December 8, 2022

Network Security Project

Network Security and Forensics (CSEC462 – Fall 2221)

Mehul Sen
ms1450@rit.edu

Table of Contents

1. Executive Summary

This paper covers the CTI report by CISA A20-336A. The report describes the common techniques, tactics, and procedures (TTPs) employed by threat actors targeting U.S. think tanks. It also recommends mitigations for leaders, staff, and cybersecurity personnel. We used the OODA loop to analyse the CTI report and identify ten MITRE ATT&CK TTPs. We also used CIS Controls v8 to Enterprise ATT&CK v8.2 and the network topology provided to us to identify eighteen mitigations and seven security controls that could be applied to the TTPs based on the network infrastructure.

After identifying all the possible mitigations for the TTPs listed in the CTI report, we used a prioritization process that incorporated the weight of each mitigation as well as the number of times a CIS security control appeared as valid mitigation to identify the most impactful security controls that can be implemented on the network. The top four prioritized security controls identified were (descending order): Secure Configuration of Enterprise Assets and Software, Penetration Testing, Network Infrastructure Management, and Network Monitoring and Defence.

The technologies chosen to implement each of these security controls were:

- Firewall and Packet Filtering (iptables)

They can separate different parts of the network based on the levels of trust associated with them as well as custom filters. They primarily operate on layers two to four of the OSI model and act as a preventative security control.

- Network Security Monitors (zeek)

They passively observe and ingest network traffic and categorize each set of traffic data based on their properties and check for suspicious activities or threats. They primarily operate on layers two to seven of the OSI model and act as a detective security control.

- Proxy Server (Dante)

They can protect against attacks on the IP space by acting as a proxy for host devices. They primarily operate on layer five of the OSI model and act as a preventative security control.

- Network Intrusion Detection System (Snort)

They monitor the traffic flowing through the network and look for any suspicious events and activities. They primarily operate on layers two to seven of the OSI model and act as a detective security control.

This paper also lists the purpose that each of these tools fulfil, the installation guide that can be used to install the tool, an implementation section that states how the tool can be implemented into the network and a justification section that justifies the usage of that tool and links it to the TTPs and mitigations derived earlier.

2. CTI Summary

The CISA Report A20-336A titled “Advanced Persistent Threat Actors Targeting U.S. Think Tanks” describes the various tactics, techniques, and procedures (TTPs) used by advanced persistent threat actors to target U.S. think tanks. The COVID-19 pandemic has caused an increase in employees and customers reaching an organization’s network remotely. This has provided threat actors with more opportunities to exploit and leverage remote connections. This report provides some mitigations targeted towards leadership, best practices for users and staff and technologies and configurations that IT Staff and cybersecurity personnel can implement to further increase their organization’s security posture.

This report is a cyber threat intelligence(CTI) report that provides operational intelligence. It does not list the IP addresses, domains and other specific information used by the attackers or list out the exact security controls that can be implemented to defend against the attackers. Instead, it provides the various tactics, techniques, and procedures (TTPs) utilized by the attackers and best practices to mitigate threats.

This report comes from FBI and CISA so we can assume that it is trustworthy. We can also determine if it is applicable to our organization using the Observe, Orient, Decide and Act (OODA) loop.

- **Observe**: This involves obtaining and reading the CTI Report.
- **Orient**: After obtaining a digital copy of the report, we can orient ourselves and combine the report findings with our organizational infrastructure. This would include understanding our organization’s network, existing security controls, TTPs mentioned by the CTI report and relevant mitigations as mentioned by CIS Controls.

2.1. Current Network Topology

The current network topology of our organization is as follows:

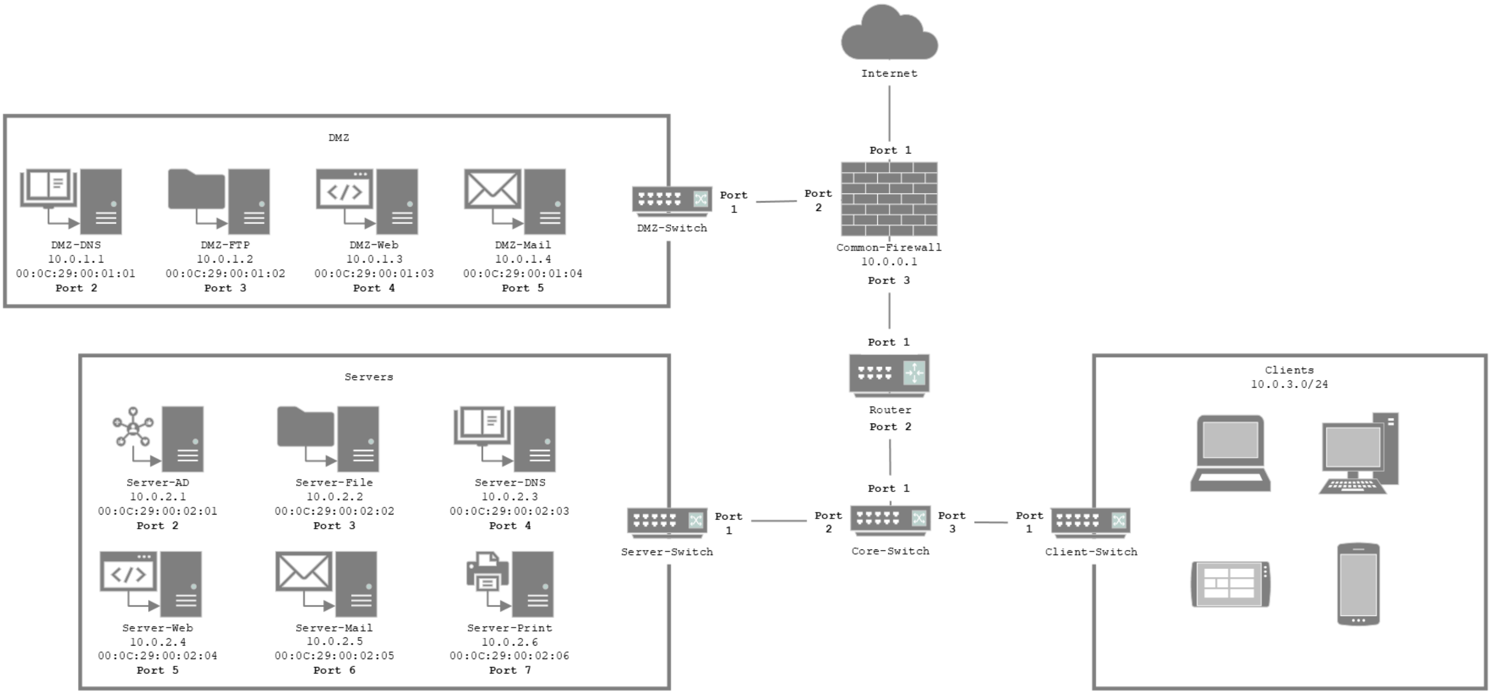

Figure 1 - Current Network Topology

There are three networks, the DMZ Network (10.0.1.0/24), the Servers Network (10.0.2.0/24) and the Clients Network (10.0.3.0/24). The DMZ Network contains a public DNS server, public file server, public website server and a public mail server. The Servers Network contains the active directory and DHCP Server, network file share server, internal DNS Server, internal web server, internal mail server and an internal print server. The Clients Network contains client devices such as laptops, desktops, tablets, and phones.

2.2. CTI TTPs

The CTI report lists several TTPs and mitigations, we can utilize the MITRE ATT&CK framework and use its tactics and techniques to identify the mitigation and detection methods for each. The networks based TTPs mentioned in the report are:

TTP Name	**TTP ID**	**ATT&CK Tactic(s)**	**Mitigation**	**Detection**
Drive-by Compromise	T1189	Initial Access	Application Isolation and Sandboxing (M1048), Exploit Protection (M1050), Restrict Web-Based Content (M1021), Update Software (M1051)	Firewall, Proxy, Network Intrusion Detection Systems
Remote System Discovery	T1018	Discovery	Cannot be mitigated due to its abuse of system features	Monitor Network Traffic
Network Sniffing	T1040	Credential Access, Discovery	Encrypt Sensitive Information (M1041), Multi-factor Authentication (M1032)	Monitor Network Traffic
Network Service Scanning	T1046	Discovery	Disable or Remove Feature or Program (M1042), Network Intrusion Prevention	Monitor Network Traffic,

			(M1031), Network Segmentation (M1030)	Network Intrusion Detection Systems
System Network Connections Discovery	T1049	Discovery	Cannot be mitigated due to its abuse of system features	Monitor Network Traffic
Remote Services: Remote Desktop Protocol	T1021.001	Lateral Movement	Audit (M1047), Disable or Remove Feature or Program (M1042), Limit Access to Resource Over Network (M1035), Multi-factor Authentication (M1032), Network Segmentation (M1030), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018)	Monitor Network Traffic
Remote Services: SSH	T1021.004	Lateral Movement	Disable or Remove Feature or Program (M1042), Multi-factor Authentication (M1032), User Account Management (M1018)	Monitor Network Traffic
Exploitation of Remote Services	T1210	Lateral Movement	Application Isolation and Sandboxing (M1048), Disable or Remove Feature or Program (M1042), Exploit Protection (M1050), Network Segmentation (M1030), Privileged Account Management (M1026), Threat Intelligence Program (M1019), Update Software (M1051), Vulnerability Scanning (M1016)	Monitor Network Traffic
Command and Control	TA0011 (T1001.001, T1008, T1071.001, T1071.002, T1071.003, T1071.004, T1090.002, T1090.003, T1090.004, T1092, T1095, T1102.001, T1102.002, T1104, T1105, T1132.001,	Command and Control	Network Intrusion Prevention (M1031), Filter Network Traffic (M1037), Disable or Remove Feature or Program (M1042), Operating System Configuration (M1028), Network Segmentation (M1030), Restrict Web-based Content (M1021), Execution Prevention (M1038)	Monitor Network Traffic, Monitor File Access on Removable Media, Monitor File Creation and File Transfer, Monitor Applications and Processes

	T1219, T1568.002, T1571, T1572, T1573.001, T1573.002)			related to remote admin tools
Exfiltration	TA0010 (T1041, T1048.003)	Exfiltration	Network Intrusion Prevention (M1031), Filter Network Traffic (M1037), Network Segmentation (M1030)	Monitor Network Traffic

Table 1 - ATT&CK TTPs and mitigations

2.3. CIS Controls

Based on the mitigations identified in Table 1, we can use the CIS Controls v8 ATT&CK High Level Mapping to identify the corresponding CIS Control which relate to networking. The mitigations and the suggested CIS controls for each mitigation are:

Mitigation	**Weight**	**CIS Control**	**CIS Safeguards**	**Title**	**Description**
M1016 – Vulnerability Scanning	1	18	18.1, 18.2, 18.3, 18.5	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.
M1018 – User Account Management	2	8	8.1, 8.2, 8.3	Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
		12	12.2, 12.5	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.
M1019 - Threat Intelligence Program	1	-		-	-
M1021 - Restrict Web-based Content	2	9	9.2, 9.3, 9.6	Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.
M1026 - Privileged Account Management	2	12	12.2, 12.5	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting

					vulnerable network services and access points.
M1028 - Operating System Configuration	2	8	8.1, 8.2, 8.3	Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
		18	18.3, 18.5	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.
M1030 - Network Segmentation	5	3	3.12	Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
		4	4.2, 4.4	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
		12	12.2	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.
		13	13.10	Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.
M1031 - Network Intrusion Prevention	3	4	4.2	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

		9	9.2	Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.
		13	13.3, 13.8	Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.
M1032 - Multi-factor Authentication	3	-	-	-	-
M1035 - Limit Access to Resource Over Network	1	4	4.2	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
		12	12.2, 12.6	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.
		13	13.10	Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.
M1037 - Filter Network Traffic	2	4	4.2	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software

					(operating systems and applications).
		9	9.2, 9.3	Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.
		13	13.4, 13.10	Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.
		18	18.2, 18.3	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.
M1038 - Execution Prevention	1	-	-	-	-
M1041 - Encrypt Sensitive Information	1	3	3.12	Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
		4	4.2, 4.6	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
M1042 - Disable or Remove Feature or Program	5	18	18.2, 18.3, 18.5	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

M1047 - Audit	1	8	8.1, 8.2, 8.3, 8.5, 8.9, 8.10, 8.11	Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
		18	18.3, 18.5	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.
M1048 - Application Isolation and Sandboxing	2	-	-	-	-
M1050 - Exploit Protection	2	13	13.10	Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.
M1051 - Update Software	2	12	12.1	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.
		18	18.1, 18.2, 18.3, 18.5	Penetration Testing	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Table 2 - ATT&CK Mitigations and CIS Controls

Note: The Weight column describes the frequency of that mitigation appearing as a valid mitigation solution for the CTI TTPs listed in Table 1.

- **Decide**: Based on the information derived from the CTI Report and the CIS Controls used, we can decide on which portions of the report are applicable to our infrastructure.
- **Act**: Finally, we can act on the decisions made in the Decide phase and apply the prioritized modifications to the infrastructure.

3. Prioritization Process

Once we have established the CIS Security controls required to mitigate the threats mentioned in the CTI report, we then need to prioritize the security controls that would have the biggest impact on improving the security stance for the organization.

This can be done by calculating the number of times a CIS Control is referenced by each of the mitigations in Table 2. We also need to take into consideration the weight of each of mitigation based on the number of times they appear in Table 1. If we add up the count and total weight of the mitigations, we obtain the impact score for each of the CIS Control. The control with the largest impact score will have the greatest impact on the network security of an organization, while the control with the lowest impact score will have the least impact.

CIS Control	Number and weight of Mitigations	Impact Score
3	2 (1, 5)	6
4	5 (1, 2, 1, 3, 5)	13
8	3 (1, 2, 2)	5
9	3 (2, 3, 2)	7
12	5 (2, 1, 5, 2, 2)	12
13	5 (2, 2, 1, 3, 5)	11
18	6 (2, 1, 5, 2, 2, 1)	13

Table 3 - CIS Control impact scores

3.1. CIS Controls Priority List

Based on the calculation above, we can identify that CIS Control 4 and 18 have the largest impact, while CIS Control 8 has the least. We can also create a prioritization list as follows with the topmost control having the highest priority:

Priority	**CIS Control**
1	4 - Secure Configuration of Enterprise Assets and Software
2	18 - Penetration Testing
3	12 - Network Infrastructure Management
4	13 - Network Monitoring and Defence
5	9 - Email and Web Browser Protections
6	3 - Data Protection
7	8 - Audit Log Management

Table 4 - CIS Control Priority List

3.2. CIS Controls Implementation

Next, we can decide on the implementation of these controls. A high-level implementation of each of the discussed CIS Security controls is as follows:

CIS Security Control	**CIS Control Name**	**CIS Safeguard(s)**	**High-Level Implementation**
3	Data Protection	**3.12 –** Segment Data Processing and Storage Based on Sensitivity	Implement Trunk and VLANs to segment the data flowing through the network.
4	Secure Configuration of Enterprise Assets and Software	**4.2 –** Establish and Maintain a Secure Configuration Process for Network Infrastructure	Implement Firewall on the Servers and packet filtering.

		4.4 – Implement and Manage a Firewall on Servers **4.6 –** Securely Manage Enterprise Assets and Software	
8	Audit Log Management	**8.1 -** Establish and Maintain an Audit Log Management Process **8.2 –** Collect Audit Logs **8.3 –** Ensure Adequate Audit Log Storage **8.5 –** Collect Detailed Audit Logs **8.9 –** Centralize Audit Logs **8.10 –** Retain Audit Logs **8.11 –** Conduct Audit Log Reviews	Implement NetFlow to centralize collecting, analysing, and storing traffic data.
9	Email and Web Browser Protections	**9.2 –** Use DNS Filtering Services **9.3 –** Maintain and Enforce Network-Based URL Filters **9.6 –** Block Unnecessary File Types	Implement DNSSEC and SSL/TLS
12	Network Infrastructure Management	**12.1 –** Ensure Network Infrastructure is Up to Date **12.2 –** Establish and Maintain a Secure Network Architecture **12.5 –** Centralize Network Authentication, Authorization, and Auditing (AAA) **12.6 –** Use of Secure Network Management and Communication Protocols	Implement a proxy server to centralize authentication, authorization, and auditing
13	Network Monitoring and Defence	**13.3 –** Deploy a Network Intrusion Detection Solution **13.4 –** Perform Traffic Filtering Between Network Segments **13.8 –** Deploy a Network Intrusion Prevention Solution **13.10 –** Perform Application Layer Filtering	Implement a Network Intrusion Detection System
18	Penetration Testing	**18.1 –** Establish and Maintain a Penetration Testing Program **18.2 –** Perform Periodic External Penetration Tests **18.3 –** Remediate Penetration Test Findings **18.5 –** Perform Periodic Internal Penetration Tests	Perform frequent penetration testing and implement Network Security Monitoring to detect incidents.

Table 5 - CIS Controls High-level implementation

Based on Table 4 and Table 5, the four security controls we will be implementing are as follows:

- Firewall and Packet Filtering
- Network Security Monitors
- Proxy Server
- Network Intrusion Detection System

4. Security Control 1 – Firewall

4.1. Purpose

Firewalls are a preventative security control; they allow for segmentation of a network. They can separate different parts of the network based on the levels of trust associated with them. Implementing a firewall in the network allows us to create a barrier between the trusted and the untrusted network. It also provides us with a choke point through which all traffic passes, allowing us to set up rules and make decisions on what traffic should/should not be permitted to pass. A stateful packet filter allows us to inspect and review packets at data link layers, network layer and transport layer. It also allows us to keep track of network connections.

4.2. Installation

For our network infrastructure, we will be using *netfilter* stateful packet filtering on Ubuntu 22.04 machines (10.0.0.1, 10.0.0.2). We will be implementing these through the user space tool, *iptables*.

For additional information and installation instructions on netfilter, refer https://www.netfilter.org/

a. Run the following command:

```
sudo apt-get update
```

b. To install the firewall, ensure the following packages are installing within linux. This can be done through the following command: `which [package name]`

```
1. ifconfig
2. iptables
3. arp
4. iptables-save
5. iptables-restore
```

If any of the packages are missing, they need to be installed via the package manager using the following command:

```
sudo apt-get install [package name]
```

c. Run the following command to flush any pre-existing firewall tables:

```
sudo iptables -t [table name] -F -v
```

```
1. filter
2. nat
3. mangle
4. raw
5. security
```

Once flushed, you can also view each of the tables to ensure their chains are empty using the following command:

```
sudo iptables -t [table name] -L -n -v -line-numbers
```

d. netfilter should now be installed and ready for the firewall to be implemented.

4.3. Implementation

Two firewalls need to be implemented within the network; these are as follows:

- Common-Firewall (10.0.0.1)

- Firewall-Internal (10.0.0.2)

The common firewall is the shared firewall linked with the router through Port 1. Common-Firewall can be installed between DMZ-Switch Port 1, Router Port 1, and the Internet. This firewall will have all traffic entering the network flowing through it. It will also be filtering traffic for the DMZ and the Clients network. Firewall-Internal can be installed between Server-Switch Port 1 and Core-Switch Port 2. This firewall will filter traffic entering the Servers network.

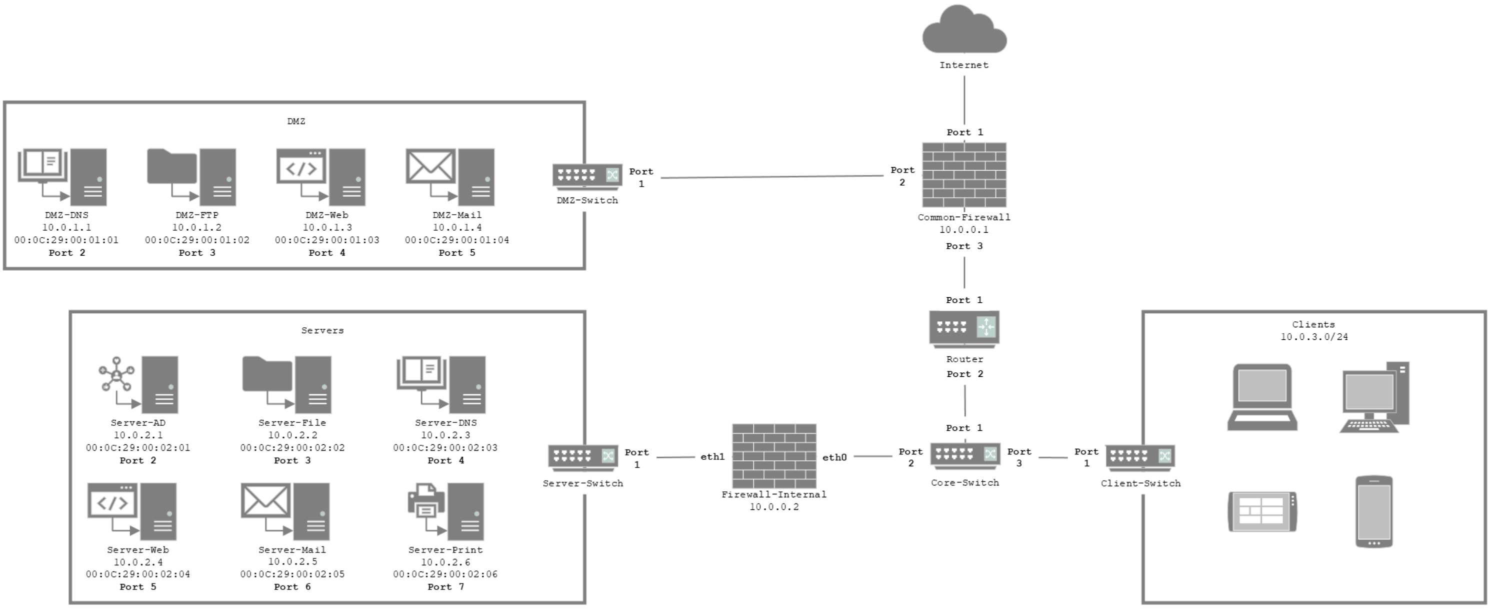

Figure 2 - Firewall Implementation

Firewall filters traffic based on a list of rules, they decide on either allowing traffic to pass through or to denying the traffic. We will be utilizing a stateful packet filtering firewall so that we can track the connection states and make decisions based on the status of the connections. Both these firewalls have common rules that block any inbound or outbound traffic that is not explicitly allowed, they should also allow all established and related inbound connections, allow established outbound connections, allow loopback connections, and allow the internal network to access the external network while also drop any invalid packets.

The following rules are common to both the firewalls and should be applied to both in their mentioned order:

No.	Action	Direction	Source	Destination	Protocol	Connection State
1	Deny	*	*:*	*:*	*	*
2	Allow	Inbound	*:*	*:*	*	Established, Related
3	Allow	Outbound	*:*	*:*	*	Established
4	Allow	Loopback	*:*	*:*	*	*
5	Allow	Forward	*:*	*:*	*	*
6	Deny	Inbound	*:*	*:*	*	Invalid

Table 6 - Shared Firewall Rules

These can be applied using the following commands:

```
sudo iptables –t filter –A INPUT –j DROP –v
```

```
       sudo iptables -t filter -A INPUT -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT

       sudo iptables -t filter -A OUTPUT -m conntrack --ctstate ESTABLISHED -j
ACCEPT
       sudo iptables -t filter -A INPUT -i lo -j ACCEPT

       sudo iptables -t filter -A OUTPUT -o lo -j ACCEPT

       sudo iptables -t filter -A FORWARD -j ACCEPT

       sudo iptables -t filter -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Common-Firewall (10.0.0.1)

Common-Firewall should have rules such that it would block any inbound traffic with the source IP as internal network and outbound traffic with the destination IP as the internal network. It should also allow inbound DNS traffic to the DMZ-DNS, inbound FTP traffic to DMZ-FTP, inbound web traffic to DMZ-Web.

The following rules should be applied to Common-Firewall in their mentioned order:

No.	Action	Direction	Source	Destination	Protocol	Connection State
1	Deny	Inbound	10.0.1.0/24	*:*	*	*
2	Deny	Outbound	*:*	10.0.1.0/24	*	*
3	Allow	Inbound	*:*	10.0.1.1:53	*	New, Established
4	Allow	Inbound	*:*	10.0.1.2:21	TCP	New, Established
5	Allow	Inbound	*:*	10.0.1.3:80	TCP	New, Established
6	Allow	Inbound	*:*	10.0.1.3:443	TCP	New, Established
7	Allow	Inbound	*:*	10.0.1.4:25	TCP	New, Established

Table 7 – Common-Firewall Rules

These can be applied using the following commands:

```
       sudo iptables -t filter -A INPUT -s 10.0.1.0/24 -j DROP

       sudo iptables -t filter -A OUTPUT -d 10.0.1.0/24 -j DROP

       sudo iptables -t filter -A INPUT -p udp -d 10.0.1.1 --dport 53 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

       sudo iptables -t filter -A INPUT -p tcp -d 10.0.1.1 --dport 53 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

       sudo iptables -t filter -A INPUT -p tcp -d 10.0.1.2 -dport 21 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

       sudo iptables -t filter -A INPUT -p tcp -d 10.0.1.3 -dport 80 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

       sudo iptables -t filter -A INPUT -p tcp -d 10.0.1.3 -dport 443 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

       sudo iptables -t filter -A INPUT -p tcp -d 10.0.1.4 -dport 25 -m
conntrack -ctstate NEW,ESTABLISHED -j ACCEPT
```

We do not need to configure outbound rules for each service since we configured the common rules to allow outbound connections using stateful packet filtering as mentioned in Table 6.

Firewall-Internal (10.0.0.2)

Firewall-Internal should have rules such that it would block any inbound traffic with the source IP as internal network and outbound traffic with the destination IP as the internal network. It should also allow inbound DNS traffic to the Server-DNS, inbound FTP traffic to Server-File, inbound web traffic to Server-Web only from the DMZ network and the Clients network.

The following rules should be applied to Firewall-Internal in their mentioned order:

No.	Action	Direction	Source	Destination	Protocol	Connection State
1	Deny	Inbound	10.0.2.0/24:*	*:*	*	*
2	Deny	Outbound	*:*	10.0.2.0/24	*	*
3	Allow	Inbound	10.0.1.0/24:*	10.0.2.3:53	*	New, Established
4	Allow	Inbound	10.0.3.0/24:*	10.0.2.3:53	*	New, Established
5	Allow	Inbound	10.0.1.0/24:*	10.0.2.2:21	TCP	New, Established
6	Allow	Inbound	10.0.3.0/24:*	10.0.2.2:21	TCP	New, Established
7	Allow	Inbound	10.0.1.0/24:*	10.0.2.4:80	TCP	New, Established
8	Allow	Inbound	10.0.3.0/24:*	10.0.2.4:80	TCP	New, Established
9	Allow	Inbound	10.0.1.0/24:*	10.0.2.4:443	TCP	New, Established
10	Allow	Inbound	10.0.3.0/24:*	10.0.2.4:443	TCP	New, Established
11	Allow	Inbound	10.0.1.0/24:*	10.0.2.5:25	TCP	New, Established
12	Allow	Inbound	10.0.3.0/24:*	10.0.2.5:25	TCP	New, Established

Table 8 - Firewall-Internal Rules

These can be applied using the following commands:

```
        sudo iptables -t filter -A INPUT -s 10.0.2.0/24 -j DROP

        sudo iptables -t filter -A OUTPUT -d 10.0.2.0/24 -j DROP

        sudo iptables -t filter -A INPUT -p udp -s 10.0.1.0/24 -d 10.0.2.3 --
dport 53 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p udp -s 10.0.3.0/24 -d 10.0.2.3 --
dport 53 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.1.0/24 -d 10.0.2.3 --
dport 53 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.3.0/24 -d 10.0.2.3 --
dport 53 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.1.0/24 -d 10.0.2.2 --
dport 21 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.3.0/24 -d 10.0.2.2 --
dport 21 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.1.0/24 -d 10.0.2.4 --
dport 80 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.3.0/24 -d 10.0.2.4 --
dport 80 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.1.0/24 -d 10.0.2.4 --
dport 443 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.3.0/24 -d 10.0.2.4 --
dport 443 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT
```

```
        sudo iptables -t filter -A INPUT -p tcp -s 10.0.1.0/24 -d 10.0.2.5 --
dport 25 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT

        sudo iptables -t filter -A INPUT -p tcp -s 10.0.3.0/24 -d 10.0.2.5 --
dport 25 -m conntrack -ctstate NEW,ESTABLISHED -j ACCEPT
```

Firewall rules for the AD Server (10.0.2.1), and Print Server (10.0.2.6) can be configured based on the ports and protocols used by the server. We do not need to configure outbound rules for each service since we configure the common rules to allow outbound connections using stateful packet filtering.

The firewall rules currently set can be viewed using the following command:

```
sudo iptables -L -n -v --line-numbers
```

Finally, the rules can be saved and restored using the following commands:

```
sudo iptables-save > ./rules

sudo iptables-restore < ./rules
```

Note: This is not an exhaustive list of all the firewall rules. Rules may need to be added or modified depending on the additional services running or installed on the network.

4.4. Justification

Firewalls fall under CIS Controls 4: Secure Configuration of Enterprise Assets and Software and are part of the following mitigations based on Table 2:

a. M1030 - Network Segmentation
b. M1031 - Network Intrusion Prevention
c. M1035 - Limit Access to Resource Over Network
d. M1037 - Filter Network Traffic
e. M1041 - Encrypt Sensitive Information

These are mitigations for the following threats outlined in the CTI report based on Table 1:

a. T1040 - Network Sniffing
b. T1046 - Network Service Scanning
c. T1021.001 - Remote Services: Remote Desktop Protocol
d. T1210 - Exploitation of Remote Services
e. TA0011 - Command & Control
f. TA0010 - Exfiltration

Firewall allows us to separate the traffic based on the trust level of the servers and the devices within a network. They can detect and block unauthorized access and forged malicious traffic. They can block malicious traffic, thus preventing unauthorized network sniffers and scans (threats a, b). Since the topmost firewall rule blocks all traffic, it prevents any accidental remote services traffic from slipping out, any valid traffic needs to be explicitly allowed through the firewall for the service to work (threats c, d). The firewall also blocks any outbound malicious connections the attacker might want to set up for command and control or exfiltration from within the network (threats e, f).

5. Security Control 2 – Network Security Monitors

5.1. Purpose

Network Security monitors are a detective security control. They can identify incidents and find intruders before they get a chance to cause damage to the network. They passively observe and ingest network traffic and categorize each set of traffic data based on their properties and check for suspicious activities or threats. Network security monitors can inspect traffic from data link layer, network layer, transport layer, session layer, presentation layer and application layer.

5.2. Installation

For our network infrastructure, we will use *Zeek* as a network security monitor on an Ubuntu 22.04 machine (10.0.0.3).

For additional information and installation instructions on zeek, refer https://docs.zeek.org/en/master/

a. While Zeek can be installed through Docker images, binary packages, homebrew on MAC devices, port collection on FreeBSD or manually by building it from source. We will be using binary packages to install Zeek.

b. Run the following commands to add the relevant OBS package repository to our system:

```
      echo 'deb
http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04/ /' |
sudo tee /etc/apt/sources.list.d/security:zeek.list

      curl -fsSL
https://download.opensuse.org/repositories/security:zeek/xUbuntu_22.04/Release
.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/security_zeek.gpg >
/dev/null
```

c. Once added, use the following commands to install Zeek using the system's package manager:

```
sudo apt update

sudo apt install zeek
```

d. Zeek should now be installed, with its binary packages store in /opt/zeek directory.

e. Add Zeek binary path to PATH, using the following commands:

```
echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc

source ~/.bashrc
```

5.3. Implementation

A single node of Zeek running on needs to be implemented within the network. This can be connected through interface eth0 to the Core-Switch through a new port, Port 4. This would allow it access to all three of the networks within the infrastructure.

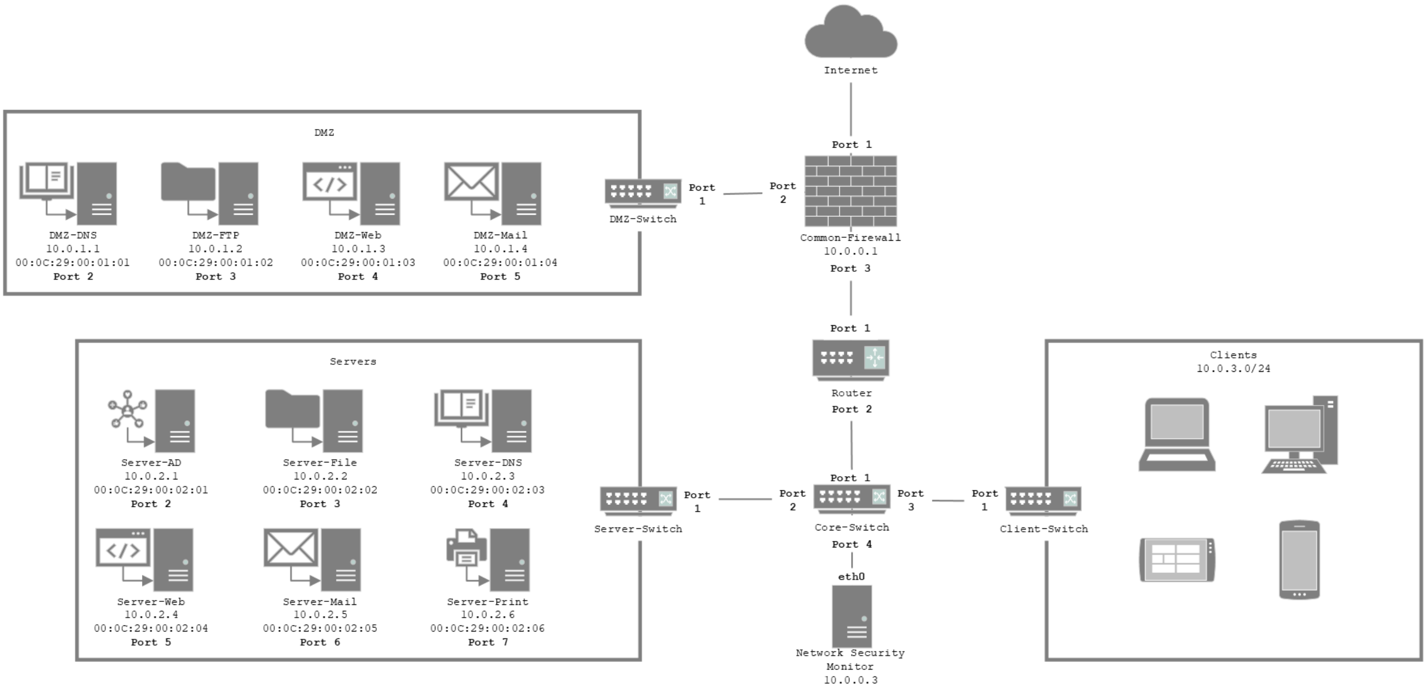

Figure 3 - NSM Implementation

We need to modify the configuration files for Zeek to fit our requirements. The configuration files are stored within /opt/zeek/etc and can be configured as follows:

a. **networks.cfg**

```
#List of local networks in CIDR notation, optionally followed by a
#descriptive tag.
#For example, "10.0.0.0/8" or "fe80::/64" are valid prefixes

10.0.1.0/24   DMZ IP space
10.0.2.0/24   Servers IP space
10.0.3.0/24   Clients IP space
```

This configuration will define the IP space for all the networks in our infrastructure.

b. node.cfg

Since we are using a standalone node, we do not need to change the configuration of this file, we can modify the interface name if required.

c. zeekctl.cfg

The default configuration for this file does not need to be changed, we can change the MailTo recipient address if setting up emails from Zeek.

Once configured, the following command can be run to perform various actions:

```
sudo /opt/zeek/bin/zeekctl [command]
```

List of commands that can be run:

1. check : Validate the configuration files
2. deploy : Start the Zeek instance
3. status : Check the status of the Zeek instance

Zeek will start analysing the traffic as per the default policy and will store the traffic within the `/opt/zeek/logs/current` directory.

Zeek's architecture is composed of two major components, the Event Engine which converts incoming traffic into higher level events, summarizing the traffic collected from the network and the Policy Script interpreter which adds context to the generated events and executes event handlers. Custom scripts can also be used to create alerts and detect specific attacks. These scripts are in /opt/zeek/share. These can be downloaded online or created and added onto Zeek to provide additional utility. The following is a project that uses Zeek to detect ATT&CK-based adversarial activity https://github.com/mitre-attack/bzar. It can be configured to fit the current environment and perform complex analytics for detecting ATT&CK like activity.

5.4. Justification

Network Security Monitors fall under CIS Controls 18: Penetration Testing and are part of the following mitigations based on Table 2:

a. M1016 – Vulnerability Scanning
b. M1028 – Operating System Configuration
c. M1037 – Filter Network Traffic
d. M1042 – Disable or Remove Feature or Program
e. M1047 – Audit
f. M1051 – Update Software

These are mitigations for the following threats outlined in the CTI report based on Table 1:

a. T1189 - Drive-by Compromise
b. T1046 - Network Service Scanning
c. T1021.001 - Remote Services: Remote Desktop Protocol
d. T1021.004 - Remote Services: SSH
e. T1210 - Exploitation of Remote Services
f. TA0011 - Command and Control
g. TA0010 – Exfiltration

Network Security Monitor allows us to collect and analyse traffic on specified networks. It is also able to categorize the traffic events based on conditions set by the policies and scripts being used. This allows NSM to identify any malicious traffic on the monitored network, alerting us to take the respective security measures. While they do not block any traffic, they are able to perform high-level complex traffic analysis and give us detailed insight into the traffic, this allows us to make informed decisions when dealing with Drive-by Compromise attacks, exploitation of RDP, SSH or other remote services (threats a, b, c, d, e). Network Security Monitors are also able to identify outbound connections and detect command and control and exfiltration attempts (threats f, g).

6. Security Control 3 – Proxy Server

6.1. Purpose

Proxy Servers are a preventative security control. They communicate with the internet on behalf of the host devices. These allow anonymity and can check if a session is legitimate or malicious. They protect against attacks on the IP space by acting as proxy for host devices and can also perform deep content inspection. Proxy servers can also perform access control and log all connections made from the clients to the server. Proxy servers are primarily located at the session layer.

6.2. Installation

For our network infrastructure, we will use *Dante,* a circuit-level SOCKS client and server deployed as a forward proxy for the clients' network. It requires a SOCKS server and a SOCKS client to be configured, we will be using Ubuntu 22.04 to install the SOCKS server (10.0.0.4). We will also be listing out the client installation for Dante SOCKS client on an Ubuntu 22.04 machine through Firefox, however the SOCKS Proxy can be utilized by other devices within the network by changing their respective proxy settings manually.

For additional information and installation instructions on Dante, refer https://www.inet.no/dante/

Dante Server Installation:

a. Run the following command to update package listings:

```
sudo apt update
```

b. To install Dante server, install the following packages on the server using the package manager with the following command:

```
1. dante-server
2. net-tools
```

```
sudo apt-get install [package name]
```

c. Check if Dante is installed successfully on the server using the following command:

```
sudo systemctl status danted.service
```

Dante Client Installation:

a. Run the following command to update package listings:

```
sudo apt update
```

b. To install Dante Server, install the following packages on the client using the package manager with the following command:

```
1. dante-client
2. net-tools
3. firefox
```

```
sudo apt-get install [package name]
```

Dante SOCKS client and server should now be installed the devices.

6.3. Implementation

A proxy server needs to be implemented for the Clients network to route all the client devices through the proxy server. This is done by implementing a screened subnet network configuration. We need to implement an additional router, “Internal-Router” before the Client-Switch. The Proxy-Server can connect to Port 3 of the Core-Switch and Port 1 of the Internal-Router. Port 2 of the Internal-Router can then connect to Port 1 of the Client-Switch. The subnet where the proxy server will reside is defined as the Screened network.

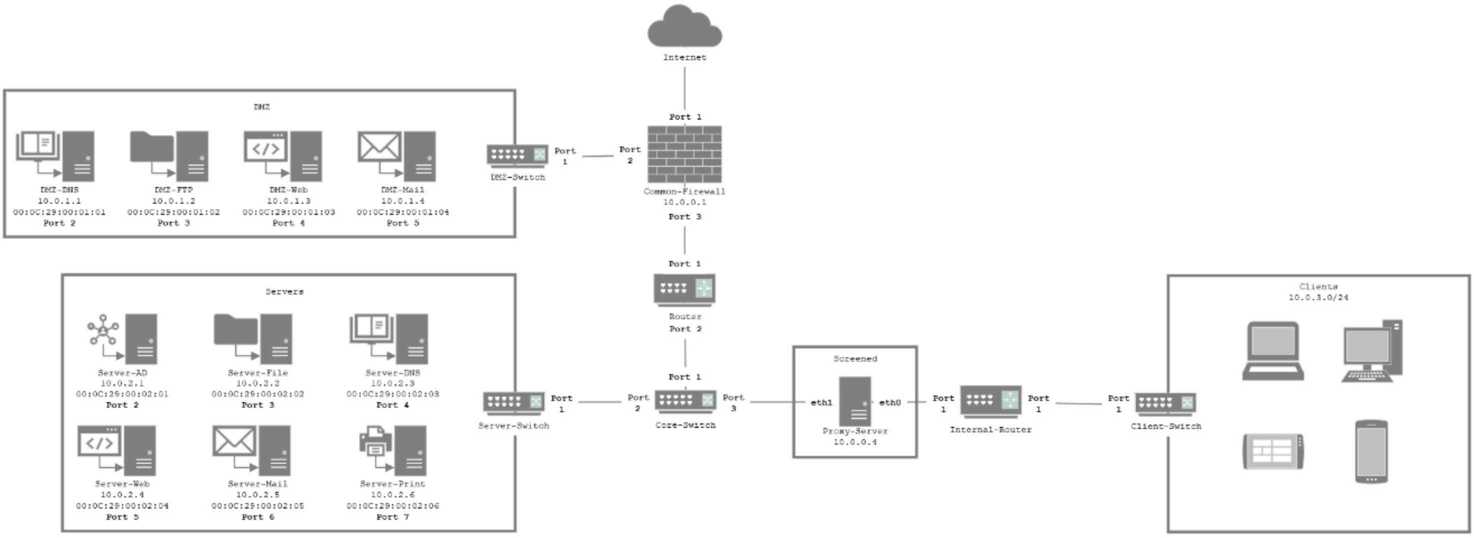

Figure 4 - Proxy Server Implementation

We will be considering interface eth0 as the internal network facing the clients, while interface eth1 will be considered as the external network facing the core switch.

We need to modify the configuration files for both the SOCKS server and the client such that they fit our requirements. These configurations are as follows:

1. **Dante Server:**

The configuration file for the proxy server is `/etc/danted.conf` which should have the following configuration:

```
errorlog: /var/log/sockd.errlog
logoutput: /var/log/sockd.log
debug: 4
user.privileged: root
user.unprivileged: nobody
# Internal Network
internal: 10.0.0.4 port = 1080
# External Network
external: eth1
# Allow connections from the Clients network (10.0.3.0/24)
client pass {
       from: 10.0.3.0/24 to: 0.0.0.0/0
       log: error # connect disconnect
}
socks pass {
       from: 0.0.0.0/0 to: 0.0.0.0/0
}
```

The above configuration will ensure that the Dante server will log the connections to `/var/log/sockd.log` and errors to `/var/log/sockd.errlog`. It also allows dante to have root permissions. The internal network is defined as 10.0.0.4:1080 which will be the proxy server, while the external network is eth1. The configuration also allows clients from 10.0.3.0/24 to connect to the server.

We also need to ensure that port 1080 is open on the proxy server and the Internal router is set up properly such that traffic can pass from the Clients network to the screened network. Once configured, restart the dante server with the new configuration changes using the following command:

```
sudo systemctl restart danted.service
```

2. **Dante Client:**

The configuration file for a proxy client is `/etc/dante.conf` which should have the following configuration:

```
errorlog: socks.errlog
logoutput: socks.log
debug: 4

#Route to SOCKS server which supports SOCKS version 5
route {
      from: 0.0.0.0/0 to: 0.0.0.0/0 via: 10.0.0.4 port = 1080
      proxyprotocol: socks_v5
      method: none
}
```

The above configuration will ensure that the dante client will log the connections to socks.log and errors to `socks.errlog`. The route that the client takes is through the dante server at 10.0.0.4:1080 using only SOCKS v5 protocol.

Within the Firefox Web Browser, change the proxy settings to connect to the proxy server. This can be done using the following steps:

a. Open Firefox "Connection Settings"
b. Select "Manual Proxy Configuration"
c. Enter "10.0.0.4" in the "SOCKS Host" field
d. Enter "1080" in the "Port" field.
e. Select "SOCKS v5"

All the client traffic should now be passing via the proxy server instead of directly through the client devices.

6.4. Justification

Proxy Servers fall under CIS Controls 12: Network Infrastructure Management and are part of the following mitigations based on Table 2:

a. M1018 – User Account Management
b. M1026 – Privileged Account Management
c. M1030 - Network Segmentation
d. M1035 - Limit Access to Resource Over Network
e. M1051 – Update Software

These are mitigations for the following threats outlined in the CTI report based on Table 1:

a. T1189 - Drive-by Compromise
b. T1046 - Network Service Scanning
c. T1021.001 - Remote Services: Remote Desktop Protocol
d. T1021.004 - Remote Services: SSH
e. T1210 - Exploitation of Remote Services
f. TA0011 - Command and Control
g. TA0010 - Exfiltration

Proxy Server allows us to communicate from the client network to the internet through the proxy server. The implemented screened subnet separates the exterior router and the interior router providing us with an additional layer of protection for the clients. This allows greater visibility into the traffic and provides additional logging capabilities. The internal router is also able to limit the traffic coming from the proxy server and it can detect and prevent any drive-by attacks, network scanning and exploitation of remote services by an attacker (threats a, b, c, d, e). This also makes it difficult for an attacker to set up command and control and exfiltration due to the multiple routers and all the traffic flowing through a heavily monitored proxy server (threats f, g).

7. Security Control 4 – Network IDS

7.1. Purpose

Network Intrusion Detection Systems are a detect security control. They monitor the traffic flowing through the network and can alert us if they detect any suspicious events and activities. They can also be used to sniff and log flowing packets in promiscuous mode. An IDS monitors all the network packets and works on data link layer, network layer, transport layer, session layer, presentation layer and application layer.

7.2. Installation

For our network infrastructure, we will use Snort, an open-source Network Intrusion Detection system. Snort will allow us to set up rules and alerts to monitor traffic on the network. Snort will be installed on an Ubuntu 22.04 machine (10.0.0.5).

For additional information and installation instructions on Snort, refer https://www.snort.org/documents#OfficialDocumentation

a. Run the following command to update package listings:

```
sudo apt update
```

b. To install snort, ensure the following packages are installing within linux. This can be done through the following command: `which [package name]`

```
1. gcc
2. libpcre3-dev
3. zlib1g-dev
4. libluajit-5.1.dev
5. libpcap-dev
6. openssl
7. libssl-dev
8. libnghttp2-dev
9. libdumbnet-dev
10. bison
11. flex
12. libdnet
13. autoconf
14. libtool
```

If any of the packages are missing, they need to be installed via the package manager using the following command:

```
sudo apt-get install [package name]
```

c. Use the following commands to install snort using the package manager:

```
sudo apt-get install snort
```

d. While asking for interface(s) to listen on, select `eth0`.

e. Select the local network address range as `10.0.2.0/24, 10.0.3.0/24`.

f. Snort should now be installed on the server machine.

7.3. Implementation

The Network IDS can be implemented on for the Servers network and the Clients network. Snort running on Ubuntu 22.04 (10.0.0.5) can be connected to the Core-Switch through a new port, Port 5 through eth0. This would allow it access to the two internal networks within the infrastructure.

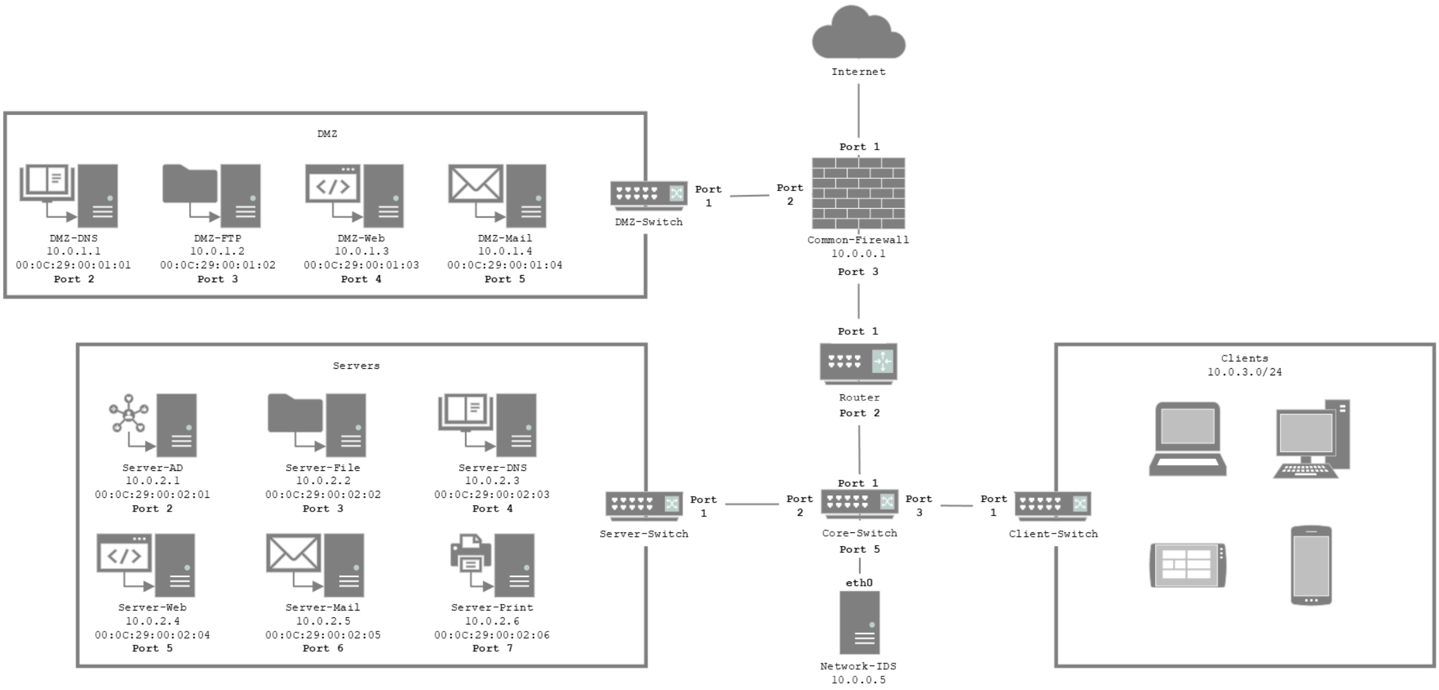

Figure 5 - Network IDS Implementation

We need to ensure that the server's network interface card is set to promiscuous mode so that it can monitor all traffic flowing through the network. This is done using the following command:

```
sudo ip link set eth1 promisc on
```

Next, download snort community rules, extract, and copy them into the rules folder in `/etc/snort/rules` using the following commands:

```
wget https://www.snort.org/downloads/community/community-rules.tar.gz -
O /etc/snort/rules/community.tar.gz

sudo tar -xvf /etc/snort/rules/community.tar.gz

sudo cp community-rules/* /etc/snort/rules
```

We will modify the configuration files for Snort to fit our requirements. The configuration files are stored within `/etc/snort` and can be configured as follows:

a. `snort.conf`

Modify the following commands within the configuration file, do not change the commands not included below.

```
ipvar HOME_NET 10.0.2.0/24, 10.0.3.0/24
ipvar EXTERNAL_NET !$HOME_NET
ipvar DNS_SERVERS 10.0.2.3/32
ipvar HTTP_SERVERS 10.0.2.4/32
ipvar FTP_SERVERS 10.0.2.2/32
ipvar SMTP_SERVERS 10.0.2.5/32
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules
```

Note: Additional servers can be configured within the configuration file by adding them next to the current servers separated by ','.

We can validate the snort configuration using the following command:

```
sudo snort -T -c /etc/snort/snort.conf
```

Local rules can also be added to snort by creating the /etc/snort/rules/local.rules file. The following are a few rules that should be added to the local.rules file:

Action	Protocol	Source	Destination	Option
alert	TCP	$HOME_NET:any	any:any	Since the Administrator account in windows machines should never be logged through remotely, we can set up a rule to alert us if we see "C:\Users\Administrator" as potential command shell access. Converting this into hex gives us "43 3A 5C 55 73 65 72 73 5C 41 64 6D 69 6E 69 73 74 72 61 74 6F 72"
alert	TCP	$HOME_NET:any	any:any	Since the root account should never be logged through remotely, we can set up a rule to alert us if we see "root@" as potential root shell access. Converting this into hex gives us "72 6F 6F 74 40"
alert	TCP	$EXTERNAL_NET:any	$HOME_NET:any	If we see a .exe file being transferred from the external network to the internal network, this could indicate a potential malicious file.
alert	TCP	10.0.1.0/24:any	$HOME_NET:any	If we see any traffic coming from the DMZ network to the internal network or vice versa, that could indicate some suspicious activity.
alert	TCP	any:any	$HOME_NET:any	If we see over 70 TCP SYN or SYN-ACK messages on a device in a time frame of 10 seconds within the internal networks, we can set up a rule to alert us as a potential TCP SYN Flood.

Table 9 - Snort Custom Rules

These rules can be added to snort by adding the following commands to `/etc/snort/rules/local.rules`:

```
alert tcp $HOME_NET any -> any (msg:”Command Shell Access”;
content:”|43 3A 5C 55 73 65 72 73 5C 41 64 6D 69 6E 69 73 74 72 61
74 6F 72|”; sid:1000001; rev:1;)

alert tcp $HOME_NET any -> any (msg:”Command Shell Access”;
content:”|72 6F 6F 74 40|”; sid:1000002; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:”EXE file
detected”; file_type: EXE; sid:1000003; rev:1;)

alert tcp 10.0.1.0/24 any <> $HOME_NET any (msg:”Communicating
with DMZ Network”; sid:1000004; rev:1;)

alert tcp any any -> $HOME_NET any (msg:”TCP SYN Flood”; flags:!A;
flow:stateless; detection_filter:track by_dst, count:70, seconds
10; sid:1000005; rev:1;)
```

Snort can detect malicious traffic by using both signature matching (looking for a pattern in the network traffic) or through heuristic matching (looking for anomalies in the network traffic). The first four rules follow a signature approach, while the last rule follows a heuristic approach.

Finally, we can run Snort using the following command:

```
sudo snort -A console -c /etc/snort/snort.conf -l /var/log/snort
```

This command will send all the alerts to the console, it will use the configurations set in the `/etc/snort/snort.conf` file and log all events to `/var/log/snort` directory.

Snort architecture is composed of the five components, the packet decoder which pulls packets from the network interface and prepares them to be pre-processed, the pre-processor which detects anomalies in the packet headers and defragments the packets, the detection engine which detects any intrusion activity based on a set of rules, the logging and alerting system which logs traffic as text files and the output modules which can be used to control the output generated by the logging and alerting system.

7.4. Justification

Network IDS falls under CIS Controls 13: Network Monitoring and Defence and are part of the following mitigations based on Table 2:

a. M1030 – Network Segmentation
b. M1031 – Network Intrusion Prevention
c. M1035 - Limit Access to Resource Over Network
d. M1037 – Filter Network Traffic
e. M1050 – Exploit Protection

These are mitigations for the following threats outlined in the CTI report based on Table 1:

a. T1189 - Drive-by Compromise
b. T1046 - Network Service Scanning
c. T1021.001 - Remote Services: Remote Desktop Protocol
d. T1210 - Exploitation of Remote Services
e. TA0011 - Command and Control
f. TA0010 - Exfiltration

Snort uses the configured rules to identify malicious traffic within the network and sends alerts if it sees any malicious behaviour. This allows us to quickly detect and defend against any attacks on the network. Snort will be able to detect any network scan attempts, administrative or root shell usage and any anomalous network traffic (threats a, b). We are also using the large community ruleset which can identify common malware used for drive-by compromise and exploitation of remote services (threats c, d). Snort can also detect command and control and data exfiltration attempts through its use of the installed ruleset (threats e, f).