



National Security  
Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## MULTI-SITE CONNECTIVITY CAPABILITY PACKAGE

This Commercial Solutions for Classified (CSfC) Capability Package describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with Internet Protocol Security (IPsec), Media Access Control Security (MACsec), or both encryption protocols.

Version 0.8  
May 4, 2016



# Multi-Site Connectivity Capability Package



## CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Multi-Site Connectivity (MSC) Capability Package	0.8	May 4, 2016	Initial release of CSfC Multi-Site Connectivity (MSC) guidance.



# Multi-Site Connectivity Capability Package



## TABLE OF CONTENTS

- 1 Introduction ..... 9
- 2 Purpose of This Document ..... 9
- 3 Use of This Document ..... 9
- 4 Description of the MSC Solution ..... 11
  - 4.1 Networks ..... 11
    - 4.1.1 Red Network ..... 12
    - 4.1.2 Gray Network ..... 12
    - 4.1.3 Black Network ..... 12
  - 4.2 Data, Management, and Control Plane Traffic ..... 13
  - 4.3 High-Level Design ..... 14
    - 4.3.1 Multiple Sites ..... 14
      - 4.3.1.1 Independently Managed Sites ..... 15
      - 4.3.1.2 Centrally Managed Sites ..... 15
    - 4.3.2 Multiple Security Levels ..... 16
      - 4.3.2.1 Networks Operating at the Same Classification Level ..... 17
      - 4.3.2.2 Networks Operating at Different Classification Levels ..... 18
    - 4.3.3 Layering Options ..... 21
    - 4.3.4 Authentication ..... 23
  - 4.4 Other Protocols ..... 23
  - 4.5 Availability ..... 24
- 5 Solution Components ..... 25
  - 5.1 Outer Encryption Components ..... 25
  - 5.2 Gray Network Firewalls ..... 26
  - 5.3 Gray Management Services ..... 26
    - 5.3.1 Gray Administration Workstation ..... 27
    - 5.3.2 Outer Certificate Authority (Located on Gray Network) ..... 27
    - 5.3.3 Gray Certificate Revocation Services ..... 27
    - 5.3.4 Outer Key Generation Component ..... 28
    - 5.3.5 Gray Security Information and Event Management (SIEM) ..... 28



# Multi-Site Connectivity Capability Package



- 5.4 Inner Encryption Components ..... 28
- 5.5 Red Management Services..... 29
  - 5.5.1 Red Administration Workstation ..... 29
  - 5.5.2 Inner Certificate Authority (Located on Red Network)..... 29
  - 5.5.3 Red Certificate Revocation Services..... 30
  - 5.5.4 Inner Key Generation Component (Located on Red Network)..... 30
  - 5.5.5 Red Security Information and Event Management (SIEM) ..... 30
- 5.6 Other Controls..... 31
- 6 Continuous Monitoring..... 31
  - 6.1 Monitoring Network Traffic ..... 31
  - 6.2 Monitoring Log Data ..... 34
- 7 Key Management ..... 34
  - 7.1 Certificates ..... 34
    - 7.1.1 Certificate Issuance, Renewal and Rekey..... 34
    - 7.1.2 External Distribution of Certificate Revocation Lists ..... 35
  - 7.2 Connectivity Association Keys..... 37
    - 7.2.1 Connectivity Association Key Issuance, Renewal and Rekey ..... 38
    - 7.2.2 Connectivity Association Key Compromise Recovery ..... 39
- 8 Threats ..... 39
  - 8.1 Passive Threats..... 39
  - 8.2 External (Active) Threats..... 40
    - 8.2.1 Rogue Traffic ..... 40
    - 8.2.2 Malware and Untrusted Updates ..... 41
    - 8.2.3 Denial of Service..... 41
    - 8.2.4 Social Engineering ..... 42
  - 8.3 Insider Threats ..... 42
  - 8.4 Supply Chain Threats ..... 42
  - 8.5 Integrator Threats..... 44
- 9 Requirements Overview ..... 44
  - 9.1 Threshold and Objective Requirements ..... 44



# Multi-Site Connectivity Capability Package



- 9.2 Requirements Designators..... 45
- 10 Requirements for Selecting Components..... 46
- 11 Configuration Requirements..... 48
  - 11.1 Overall Solution Requirements ..... 49
  - 11.2 VPN Gateway Requirements..... 50
  - 11.3 MACsec Device Requirements ..... 52
  - 11.4 Additional Requirements for Inner Encryption Components ..... 54
  - 11.5 Additional Requirements for Outer Encryption Components ..... 54
  - 11.6 Port Filtering Requirements for Solution Components ..... 55
  - 11.7 Configuration Change Detection Requirements..... 57
  - 11.8 Device Management Requirements ..... 58
  - 11.9 Continuous Monitoring Requirements ..... 60
  - 11.10 Auditing Requirements ..... 61
  - 11.11 Key Management Requirements ..... 63
    - 11.11.1 General Requirements..... 63
    - 11.11.2 Certificate Issuance Requirements ..... 65
    - 11.11.3 Certificate Renewal and Rekey Requirements..... 67
    - 11.11.4 Certificate Revocation Requirements ..... 67
    - 11.11.5 CAK Generation and Distribution Requirements ..... 69
    - 11.11.6 CAK Usage Requirements..... 70
    - 11.11.7 CAK Update Requirements ..... 71
    - 11.11.8 CAK Compromise Recovery Requirements ..... 71
  - 11.12 Gray Network Firewall Requirements..... 72
- 12 Requirements for Solution Operation, Maintenance, and Handling..... 73
  - 12.1 Requirements for the Use and Handling of Solutions ..... 73
  - 12.2 Requirements for Incident Reporting ..... 75
- 13 Role-Based Personnel Requirements..... 77
- 14 Information to Support AO ..... 79
  - 14.1 Solution Testing ..... 80
  - 14.2 Risk Assessment ..... 81



# Multi-Site Connectivity Capability Package



- 14.3 Registration of Solutions..... 81
- 15 Testing Requirements ..... 82
  - 15.1 Product Selection ..... 82
  - 15.2 Overall Solution..... 84
  - 15.3 VPN Gateway Configurations..... 85
  - 15.4 MACsec Device Configurations ..... 86
  - 15.5 Inner and Outer Encryption Component Configurations..... 87
  - 15.6 Port Filtering ..... 89
  - 15.7 Configuration Change Detection..... 90
  - 15.8 Continuous Monitoring ..... 90
  - 15.9 Auditing..... 92
  - 15.10 Key Management ..... 95
    - 15.10.1 Certificate Authorities and Certificates..... 95
    - 15.10.2 Key Generation Components and Connectivity Association Keys ..... 99
  - 15.11 Gray Network Firewall ..... 101
    - 15.11.1 Gray Network Firewall Filtering Rules..... 101
    - 15.11.2 Gray Network Firewall HTTP Filtering Rules ..... 102
    - 15.11.3 Gray Network Firewall Management..... 103
    - 15.11.4 Gray Network Firewall Address Spoofing ..... 104
    - 15.11.5 Gray Network Firewall HTTP Deep Packet Inspection ..... 105
  - 15.12 Incident Reporting Guidance ..... 107
  - 15.13 Implementation of Guidance ..... 107
  - 15.14 Solution Functionality ..... 108
- Appendix A. Glossary of Terms..... 109
- Appendix B. Acronyms ..... 113
- Appendix C. References ..... 116



# Multi-Site Connectivity Capability Package



## TABLE OF FIGURES

Figure 1. Two Encryption Tunnels Protect Data across an Untrusted Network ..... 11

Figure 2. MSC Solution Connecting Two Independently Managed Sites..... 14

Figure 3. MSC Solution Connecting a Central Management Site and a Remote Site ..... 16

Figure 4. MSC Solution for Two Networks at the Same Classification Level ..... 17

Figure 5. Using Outer Encryption Components for Gray Network Filtering ..... 19

Figure 6. Using Standalone Gray Network Firewalls for Gray Network Filtering..... 20

Figure 7. Encapsulating MACsec on an Internal Interface ..... 22

Figure 8. Encapsulating MACsec with a Separate Device ..... 22

Figure 9. MSC Solution with Redundant Outer Encryption Components..... 24

Figure 10. MSC Solution Continuous Monitoring ..... 32

Figure 11. MSC Solution using CRL Distribution Points and OCSP Responders ..... 36

## TABLE OF TABLES

Table 1. Layering Options ..... 21

Table 2. Requirement Digraphs ..... 45

Table 3. Product Selection (PS) Requirements ..... 46

Table 4. Overall Solution Requirements (SR) ..... 49

Table 5. IPsec Encryption (Approved Algorithms for Classified)..... 50

Table 6. VPN Gateway (VG) Requirements ..... 51

Table 7. MACsec Encryption (Approved Algorithms for Classified) ..... 52

Table 8. MACsec Device (MD) Requirements ..... 52

Table 9. Additional Requirements for Inner Encryption Components (IR) ..... 54

Table 10. Additional Requirements for Outer Encryption Components (OR) ..... 54

Table 11. Port Filtering (PF) Requirements for Solution Components ..... 55

Table 12. Configuration Change Detection (CM) Requirements ..... 57

Table 13. Device Management (DM) Requirements ..... 58

Table 14. Requirements for Continuous Monitoring (MR) ..... 60

Table 15. Auditing (AU) Requirements ..... 61

Table 16. General Key Management (KM) Requirements ..... 63

Table 17. Certificate Issuance Requirements ..... 65



# Multi-Site Connectivity Capability Package



Table 18. Certificate Renewal and Rekey Requirements.....	67
Table 19. Certificate Revocation Requirements .....	67
Table 20. CAK Generation and Distribution Requirements .....	69
Table 21. CAK Usage Requirements.....	70
Table 22. CAK Update Requirements.....	71
Table 23. CAK Compromise Recovery Requirements .....	71
Table 24. Gray Network Firewall (FW) Requirements.....	72
Table 25. Requirements for the Use and Handling of Solutions.....	73
Table 26. Incident Reporting Requirements (RP) .....	76
Table 27. Role-Based Personnel Requirements.....	78
Table 28. Test (TR) Requirements.....	81



# Multi-Site Connectivity Capability Package



## 1 INTRODUCTION

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

IAD is delivering a generic CSfC Multi-Site Connectivity (MSC) CP to meet the demand for data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products. MSC CP Version 0.8 enables customers to implement layered encryption between two or more sites. This CP takes lessons learned from multiple proof-of-concept demonstrations. These demonstrations included a layered use of COTS products for the protection of classified information.

## 2 PURPOSE OF THIS DOCUMENT

This CP provides high-level reference designs and corresponding configuration information that allow customers to select COTS products from the CSfC Components Lists for their MSC Solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while in transit. As described in Section 10, customers must ensure that the components selected from the CSfC Components Lists will permit the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold requirements, or the corresponding Objective requirements applicable to the selected capabilities, must be implemented, as described in Section 9.

Customers who want to use this CP must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (<https://www.nsa.gov/resources/everyone/csfc>).

## 3 USE OF THIS DOCUMENT

This document may not be used for a CSfC solution without formally obtaining support from NSA for the effort prior to presenting a solution to the implementing organization's Authorizing Official (AO). United States Government entities interested in presenting solutions to their AOs in accordance with this guidance must first obtain NSA support by submitting a request for CP application support to their NSA/IAD Client Advocate. In the future, however, customers and their solution providers will be able to use a later version of this guidance to implement solutions without such NSA/IAD involvement. Until that time, customers and solution providers may still register solutions designed according to Version 3.2 of the Virtual Private Network (VPN) CP, dated 20 August 2015; see Section 3 of that document for details.



# Multi-Site Connectivity Capability Package



Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the MSC CP Maintenance Team at [msc\\_cp@nsa.gov](mailto:msc_cp@nsa.gov).

Committee on National Security Systems (CNSS) Policy No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems (NSS)*, is in the process of being updated to reflect the recently published CNSS Advisory Memorandum (AM) Information Assurance (IA) 02-15. CNSS AM IA 02-15 expands on the guidance contained in CNSS Policy No. 15 and identifies additional public algorithms to protect information within NSS. Specifically, the following algorithms will be required to protect all NSS up to Top Secret:

- AES 256 (confidentiality)
- RSA 3072 or ECDSA P-384 (digital signature and authentication)
- RSA 3072, DH 3072 or ECDH P-384 (key exchange)
- SHA-384 (hashing and integrity)

MSC Solutions shall comply with CNSS policies and instructions. Any conflicts identified between this CP and NSS or local policy should be provided to the MSC CP Maintenance Team.

The following Legal Disclaimer relates to the use of this CP:

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

The User of this CP agrees to hold harmless and indemnify the United States (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 CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.



# Multi-Site Connectivity Capability Package

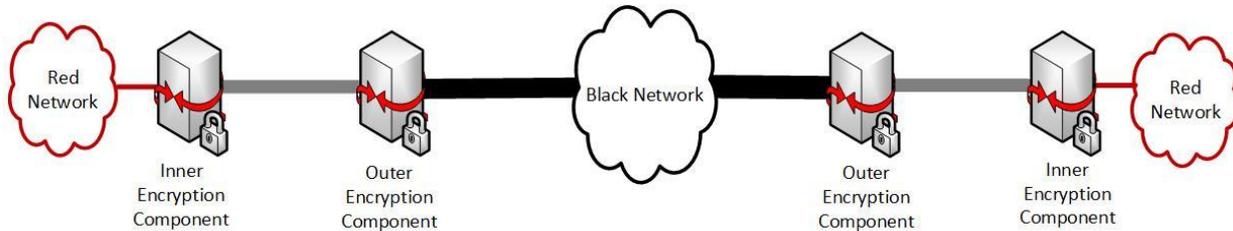


## 4 DESCRIPTION OF THE MSC SOLUTION

This CP describes a general MSC Solution to protect classified information as it travels across either an untrusted network or a network of a different classification level. The solution supports interconnecting two or more networks operating at the same security level via encryption tunnels, where the security level encompasses the classification level, list of compartments, dissemination controls, and other such controls over information. The solution provides sufficient flexibility to be applicable to many use cases of MSC implementations.

The MSC Solution uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either Internet Protocol Security (IPsec) generated by a VPN Gateway or Media Access Control Security (MACsec) generated by a MACsec Device. VPN Gateways and MACsec Devices are implemented as part of the network infrastructure.

Throughout this CP, the term “Encryption Component” refers generically to either a VPN Gateway or a MACsec Device. “Inner Encryption Component” refers to the component that terminates the Inner layer of encryption and “Outer Encryption Component” refers to the component that terminates the Outer layer of encryption.



**Figure 1. Two Encryption Tunnels Protect Data across an Untrusted Network**

As shown in Figure 1, before being sent across the untrusted network, each packet or frame of classified data is encrypted twice: first by an Inner Encryption Component, and then by an Outer Encryption Component. At the other end of the data flow, the received packet is correspondingly decrypted twice: first by an Outer Encryption Component, and then by an Inner Encryption Component.

Products listed on a CSfC Components Lists are not guaranteed to be interoperable with all other products on the Components List. Customers and integrators should perform interoperability testing to ensure the components selected for their MSC Solution are interoperable.

### 4.1 NETWORKS

This CP uses the following terminology to describe the various networks that comprise a MSC Solution and the types of traffic present on each. The terms Red, Gray, and Black refer to the level of protection applied to the data as described below.



# Multi-Site Connectivity Capability Package



## 4.1.1 RED NETWORK

Red data consists of unencrypted classified data while Gray data consists of singly encrypted classified data. A Red network contains Red data and can contain Gray data. The Red network is logically located behind an Inner Encryption Component. The networks connected to one another through the MSC Solution are Red networks. Red networks are under the control of the solution owner or a trusted third party. Red networks may only communicate with one another through the MSC Solution if the networks operate at the same security level.

## 4.1.2 GRAY NETWORK

A Gray network contains classified data that has been encrypted once. The network between an Inner Encryption Component and an Outer Encryption Component is a Gray network. The Gray network is physically and logically under the control of the solution owner or a trusted third party. A MSC Solution compliant with this CP treats a Gray network as a classified network even though all classified data is singly encrypted. If a solution owner's classification authority determines that the data on a Gray network is classified, perhaps by determining the Internet Protocol (IP) addresses used on the Gray network interfaces are classified at some level, then the MSC Solution described in this CP cannot be implemented, as it is not designed to ensure that such information will be afforded two layers of protection.

Gray networks are either physically or cryptographically divided into two sub-networks, as follows:

- Gray Management network – The part of a Gray network that contains the management functions to run components supporting the Outer Encryption Component, including the Outer tunnel Certificate Authority (CA) and the Gray admin and audit server functions. Note, the Inner and Outer CAs can both reside within the Red network.
- Gray Data network – The part of a Gray network that carries data between Inner Encryption Components and Outer Encryption Components.

## 4.1.3 BLACK NETWORK

A Black network contains classified data that has been encrypted twice. The network connecting the Outer Encryption Components together is a Black network. Black networks are not necessarily (and often will not be) under the control of the solution owner, and may be operated by an untrusted third party.



# Multi-Site Connectivity Capability Package



## 4.2 DATA, MANAGEMENT, AND CONTROL PLANE TRAFFIC

Data plane traffic is classified information, encrypted or not, that is being passed through the MSC Solution. The MSC Solution exists to encrypt and decrypt data plane traffic. All data plane traffic within the Gray and Black networks is encapsulated within the IPsec and MACsec protocols.

Management plane traffic is used to configure and monitor Solution Components. It includes the communications between a system administrator and a component, as well as the logs and other status information forwarded from a Solution Component to a log server, Security Information and Event Manager (SIEM), or similar repository. Management plane traffic on Red and Gray networks is encapsulated within the Secure Shell version 2 (SSHv2), IPsec, MACsec, or Transport Layer Security (TLS).

Control plane traffic consists of other protocols necessary for the network to function that carry neither data nor management traffic. Control plane traffic is typically not initiated directly on behalf of a user (unlike data traffic) or a system administrator (unlike management traffic). Many, but not all, control plane protocols operate at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) model.

Examples of control plane traffic include, but are not limited to, the following:

- Network address configuration (e.g., Dynamic Host Configuration Protocol (DHCP), Neighbor Discovery Protocol (NDP))
- Address resolution (e.g., Address Resolution Protocol (ARP), NDP)
- Name resolution (e.g., Domain Name System (DNS))
- Time synchronization (e.g., Network Time Protocol (NTP), Precision Time Protocol (PTP))
- Route advertisement (e.g., Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Border Gateway Protocol (BGP))
- Certificate status distribution (e.g., Online Certificate Status Protocol (OCSP), Hypertext Transfer Protocol (HTTP) download of Certificate Revocation Lists (CRLs))

In general, this CP does not impose detailed requirements on control plane traffic, although control plane protocols may be used to implement certain requirements. For example, requirements MSC-SR-4 and MSC-SR-5 (see Section 11.1) require that time synchronization be performed, but do not require the use of any particular time synchronization protocol or technique. Notable exceptions are for IPsec session establishment and for certain certificate status distribution scenarios (see Section 7.1.2) where, given their impact on the security of the solution, this CP does provide detailed requirements. Unless otherwise specified in this CP, the usage of specific control plane protocols is left to the solution owner to approve, but any control plane protocols not approved by the solution owner should be disabled.



# Multi-Site Connectivity Capability Package



Data plane and management plane traffic are generally required to be separated from one another by using physical or cryptographic separation. Use of a Virtual Local Area Network (VLAN) alone is not sufficient to separate data plane and management plane traffic. As a result, a solution may, for example, have a Gray Data network and a Gray Management network which are separate from one another, where the components on the Gray Management network are used to manage the components on the Gray Data network. Given that some control plane traffic is necessary for a network to function, there is no general requirement that control plane traffic be similarly separated, unless otherwise specified.

## 4.3 HIGH-LEVEL DESIGN

The MSC Solution is adaptable to support capabilities for multiple sites and/or multiple security levels, depending on the needs of the customer implementing the solution. If a customer does not have a need for supporting multiple sites or multiple security levels, then those elements need not be included as part of the implementation. However, any implementation of the MSC Solution must satisfy all of the applicable requirements specified in this CP, as explained in Section 9.

### 4.3.1 MULTIPLE SITES

Figure 2 depicts two Red networks at different sites that operate at the same security level, connected to one another through the MSC Solution. Here, each Red network has two Encryption Components associated with it: an Inner Encryption Component connected to the Red network, and an Outer Encryption Component between the Inner Encryption Component and the Black network.

There are two layers of encryption tunnels between any pair of sites communicating directly with one another: one encryption tunnel between their Outer Encryption Components, and a second encryption tunnel between their Inner Encryption Components. Each set of Inner or Outer Encryption Components can provide encryption using either IPsec or MACsec.

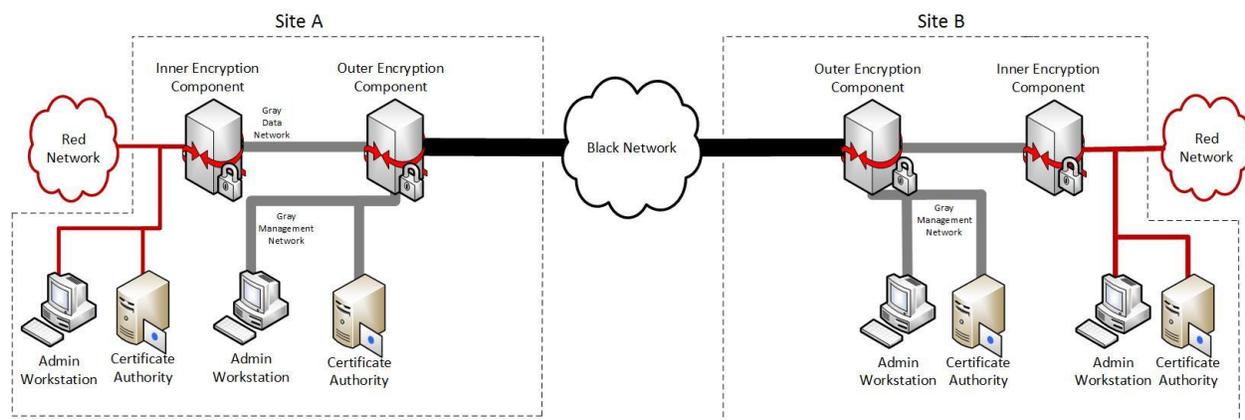


Figure 2. MSC Solution Connecting Two Independently Managed Sites



# Multi-Site Connectivity Capability Package



There is no limit to the number of sites that may be incorporated into a single MSC Solution.

Sites in the solution may be managed independently of one another, or may be remotely managed from a central site.

#### ***4.3.1.1 Independently Managed Sites***

For independently managed sites, each site performs the administration of its own Encryption Components and has the option of using either locally-run Certificate Authorities (CAs) that they manage and control (see Figure 2) or, where available, enterprise CAs which are not necessarily managed by the solution owner. Each site needs to ensure that the Encryption Components selected interoperate with those at the other sites.

Since there is no remote management, no management traffic will cross the Black network, encrypted or otherwise. Any VPN Gateways at each site need to have the signing certificates and revocation information for the corresponding CAs used by the other sites in the MSC Solution. This high-level design requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. Similarly, any MACsec Devices at each site need to have the same Connectivity Association Key (CAK) used by other sites in the MSC Solution.

This model has the advantage of allowing communication between larger organizations that have a need to share information while maintaining independence.

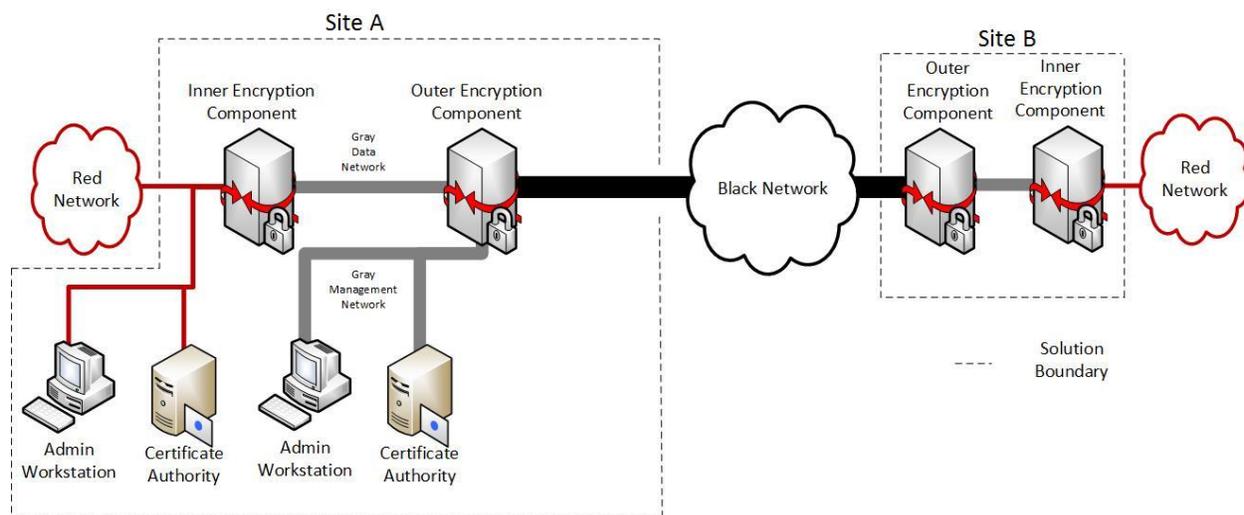
Note that while Figure 2 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same design as those in the figure.

#### ***4.3.1.2 Centrally Managed Sites***

If remote management is used, personnel at a single geographic site administer and perform keying for all the various sites included in the solution, as shown in Figure 3. In this case, because the administration is done by one group of Security Administrators and CA Administrators (see Section 13), they can ensure the interoperability of each site as new sites are added. A maximum of two CAs are needed: one on the Red network for all the Inner VPN Gateways and one on the Gray Management network for all the Outer VPN Gateways. If available, enterprise CAs should be used. If MACsec Devices are being used on either or both layers, CAs are not required since these devices are using CAKs.



# Multi-Site Connectivity Capability Package



**Figure 3. MSC Solution Connecting a Central Management Site and a Remote Site**

Because the central management site manages the Encryption Components at the other sites over the network, encryption is used to logically separate data and management traffic as it passes between sites. Gray management traffic is encrypted using SSHv2, TLS, IPsec, or MACsec before being routed through the Outer Encryption Component to another site. The SSHv2, TLS, IPsec or MACsec serves as the inner layer of encryption for Gray management traffic, and the encryption tunnel provided by the Outer Encryption Component serves as the outer layer of encryption. Red management traffic is similarly encrypted before being routed through the Inner and Outer Encryption Components to another site. As a result, all management traffic between sites is encrypted at least twice before traversing the Black network.

This model makes it easier to add sites because of the centralized administration.

Note that while Figure 3 depicts only two sites, this solution can scale to include numerous sites, with each additional site having the same high-level design as the remotely managed site in the figure.

## 4.3.2 MULTIPLE SECURITY LEVELS

A single implementation of the MSC Solution may support Red networks of different security levels. The MSC Solution provides secure connectivity between the Red networks within each security level while preventing Red networks of differing security levels from communicating with one another. This enables a customer to use the same physical infrastructure to carry traffic from multiple networks. Although each Red network will still require its own Inner Encryption Component, a site may use a single Outer Encryption Component to encrypt and transport traffic that had been encrypted by Inner Encryption Components of varying security levels.



# Multi-Site Connectivity Capability Package



There is no limit to the number of different security levels that a MSC Solution may support. Unclassified networks can also be included behind the Outer Encryption Component.

MSC Solutions supporting multiple security levels may include independently managed sites (see Section 4.3.1.1) or centrally managed sites (see Section 4.3.1.2). Given both cases, separate CAs, CAKeys, and management devices are needed to manage the Inner Encryption Components at each security level. For example, Figure 3 depicts a Central Management Site and a Remote Site, but Network 1 and Network 2 each have their own CA, CAKeys, and management devices, which prevent their Inner Encryption Components from being able to authenticate with one another.

### 4.3.2.1 Networks Operating at the Same Classification Level

When Red networks that operate at the same classification level but at different security levels, the cryptographic separation provided by the Inner Encryption Components is sufficient to protect against unintended data flows between security levels. Two Inner Encryption Components for networks of different classification levels will be unable to mutually authenticate with each other because they trust different CAs which do not have a trust relationship with one another or they use different CAKeys which will not provide authentication. This prevents the establishment of an encryption tunnel between the two components.

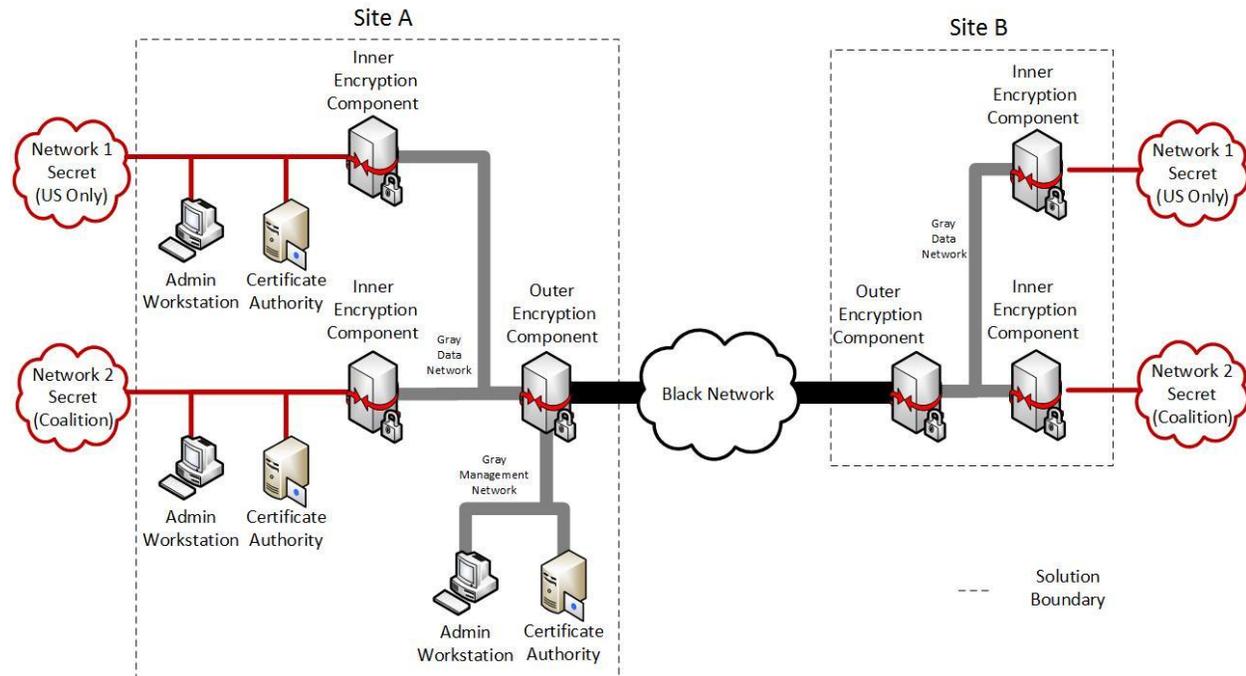


Figure 4. MSC Solution for Two Networks at the Same Classification Level



# Multi-Site Connectivity Capability Package



Figure 4 illustrates a MSC Solution between two sites that carries traffic between two Red networks: a Secret U.S.-only network (Network 1) and a Secret Coalition network (Network 2). Because Network 1 and Network 2 both operate at the Secret classification level, their singly-encrypted traffic can be carried over the Gray network without any additional security controls in place.

Although not required by this CP, a solution owner may choose to implement the additional security described in Section 4.3.2.2 to provide additional protection against unintended data flows between Red networks at the same classification level.

### ***4.3.2.2 Networks Operating at Different Classification Levels***

A single implementation of the MSC Solution may support Red networks of different security levels, to include unclassified networks. The MSC Solution provides secure connectivity between the Red networks within each security level while preventing Red networks of differing security levels from communicating with one another. This enables a customer to use the same infrastructure to carry traffic from multiple networks.

For Red networks of different classification levels, the cryptographic separation of their traffic on a Gray network, as described in Section 4.3.2.1, is still present. However, because the consequences of an unintended data flow between different classification levels are more severe than of one with a single classification level, an additional mechanism is necessary to further guard against such a flow from occurring.

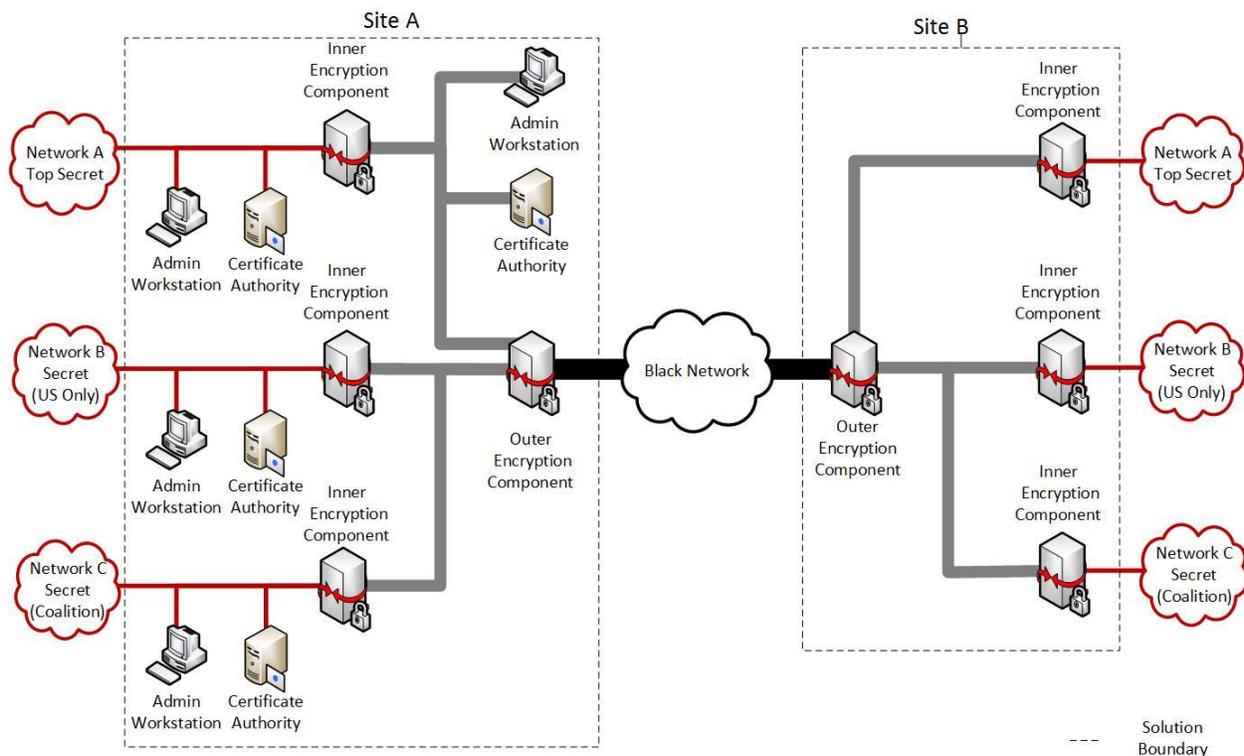
This CP uses packet filtering within Gray networks as an additional mechanism to prevent data flows between networks of different classification levels. Any physical path through a Gray network between multiple Inner Encryption Components supporting Red networks of different classification levels must include at least one filtering component. This filtering component restricts the traffic flowing through it based primarily on the Gray network source and destination addresses, only allowing a packet through if the source and destination components are intended to communicate with one another and dropping the packet if they are not.

When multiple classification levels are being used, it is critical to enforce proper IP address assignment and firewall rulesets. The IP address assigned must be unique to that classification level such that each network's Encryption Component is only able to send and receive traffic to its respective Encryption Component at the other site.

Additionally, filtering components are included between the components used for management of the Gray networks themselves (namely, Administration Workstations and locally-run CAs) and Inner Encryption Components that support Red networks of a lower classification level than the highest-classification Red network supported by the solution. In other words, Administration Workstations and locally-run CAs on Gray networks are treated as and grouped with the Inner Encryption Component with the highest-classification Red network.



# Multi-Site Connectivity Capability Package



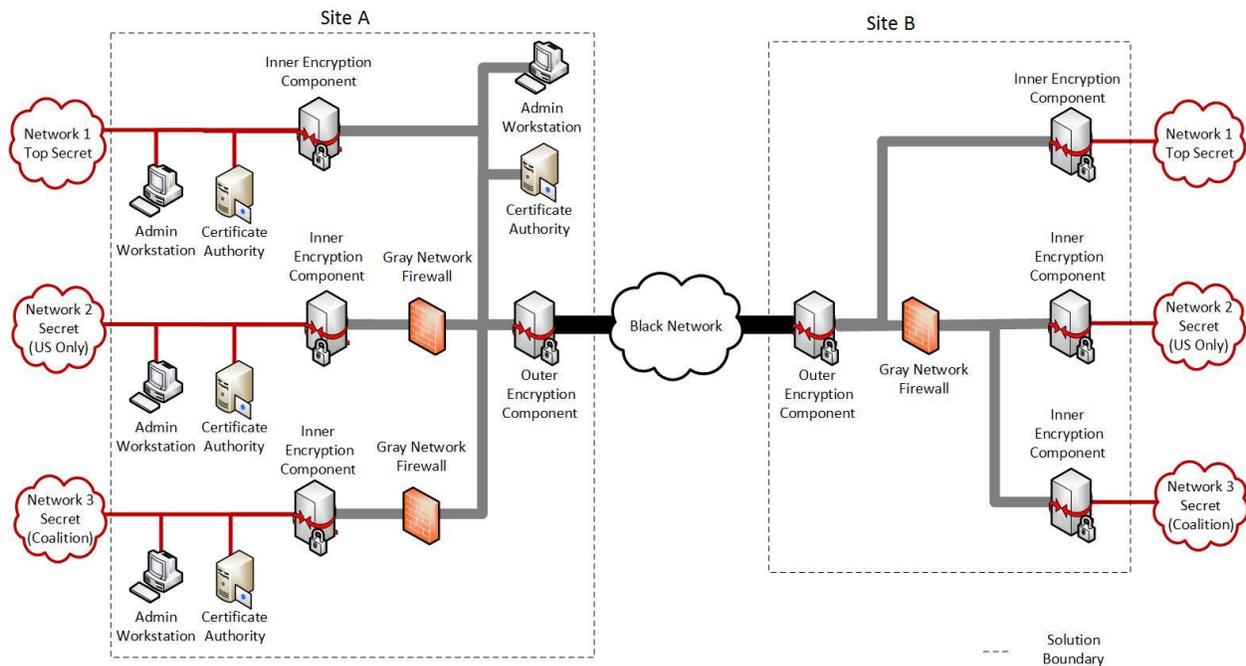
**Figure 5. Using Outer Encryption Components for Gray Network Filtering**

This CP provides some flexibility in where this filtering takes place within the Gray network. The simplest option is to implement the filtering on the Outer Encryption Components, as shown in Figure 6. Here, the MSC Solution is supporting three Red networks: one Top Secret network (Network 1) and two Secret networks (Networks 2 and 3). Any path through the Gray network between an Inner Encryption Component for a Secret network and an Inner Encryption Component for the Top Secret network (or for the Gray Network's Administration Workstation or CA) includes at least one Outer Encryption Component, which performs the filtering function. Effectively, the Gray network at each site is split into two separate networks which only meet at the Outer Encryption Component: one supporting the Secret networks, and one supporting the Top Secret network (and Gray network management).

Note that there is no filtering component on the path between the Inner Encryption Components for Network 2 and Network 3 within each site, but this is acceptable because Networks 2 and 3 operate at the same classification level; see Section 4.3.2.1 for more details.



# Multi-Site Connectivity Capability Package



**Figure 6. Using Standalone Gray Network Firewalls for Gray Network Filtering**

However, some solutions may be subject to physical constraints that prevent relying exclusively on the Outer Encryption Components to provide the filtering function. To accommodate these situations one or more Gray Network Firewalls can be included in a Gray network to perform the filtering in addition to the Outer Encryption Components, as shown in Figure 6. Here, the Gray network is laid out in such a way that the paths between any two Inner Encryption Components within the same site do not pass through an Outer Encryption Component. Instead, standalone Gray Network Firewalls have been placed at each site between the Inner Encryption Components for the Secret networks and the rest of the Gray network; these Gray Network Firewalls are responsible for dropping any packets between an Inner Encryption Component for Network 1 and an Inner Encryption Component for Network 2 or 3.

Figure 6 also illustrates that there is flexibility in the specific placement of Gray Network Firewalls, as long as their placement satisfies the requirement that any path between Inner Encryption Components for networks of different classification levels is met. Site A and Site B in the figure demonstrate two possible placements of Gray Network Firewalls that would satisfy this requirement, although other acceptable placements are also possible.

Including one or more standalone Gray Network Firewalls in a solution does not remove the requirement to perform the filtering on the Outer Encryption Component as well. Outer Encryption Components are uniquely positioned to block traffic between Inner Encryption Components supporting Red networks of different classification levels when one of those Inner Encryption Components is located at a different site.



# Multi-Site Connectivity Capability Package



### 4.3.3 LAYERING OPTIONS

Each layer of the MSC Solution can use either an IPsec tunnel or MACsec tunnel. An IPsec tunnel is established between VPN Gateways. A MACsec tunnel is established between MACsec Devices. Table 1 identifies four different layering options provided by this CP.

**Table 1. Layering Options**

Configuration	Inner Tunnel	Outer Tunnel
1	IPsec	IPsec
2	IPsec	MACsec
3	MACsec	IPsec
4	MACsec	MACsec

**NOTE: The fourth configuration (MACsec on both layers) may not be available in the final release of this CP. Customers desiring to use a configuration with MACsec on both layers should contact their Client Advocate.**

MACsec was designed to provide hop-to-hop security within a Local Area Network (LAN). As MACsec-encrypted traffic arrives at an interface, it is typically decrypted, examined, and re-encrypted after determining its destination.

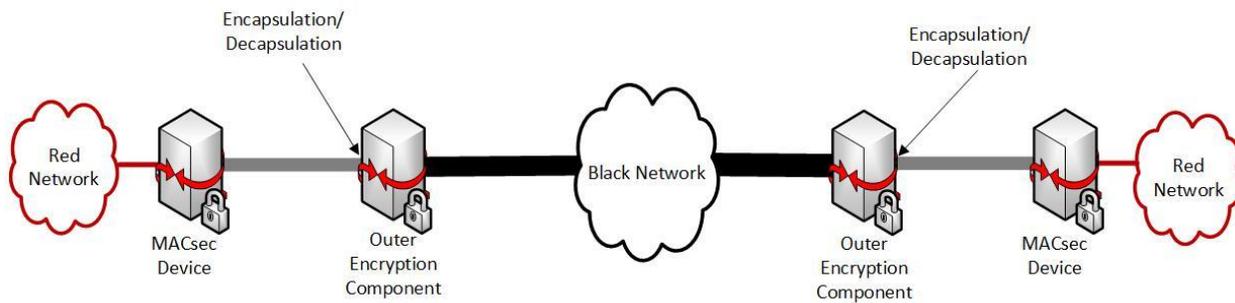
The MACsec-encrypted traffic needs to be encapsulated if the MACsec Device is the first layer of encryption in the MSC Solution or if the MACsec-encrypted traffic needs to traverse an IP-based network. The reason for encapsulation is to ensure the MACsec-encrypted traffic is not decrypted prior to reaching its destination and to ensure the second layer of encryption can be applied.

In some commercial MACsec Devices, encapsulation can be applied on the internal interface by creating a pseudowire (see Figure 7). If this feature is not supported, a standalone device is needed to encapsulate the MACsec-encrypted data (see Figure 8). If using a standalone device, the internal interface will be connected to the Internal MACsec Device and the external interface will be connected to the Outer Encryption Component. Since this router or switch resides in the Gray network, all requirements for Solution Components must be implemented for it.

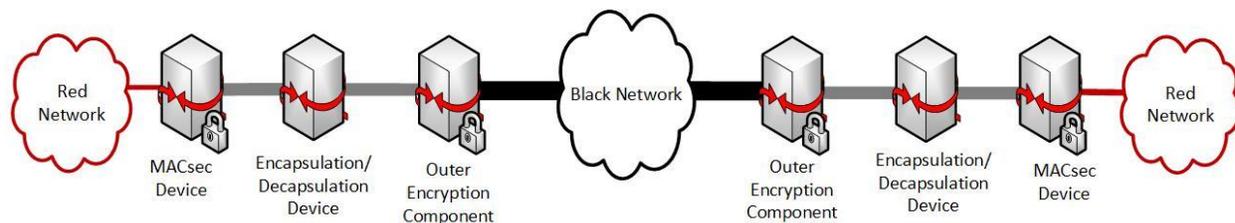
This CP does not mandate the use of a specific protocol for encapsulation. Options include, but are not limited to, Layer 2 Tunneling Protocol version 3 (L2TPv3) and Ethernet over Multiprotocol Label Switching (EoMPLS).



# Multi-Site Connectivity Capability Package



**Figure 7. Encapsulating MACsec on an Internal Interface**



**Figure 8. Encapsulating MACsec with a Separate Device**

There are some scenarios when a MACsec Device provides the outer tunnel of encryption and the MACsec-encrypted traffic needs to be encapsulated prior to handing it off to the Black network. In these scenarios, this additional step falls outside the boundary of the MSC Solution. However, applying the general requirements for Solution Components is highly recommended.

In the current MACsec standard, the entire frame is encrypted with the exception of the source and destination addresses. Draft amendment IEEE 802.1AEcg provides the option of moving the Virtual LAN (VLAN) identification (ID) tag out of the encrypted payload and into the clear in the header. The benefits of moving the VLAN ID tag into the clear include service multiplexing (i.e., multiple point-to-point or multipoint services existing on a single physical interface) and providing quality of service (QoS) across a Service Provider's network. This CP allows VLAN ID tags to be used in the clear, if supported in the MACsec Device.

At high speeds, some MACsec Devices may be configured to use an eXtended Packet Number (XPN), as described in IEEE 802.1AEbw2013. Without XPN, the key space for the Secure Association Key (SAK) may be exhausted quickly at high speeds and re-keying at high speeds may interrupt traffic flow. This CP allows the XPN feature to be used, if supported in the MACsec Device.



# Multi-Site Connectivity Capability Package



## 4.3.4 AUTHENTICATION

The MSC Solution provides mutual device authentication between Outer Encryption Components and Inner Encryption Components. The method of authentication is different for VPN Gateways and MACsec Devices.

VPN Gateways authenticate via public key certificates. This CP requires all authentication certificates issued to VPN Gateways to be Non-Person Entity (NPE) certificates. This CP also requires an Inner CA when the Inner Encryption Component is a VPN Gateway and an Outer CA when the Outer Encryption Component is a VPN Gateway.

MACsec Devices authenticate using a Pre-Shared Key (PSK) called a CAK. This CP requires all CAKs and their associated Connectivity Key Names (CKNs) to be generated using an NSA-approved Key Generation Component (KGC). For each MACsec tunnel, a Key Server is identified. The Key Server authenticates the other MACsec Device and provides a SAK to provide confidentiality and integrity for the MACsec tunnel.

## 4.4 OTHER PROTOCOLS

Throughout this document, when IP traffic is discussed, it can refer to either IPv4 or IPv6 traffic, unless otherwise specified. In addition, Red, Gray and Black networks can run either IPv4 or IPv6, and each network is independent from the others in making that decision. In the remainder of the document, if no protocols or standards are specified then any appropriate protocols may be used to achieve the objective.

Public standards conformant Layer 2 control protocols such as ARP are allowed as necessary to ensure the operational usability of the network. Public standards conformant Layer 3 control protocols such as Internet Control Message Protocol (ICMP) may be allowed based on local AO policy, but the default configuration of this solution is for all Layer 3 control protocols to be disabled. Red and Gray network multicast messages and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) may also be allowed depending on local AO policy. Multicast messages received on external interfaces of the Outer Encryption Component shall be dropped.

It is expected that the MSC Solution can be implemented in such a way as to take advantage of standards based routing protocols that are already being used in the network. For example, networks that currently use Generic Routing Encapsulation (GRE) or OSPF protocols can continue to use these in conjunction with this solution to provide routing as long as the AO approves their use.

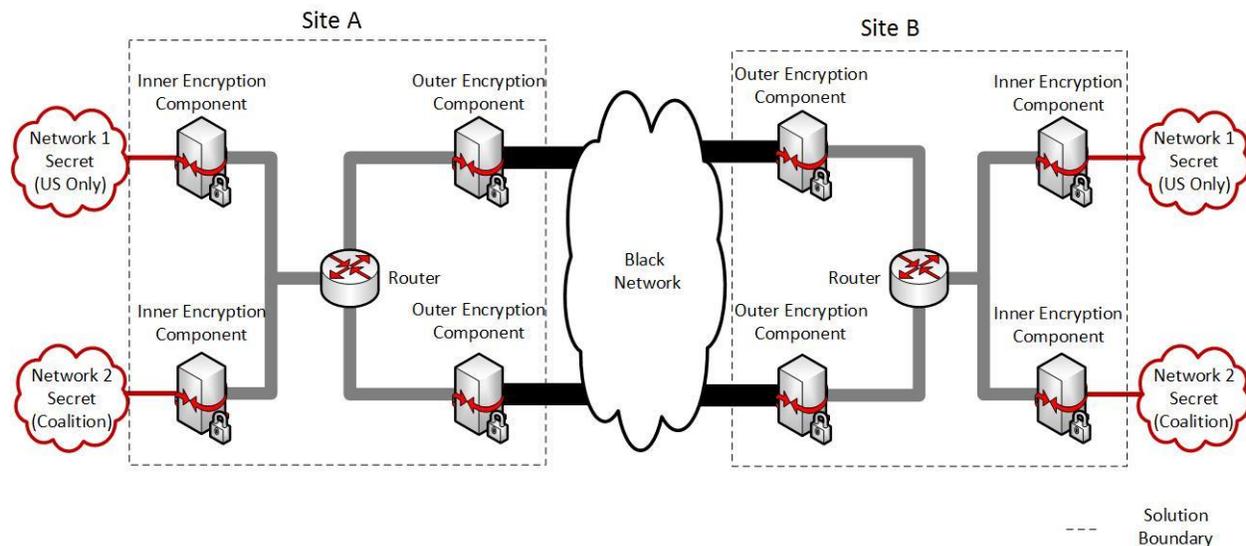


# Multi-Site Connectivity Capability Package



## 4.5 AVAILABILITY

The high-level designs described in Section 4.3 are not designed with the intent of automatically providing high availability, and supporting solution implementations for which high availability is important is not a goal. However, this CP does not prohibit adding redundant components in parallel to allow for component failover or to increase the throughput of the MSC Solution, as long as each redundant component adheres to the requirements of this CP.



**Figure 9. MSC Solution with Redundant Outer Encryption Components**

For example, Figure 9 illustrates a MSC Solution between two sites where each site has a redundant Outer Encryption Component. Management components are omitted from the figure for clarity. There are two outer encryption tunnels that transit the Black network: one between the upper pair of Outer Encryption Components, and one between the lower pair of Outer Encryption Components. Each site's Gray network contains an ordinary router between the Inner and Outer Encryption Components which selects which Outer Encryption Component to route outbound packets to. This router is part of the solution only in the sense that it is part of the network infrastructure of the Gray network; this CP does not levy any security requirements on the router/switch. The MSC Solution can maintain connectivity between the two sites even if one of the Outer Encryption Components fails, because traffic will be routed through the tunnel that has not failed.

The above is only a simple example of how redundancy could be added if needed for a MSC Solution. Implementing standby or failover Encryption Components, performing load balancing between Encryption Components, or other techniques to improve the availability or throughput of the solution are outside the scope of this CP and are not discussed further.



# Multi-Site Connectivity Capability Package



## 5 SOLUTION COMPONENTS

In the high-level designs discussed in the previous section, all communications flowing across a Black network are protected by at least two layers of encryption, implemented using IPsec tunnels generated by VPN Gateways or MACsec tunnels generated by MACsec Devices. Mandatory aspects of the solution also include Administration Workstations, CAs for key management using Public Key Infrastructure (PKI), Key Generation Components (KGCs) for generating CAKeys, and Gray Network Firewalls for when networks of different classification levels share the same Outer Encryption Component.

Each Solution component is described in more detail below. The descriptions include information about the security provided by the components as evidence for why they are deemed necessary for the solution. Components are selected from the CSfC Components Lists in accordance with the Product Selection requirements of this CP (see Section 10).

Additional components, discussed in Section 5.6, can be added to the solution to help reduce the overall risk. However, these are not considered mandatory components for the security of the solution; therefore, this CP does not place configuration or security requirements on the components.

### 5.1 OUTER ENCRYPTION COMPONENTS

The Outer Encryption Component is located at the edge of the private network and can be either a VPN Gateway or a MACsec Device. The Outer Encryption Component establishes an encrypted tunnel using IPsec or MACsec with peer Outer Encryption Components, which provides device authentication, confidentiality, and integrity of information traversing Black networks.

Although the Outer Encryption Component is a perimeter device and thus more exposed to external attacks, the Outer Encryption Component is also capable of protecting the network from unauthenticated traffic through use of an internal filtering capability. This allows specification of rules that prohibit unauthorized data flows, which helps mitigate Denial of Service (DoS) attacks and resource exhaustion. This CP does not require that the Outer Encryption Component terminate all tunnels on a single physical interface; however, all such external interfaces shall conform to the port filtering requirements in Section 11.6. The Outer Encryption Component is implemented identically for all the high-level designs covered in this CP.

Outer Encryption Components are also responsible for filtering traffic on its Gray network interfaces to prevent Inner Encryption Components for networks of different classification levels from being able to send packets to one another. Since this filtering is primarily based on the source and destination addresses in the packet on a Gray network, the Gray networks themselves must use an addressing scheme that supports the necessary filtering (such as using separate address ranges for the Gray interfaces of Inner Encryption Components supporting each Red network). This filtering on Gray network traffic is performed even for solutions that only support Red networks of a single classification level, as in that situation the actual filtering needed to comply with this CP would be simple.



# Multi-Site Connectivity Capability Package



In addition to performing the functions described in this CP, an Outer Encryption Component may also use AO-approved routing protocols on the Gray network it is connected to. The Outer Encryption Component cannot route packets between Gray and Black networks; any packets received on a Gray network interface and sent out a Black network interface must be transmitted within an IPsec or MACsec tunnel configured according to this CP. There is some data that will originate from the Outer Encryption Component (such as control traffic (e.g., Bidirectional Forwarding Detection (BFD)), logging and audit data, which will potentially be sent to a Gray Management network at another site) that will only go through the outer encryption tunnel. This is the only exception to having two layers of encryption for data going over a Black network and is considered acceptable given the limited intelligence value of that information and the fact that it does not contain classified data. However, management traffic on a Gray network, which originates from the Administration Workstation, must include two layers of encryption as described in this CP (see Section 11.8).

For load balance or other performance reasons, multiple Outer Encryption Components that comply with the requirements of this CP are acceptable.

## 5.2 GRAY NETWORK FIREWALLS

A MSC Solution that supports multiple Red networks may include one or more Gray Network Firewalls, as described in Section 4.3.2.2. The primary purpose of a Gray Network Firewall is to block any packets sent between Inner Encryption Components for Red networks of different classification levels. A Gray Network Firewall also blocks any packets sent between management components on the Gray network and Inner Encryption Components for Red networks that operate at a classification level other than the highest classification level of data protected by the solution. Gray Network Firewalls are physically protected as classified devices.

A standalone Gray Network Firewall, selected from the CSFC Components List, would typically only be used in solutions where the physical design of the Gray network includes paths between Inner Encryption Components for Red networks of different classification levels that do not pass through the Outer Encryption Components. Effectively, each Gray Network Firewall is another instance of the Gray network filtering performed by the Outer Encryption Component. For load balance or other performance reasons, multiple Gray Network Firewalls that comply with the requirements of this CP are acceptable.

## 5.3 GRAY MANAGEMENT SERVICES

Secure administration of components in the Gray network and continuous monitoring of the Gray network are essential roles provided by the Gray Management Services. Gray Management Services are composed of a number of components which each can play a distinct role in the overall security of the solution. This CP allows flexibility in the placement of some Gray Management Services as described below. The Gray Management Services are physically protected as classified devices.



# Multi-Site Connectivity Capability Package



## 5.3.1 GRAY ADMINISTRATION WORKSTATION

The Gray Administration Workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Outer Encryption Component, Gray Network Firewall, and all Gray Management Service components. The Gray Administration Workstations are not permitted to maintain, monitor, or control Inner Encryption Components or Red Management Services. All MSC Solutions will have at least one Gray Administration Workstation.

Administration Workstations shall be dedicated for the purposes given in this CP, and shall not be used to manage any non-CSfC solutions. As such, a dedicated virtual machine on an administration device used for a non-CSfC solution cannot be used to manage CSfC solutions.

For MSC Solutions with multiple Red networks with different security levels using a single Outer Encryption Component, a separate Administration Workstation is needed to manage the Gray Management Services of each security level.

## 5.3.2 OUTER CERTIFICATE AUTHORITY (LOCATED ON GRAY NETWORK)

An Outer CA located on the Gray network issues digital certificates for the Outer VPN Gateways in the solution. These certificates are used for authentication in establishing an Outer IPsec tunnel between pairs of VPN Gateways.

If an Outer CA is located in the Gray network and the Inner tunnel is also provided by VPN Gateways, this CP requires a physically separate Inner CA located in the Enterprise/Red network. The Inner CA issues certificates to Inner VPN Gateways. This separation provides key management separation between the two independent layers of encryption.

To improve integration with existing Enterprise Public Key Infrastructure (PKI), this CP allows for flexibility in the placement of CAs. As an alternative to implementing the Outer CA as a Gray Management Service, customers can choose to implement the Outer CA on the Enterprise/Red network (see Section 7.1.1). When the Outer CA is located in the Enterprise/Red network it is not managed by the Gray Management Services.

## 5.3.3 GRAY CERTIFICATE REVOCATION SERVICES

Certificate Revocation List (CRL) Distribution Points (CDP) and Online Certificate Status Protocol (OCSP) Responders are servers other than a CA that make revocation information available to components. Outer CDPs and OCSP Responders are deployed on the external side of the Outer VPN Gateway for which revocation information is being made available. Collectively Outer CDPs and OCSP Responders are referred to as Gray Certificate Revocation Services. The Gray Certificate Revocation Services ensure the Outer VPN Gateway can verify the status of the certificates used by the Outer VPN Gateway to which it is attempting to establish a connection.



# Multi-Site Connectivity Capability Package



CDPs and OCSP Responders are not required components of this CP, but if not used the organization must implement other means, such as whitelists, to ensure that once a certificate is revoked it cannot successfully establish an Outer IPsec tunnel with the solution infrastructure.

The use of CDPs and OCSP Responders in MSC Solutions is discussed in detail in Section 7.1.2.

## 5.3.4 OUTER KEY GENERATION COMPONENT

A locally-operated Outer KGC generates CAKeys only for Outer MACsec Devices. An Outer KGC is not a mandatory component of the MSC Solution. CAKeys for Outer MACsec Devices can be generated on an Inner KGC.

The use of KGCs in MSC Solutions is discussed in detail in Section 7.2.

## 5.3.5 GRAY SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The Gray SIEM collects and analyzes log data from the Outer Encryption Component, Gray Network Firewall, and other Gray Management Service components. Log data may be encrypted between the originating component and the Gray SIEM with SSHv2, TLS, IPsec, or MACsec to maintain confidentiality and integrity of the log data. At a minimum, an auditor reviews the Gray SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the Outer Encryption Component or Gray Network Firewall receives and drops any unexpected traffic which could indicate a compromise. These functions can also be performed on an Enterprise/Red SIEM if AO-approved one-way taps are used as described in this CP (see Section 6.2).

A Gray SIEM is not a mandatory component of the MSC Solution.

## 5.4 INNER ENCRYPTION COMPONENTS

Inner Encryption Components can be either VPN Gateways or MACsec Devices. For load balance or other performance reasons, multiple Inner Encryption Components that comply with the requirements of this CP are acceptable.

Similar to an Outer Encryption Component, an Inner Encryption Component provides authentication of peer VPN Gateways or MACsec Devices, cryptographic protection of data in transit, and configuration and enforcement of network packet handling rules.

In addition to performing the functions described in this CP, an Inner Encryption Component may also use AO-approved routing protocols on the Red network it is connected to. An Inner Encryption Component shall not route packets between Red and Gray networks; any packets received on a Red network interface and sent to a Gray network interface must be transmitted within an IPsec or MACsec tunnel configured according to this CP.

When an Inner MACsec Device is used, the MACsec traffic will need to be encapsulated prior to being processed by the Outer Encryption Component, regardless of whether it's a VPN Gateway or a MACsec



# Multi-Site Connectivity Capability Package



Device. Some VPN Gateways and MACsec Devices allow this encapsulation to occur on the incoming interface, prior to encrypting traffic for the Outer tunnel. If the selected VPN Gateway or MACsec Device does not have this feature, a separate standalone router or switch is necessary to provide encapsulation and all requirements for Solution Components in this CP shall apply to it. Any AO-approved encapsulation protocol may be used.

## 5.5 RED MANAGEMENT SERVICES

Secure Administration of Inner Encryption Components is provided by the Red Management Services. Red Management Services are composed of a number of components which can each play a distinct role in the overall security of the solution. This CP allows flexibility in the placement of some Red Management Services as described below.

### 5.5.1 RED ADMINISTRATION WORKSTATION

The Red Administration Workstation is responsible for maintaining, monitoring, and controlling all security functionality for the Inner Encryption Components and all Red Management Service components. Red Administration Workstations are not permitted to maintain, monitor, or control Outer Encryption Components or Gray Management Services. All MSC Solutions will have at least one Red Administration Workstation.

Administration Workstations shall be dedicated for the purposes given in this CP, and shall not be used to manage any non-CSfC solutions. As such, a dedicated virtual machine on an administration device used for a non-CSfC solution cannot be used to manage CSfC solutions.

### 5.5.2 INNER CERTIFICATE AUTHORITY (LOCATED ON RED NETWORK)

MSC Solutions will always have at least one CA located in the Red network. At a minimum an Inner CA is included in the Red network to issue digital certificates for the Inner VPN Gateways in the solution. These certificates are used for authentication in establishing the inner IPsec tunnel between pairs of Inner VPN Gateways.

This CP also allows Outer CAs to be included in the Red network to issue digital certificates for the Outer VPN Gateways. These certificates are used for device authentication in establishing the outer IPsec tunnel between pairs of VPN Gateways. When an Outer CA is placed in the Red network it is critical to have AO-approved mechanisms in place to transfer revocation information to the Black network to ensure it is accessible to peer Outer VPN Gateways. When an Enterprise PKI capability is used, it is managed with existing processes and capabilities. Enterprise CAs provide certificate management services for the MSC Solution over the Enterprise/Red network.

If the solution is supporting Red networks of different security levels, then a separate CA is needed for the Inner VPN Gateways of each security level.



# Multi-Site Connectivity Capability Package



Each CA used in the solution shall have an approved Certificate Policy/ Certificate Practice Statement (CP/CPS) that addresses certificate generation, handling, distribution, storage, destruction, and key recovery and compromise recovery. Refer to NIST SP 800-57 for guidance.

If the organization has existing enterprise CAs that satisfy the requirements of this CP, those CAs should be used as part of the MSC Solution rather than setting up new CAs dedicated to this solution. Otherwise a locally managed CA will need to be deployed requiring that a CA product be selected from the CSfC Components List.

## 5.5.3 RED CERTIFICATE REVOCATION SERVICES

CDPs and OCSP Responders are servers other than a CA that make revocation information available to components. Red CDPs and OCSP Responders make revocation information available to Inner VPN Gateways. Collectively Red CDPs and OCSP Responders are referred to as Red Certificate Revocation Services. The Red Certificate Revocation Services ensure the Inner VPN Gateway can verify the status of the certificates used by the Inner VPN Gateway to which it is connecting.

CDPs and OCSP Responders are not required components of this CP, but if not used the organization must implement other means, such as whitelists, to ensure that, once a certificate is revoked, it cannot successfully establish an Inner Tunnel with a VPN Gateway.

The use of CDPs and OCSP Responders in MSC Solutions is discussed in detail in Section 7.1.2.

## 5.5.4 INNER KEY GENERATION COMPONENT (LOCATED ON RED NETWORK)

MSC Solutions will always have at least one KGC located in the Red network. At a minimum an Inner KGC is included in the Red network to issue CAKs for the Inner MACsec Devices in the solution. These CAKs are used for authentication in establishing the MACsec tunnel between a pair of Inner MACsec Devices.

This CP also allows the Inner KGC to issue CAKs for the Outer MACsec Devices. These CAKs are used for device authentication in establishing the MACsec tunnel between a pair of MACsec Devices. When the Inner KGC issues CAKs for Outer MACsec Devices, it is critical to have AO-approved mechanisms in place to transfer the CAKs to the Outer MACsec Devices.

The use of KGCs in MSC Solutions is discussed in detail in Section 7.2.

## 5.5.5 RED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Red SIEMs collect and analyze log data from the Inner Encryption Components and other Red Management Service components. Log data may be encrypted between the originating component and the Red SIEM with SSHv2, TLS, IPsec, or MACsec to ensure confidentiality and integrity. At a minimum an auditor reviews the Red SIEM on a weekly basis. The SIEM is configured to provide alerts for specific events including if the Inner Encryption Components receive and drop any unexpected traffic which could indicate a compromise.



# Multi-Site Connectivity Capability Package



While Red SIEMs are not a mandatory component of the MSC Solution, customers are encouraged to leverage existing Enterprise SIEM capabilities to monitor log data from Inner Encryption Components and Red Management Services. Although a Red SIEM is not required, it is still required to analyze logs from all Inner Encryption Components on at least a weekly basis. A Red SIEM may also be used to analyze log data from Gray network components when used in conjunction with one-way taps as described in this CP (see Section 6.2).

## 5.6 OTHER CONTROLS

There are additional controls that could be used within this solution to potentially reduce the overall risk. A screening router can be used to filter packets from Black networks before they arrive at Outer Encryption Components and Outer CDPs or OCSP Responders. The screening router could be part of an existing Black network (e.g., Customer Edge Router), or could be added between Outer Encryption Components and existing Black network components. However, since the screening router would become part of a Black network, it is not considered to be part of the MSC Solution itself.

Additionally, if an integrator is used for implementation of this solution, the customer can require separation of roles between individuals working on Red and Gray components. The separation of roles ensures that during the development of the solution no single individual can compromise Red and Gray components simultaneously.

## 6 CONTINUOUS MONITORING

Continuous monitoring allows customers to detect, react to, and report any attacks which occur on their solution. This continuous monitoring also enables the detection of any configuration errors to Solution Components.

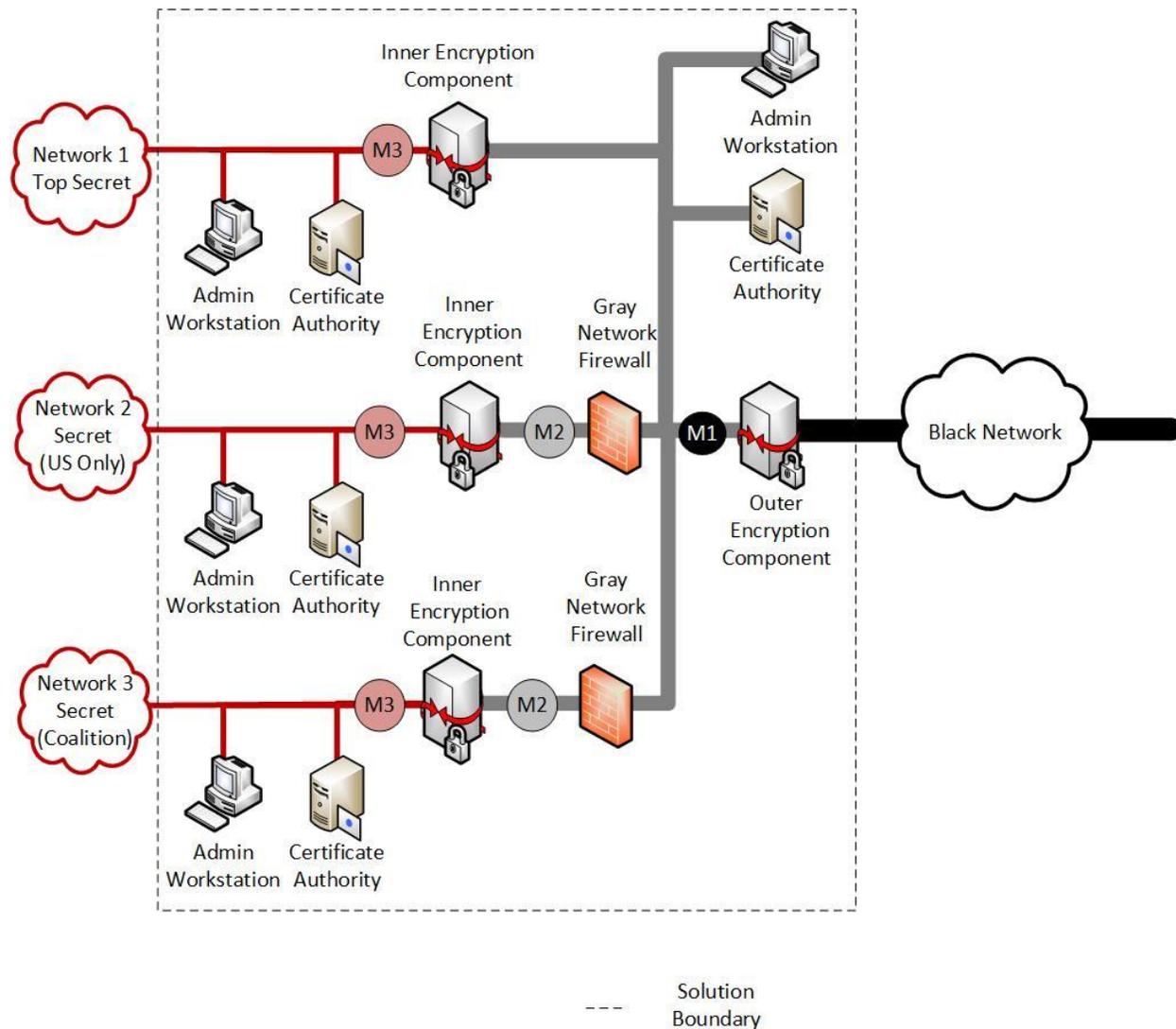
At a minimum, this CP requires an Auditor to review alerts, events, and logs on a weekly basis. This minimum review period allows customers in Tactical Environments to implement solutions where it may not be feasible to perform real-time monitoring. Operational and Strategic implementations of the MSC Solution should review alerts, events, and logs on a much more frequent period and in many cases may leverage Operations Centers to perform 24/7 monitoring of the solution.

### 6.1 MONITORING NETWORK TRAFFIC

This CP recommends monitoring network traffic in at least one of three areas within the solution infrastructure. Network traffic can be monitored using an Intrusion Detection System (IDS); however, it is preferable to use an Intrusion Prevention System (IPS) to enable real-time responses. While monitoring only one of the three locations is recommended, customers monitoring all three points have the best visibility enabling detection of malicious activity or misconfiguration of components.



# Multi-Site Connectivity Capability Package



**Figure 10. MSC Solution Continuous Monitoring**

Figure 10 depicts three locations that customers can select to implement network monitoring capabilities. There are several alternatives for deploying the IDS at one or all of the Monitoring Points (M1, M2, and/or M3). IDSs can ingest traffic from network taps, Switched Port Analyzers (SPANs), or in line with the solution. Similarly, an IPS can be placed either inline or in promiscuous mode. When operating in promiscuous mode, the IPS analyzes traffic at M1, M2, or M3 and issues commands to firewalls (standalone or integrated) to block traffic flows. The following paragraphs define each of the three Monitoring Points. These descriptions detail the analysis and alerts which would be generated by the IDS. If a customer decides to implement an IPS, then it should be configured to block that traffic flow and also send an alert.



# Multi-Site Connectivity Capability Package



**Monitoring Point 1 (M1)** is located on the internal side of the Outer Encryption Component. At a minimum, a M1 IDS is configured to send alert upon detection of any traffic which should have been blocked by the Outer Encryption Component. These alerts indicate a failure of the filtering or encryption functions of the Outer Encryption Component and are either indicative of an improper configuration or a potential compromise. Normal traffic at M1 includes IPsec, MACsec, control plane traffic, and management traffic. It is important that customers understand what ports and protocols are used by each of the Inner Encryption Components to ensure that filters are properly configured and IDSs are well tuned. Nearly all traffic traversing M1 is encrypted either with IPsec, MACsec, or SSHv2, which prevents the ability to perform deep packet inspection. Management of a M1 IDS occurs from a Gray network.

**Monitoring Point 2 (M2)** is located between the Gray Network Firewall and the Inner Encryption Component when networks of different classification levels share the Outer Encryption Component. At a minimum, a M2 IDS is configured to send an alert upon detection of any traffic which should have been blocked by the Gray Network Firewall, especially traffic from the network with the higher classification. These alerts indicate a failure of the filtering functions by the Gray Network Firewall and are either indicative of an improper configuration or a potential compromise. Normal traffic at M2 includes IPsec, control plane traffic, and management traffic. It is important that customers understand what ports and protocols are used by each of the Inner Encryption Components to ensure that firewall filters are properly configured and IDSs are well tuned. Nearly all traffic traversing M2 is encrypted either with IPsec, MACsec or SSHv2, which prevents the ability to perform deep packet inspection. Management of a M2 IDS occurs from the Gray Management Services.

**Monitoring Point 3 (M3)** is located between the Inner Encryption Component and the Enterprise/Red network. At a minimum, a M3 IDS is configured to send an alert upon detection of any traffic which should have been blocked by the Inner Encryption Component. These alerts indicate a failure of the filtering function of the Inner Encryption Component. Of the three monitoring points, M3 is the most difficult to define a normal baseline, but in many implementations, monitoring at M3 allows for deep packet inspection since traffic is not encrypted. Management of the M3 IDS occurs from the Red Management Services.

**Monitoring Multiple Points:** Although this CP only requires monitoring of one out of the three points, customers are encouraged to monitor all three locations. To ensure that no bypass of the Outer or Inner Encryption Components occurs, customers can implement three IDS(s)/IPS(s). Implementation of three separate components to monitor each point ensures that malicious traffic cannot inadvertently be transferred to the Enterprise/Red network, but it also increases cost and complexity for managing the solution. This approach also prevents correlation of data as it traverses throughout the solution.

Alternatively, to allow correlation of data at multiple points this CP allows a one-way tap located at M1 or M2 to feed the IDS located in an enclave of the Red Network that is isolated from the Enterprise/Red network. The one-way tap used must physically only allow data flow from M1 or M2 to the Enterprise/Red network. Additionally, the selected one-way tap must be approved by the AO.



# Multi-Site Connectivity Capability Package



Movement of network traffic from M3 to the Gray network is explicitly prohibited. Prior to implementing one-way taps as part of the MSC Solution, AOs need to be aware of the Residual Risks associated with transferring data from Gray networks to a Red network of a higher classification.

## 6.2 MONITORING LOG DATA

SIEMs are not a mandatory components of the MSC Solution. However, customers are still required to analyze logs from all Solution Components on at least a weekly basis.

SIEMs collect, aggregate, correlate, and analyze log data from Solution Components and provide alerts to Auditors when anomalous behavior is detected.

To protect the integrity of the data, all logs sent to the SIEM should be encrypted with SSHv2, TLS, IPsec or MACsec. At a minimum the SIEM is configured to send alerts upon receiving a log entry for blocked packets from an Encryption Component or Gray Network Firewall.

To allow correlation of data from both Gray and Red components, this CP allows a one-way tap located in the Gray network to feed Gray Log Data to a Red SIEM located in an enclave of the Red network that is isolated from the Enterprise/Red network. The one-way tap used must physically only allow log data to flow from Gray Components to the Enterprise/Red network. Additionally, the selected one-way tap must be approved by the AO.

## 7 KEY MANAGEMENT

One of the most difficult parts of any solution is determining how the key management will be implemented in a secure manner. In the MSC Solution, certificates are used for VPN Gateways and CAKeys are used for MACsec Devices.

### 7.1 CERTIFICATES

This section provides details on issuing, renewing, rekeying and revoking certificates for VPN Gateways.

#### 7.1.1 CERTIFICATE ISSUANCE, RENEWAL AND REKEY

In this solution, the only certificates necessary are for the device authentication certificates on VPN Gateways at the end of each IPsec tunnel. The certificates and private keys used in the solution are considered Controlled Unclassified Information (CUI), because they are only used for mutual device authentication, not for traffic encryption.

If IPsec is securing both tunnels, no single CA can provide keys to both Inner and Outer VPN Gateways. The CAs for Outer VPN Gateways are located on a Gray Management network, connected to an Outer VPN Gateway. A locally-run CA may need to be stood up to key Outer VPN Gateways, requiring that a CA product be selected from the NSA-approved CSfC Component List for Outer tunnel PKI. In addition, a Certificate Policy/Certification Practice Statement (CPS) document must be created or tailored for each CA used in the solution. It is then the AO's responsibility to approve the use of a CA. If an Outer tunnel



# Multi-Site Connectivity Capability Package



CA is an Enterprise CA already running on the necessary Gray Management network, no additional approval is necessary for use of the CA.

CAs for Inner VPN Gateways are located on Red networks, which may allow for use of existing Enterprise CAs already operational on the Red network. For networks in which an existing Enterprise CA is not available, the use of a locally-run CA on the Red network is an acceptable alternative. If an Inner tunnel CA is an Enterprise CA already running on a Red network, no additional approval is necessary for use of this CA. For example, a solution may use an Enterprise CA (such as a CNSS-approved CA, which follows CNSS Instruction (CNSSI) 1300 under the National Security Systems (NSS) PKI Root CA, to issue certificates to an Inner VPN Gateway. If, however, an Inner tunnel CA uses a locally-run CA on a Red network, the approval process given in the preceding paragraph for an Outer tunnel CA applies and must be followed.

Each VPN Gateway has at least one CA signing certificate (sometimes referred to as a Trust Anchor), which is used by the VPN Gateway to authenticate to other VPN Gateways in the solution. If centralized management is used throughout the solution, there will be only one CA signing certificate in each VPN Gateway. Otherwise, one CA signing certificate is installed in each Inner VPN Gateway for each Inner Tunnel CA used in the system. Similarly, one CA signing certificate will be installed in each Outer VPN Gateway for each Outer Tunnel CA used in the system.

Each VPN Gateway will contain a private key that corresponds to a certificate issued by its CA, and one or more CA signing certificates as described above. Each VPN Gateway will also contain revocation information. The private key may be locally generated and must be adequately protected. Both Inner and Outer tunnel PKIs shall use Elliptic Curve Digital Signature Algorithm (ECDSA) over the curve P-384 with SHA-384 or RSA 3072 bit or greater signatures within X.509 certificates. The algorithms and elliptic curves that are approved for use in the VPN Gateways are found in Table 5 (see Section 11.2).

The MSC Solution described here requires certificates to establish the secure tunnels between VPN Gateways. Without certificates, the network cannot function. Thus, an out-of-band method must be used to issue the initial certificates to the VPN Gateways. Subsequent rekeying, however, should take place over the network through this solution prior to the current key's expiration. The key validity period for certificates issued by locally-run CAs cannot exceed 14 months, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to VPN Gateways within 24 hours of CRL issuance.

## 7.1.2 EXTERNAL DISTRIBUTION OF CERTIFICATE REVOCATION LISTS

Part of the security of the MSC solution depends on the certificate-based mutual authentication that occurs between two VPN Gateways establishing an IPsec tunnel. One step of this mutual authentication entails checking whether the certificate used by the other VPN Gateway has been revoked, which requires each VPN Gateway to have access to a current CRL. As the number of sites interconnected through the MSC Solution increases, out-of-band CRL distribution becomes increasingly burdensome

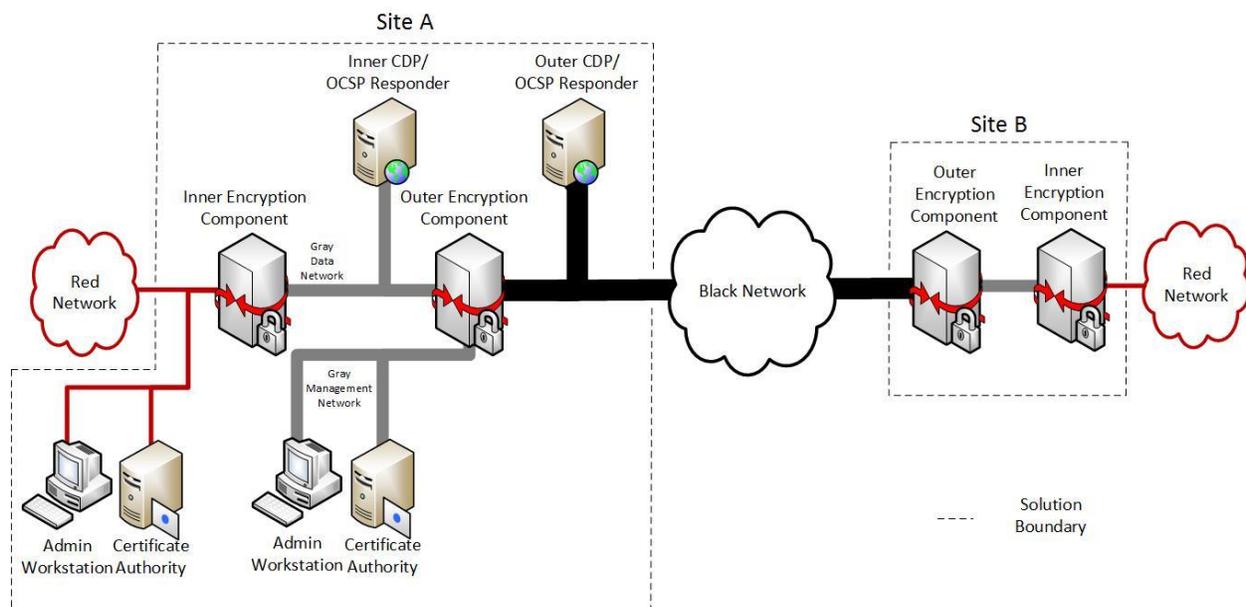


# Multi-Site Connectivity Capability Package



and error-prone. Although VPN Gateways may retrieve the latest CRL directly from the appropriate CA, for Remote Sites this requires first establishing an IPsec tunnel to the Central Management Site where the CAs are located. These additional IPsec tunnels increase the time needed to establish an IPsec tunnel between two Remote Sites. Furthermore, the Remote Site's VPN Gateways still require out-of-band CRL distribution to be able to check for revocation of the certificates used by VPN Gateways at the Central Management Site, since the IPsec tunnel to the Central Management Site must be established before the CRLs can be obtained from the CAs.

To avoid these issues, this CP permits the distribution of CRLs on the external side of the VPN Gateways, which allows the VPN Gateways to retrieve the current CRL without first establishing an IPsec tunnel. A CDP or OCSP Responder resides on a different network than the CA that produced the CRL it hosts. An Outer CDP or OCSP Responder resides on a Black network and hosts a CRL created by the CA on a Gray network. Similarly, an Inner CDP or OCSP Responder resides on a Gray network and hosts a CRL created by the CA on a Red network. Because the CDP or OCSP Responder and its CA reside on different networks, a one-way transfer mechanism is needed to periodically distribute the current CRL from the CA to the CDP or OCSP Responder; the details of the one-way transfer mechanism are left to a solution's AO.



**Figure 11. MSC Solution using CRL Distribution Points and OCSP Responders**

Figure 11 illustrates the placement of CDPs and OCSP Responders to make CRLs accessible to Remote Sites on the Black network before IPsec tunnel establishment. During negotiation of the outer encryption tunnel, the Outer VPN Gateways contact the Outer CDP or OCSP Responder on the Black network to download the latest CRL produced by the Outer CA. Similarly, during negotiation of the inner



# Multi-Site Connectivity Capability Package



encryption tunnel, the Inner VPN Gateways contact the Inner CDP or OCSP Responder on the Gray network to download the latest CRL produced by the Red CA.

The use of CDPs and OCSP Responders on the external side of the VPN Gateways requires that the contents of the CRLs hosted on them are unclassified, since the CDPs and OCSP Responders are located on networks that the design of the MSC Solution treats as unclassified. If a solution owner's classification authority decides that its CRLs are classified, then its MSC Solutions would be unable to make use of external CDPs and OCSP Responders.

For solutions that support networks of different security levels (see Section 4.3.2.2), a single Inner CDP or OCSP Responder may be used to host the CRLs for the Inner VPN Gateways of multiple Red networks.

A solution owner may choose to implement zero, one, or multiple CDPs or OCSP Responders on Black and Gray networks, based on their expected utility in facilitating CRL distribution to Remote Sites. Having multiple redundant CDPs or OCSP Responders on the same network improves the availability of CRL distribution, since a VPN Gateway only needs to be able to contact one CDP or OCSP Responder to obtain the CRL. Conversely, in a small-scale solution, manual out-of-band distribution of CRLs may be more cost-effective than deploying and maintaining CDPs or OCSP Responders.

## 7.2 CONNECTIVITY ASSOCIATION KEYS

This section provides details on issuing, renewing, rekeying and revoking CAKs, the PSKs used by MACsec Devices for authentication. CAK management is a critical function. If a CAK is compromised, all MACsec Devices using that CAK need to be updated with a new CAK. This is different from a certificate-based solution in that revocation of any given certificate only impacts the device associated with that certificate. CAK management can be provided by Enterprise services (e.g., Key Management Infrastructure (KMI)) or via locally-operated services.

Enterprise CAK management services are those services that can be provided on a Department-wide or Agency-wide scale, and include services such as CAK generation; CAK distribution; CAK accounting and CAK compromise reporting. A department-wide program that can provide these types of services is the NSA KMI. The KMI also allows agencies to locally manage CAKs using a specialized Management Client (MGC).

Currently, the MGC does not have a commercial standard interface. However, customers can acquire or develop a custom application that can receive key from KMI and reformat it for secure distribution to and installation on MACsec Devices.

If an Enterprise CAK is not feasible, customers can deploy their own locally-operated, NSA-approved KGC to generate and manage CAKs for MACsec Devices.



# Multi-Site Connectivity Capability Package



The customer is responsible for developing a Key Management Plan (KMP) for the CAKs used in the MSC Solution. The KMP must be approved by the National Cryptographic Solutions Management Office (NCSMO). The KMP addresses the following with regard to the CAKs:

- CAK technical specifications, including the format for the CAK to be installed onto the MACsec Devices;
- Operational environment for the MSC Solution;
- MSC Solution Components that use and manage CAKs, including planned volumes;
- Processes for CAK ordering, generation, distribution and storage, including physical and technical controls;
- Accounting processes and controls for CAKs;
- Compromise management and recover (how service is restored in the event of CAK compromise);
- CAK archival and recovery, if necessary (how CAKs are recovered in case of loss);
- Interoperability requirements with other systems and solutions; and
- Roles and responsibilities for managing CAKs.

In addition to a KMP, customers may need to obtain an IAD MD-110 waiver since commercial equipment typically allow CAKs to exist in red form during part of the CAK life-cycle management process.

Customers are strongly encouraged to contact their Client Advocate early in the process to obtain the NCSMO's assistance in developing the KMP, selecting a NSA-approved KGC, or obtaining an IAD MD-110 waiver.

## **7.2.1 CONNECTIVITY ASSOCIATION KEY ISSUANCE, RENEWAL AND REKEY**

Each MACsec Device has at least one CAK, which is used by the MACsec Device to authenticate with another MACsec Device. A different CAK is required for every pair of MACsec Devices establishing an encryption tunnel. Also, if both layers of the solution use MACsec, different CAKs are required for the inner and outer encryption tunnels.

CAKs must be securely distributed to the MACsec Devices. Secure distribution can be achieved via technical means (e.g., encryption) or procedural controls. A pre-placed PSK Encryption Key (PEK) can be used to encrypt CAKs. A separate PEK should be used for each site.

CAK Administrators (CAKA) install the CAKs into the MACsec Devices. CAKAs account for CAKs to ensure their location and use is known at all times. In the case of compromise, CAKAs need to be able to



# Multi-Site Connectivity Capability Package



determine where all instances of a given CAK exist and update that CAK in accordance with compromise reporting and recovery procedures.

CAKs require periodic updating to limit the amount of operational exposure for the CAKs. CAKs must be updated at least every 30 days. Likewise, PEKs must be updated at least every 90 days.

## 7.2.2 CONNECTIVITY ASSOCIATION KEY COMPROMISE RECOVERY

CAK compromise recovery is a critical function within the MSC Solution. Therefore, good accounting records are necessary to know which CAKs are installed on which MACsec devices. When a CAK is compromised, the CAK must be updated immediately at both sites. CAK compromise recovery procedures are documented in the KMP.

## 8 THREATS

This section details how the required components work together to provide overall security in the solution. Figure 2 through Figure 9 show the boundary of the MSC Solution for each high-level design covered by this CP.

An assessment of security was conducted on each of the high-level designs described in this CP while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of transporting data over secure or unsecure networks. By examining these threats, the organization can have a better understanding of the risks they are accepting by implementing the solution and how these risks affect the Confidentiality, Integrity, and Availability of the network, systems, and data. To obtain the classified risk assessment associated with this CP, please contact the NSA via your Client Advocate.

### 8.1 PASSIVE THREATS

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

The security against a passive attack targeting the data in transit across the Black network is provided by the layered encryption tunnels using IPsec or MACsec. To mitigate passive attacks, two layers of CNSA Suite encryption, Advanced Encryption Standard (AES), are employed to provide confidentiality for the solution. Use of AES is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The Inner and Outer Encryption Components that are used to set up the two tunnels must be independent in a number of ways (see Section 10). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both tunnels.



# Multi-Site Connectivity Capability Package



The use of one or more Outer CDPs or OCSP Responders to distribute unencrypted CRLs on a Black network potentially allows a passive threat actor with access to the Black network path between an Outer CDP/OCSP Responder and Outer VPN Gateway to obtain a copy of the CRL issued by an Outer CA. However, the content of the CRL is primarily limited to a list of serial numbers of revoked certificates, the date and time when each certificate was revoked, and a high-level reason why each certificate was revoked (such as key compromise or cessation of operation). The CRL does not specify what certificates are still valid, nor does it identify the physical or network locations of any components in the solution. The CRL also does not reveal any information about certificates issued by anything other than the Outer CA. If a solution owner's AO considers the limited information in a CRL too sensitive to distribute on the Black network, the solution owner can choose not to implement Outer CDPs/OCSP Responders and rely on other means to distribute CRLs to Outer VPN Gateways in a timely fashion.

## 8.2 EXTERNAL (ACTIVE) THREATS

This threat refers to outsiders gaining unauthorized access to a system or network, exfiltration of sensitive Red network data, or degradation of availability of the system or network. Threat actions include introducing viruses, malware, or worms with the intention to compromise the network or exfiltrate data, or to analyze the design of the network or system for future attacks. Adversaries could gain access to an Encryption Component, and then exploit or compromise other devices on the network. DoS or Distributed DoS (DDoS) attacks compromise availability of the system, degrading/disrupting secure communication across a Black network. Further external threat actions would include social engineering attacks to assist attackers with gaining additional access to a network for the purpose of compromising a system or network, traffic injection or modification attacks, or replay attacks.

### 8.2.1 ROGUE TRAFFIC

One method for detecting rogue traffic from an external attack as it attempts to pass through one or both Encryption Components is by having the port filtering native to each Encryption Component enabled and configured to audit and log any traffic that is not of the format described in the configuration. This will allow the Auditors and/or the Security Administrators to detect whether the Outer Encryption Component has been breached, thus providing an early warning of a potential intrusion. It will also provide detection of misconfigured Outer Encryption Components.

Another method for detecting a potential intrusion into the solution is requiring automated configuration change detection on Red and Gray Management networks to ensure Encryption Component configurations are not changed without the knowledge of Auditors and Security Administrators. Auditors also ensure through the audit logs that all configuration changes are valid. This will counter attacks that take advantage of Encryption Component misconfigurations.



# Multi-Site Connectivity Capability Package



CDPs and OCSP Responders are protected from rogue traffic by implementing port filtering on the server. Rogue traffic to CDPs and OCSP Responders can be further mitigated by implementing a firewall or other packet filtering device between the CDP/OCSP Responder and the rest of the network.

## 8.2.2 MALWARE AND UNTRUSTED UPDATES

Administration Workstations and CAs for Inner Encryption Components shall be distinct from the Administration Workstations and CAs for a Gray network. This separation minimizes the potential for malware on a single device to impact components supporting both Inner and Outer Encryption tunnels.

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

## 8.2.3 DENIAL OF SERVICE

DoS attack risks cannot be completely mitigated. MSC Solutions in compliance with this CP are required to drop all packets that are not Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), MACsec Key Agreement (MKA), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) or other approved protocols on the appropriate interfaces, which significantly reduces the potential of flooding attacks. For customers requiring more protection against these attacks, one option is the use of a perimeter router between the Outer Encrypting Component and Black networks to filter traffic before it reaches the Outer Encryption Component. Another option for customers requiring more protection is to add additional filtering based on specifics like known network IP addresses to filter traffic from devices not included in this solution or leasing private lines for the Black network. Other mitigations are acceptable and up to the AO to approve their use.

A single Encryption Component failure is likely to result in a DoS condition. One assumption underlying this solution is that high assurance of availability is not required. If availability is critical for the customer, protection against DoS attacks can be achieved through network redundancy and instituting DoS response procedures when loss of availability is detected.

When using Outer CDPs or OCSP Responders to distribute CRLs to Outer VPN Gateways on a Black network, a sustained DoS attack on the CDPs/OCSP Responders could prevent Outer VPN Gateways from receiving updated CRLs. If the CRLs cached at the other VPN Gateways then expire, they would be unable to establish IPsec tunnels due to the inability to check the revocation status of certificates during the mutual authentication process. Deploying multiple Outer CDPs or OCSP Responders reduces the likelihood of a successful DoS attack on this part of the solution, since as long as even one Outer CDP/OCSP Responder is available, Outer VPN Gateways will be able to retrieve CRL updates.



# Multi-Site Connectivity Capability Package



Additionally, a solution using CDPs or OCSP Responders should still have procedures in place for out-of-band CRL distribution to use in the event that all Outer CDPs/OCSP Responders become unavailable.

## 8.2.4 SOCIAL ENGINEERING

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

## 8.3 INSIDER THREATS

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

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

To mitigate insider threats, separation of roles within the solution is required (see Section 130). In addition, logging and auditing of security critical functionality (see Section 11.10) is required. Also, strong authentication of the Security Administrator and Auditor are required for access to ensure accountability of these individuals. Finally, outbound filters on Encryption Components and firewalls are configured to block traffic leaving the internal network that does not go through the encryption tunnels. An IDS is also recommend on, at a minimum, the Black, Gray, or Red network to help identify unusual or suspicious traffic that could result from a failure, misconfiguration, or attack on Inner or Outer Encryption Components.

## 8.4 SUPPLY CHAIN THREATS

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems and networks upon which the ability to perform U.S. Government missions rely. The supply chains for those ICT components are the underpinnings of those systems and networks, and supply chain attacks are attempts to proactively compromise those underpinnings.



# Multi-Site Connectivity Capability Package



Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component; they are only able to provide assurances based on their reliance on established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor, retailer, reseller, or shipper and then attempting to insert or install a modification or a counterfeit piece of hardware into a component that is destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process (see CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

Doctrinal requirements are placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks. To further mitigate Supply Chain Threats implementing organizations should use the following guidance:

- Establish an ICT SCRM program which conforms to applicable policy based on external and organizational requirements and constraints. The ICT SCRM program should be integrated into the organizational business and mission processes.
- Assess all aspects of the performance of potential vendors, not only the product quality, cost, and performance, but also supply chain risk factors of vendor selection. These risk factors include political ties to foreign governments, citizenship of employees, partner affiliations, employee clearance levels, and location of suppliers and sub-suppliers.
- Ensure that each component selected from the CSfC Components List go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended



# Multi-Site Connectivity Capability Package



application of the component (see CNSSD 505 Supply Chain Risk Management and Intelligence Community Directive (ICD) 731 Supply Chain Risk Management).

- Conduct a Criticality Analysis by which mission-critical functions and components are identified and prioritized with respect to improving acquirer practices (see Defense Acquisition Guidebook, Chapter 13).

Supply chain risk management is a critical consideration in acquiring commercial products. Even after selecting components from the CSfC Components List and utilizing a rigorous acquisition process, an AO must perform due diligence when integrating commercial components for mission operations.

## 8.5 INTEGRATOR THREATS

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures.

To mitigate this threat, integrators are required to be cleared to the highest level of data protected by the MSC Solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution. More information on the NSA's list of trusted integrators can be found on the NSA CSfC Website in the "Criteria for CSfC Integrators" section at this link: <https://www.nsa.gov/resources/everyone/csfc>.

## 9 REQUIREMENTS OVERVIEW

The following five sections (Sections 10 through 15) specify requirements for implementations of MSC Solutions compliant with this CP. However, not all requirements in the following sections will apply to each compliant solution.

### 9.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

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

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.



# Multi-Site Connectivity Capability Package



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

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible 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 CP may become Threshold requirements in a future version of this CP. Solution owners are encouraged to implement Objective requirements where possible to facilitate compliance with future versions of this CP.

## 9.2 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier consisting of the prefix “MSC,” a digraph that groups related requirements together (e.g., “KM”), and a sequence number (e.g., 11). Table 2 lists the digraphs used to group together related requirements and identifies the sections in which those requirement groups can be found.

**Table 2. Requirement Digraphs**

Digraph	Description	Section	Table
PS	Product Selection Requirements	Section 10	Table 3
SR	Overall Solution Requirements	Section 11.1	Table 4
VG	VPN Gateway Requirements	Section 11.2	Table 6
MD	MACsec Device Requirements	Section 11.3	Table 8
IR	Additional Requirements for Inner Encryption Components	Section 11.4	Table 9
OR	Additional Requirements for Outer Encryption Components	Section 11.5	Table 10
PF	Port Filtering Requirements for Solution Components	Section 11.6	Table 11
CM	Configuration Change Detection Requirements	Section 11.7	Table 12
DM	Device Management Requirements	Section 11.8	Table 13
MR	Continuous Monitoring Requirements	Section 11.9	Table 14
AU	Auditing Requirements	Section 11.10	Table 15



# Multi-Site Connectivity Capability Package



Digraph	Description	Section	Table
KM	Key Management Requirements	Section 11.11	Table 16 through Table 23
FW	Gray Firewall Requirements	Section 11.12	Table 24
GD	Requirements for the Use and Handling of Solutions	Section 12.1	Table 25
	Role-Based Personnel Requirements	Section 13	Table 27
RP	Incident Reporting Requirements	Section 12.2	Table 26
TR	Testing Requirements	Section 14.1	Table 28

## 10 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. The requirements in Table 3 will increase the level of effort required to compromise this solution.

**Table 3. Product Selection (PS) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PS-1	The products used for any VPN Gateways shall be chosen from the list of IPsec VPN Gateways on the CSfC Components List.	T=O	
MSC-PS-2	The products used for any MACsec Device shall be chosen from the list of MACsec Ethernet Encryptors on the CSfC Components List.	T=O	
MSC-PS-3	The products used for any Firewalls shall be chosen from the list of Stateful Traffic Filtering Firewalls (TFFW) on the CSfC Components List.	T=O	
MSC-PS-4	The products used for any CAs shall either be chosen from the list of CAs on the CSfC Components List or the CAs shall be pre-existing Enterprise CAs (e.g., DoD PKI, IC PKI).	T=O	
MSC-PS-5	Intrusion Prevention Systems (IPS) shall be chosen from the list of IPS on the CSfC Components List.	O	Optional
MSC-PS-6	The Inner Encryption Component and the Outer Encryption Component shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence. Differences between Service Packs (SP) and version numbers for a particular vendor's operating system (OS) do not provide adequate diversity.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PS-7	The cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	Optional
MSC-PS-8	If the solution contains an Inner CA and an Outer CA, the cryptographic libraries shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different libraries from the same manufacturer, where NSA has determined that the libraries meet the CSfC criteria for implementation independence.	O	Optional
MSC-PS-9	Gray Network Firewalls and Inner Encryption Components shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be two different products from the same manufacturer, where NSA has determined that the two products meet the CSfC criteria for implementation independence.	T=O	
MSC-PS-10	The Inner Encryption Component and Outer Encryption Component shall use physically separate components, such that no component is used for more than one function.	T=O	
MSC-PS-11	The Inner Encryption Component and Gray Network Firewall shall use physically separate components, such that no component is used for more than one function.	T=O	
MSC-PS-12	If the solution contains an Inner CA and an Outer CA, the CAs shall either: come from different manufacturers, where neither manufacturer is a subsidiary of the other; or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence; or use an Enterprise PKI approved by the AO.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PS-13	Each component that is selected out of the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process. (See CNSSD 505 SCRM for additional guidance.)	T=O	
MSC-PS-14	Components shall be configured to use the NIAP-certified evaluated configuration.	T=O	

## 11 CONFIGURATION REQUIREMENTS

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

CPs provide architecture and configuration information that allows customers to select COTS products from CSfC Components Lists for their solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data. CSfC Components Lists consist of eligible COTS products identified by model/version numbers that have met appropriate Protection Profile requirements.

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

The products that are approved for use in this solution will be listed on the CSfC Components List on the IAD/CSfC website ([https:// www.nsa.gov/resources/everyone/csfc](https://www.nsa.gov/resources/everyone/csfc)). No single commercial product shall be used to protect classified information. The only approved methods for using COTS products to protect classified information in transit is through an approved CP.

Once the products for the solution are selected, each product shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)



# Multi-Site Connectivity Capability Package



## 11.1 OVERALL SOLUTION REQUIREMENTS

Table 4 provides the overall solutions requirements for this CP.

**Table 4. Overall Solution Requirements (SR)**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-SR-1	Network services provided by control plane protocols (such as DNS and NTP) shall be located on the inside network (i.e., Gray network for Outer Encryption Component and Red network for Inner Encryption Component).	T=O	
MSC-SR-2	Sites that need to communicate shall ensure that each tunnel's Encryption Components selected by each site are interoperable.	T=O	
MSC-SR-3	The time of day on the Inner Encryption Components and Red Management Services shall be synchronized to a time source located in the Enterprise/Red network.	T=O	
MSC-SR-4	The time of day on the Outer Encryption Components, Gray Network firewall, and Gray Management Services shall be synchronized to a time source located in the Gray Management network.	T=O	
MSC-SR-5	Default accounts, passwords, community strings, and other default access control mechanisms for all Solution Components shall be changed or removed.	T=O	
MSC-SR-6	All components shall be properly configured in accordance with local policy and applicable U.S. Government guidance. In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	T=O	
MSC-SR-7	All physical paths within a Gray network between two Inner Encryption Components for Red networks of different classification levels shall include an Outer Encryption Component or a Gray Network Firewall.	T=O	
MSC-SR-8	All physical paths within a Gray network between a CA, an Administration Workstation, or a CDP/OCSP Responder and an Inner Encryption Component for a Red network whose classification level is lower than the highest classification of data protected by the solution shall include an Outer Encryption Component or a Gray Network Firewall.	T=O	
MSC-SR-9	The only approved physical paths leaving the Red network shall be through a MSC Solution in accordance with this CP or via an AO-approved solution for protecting data in transit.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-SR-10	Solution Components shall receive virus signature updates as required by the local agency policy and the AO.	T=O	
MSC-SR-11	When multiple Inner Encryption Components share an Outer Encryption Component, they shall be placed in parallel.	T=O	
MSC-SR-12	Inner Encryption Components shall not perform switching or routing for other Encryption Components	T=O	

## 11.2 VPN GATEWAY REQUIREMENTS

This section addresses requirements for VPN Gateways. Table 5 identifies the algorithms approved for IPsec encryption. Table 6 provides requirements for VPN Gateways.

**Table 5. IPsec Encryption (Approved Algorithms for Classified)**

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature) (Threshold – Unclassified Only)	RSA 2048	FIPS PUB 186-4
Authentication (Digital Signature) (Objective) (Threshold – All Classified NSS)	RSA 3072 or ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-4 FIPS PUB 186-4 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
Key Exchange/ Establishment	ECDH over the curve P-384 (DH Group 20) or RSA 3072 or DH 3072	NIST SP 800-56A IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460 NIST SP 800-56A
Integrity (Hashing)	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460



# Multi-Site Connectivity Capability Package



**Table 6. VPN Gateway (VG) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-1	The proposals offered by VPN Gateways in the course of establishing the IKE Security Association (SA) and the ESP SA for Inner and Outer Tunnels shall be configured to offer algorithm suite(s) containing only CNSA Suite algorithms (see Table 5).	T=O	
MSC-VG-2	Default, self-signed or proprietary device certificates, which are frequently pre-installed by the vendor, for any VPN Gateway shall not be used for establishing SAs.	T	MSC-VG-3
MSC-VG-3	Default, self-signed or proprietary device certificates, which are frequently preinstalled by the vendor, for any VPN Gateways shall be removed.	O	MSC-VG-2
MSC-VG-4	A unique device certificate shall be loaded onto each VPN Gateway along with the corresponding CA (signing) certificate.	T=O	
MSC-VG-5	The private key stored on VPN Gateways shall not be accessible through an interface.	T=O	
MSC-VG-6	A device certificate shall be used for VPN Gateway authentication during IKE.	T=O	
MSC-VG-7	VPN Gateway authentication shall include a check that the certificate is authorized, which can include a Certificate Revocation List (CRL), OCSP Responder, or whitelist.	T=O	
MSC-VG-8	The VPN Gateway authentication shall include a check that the certificate is not expired.	T=O	
MSC-VG-9	Both IPsec tunnels shall use IKEv2 (IETF RFC 5996) key exchange.	T=O	
MSC-VG-10	All VPN Gateways shall use Cipher Block Chaining for IKE encryption.	T=O	
MSC-VG-11	All VPN Gateways shall use Cipher Block Chaining for ESP encryption with an HMAC for integrity.	T	MSC-VG-12
MSC-VG-12	All VPN Gateways shall use Galois Counter Mode for ESP encryption.	O	MSC-VG-11
MSC-VG-13	All VPN Gateways shall set the IKE SA lifetime to at most 24 hours.	T=O	
MSC-VG-14	All VPN Gateways shall set the ESP SA lifetime to at most 8 hours.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-VG-15	Inner VPN Gateways shall only authenticate and establish an IPsec tunnel with one another if their Red networks operate at the same security level (as defined in this CP).	T=O	
MSC-VG-16	All VPN Gateways shall re-authenticate the identity of the VPN Gateway at the other end of the established tunnel before rekeying the IKE SA.	T=O	

## 11.3 MACSEC DEVICE REQUIREMENTS

This section addresses requirements for MACsec Devices. Table 7 identifies the algorithms approved for MACsec encryption. Table 8 provides requirements for MACsec Devices.

**Table 7. MACsec Encryption (Approved Algorithms for Classified)**

Security Service	Algorithm Suite	Specifications
Confidentiality (Encryption)	AES-GCM-256 AES-GCM-XPB-256	FIPS PUB 197 IEEE 802.1AEbw IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Key Wrap	AES-CMAC-256	FIPS PUB 197 NIST SP 800-38F

**Table 8. MACsec Device (MD) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-MD-1	MACsec Devices shall use AES Key Wrap in CMAC mode for key distribution and AES GCM for MACsec; both shall use cryptographic key sizes of 256 bits.	T=O	
MSC-MD-2	MACsec Devices shall authenticate using Pre-Shared Keys (PSKs), known as Connectivity Association Keys (CAKs).	T=O	
MSC-MD-3	CAKs shall be AES 256 bits and generated on a KGC.	T=O	
MSC-MD-4	MACsec Devices shall have the length of the Connectivity Association Key Name (CKN) set to a minimum of 8 bytes (64 bits).	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-MD-5	For each pair of MACsec Devices establishing an encryption tunnel, one of the two shall be configured to be the Key Server by setting this value to 0 (zero). The other MACsec Device shall have its Key Server value set to 1.	T=0	
MSC-MD-6	MACsec Devices shall enable data delay protection for MKA.	T=0	
MSC-MD-7	MACsec Devices shall have an MKA Lifetime Timeout limit set to 6.0 seconds and Hello Timeout limit set to 2.0 seconds.	T=0	
MSC-MD-8	MACsec Devices shall have the replay window set to 2 or as low as possible given the nature of the Black network being traversed.	T=0	
MSC-MD-9	MACsec Devices shall require all traffic on an external facing port to be encrypted (e.g., must-secure).	T=0	
MSC-MD-10	MACsec Device configuration files, whether printed or electronically copied, shall be protected to the highest classification of the MACsec Device's CAK.	T=0	
MSC-MD-11	MACsec Devices shall have the Confidentiality Offset set to 0 (zero).	T=0	
MSC-MD-12	If a standalone device is required to provide encapsulation of MACsec traffic between an Inner MACsec Device and an Outer Encryption Component, the standalone device shall be considered a Solution Component when satisfying requirements in Section 11.1.	T=0	



# Multi-Site Connectivity Capability Package



## 11.4 ADDITIONAL REQUIREMENTS FOR INNER ENCRYPTION COMPONENTS

Additional requirements for Inner Encryption Components are identified in Table 9.

**Table 9. Additional Requirements for Inner Encryption Components (IR)**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-IR-1	Inner VPN Gateways shall use Tunnel mode IPsec or Transport mode IPsec with an associated IP tunneling protocol (e.g., Transport Mode IPsec with GRE).	T=O	
MSC-IR-2	Sizes for packets or frames leaving the external interface of Inner Encryption Components shall be configured to reduce fragmentation and impact performance. This requires proper configuration of the Maximum Transmission Unit (MTU) (for IPv4 or MACsec) or Path MTU (PMTU) (for IPv6) and should consider Black network and Outer Encryption Component MTU/PMTU values to achieve this.	O	Optional
MSC-IR-3	Inner Encryption Components shall not allow any packets received on an interface connected to a Red network to bypass encryption and be forwarded out through an interface connected to a Gray network.	T=O	
MSC-IR-4	Inner Encryption Components shall not allow any packets received on an interface connected to a Gray network to bypass decryption and be forwarded out through an interface connected to a Red network.	T=O	

## 11.5 ADDITIONAL REQUIREMENTS FOR OUTER ENCRYPTION COMPONENTS

Additional requirements for Outer Encryption Components are identified Table 10.

**Table 10. Additional Requirements for Outer Encryption Components (OR)**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-OR-1	Outer VPN Gateways shall use Tunnel mode IPsec.	T=O	
MSC-OR-2	Outer Encryption Components shall not allow any packets received on an interface connected to a Gray network to bypass encryption and be forwarded out through an interface connected to a Black network.	T=O	
MSC-OR-3	All traffic received by the Outer Encryption Components on an interface connected to a Gray network, with the exception of Control Plane traffic, shall have already been encrypted once.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-OR-4	Outer Encryption Components shall not allow any packets received on an interface connected to a Black network to bypass decryption.	T=O	
MSC-OR-5	The Outer Encryption Components shall not permit split-tunneling.	T=O	
MSC-OR-6	Outer Encryption Components shall not perform routing.	T=O	

## 11.6 PORT FILTERING REQUIREMENTS FOR SOLUTION COMPONENTS

Requirements for port filtering for Solution Components are identified in Table 11.

**Table 11. Port Filtering (PF) Requirements for Solution Components**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-1	All Solution Components shall have all network interfaces restricted to the smallest address ranges, ports, and protocols possible.	T=O	
MSC-PF-2	All Solution Components shall have all unused network interfaces disabled.	T=O	
MSC-PF-3	For all Outer VPN Gateway interface connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, ESP, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-4	For all Outer MACsec Device interface connected to a Black network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only EAP-TLS and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed.	T=O	
MSC-PF-5	For all interfaces connected to a Gray network, traffic filtering rules shall be applied to both inbound and outbound traffic, such that only IKE, IPsec, MKA, MACsec, and control plane protocols (as defined in this CP) approved by organization-defined policy are allowed. All packets not explicitly allowed shall be blocked.	T=O	
MSC-PF-6	Any service or feature that allows an Outer Encryption Component to contact a third party server (such as one maintained by the manufacturer) shall be blocked.	T	MSC-PF-7



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-7	Any service or feature that allows an Outer Encryption Component to contact a third party server (such as one maintained by the manufacturer) shall be disabled.	O	MSC-PF-6
MSC-PF-8	Each Encryption Component shall only accept management traffic on the physical ports connected to its management network.	T=O	
MSC-PF-9	Multicast messages received on external interfaces of Outer Encryption Components shall be dropped.	T=O	
MSC-PF-10	For solutions using IPv4, an Outer VPN Gateways using IPsec shall drop all packets that use IP options.	T=O	
MSC-PF-11	For solutions using IPv4, each VPN Gateway shall only accept packets with Transmission Control Protocol (TCP), User Data Protocol (UDP), Encapsulating Security Payload (ESP), or ICMP in the IPv4 Protocol field and drop all other packets.	T=O	
MSC-PF-12	For solutions using IPv6, each VPN Gateway shall only accept packets with ESP, TCP, UDP, or ICMPv6 in the IPv6 Next Header field and drop all other packets.	T=O	
MSC-PF-13	The Gray network interfaces of Outer Encryption Components shall allow IKE and IPsec, or MACsec traffic, as appropriate, that is between two Inner Encryption Components protecting networks of the same classification level or that is being used for management of the Gray network.	T=O	
MSC-PF-14	The Gray network interfaces of Outer VPN Gateways shall allow HTTP traffic between Inner VPN Gateways and Inner CDPs/OCSP Responders.	T	MSC-PF-15 and MSC-PF-16
MSC-PF-15	The Gray network interfaces of Outer VPN Gateways shall allow HTTP GET requests from Inner VPN Gateways to Inner CDPs for the URL of the CRL needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-PF-14
MSC-PF-16	The Gray network interfaces of Outer VPN Gateways shall allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280, and block all other HTTP responses.	O	MSC-PF-14
MSC-PF-17	The Gray network interfaces of Outer Encryption Components shall only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same classification level.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-PF-18	The Gray network interfaces of Outer Encryption Components shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O	
MSC-PF-19	The Gray network interfaces of Outer Encryption Components shall allow management and control plane protocols (as defined in this CP) that have been approved by policy.	T=O	
MSC-PF-20	The Gray network interfaces of Outer Encryption Components shall deny all traffic that is not explicitly allowed by requirements MSC-PF-8, MSC-PF- 13, MSC-PF-14, MSC-PF-15, or MSC-PF-19.	T=O	
MSC-PF-21	CDPs/OCSP Responders shall only allow inbound HTTP traffic.	T=O	

## 11.7 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 12 defines the requirements for Configuration Change Detection.

**Table 12. Configuration Change Detection (CM) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-CM-1	A baseline configuration for all components shall be maintained by the Security Administrator and be available to the Auditor.	T=O	
MSC-CM-2	An automated process shall ensure that configuration changes are logged.	T=O	
MSC-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	T=O	
MSC-CM-4	All Solution Components shall be configured with a monitoring service that detects all changes to configuration.	T=O	



# Multi-Site Connectivity Capability Package



## 11.8 DEVICE MANAGEMENT REQUIREMENTS

Table 13 defines the requirements for Device Management.

**Table 13. Device Management (DM) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-1	Administration Workstations shall be dedicated for the purposes given in this CP and shall be physically separated from workstations used to manage non-CSfC solutions.	T=O	
MSC-DM-2	Administration Workstations shall physically reside within a protected facility where CSfC solution(s) are managed.	T=O	
MSC-DM-3	Administration Workstations shall connect from an internal port. Specifically, the Inner Encryption Component shall be managed from the Red network and the Outer Encryption Component shall be managed from the Gray network.	T=O	
MSC-DM-4	A separate LAN or VLAN on the Enterprise/Red network shall be used exclusively for all management of Inner Encryption Components and Solution Components within the Red network.	T=O	
MSC-DM-5	A separate LAN or VLAN on the Gray network shall be used exclusively for all management of Outer Encryption Components and Solution Components within the Gray network.	T=O	
MSC-DM-6	The Gray Management network shall not be directly connected to Non-secure Internet Protocol Router Network (NIPRNet) or any other Unclassified network not dedicated to the administration of CSfC solutions.	T=O	
MSC-DM-7	All components shall be configured to restrict the IP address range for the network administration device to the smallest range possible. Note that locally managing Solution Components is also acceptable.	T=O	
MSC-DM-8	All administration of Solution Components shall be performed from an Administration Workstation remotely using one of SSHv2, IPsec, MACsec, or TLS 1.2 or later version, or by managing the Solution Components locally.	T=O	
MSC-DM-9	Security Administrators shall authenticate to Solution Components before performing administrative functions.	T	MSC-DM-10



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-DM-10	Security Administrators shall authenticate to Solution Components with CNSA Suite compliant certificates before performing administrative functions remotely.	O	MSC-DM-9
MSC-DM-11	Security Administrators shall initiate certificate signing requests for Solution Components as part of their initial keying within the solution.	T=O	
MSC-DM-12	Administration Workstations that interact with the Certificate Authority for the Outer VPN Gateways must be located on the Gray network.	T=O	
MSC-DM-13	VPN Gateways shall obtain certificates through the use of PKCS #10 and #7 requests.	T	MSC-DM-14
MSC-DM-14	Devices shall use Enrollment over Secure Transport (EST) as detailed in IETF RFC 7030 for certificate management.	O	MSC-DM-13
MSC-DM-15	The same Administration Workstation shall not be used to manage Inner Encryption Components and Outer Encryption Components.	T=O	
MSC-DM-16	Outer Encryption Components and Solution Components within the Gray network shall forward log entries to a SIEM on the Gray Management network within 10 minutes.	T=O	
MSC-DM-17	Inner Encryption Components and Solution Components within the Red network shall forward log entries to a SIEM on the Red Management network within 10 minutes.	T=O	
MSC-DM-18	All logs forwarded to a SIEM on the Gray Management network shall be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	Optional
MSC-DM-19	All logs forwarded to a SIEM on a Red Management network shall be encrypted using SSHv2, IPsec, MACsec, or TLS 1.2 or later.	O	Optional
MSC-DM-20	Outer Encryption Components shall only be managed by Security Administrators cleared to at least the highest level of classification of each Red network supported by the Outer Encryption Component at the physical site the Outer Encryption Component is located.	T=O	
MSC-DM-21	When managing Solution components over the Black network, the management traffic shall be encrypted with algorithms IAW Table 5 and Table 7.	T=O	



# Multi-Site Connectivity Capability Package



## 11.9 CONTINUOUS MONITORING REQUIREMENTS

Continuous monitoring requirements are identified in Table 14.

**Table 14. Requirements for Continuous Monitoring (MR)**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-MR-1	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Detection System (IDS).	T	MSC-MR-2
MSC-MR-2	Traffic from the Black, Gray, or Red networks shall be monitored from an Intrusion Protection System (IPS).	O	MSC-MR-1
MSC-MR-3	An IDS shall be deployed between the Outer Encryption Component and Gray Network Firewall (M1), or between the Gray Network Firewall and the Inner Encryption Component (M2), or on the internal side of the Inner Encryption Component (M3).	O	MSC-MR-4 MSC-MR-5 MSC-MR-6
MSC-MR-4	An IDS shall be deployed between the Outer Encryption Component and Gray Network Firewall (M1), and between the Gray Network Firewall and the Inner Encryption Component (M2), and on the internal side of the Inner Encryption Component (M3).	O	MSC-MR-3 MSC-MR-5 MSC-MR-6
MSC-MR-5	An IPS shall be deployed between the Outer Encryption Component and Gray Network Firewall (M1), or between the Gray Network Firewall and the Inner Encryption Component (M2), or on the internal side of the Inner Encryption Component (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-6
MSC-MR-6	An IPS shall be deployed between the Outer Encryption Component and Gray Network Firewall (M1), and between the Gray Network Firewall and the Inner Encryption Component (M2), and on the internal side of the Inner Encryption Component (M3).	O	MSC-MR-3 MSC-MR-4 MSC-MR-5
MSC-MR-7	Each IDS in the solution shall be configured to send alerts to the Security Administrator.	O	MSC-MR-8
MSC-MR-8	Each IPS in the solution shall be configured to send alerts to the Security Administrator.	O	MSC-MR-7
MSC-MR-9	Each IDS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	MSC-MR-10
MSC-MR-10	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized destination IP addresses.	O	MSC-MR-9
MSC-MR-11	Each IDS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	MSC-MR-12



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-MR-12	Each IPS in the solution shall be configured with rules that block and generate alerts upon detection of any unauthorized source IP addresses.	O	MSC-MR-11
MSC-MR-13	A SIEM component shall be placed within the Gray network unless devices are configured to push events to an Enterprise/Red network SIEM through an AO-approved one-way tap.	T=O	
MSC-MR-14	A SIEM shall be configured to send alerts to the Auditor when anomalous behavior is detected (i.e., blocked packets from the Outer Encryption Component or Gray Network Firewall).	T=O	
MSC-MR-15	The Gray SIEM shall collect logs from the Outer Encryption Component, Gray Network Firewall, and any components located within the Gray Management Services.	T=O	
MSC-MR-16	Logs sent to the Gray SIEM shall be encrypted with SSHv2, IPsec, MACsec, or TLS 1.2 or later.	T=O	
MSC-MR-17	One-way taps deployed as part of the solution shall be approved for use by the AO.	T=O	
MSC-MR-18	One-way taps deployed as part of the solution shall only allow monitoring data to flow from Monitoring Point 2 (M2) and/or Monitoring Point 1 (M1) to an enclave at the Red level that is isolated from the Red/Enterprise network.	T=O	

## 11.10 AUDITING REQUIREMENTS

Auditing requirements for the MSC Solution are identified in Table 15.

**Table 15. Auditing (AU) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-1	Encryption Components shall log establishment of an encryption tunnel.	T=O	
MSC-AU-2	Encryption Components shall log termination of an encryption tunnel.	T=O	
MSC-AU-3	Solution Components shall log all actions performed on the audit log (off-loading, deletion, etc.).	T=O	
MSC-AU-4	Solution Components shall log all actions involving identification and authentication.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-5	Solution Components shall log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.	T=0	
MSC-AU-6	Solution Components shall log all actions performed by a user with super-user or administrator privileges.	T=0	
MSC-AU-7	Solution Components shall log escalation of user privileges.	T=0	
MSC-AU-8	Solution Components shall log generation, loading, and revocation of certificates.	T=0	
MSC-AU-9	Solution Components shall log changes to time.	T=0	
MSC-AU-10	Solution Components shall log when packets received on Gray network interfaces are dropped or blocked.	T=0	
MSC-AU-11	Solution Components shall log the results of built-in self-tests.	T=0	
MSC-AU-12	MACsec Devices shall log creation and updates of Secure Association Keys.	T=0	
MSC-AU-13	MACsec Devices shall log administrator lockout due to excessive authentication failures.	T=0	
MSC-AU-14	MACsec Devices shall log detected replay attempts.	T=0	
MSC-AU-15	Each log entry shall record the date and time of the event.	T=0	
MSC-AU-16	Each log entry shall include the identifier of the event.	T=0	
MSC-AU-17	Each log entry shall record the type of event.	T=0	
MSC-AU-18	Each log entry shall record the success or failure of the event to include failure code, when available.	T=0	
MSC-AU-19	Each log entry shall record the subject identity.	T=0	
MSC-AU-20	Each log entry shall record the source address for network-based events.	T=0	
MSC-AU-21	Each log entry shall record the user and, for role-based events, role identity, where applicable.	T=0	
MSC-AU-22	VPN Gateways shall log the failure to download the CRL from a CDP or OCSP Responder.	T=0	
MSC-AU-23	VPN Gateways shall log if the version of the CRL downloaded from a CDP or OCSP Responder is older than the current cached CRL.	T=0	
MSC-AU-24	VPN Gateways shall log if signature validation of the CRL downloaded from a CDP or OCSP Responder fails.	T=0	
MSC-AU-25	Auditors shall compare and analyze collected network flow data against the established baseline on at least a weekly basis.	T=0	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-AU-26	Locally-run CAs shall comply with the audit and archival requirements defined in IETF RFC 3647 Sections 4.5.4 and 4.5.5, respectively.	T=O	
MSC-AU-27	Locally-run CAs shall comply with periodic audit and assessment requirements defined in IETF RFC 3647 Section 4.8.	T=O	
MSC-AU-28	Audits and assessments for CAs shall be performed by personnel who are knowledgeable in the CAs' operations, as well as the CAs' CP and CPS requirements and processes, respectively.	T=O	
MSC-AU-29	KGCs that deliver CAK management services for MSC Solutions are to comply with audit and assessment requirements defined by the customer's operational security doctrine and enterprise KGC (if applicable).	T=O	
MSC-AU-30	Audits and assessments are to be performed by personnel who are knowledgeable in the KGCs' operations, as well as the KGCs' audit requirements and processes, respectively.	T=O	

## 11.11 KEY MANAGEMENT REQUIREMENTS

This section details key management requirements for the MSC Solution. General requirements are identified, followed by requirements specific to certificates and CAKs.

### 11.11.1 GENERAL REQUIREMENTS

General key management requirements are identified in Table 16.

**Table 16. General Key Management (KM) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-1	Certificate and CAK management services for the Inner tunnel shall be provided through the Red network.	T=O	
MSC-KM-2	Certificate and CAK management services for the Outer tunnel shall be provided through either the Gray or Red network.	T=O	
MSC-KM-3	CAK management services (enterprise or locally-owned) shall be connected to the local Red network.	O	Optional



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-4	If the CAK Management Services operate at the same classification level as a Red network, a non-CDS Controlled Interface shall be used to control information flow between the CAK management services and the Red network.	T=O	
MSC-KM-5	If the CAK Management Services operate at a different classification level than a Red network or Gray network, a Controlled Interface that is also a CDS shall be used to control information flow between the CAK management services and the Red network or Gray network.	T=O	
MSC-KM-6	If multiple Red enclaves exist in the MSC Solution and the Outer CA resides in the Red network, the Outer CA must reside in the Red network with the highest classification level.	T=O	
MSC-KM-7	All device certificates issued by the Gray and Inner CAs, and their corresponding private keys, shall be treated as CUI (or higher as determined by the AO).	T=O	
MSC-KM-8	All certificates issued by the Outer and Inner CAs for the MSC Solution shall be Non-Person Entity (NPE) certificates.	T=O	
MSC-KM-9	Authentication certificates issued by the Gray and Inner CAs for the Solution shall be X.509 v3 certificates as defined in ITU-T Recommendation X.509.	T=O	
MSC-KM-10	CAKs issued to Outer Encryption Components are Unclassified, but are to be treated as CUI.	T=O	
MSC-KM-11	CAKs issued to Inner Encryption Components are classified to the level of the Red network.	T=O	
MSC-KM-12	Enterprise certificate and CAK management services shall be used to the greatest extent possible.	O	Optional
MSC-KM-13	The key sizes and algorithms for CA certificates and authentication certificates issued to VPN Gateways and Administrative Device Components shall be as illustrated in Table 5.	T=O	
MSC-KM-14	All public/private key pairs and certificates for VPN Gateways shall be used for authentication only.	T=O	
MSC-KM-15	All CAKs generated by or issued to an Encryption Component are to be used in strict accordance with approved protocols identified in this CP.	T=O	
MSC-KM-16	CAs shall not escrow private keys.	T=O	
MSC-KM-17	Outer and Inner CAs shall not have access to private keys used in the Solution Components.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-18	A locally-run CA supporting an Inner Tunnel VPN Gateway shall be physically separated from a locally-run CA supporting an Outer Tunnel VPN Gateway.	T=O	
MSC-KM-19	The Outer and Inner CAs shall each operate in compliance with a Certificate Policy and Certification Practice Statement (CPS) that are formatted in accordance with Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647.	T=O	
MSC-KM-20	KGCs and the MSC Solution being supported shall operate in compliance with a NSA-approved Key Management Plan (KMP).	T=O	
MSC-KM-21	MSC Solutions using CAKeys are to obtain an IAD MD 110 waiver if the CAKeys exist in red form during any part of the CAKey life-cycle management process.	T=O	
MSC-KM-22	CAs shall run anti-virus software.	T=O	
MSC-KM-23	Authentication certificate profiles for the Gray and Inner CAs for the MSC Solution shall comply with IETF RFC 5280.	T=O	
MSC-KM-24	Private keys associated with on-line, locally run Outer and Inner CAs shall be protected using Hardware Security Modules (HSMs) validated to at least FIPS 140-2 Level 2. "On-line" means the CA is always powered on.	T=O	

## 11.11.2 CERTIFICATE ISSUANCE REQUIREMENTS

Requirements for issuing certificates are provided in Table 17.

**Table 17. Certificate Issuance Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-25	Gray and Red Management Services Components shall be initially keyed and loaded with certificates within a physical environment certified to protect the highest classification of the MSC Solution.	T=O	
MSC-KM-26	Outer and Inner CAs shall use Public Key Cryptographic Standard (PKCS)#10 and PKCS#7 to issue authentication certificates to VPN Gateways, and Gray and Red Management Services Components.	T	MSC-KM-27



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-27	Outer and Inner CAs shall use IETF RFC 7030 Enrollment over Secure Transport (EST) to issue authentication certificates to VPN Gateways, and Gray and Red Management Services Components.	O	MSC-KM-26
MSC-KM-28	Certificate signing requests for Gray and Red Management Services Components shall be submitted to the CA in accordance with the CA's Certificate Policy (CP) and Certification Practices Statement (CPS).	T=O	
MSC-KM-29	Outer and Inner CAs shall issue certificates in accordance with their Certificate Policies and CPSs.	T=O	
MSC-KM-30	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure the CAs issue certificates within a defined and limited name space and assert: Unique Distinguished Names (DNs) Appropriate key usages A registered policy Object Identifier (OID)	T=O	
MSC-KM-31	Outer and Inner CAs shall assert at least one CRL Distribution Point (CDP) Uniform Resource Locator (URL) in certificates issued to Solution Infrastructure VPN Gateways, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRLs.	T=O	
MSC-KM-32	The key validity period for certificates issued by non-Enterprise, locally run CAs to Solution Components shall not exceed 36 months.	T=O	
MSC-KM-33	Inner CAs shall only issue certificates to Inner VPN Gateways and Red Network Components of MSC Solutions.	T=O	
MSC-KM-34	Outer CAs shall only issue certificates to Outer VPN Gateways and Gray Network Components of MSC Solutions.	T=O	
MSC-KM-35	The Inner VPN Gateway shall only trust the Inner CA used for its network.	T=O	
MSC-KM-36	The Outer VPN Gateway shall only trust the Outer CA used within the solution.	T=O	
MSC-KM-37	The key validity period for certificates issued by Locally-run CAs shall not exceed 14 months.	T=O	
MSC-KM-38	New certificates shall be issued as needed in accordance with local policy.	T=O	



# Multi-Site Connectivity Capability Package



## 11.11.3 CERTIFICATE RENEWAL AND REKEY REQUIREMENTS

Requirements for renewing and rekeying certificates are provided in Table 18.

**Table 18. Certificate Renewal and Rekey Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-39	Certificate renewal or rekey shall occur prior to a certificate expiring.	T=O	
MSC-KM-40	If rekeying of the VPN Gateways is not completed prior to expiration of keys, they shall be rekeyed through the same process as initial keying.	T=O	
MSC-KM-41	Certificate renewal or rekey shall be performed in accordance with the CA's Certificate Policy and CPS.	T=O	
MSC-KM-42	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7.	T	MSC-KM-43
MSC-KM-43	Outer and Inner CAs shall issue renewed/rekeyed authentication certificates to Solution Components using EST (RFC 7030).	O	MSC-KM-42

## 11.11.4 CERTIFICATE REVOCATION REQUIREMENTS

Requirements for revoking certificates are provided in Table 19.

**Table 19. Certificate Revocation Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-44	CRL profiles shall comply with IETF RFC 5280.	T=O	
MSC-KM-45	Outer and Inner CAs shall revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O	
MSC-KM-46	Outer and Inner CAs shall make certificate revocation information available in the form of CRLs signed by the CAs.	T=O	
MSC-KM-47	Procedures for requesting certificate revocation shall comply with the CA's Certificate Policy and Certification Practices Statement.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-48	Certificate Policies and CPSs for non-Enterprise, locally run CAs shall ensure revocation procedures address the following: Removal of a revoked infrastructure device (e.g., VPN Gateway) from the network Re-establishment of a Solution Component whose certificate was revoked Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP addresses	T=O	
MSC-KM-49	Enterprise CAs shall create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O	
MSC-KM-50	Non-enterprise, locally run CAs shall publish new CRLs at least once every 28 days.	T=O	
MSC-KM-51	Non-enterprise, locally run CAs shall create a new CRL within one hour of a certificate being revoked.	T=O	
MSC-KM-52	Solution Components shall have access to new certificate revocation information within 24 hours of the CA creating a new CRL.	T=O	
MSC-KM-53	CRLs shall expire no later than 31 days after their issue date.	T=O	
MSC-KM-54	Non-enterprise, locally run CAs shall ensure that newly created CRLs are published at least 7 days prior to the expiration of the current CRLs.	T=O	
MSC-KM-55	The MSC Solution shall provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Responder on the Red and Gray network that is compliant with IETF RFC 6960.	O	Optional
MSC-KM-56	Certificate revocation status messages delivered by an OCSP Responder shall be digitally signed and compliant with IETF RFC 6960.	O	Optional
MSC-KM-57	Outer and Inner CAs shall make CRLs available to authorized CRL Distribution Points (CDPs), so that the CRLs can be accessed by Solution Components.	T=O	
MSC-KM-58	CRLs hosted by CDPs shall not contain extensions other than what is specified in IETF RFC 5280.	T=O	
MSC-KM-59	CRLs hosted on Inner CDPs shall be signed by the associated Red Network CA.	T=O	
MSC-KM-60	CRLs hosted on Outer CDPs shall be signed by the associated Gray Network CA.	T=O	
MSC-KM-61	CDPs shall only issue CRLs over port 80 (HTTP).	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-62	CRLs shall be transferred via an AO-approved one-way transfer mechanism from Red Network CAs to associated Inner CDP servers.	T=O	
MSC-KM-63	CRLs shall be transferred via an AO-approved one-way transfer mechanism from Gray Network CAs to associated Outer CDP servers.	T=O	
MSC-KM-64	Newly issued CRLs shall be transferred to CDP servers at least 4 days prior to the expiration of the current CRLs.	T=O	
MSC-KM-65	VPN Gateways shall attempt to download the latest CRL from a CDP at least once every 24 hours.	T=O	
MSC-KM-66	CDPs shall only accept traffic on port 80 and ports used for remote management traffic.	T=O	
MSC-KM-67	CDPs shall only accept connections from known VPN Gateway or Administration Workstation addresses or address ranges.	T=O	
MSC-KM-68	If an integrity check of a CRL pulled from a CDP fails, then VPN Gateways shall use the current cached CRL.	T=O	
MSC-KM-69	If a CDP is offline or contains an invalid CRL, then Inner and Outer VPN Gateway CRLs shall be manually updated prior to the expiration of the current CRLs.	T=O	
MSC-KM-70	Red Network CAs shall set the CRL Distribution Points extension of the certificates it generates for the MSC Solution to the list of URLs hosted by Inner CDPs from which Inner VPN Gateways can download the CRL.	T=O	
MSC-KM-71	Gray Network CAs shall set the CRL Distribution Points extension of the certificates it generates for the MSC Solution to the list of URLs hosted by Outer CDPs from which Outer VPN Gateways can download the CRL.	T=O	

## 11.11.5 CAK GENERATION AND DISTRIBUTION REQUIREMENTS

Requirements for generating and distributing CAKs are provided in Table 20.

**Table 20. CAK Generation and Distribution Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-72	Generation of CAKs shall be performed by an NSA-approved Key Generation Component (KGC). NSA-approved means: a) a component from the CSfC Approved Products List; or b) a component approved for the CSfC solution by IADIR; or c) an already approved enterprise service.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-73	Centralized generation, distribution and management of CAKs shall be performed by a dedicated KGC.	T=O	
MSC-KM-74	An Inner KGC shall generate CAKs for Inner MACsec Devices and may generate CAKs for Outer MACsec Devices.	T=O	
MSC-KM-75	If an Inner KGC generates CAKs for Outer MACsec Devices, the CAKs shall be transferred via an AO-approved one-way transfer mechanism	T=O	
MSC-KM-76	An Outer KGC may only generate CAKs for Outer MACsec Devices.	T=O	
MSC-KM-77	CAKs shall be AES 256 bits.	T=O	
MSC-KM-78	CAKs shall not be exposed in plaintext form until they are ready to be installed onto MACsec Devices. Installation of CAKs may be performed via file transfer or text input.	T=O	
MSC-KM-79	CAKs shall be protected from unauthorized disclosure when they are distributed outside of a controlled boundary or over unprotected communications channels through appropriate manual distribution procedures and methods, as defined in the KMP.	T	MSC-KM-80
MSC-KM-80	CAKs shall be protected from unauthorized disclosure when they are distributed outside of a controlled boundary or over unprotected communications channels through the use of pre-placed symmetric PSK Encryption Keys (PEKs) or an approved key distribution protocol.	O	MSC-KM-79
MSC-KM-81	PEKs shall be AES 256 bits.	T=O	
MSC-KM-82	The classification of pre-placed PEKs shall be the same as the classification of the CAKs that are encrypted with the pre-placed PEKs.	T=O	

## 11.11.6 CAK USAGE REQUIREMENTS

Requirements for using CAKs are provided in Table 21.

**Table 21. CAK Usage Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-83	CAKs are to only be used with the MACsec protocol.	T=O	
MSC-KM-84	CAKs and PEKs are to be stored within an approved cryptographic boundary within a Solution Component.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-85	CAKs and PEKs exported from a Solution Component are to be protected from unauthorized disclosure through manual procedure protection methods.	T	MSC-KM-86
MSC-KM-86	CAKs and PEKs exported from a Solution Component are to be protected from unauthorized disclosure through encryption.	O	MSC-KM-85
MSC-KM-87	A compromised CAK/PEK is to never be used in the MSC Solution.	T=O	

## 11.11.7 CAK UPDATE REQUIREMENTS

Requirements for updating CAKs are provided in Table 22.

**Table 22. CAK Update Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-88	The same CAK shall be used in only one pair of MACsec Devices that are establishing an encryption tunnel.	T=O	
MSC-KM-89	CAKs shall be updated every 30 days, or as defined by the KMP.	T=O	
MSC-KM-90	PEKs are to be updated every 90 days, or as defined by the KMP.	T=O	

## 11.11.8 CAK COMPROMISE RECOVERY REQUIREMENTS

Requirements for recovering from compromised CAKs are provided in Table 23.

**Table 23. CAK Compromise Recovery Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-91	The KMP shall document the CAK/PEK compromise recovery process, to include: <ul style="list-style-type: none"> <li>Removal of a compromised infrastructure device (e.g., MACsec Devices) from the network, and</li> <li>Re-establishing a MACsec Device after its CAK is compromised.</li> </ul>	T=O	
MSC-KM-92	Accounting procedures need to support CAK and PEK compromise recovery to ensure all copies of compromised CAKs and PEKs are identified and updated.	T=O	
MSC-KM-93	CAKs/PEKs are to be updated immediately if they are considered compromised.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-94	If a CAK/PEK is considered compromised, a compromise notification shall be submitted to the KGC along with a request to update the CAK/PEK.	T=O	
MSC-KM-95	If a CAK/PEK is compromised, the procedures for CAK/PEK compromise reporting as defined by the applicable KMP shall be followed.	T=O	
MSC-KM-96	If a compromised device is to be reused, that device must go through the initial CAK issuance process.	T=O	

## 11.12 GRAY NETWORK FIREWALL REQUIREMENTS

Table 24 provides requirements for Gray Network Firewalls that are used when networks of different classification share an Outer Encryption Component.

**Table 24. Gray Network Firewall (FW) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-FW-1	Gray Network Firewalls shall permit IKE, IPsec, EAP-TLS and MACsec traffic between two Inner Encryption Components protecting networks of the same classification level.	T=O	
MSC-FW-2	Gray Network Firewalls shall allow HTTP traffic between Inner VPN Gateways and Gray CDP/OCSP Responder.	T	MSC-FW-3 and MSC-FW-4
MSC-FW-3	Gray Network Firewalls shall allow HTTP GET requests from Inner VPN Gateways to Inner CDPs/OCSP Responders for the URL of the CRL needed by the Inner VPN Gateway, and block all other HTTP requests.	O	MSC-FW-2
MSC-FW-4	Gray Network Firewalls shall allow HTTP responses from Inner CDPs/OCSP Responders to Inner VPN Gateways that contain a well-formed CRL per IETF RFC 5280, and block all other HTTP responses.	O	MSC-FW-2
MSC-FW-5	Gray Network Firewalls shall only accept management traffic on the physical ports connected to the Gray Management network.	T=O	
MSC-FW-6	Gray Network Firewalls shall only permit packets whose source and destination IP addresses match the external interfaces of Inner Encryption Components that support Red networks of the same classification level.	T=O	
MSC-FW-7	Gray Network Firewalls shall block all packets whose source address does not match a list of addresses or address ranges known to be reachable from the interface on which the packet was received.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-FW-8	Gray Network Firewalls shall allow control plane traffic (NTP, DHCP, DNS).	T=O	
MSC-FW-9	Gray Network Firewalls shall deny all traffic that is not explicitly allowed by requirements MSC-FW-1, MSC-FW-2, MSC-FW-3, MSC-FW-4, MSC-FW-5 or MSC-FW-8.	T=O	

## 12 REQUIREMENTS FOR SOLUTION OPERATION, MAINTENANCE, AND HANDLING

### 12.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The requirements in Table 25 shall be followed regarding the use and handling of the solution.

**Table 25. Requirements for the Use and Handling of Solutions**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-1	All Solution Components shall be physically protected as classified devices, classified at the level of the network with the highest classification in the solution or in any other MSC Solutions with which it is interconnected.	T=O	
MSC-GD-2	Only authorized and appropriately cleared (or escorted) administrators and security personnel shall have physical access to the Solution Components.	T=O	
MSC-GD-3	All components of the solution shall be disposed of as classified devices, unless declassified using AO-approved procedures.	T=O	
MSC-GD-4	Acquisition and procurement documentation shall not include information about how the equipment will be used, to include that it will be used to protect classified information.	T=O	
MSC-GD-5	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of this CP.	T=O	
MSC-GD-6	The AO will ensure that a compliance audit shall be conducted every year against the latest version of this CP as part of the annual solution re-registration process.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-7	Results of the compliance audit shall be provided to and reviewed by the AO.	T=0	
MSC-GD-8	Customers interested in registering their solution against this CP shall register with NSA and receive approval prior to the AO authorization to operate.	T=0	
MSC-GD-9	The implementing organization shall complete and submit an MSC CP requirements compliance matrix to their respective AO.	T=0	
MSC-GD-10	Registration and re-registration against this CP shall include submission of CP registration forms and compliance matrix to NSA.	T=0	
MSC-GD-11	When a new approved version of the MSC CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months.	T=0	
MSC-GD-12	Solution implementation information, which was provided to NSA during solution registration, shall be updated annually (in accordance with Section 14.3) as part of the annual re-registration process.	T=0	
MSC-GD-13	Audit log data shall be maintained for a minimum of 1 year.	T=0	
MSC-GD-14	The amount of storage remaining for audit events shall be assessed quarterly to ensure that adequate memory space is available to continue recording new audit events.	T=0	
MSC-GD-15	Audit data shall be frequently off-loaded to a backup storage medium.	T=0	
MSC-GD-16	A set of procedures shall be developed by the implementing organization to provide guidance for identifying and reporting security incidents associated with the audit events to the proper authorities and to the data owners.	T=0	
MSC-GD-17	The implementing organization shall 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.	T=0	
MSC-GD-18	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for off-loading audit log data for long-term storage.	T=0	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-19	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for responding to an overflow of audit log data within a product.	T=O	
MSC-GD-20	The implementing organization shall develop a continuity of operations plan for auditing capability which includes a mechanism or method for ensuring that the audit log can be maintained during power events.	T=O	
MSC-GD-21	Strong passwords shall be used that comply with the requirements of the AO.	T=O	
MSC-GD-22	Security critical patches shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP.	T=O	
MSC-GD-23	Local policy shall dictate how the Security Administrator will install patches to Solution Components.	T=O	
MSC-GD-24	Solution components shall comply with local TEMPEST policy.	T=O	
MSC-GD-25	All hardware components shall be tracked through an AO-approved inventory management process that identifies each component as part of a CSfC Solution.	T=O	

Additional MSC-GD requirements can be found in Section 13.

## 12.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 26 lists requirements for reporting security incidents to NSA to be followed in the event that a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators (SAs), Certificate Authority Administrators (CAAs), CAK Administrators (CAKAs), and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for the operations and maintenance of the solution will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary, but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.



# Multi-Site Connectivity Capability Package



Table 26 only provides requirements directly related to the incident reporting process. See Section 11.9 for requirements supporting the detection of events that may reveal that a reportable incident has occurred.

**Table 26. Incident Reporting Requirements (RP)**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-RP-1	Solution owners shall report confirmed incidents meeting the criteria in MSC-RP-3 through MSC-RP-14 within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter issued for the solution.	T=O	
MSC-RP-2	At a minimum, the organization shall provide the following information when reporting security incidents: <ul style="list-style-type: none"> <li>• CSfC Registration Number</li> <li>• Point of Contact (POC) name, phone, email</li> <li>• Alternate POC name, phone, email</li> <li>• Classification level of affected solution</li> <li>• Name of affected Network(s)</li> <li>• Affected component(s) manufacturer/ vendor</li> <li>• Affected component(s) model number</li> <li>• Affected component(s) version number</li> <li>• Date and time of incident</li> <li>• Description of incident</li> <li>• Description of remediation activities</li> <li>• Is Technical Support from NSA requested? (Yes/No)</li> </ul>	T=O	
MSC-RP-3	Solution owners shall report a security failure in any of the CSfC Solution Components.	T=O	
MSC-RP-4	Solution owners shall report any evidence of a compromise or spillage of classified data caused by a failure of the CSfC solution.	T=O	
MSC-RP-5	For Gray Network interfaces, solution owners shall report any malicious inbound and outbound traffic.	T=O	
MSC-RP-6	Solution owners shall report any evidence of an unauthorized device/user gaining access to the classified network via the solution.	T=O	
MSC-RP-7	Solution owners shall report if a Solution Component sends traffic with an unauthorized destination address.	T=O	
MSC-RP-8	Solution owners shall report any malicious configuration changes to the components.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-RP-9	Solution owners shall report any unauthorized escalation of privileges to any of the CSfC Solution Components.	T=O	
MSC-RP-10	Solution owners shall report any evidence of malicious physical tampering with Solution Components.	T=O	
MSC-RP-11	Solution owners shall report any evidence that one or both of the layers of the solution failed to protect the data.	T=O	
MSC-RP-12	Solution owners shall report any significant degradation of services provided by the solution.	T=O	
MSC-RP-13	Solution owners shall report malicious discrepancies in the number of connections established by the Outer Encryption Component.	T=O	
MSC-RP-14	Solution owners shall report malicious discrepancies in the number of connections established by the Inner Encryption Component.	T=O	

## 13 ROLE-BASED PERSONNEL REQUIREMENTS

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

**Security Administrator** – The Security Administrator shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the MSC Solution. Security Administrator duties include but are not limited to:

- 1) Ensuring that the latest security-critical software patches and updates (such as Information Assurance Vulnerability Alerts (IAVAs)) are applied to each product.
- 2) Documenting and reporting security-related incidents to the appropriate authorities.
- 3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic support activities may require that the Security Administrator escort uncleared personnel.
- 4) Employing adequate defenses of auxiliary network devices to enable proper and secure functionality of the MSC Solution.
- 5) Ensuring that the implemented MSC Solution remains compliant with the latest version of this CP.

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



# Multi-Site Connectivity Capability Package



- 1) Administering the CA, including authentication of all components requesting certificates.
- 2) Maintaining and updating the CRL.

**CAK Administrator (CAKA)** – The CAKA shall be responsible for maintaining, monitoring, and controlling all security functions for the KGC products. CAKA duties include but are not limited to:

- 1) Administering the KGC, including authentication of all components requesting CAKs and PEKs.
- 2) Maintaining and updating the CAK revocation list.

**Auditor** – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator, CAA, or CAKA and events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the MSC Solution. Auditor duties include but are not limited to:

- 1) Reviewing, managing, controlling, and maintaining security audit log data.
- 2) Documenting and reporting security-related incidents to the appropriate authorities.
- 3) The Auditor will only be authorized access to Outer and Inner administration components.

**Solution Integrator** – In certain cases, an external integrator may be hired to implement a MSC Solution based on this CP. Solution Integrator duties may include but are not limited to:

- 1) Acquiring the products that compose the solution.
- 2) Configuring the MSC Solution in accordance with this CP.
- 3) Documenting, testing, and maintaining the solution.
- 4) Responding to incidents affecting the solution.

Additional policies related to the personnel that perform these roles in a MSC Solution are identified in Table 27.

**Table 27. Role-Based Personnel Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-26	The Security Administrator, CAAs, CAKAs, Auditor, and Solution Integrators shall be cleared to the highest level of data protected by the MSC Solution. When an Enterprise CA/KGC is used in the solution, the CAA/CAKA already in place may also support this solution, provided they meet this requirement.	T=O	



# Multi-Site Connectivity Capability Package



Req #	Requirement Description	Threshold / Objective	Alternative
MSC-GD-27	The Security Administrator, CAA, CAKA, and Auditor roles shall be performed by different people.	T=O	
MSC-GD-28	All Security Administrators, CAAs, CAKAs, and Auditors shall meet local Information Assurance (IA) training requirements.	T=O	
MSC-GD-29	The CAA(s)/CAKA(s) for the Inner tunnel shall be different individuals from the CAA(s)/CAKA(s) for the Outer tunnel.	T=O	
MSC-GD-30	The Security Administrator(s) for the Inner Encryption Components and supporting components on Red networks shall be different individuals from the Security Administrator(s) for the Outer Encryption Components and supporting components on Gray networks.	T=O	
MSC-GD-31	Administrators shall periodically inspect the physical attributes of infrastructure hardware for signs of tampering or other unauthorized changes.	O	Optional
MSC-GD-32	The Auditor shall review all logs specified in this CP at least once a week.	T=O	
MSC-GD-33	Security Administrators shall initiate the certificate revocation process prior to disposal of any Solution Component.	T=O	
MSC-GD-34	Auditing of the Outer and Inner CA operations shall be performed by individuals who were not involved in the development of the CP and CPS, or integration of the MSC Solution.	T=O	
MSC-GD-35	Auditing of the Key Generation Component operations shall be performed by individuals who were not involved in the development of the KMP, or integration of the MSC Solution.	T=O	

## 14 INFORMATION TO SUPPORT AO

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

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a Test Plan and perform testing of the MSC Solution (see Section 14.1).



# Multi-Site Connectivity Capability Package



- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 14.2.
- The customer provides the results from testing and system certification and accreditation to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from this CP have been properly implemented in accordance with this CP.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 14.3.
- Customers who want to use a variant of the solution detailed in this CP will contact their NSA/IAD Client Advocate to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the MSC CP, and the results shall be provided to the AO.
- The AO will ensure that certificate revocation information is updated on all the Solution Components in the MSC Solution in the case of a compromise.
- The AO will ensure that any Layer 2 or Layer 3 control plane protocols that are used in the solution are necessary for the operation of the network and that local policy supports their use.
- The AO will report incidents affecting the solution in accordance with Section 12.2.

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

## 14.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a MSC Solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the Test Plan and Procedures and for the execution of those procedures to validate the implementation and functionality of the MSC Solution. The entire solution, to include each component described in Section 5, is addressed by this Test Plan.

- 1) Set up the baseline network and configure all components.
- 2) Document the baseline network configuration. Include product model and serial numbers, and software version numbers at a minimum.



# Multi-Site Connectivity Capability Package



- 3) Develop a Test Plan for the specific implementation using the test requirements from Section 15. Any additional requirements imposed by the local AO should also be tested, and the Test Plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.
- 4) Perform testing using the Test Plan derived in Step 3. Network testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
- 5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the MSC Solution functions properly and meets the configuration requirements from Section 11. Testing of these requirements should be used as a minimum framework for the development of the detailed Test Plan and Procedures.

**Table 28. Test (TR) Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-TR-1	The organization implementing the Capability Package shall perform all tests listed in Section 15.	T=O	

## 14.2 RISK ASSESSMENT

The Risk Assessment of the MSC Solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request this document, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the Risk Assessment is available on the SIPRNet CSfC website. The AO shall be provided a copy of the NSA Risk Assessment for their consideration in approving the use of the solution.

## 14.3 REGISTRATION OF SOLUTIONS

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. This registration will allow NSA to track where MSC Solutions are instantiated and to provide the AOs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process is available at <https://www.nsa.gov/resources/everyone/csfc>.



# Multi-Site Connectivity Capability Package



Solution registrations are valid for one year from the date the solution registration is approved, at which time customers are required to re-register their solution to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this IAD-approved CP is published, customers will have six months to bring their solutions into compliance with the new version of this CP and re-register their solution (see requirement MSC-GD-11). Customers are also required to update their registrations whenever the information provided on the registration form changes.

## 15 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure they have properly configured the solution. As defined in Section 9, to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO regarding compliance of the solution with this CP. Note that the details of the procedures are the responsibility of the final developer of the solution test plan in accordance with AO-approved network procedures. The AO is ultimately responsible for ensuring that all requirements from this CP have been properly implemented.

### 15.1 PRODUCT SELECTION

This section contains a procedure to verify that the components in this CP were selected to ensure independence in several important features.

**Requirements being tested:** MSC-PS-1 through MSC-PS-14, MSC-SR-2,

**Procedure Description:**

- 1) For each VPN Gateway, perform the following:
  - a) Verify that the Inner and Outer VPN Gateways are on the list of IPsec VPN Gateways on the CSfC Components List. (MSC-PS-1)
- 2) For each MACsec Device, perform the following:
  - a) Verify that the Inner and Outer MACsec Devices are on the list of MACsec Ethernet Encryptors on the CSfC Components List. (MSC-PS-2)
- 3) For the Inner Encryption Component and the Outer Encryption Component, perform the following:



# Multi-Site Connectivity Capability Package



- a) Verify that the Inner Encryption Component and Outer Encryption Component either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MSC-PS-6).
  - b) Verify that the cryptographic libraries used by the Inner Encryption Component and Outer Encryption Component either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MSC-PS-7)
  - c) Verify the Inner Encryption Component and Outer Encryption Component are running on physically separate hardware platforms. (MSC-PS-10)
- 4) For each CA, perform the following:
- a) Verify the Inner and Outer tunnel CAs came from the list of CAs on the CSfC Components List or are Enterprise CAs. (MSC-PS-4)
  - b) Verify that the cryptographic libraries used by the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MSC-PS-8)
  - c) Verify that the Inner and Outer CAs either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MSC-PS-12)
- 5) For each Gray Network Firewall and Inner Encryption Component, perform the following:
- a) Verify that the Gray Network Firewall and Inner Encryption Component either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (MSC-PS-9)
  - b) Verify the Gray Network Firewall and Inner Encryption Component are running on physically separate hardware platforms. (MSC-PS-11)
- 6) For each Gray Network Firewall, perform the following:
- a) Verify that the Gray Network Firewalls are on the list of Firewalls on the CSfC Components List. (MSC-PS-3)
- 7) For each IPS, perform the following:
- a) Verify that the IPS is on the list of IPSs on the CSfC Components List. (MSC-PS-5)
- 8) For all components in the solution:
- a) Verify that each component has gone through a Product Supply Chain Threat Assessment. (MSC-PS-13)



# Multi-Site Connectivity Capability Package



- b) Verify that the components are configured to use the NIAP-certified evaluated configuration. (MSC-PS-14)
- 9) For sites requiring interoperability, ensure that VPN Gateways selected for each tunnel can be configured to communicate using the requirements specified in this Capability Package. (MSC-SR-2)

## Expected Result:

The results of the inspection should reveal that the MSC Solution components conform to this CP.

## 15.2 OVERALL SOLUTION

This section contains a procedure to create an accurate record of the physical components composing the MSC Solution (including workstations, VPN Gateways, CAs, and wiring). The test will also ensure that the physical implementation of the MSC Solution matches one of the high-level designs given in the VPN Capability Package.

**Requirements being tested:** MSC-SR-1, MSC-SR-3 through MSC-SR-9, MSC-SR-11

## Procedure Description:

- 1) Verify that the physical location of any network services for the Outer Encryption Component is located on the appropriate Gray Management network. Similarly, verify these components for the Inner Encryption Component are located on the appropriate Red network. (MSC-SR-1)
- 2) Verify that the time of day on the Inner Encryption Components and Red Management Services are synchronized with a time source located in the Red Network. (MSC-SR-3)
- 3) Verify that the time of day on the Outer Encryption Components, Gray Network Firewall, and Gray Management Services are synchronized with a time source located in the Gray Network. (MSC-SR-4)
- 4) Verify that all default accounts, passwords, community strings and other default access controls have been either changed or removed. (MSC-SR-5)
- 5) If Red networks of different classification levels share an Outer Encryption Component, verify different ports are used on the Outer Encryption Component or a Gray Network Firewall is located before the Red network of a lower classification level. (MSC-SR-7)
- 6) If Red networks of different classification levels share an Outer Encryption Component, verify the Gray network between the CA, Administration Workstations, or CDP/OCSP Responder and Inner Encryption Component for a Red network of a lower classification level are on a different port on the Outer Encryption Component or behind a Gray Network Firewall. (MSC-SR-8)



# Multi-Site Connectivity Capability Package



- 7) Ensure there are no wireless or physical connections to the solution that are not included in this CP, which may allow traffic to leave a Red or Gray network in a manner that does not go through the MSC Solution (or an NSA-certified encryptor). (MSC-SR-9)
- 8) Verify that when using multiple Inner Encryption Components, those components are placed in parallel. (MSC-SR-11)

## Expected Result:

For Step 1, Gray Management network traffic should be separate from Red Management network traffic. For Steps 2 and 3, the time of day should be synchronized to the appropriate sources. For Step 4, all defaults should be changed or removed. For steps 5 and 6, the Gray Network Firewall should be appropriately located or separate ports on the Outer Encryption Component should be used. For step 7, there should be no extraneous wireless or physical connections allowing data to leave Red or Gray networks besides through the MSC Solution (or an NSA-certified encryptor). For Step 8, Inner Encryption Components are accurately placed.

## 15.3 VPN GATEWAY CONFIGURATIONS

This section contain procedures to ensure that the configurations for all the VPN Gateways in the MSC Solution follow the requirements given in this CP.

**Requirements being tested:** MSC-VG-1 through MSC-VG-4, MSC-VG-6 through MSC-VG-15, MSC-VG-17

### Procedure Description:

- 1) For each VPN Gateway in the solution, perform the following:
  - a) Obtain the current configuration for the VPN Gateway.
  - b) Verify a unique device certificate is loaded with the corresponding CA signing certificate. (MSC-VG-4)
  - c) Verify a device certificate from a CA included in the MSC Solution is listed in the configuration for authentication. (MSC-VG-6)
  - d) Ensure the corresponding CA signing certificate and certificate revocation information are on the VPN Gateway. (MSC-VG-7)
  - e) Verify the requirements MSC-VG-1 through MSC-VG-3 and MSC-VG-8 through MSC-VG-15 are configured properly.
  - f) Verify that the VPN Gateways are configured to re-authenticate the identity of the VPN Gateways at the other end before rekeying the IKE SA. (MSC-VG-17)



# Multi-Site Connectivity Capability Package



## Expected Result:

For Step 1, all VPN Gateways should be configured properly according to the requirements found in this CP.

## 15.4 MACSEC DEVICE CONFIGURATIONS

This section contains a procedure to ensure that the configurations for all the MACsec Devices in the MSC Solution follow the requirements given in this CP.

**Requirements being tested:** MSC-MD-1 through MSC-MD-11

### Procedure Description:

- 1) For each MACsec Device, perform the following:
  - a) Obtain the current configuration for the MACsec Device.
  - b) Verify AES Key Wrap in CMAC mode is used for key distribution and AES GCM is used for encryption; also verify key sizes for both are set to 256 bits. (MSC-MD-1)
  - c) Verify authentication is being performed with a CAK. (MSC-MD-2)
  - d) Verify the CAK is 256 bits and confirm it was generated in accordance with the KMP. (MSC-MD-3)
  - e) Verify the CKN is set to a minimum of 64 bits. (MSC-MD-4)
  - f) Verify the Key Server value is set to 0 (zero) if the MACsec Device is the designated Key Server for the MACsec pair; otherwise ensure the value is set to 1. (MSC-MD-5)
  - g) Ensure data delay protection for MKA is enabled. (MSC-MD-6)
  - h) Ensure the MKA Lifetime Timeout limit is set to 6.0 seconds and the Hello Timeout limit is set to 2.0 seconds. (MSC-MD-7)
  - i) Verify the replay window is set to 2; otherwise confirm it is the lowest possible number given the nature of the Black network being traversed. (MSC-MD-8)
  - j) Verify all traffic on the external facing ports require encryption. (MSC-MD-9)
  - k) Verify that printed or electronic versions of the configuration files are protected to the highest classification of the MACsec Device's CAK. (MSC-MD-10)
  - l) Ensure the Confidentiality Offset is set to 0 (zero). (MSC-MD-11)



# Multi-Site Connectivity Capability Package



## Expected Result:

For Step 1, all MACsec Devices should be configured properly according to the requirements found in this CP.

## 15.5 INNER AND OUTER ENCRYPTION COMPONENT CONFIGURATIONS

This section contains procedures to ensure that the configurations for all the Inner and Outer Encryption Components in the MSC Solution follow the requirements given in this CP.

**Requirements being tested:** MSC-SR-3 through MSC-SR-6, MSC-SR-11, MSC-SR-12, MSC-DM-1, MSC-DM-4 through MSC-DM-6, MSC-DM-8 through MSC-DM-11, MSC-DM-14, MSC-DM-15, MSC-DM-21, MSC-IR-1 through MSC-IR-4, MSC-OR-1, MSC-OR-3 through MSC-OR-6

## Procedure Description:

- 1) For each Encryption Component, perform the following:
  - a) Ensure that default accounts, passwords, community strings, and other default access control mechanisms are changed or removed. (MSC-SR-5)
  - b) Ensure that all components are configured in accordance with local policy and applicable U.S. Government guidance, or, in the event of conflict between this CP and local policy, this CP takes precedence. (MSC-SR-6)
  - c) Ensure that Inner Encryption Components are not performing switching or routing for other Encryption Components. (MSC-SR-12)
  - d) Ensure the time of day on the Inner Encryption Component and Red Management Services matches the current time. This should be within a small margin of error, to be determined by the AO. (MSC-SR-3)
  - e) Ensure the time of day on the Outer Encryption Component, Gray Network Firewall and Gray Management Services matches the current time. This should be within a small margin of error, to be determined by the AO. (MSC-SR-4)
- 2) For each Inner Encryption Component, use the configuration from 1a and perform the following:
  - a) Log into any Inner VPN Gateways and verify that they are configured to use Tunnel or Transport mode IPsec with an associated IP Protocol (e.g., GRE). (MSC-IR-1)
  - b) Log into any Inner VPN Gateways and verify that the MTU (for IPv4) or the PMTU (for IPv6) has been configured to an appropriate size. (MSC-IR-2)



# Multi-Site Connectivity Capability Package



- c) Using a packet analyzer tool on the Inner Encryption Component, verify that traffic leaving the external interface going to the Outer Encryption Component is encrypted. (MSC-IR-3)
  - d) Using a packet analyzer tool on the Inner Encryption Component, verify that traffic coming through the external interface of the Inner Encryption Component is decrypted. (MSC-IR-4)
  - e) Verify a separate LAN or VLAN is established on the Enterprise/Red network and using a packet sniffer, inspect traffic within the Enterprise/Red Network to ensure it is being used exclusively for all management of Inner Encryption Components and Solution Components within the Red network. (MSC-DM-4)
- 3) For each Outer Encryption Component, use the configuration from 1a and perform the following:
- a) Log into the Outer VPN Gateways and verify that they are configured to use Tunnel mode IPsec. (MSC-OR-1)
  - b) Using a packet analyzer tool on the Outer Encryption Component, verify that traffic leaving the external interface going to the Black Network is encrypted. (MSC-OR-3)
  - c) Using a packet analyzer tool on the Outer Encryption Component, verify that traffic coming through the external interface of the Outer Encryption Component is decrypted. (MSC-OR-4)
  - d) Verify that any Outer Encryption Components are not configured to perform split tunneling or routing. (MSC-OR-5, MSC-OR-6)
  - e) Verify that a separate LAN or VLAN is established on the Gray network and using a packet sniffer, inspect traffic within the Gray network to ensure it is being used exclusively for all management of Outer Encryption Components, Gray Network firewall, and Solution Components within the Gray network. (MSC-DM-5)
- 4) For all device administration, verify that requirements MSC-DM-1, MSC-DM-8, MSC-DM-21, and MSC-SR-11 are configured properly.
- 5) For each administration workstation, ensure the Security Administrator is required to authenticate to the component before being granted access. (MSC-DM-9)
- 6) For each administration workstation, ensure the Security Administrator is required to authenticate to Solution Components using CNSA Suite compliant certificates. (MSC-DM-10)
- 7) Ensure that certificate signing requests are initiated by the Security Administrator as part of their initial keying within the solution. (MSC-DM-11)
- 8) Ensure that devices that use EST as detailed in RFC 7030 for certificate management. (MSC-DM-14)



# Multi-Site Connectivity Capability Package



- 9) Ensure that the same Administration Workstation is not used to manage both Inner and Outer Encryption Components. (MSC-DM-15)
- 10) Ensure that requirement MSC-DM-6 has been configured properly.

## Expected Results:

For Steps 1 through 3, the Inner and Outer Encryption Components should be configured properly according to the requirements found in this CP. For Steps 4 through 10, all administration devices should be configured properly according to the requirements found in this CP.

## 15.6 PORT FILTERING

This section contains procedures to ensure that the port filtering configurations for the MSC Solution follow the requirements in this CP.

**Requirements being tested:** MSC-PF-1 through MSC-PF-7 and MSC-PF-9 through MSC-PF-12

### Procedure Description:

- 1) Perform the following steps on each of the Solution Components:
  - a) Log into the component.
  - b) Verify through the configuration file that network interfaces are restricted to the smallest address range, ports, and protocols. (MSC-PF-1)
  - c) Verify through the configuration file that all unused network interfaces are disabled. (MSC-PF-2)
- 2) For the Outer Encryption Components, perform the following:
  - a) Obtain the current configuration for the Outer Encryption Component.
  - b) Verify that the requirements of MSC-PF-3, MSC-PF-4, MSC-PF-6, MSC-PF-7, and MSC-PF-9 through MSC-PF-12 are met.
- 3) For the Inner Encryption Components, perform the following:
  - a) Obtain the current configuration for the Inner Encryption Component.
  - b) Verify the requirement MSC-PF-5 is met.

### Expected Results:

Port filtering is performed correctly and in compliance with requirements in this CP.



# Multi-Site Connectivity Capability Package



## 15.7 CONFIGURATION CHANGE DETECTION

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

**Requirements being tested:** MSC-CM-1 through MSC-CM-4

### Procedure Description:

- 1) The following steps shall be performed for each of the Solution Components.
  - a) Log into the Solution Component.
  - b) Compare the current version of the Solution Component's configuration with the stored baseline and ensure the current version matches the stored configuration. (MSC-CM-1)
  - c) Make a change to the configuration, preferably something that is not fundamental to the security of the MSC Solution.
  - d) Look in the audit log to determine if a log entry has been generated about the configuration change and that the changes from 1c are recorded. (MSC-CM-2, MSC-CM-3)
  - e) Inspect the monitoring service to verify that the service has detected a change in configuration. (MSC-CM-4)

### Expected Result:

The Auditor will validate the baseline configuration was stored in Step 1b. In Step 1d, there should be a log entry created for the configuration change in the audit log including the actual configuration change. Lastly, if there was a configuration change, a monitoring service will detect a change in the configuration.

## 15.8 CONTINUOUS MONITORING

This section contains procedures for ensuring traffic is monitored for and alerts generated for potential unauthorized/malicious traffic. It also contains procedures for ensuring a SIEM is in place to collect logs and that it is configured correctly.

**Requirements being tested:** MSC-MR-1 through MSC-MR-18

### Procedure Description:

- 1) Ensure that an IDS/IPS is deployed to monitor traffic in at least one of three locations (MSC-MR-1 through MSC-MR-6):



# Multi-Site Connectivity Capability Package



- a) Between the Outer Encryption Component and Gray Network Firewall (M1)
- b) Between the Gray Network Firewall and the Inner Encryption Component (M2)
- c) On the internal side of the Inner Encryption Component (M3)
- 2) Ensure that each IDS/IPS in the solution is configured to send alerts to the Security Administrator and, where possible, block malicious traffic. (MSC-MR-7, MSC-MR-8)
- 3) Ensure that each IDS/IPS in the solution is configured with the rules that will generate alerts and, where possible, block traffic for any unauthorized source and destination IP addresses. (MSC-MR-9 through MSC-MR-12)
- 4) Ensure that a SIEM is implemented. (MSC-MR-13 through MSC-MR-16)
  - a) Ensure the SIEM is implemented in the Gray network.
  - b) Otherwise, if the SIEM is implemented within the Enterprise/Red network, ensure devices are configured to push events to an Enterprise/Red SIEM and through an AO-approved one-way tap.
  - c) Send packets expected to be blocked by the Outer Encryption Component or Gray Network Firewall. Ensure the SIEM sends alerts to the Auditor when anomalous behavior such as this is detected.
  - d) Ensure that logs from the Outer Encryption Component, Gray Network Firewall, and any other components located within the Gray Management Services are collected on the Gray SIEM.
  - e) Ensure these logs are encrypted with SSHv2, IPsec, MACsec, or TLS v1.2 or later.
- 5) Ensure that any one-way taps are deployed as per MSC-MR-17 and MSC-MR-18.
  - a) Ensure that any one-way taps deployed as part of the solution are approved for use by the AO.
  - b) Ensure that the SIEM implemented at the Red level that collects black and/or gray monitoring data sent through any one-way tap is deployed in an enclave isolated from the Red/Enterprise network.
  - c) Ensure that monitoring data flowing from M2 and/or M1 can transit to the SIEM if implemented at the Red level.
  - d) Attempt to send other data through the one-way taps to determine if this data is blocked.

## Expected Results:



# Multi-Site Connectivity Capability Package



For Steps 1 – 3, an IDS or IPS is in place to monitor, block where possible, and send alerts as appropriate. For Steps 4 and 5, a SIEM shall be implemented either in the Gray network or the Red/Enterprise network via one-way taps, as approved by the AO, and only monitoring data that will be able to transit through these taps.

## 15.9 AUDITING

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

**Requirements being tested:** MSC-AU-1 through MSC-AU-9, MSC-AU-11, MSC-AU-15 through MSC-AU-25, MSC-DM-16 through MSC-DM-19

### Procedure Description:

- 1) Examples for testing the ability of each Encryption Component to audit and log audit events specified in this CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry in accordance with Section 11.10.
  - a) All actions performed by a user with superuser privileges (auditor, administrator, etc.) and any escalation of user privileges. (MSC-AU-6, MSC-AU-7)
    - i) Log in as an administrator to the Encryption Component.
    - ii) Perform a variety of administrator actions on the Encryption Component.
    - iii) Verify a log entry was created for each action taken in Step ii that required superuser privileges and also states the escalation of privileges.
    - iv) Revert back to the baseline configuration, eliminating the changes made in Step ii.
    - v) Repeat the above with the Auditor role.
  - b) Changes to time. (MSC-AU-9)
    - i) Log in as a Security Administrator to the Encryption Component.
    - ii) Modify the system time on the Encryption Component by at least 1 hour.
    - iii) Verify a log entry was created due to the change in system time and by whom.
    - iv) Revert the system time back to the accurate time of day.



# Multi-Site Connectivity Capability Package



- c) Log into and out of the MSC Solution as a normal user and send traffic to the Red Network. Then log into the central log server as an Auditor, and inspect the audit entry for the following: (MSC-DM-16, MSC-DM-17)
    - i) Verify that the log on as a normal user is logged and has an identifiable code for the type of event. (MSC-AU-4, MSC-AU-17)
    - ii) Verify that the log entry identifies the subject accessing the solution. (MSC-AU-19)
    - iii) Verify that the log entry identifies the event. (MSC-AU-16)
    - iv) Verify that the log entry includes the time, date, and the time zone offset. (MSC-AU-15)
  - d) Establish and terminate an IPsec tunnel. Verify in the logs, that these two events were logged. Repeat for a MACsec tunnel. (MSC-AU-1, MSC-AU-2)
  - e) Ensure all built-in self-test results have been recorded in the audit log which may indicate failures in cryptographic functionality. (MSC-AU-11)
    - i) Completely power down the Encryption Component.
    - ii) Power the Encryption Component back up so that the automatic self-tests are run.
    - iii) Verify a log entry was created due to running the self-test.
  - f) Log into a Solution Component as a Security Administrator and delete previously recorded audit log. Verify the log recorded this deletion. (MSC-AU-3)
  - g) As the Certificate Administrator, log into the audit log and attempt to delete a log entry. Verify this action is recorded with a failure code. (MSC-AU-5, MSC-AU-18)
  - h) Verify a log entry was created for the attempted unauthorized action.
- 2) Verify the source address for all audit log entries is recorded. (MSC-AU-20, MSC-AU-21)
  - 3) Verify that all logs forwarded to a log server on a Gray Management network are configured to be encrypted while in transit using SSHv2, IPSEC, MACsec, or TLS 1.2 or later with the appropriate CNSA Suite algorithm supported by the solution. (MSC-DM-18)
  - 4) Verify that all logs forwarded to a log server on a Red Management network are configured to be encrypted while in transit using SSHv2, IPsec, MACsec, or TLS 1.2 or later with the appropriate CNSA Suite algorithm supported by the solution. (MSC-DM-19)
  - 5) Verify the procedure required by MSC-AU-25 is currently in place by the implementing organization and is followed.



# Multi-Site Connectivity Capability Package



- 6) Verify VPN Gateways log the failure to pull the CRL from the respective CDP/OCSP Responder. (MSC-AU-22)
  - a) CDP Servers and OSCP Responders shall remove all CRLs.
  - b) Connecting VPN Gateways shall attempt to pull the CRL from the respective CDP/OCSP Responder.
  - c) Review the VPN Gateways audit logs to verify that a log report is generated from failure to pull the CRL.
- 7) Verify VPN Gateways log if the version of the CRL on the CDP/OCSP Responder is older than the current cached CRL. (MSC-AU-23)
  - a) Load the CDP/OCSP Responder with CRLs that are older than the current cached CRLs on the VPN Gateway.
  - b) Have the VPN Gateway attempt to pull the CRLs.
  - c) Review the VPN Gateway audit logs to verify that a log report is generated.
- 8) Verify the VPN Gateway logs if signature validation of CRL on the CDP/OCSP Responder fails. (MSC-AU-24)
  - a) Load the CDP/OCSP Responder with CRLs that contain invalid signature.
  - b) Have the VPN Gateway pull the CRLs.
  - c) Review the VPN Gateway audit logs to verify that a log report is generated due to an invalid CRL signature.
- 9) For all Solution Components, install appropriate certificates, generated by the approved CA, and configure the solution so that components use the certificates for authentication.
  - a) Verify an entry to the audit log has been created due to certificate loading and generation (MSC-AU-8)
  - b) Initiate a revocation of certificates for the Solution Components.
  - c) Verify that an entry in the audit log has been created due to certificate revocation. (MSC-AU-8)

## Expected Result:

For Step 1, all occurrences of auditable events given should generate an entry in the audit log. For Step 2, the source address should be the Encryption Component's loopback address. For Steps 3-4, all logs



# Multi-Site Connectivity Capability Package



forwarded on Red Management and Gray Management networks should be encrypted with the appropriate protocols. For Steps 5-7, there should be an audit log entry created for each activity. For Step 8, a log should be generated for generation and revocation of certificates.

## 15.10 KEY MANAGEMENT

This section contains procedures to ensure all CAs, certificates, KGCs and CAKs used in the MSC Solution are following the requirements in this CP.

### 15.10.1 CERTIFICATE AUTHORITIES AND CERTIFICATES

This section contains procedures to ensure all CAs and certificates used in the MSC Solution are following the requirements in this CP.

**Requirements being tested:** MSC-KM-1, MSC-KM-2, MSC-KM-5, MSC-KM-7, MSC-KM-9, MSC-KM-13, MSC-KM-14, MSC-KM-16 through MSC-KM-18, MSC-KM-24 through MSC-KM-34, MSC-KM-39, MSC-KM-41 through MSC-KM-45, MSC-KM-47 through MSC-KM-52, MSC-KM-54 through MSC-KM-56, and MSC-KM-61, MSC-AU-26 through MSC-AU-28, MSC-PF-21

#### Procedure Description:

- 1) Perform the following to validate the correct deployment of CAs:
  - a) For CAs, verify the configuration of the MSC Solution to ensure that Outer CAs deliver services through either the Gray or Red networks and Inner CAs only deliver services through the Red network (MSC-KM-1, MSC-KM-2)
  - b) For CAs, verify that the Outer and Inner CAs are physically separate from one another. (MSC-KM-18)
  - c) For Locally-run CAs that operate on-line, verify the CAs use FIPS 140-2 Level 2 or higher HSMs to protect the CAs' private signing keys. (MSC-KM-24)
  - d) For all CAs, verify that the CA does not have access to any Solution Components' private keys. (MSC-KM-17)
- 2) Perform the following to validate the structure of certificates issued by CAs:
  - a) Obtain a sample set of test certificates issued to Solution Components.
  - b) Verify the Distinguished Name in each certificate identifies an NPE. (MSC-KM-30)
  - c) Verify the Key Usage extension in the certificate only asserts "digitalSignature". (MSC-KM-14)



# Multi-Site Connectivity Capability Package



- d) Verify the certificates are compliant with the data standard for Version 3 certificates defined in ITU-T Recommendation X.509. (MSC-KM-9)
  - e) Verify the certificates are compliant with IETF RFC 5280 profile requirements. (MSC-KM-31)
  - f) Verify the certificates are compliant with key sizes and algorithms specified in this CP. (MSC-KM-13)
- 3) Perform the following to validate correct policy implementation as it relates to CAs and certificates issued by the CAs:
- a) Verify the CA has a Certificate Policy and a CPS in place that is compliant with IETF RFC 3647, and that the CA operates in accordance with the policy and CPS. (MSC-KM-29, MSC-AU-26, MSC-AU-27, MSC-AU-28)
  - b) Verify the Certificate Policy states device authentication certificates issued by the CA, along with corresponding private keys, are considered CUI, and user private keys are classified to the level determined by the AO. (MSC-KM-7)
- 4) Perform the following steps to validate the certificate issuance capability of the MSC Solution:
- a) Verify that a physical environment is identified to initially load keys and certificates onto Solution Components, where the environment is certified to protect information at the highest classification level of the Red network. (MSC-KM-25)
  - b) Verify that the key and certificate provisioning for Solution Components ensures private keys are never escrowed. (MSC-KM-16)
  - c) Generate a public/private key pair for the Outer VPN Gateway that complies with the key size and algorithm requirements in this CP.
  - d) Generate a certificate request for the Outer VPN Gateway, and ensure the request complies with PKCS#10.
  - e) Submit the certificate request to the Outer CA and verify that the CA returns a signed certificate request using PKCS#7. (MSC-KM-26)
  - f) Repeat steps 4c through 4e for each Inner VPN Gateway.
  - g) If the MSC Solution supports IETF RFC 7030 (EST), verify that the certificate request, response and installation process complies with EST. (MSC-KM-27)
  - h) Verify that the certificate request and issuance processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (MSC-KM-28, MSC-KM-29)



# Multi-Site Connectivity Capability Package



- i) For locally run CAs, verify the Certificate Policies and CPSs to ensure certificates issued by the CAs: 1) enforce unique DNs; 2) assert key usages as defined by MSC-KM-5; and 3) assert a registered policy OID.
  - j) For locally run CAs, examine the contents of a sample set of issued certificates to ensure that the certificates assert: 1) unique DNs; 2) key usages as defined by MSC-KM-5; and 3) a registered policy OID. (MSC-KM-30)
  - k) For all CAs, examine the contents of a sample set of issued certificates and ensure that at least one valid CDP is asserted in the CDP extension of the certificates. (MSC-KM-31)
  - l) For locally run CAs, ensure the validity periods asserted in certificates issued by the CAs do not exceed 36 months for Solution Components. (MSC-KM-32)
  - m) Verify the Inner CAs can only issue certificates to Inner VPN Gateways and Red network components. (MSC-KM-33)
  - n) Verify the Outer CAs can only issue certificates to Outer VPN Gateways and Gray network components. (MSC-KM-34)
- 5) Perform the following steps to validate the certificate renewal and rekey capability:
- a) Verify that the certificate renew and rekey processes comply with the Outer and Inner CAs' Certificate Policies and CPSs. (MSC-KM-41)
  - b) Verify that the Outer and Inner CAs' Certificate Policies and CPSs require certificate renew and rekey be performed prior to a certificate expiring, and require Solution Components go through the initial certificate issuance process if the certificate is expired. (MSC-KM-39)
  - c) Generate a new public/private key pair for the Outer VPN Gateway that complies with the key size and algorithm requirements in this CP.
  - d) Generate a certificate renew and rekey request for the Outer VPN Gateway, and ensure the request complies with PKCS#10.
  - e) Submit the certificate request to the Outer CA, and verify that the CA returns a signed certificate using PKCS#7. (MSC-KM-42)
  - f) Repeat steps 5c through 5e for each Inner VPN Gateway.
  - g) If the MSC Solution supports IETF RFC 7030 (EST), verify the certificate renew and rekey request, response and installation process complies with EST. (MSC-KM-43)
- 6) Perform the following steps to validate the certificate revocation and CDP capabilities:



# Multi-Site Connectivity Capability Package



- a) Verify the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for revoking certificates, where certificate revocation is required when the binding between the subject information and public key within the certificate is no longer considered valid. (MSC-KM-45)
- b) Verify the Outer and Inner CAs' Certificate Policies and CPSs define requirements and procedures for requesting the revocation of certificates. (MSC-KM-47)
- c) For locally run CAs, verify the Outer and Inner CAs' Certificate Policies and CPSs define certificate revocation requirements and procedures that address: 1) removal of a revoked Solution Component from the MSC Solution; and 2) re-establishment of a Solution Component after certificate revocation is performed. (MSC-KM-48)
- d) Verify that the Outer and Inner CAs have the capability to generate CRLs after certificate revocation functions are performed. (MSC-KM-51)
- e) Obtain CRLs from the Outer and Inner CAs and ensure their structures are compliant with the data standard for Version 2 CRLs defined in ITU-T Recommendation X.509, and with the CRL profile standard defined by IETF RFC 5280. (MSC-KM-44)
- f) Obtain CRLs from the Outer and Inner CAs and upload them onto the CDPs.
- g) Verify that Solution Components can access the CDPs and download the CRLs issued by the Outer and Inner CAs via HTTP. (MSC-KM-61, MSC-PF-21)
- h) For Enterprise CAs, verify that the Certificate Policies and CPSs define requirements and procedures for publishing CRLs. (MSC-KM-49)
- i) For locally run CAs, verify that the Certificate Policies and CPSs define requirements and procedures for: 1) publishing new CRLs at least once every 28 days; 2) creating a new CRL within one hour of a certificate being revoked; and 3) publishing a newly created CRL at least 7 days before the expiration of the current CRL. (MSC-KM-50, MSC-KM-51, MSC-KM-54)
- j) Verify the MSC Solution has procedures defined to transfer new CRLs to CDPs within 24 hours of the CRLs being created. (MSC-KM-52)
- k) For MSC Solutions that support OCSP to provide certificate revocation status information, verify the OCSP Responders are deployed on the Gray and Red networks to deliver OCSP responses in accordance with IETF RFC 6960. (MSC-KM-55)
- l) Generate an OCSP request from the connecting Outer VPN Gateway and send the request to the OCSP Responder operating in the Black network.



# Multi-Site Connectivity Capability Package



- m) Generate an OCSP response from the OCSP Server in the Black network and deliver it to the connecting Outer VPN Gateway.
- n) Examine the OCSP response and verify that it is digitally signed and compliant with IETF RFC 6960. (MSC-KM-56)

## Expected Results:

CAs, CDPs, OCSP Responders and certificates are correctly deployed and in compliance with requirements in this CP.

### 15.10.2 KEY GENERATION COMPONENTS AND CONNECTIVITY ASSOCIATION KEYS

This section contains procedures for ensuring the KGCs and CAKeys used within the solution comply with the requirements of this CP.

**Requirements being tested:** MSC-KM-1, MSC-KM-2, MSC-KM-4, MSC-KM-5, MSC-KM-10, MSC-KM-11, MSC-KM-15, MSC-KM-20, MSC-KM-21, MSC-KM-72, MSC-KM-74 through MSC-KM-83, MSC-KM-85 through MSC-KM-92, MSC-KM-94, MSC-KM-95

## Procedure Description:

- 1) Perform the following to validate the correct deployment of CAKey Management Services and KGCs:
  - a) For CAKey Management Services (including KGCs), verify the configuration of the MSC Solution to ensure that Outer CAKey Management Services are provided through either the Gray or Red networks and Inner CAKey Management Services are provided by the Red network. (MSC-KM-1, MSC-KM-2)
  - b) If CAKey Management Services operate at the same classification level as a Red network, verify a Controlled Interface is used to control information flow between the CAKey Management Services and the Red network. (MSC-KM-4)
  - c) If CAKey Management Services operate at a different classification level than a Red network or Gray network, verify a CDS Controlled Interface is used to control information flow between the CAKey Management Services and the Red or Gray networks. (MSC-KM-5)
  - d) Verify KGCs and the MSC Solution are operating in compliance with an NSA-approved Key Management Plan. (MSC-KM-20)
  - e) Verify an IAD MD 110 waiver was obtained, if necessary. (MSC-KM-21)
  - f) Verify CAKeys are generated by a NSA-approved KGC. (MSC-KM-72)



# Multi-Site Connectivity Capability Package



- g) Verify an Inner KGC generates CAKs for Inner MACsec Devices or Outer MACsec Devices. (MSC-KM-74)
  - h) Verify an Outer KGC only generates CAKs for Outer MACsec Devices. (MSC-KM-76)
  - i) If an Inner KGC generates a CAK for Outer MACsec Devices, verify an AO-approved one-way transfer mechanism is used. (MSC-KM-75)
  - j) Confirm that CAKs are 256 bits. (MSC-KM-77)
  - k) Confirm that CAKs are not exposed in plaintext form until they are ready to be installed onto MACsec Devices. (MSC-KM-78)
  - l) Verify the KMP identifies the methods for protecting CAKs from unauthorized disclosure while being distributed and at any time while exported from MACsec Devices, and confirm the policies and procedures are followed. (MSC-KM-79, MSC-KM-80, MSC-KM-85, MSC-KM-86)
  - m) If PEKs are used to protect CAKs, confirm that PEKs are 256 bits and are protected to the same classification as the CAKs being encrypted. (MSC-KM-81, MSC-KM-82)
  - n) Confirm that CAKs are only used with the MACsec protocol. (MSC-KM-83)
  - o) Confirm the KMP states that compromised CAKs and PEKs are never to be used in the MSC Solution. (MSC-KM-87)
- 2) Perform the following to validate the updating of CAKs and PEKs:
- a) Verify the KMP states that the same CAK may only be used by a pair of MACsec Devices establishing an encrypted tunnel. (MSC-KM-88)
  - b) Log into a MACsec Device and verify the CAK is set to expire in 30 days. (MSC-KM-89)
  - c) Repeat Step 2a for every MACsec Device.
  - d) Verify that the KMP states how often PEKs are to be updated and confirm the process and procedures are followed. (MSC-KM-90)
- 3) Perform the following to validate CAK compromise and recovery:
- a) Confirm the KMP documents the CAK/PEK compromise recovery process, including removal of compromised MACsec Devices and re-establishing MACsec Devices after its CAK is compromised. (MSC-KM-91)
  - b) Confirm the KMP documents accounting procedures to support CAK and PEK compromise recovery. (MSC-KM-92)



# Multi-Site Connectivity Capability Package



- c) Confirm the KMP documents procedures for compromise notification and reporting. (MSC-KM-94, MSC-KM-95)

## Expected Results:

KGCs, CAKs and PEKs are correctly deployed and in compliance with requirements in this CP.

## 15.11 GRAY NETWORK FIREWALL

This section contains procedures for ensuring that the placement of Gray Network Firewalls within the solution comply with the requirements of this CP.

### 15.11.1 GRAY NETWORK FIREWALL FILTERING RULES

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only encrypted traffic allowed through the firewall is between Inner Encryption Components that are allowed to establish encryption tunnels with one another.

**Requirements being tested:** MSC-AU-10, MSC-FW-1, MSC-FW-6, MSC-FW-9

## Procedure Description:

- 1) For each Inner Encryption Component within the solution (hereafter referred to as Inner Encryption Component A):
  - a) For each other Inner Encryption Component within the solution that protects a Red network of the same security level:
    - i) Attempt to establish an IPsec/MACsec connection to it from Inner Encryption Component A.
    - ii) Verify that the IPsec/MACsec connection was established. (MSC-FW-1, MSC-FW-6)
  - b) For each Inner Encryption Component within the solution that protects a Red network of a different security level (hereafter referred to as Inner Encryption Component B):
    - i) Identify the first Gray Network Firewall on the physical path from Inner Encryption Component A and Inner Encryption Component B. If no such Firewall exists, skip the remainder of Step 1(b).
    - ii) Place a packet sniffer on the interface of the Gray Network Firewall facing Inner Encryption Component B.
    - iii) Attempt to establish an IPsec VPN connection from Inner Encryption Component A to Inner Encryption Component B.
    - iv) Verify that the IPsec/MACsec connection was not established.



# Multi-Site Connectivity Capability Package



- v) Verify that the packet sniffer did not record any IKE, IPsec, EAP-TLS or MACsec packets with a source address of Inner Encryption Component A and a destination address of Inner Encryption Component B. (MSC-FW-9)
- vi) Verify that the Gray Network Firewall logs contain an event for an IKE, IPsec, EAP-TLS or MACsec packet with a source address of Inner Encryption Component A and a destination address of Inner Encryption Component B. (MSC-AU-10)

## Expected Result:

In Step 1(a), the Gray Network Firewall allows IKE, IPsec, EAP-TLS, and MACsec traffic between pairs of Inner Encryption Component that are allowed to establish encryption tunnels with one another. In Step 1(b), the Gray Network Firewall denies IKE, IPsec, EAP-TLS, and MACsec traffic between pairs of Inner Encryption Component that protect Red networks of different classification levels.

### 15.11.2 GRAY NETWORK FIREWALL HTTP FILTERING RULES

This section contains a procedure for ensuring that the filtering rules on Gray Network Firewalls are configured so that the only HTTP traffic allowed through the firewall is from an Inner VPN Gateway to an Inner CDP.

**Requirements being tested:** MSC-AU-10, MSC-FW-2, MSC-FW-9

## Procedure Description:

- 1) For each Inner VPN Gateway within the solution:
  - a) For each Inner CDP within the solution:
    - i) Attempt to have the Inner VPN Gateway download the current CRL from an Inner CDP.
    - ii) Verify that the download was successful. (MSC-FW-2)
    - iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).
    - iv) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Gateway.
    - v) From the Inner CDP, attempt to make an HTTP request to the Inner VPN Gateway.
    - vi) Verify that the request failed.
    - vii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (MSC-FW-9)



# Multi-Site Connectivity Capability Package



- viii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (MSC-AU-10)
- b) For every other device on the Gray network that is not an Inner CDP:
  - i) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the other device. If no such Gray Network Firewall exists, skip the remainder of Step 1(b).
  - ii) Place a packet sniffer to the interface of the Gray Network Firewall facing the other device.
  - iii) Attempt to have the Inner VPN Gateway download a CRL from the other device.
  - iv) Verify that the download failed.
  - v) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the other device. (MSC-FW-8)
  - vi) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the Inner VPN Gateway and a destination address of the other device. (MSC-AU-10)

## Expected Results:

In Step 1(a), the Gray Network Firewall allows HTTP requests from the Inner VPN Gateway to the Inner CDP, but not from the Inner CDP to the Inner VPN Gateway. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Gateway to devices that are not Inner CDPs.

### 15.11.3 GRAY NETWORK FIREWALL MANAGEMENT

This section contains a procedure for ensuring that Gray Network Firewalls can only be managed from the Administration Workstation on the Gray Management network.

**Requirements being tested:** MSC-AU-10, MSC-FW-5

## Procedure Description:

- 1) For each Gray Network Firewall within the solution:
  - a) From the Administration Workstation on the Gray Management network, attempt to connect to the Gray Network Firewall's remote management interface.
  - b) Verify that the connection attempt was successful. (MSC-FW-5)
  - c) For each physical network interface on the Gray Network Firewall except the one through which the Administration Workstation connects:



# Multi-Site Connectivity Capability Package



- i) From a device reachable from the physical network interface, attempt to connect to the Gray Network Firewall's remote management interface.
- ii) Verify that the connection attempt failed. (MSC-FW-5)
- iii) Verify that the Gray Network Firewall logs contain an event for a packet with a source address of the selected device and a destination address of the Gray Network Firewall. (MSC-AU-10)

## Expected Results:

In Step 1(b), the Gray Network Firewall allows management traffic from the Administration Workstation. In Step 1(c), the Gray Network Firewall blocks attempts to access the management interface through other physical network interfaces.

### 15.11.4 GRAY NETWORK FIREWALL ADDRESS SPOOFING

This section contains a procedure for ensuring that Gray Network Firewalls detect spoofing of source addresses in traffic sent through it.

**Requirements being tested:** MSC-AU-10, MSC-FW-7

## Procedure Description:

- 1) For each Gray Network Firewall within the solution:
  - a) For each physical network interface on the Gray Network Firewall:
    - i) Select a device on the network connected to that interface of the Gray Network Firewall. Hereafter the device will be called Device A.
    - ii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to. Hereafter the device will be called Device B.
    - iii) Select a device on the network connected to an interface of the Gray Network Firewall that Device A is not connected to, and that Device B is allowed to communicate with. Hereafter the device will be called Device C.
  - iv) Place a network sniffer between the Gray Network Firewall and Device C.
  - v) Configure Device A to use the IP address of Device B.
  - vi) Attempt to send traffic from Device A (spoofing Device B's IP address) to Device C, of a type that Device B is allowed to send to Device C.



# Multi-Site Connectivity Capability Package



- vii) Verify that the packet sniffer did not observe any packets with a source address of Device B and a destination address of Device C. (MSC-FW-7)
- viii) Verify that the Gray Network Firewall logs contain an event for a packet received on the physical interface through which Device A connects, with a source address of Device B and a destination address of Device C. (MSC-AU-10)

## Expected Results:

Each Gray Network Firewall detects the use of spoofed addresses and does not allow packets with spoofed source addresses from passing through, even if non-spoofed traffic from that source address would be allowed.

### 15.11.5 GRAY NETWORK FIREWALL HTTP DEEP PACKET INSPECTION

This section contains a procedure for ensuring that the deep packet inspection performed by the Gray Network Firewalls is configured so only the specific types of HTTP traffic desired between Inner VPN Gateways and Inner CDPs is allowed.

**Requirements being tested:** MSC-AU-10, MSC-FW-3, MSC-FW-4, MSC-FW-9

## Procedure Description:

- 1) For each Inner VPN Gateway within the solution:
  - a) For each Inner CDP within the solution:
    - i) Attempt to have the Inner VPN Gateway download the current CRL from the Inner CDP.
    - ii) Verify that the download was successful. (MSC-FW-3, MSC-FW-4)
    - iii) Identify the first Gray Network Firewall on the physical path from the Inner VPN Gateway to the Inner CDP. If no such Gray Network Firewall exists, skip the remainder of Step 1(a).
    - iv) Replace the CRL on the Inner CDP with a text file.
    - v) Place a packet sniffer on the interface of the Gray Network Firewall facing the Inner VPN Gateway.
    - vi) Attempt to have the Inner VPN Gateway download the current CRL from the Inner CDP.
    - vii) Verify that the request failed.
    - viii) Verify that the packet sniffer did not record any packets with a source address of the Inner CDP and a destination address of the Inner VPN Gateway that contains an HTTP response payload. (MSC-FW-4)



# Multi-Site Connectivity Capability Package



- ix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP response payload with a source address of the Inner CDP and a destination address of the Inner VPN Gateway. (MSC-AU-10)
  - x) Restore the CRL on the Inner CDP.
  - xi) Move the packet sniffer to the interface of the Gray Network Firewall facing the Inner CDP.
  - xii) Attempt to have the Inner VPN Gateway download a CRL from the Inner CDP using an incorrect URL.
  - xiii) Verify that the request failed.
  - xiv) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (MSC-FW-3)
  - xv) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (MSC-AU-10)
  - xvi) Attempt to have the Inner VPN Gateway issue an HTTP POST request for the URL of the CRL on the Inner CDP.
  - xvii) Verify that the request failed.
  - xviii) Verify that the packet sniffer did not record any packets with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (MSC-FW-3)
  - xix) Verify that the Gray Network Firewall logs contain an event for an improper HTTP request with a source address of the Inner VPN Gateway and a destination address of the Inner CDP. (MSC-AU-10)
- b) For every other device on the Gray network that is not an Inner CDP, follow the procedure for Step 1(b). (MSC-AU-10, MSC-FW-9)

## Expected Results:

In Step 1(a), the Gray Network Firewall allows only HTTP traffic between the Inner VPN Gateway and Inner CDP that consists of a GET request for the appropriate CRL and a response containing the CRL. In Step 1(b), the Gray Network Firewall denies HTTP requests from the Inner VPN Gateway to devices that are not Inner CDPs.



# Multi-Site Connectivity Capability Package



## 15.12 INCIDENT REPORTING GUIDANCE

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

**Requirements being tested:** MSC-RP-1 through MSC-RP-14

### Procedure Description:

- 1) Verify the procedures given in MSC-RP-1 through MSC-RP-14 were/are followed and are currently in place.

### Expected Results:

For Step 1, all of these procedures have been followed or are in place.

## 15.13 IMPLEMENTATION OF GUIDANCE

This section ensures there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the MSC Solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in this CP.

**Requirements being tested:** MSC-GD-1 through MSC-GD-35, MSC-SR-10

### Procedure Description:

- 1) Verify the procedures for obtaining virus signature updates as required by local agency policy and the AO were/are followed and/or are in place. (MSC-SR-10)
- 2) Verify the procedures given in MSC-GD-1 through MSC-GD-4, and MSC-GD-13 through MSC-GD-25 were/are followed and/or are currently in place.
- 3) Verify the solution owner understands that he/she shall allow and fully cooperate with an NSA-ordered IA compliance audit of this solution implementation. (MSC-GD-5)
- 4) Verify the solution owner and AO are aware that a compliance audit will be conducted every year. (MSC-GD-6)
- 5) Verify the AO is aware that they shall receive the results of the compliance audit and are responsible for reviewing the completed audit. (MSC-GD-7)
- 6) Verify the customer is aware that when they are interested in registering their solution against this CP, that NSA must grant them an approval prior to the AO authorizing the solution for operation. (MSC-GD-8)



# Multi-Site Connectivity Capability Package



- 7) Verify the customer completes and submits the compliance matrix to the AO. (MSC-GD-9)
- 8) Verify the customer is aware that registration and re-registration against this CP includes submission of CP registration forms and compliance matrix to NSA. (MSC-GD-10)
- 9) Verify the solution owner and AO are aware that when new versions of the MSC CP are published by NSA they will have 6 months to bring their solution into compliance with the new version. (MSC-GD-11)
- 10) Verify the solution owner and AO are aware that they shall provide updated solution information to NSA on a yearly basis. (MSC-GD-12)
- 11) Verify the personnel requirements given in MSC-GD-26 through MSC-GD-35 are met by the personnel supporting this implementation of the MSC Solution.

## **Expected Result:**

For Steps 1-10, all of these procedures have been followed or are in place. For Step 11, assigned personnel meet the stated personnel requirements.

## **15.14 SOLUTION FUNCTIONALITY**

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

**Requirements being tested:** MSC-TR-1

### **Procedure Description:**

- 1) The implementing organization's AO will inspect the test report to ensure all testing requirements have been met. (MSC-TR-1)

### **Expected Result:**

The report will ensure the implementing organization complies with this CP.



# Multi-Site Connectivity Capability Package



## APPENDIX A. GLOSSARY OF TERMS

---

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

**Assurance** – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (CNSSI 4009)

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

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

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

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

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

**Capability Package** – 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. This package will point to potential products that can be used as part of this solution.

**Central Management Site** – A site within a MSC Solution that is responsible for remotely managing the Solution Components located at other sites.

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



# Multi-Site Connectivity Capability Package



**Certification and Accreditation (C&A)** – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

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

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

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

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

**Control Plane Protocol** – A routing, signaling, or similar protocol whose endpoints are network infrastructure devices such as VPN Gateways or routers. Control plane protocols carry neither user data nor management traffic.

**CRL Distribution Point (CDP)** – A web server that hosts a copy of a CRL issued by a CA for VPN Gateways to download.

**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]

**Data Plane Protocol** – A protocol that carries the data being transferred through the solution.

**Encryption Component** – Either a VPN Gateway or a MACsec Device.



# Multi-Site Connectivity Capability Package



**External Interface** – The interface on an Encryption Component that connects to the outer network (i.e., the Gray network on the Inner Encryption Component or the Black network on the Outer Encryption Component).

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

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

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

**Gray Network Firewall** – A stateful traffic filtering firewall placed on the Gray network to provide additional separation between flows of singly-encrypted data of different classification levels.

**Independently Managed Site** – A site within a MSC Solution whose Solution Components are locally managed and that does not remotely manage other sites' Solution Components.

**Internal Interface** – The interface on an Encryption Component that connects to the inner network (i.e., the Gray network on the Outer Encryption Component or the Red network on the Inner Encryption Component).

**Locally Managed Device** – A device that is being managed by the direct connection of the Administration Workstation to the device in a hardwired fashion (such as a console cable).

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

**Management Plane Protocol** – A protocol that carries either traffic between a system administrator and a component being managed, or log messages from a Solution Component to a log server or similar repository.

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

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

**Red Network** – A network that contains unencrypted classified data.



# Multi-Site Connectivity Capability Package



**Remotely Managed Device** – A device that is being managed by any other method besides that given in the definition of a Locally Managed Device.

**Remote Site** – A site within a MSC Solution whose Solution Components are remotely managed by a Central Management Site.

**Security Level** – The combination of classification level, list of compartments, dissemination controls, and other controls applied to the information within a network.



# Multi-Site Connectivity Capability Package



## APPENDIX B. ACRONYMS

Acronym	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AM	Advisory Memorandum
AO	Authorizing Official
ARP	Address Resolution Protocol
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
C&A	Certification and Accreditation
CA	Certificate Authority
CAA	Certificate Authority Administrator
CAK	Connectivity Association Key
CAKA	Connectivity Association Key Administrator
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CKN	Connectivity Association Key Name
CMAC	Cipher-based Message Authentication Code
CNSA	Commercial National Security Algorithm [Suite]
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Capability Package
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
DDoS	Distributed Denial of Service
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DM	Device Management
DNS	Domain Name System
DoD	Department of Defense
DoS	Denial of Service
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EoMPLS	Ethernet over Multiprotocol Label Switching



# Multi-Site Connectivity Capability Package



Acronym	Definition
ESP	Encapsulating Security Payload
EST	Enrollment Over Secure Transport
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GOTS	Government Off-the-Shelf
GRE	Generic Routing Encapsulation
HMAC	Host-based Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alerts
IC	Intelligence Community
ICD	Intelligence Community Directive
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
JIMS	Joint Incident Management System
KGC	Key Generation Component
KM	Key Management
KMI	Key Management Infrastructure
L2TPv3	Layer 2 Tunneling Protocol Version 3
MACsec	Media Access Control Security
MGC	Management Client
MSC	Multi-Site Connectivity
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency



# Multi-Site Connectivity Capability Package



Acronym	Definition
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit
PSK	Pre-Shared Key
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request for Comment
RIP	Routing Information Protocol
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SA	Security Association
SAK	Secure Association Key
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIPRNet	Secret Internet Protocol Router Network
SP	Service Packs
SSH	Secure Shell
SSHv2	Secure Shell Version 2
T	Threshold
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TFFW	Traffic Filtering Firewall
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
XPN	eXtended Packet Number



# Multi-Site Connectivity Capability Package



## APPENDIX C. REFERENCES

---

CNSSI 1300	<i>CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy</i>	December 2014
CNSSI 4009	<i>CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.</i> <a href="http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf">http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf</a>	April 2015
CNSSP 11	<i>CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products.</i>	June 2013
CNSSP 15	<i>CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems</i>	October 2012
CNSS AM IA 02-15	<i>Use of Public Standards for the Secure Sharing of Information Among National Security Systems</i>	July 2015
CNSSD 505	<i>CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)</i>	March 2012
FIPS 140-2	<i>Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication</i> <a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a>	May 2001
FIPS 180-4	<i>Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)</i>	August 2015
FIPS 186	<i>Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)</i>	July 2013
FIPS 197	<i>Federal Information Processing Standard 197, Advanced Encryption Standard (AES)</i>	November 2001
FIPS 201-1	<i>Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication</i> <a href="http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf">http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf</a>	June 2006
RFC 2409	<i>IETF RFC 2409 The Internet Key Exchange (IKE). D. Harkins and D. Carrel.</i>	November 1998
RFC 3647	<i>IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force</i>	November 2003
RFC 4252	<i>IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol. T. Ylonen and C. Lonvick.</i>	January 2006
RFC 4253	<i>IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol. T. Ylonen and C. Lonvick.</i>	January 2006



# Multi-Site Connectivity Capability Package



RFC 4254	<i>IETF RFC 4254 The Secure Shell (SSH) Connection Protocol.</i> T. Ylonen and C. Lonvick.	January 2006
RFC 4256	<i>IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH).</i> F. Cusack and M. Forssen.	January 2006
RFC 4302	<i>IETF RFC 4302 IP Authentication Header.</i> S. Kent	December 2005
RFC 4303	<i>IETF RFC 4303 IP Encapsulating Security Payload.</i> S. Kent	December 2005
RFC 4307	<i>IETF RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).</i> J. Schiller	December 2005
RFC 4308	<i>IETF RFC 4308 Cryptographic Suites for IPsec.</i> P. Hoffman	December 2005
RFC 4754	<i>IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA).</i> D. Fu and J. Solinas.	January 2007
RFC 5246	<i>IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2.</i> T. Dierks and E. Rescorla.	August 2008
RFC 5280	<i>IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> D. Cooper, et. al.	May 2008
RFC 5759	<i>IETF RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile.</i> J. Solinas and L. Ziegler.	January 2010
RFC 5996	<i>IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2).</i> C. Kaufman, et. al.	September 2010
RFC 6239	<i>IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH).</i> K. Igoe.	May 2011
RFC 6379	<i>IETF RFC 6379 Suite B Cryptographic Suites for IPsec.</i> L. Law and J. Solinas.	October 2011
RFC 6380	<i>IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec).</i> K. Burgin and M. Peck.	October 2011
RFC 6460	<i>IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS).</i> M. Salter and R. Housley.	January 2012
RFC 6818	<i>IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.</i> P. Yee	January 2013
RFC 7030	<i>IETF RFC 7030 Enrollment over Secure Transport.</i> M. Pritikin, P. Yee, and D. Harkins.	October 2013
SP 800-53	<i>NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations.</i> Joint Task Force Transformation Initiative.	May 2013
SP 800-56A	<i>NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.</i> E. Barker, et. al.	May 2013



# Multi-Site Connectivity Capability Package



SP 800-56B	<i>NIST Special Publication 800-56B Rev. 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography.</i> E. Barker, et. al.	October 2014
SP 800-56C	<i>NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion.</i> L. Chen.	November 2011
SP 800-131A	<i>NIST Special Publication 800-131A Rev. 1, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths.</i> E. Barker.	November 2015
SP 800-147	<i>NIST Special Publication 800-147, BIOS Protection Guidelines.</i> D. Cooper, et. al.	June 2011