


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Wireless Intrusion Detection System/Wireless Intrusion Prevention System (WIDS/WIPS) Annex V1.0

Version 1.0
2 February 2021


CHANGE HISTORY

Title	Version	Date	Change Summary
Commercial Solutions for Classified (CSfC) Wireless Intrusion Detection System (WIDS)/ Wireless Intrusion Prevention System (WIPS)	0.8	September 2019	Initial release of WIDS/WIPS Annex for public comment.
Commercial Solutions for Classified (CSfC) Wireless Intrusion Detection System (WIDS)/ Wireless Intrusion Prevention System (WIPS)	1.0	2 February 2021	Release of WIDS/WIPS Annex.

Table of Contents

Table of Figures

List of Tables

1 INTRODUCTION

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

CSD is delivering the Wireless Intrusion Detection System (WIDS)/Wireless Intrusion Prevention System (WIPS) Annex to meet the demand for commercial monitoring and protection of wireless 802.11 End User Devices (EUD) (e.g., tablets, smartphones, and laptop computers) accessing secure enterprise services over a campus wireless network or authorized wireless deployment. In addition to the WIDS/WIPS Annex requirements for CSfC cryptographic solutions, CSfC provides additional guidance for U.S. Government customers to deploy WIDS/WIPS solutions for monitoring controlled spaces, even in the absence of a CSfC cryptographic solution (See Appendix A). Cryptographic algorithms, known as Commercial National Security Algorithms (CNSA), are used to protect classified data using products in a dual layered approach. This Annex builds on lessons learned from three proof-of-concept demonstrations, implemented through layered use of COTS products for the protection of classified information.

2 PURPOSE AND USE

This Annex provides reference architecture and corresponding configuration information that allows customers to select COTS products from the CSfC Components List to develop a WIDS/WIPS solution and then properly configure those products to achieve a level of assurance sufficient for a solution used to protect classified Data-in-Transit (DIT). Throughout this document, requirements imposed on the WIDS/WIPS implementation are identified by a label consisting of the prefix “WIDS,” a two-letter category, and a sequence number (e.g., WIDS-GR-11). To successfully implement a solution based on this Annex, all Threshold (T) requirements, or the corresponding Objective (O) requirements, must be implemented as described in Section 9.1.

Customers who want to use this Annex must register their solution with NSA. Additional information about the CSfC process is available on the CSfC web page (http://www.nsa.gov/resources/everyone/csfc/). Customers using the guidance presented in Appendix A for deployment of a WIDS/WIPS solution in the absence of CSfC cryptographic solution are not required to register their solution with the NSA.

The WIDS/WIPS Annex Version 1.0, when approved by the Deputy National Manager (D/NM) for National Security Systems, will be reviewed twice a year to ensure that the defined capabilities and other instructions still provide the security services and robustness required to account for technology development, new security issues, and new use cases. Solutions designed using this Annex must be registered with NSA/CSD. Once registered, a signed CSD Approval Letter will be sent validating that the WIDS/WIPS solution is registered as a CSfC solution validated to meet the requirements of the latest WIDS/WIPS Annex and is approved to protect classified information. Any solution designed according to this Annex may be used for one year and must then be revalidated against the most current published

version of this Annex. Top Secret Solutions will be considered on a case-by-case basis. Customers are encouraged to engage their Client Advocate or the CSfC Program Management Office team early in the process to ensure the solutions are properly scoped, vetted, and that the customers have an understanding of risks and available mitigations.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/CSS Client Advocate and the WIDS/WIPS Annex maintenance team at **CSFC_WIDS_team@nsa.gov**.

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),* identifies 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)

WIDS/WIPS solutions must comply with the Committee on National Security Systems (CNSS) policies and instructions. Any conflicts identified between this Annex and NSS or local policy should be provided to the WIDS/WIPS Maintenance team. If a conflict arises between NSS, local policy, and this Annex, NSS and/or local policy should be followed until a time when the WIDS/WIPS Maintenance team rectifies the conflict.

3 LEGAL DISCLAIMER

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

The user of this Annex agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

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

4 OVERVIEW

A WIDS consists of sensors (preferably dedicated) and a central controller working together to provide 24/7 monitoring, primarily to the 802.11 Wireless Local Area Network (WLAN) spectrum and protocol, to detect, identify, and geo-locate WLAN devices within the controlled space. A WIDS is vital for the security of a WLAN Access System deployed within a controlled space. A WIDS may be used to monitor controlled space without a CSfC WLAN Access System, this case is outside the scope of the CSfC guidance (for additional guidance see Appendix A). The WIDS may be capable of detecting or monitoring traffic of additional protocols other than 802.11 WLAN such as 802.15.4 based protocols, which enhances the security of the controlled space. However, a WIDS is not required to monitor additional protocols outside of 802.11 when supporting a WLAN Access Solution. A WIDS monitors all 802.11 WLAN traffic emanating from and traversing the controlled space, thus inadvertent collection of any 802.11 signals is possible when operating a WIDS.

A WIPS consists of sensors (preferably dedicated), and a central controller working together to provide 24/7 active defense of an authorized wireless network by preventing unauthorized connection. A WIDS may have the capability of a WIPS or a separate WIPS can be deployed if the chosen WIDS does not have the WIPS capability. Currently, a WIPS is an optional capability that may be deployed with a CSfC solution at the discretion of the Authorizing Official (AO). A WIPS has the capability to actively protect a WLAN by restricting unauthorized WLAN devices from connecting to authorized WLAN devices within controlled spaces; defending authorized WLAN networks from any attempted attacks with the goal of disrupting, degrading or connecting to an authorized WLAN networks. WIPSs are capable of causing Distributed Denial-of-Service (DDoS) against 802.11 clients within their controlled space. The capabilities of both WIDS and the WIPS must be considered by the AO when deploying WIPS. For defensive purposes, the AO should seek additional guidance from their relevant decision making bodies regarding inadvertent collection of signals and potential DDoS of wireless clients within their controlled space when deploying a WIDS and/or WIPS solution.

A CSfC solution requires a WIDS only if there is a static WLAN Access System within the CSfC solution such as within the Campus WLAN CP or the Mobile Access (MA) CP using the government private wireless use case. Deploying a WIDS/WIPS within a CSfC solution requires that the WIDS/WIPS be selected from the CSfC Components List and must be configured to use the National Information Assurance Partnership (NIAP) - evaluated configuration. A WIDS/WIPS within a CSfC solution may be deployed in several different configurations, contingent on the CSfC deployment architecture, type of WIDS/WIPS deployed and AO decision. These configurations include being integrated into the WLAN Access System and Overlay deployments for the WIDS/WIPS.

5 DEPLOYMENT ARCHITECTURE

A WIDS is required if a WLAN Access System is used within the solution, either in accordance with (IAW) the Campus WLAN CP or a static MA CP using government private wireless use case within a controlled space. The WIDS/WIPS must be selected from the CSfC Components List and must be configured to use the NIAP-evaluated configuration. A long-term (over 6 months) deployment of a Campus WLAN solution will always require a WIDS to monitor its WLAN Access System and clients as part of its Continuous Monitoring (CM) solution. An MA solution only requires a WIDS if it is a long-term (over 3 months) static

deployment which uses a WLAN Access System within a controlled space to access its Outer Encryption Components IAW MA CP's government private wireless use case. For more information and guidance on the deployment of a Campus WLAN solution or Mobile Access solution, see the relevant CPs located on the CSfC website at https://www.nsa.gov/resources/everyone/csfc).

5.1 WIDS/WIPS Deployments

A WIDS/WIPS deployed to support a CSfC solution can be arranged in multiple configurations which include a WIDS/WIPS integrated into WLAN Access Systems, an Overlay WIDS/WIPS within a CSfC network, or an Overlay WIDS/WIPS outside of the CSfC network. When a WIDS/WIPS is integrated into a WLAN Access System, the WLAN Access System must have the capability to act as an authorized WIDS/WIPS. This integrated solution has the benefit of reducing the number of required components and complexity of the WIDS/WIPS. If the WLAN Access System cannot act as a WIDS/WIPS, an overlay WIDS/WIPS must be used to monitor of the WLAN Access System. WIDS/WIPS sensors can be deployed on the same network as the WLAN Access System's Access Points (APs) if the WIDS/WIPS is integrated into the WLAN Access System. However, if the WIDS/WIPS is an Overlay then the WIDS/WIPS sensors must be on a separate network.

5.1.1 Integrated WIDS/WIPS Deployments

Figure 1 shows a possible configuration where the WIDS/WIPS is deployed integrated into the WLAN Access System within the Campus WLAN CP. This deployment includes the WIDS as part of the WLAN Access System and would be controlled from the Gray Management Network. Both the WLAN APs and WIDS Sensors are part of the Gray Network and must be protected as such.

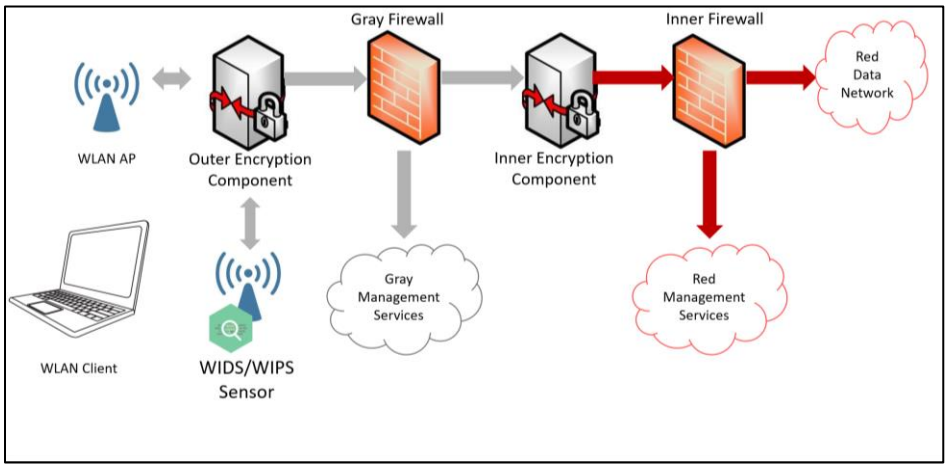

Figure 1. WLAN with Integrated Gray WIDS/WIPS

Figure 2 shows a similar configuration where the WIDS is integrated into the WLAN Access System of the MA CP. This configuration depicts the WIDS/WIPS as a function of the WLAN Access system while being controlled from the Black Management Network. See Section 5.1.3 for information on the deployment of WIDS/WIPS sensors.

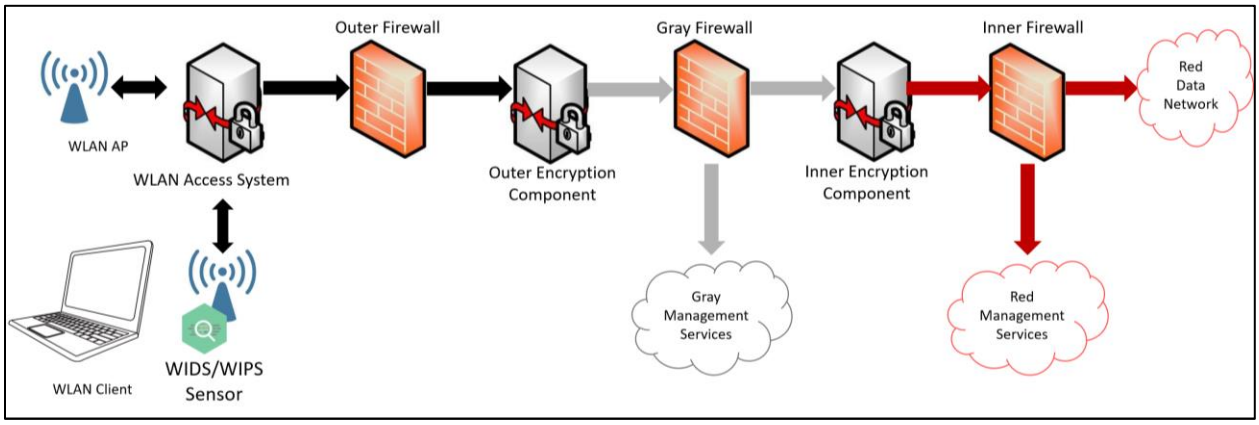

Figure 2: MA with Integrated WIDS/WIPS

Vendors implement encryption differently between the WLAN Client and the WLAN Controller and depending on how this encryption is implemented it changes the way the WIDS/WIPS sensors are handled. One implementation of encryption is where the WLAN AP passes all traffic to the WLAN Controller for decryption. In the Campus WLAN CP, the implementation of the WLAN APs are considered to be part of the Black Network and need to be protected accordingly. As shown in Figure 3, when these WLAN APs are used as WIDS sensors, they too are considered part of the Black Network. The second type of encryption is when the WLAN AP terminates the outer encryption layer. In this case, the WLAN APs are considered to be part of the Gray Network and must be protected accordingly. This is true even if there is a layer of encryption between the WLAN AP and Controller. The determining factor depends where the WLAN Client's Outer encryption terminates. This implementation means that the WLAN AP acting as a WIDS/WIPS sensor, is treated as part of the Gray Network (See Figure 1).

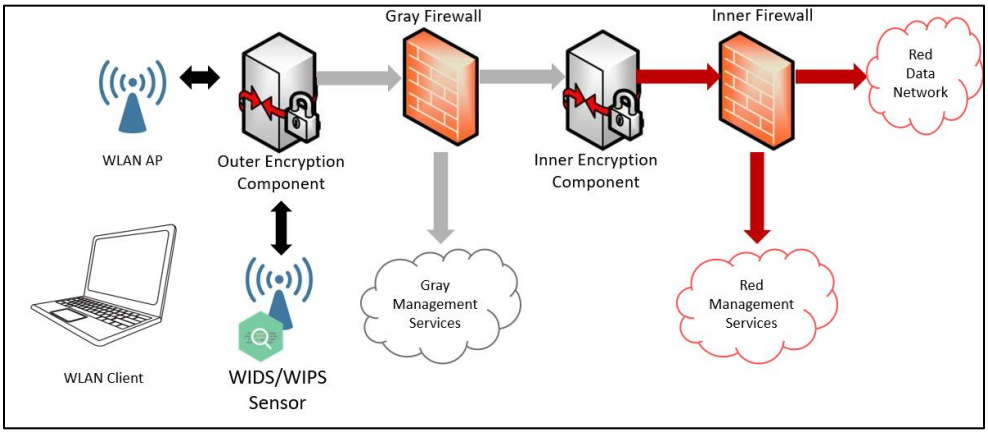

Figure 3: Campus WLAN CP Black Integrated WIDS

5.1.2 Overlay WIDS/WIPS Deployments

A WIDS/WIPS may also be deployed as an Overlay WIDS/WIPS that is not integrated into the WLAN Access System within a Campus WLAN or MA CP. This configuration may be required if the WLAN Access System does not have a WIDS capability or the chosen WIDS/WIPS is not part of a WLAN Access System. In this case, the WIDS/WIPS may reside in either the Black Management, Gray Management, or an independent network outside of the CSfC solution. Additionally, any time an Overlay WIDS/WIPS is used, the WIDS/WIPS controller or controllers must not be directly connected to the Management Network

but instead, must go through a firewall for inspection of allowed traffic and/or blocking of disallowed traffic. When deployed within the Black or Gray Management Network a WIDS/WIPS controller must traverse the associated firewall to access the management network. **Figure 4** Figure 4 shows an MA deployment with an Overlay WIDS/WIPS in the Gray Management and all components of the WIDS/WIPS would reside and be controlled from Gray Management. The WIDS/WIPS in this scenario cannot correlate data with the WLAN Access System, also the WIDS/WIPS Sensors are all considered to be part of the Gray Management Network which will greatly increase both the size and surface of the Gray Management Network. This configuration has the benefit of leveraging the Gray Management services that are already being used and can leverage additional capabilities such as Enterprise Gray (see Section 5.2).

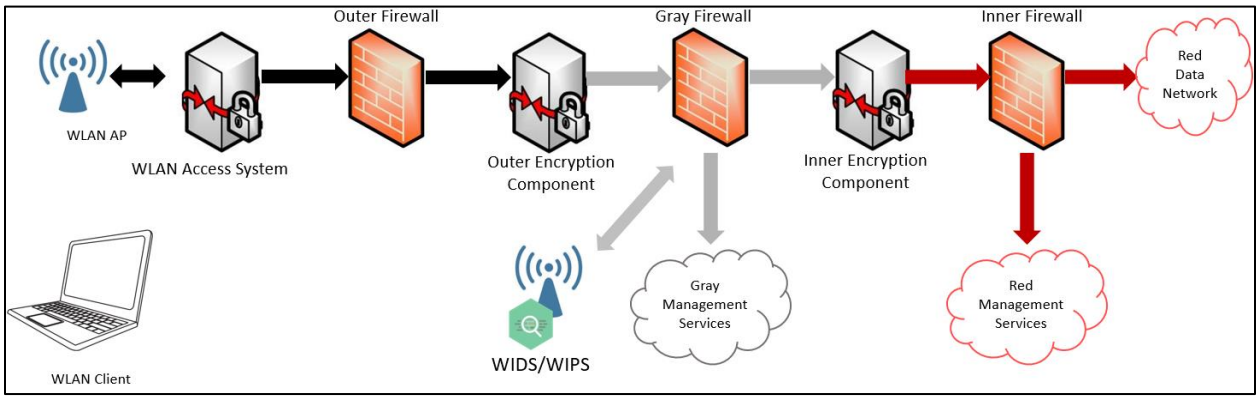

Figure 4: MA with Overlay WIDS/WIPS in Gray Management

Figure 5 shows an MA solution with an Overlay WIDS/WIPS that is part of the Black Management Network. The WIDS/WIPS in this scenario can correlate data with the WLAN Access System. Also, the WIDS/WIPS requires the Black Management Network support the WLAN Access System and the WIDS/WIPS. In this configuration, all the WIDS/WIPS sensors are part of the Black Management Network and must be protected as such.

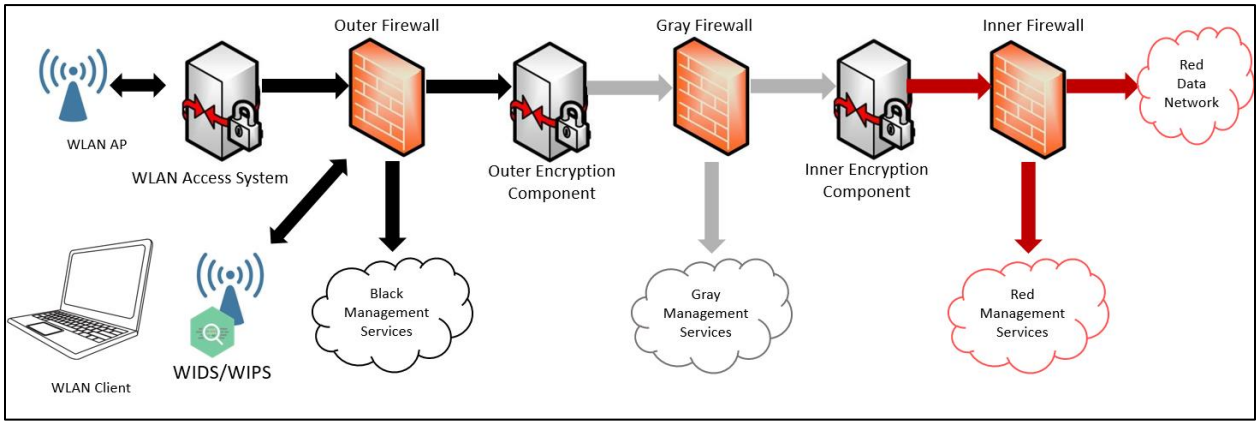

Figure 5: MA with Overlay WIDS/WIPS in Black Management

When a WIDS/WIPS is used within the Campus WLAN CP, it can be deployed within the Gray Management Network, Red Management Network or outside the CSfC solution. Figure 6 shows a WIDS/WIPS controlled and managed within the Gray Management Network. This configuration is similar

to the configuration shown in **Figure 4** with MA and has nearly an identical capability and use except that since the WLAN Access System and WIDS/WIPS are collocated on the same network their data can be correlated between each other.

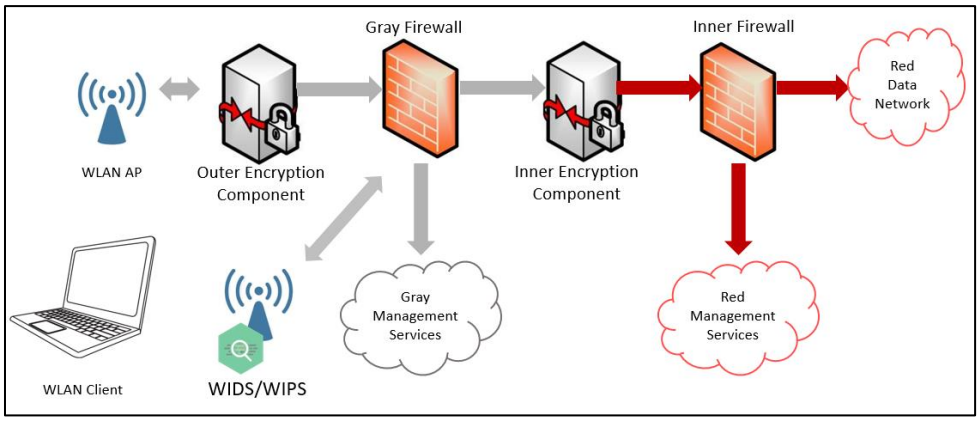

Figure 6: WLAN with Overlay WIDS/WIPS in Gray Management

5.1.3 WIDS/WIPS Sensor Deployments

The deployment of the WIDS/WIPS sensors impacts functionality, security and complexity of the networks. The Overlay WIDS/WIPS and the integrated WIDS/WIPS both have unique concerns which must be addressed when deploying the WIDS/WIPS sensors.

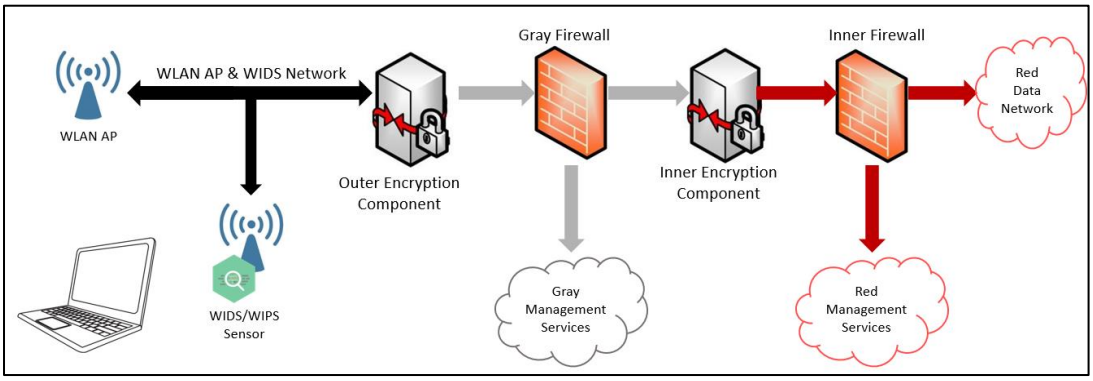

Figure 7: WLAN with Integrated WIDS/WIPS Single Network

As shown in Figure 7, it is preferable to have the WIDS/WIPS sensors on their own network. However, sharing the same network for WIDS/WIPS sensors and WLAN Access System is allowable for both Campus WLAN and MA solutions. Additional measures, such as using a Virtual Local Area Networks (VLANs), should be taken to segregate the WIDS/WIPS sensors and WLAN APs.

As shown in Figure 8, when using an Overlay WIDS/WIPS, it is required that the WIDS/WIPS sensors be deployed on a separate network from the WLAN APs. This ensures that the WIDS/WIPS sensors and controllers do not pose a risk to the network, but at the cost of requiring an entire secondary network for both the APs and WIDS/WIPS sensors monitoring the network. In this case, the WIDS/WIPS can be deployed in the Black Management Network, Gray Management Network, or outside of the CSfC solution, but it is recommended the WIDS/WIPS be co-located with the WLAN Access System so that the

system can be used together to better correlate data between the two. The WIDS/WIPS controller and sensors would be part of the network they are attached to and in Figure 8's example, the WIDS/WIPS sensors and controller would be part of the Gray Management Network.

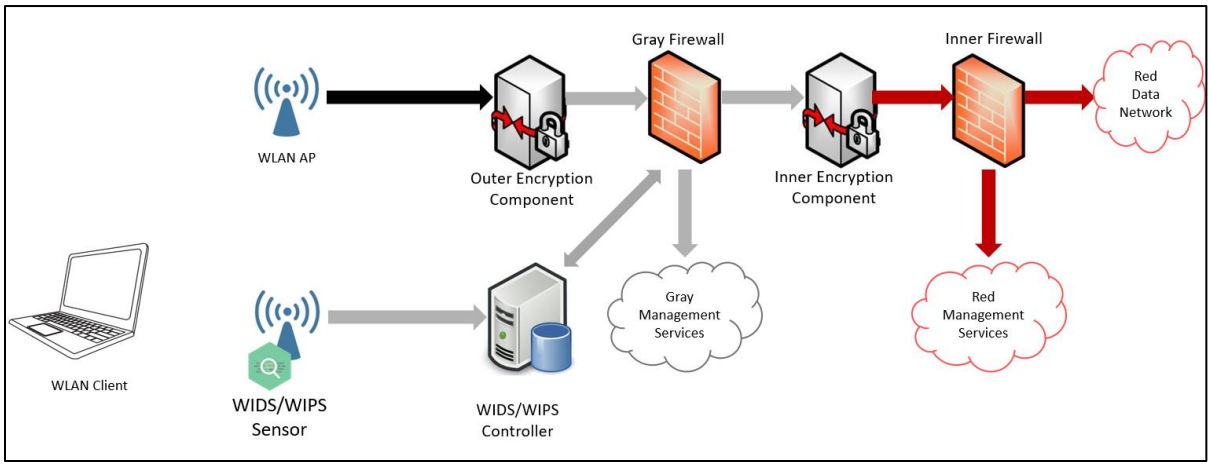

Figure 8: WLAN with Separate WIDS/WIPS Networks

5.2 WIDS/WIPS SECURITY

Security of a deployed WIDS/WIPS is required for management, control, and network functionality of the WIDS/WIPS components. The components that make up a WIDS/WIPS include the WIDS/WIPS sensor, WIDS/WIPS controller, workstation, as well as other supporting components. Communications between the WIDS/WIPS sensors and the WIDS/WIPS controller must use secure communication (e.g., SSHv2, Internet Protocol Security (IPsec), Direct Transport Layer Security (DTLS), or TLS (1.2 or 1.3)/Hypertext Transfer Protocol Secure (HTTPS)) and the communication between the WIDS/WIPS controller, workstation and other supporting components must also use secure communication (e.g., SSHv2, IPsec, DTLS, or TLS (1.2 or 1.3)/HTTPS). All forms of unsecure management, control and sending data must be disabled for each WIDS/WIPS Component.

As shown in Figure 9, a firewall must be in place to block all communications between the WIDS controller and relevant management network. The firewall protects both the management network and the WIDS/WIPS controller by monitoring and controlling all traffic to and from the WIDS/WIPS controller. The firewall must filter all unnecessary protocols from reaching the WIDS/WIPS controller. The protocols that are exempt from being filtered include, but are not limited to, TLS (1.2 or 1.3), SSHv2, IPsec, Network Time Protocol (NTP), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and system log. In addition to the firewall, the WIDS/WIPS controller must be secured to minimize the potential risk to the solution. First, there must be no capability to manage or control the WIDS/WIPS controller from the interfaces that connect to the sensors. Second, there must not be any routing through the WIDS/WIPS controller between the sensors and the Gray Management Network. Finally, the WIDS/WIPS controller must have a management interface used to control, manage, and access Gray Management resources.

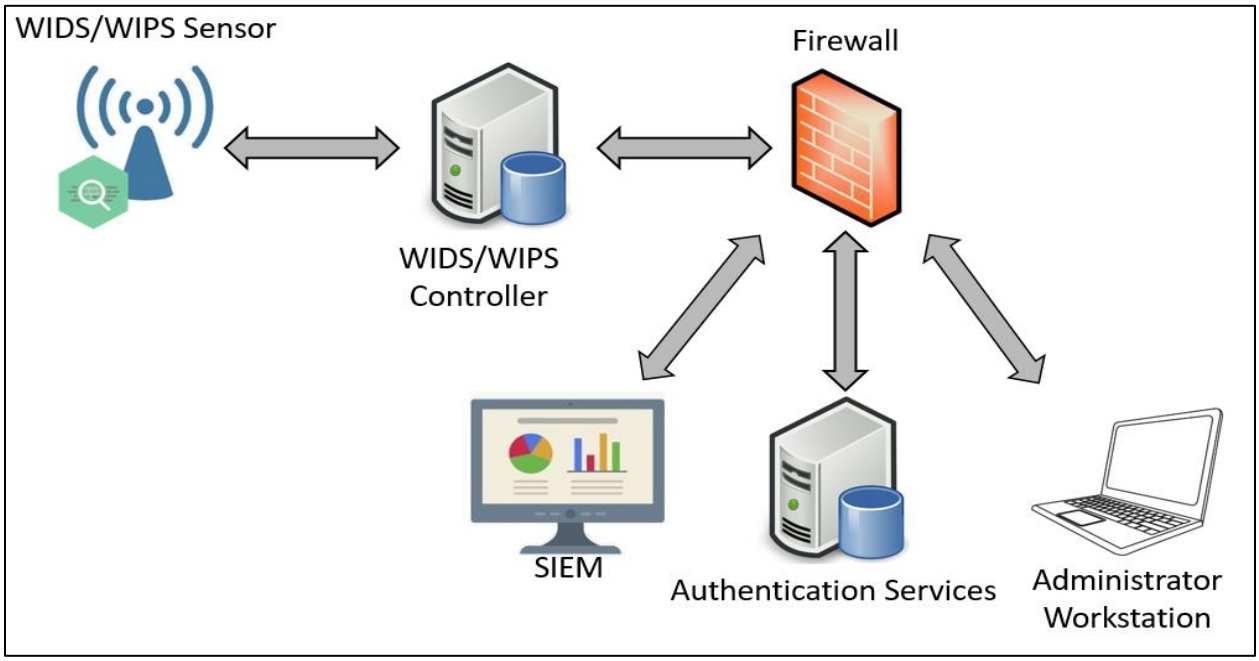

Figure 9: WIDS/WIPS Components

A centralized authentication service is a fundamental base of any network and WIDS/WIPS, even if it does support local account administration. The system must still use an external authentication service such as Remote Authentication Dial in User Service (RADIUS), Active Directory, or Kerberos. The WIDS/WIPS can leverage the same authentication system that is being used by its relevant Management Network. All WIDS/WIPS components must be integrated into the network's existing CM capability such as an Intrusion Detection System (IDS), or Security Information and Event Management (SIEM) thus all WIDS/WIPS components must send all system logs to the solution's CM capability.

If the WIDS/WIPS solution is deployed within the Gray Management Network, it may leverage the capabilities found within the *CSfC Enterprise Gray Implementation Requirements Annex* to allow for secured communications between WIDS/WIPS solutions, sharing of centralized resources, and remote management of the WIDS/WIPS solution. This capability requires that two or more Gray Management Networks be connected using either an additional Gray Encryption Component or capable firewall. For more information about the Enterprise Gray capabilities or requirements see the *CSfC Enterprise Gray Implementation Requirements Annex.*

The system logs that are collected from the WIDS/WIPS component must log any login event and must include any failed login attempts, successful logins, and administrator logins. The system logs must also include any changes to the authentication system that includes creation, deletion, or modification of user accounts and any changes to groups or group membership. The WIDS/WIPS components must log any attempt for escalation of privileges. The WIDS/WIPS components must log when there is any configuration changes and whether they are successful or useful. The WIDS/WIPS controller must also log the status of the WIDS/WIPS sensors and must include when a new sensor is connected, when a sensor is unreachable, and when any sensor has an error status. These system logs monitor the WIDS/WIPS for any possible errors and potential security issues and should be used with additional guidance required for CM within the solution.

5.3 CONTINUOUS MONITORING

When deploying a WIDS/WIPS, logging and notification of the events within the controlled space are required for the proper operations and to maintain security of the controlled space. The WIDS/WIPS must have the capability to create notifications and alerts of events that it detects. The AO may deem it necessary that the alert and notification capabilities of the WIDS/WIPS meet their needs for monitoring. The AO alternatively can integrate the WIDS/WIPS into a CM capability, such as a SIEM or IDS, to notify and alert security administrators of events detected by the WIDS/WIPS. In this case, WIDS/WIPS must be integrated into a CM capability and either send its notifications to a CM capability or send its raw data to a CM capability and have it alert on events. The AO and local policy dictate how often these events, logs and, notifications must be reviewed. It is recommended that the time frame between reviews be no longer than one week.

Either the CM capability, or the WIDS/WIPS interface must filter on notifications based on types, severity and number of notifications received. For additional information on CM within CSfC, see the *CSfC Continuous Monitoring Annex*. As shown in Figure 10, a WIDS/WIPS must be integrated into the solution's CM capability in relation to data processing, alerting, notification and retention. Even if the WIDS/WIPS is used for notifications, all logs from the WIDS/WIPS must be sent to the CM solution for data retention or there must be another system that retains data for the given amount of time. The AO and relevant policy will determine the retention time of this data. It is recommended to keep this data at a minimum of one year.

The interface between the WIDS/WIPS Controller and the Firewall such as the Gray Management Firewall must be monitored as part of the Management Network. All monitoring requirements from the *CSfC Continuous Monitoring Annex* MP6, must be applied to a Gray WIDS/WIPS connection WIDS/WIPS. For a WIDS/WIPS deployed within the Black Network, or a stand-alone network outside of the CSfC network the following must be monitored on the given interface.

The WIDS/WIPS must log and forward to a CM capability the following: any user events, failed login attempt, whenever a new user is created, whenever a user is added to a group, any change is made to group privilege, any user account attribute is changed, and when any authentication rule is created or modified. The firewall providing network access must log any attempts to conduct a network scan from the WIDS/WIPS or any attempts for the network to scan the WIDS/WIPS solution. Additionally, the firewall must alert on any unusual traffic between the WIDS/WIPS controller and the management network. This unusual traffic may include, but is not limited to, attempting to use unauthorized ports or protocols, attempting to contact an IP address outside of the management network, or a large amount of traffic traversing the firewall. The firewall and controller must log if any protocol outside SSH, ESP or TLS is being used to log into the WIDS/WIPS. The firewall must log any DNS queries from the WIDS/WIPS controller to a domain outside of its management network. The WIDS/WIPS Controller needs to log any configuration changes made to it, or its sensors to the networks CM capability. Finally, the WIDS/WIPS controller must have a reoccurring vulnerability scan conducted on it within a time designated by the AO and relevant governing policies.

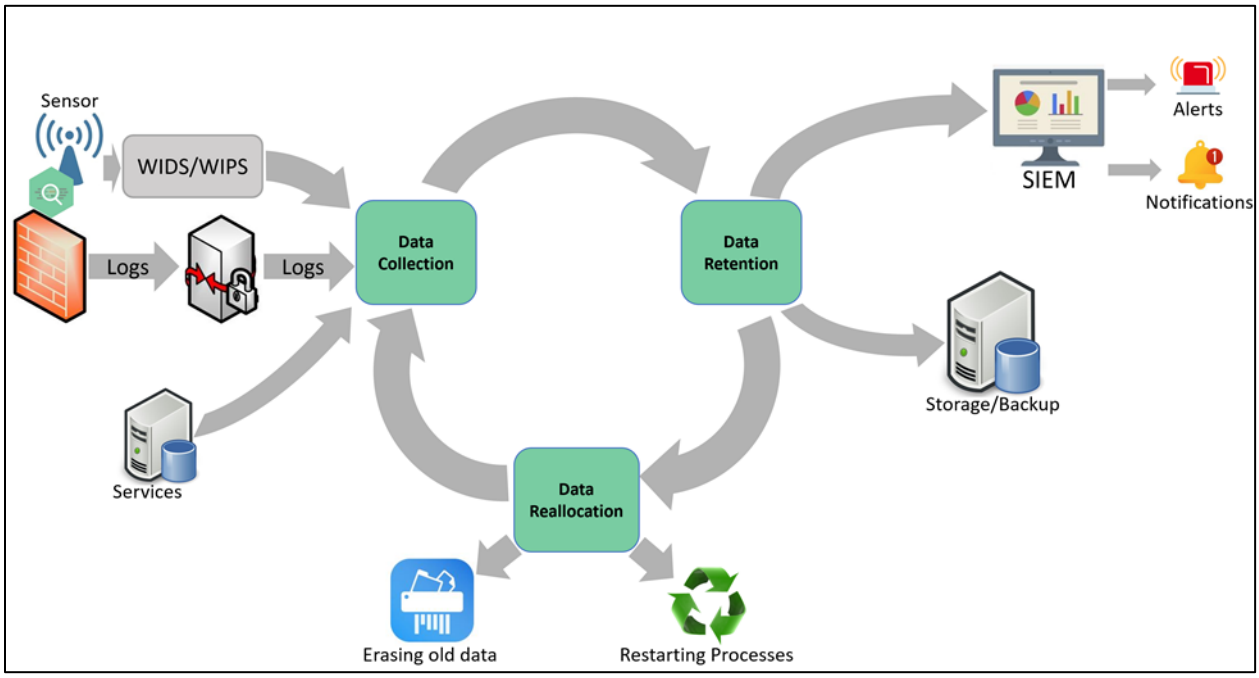

Figure 10: WIDS/WIPS Dataflow Model

6 WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

A WIDS consists of sensors (preferably dedicated), and a central controller working together to provide 24/7 monitoring of the 802.11 WLAN spectrum and protocols. The WIDS identifies unauthorized devices interfering with authorized devices, identifies authorized devices operating outside the 802.11 protocol, configuration parameters, and identifies the physical location of all 802.11 devices within the controlled space. The WIDS may be capable of either detecting or monitoring traffic of additional protocols other than 802.11 WLAN; which greatly enhances the security of the controlled space, however this is not required when supporting a WLAN Access Solution. Additional protocols may include cellular protocols, additional 802.11 protocols, 802.14 protocols, other low latency protocols, and other long range wireless protocols.

IAW the Campus WLAN CP or the MA CP, a WIDS is required in a CSfC deployment if a static WLAN Access System is used within the solution. The WIDS must be selected from the CSfC Components List and must be configured to use the NIAP-evaluated configuration. A long-term deployment of a Campus WLAN solution will always require a WIDS to monitor its WLAN Access System and clients as part of its CM solution. If the Campus WLAN solution uses another transport method other than 802.11 in the 2.4 GHz or 5.0 GHz bands, it is recommended that the WIDS is capable to monitor the chosen protocol. A MA solution only requires a WIDS if it is a long-term deployment using a WLAN Access System within a controlled space to access its Outer Encryption Components. For additional guidance on the deployment of a Campus WLAN, or MA solution, see the applicable CP.

6.1 WLAN DETECTION

WLAN detection for the WIDS only involves the detection of the 802.11 2.4 GHz and 5.0 GHz bands and does not need to include other bands supported by the 802.11 bands. If deemed necessary by the AO, the 3.6 GHz and 60 GHz may be included in the scope of the WIDS system. The WIDS system must monitor 802.11 channels within the 2.4 GHz and 5.0 GHz bands both inside and outside the local country's regulatory domain. The system must also perform protocol analysis of captured signals to detect violations of 802.11 WLAN standards. If a WLAN Access System is monitored, then the WIDS must be able to process 802.11 traffic at the same data rate that the WLAN Access System supports. While in the controlled space, the WIDS must be able to geo-locate all WLAN emitters within the 802.11 2.4 GHz and 5.0 GHz bands. A WIDS may additionally have the capability to geo-locate devices communicated on supported 802.11 protocols to a 5 meter radius.

Table 1. 802.11 Monitoring Protocol

Protocol	Frequencies	Monitoring
802.11 b/g/n/ax Wi-Fi	2.4 GHz	Required
802.11 a/n/ac/ax Wi-Fi	5.0 GHz	Required
802.11	6.0 GHz	Optional
802.11 y	3.6 GHz	Optional
802.11 ad/ay WiGig	60 GHz	Optional

The system must be configured to detect when 802.11 WLAN emitters within the controlled space acts maliciously or anomalously. Users must be able to create custom attack signatures to aid in the monitoring of the network and controlled space. A WLAN Access System baseline must be created with the WIDS and this baseline must be used comparatively to detect anomalies that deviate from the created baseline. The events that should be used to detect anomalies and malicious traffic include, but not limited to, WLAN bridges, Denial-of-Service (DoS) attacks, and WLAN emitters working outside of the local regions legal channels. The Received Signal Strength Indictor (RSSI) calculated at the WIDS sensor, must be captured and logged to aid in the geo-location and detection of anomalous traffic within the controlled space. If an RSSI is detected that is equal to, or above the local country's local regulator limit, the WIDS must log and create a notification for this event. The system must also detect and log if there are DoS attacks being conducted within the operational space, either against the WLAN Access System, or other WLAN emitters within that space. These DoS attacks include radio frequency (RF) based DoS attacks, deauthentication flooding, and disassociation flooding DoS attacks. 802.11 WLAN bridges must also be detected and logged within the controlled space with special emphasis on whether any component connected to the WLAN Access System is conducting wireless bridging, as this type of connection should never be allowed by a WLAN Access System. Additionally, any action related to wireless bridging must be detected such as a device attempting to form a bridge, a single device beaconing for bridges, and two or more devices transmitting bridges data frames. An additional capability that the system may have is for the automatic capture of raw data frames triggered when any malicious, or anomalous traffic is detected by the WIDS sensor. An additional capability that a WIDS may

have is to automatically capture data frames triggered if an event, malicious activity or anomalous traffic has been detected.

6.1.1 Authorized Wireless Network Devices Detection

A Allowlist is a list of authorized WLAN devices, which are allowed to, or be a component of, the WLAN Access System, and the configuration which they are expected to operate. The authorized wireless network devices, include the wireless clients, APs and WIPS devices that are deployed as part of the WLAN Access System and must be documented in a Allowlist and included in the WIDS. Additionally, the Service Set Identifiers (SSIDs) of the Allowlisted APs, the channels those SSIDs broadcasting, authorized authentication method of the authorized network, and the encryption method of the authorized network must all be documented in the WIDS. All Allowlisted wireless network devices must have their bandwidth usage, connection status, association, number of connected devices, authentication status and, time usage monitored and tracked by the WIDS.

All frames between the authorized APs and authorized clients must be monitored by the WIDS and analyzed for any malicious or anomalous traffic. Additionally, the system must monitor whether or not there are any frame types or subtypes going between any authorized wireless network devices and any unauthorized devices. The WIDS must log any traffic that is detected between authorized and unauthorized devices. If authorized wireless network devices are detected deviating from the documented Allowlisted information, such as using an unauthorized channel, broadcasting an unauthorized SSID (including hidden SSID), association to an unauthorized SSID, deviating from an authorized association method, or not using the authorized encryption method, they must be logged, and a notification created of the deviation from normal operation. As shown in Figure 11, a log and notification must be made by the system when a peer-to-peer connections, ad-hoc networks or wireless bridges are made by any authorized client device to either an authorized or unauthorized client as this behavior can circumvent the security of the WLAN Access System and potentially give other devices unauthorized access to the network.

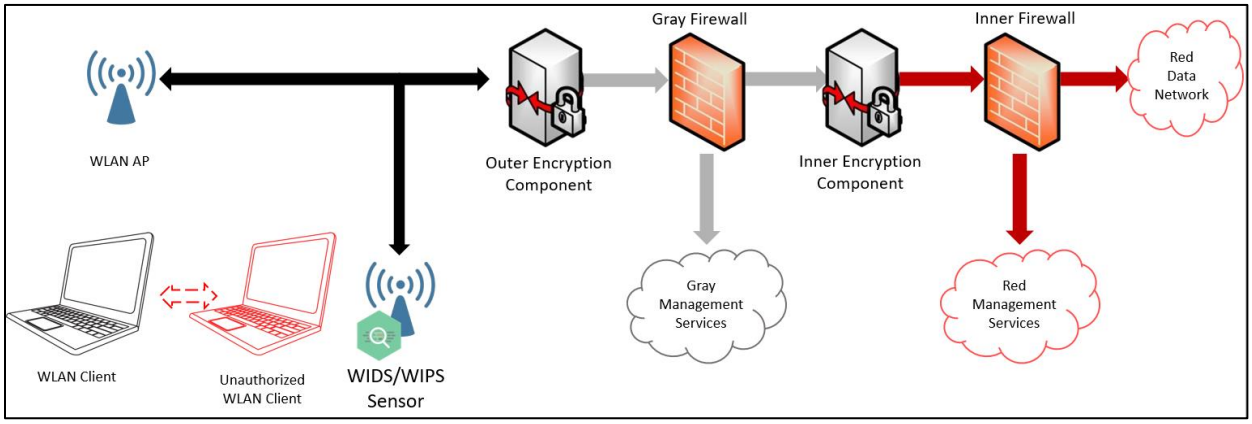

Figure 11: Unauthorized Wireless Peer-to-Peer Connection

If the WIDS system is integrated into the WLAN Access System and has visibility into the authorized client's wired interface, then it should have the capability to detect and log if the client is connected to a rogue AP and the wired connection is connected to the authorized network. The WIDS must log and

notify if an authorized wireless network device's Media Access Control (MAC) is detected and/or geo-located in two or more physically distinct places at the same time. This event could indicate that a malicious device is attempting to use the MAC address to spoof an authorized device. Depending on the configuration of the system, the system must also log when the authorized wireless network device's MAC is detected in more than two locations not at the same time showing it is either moving through controlled spaces and/or someone or something is spoofing the MAC address. The WIDS must detect and log illegal state transitions, such as a client device transmitting data frames through an AP to a network device before being associated and authenticated.

6.1.2 Unauthorized Client and Access Points Detection

Depending on the environment in which a WIDS is deployed, an unauthorized wireless device can be any device detected within the controlled space of the system, or only APs within the controlled space and any device attempting to connect to the WLAN Access System. The AO along with other decision-making bodies must define what an unauthorized wireless device is within the operational space and develop a plan of action on how to respond to unauthorized wireless devices detected by the WIDS. The AO must understand, depending on the reaction to unauthenticated wireless devices, that additional man-hours may be required to fulfill such a plan of action.

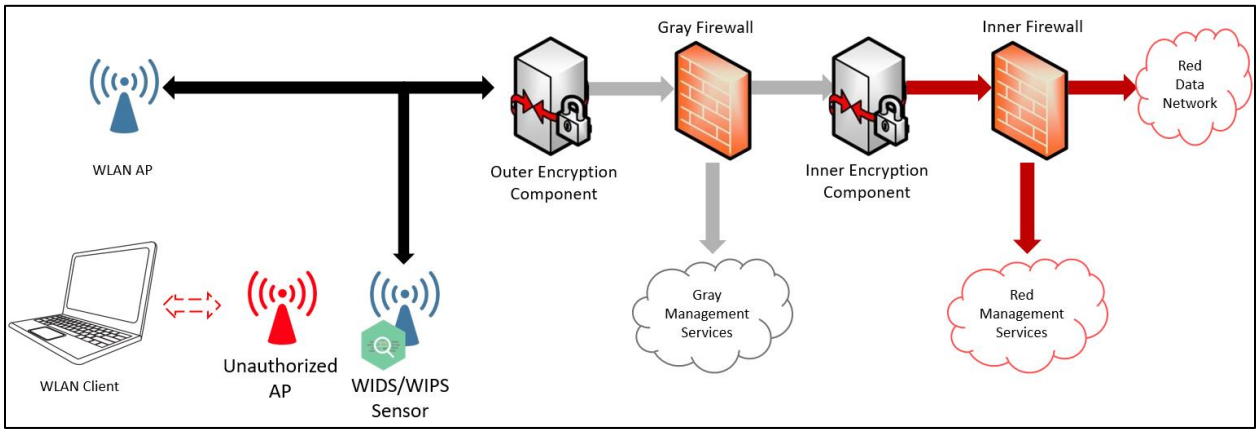

Figure 12: Unauthorized Wireless AP

APs and WLAN clients within the controlled space, that are not part of the Allowlist are considered unauthorized devices and must be detected by the WIDS. The AO and other decision-making bodies must also consider that wireless devices outside of the controlled space will be detected by the WIDS as the signals propagate into the controlled space. The most important detection capability, is if any unauthorized device attempts to connect, or is connected to any authorized device. Such an event must be detected, logged, and a notification created within the CM solution. All unauthorized wireless devices' status must be monitored in real time and logs of the status must be created. The status includes, but not limited to, whether the client is offline, associated, or authentication is pending.

A difficult task for the WIDS is to detect MAC Spoofing where an unauthorized device spoofs the MAC address of an authorized device within the Allowlist in an attempt to circumvent the detection capability of the WIDS. MAC Spoofing cannot be counteracted by the WIDS. The best measure against MAC Spoofing is the detection of such an attack, the geo-location of the devices performing the attack, and

long-term behavioral analysis of authorized wireless devices within the controlled space. A simple method of detecting such an attack is to track when and where the authorized devices operate within the WIDS controlled space. If an authorized wireless device is detected at the same time at two separate locations, then that is an indicator of MAC Spoofing and must be logged and a notification generated. Another indication of possible MAC Spoofing is identifying an authorized device within a location it has never been detected before. This event must be logged and a notification must be generated. This method of identification of a device performing MAC Spoofing requires a high degree of knowledge of the authorized clients within the system to be effective and not give high numbers of false positives. More advanced SIEM systems with behavior analytics may be useful in the detection of MAC Spoofing but require a far more significant investment of time and resources.

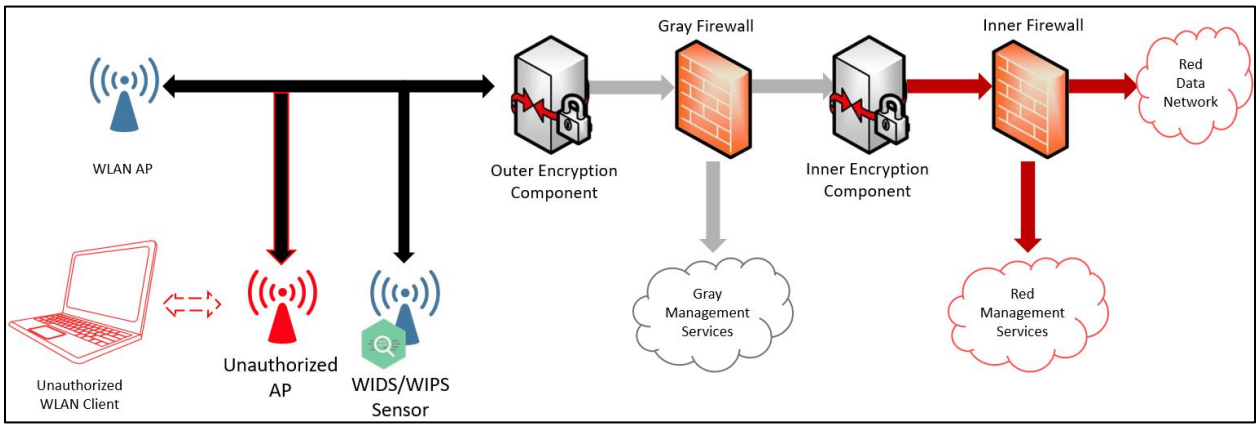

Figure 13: Unauthorized Wired AP

A rogue AP is an unauthorized AP that acts maliciously, or anomalously within the controlled space by either attempting to spoof an authorized AP, provides an unauthorized network for authorized and unauthorized clients, or tries to circumvent the WLAN Access System. A WIDS must have the capability to create administrator-defined rogue AP detection classification rules. As seen in Figure 13, a WIDS may also have the capability to detect if a rogue AP is connected to the wired network serving out unauthorized connections to the WLAN Access System and if detected the WIDS must be logged and a notification created.

6.2 Extended Detection

A WIDS deployed for CSfC is only required to monitor the WLAN Access System using 802.11 WLAN within the 2.4 GHz and 5.0 GHz frequencies. Any additional capability to detect protocols outside of the 802.11 WLAN 2.4 GHz and 5.0 GHz frequency bands is an optional capability and not required when a WIDS system monitors a controlled space, or monitors a WLAN Access System. If the WLAN Access System is not using an 802.11 WLAN Access System, and instead using another form of transport, then a WIDS is not required but highly recommended and should be used when possible. The AO may make the decision to deploy a WIDS capable of monitoring the specific WLAN Access System being implemented.

Additionally, the AO may want to have the capability to detect other protocols within a controlled space which is outside of the required 802.11 WLAN standard. In this case the AO may want to deploy a WIDS capable of detecting the desired protocols or a secondary WIDS to augment the detection capability. If a secondary WIDS is deployed, it must be deployed IAW Section 5.1. These protocols may include, but are

not limited to: cellular communications, Wireless Personal Area Network (WPAN) protocols, short range high bandwidth protocols and long range low band width protocols.

6.2.1 CELLULAR DETECTION

Cellular refers to the broadband cellular communication protocols such as Global System for Mobile Communication (GSM), Long Term Evolution, etc., which the physical spectrum that they occupy vary depending on technology and country. Cellular is common within consumer communication devices and used for long range communications back to a base station. There is a three phased approach for the detection of cellular emitters within a controlled space which are: the detection of cellular signals within the controlled space, the geo-location of the cellular emitter within the controlled space, and collection of the identifiers of the cellular emitter.

The simplest and minimal form of cellular detection is when a WIDS sensor is capable of detecting the mere presence of cellular signals by monitoring the physical energy of the signals within a controlled space. Improving on the detection capability would be to discretely identify the detected signals into individual cellular emitters to allow for the awareness of the number of devices. To greatly enhance the security posture of the controlled space, the WIDS could be able to geo-locate the discrete cellular emitters within the controlled space. The capability of a WIDS to detect temporary identifiers from cellular emitters allows for the identification of the cellular emitters within the controlled space. This phased approach to WIDS cellular detection is an optional capability which is not required, but the AO may decide to implement none, some, or all of these approaches.

6.2.2 WIRELESS PERSONAL AREA NETWORK (WPAN) DETECTION

WPAN refers to low powered machine-to-machine communications used for control systems within the controlled spaces. This detection capability refers to the different wireless technologies used within the fields of Internet of Things (IoT), medical devices, Industrial Control Systems, and building automation. These protocols can include but are not limited to; Bluetooth, Bluetooth Low Energy (BLE), ZigBee, Z-Wave, etc. A phased detection approach, similar to the cellular detection capability is recommended for the desired protocols. The AO must choose which protocols, if any, that should be monitored and which level of detection is required for the chosen protocols. Bluetooth and BLE should be considered by the AO for detection because of both the prevalence in IoT and standard wireless devices. In addition, the AO should highly consider this capability if there is a system within the controlled space operating using a WPAN protocol for both situational awareness and defense of that system.

The simplest and minimal form of WPAN detection is when a WIDS sensor is able to detect the mere presence of WPAN signals by monitoring the physical energy of the signals within a controlled space. An improvement over detection of the given protocols would be the ability to discreetly identify different WPAN emitters within the controlled space this would greatly enhance the security posture of the controlled space. A further step beyond the detection of discrete WPAN emitters would be the ability to geo-locate these emitters within the controlled space. Additionally, the WIDS should have the capability to capture the hardware addresses that these devices use to communicate, if not the ability to conduct network capture of the WPAN protocol itself. This phased approach to WIDS WPAN detection is an optional capability which is not required but the AO may decide to implement none, some, or all of these approaches.

7 WIRELESS INTRUSION PREVENTION SYSTEM (WIPS)

A WIPS consists of sensors (preferably dedicated), and a central controller working together to provide 24/7 active defense of a wireless network preventing unauthorized connection. The system can either be overlay or integrated into the WLAN Access System. WIPS is designed to protect authorized 802.11 devices within controlled spaces from unauthorized devices attempting to connect to them.

A WIPS is not required in a CSfC deployment when a WLAN Access System is used, but greatly enhances the security of a wireless deployment. A WIPS within a CSfC solution can either be an overlay solution, or an integrated solution deployed alongside the wireless controller. In an integrated deployment, WIPS must reside along with the wireless controller either within the Gray Network or a control segment of the Black Network. In an overlay WIPS deployment, the WIPS system can either be deployed within the Gray Network, or a controlled network segment. Refer to Section 5 for more information on deployment of WIPS solutions within the CSfC architecture.

7.1 WIPS DEPLOYMENT CONSIDERATIONS

Before considering to deploy a WIPS with a wireless access solution, the AO must understand the technical capability of the WIPS, and the legal authorities under which the system operates. A WIPS is capable of a DDoS which can shut down all standard Wi-Fi communications and prevent unauthorized signals from forming within the controlled space. This capability is extremely powerful for defending an authorized wireless network within the controlled space but can lead to inadvertently disrupting Wi-Fi devices. A WIPS is not an ideal solution in a controlled space that is collocated, adjacent to, or near a location that allows for Wi-Fi devices, has its own Wi-Fi network, or is a public space. WIPS must be tuned to only defend the authorized network and to ignore all other networks and devices it detects.

7.2 WIPS OPERATIONS

For the proper function of a WIPS and to ensure that the WIPS does not conduct inadvertent DDoS attacks against unintended wireless devices, a properly maintained and detailed Allowlist is required. The Allowlist is the detailed list of all devices connected to a WLAN Access System and all its expected operating behavior. With this list, rules can be made to defend the Allowlisted devices from unauthorized devices and from connecting to the network while in a misconfigured or insecure state. There can be more than one Allowlist that the WIPS system monitors. In this case, each Allowlist is separate from each other and no interaction between devices on a separate Allowlist is allowed. The Graylist is an optional list of expected devices within the controlled space which are known and allowed to operate within the area. Graylist devices are not allowed to connect to any Allowlist devices. The Denylist, is a list of all devices not contained in the Allowlist, or Graylist. If it exists, these devices must be prevented from forming any connection to any devices on the Allowlist (See Section 7.2.1).

7.2.1 WIPS ALLOWLIST

The Allowlist is the detailed list of all devices connected to a WLAN Access System and all its expected operating behavior. A WIPS solution deployed to secure a WLAN Access System requires all information on the Allowlist of the WLAN Access System to remain current. For details on the Allowlist see section 6.1.1. This Allowlist must be maintained and accessible by the WIPS at all times to ensure that the WIPS

does not either deny access to an authorized device, or allow an unauthorized device to attempt to connect to the network.

With a Allowlist established, the standard operating procedures of the network can be created. Any device not specifically on the Allowlist should be blocked from establishing any network connection to the authorized WLAN Access System and a notification should be made of this event. This includes any non-Allowlisted devices attempting to make a network connection to either the WLAN AP or the WLAN EUDs. Furthermore, the WIPS should be capable of monitoring the Allowlisted WLAN APs and WLAN EUDs and if they are detected deviating from the normal operating parameters of the WLAN Access System, they should be blocked from network connectivity and a notification made of this event. This includes operating on a different channel than expected, attempting to connect to another network, attempting to create a wireless bridge, etc.

7.2.2 WIPS GRAYLIST

The Graylist is a list of devices allowed within the controlled space but are not allowed network connectivity and not allowed to communicate with any device on the Allowlist. These devices include any known building automation, IoT devices and personal devices that are allowed within the building. The existence of a Graylist is left up to the AO and relevant security policy. This list only exists for situational awareness of a controlled space and exclusion of these devices from the Denylist. The WIPS system should still block all network communications to or from the Graylist devices and the Allowlisted WLAN APs and WLAN EUDs.

7.2.3 WIPS DENYLIST

The Denylist is an inclusive list of every device not on the Allowlist or Graylist. The AO using the relevant security policy, must decide on the handling of the Denylist by the WIPS. It is recommended that the WIPS remain completely defensive in this case and only defend the Allowlisted WLAN APs and WLAN EUDs from any misconfiguration or unauthorized connections. The AO may decide, to block all Denylisted devices from forming any network connections to prevent them from communicating using a WLAN this is not recommended and should only be used in the most controlled environment.

8 INFORMATION TO SUPPORT AO

This section details items which will assist the system AO in the operation of CSfC WIDS/WIPS Solutions. The customer and AO have obligations to perform the following:

- The customer and the AO must create an operation plan for how rogue devices are treated when detected by the WIDS System: whether all devices outside of the approved WLAN Access System are considered rogue devices or only those attempting to connect to the approved WLAN Access System.

- If a WIPS is deployed, the customer and AO must create an operation plan on how the WIPS will operate. Determine whether it prevents all connections from forming or only prevents communications to the approved WLAN Access System.

- The customer and AO must keep an updated map of the facility and identify where all authorized AP and WIDS/WIPS sensors are deployed.
- The customer must decide whether to geographically locate devices within the controlled space and additionally, to what degree the locations must be accurate.
- If the WIDS can geo-locate devices, the customer may want to designate areas where certain wireless devices are allowed and where they are not allowed. Such as devices being allowed at entrances or common areas; and devices being forbidden from certain areas.
- The customer and AO may decide to use a secondary WIDS or similar system to enhance the detection capability within the controlled space. This secondary system must still be deployed according to Section 5 and be NIAP validated.
- The customer and AO may decide to include additional protocols that the WIDS monitors and protects, such as cellular or Bluetooth. Additionally, they must decide what level of detection is required by their solution (See Section 6.2).
- The customer and AO must determine an acceptable alert configuration threshold for the WIDS/WIPS sensors before reporting begins.

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

9 REQUIREMENTS OVERVIEW

Sections 9 through 10 specify requirements for implementation of WIDS solutions compliant with this Annex.

9.1 THRESHOLD AND OBJECTIVE REQUIREMENTS

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

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

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 listed as Objective in this Annex may become Threshold requirements in a future version of this Annex. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this Annex.

9.2 REQUIREMENTS DESIGNATORS

Each requirement defined in this Annex has a unique identifier consisting of the prefix "WIDS," a digraph that groups related requirements together (e.g., "WI"), and a sequence number (e.g., 11).

Table 2 lists the digraphs used to group related requirements together, and identifies the sections in which those requirement groups can be found.

Table 2. Requirement Digraphs

Digraph	Description	Section	Table
GR	WIDS General Requirements	Section 10.1	Table 3
WL	WIDS WLAN Detection Requirements	Section 10.2	Table 4
ED	WIDS Extended Detection Requirements	Section 10.3	Table 5
WIP	WIPS WLAN Requirements	Section 10.4	Table 6
AU	Auditing Requirements	Section 10.5	Table 7
CM	Continuous Monitoring Requirements	Section 10.6	Table 8
TR	Testing Requirements	Section 10.7	Table 9

10 WIDS/WIPS REQUIREMENTS

10.1 WIRELESS INTRUSION DETECTION SYSTEM (WIDS) GENERAL REQUIREMENTS

Table 3 identifies the WIDS's general requirements for deployment. WIDS/WIPS refers to requirements that apply to WIDS and WIPS, if deployed.

Table 3. WIDS General Requirements (GR)

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-GR-1	A WIDS must be in place to monitor long-term (over 3 months) static CSfC Solution which uses a WLAN Access System IAW the Campus WLAN CP.	T=O	
WIDS-GR-2	A WIDS must be in place to monitor long-term (over 3 months) static CSfC Solution which uses a WLAN Access System IAW the Mobile Access CP government private wireless use case within a controlled space.	T=O	
WIDS-GR-3	The product(s) used for the WIDS/WIPS must be chosen from the list of WIDS/WIPS on the CSfC Components List.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-GR-4	WIDS/WIPS Components must be configured to use the NIAP-certified evaluated configuration.	T=O	
WIDS-GR-5	The WIDS being deployed to monitor the WLAN Access System must be either Integrated into the WLAN Access System or a separate Overlay WIDS.	T=O	
WIDS-GR-6	If the WLAN Access System is deployed as an integrated WIDS/WIPS, the WIDS/WIPS sensors must be deployed on, and controlled from, the same network segment that the WLAN Access Systems AP(s) operate on.	T	WIDS-GR-7
WIDS-GR-7	If the WLAN Access System is deployed as an integrated WIDS/WIPS, the WIDS/WIPS sensors must be on their own physically separate network dedicated to the WIDS sensors.	O	WIDS-GR-6
WIDS-GR-8	If the WIDS/WIPS is deployed as an overlay WIDS, the WIDS/WIPS must be deployed on the Black Management Network, Gray Management Network or a standalone network.	T=O	
WIDS-GR-9	If the WIDS/WIPS is deployed as an overlay WIDS, the WIDS/WIPS sensors must be on their own physically separate network only connected to the WIDS/WIPS Controller.	T=O	
WIDS-GR-10	All communication between WIDS/WIPS components must be done via a secure connection using Secure Shell (SSHv2), IPsec, TLS 1.2 or 1.3, DTLS, or TLS/HTTPS.	T=O	
WIDS-GR-11	The WIDS/WIPS components must disable non-secure communication paths used for management and event monitoring including Hypertext Transfer Protocol (HTTP), SNMPv1, File Transfer Protocol (FTP), and Telnet.	T=O	
WIDS-GR-12	The WIDS/WIPS controller must utilize a management interface used to control, manage and access management resources.	T=O	
WIDS-GR-13	If the WIDS/WIPS is deployed as an overlay WIDS, the management interface of the WIDS/WIPS controller must be connected to the management firewall or WIDS/WIPS firewall for the controller's connection to the management network.	T=O	
WIDS-GR-14	The management firewall connected to the WIDS/WIPS must only allow necessary protocols to reach the WIDS controller. The necessary protocols may include, but not limited to; TLS (1.2 or 1.3), DTLS, SSHv2, IPsec, NTP, DNS, DHCP, and system log.	T=O	
WIDS-GR-15	The WIDS/WIPS controller must be configured to block or deny all attempts to manage the WIDS controller from interfaces which are connected to the WIDS sensors.	T=O	
WIDS-GR-16	The WIDS/WIPS controller must not allow routing through itself to allow for connections between the sensors and the management network.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-GR-17	The WIDS/WIPS components, excluding the sensors must be integrated into existing network authentication to allow for centralized management of roles and access of the WIDS/WIPS.	T=O	

10.2 WLAN Detection Requirements for Wireless Intrusion Detection System (WIDS)

Table 4 identifies WIDS WLAN detection requirements.

Table 4. WLAN (WL) Detection Requirements for WIDS

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-WL-1	The WIDS must have an up-to-date Allowlist of all authorized wireless network devices (e.g., APs and EUDs) operating within its coverage area.	T=O	
WIDS-WL-2	The WIDS must detect and log AP(s) that are not on the Allowlist, but are within the coverage area of the WIDS sensors.	T=O	
WIDS-WL-3	The WIDS must detect and log EUDs which are not on the Allowlist, but are within the coverage area of the WIDS sensors.	T=O	
WIDS-WL-4	The WIDS/WIPS must detect and log if a rogue AP is connected via wire to the WIDS/WIPS sensor network.	O	Optional
WIDS-WL-5	The WIDS must detect and log any unauthorized wireless hardware attempting to gain access to the wireless network being serviced by the authorized WLAN Control System.	T=O	
WIDS-WL-6	The WIDS must geographically locate all supported 802.11 wireless emitters operating in the coverage area of the WIDS sensors.	O	Optional
WIDS-WL-7	The WIDS must be configured to monitor and log all 802.11 frame types and subtypes between unauthorized EUDs and authorized APs.	T=O	
WIDS-WL-8	The WIDS must be configured to monitor and log all 802.11 frame types and subtypes between unauthorized APs and authorized EUDs.	T=O	
WIDS-WL-9	The WIDS must be configured to monitor and log all 802.11 frame types and subtypes between authorized APs and authorized EUDs.	T=O	
WIDS-WL-10	The WIDS must capture the raw frames that triggered an alert as well as options on how long to continue capturing the frames.	O	Optional
WIDS-WL-11	The WIDS must monitor and analyze traffic from all 802.11 A/G/B/N/AC channels within the 2.4 GHz and 4.9/5.0 GHz bands including those outside local regulatory domain.	T=O	
WIDS-WL-12	The WIDS must detect and log the use of unauthorized wireless channels by Allowlisted devices.	T=O	
WIDS-WL-13	The WIDS must detect and log Allowlisted APs using SSIDs not permitted on the network (including hidden SSID).	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-WL-14	The WIDS must detect and log unauthorized APs broadcasting the same SSID as a Allowlisted AP.	T=O	
WIDS-WL-15	The WIDS must detect and log Allowlisted EUDs associating to SSIDs not permitted on the network (including hidden SSID).	T=O	
WIDS-WL-16	The WIDS must detect and log Allowlisted devices attempting to use unauthorized authentication methods.	T=O	
WIDS-WL-17	The WIDS must detect and log Allowlisted devices attempting to use unauthorized encryption schemes.	T=O	
WIDS-WL-18	The WIDS must be configured to process 802.11 traffic up to the data rate that is supported by the equipment in the wireless network.	O	Optional
WIDS-WL-19	The WIDS must detect and log the signal strength of 802.11 emitters operating in the coverage area of the WIDS sensors.	T=O	
WIDS-WL-20	The WIDS must detect and log when an 802.11 emitter is transmitting a signal with unusually high signal strength for an extended period of time.	T=O	
WIDS-WL-21	The WIDS must detect and log Radio Frequency (RF)-based Denial-of-Service (DoS) attacks.	T=O	
WIDS-WL-22	The WIDS must perform protocol anomaly analysis to detect and log violations of 802.11 standard.	O	Optional
WIDS-WL-23	The WIDS must detect and log deauthentication flooding.	T=O	
WIDS-WL-24	The WIDS must detect and log disassociation flooding.	T=O	
WIDS-WL-25	The WIDS must detect and log when the network's activity deviates from an established network baseline.	O	Optional
WIDS-WL-26	The WIDS must detect and log bandwidth usage.	O	Optional
WIDS-WL-27	The WIDS must detect and log the number of EUDs connected to the authorized WLAN Access System.	T=O	
WIDS-WL-28	The WIDS must detect and log usage times of EUDs with the authorized WLAN Access System.	T=O	
WIDS-WL-29	The WIDS must detect and log connection status of each client (authorized or unauthorized) in near real time including, but not limited to, whether the client is offline, associated, or authentication is pending.	O	Optional
WIDS-WL-30	The WIDS must detect and log illegal state transitions, such as a client device transmitting data frames through an AP to a network device before being associated and authenticated.	O	Optional
WIDS-WL-31	The WIDS must detect and log an event where an attacker spoofs the Media Access Control (MAC) address of an authorized client to attempt to connect to the legitimate network.	O	Optional
WIDS-WL-32	The WIDS must detect and log an event where a Allowlisted EUD's MAC address appears in multiple physically distant locations.	T=O	
WIDS-WL-33	The WIDS must detect and log Allowlisted EUDs establishing peer-to-peer connections with other Allowlisted devices or unauthorized devices.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-WL-34	The WIDS must detect and log EUDs bridging two network interfaces (wired and wireless).	O	Optional
WIDS-WL-35	The WIDS must detect and log the presence of an 802.11 bridge, Ad-Hoc networks or point-to-point networks.	T=O	
WIDS-WL-36	The WIDS must detect and log the presence of a single device transmitting beacons looking for a bridge.	T=O	
WIDS-WL-37	The WIDS must detect and log the presence of two or more devices transmitting bridge data frames.	T=O	

10.3 Wireless Intrusion Detection Systems (WIDS) Extended Detection Requirements

Table 5 identifies the WIDS's extended detection requirements for the detection and geo-location of additional protocols outside of 802.11 WLAN. These capabilities are currently optional in the Annex and not required, however, the AO may decide to implement a system with such capabilities.

Table 5. WIDS Extended Detection (ED) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-ED-1	The WIDS must monitor and analyze traffic from all 802.11 channels within the 3.6 GHz bands.	O	Optional
WIDS-ED-2	The WIDS must monitor and analyze traffic from all 802.11 channels within 6.0 GHz bands.	O	Optional
WIDS-ED-3	The WIDS must monitor and analyze traffic from all 802.11 channels within 60 GHz band.	O	Optional
WIDS-ED-4	The WIDS must detect when a cellular device is operating within the controlled space.	O	Optional
WIDS-ED-5	The WIDS must detect and identify different cellular emitters within the controlled space.	O	Optional
WIDS-ED-6	The WIDS must geo-locate discrete cellular devices within its controlled space.	O	Optional
WIDS-EU-7	The WIDS must detect Bluetooth classic within its controlled space.	O	Optional
WIDS-EU-8	The WIDS must detect and identify different Bluetooth classic devices within its controlled space.	O	Optional
WIDS-ED-9	The WIDS must geo-locate discrete Bluetooth classic devices within its controlled space.	O	Optional
WIDS-EU-10	The WIDS must detect BLE devices within its controlled space.	O	Optional
WIDS-EU-11	The WIDS must detect and identify different BLE devices within its controlled space.	O	Optional
WIDS-ED-12	The WIDS must geo-locate discrete BLE devices within its controlled space.	O	Optional

10.4 Wireless Intrusion Prevention System (WIPS) Requirements

Table 6 identifies the WIPS requirements for the defense of 802.11 WLAN Access Systems. These capabilities are currently optional in the Annex and not required, however, the AO may decide to implement a system with such capabilities.

Table 6. WIPS Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-WIP-1	A WIPS must be in place to monitor a long-term (over 3 months) static CSfC Solution which uses a WLAN Access System IAW the Campus WLAN CP.	O	Optional
WIDS-WIP-2	A WIPS must be in place to monitor a long-term (over 3 months) static CSfC Solution which uses a WLAN Access System IAW the Mobile Access CP government private wireless use case within a controlled space.	O	Optional
WIDS-WIP-3	A WIPS must be used to prevent any unauthorized device from forming a network connection with an authorized Allowlisted device.	O	Optional
WIDS-WIP-4	A WIPS must be used to prevent any communication of an authorized Allowlisted device if functioning outside of authorized use.	O	Optional
WIDS-WIP-5	If the AO and local policy requires, the WIPS must prevent any network connections from forming between any Denylisted devices.	O	Optional

10.5 WIDS AUDITING REQUIREMENTS

Table 7 identifies the WIDS Auditing Requirements.

Table 7. WIDS Auditing (AU) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-AU-1	All WIDS/WIPS components excluding the WIDS Sensors must send all generated system log data on to the solution's CM capability (such as a SIEM or IDS).	T=O	
WIDS-AU-2	The WIDS/WIPS components excluding the WIDS Sensors must log any failed attempt to log into its management interface.	T=O	
WIDS-AU-3	The WIDS/WIPS components excluding the WIDS Sensors must log whenever a new user is created.	T=O	
WIDS-AU-4	The WIDS/WIPS components excluding the WIDS Sensors must log whenever an attempt to escalate privileges on the WIDS components is detected.	T=O	
WIDS-AU-5	The WIDS/WIPS components excluding the WIDS Sensors must log whenever a user is added to a group.	T=O	
WIDS-AU-6	The WIDS/WIPS components excluding the WIDS Sensors must log whenever a change is made to group privileges.	T=O	
WIDS-AU-7	The WIDS/WIPS components excluding the WIDS Sensors must log whenever a user account attribute is changed.	T=O	
WIDS-AU-8	The WIDS/WIPS components excluding the WIDS Sensors must log whenever an authentication rule is created or modified.	T=O	
WIDS-AU-9	The WIDS/WIPS components excluding the WIDS Sensors must log any configuration change on the WIDS components.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-AU-10	The WIDS/WIPS components excluding the WIDS Sensors must log any configuration failures or errors.	T=O	
WIDS-AU-11	The WIDS/WIPS components excluding the WIDS Sensors must log when a WIDS sensor connects to the controller.	T=O	
WIDS-AU-12	The WIDS/WIPS components excluding the WIDS Sensors must log when a WIDS sensor disconnects or fails to communicate.	T=O	
WIDS-AU-13	The WIDS/WIPS components excluding the WIDS Sensors must log when there is an error state in any of the WIDS components.	T=O	

10.6 CONTINUOUS MONITORING REQUIREMENTS

The interface between the WIDS/WIPS Controller and the Management Firewall such as the Gray Management Firewall must be monitored as part of the Management Network. All monitoring requirements from the *CSfC Continuous Monitoring Annex* MP6 must be applied to a Gray WIDS/WIPS connection.

The following CM requirements apply to the interface between the WIDS/WIPS Controller and Management Firewall if they are part of the Black Management Network or part of a standalone network.

Table 8 identifies the Continuous Monitoring Requirements.

Table 8. Continuous Monitoring (CM) Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-CM -1	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log any failed login attempt.	T=O	
WIDS-CM-2	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log whenever a new user is created.	T=O	
WIDS-CM-3	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log whenever a user is added to a group.	T=O	
WIDS-CM-4	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log whenever a change is made to group privileges.	T=O	
WIDS-CM-5	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log whenever a user account attribute is changed.	T=O	
WIDS-CM-6	The authentication service supporting the WIDS/WIPS components excluding the WIDS Sensors must log whenever an authentication rule is created or modified.	T=O	
WIDS-CM-7	The monitoring capability must log any attempt to scan the WIDS/WIPS components excluding the WIDS Sensors, Management Firewall and any other component supporting the WIDS.	T=O	

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-CM-8	The monitoring capability must log if unusual traffic is detected between the WIDS/WIPS components and/or management firewall.	T=O	
WIDS-CM-9	The monitoring capability must log if a protocol outside of SSH, IPsec, or TLS is used to login into network components or management services from a dedicated management workstation or authorized management device.	T=O	
WIDS-CM-10	The monitoring capability must log any DNS queries on the WIDS Controller or any supporting components make to a domain or IP outside of the management network.	T=O	
WIDS-CM-11	If a CDP is used to support the WIDS Components, the WIDS Components must log if the version of the CRL downloaded from a CDP is older than the current cached CRL.	T=O	
WIDS-CM-12	If a CDP is used to support the WIDS Components, the WIDS Components must log if signature validation of the CRL downloaded from a CDP fails.	T=O	
WIDS-CM-13	The WIDS Components must log administrator lockout due to excessive authentication failures.	T=O	
WIDS -CM-14	Vulnerability scans must be conducted on the WIDS components within a time designated by the AO and relevant governing policies.	T=O	

10.7 TESTING REQUIREMENTS

Table 9 identifies the Testing Requirements.

Table 9. Testing Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
WIDS-TR-1	The organization implementing the annex must perform all tests listed in WIDS/WIPS Testing Annex.	T=O	

APPENDIX A. WIDS/WIPS GUIDANCE FOR SYSTEMS NOT INTEGRATED WITH CSFC DATA-IN-TRANSIT SOLUTIONS

OVERVIEW

The WIDS/WIPS Annex provides guidance for CSfC customers to deploy a WIDS/WIPS in their CM solution if they have the WLAN Access System in accordance to the Mobile Access CP or Campus WLAN CP. This Appendix provides engineering instructions and guidance for the deployment of WIDS/WIPS solutions to monitor controlled spaces in the absence of a CSfC cryptographic solution. This guidance should be used by customers deploying a WIDS/WIPS solution without a CSfC Campus WLAN or Mobile Access solution. Use of this Appendix alone does not provide CSfC cryptographic protection, nor is the use of this Appendix required to be registered as a CSfC solution.

A WIDS consists of sensors (preferably dedicated), and a central controller working together to provide 24/7 monitoring of the wireless spectrum focusing on 802.11 WLAN to detect, identify, and geo-locate wireless device within controlled space. A WIDS is vital if a WLAN Access System is deployed for communication within a space and enhances the security posture of a controlled space even if a WLAN Access System is not present. The WIDS must be capable of detecting 802.11 WLAN devices but the detection of additional protocols and RF energy enhances the security of the controlled space. A WIPS is currently optional and is not required within a controlled space whether or not a WLAN Access System is within the controlled space.

A WIPS consists of sensors (preferably dedicated), and a central controller working together to provide 24/7 active defense of a wireless network preventing unauthorized connection. A WIDS may have the capability of a WIPS and can be used as one, but a WIPS is not required at this time for monitoring controlled spaces. A WIPS is designed to protect authorized 802.11 devices within controlled spaces from any unauthorized device attempting to connect to them; defending authorized 802.11 networks and authorized clients from any attempts to attack, disrupt or connect to the clients or the wireless networks. These systems are capable of causing DDoS against 802.11 clients within their controlled space. Both the capabilities of the WIDS and the WIPS must be considered by the AO when deploying either a WIDS or WIPS. The AO should seek additional guidance from their relevant decision making bodies on inadvertent collection of signals and potential DDoS of wireless clients within their controlled space.

Deploying a WIDS/WIPS to monitor a controlled space requires that the WIDS/WIPS be a NIAP validated product and must be configured to use the NIAP-certified evaluation configuration. A WIDS/WIPS being deployed within a controlled space has a number of different configurations in which the system can be arranged. These configurations include being integrated into the WLAN Access System and overlay deployments for the WIDS/WIPS solution.

DEPLOYMENT ARCHITECTURE

A WIDS/WIPS is required if a WLAN Access System is used within the controlled space or if relevant policy requires a WIDS/WIPS be deployed for monitoring of the controlled space. The WIDS/WIPS must be selected from the NIAP Components List and it must be configured to use the NIAP-evaluated

configuration. It is recommended that a WIDS/WIPS solution only be used to monitor long term static locations and not for tactical or mobile environments. However refer to relevant policy or AO decision when determining when a WIDS/WIPS is required for the given deployment.

WIDS/WIPS Deployments

A WIDS/WIPS solution can be arranged in two general configurations which include a WIDS/WIPS integrated into WLAN Access Systems or an overlay WIDS/WIPS solution. When a WIDS/WIPS is integrated into a WLAN Access System, the WLAN Access System must have the capability to act as an authorized WIDS/WIPS. If a WLAN Access System is already deployed, this integrated solution has the benefit of reducing the number of required components and complexity of the WIDS/WIPS. If the WLAN Access System cannot act as a WIDS/WIPS, an overlay WIDS/WIPS must be used for monitoring of the WLAN Access System. When relevant policy, or an AO's decision determines that a WIDS/WIPS is required for a controlled space without a WLAN Access System, then an overlay WIDS/WIPS must be deployed. WIDS/WIPS is integrated into the WLAN Access System, WIDS/WIPS sensors can be deployed on the same network as the WLAN Access System's APs. However, if the WIDS/WIPS is an overlay the WIDS/WIPS sensors must be on a separate network.

Integrated WIDS/WIPS

A WIDS/WIPS that is integrated into an already existing WLAN Access System must have separate dedicated APs acting as WIDS/WIPS Sensors and WLAN Access APs. The same WLAN Access Controller can be used to manage both of the sensors and APs but, the APs and sensors must be separated logically from each other and not allowed to communicate with each other. Additionally, there must be a firewall between the WLAN Access Controller and the network that it manages. This prevents all but essential protocols going to and coming from the controller. This includes, but is not limited to, TLS (1.2 or 1.3), SSHv2, IPsec, NTP, DNS, DHCP, and system log. An example of this can be seen in Figure 14.

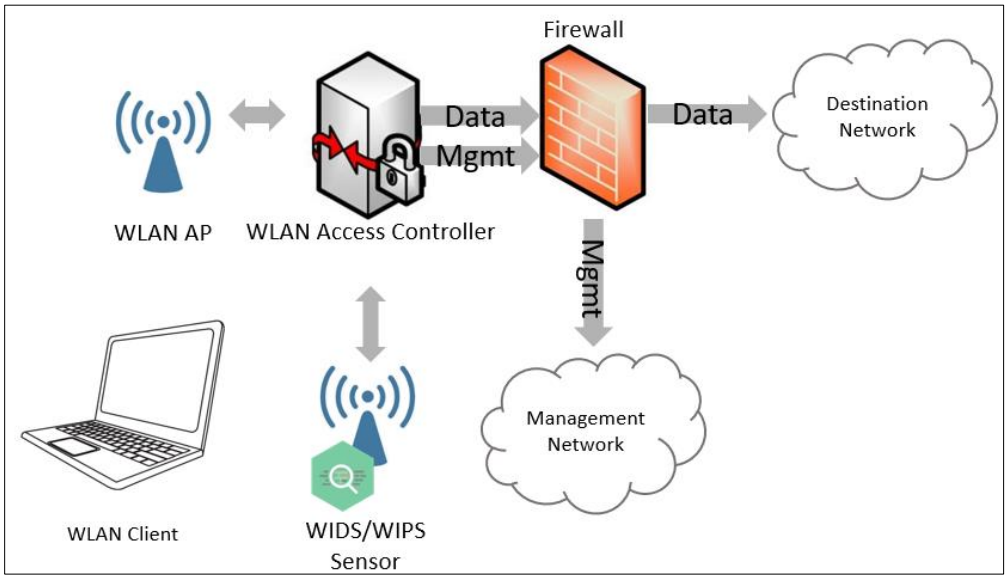

Figure 14: Integrated WIDS/WIPS

OVERLAY WIDS/WIPS

WIDS/WIPS may also deploy as an Overlay and not as a function of the WLAN Access System. If a WLAN Access System is not present, the WIDS may reside on the management network where the WLAN Access Controller is located, or on its own separate network. The WIDS sensors cannot be on the same network as the WLAN Access APs. As in the integrated WIDs/WIPS, an Overlay WIDS/WIPS controller requires a firewall between it and the network it manages to prevent all but essential protocols going to and coming from the controller. As seen in Figure 15, this includes, but is not limited to, TLS (1.2 or 1.3), SSHv2, IPsec, NTP, DNS, DHCP, and system log.

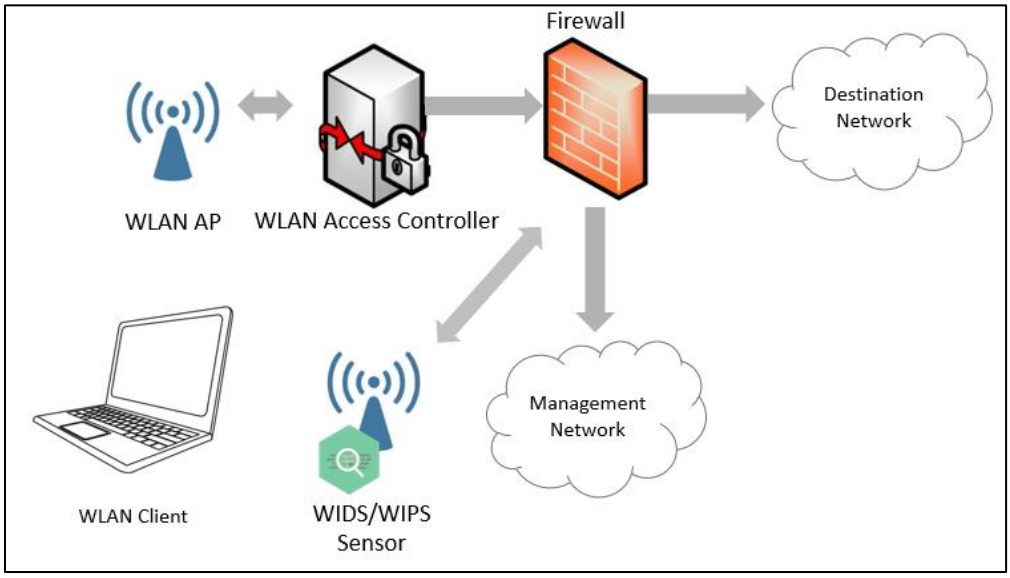

Figure 15: Overlay WIDS/WIPS

WIDS/WIPS SECURITY

Security of a deployed WIDS/WIPS is required for management, control, and network functionality of the WIDS/WIPS components. The components that make up a WIDS/WIPS include the WIDS/WIPS sensor, WIDS/WIPS controller, workstation, as well as other supporting components. Communications between the WIDS/WIPS sensors and the WIDS/WIPS controller must use secure communication (e.g., SSHv2, IPsec, or TLS (1.2 or 1.3)/HTTPS) and the communication between the WIDS/WIPS controller, workstation and other supporting components must also use secure communication (e.g., SSHv2, IPsec, or TLS (1.2 or 1.3)/HTTPS). All forms of unsecure management, control and sending data must be disabled for each WIDS/WIPS Component.

As shown in Figure 16, a firewall must block all communications between the WIDS Access controller and WLAN controller. This firewall protects both the management network and the WIDS/WIPS controller by monitoring and controlling all traffic to and from the WIDS/WIPS controller. This firewall must filter all but the necessary protocols from reaching the WIDS/WIPS controller. This includes, but is not limited to, TLS (1.2 or 1.3), SSHv2, IPsec, NTP, DNS, DHCP, and system log. In addition to the firewall, the WIDS/WIPS controller must be locked down to minimize the potential risk to the solution. First, there must be no capability to manage or control the WIDS/WIPS controller from the interfaces that are connected to the sensors. Second, there must not be any routing through the WIDS/WIPS controller

between the sensors and the management network. Finally, the WIDS/WIPS controller must have a management interface used to control, manage and access management resources.

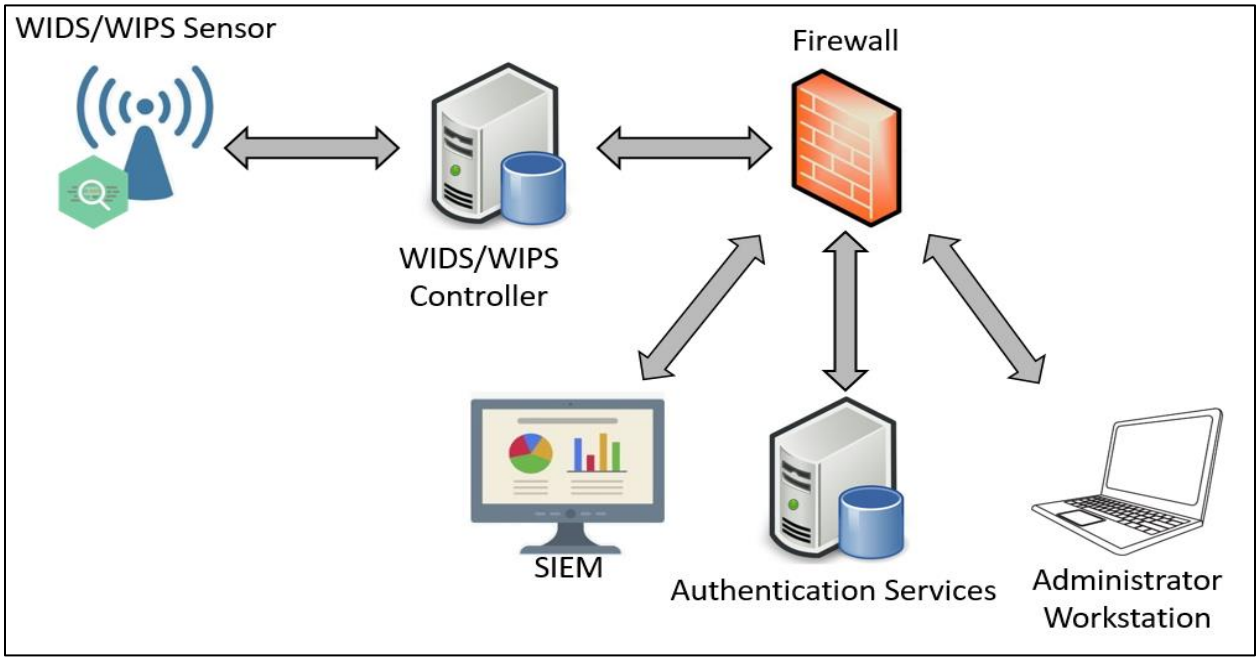

Figure 16: WIDS Components

As shown in Figure 17, the firewall can be replaced with a firewall/Virtual Private Network (VPN) gateway to provide an additional level of security for users attempting to log into the system and to provide a method of connecting multiple WIDS/WIPS solutions together. Connecting WIDS/WIPS solutions together using a VPN Gateway allows for the sharing of centralized resources, remote administration, and centralized monitoring of the WIDS/WIPS solution. This capability is considered optional to the WIDS/WIPS solution but will provide additional security for scaled WIDS/WIPS solutions.

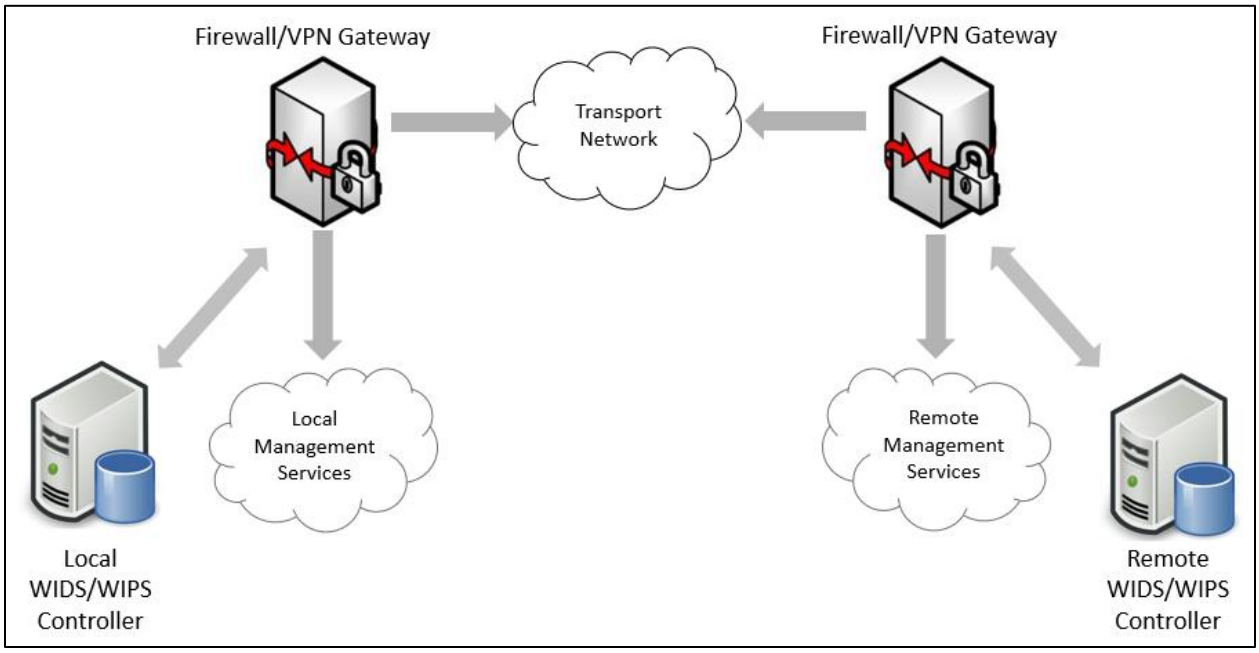

Figure 17: WIDS/WIPS Remote Systems

A centralized authentication service is fundamental for any network and WIDS/WIPS, even if it supports local account administration. The system must still use an external authentication service such as RADIUS, Active Directory, or Kerberos. All WIDS/WIPS components must be integrated into the network's existing CM capability such as an Intrusion Detection System, or Security Information and Event Management (SIEM).

The system logs that are collected from the WIDS/WIPS component must log any login event and must include any failed login attempts, successful logins, and administrator logins. The system logs must also include any changes to the authentication changes that includes creation, deletion, or modification of user accounts and any changes to groups or group membership. The WIDS/WIPS components must log any attempt for escalation of privileges. The WIDS/WIPS components must log when there are any configuration changes and whether or not the changes were successful. The WIDS/WIPS controller must also log the status of the WIDS/WIPS sensors and must include when a new sensor is connected, when a sensor is unreachable, and any sensor error status. These system logs are for the purpose of monitoring the WIDS/WIPS for any possible errors and potential security issues and should be used with any additional guidance required for CM within the solution.

WIDS/WIPS Continuous Monitoring

When deploying a WIDS/WIPS, logging and notification of the events within the controlled space are required for the proper operations and to maintain security of the controlled space. The WIDS/WIPS must have the capability to create notifications and alerts of events that it has detected. The AO may deem that this alerting and notification capability of the WIDS/WIPS meets their needs for CM of the controlled space. The AO alternatively can integrate the WIDS/WIPS into a SIEM that notifies and alerts their security administrators of events that are detected by the WIDS/WIPS. In this case, a WIDS/WIPS must support integration of its event logs into a SIEM and either sends its notifications to a SIEM, or set up the SIEM to create notifications of the events itself. The AO and local policy will dictate how often

these events, logs and notifications must be reviewed but it is recommended that the time frame between reviews be no longer than one week.

Either the SIEM, or the WIDS/WIPS interface must filter on notifications based on types, severity and number of notifications received. If being generated by the WIDS/WIPS interface, notifications should be descriptive and should show their significance. The WIDS/WIPS interface should have the capability to export events in industry standard formats such as Comma Separated Value (CSV) and Common Log Format (CLF). A WIDS/WIPS can be integrated into a larger CM capability in relation to data processing, alerting, notification and retention. Even if the WIDS/WIPS is used for notifications, all logs from the WIDS/WIPS must be sent to a long term storage system for data retention for the given amount of time. The retention time of this data must be decided by the AO and according to IAW policy but it is recommended to keep this data for a minimum of a year.

The interface between the WIDS/WIPS Controller and the management firewall must be monitored as part of the management network. The WIDS/WIPS must log and forward to a CM capability the following: user events, any failed login attempt, when a new user is created, when a user is added to a group, any change is made to group privilege, any user account attribute is changed, and when any authentication rule is created or modified. The firewall providing network access must log any attempts to conduct a network scan from the WIDS/WIPS or any attempts for the network to scan the WIDS/WIPS solution. The firewall must additionally alert on any unusual traffic between the WIDS/WIPS controller and the management network. This unusual traffic may include but is not limited to, attempting to use unauthorized ports or protocols, attempting to contact an IP address outside of the management network, or a large amount of traffic traversing the firewall. The firewall and controller must log if any protocol outside SSH, ESP or TLS is being used to log into the WIDS/WIPS. The firewall must log any DNS queries from the WIDS/WIPS controller to a domain outside of its management network. The WIDS/WIPS Controller needs to log any configuration changes made to it or its sensors to the networks cm capability. Finally, the WIDS/WIPS controller must have a recurring vulnerability scan conducted on it within a time designated by the AO and relevant governing policies.

WIRELESS INTRUSION DETECTION & WIRELESS INTRUSION PREVENTION

See Sections 6 & 7 respectively for WIDS & WIPS requirements. In those sections, ignore any specific CSfC requirements that refer to the Campus WLAN and MA CP requirements. If the deployed WIDS solutions do not monitor a WLAN Access System, then disregard Section 6.1.1. Section 6.1.1 only covers the monitoring of an authorized WLAN Access System within a controlled space. A WIPS may not be needed if a WLAN Access System is not being monitored. A WIPS focuses on defending a WLAN Access System from unauthorized connections. The WIPS still retains the capability to prevent connections from forming within the controlled space. If that is the desired effect, then the WIPS solution may still be deployed at the discretion of the AO.

APPENDIX B. GLOSSARY OF TERMS

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

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 – Ensuring timely and reliable access to and use of information (NIST SP 800-37).

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

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

Commercial National Security Algorithm (CNSA) - Set of commercial algorithms capable of protecting data through Top Secret level (previously known as Suite B).

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 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.

End User Device (EUD) – A form-factor agnostic component of the Mobile Access solution that can include a mobile phone, tablet, or laptop computer.

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

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

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

Red Network – A network that contains classified data that is not encrypted

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

Transport Layer Security (TLS) Client – A component on a TLS EUD that can provides the Inner layer of Data in Transit encryption.

APPENDIX C. ACRONYMS

Acronym	Meaning
AO	Authorizing Official
AP	Access Point
BLE	Bluetooth Low Energy
CM	Continuous Monitoring
CNSA	Commercial National Security Algorithms
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
CSfC	Commercial Solutions for Classified
CSS	Cybersecurity Solutions
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
D/NM	Deputy National Manager
DNS	Domain Name System
DoS	Denial of Service
DTLS	Direct Transport Layer Security
EUD	End User Device
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
GSM	Global System for Mobile Communication
IAW	In Accordance With
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
MA	Mobile Access
MAC	Media Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
O	Objective
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adelman algorithm
RSSI	Received Signal Strength Indicator
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Manager
SSH	Secure Shell
SSID	Service Set Identifier
SSHv2	Secure Shell Version 2
T	Threshold
TLS	Transport Layer Security

Acronym	Meaning
VLAN	Virtual Local Area Network
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WPA	Wi-F- Protected Access
WPA2	Wi-Fi Protected Access II
WPAN	Wireless Personal Area Network
VPN	Virtual Private Network

APPENDIX D. REFERENCES

CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems.* http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	April 2015
CNSSP 15	*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*	October 2016
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf	May 2001
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf	March 2006
ISO 09594-8	*Iso9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2001*	March 2013
Commercial National Security Algorithm Suite	*NSA Guidance on Encryption Algorithms* https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm	December 2015
RFC 3711	*IETF RFC 3711 The Secure Real-Time Transport Protocol (SRTP).* M. Baugher and D. McGrew.	March 2004
RFC 4252	*IETF RFC 4252 The Secure Shell (SSH) Authentication Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4253	*IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4254	*IETF RFC 4254 The Secure Shell (SSH) Connection Protocol*. T. Ylonen and C. Lonvick.	January 2006
RFC 4256	*IETF RFC 4256 Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)*. F. Cusack and M. Forssen.	January 2006
RFC 4492	*IETF RFC 4492 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk Corriente, B. Moeller, and Ruhr-Uni Bochum.	May 2006

RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5996	*IETF RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)*. C. Kaufman, et. al.	September 2010
RFC 6188	*IETF RFC 6188 The Use of AES 192 and AES 256 in Secure RTP.* D. McGrew.	March 2011
RFC 6239	*IETF RFC 6239 Suite B Cryptographic Suites for Secure Shell (SSH)*. K. Igoe.	May 2011
RFC 6379	*IETF RFC 6379 Suite B Cryptographic Suites for IPsec*. L. Law and J. Solinas.	October 2011
RFC 6380	*IETF RFC 6380 Suite B Profile for Internet Protocol Security (IPsec)*. K. Burgin and M. Peck.	October 2011
RFC 6460	*IETF RFC 6460 Suite B Profile for Transport Layer Security (TLS)*. M. Salter and R. Housley.	January 2012
SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	May 2013
EG v 1.0	*CSfC Enterprise Gray Implementation Requirements Annex v1.0*	April 2019
CM v 1.0	*CSfC Continuous Monitoring Annex v1.0*	2020
CWLAN v 2.2	*CSfC Campus Wireless Local Area Network Capability Package v2.2*	June 2018
MACP v 2.1	*CSfC Mobile Access Capability Package v2.1*	June 2018