National Security Agency
Cybersecurity Technical Report

Network Infrastructure Security Guide

June 2022

U/OO/118623-22
PP-22-0293
Version 1.1

Notices and history

Document change history

Date	Version	Description
June 2022	1.1	Minor clarifications and additional vendor links
March 2022	1.0	Report released

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guide shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco® and Cisco IOS® are registered trademarks of Cisco Systems, Inc.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Defense Industrial Base Inquiries for Cybersecurity Services:
DIB Cybersecurity Program, DIB_Defense@cyber.nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contents

Network Infrastructure Security Guide i
Contents iii
1. Introduction 1
1.1 Regarding Zero Trust 1
2. Network architecture and design 2
2.1 Install perimeter and internal defense devices 2
2.2 Group similar network systems 3
2.3 Remove backdoor connections 4
2.4 Utilize strict perimeter access controls 4
2.5 Implement a network access control (NAC) solution 5
2.6 Limit virtual private networks (VPNs) 5
3. Security maintenance 8
3.1 Verify software and configuration integrity 8
3.2 Maintain proper file system and boot management 9
3.3 Maintain up-to-date software and operating systems 10
3.4 Stay current with vendor-supported hardware 11
4. Authentication, authorization, and accounting (AAA) 12
4.1 Implement centralized servers 12
4.2 Configure authentication 13
4.3 Configure authorization 14
4.4 Configure accounting 15
4.5 Apply principle of least privilege 15
4.6 Limit authentication attempts 17
5. Local administrator accounts and passwords 17
5.1 Use unique usernames and account settings 18
5.2 Change default passwords 19
5.3 Remove unnecessary accounts 19
5.4 Store passwords with secure algorithms 19
5.5 Create strong passwords 21
5.6 Utilize unique passwords 23
5.7 Change passwords as needed 23
6. Remote logging and monitoring 24
6.1 Enable logging 25
6.2 Establish centralized remote log servers 25
6.3 Capture necessary log information 26
6.4 Synchronize clocks 27
7. Remote administration and network services 28
7.1 Disable clear text administration services 28
7.2 Ensure adequate encryption strength 30
7.3 Utilize secure protocols 31
7.4 Limit access to services 31
7.5 Set an acceptable timeout period 32
7.6 Enable Transmission Control Protocol (TCP) keep-alive 33

7.7 Disable outbound connections 33
7.8 Remove SNMP read-write community strings 34
7.9 Disable unnecessary network services 35
7.10 Disable discovery protocols on specific interfaces 36
7.11 Configure remote network administration services 36
7.11.1 Configuring SSH for remote administration 36
7.11.2 Configuring HTTP for remote administration 39
7.11.3 Configuring SNMP for remote administration 40
8. Routing 40
8.1 Disable IP source routing 41
8.2 Enable unicast reverse-path forwarding (uRPF) 41
8.3 Enable routing authentication 42
9. Interface ports 43
9.1 Disable dynamic trunking 43
9.2 Enable port security 44
9.3 Disable default VLAN 45
9.4 Disable unused ports 47
9.5 Disable port monitoring 48
9.6 Disable proxy Address Resolution Protocol (ARP) 49
10. Notification and consent banners 50
10.1 Present a notification banner 50
11. Conclusion 51
Abbreviations 52
References 54
Works cited 54
Related guidance 56

Figure 1: Network perimeter with firewalls and a DMZ 3

1. Introduction

Guidance for securing networks continues to evolve as adversaries exploit new vulnerabilities, new security features are implemented, and new methods of securing devices are identified. Improper configurations, incorrect handling of configurations, and weak encryption keys can expose vulnerabilities in the entire network. All networks are at risk of compromise, especially if devices are not properly configured and maintained. An administrator's role is critical to securing the network against adversarial techniques and requires dedicated people to secure the devices, applications, and information on the network.

An administrator's role is critical in securing networks.

This report presents best practices for overall network security and protection of individual network devices. It will assist administrators in preventing an adversary from exploiting their network. While the guidance presented here can be applied to many types of network devices, the National Security Agency (NSA) has provided sample commands for Cisco Internetwork Operating System (IOS) devices. These commands can be executed to implement recommended mitigations.

1.1 Regarding Zero Trust

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. NSA fully supports the Zero Trust security model, and much of the guidance in this report can be applied at different boundaries as recommended in Zero Trust guidance. However, this report provides guidance to mitigate common vulnerabilities and weaknesses on existing networks. As system owners introduce new network designs intended to achieve more mature Zero Trust principles, this guide may need to be modified.