Black Network to a higher classification level must traverse through an approved CDS.	All	T=O	
CM-CD-2	Data, with the exception of raw network traffic, passing from the Gray Network to a higher classification level must traverse through an approved CDS.	All	T=O	
CM-CD-3	Cyber One-Way Taps or an NSA evaluated diode may be used without a CDS to transfer raw network traffic captures between networks as long as data does not flow from higher classification to lower classification (e.g., Red to Gray).	All	T=O	
CM-CD-4	If a CDS is being leveraged within the solution, then it must adhere with all applicable organizational policy and be on the NCDSMO CDS Baseline. (For example: DoD customers must also adhere to DoDI 8540.01 and the Defense Information System Network (DISN) Connection Process Guide).	All	T=O	
CM-CD-5	If a CDS is being used to transfer data between Black Network and the Gray, and Red or another secured network then a Cyber One-Way Tap or an NSA evaluated diode must be used between the Black Network and the CDS.	All	T=O	
CM-CD-6	If a CDS is being used to transfer data between Gray Network and the Red or another secured network, then a Cyber One-Way Tap or an NSA evaluated diode must be used between the Gray Network and the CDS.	All	T=O	

DRAFT

Appendix A. Glossary of Terms

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

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

Authorizing Official (AO) – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Black Network – A network that contains classified data that has been encrypted twice.

Capability Package (CP) – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. CP instantiations are built using products selected from the CSfC Components List.

Central Management Site – A site within a solution that is responsible for remotely managing the solution components located at other sites.

Certification Authority (CA) – An authority trusted by one or more users to create and sign digital certificates. (ISO9594-8)

Cross Domain Solution (CDS) – A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

Dedicated EUD Encryption Component – A dedicated solution providing Outer Encryption or Inner Encryption layers for an EUD. See *EUD Composition Guidance Addendum* Section 10.2 and 10.3 for additional information.

End User Device (EUD) – A form-factor agnostic component of the Mobile Access (MA) or Campus Wireless (WLAN) solution that can include a mobile phone, tablet, or laptop computer. EUDs can be composed of multiple components to provide physical separation between layers of encryption.

Gray Encryption Component – An authorized device that provides the second layer of encryption for extending the Gray Management and Gray Data Networks between multiple sites. Applies to Enterprise Gray Annex only.

Gray Management Network – Provides control and management of the Outer Encryption Component and Outer Firewall. The Gray Management Network also contains all necessary components needed for

DRAFT

the operation of the Outer Firewall and Encryption Component also contains all necessary CM functions of the Gray Network.

Gray Network/Gray Data Network – A network that contains classified data that has been encrypted once.

Inner Encryption Component - An authorized device that provides the second layer of encryption for devices connecting to the solution.

Inner Firewall - A traffic filtering firewall placed between the Red Encryption Component and Red Data Network to provide filtering of ports, protocols, and IP addresses.

Malicious – Any unauthorized events that are either unexplained or in any way indicate adversary activity.

Network Monitoring Data – Information about network traffic traversing the solution. This data can include full packet captures or meta-data about the traffic.

Notification – Refers to a monitoring solution's ability to alert or notify its users of an event that is either unusual or malicious activity within the network.

Network Monitoring Data – Information about network traffic traversing the solution. This data can include full packet captures or meta-data about the traffic.

Outer Encryption Component - An authorized device that provides the first layer of encryption for devices connecting to the solution.

Outer Firewall - A traffic filtering firewall placed between the public internet and Outer Encryption Component to provide filtering of ports, protocols, and IP addresses to ensure traffic reaches the correct Outer Encryption or is dropped.

Red Management Network – Provides control and management of the Inner Encryption Component and Inner Firewall. The Red Management Network also contains all necessary components needed for the operation of the Inner Firewall and Encryption Component also contains all necessary CM functions of the Red Network with the exception of the EUD.

Red Network/Red Data Network - Contains only Red data and is under the control of the solution owner or a trusted third party. The Red Network begins at the internal interface(s) of Inner Encryption Components located between the Gray Firewall and Inner Firewall.

Security Administrator – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the CSfC solution.

DRAFT

Appendix B.Acronyms

Acronym	Meaning
AO	Authorizing Official
ARP	Address Resolution Protocol
BSSID	Basic Service Set Identifier
CAK	Connective Association Key
CDP	Certificate Revocation List (CRL) Distribution Point
CDS	Cross Domain Solution
CM	Continuous Monitoring
COTS	Commercial-Off-the-Shelf
CP	Capability Package
CRL	Certificate Revocation List
CSD	Cybersecurity Directorate
CSfC	Commercial Solutions for Classified
CTI	Cyber Threat Intelligence
DHA	Device Health Attestation
DISN	Defense Information System Network
DNS	Domain Name System
DoDI	Department of Defense Instruction
DTLS	Datagram Transport Layer Security
EUD	End User Device
HTTP	Hypertext Transfer Protocol
KGS	Key Generation System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
MACsec	Media Access Control Security
MDM	Mobile Device Management
MP	Monitoring Point
NCDSMO	National Cross Domain Strategy Management Office
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
SRTP	Secure Realtime Transfer Protocol
SSH	Secure Shell

DRAFT

Acronym	Meaning
SSHv2	Secure Shell version 2
STP	Spanning Tree Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
VEUD	Virtualized End User Device
VM	Virtual Machine

DRAFT

Appendix C. References

Document	Title	Date
CSfC Campus WLAN CP	Commercial Solutions for Classified (CSfC): *Campus Wireless Local Area Network (WLAN) Capability Package (CP), v3.0.1*	January 2023
CSfC MA CP	Commercial Solutions for Classified (CSfC): *Mobile Access Capability Package (CP), v2.5.1*	February 2022
CSfC MSC CP	Commercial Solutions for Classified (CSfC): *Multi-Site Connectivity (MSC) Capability Package (CP), v1.1*	June 2018
RFC 5424	The Syslog Protocol	March 2009
RFC 7011	*Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*	September 2013
RFC 7012	*Information Model for IP Flow Information Export (IPFIX)*	September 2013
NIST SP 800-137	*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*	September 2011
DoDI 8540.01	Department of Defense Instruction 8540.01: *Cross Domain (CD) Policy*	August 2017
CNSSI 4009	*Committee on National Security Systems (CNSS) Glossary*	April 2015
NIST	https://csrc.nist.gov/csrc/media/projects/risk-management/documents/faq-continuous-monitoring.pdf	June 2010
DoD Zero Trust Capabilities and Activities	https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilitiesActivities.pdf	January 2023

DRAFT

Appendix D. Tactical Solution Continuous Monitoring Implementations

Although the majority of customers instantiating solutions based on the CSfC Data-in-Transit solutions will be used for Strategic or Operational Environments, some organizations may deploy the CSfC Data-in-Transit in Tactical Environments. These Tactical Environments include a specific set of Size, Weight, and Power (SWaP) constraints not found in traditional environments. The guidance provided in the Appendix references architecture and corresponding high-level configuration information to help customers develop a CM solution to meet operational needs in a Tactical Environment.

Organizations intending to deploy a CSfC Data-in-Transit for Tactical Environments may use this Appendix, which accommodates the SWaP constraints unique to their environment. This Appendix may only be used to protect Tactical Data classified as SECRET or below. The CP follows CNSSI 4009, that defines Tactical Data as, "Information that requires protection from disclosure and modification for a limited duration as determined by the originator or information owner." In addition to protecting Tactical Data, organizations that register their solution using this Appendix must be deployed at the Tactical Edge. The CP also follows CNSSI 4009, which defines the Tactical Edge as, "The platforms, sites, and personnel (U.S. military, allied, coalition partners, first responders) operating at lethal risk in a battle space or crisis environment characterized by: 1) a dependence on information systems and connectivity for survival and mission success, 2) high threats to the operational readiness of both information systems and connectivity, and 3) users are fully engaged, highly stressed, and dependent on the availability, integrity, and transparency of their information systems."

If an organization's planned solution meets the three criteria above, then their solution may be registered using the Continuous Monitoring requirement accommodations in this Appendix. The CSfC registration form must explicitly state that the solution is being used in Tactical Environments and provide justification on how the above criteria are met. In general, customers registering with this Appendix will be deployed in support of Battalion and below (or equivalent) unit structure. Typically, these Tactical Environments are located in austere environments where communication infrastructure is generally limited. Due to the lack of existing communication infrastructure, the Tactical Environments are also generally characterized by the use of Government owned Black Infrastructure (Government Private Wireless Networks and/or Government Private Cellular Networks and/or Government Private Wired Networks).

Table 23 defines the Tactical Implementation Continuous Monitoring Overlay Requirements and may be used by customers meeting the criteria above when they configure, test, register, and operate their CSfC Solution. This table replaces all other requirement found in the body of the Annex with exception of the connecting to outside network. Any questions on the use of this Appendix should be directed to CSfC_CM_team@nsa.gov, mobile_access@nsa.gov and csfc@nsa.gov.

These requirements are designed to minimize impact on a Tactical Implementation by requiring only the logging of events locally keeping bandwidth usage at a minimum and local storage of the logs at a minimum as well. The AO must still develop a defined dataflow plan for the lifecycle of the data collected in the CM process which will not be overly burdensome on the solution that they are fielding.

DRAFT

If the Tactical Implementation has a connection to a greater CSfC network which does not have the same Tactical constraints on it, then that solution must be monitored in accordance with the requirements found within the body of the Annex. If this greater network is not a CSfC Network, then all requirements found in Table 10 MP5 Requirements must be implemented to monitor the connection between the Tactical Implementation and that greater network.

10.24 Tactical Implementation Continuous Monitoring

Table 23. Tactical Implementation Continuous Monitoring Overlay Requirements

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-LN-1	Each log entry must record the date and time of the event.	MA, WLAN	T=O	
CM-LN-2	Each log entry must include the identifier of the event.	MA, WLAN	T=O	
CM-LN-3	Each log entry must record the type of event.	MA, WLAN	T=O	
CM-LN-4	Each log entry must record the success or failure of the event to include failure code, when available.	MA, WLAN	T=O	
CM-LN-5	Each log entry must record the subject identity.	MA, WLAN	T=O	
CM-LN-6	Each log entry must record the source address for network-based events.	MA, WLAN	T=O	
CM-LN-7	Each log entry must record the user and, for role-based events, role identity, where applicable.	MA, WLAN	T=O	
CM-LN-8	Solution Components must log all actions performed on the audit log (e.g., off-loading, deletion).	MA, WLAN	T=O	
CM-LN-9	Solution Components must log all actions involving identification and authentication.	MA, WLAN	T=O	
CM-LN-11	Solution Components must log changes to time.	MA, WLAN	T=O	
CM-LN-12	Solution Components must log when packets received on a network interface are dropped or blocked.	MA, WLAN	T=O	
CM-LN-14	An automated process must ensure that configuration changes are logged.	MA, WLAN	T=O	
CM-GR-7	Locally run CAs must comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	MA, WLAN	T=O	
CM-GR-8	Locally run CAs must comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	MA, WLAN	T=O	
CM-GR-13	The implementing organization must develop a set of procedures to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	MA, WLAN	T=O	
CM-GR-16	The implementing organization must develop a continuity of operations plan for auditing capability that includes a mechanism or method for responding to an overflow of audit log data within a product.	MA, WLAN	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-GR-20	The implementing organization must develop a defined dataflow plan for the lifecycle of the data collected in the CM process.	MA, WLAN	T=O	
CM-MP1-2	The monitoring capability must log all traffic which has a destination other than the Outer Encryption Component or Outer Firewall.	MA	T=O	
CM-MP1-3	The monitoring capability must log any unauthorized attempts to scan the Outer Encryption Component or Outer Firewall.	MA	T=O	
CM-MP1-5	The Outer Firewall must log any configuration changes.	MA	T=O	
CM-MP2-1	The monitoring capability must log all traffic outside expected traffic passing through the Outer Encryption Component to the Gray Firewall.	MA, WLAN	T=O	
CM-MP2-2	The monitoring capability must log all traffic which has a source or destination other than the EUD/Encryption Components, Outer Encryption Component, Gray Firewall/Encryption Component, Inner Encryption Component, or Gray Data services.	MA, WLAN	T=O	
CM-MP2-3	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Outer Encryption Component, Gray Firewall/Encryption Component, Inner Encryption Component, or Gray Data services.	MA, WLAN	T=O	
CM-MP2-4	The monitoring capability must log communication between EUDs.	MA, WLAN	T=O	
CM-MP4-1	The monitoring capability must log unusual data movement within or out of the network.	MA, WLAN	T=O	
CM-MP4-2	The monitoring capability must log any attempt to connect to any external domain or IP address from the Red Network.	MA, WLAN	T=O	
CM-MP4-5	The monitoring capability must log detection of any protocol or port outside of those specifically allowed by the Inner Firewall and/or Inner Encryption Component.	MA, WLAN	T=O	
CM-MP5-6	The monitoring capability must log any attempt to scan the EUD/Encryption Components, Inner Encryption Component, Inner Firewall or Red Data Network.	MA, WLAN	T=O	
CM-MP8-3	The EUDs must log if there are three or more failed login attempts on the EUD within 24-hours.	MA, WLAN	T=O	
CM-MP8-4	The EUDs must log if configuration changes are made to the EUD.	MA, WLAN	T=O	
CM-MP8-5	The EUDs must log if there is any attempt by the EUD to reach an unauthorized IP addresses, domains, or networks.	MA, WLAN	T=O	
CM-MP8-6	The EUDs must log if an unauthorized application or program is installed on the EUD.	MA, WLAN	T=O	

DRAFT

Req #	Requirement Description	Capability Package	Threshold/ Objective	Alternative
CM-MP8-11	Encryption Component Clients must log establishment of a VPN tunnel.	MA, WLAN	T=O	
CM-MP8-12	TLS Clients must log establishment of a TLS tunnel.	MA	T=O	
CM-MP8-13	Encryption Component Clients must log termination of a VPN tunnel.	MA, WLAN	T=O	
CM-MP8-14	TLS Clients must log termination of a TLS connection.	MA	T=O	
CM-MP8-15	The EUD must log signature verification and certificate validation events.	MA, WLAN	T=O	
CM-CD-1	Data passing from the Black Network to a higher classification level must traverse through an approved CDS.	All	T=O	
CM-CD-2	Data passing from the Gray Network to a higher classification level must traverse through an approved CDS.	All	T=O	
CM-CD-3	One-way Passive Fiber Optical Network Taps may be used without a CDS to transfer raw network captures between networks as long as data does not flow from higher classification to lower classification (e.g., Red to Gray).	All	T=O	
CM-CD-4	If a CDS is being leveraged within the solution, then it must adhere with all applicable organizational policy and be on the NCDSMO CDS Baseline. (For example: DoD customers must also adhere to DoDI 8540.01 and the DISN Connection Process Guide)	All	T=O	
CM-CD-5	If a CDS is being used to transfer data between Black Network and the Gray, and Red or another secured network then a Cyber One-Way Tap or an NSA evaluated diode must be used between the Black Network and the CDS.	All	T=O	
CM-CD-6	If a CDS is being used to transfer data between Gray Network and the Red or another secured network, then a one-way Cyber One-Way Tap or an NSA evaluated diode must be used between the Gray Network and the CDS.	All	T=O	

DRAFT