University of North Carolina DoE White Team

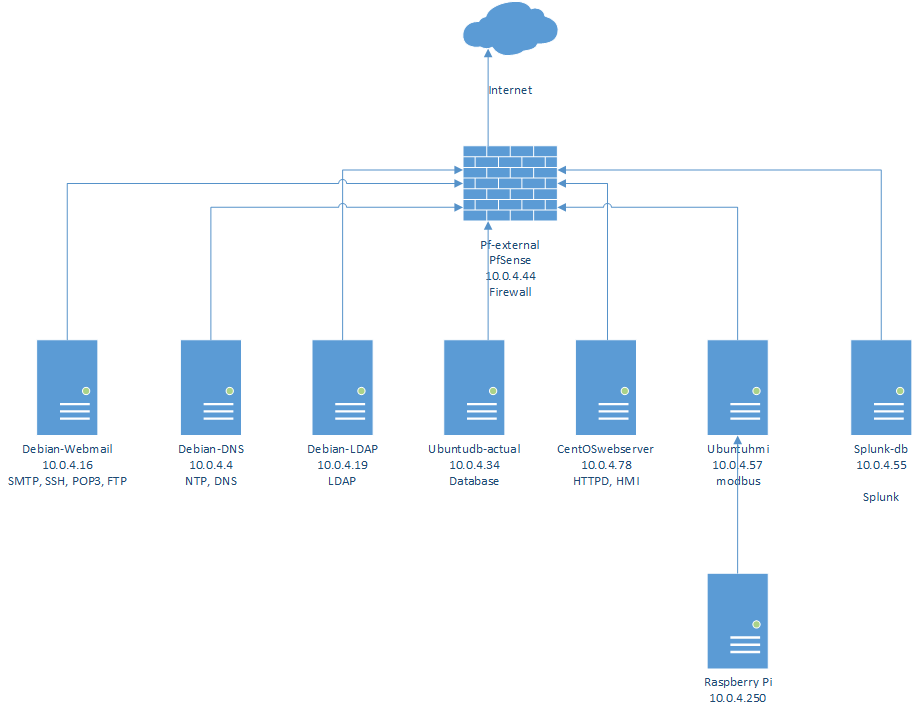


Network Documentation

|  |  |  |
| --- | --- | --- |
| VERSION | DATE | DESCRIPTION |
| 2 | 6 April 2018 | White team documentation for DoE competition |

**Table of Contents**

**Network Topology**

****

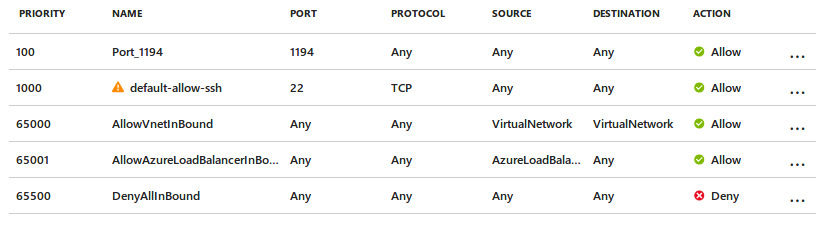
**Overview and Creativity Statement**

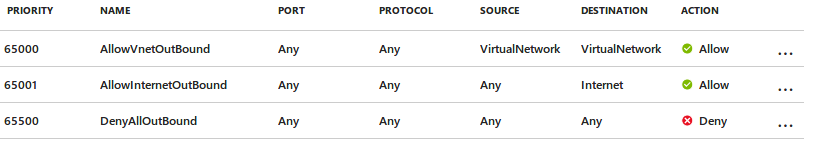
We took a multi-layered approach to defending the security of the network against intrusion. On the perimeter, we have a pfsense server that acts as a firewall and bastion host, performing port address translation. allowing only connections to authorized ports and protecting the network from attack. With it we have integrated the program, “snort,” which acts as an intrusion detection system, giving us early warning of any attacks on our network, so that we can respond in a timely manner. We have integrated the linux security module AppArmor as a Mandatory Access Control, to enact type enforcement controls on our files which will reduce the attack surface. We have also copied the provided servers to maintain as decoys in order to gather threat intelligence. We are forwarding our logs to a Splunk server to make it easy to discover anomalous traffic.

**VPN Network Interface**

Azure allows users to create network interfaces which limit incoming and outcoming connections for each virtual machine located on these servers. These are configured for each machine separately. The restrictions for the VPN are shown here:

Inbound port restrictions:

Outbound port restrictions:



**Services**

HTTP:

The server centoswebserver operates on port 80, allowing access to the wordpress website.

HTTPS:

Same server as HTTP.

LDAP:

Run on the Debian-LDAP used for adding or deleting users, or modifying their roles, and verifying users and holding permissions to access the cybati works logical controller.

NTP:

Run from Debian-DNS, and performs time service syncing all of the vms, mainly for the sake of security and logging.

SMTP:

Run on the Debian-webmail server for managing the help-desk requests.

IMAP:

Ran on the Debian-webmail for receiving emails for help-desk requests.

SNMP:

Like NTP makes sure all device are receiving data in an efficient manner.

SSH:

Run from the Debian-Webmail server, active at port 22 on all of our boxes. SSH is not enabled for root to deter brute forcing and to provide a more complete log. Enables a secure connection for authorized users.

FTP:

Run from the Debian-webmail server, this allows the administrator to update the documentation to the server and to ScoreBoard, and allows the user to download the updated documentation.

Modsecurity:

Run from the centoswebserver this software based firewall applies custom rules to protect the webserver, performing auditing, logging, and http hardening to provide protection to the Apache server running the Wordpress site.

Snort:

Performs IP monitoring and logging.

PF-external Information:

|  |  |
| --- | --- |
| Name | Pf-external |
| IP Address | 10.0.4.44 |
| Operating System | pfsense |
| Operation Level | Crucial |

Description:

This is the firewall for the network, the first line of defense for the network against intrusion.

It works as a Bastion Host to forward all the traffic to the appropriate servers.

Steps taken to secure:

Used a trusted base pfsense image.

Webserver Information:

|  |  |
| --- | --- |
| Name | Centoswebserver |
| IP Address | 10.0.4.78 |
| Operating System | CentOS |
| Operation Level | Crucial |

Description:

The CentOS webserver is setup to run the webserver, both HTTP and HTTPS, and directly interacts with the HMI server running the Raspberry Pi.

This also has a database which maintains the list of the amount of energy that has been purchased, and by whom.

Steps taken to secure:

root login is disabled; users must sudo.

User account passwords are changed.

mod\_security firewall installed and configured to secure webserver.

Python script serving / in the clear on port 20000 was removed.

mysql can only log in from the web server or localhost.

mysql password is changed.

guest and config user Locked.

Email Information:

|  |  |
| --- | --- |
| Name | Debian-webmail |
| IP Address | 10.0.4.16 |
| Operating System | Debian |
| Operation Level | Crucial |

Description:

The Debian-Webmail runs many of the crucial services needed to run the email client used by the company. It runs IMAP, SMTP, and POP3 for email services, and runs SSH for the network. It also runs the FTP so that documentation can be updated or downloaded by users and administrators.

Steps taken to secure:

What we did is not allow anyone to query users.

DNS Information:

|  |  |
| --- | --- |
| Name | Debian-DNS |
| IP Address | 10.0.4.4 |
| Operating System | Debian |
| Operation Level | Crucial |

Description:

Steps taken to secure:

Only allowed local user to use DNS lookup, disallowed zone transfer.

LDAP Information:

|  |  |
| --- | --- |
| Name | Debian-webmail |
| IP Address | 10.0.4.19 |
| Operating System | Debian |
| Operation Level | Crucial |

Description:

The Debian-LDAP runs the Active Directory for the network, allowing users to be created, updated, and deleted, and process changes in access. It is interacted with by the HMI to verify user permissions and allow them to access the web interface for Cybati.

Steps taken to secure:

Default.

HMI Information:

|  |  |
| --- | --- |
| Name | ubunthmi |
| IP Address | 10.0.4.57 |
| Operating System | Ubuntu |
| Operation Level | Crucial |

Description:

The HMI is the crucial link between the Raspberry PI running specialized hardware, and the rest of the network. It runs the modbus needed by Cybati and the Raspberry PI to properly function.

Steps taken to secure:

Default.

Raspberry Pi Information:

|  |  |
| --- | --- |
| Name | ubunthmi |
| IP Address | 10.0.4.250 |
| Operating System | Raspbian |
| Operation Level | Crucial |

Description:

The HMI is the crucial link between the Raspberry PI running specialized hardware, and the rest of the network. It runs the modbus needed by Cybati and the Raspberry PI to properly function.

Steps taken to secure:

Changed the password for user “pi” and “root”

Disabled root login.

Default.

Database Information:

|  |  |
| --- | --- |
| Name | ubuntudb-actual |
| IP Address | 10.0.4.34 |
| Operating System | Ubuntu |
| Operation Level | Crucial |

Description:

Steps taken to secure:

Removed database users that did not need access.

Installed mysql with mysql secure installation script.

Splunk Information:

|  |  |
| --- | --- |
| Name | splunk |
| IP Address | 10.0.4.55 |
| Operating System | Debian |
| Operation Level | Crucial |

Description:

It logs attacks, and protects the servers.

Steps taken to secure:

Allow only authorized access from the correct machines.