|  |
| --- |
| Team 14 |
|  |

# Memorandum

To: Management

From: Team 14

Date: February 18, 2023

Subject: Inject Name

In an effort to be proactive about protecting our sensitive data and systems, we have implemented a strict firewall policy. This policy limits inbound and outbound network traffic to only what is strictly necessary for daily operations. By restricting traffic, we can reduce the risk of security breaches and prevent unauthorized access to our network. In addition to limiting inbound and outbound traffic, we are limiting traffic between the user, internal, and public network segments in an effort to make lateral movement through the network more difficult in case one system is compromised. The following image and table provide an in-depth view of our current firewall security policy and why we have made the decision to use this rule set.

The firewall is configured to limit traffic based on a combination of applications, ports, and IP address. Application filtering work by examining the network traffic and ensuring that the traffic matches typical network activity for that application. When filtering by application, the “application-default” service, which limits traffic to the typical ports used for that service. Applications running on non-standard ports explicitly allow that port to be used. IP address and port filtering work by looking at source and destination IP addresses, and what port is being used to filter traffic.

The following figures show how our rules are configured, along with a brief description on why that rule is important. Feel free to respond with any questions.

Sincerely,

Team 14

Image 1: Screenshot of Palo Alto web interface showing firewall rules

Table 1: Firewall rule explanations and justifications

Note: Highlighted rules are disabled. A rule may be disabled to disallow access to the server, while still having the rule available to put into production quickly.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rule Name | Source | Destination | Application | Service/Ports | Action | Justification |
| Allow Ping | Any | Any | Ping | application-default | Allow | Allow ping for all devices |
| Block Bad IPs In | Suspected malicious IP addresses | Any | Any | Any | Block | Block malicious IP address from accessing our network |
| Block bad IPs Out | Any | Suspected malicious IP addresses | Any | Any | Block | Block internal resources from reaching out to malicious IPs |
| Ubuntu Web | Any | Any | Web-browsing | application-default | Allow | Allow inbound web requests to Ubuntu Web Server. |
| AD DNS In | Any | AD DNS local IP and NAT IP | DNS | application-Default | Allow | Allow inbound DNS requests to Active Directory |
| Centos  E-comm | Any | Centos local IP and NAT IP | Web-browsing | application-default | Allow | Allow inbound HTTP and HTTPS requests to e-comm server |
| Fedora Mail | Any | Fedora local IP and NAT IP | SMTP, POP3, IMAP | application-default | Allow | Allow POP3, SMTP, and IMAP to the mail server |
| Fedora AD Auth | Fedora local IP | AD local IP | LDAP | application-default | Allow | Allow the mail server to authenticate with Active Directory |
| Splunk Forwarder | Internal or User Segment | Splunk local IP | Splunk | application-default | Allow | Allow all servers to forward logs to the Splunk server |
| Debian DNS\_NTP | Any | Debian local and public IP | DNS, NTP | application-default | Allow | Allow incoming DNS and NTP requests to the Debian server |
| Default Egress Applications | Any | External Segment | Web-browsing, DNS, NTP | application-default | Allow | Allow permitted applications to make outbound requests |
| Default Egress Ports | Any | External Segment | Any | TCP 80, TCP 443 | Allow | Allow outbound requests from our network on permitted ports |
| intrazone-default | Any | Intrazone | Any | Any | Allow | Palo Alto default intrazone rule to allow all intrazone traffic |
| interzone-default | Any | Interzone | Any | Any | Block | Palo Alto default interzone rule to block all traffic between segments |