Sharing allow:
TLP - GREEN

Approved

Network Security Standard

Document ID: **SEC-07**
For: Alliance Federation
Approval Date: 2023-06-07
Approved By: NSC

1. Introduction

This document describes the network security requirements for the Alliance Federation. Implementation of these security requirements will promote a consistent level of network security across the Alliance Federation to support secure network interconnectivity and interoperability.

2. Definitions

Refer to *SEC-00 Information Security Glossary* for definitions used in this Standard.

3. Applicability

This standard applies to all networks and networking infrastructure that support Alliance Federation Systems and Services.

4. Network Security Requirements

4.1 Network Segmentation

The network architecture must be able to segment services from one another based on a risk assessment conducted on the service or asset. An example of this would be a web server with a database backend; the web server may be located in a different network security zone from the database.

Examples of security zone names[1][2]:

- Public zone
- Public access zone
- Operations zone
- Management zone
- High-Performance Computing zone
- Data Storage zone

All security zones and services in each zone must be documented.

4.2 Network Access Controls

Network access controls can exist at different layers of the network, from simple access control lists (ACL) on a layer 3 Networking Device, all the way to zero trust network access (ZTNA) solutions. The following are controls that environments must implement:

4.2.1 All traffic traversing the network from one Network Security Zone to another must be filtered through a Networking Device capable of restricting traffic by both Internet Protocol (IP) address and port number. A Networking Device capable of stateful filtering is recommended.

4.2.2 Rules must be created for specific protocols or services that are known to be needed between two endpoints in different Network Security Zones. (No “ip any any” rules)

4.2.3 The default action on all devices used for the filtering or restricting traffic must be to drop or block traffic.

4.2.4 All rules created that allow traffic to traverse between Network Security Zones must be documented.

Additional controls should be considered for Network Security Zones where data that is classified as High or Very High is accessed or stored.

It is important to evaluate the security risks when allowing traffic between different Network Security Zones; for instance some Network Security Zones like one used for a production service and one used for the development or testing of that same service must never where possible be allowed to communicate with each other.

[1] CCCS - Baseline Security Requirements for Network Security Zones

[2] NIST Special Publication - NIST SP 800-223 ipd - High-Performance Computing(HPC) Security

4.3 Encryption

All network traffic egressing an information system environment that is destined for another operated by a different organisation, or when network traffic traverses infrastructure owned or operated by a different organization should be encrypted. All data classified as High or Very High must be encrypted in transit. All internal network traffic must be encrypted where possible and where the technology allows. The risks associated with any unencrypted traffic flows must be assessed according to *SEC-05 Cybersecurity Risk Management Policy*.

4.4 Intrusion Detection and Prevention

Intrusion detection systems (IDS) or intrusion prevention systems (IPS) must be used either on the inside or outside of Networking Device to monitor all traffic destined through your upstream providers to generate alerts or take preventative actions[3]. An IDS or IPS device must be used for networks where data classified as High or Very High transits.

4.5 Logging

All Networking Devices must produce logs in accordance with *SEC-06 System Logging and Security Monitoring Standard*.

4.6 Networking Device Management

Networking Devices are a critical component to the confidentiality, integrity and availability of an information system environment. The security measures applied on these devices should be either equivalent to or higher than those required by the classification level of the data that traverses them. Networking Devices must be configured to comply with the Identity and Access Management Standard and *SEC-06 System Logging and Security Monitoring Standard.*

[3] Inspection on encrypted traffic will be limited

4.7 Network Architecture Diagrams

All sites, groups, and teams that are operating environments with multiple Network Security Zones must keep up-to-date architecture diagrams. These diagrams should depict physical and virtual connections between all Networking Devices where traffic will traverse Network Security Zones, security appliances, Internet Services Providers (ISP), and VPN connections.

5. Related Information

SEC-00 Information Security Glossary
SEC-02 Data Classification Policy
SEC-05 Cybersecurity Risk Management Policy
SEC-06 System Logging and Security Monitoring Standard
CCCS - Baseline Security Requirements for Network Security Zones