Additional Network Security Applications

Josh Lieberg

Submitted To: Tony Wan

Date Submitted: 12/10/2024

Date Due: 12/10/2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides a comprehensive overview of the Additional Network Security Applications project, which is the final project assigned to Computer Industries. This final project highlights a critical component for Computer Industries, simple but effective security measures. The project focuses on implementing three things: centralized authentication, certificate services, and a captive portal. This will enhance the overall user experience when accessing the infrastructure and make the network environments more accessible. These implementations are critical pieces to protect the sensitive information stored within Computer Industries.

The project's primary objectives include enhancing the previously configured pfSense and VyOS firewalls. The new configuration will focus on ensuring seamless operation of both firewalls in an isolated environment with the newly implemented security measures. Centralized authorization will play a huge role as all hosts will need to authenticate users to the active directory domain controller. Additionally, PAM and Kerberos hashes will be implemented on all the UNIX machines for authentication purposes.

The final component of this expansion is the implementation of a captive portal. The captive portal, added to the pfSense firewall and web configurator, will require users to authenticate with valid domain credentials. Computer Industries is adding this to their infrastructure to boost security measures on the guest environments. This project not only strengthens Computer Industries network security but also ensures a scalable, user friendly infrastructure that supports the company's commitment to protecting sensitive information and maintaining operational excellence.

BUSINESS CASE

Computer Industries is committed to boosting the overall security for its operational infrastructure. Implementing enhanced network security measures will support longer term growth if a future expansion is desired. The initiative to improve security measures aims at creating a secure, efficient, and fully scalable environment. The project involves implementing centralized authentication, certificate services, and a captive portal, which are critical in ensuring seamless and secure network operations. Figure 1 illustrates the network infrastructure prior to the implementation of these enhanced measures, highlighting the baseline setup that this project seeks to improve upon.

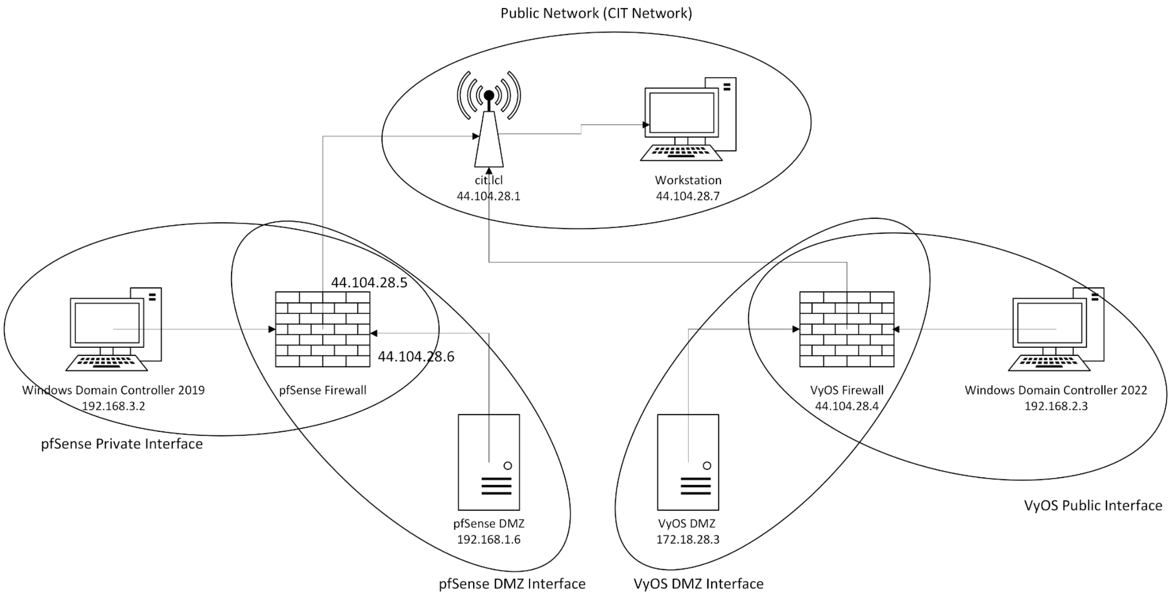

Figure 1: Logical Diagram

The solution that Computer Industries has decided to implement involves configuring two distinct network environments on both the pfSense and VyOS firewalls. Each segment will work independent of each other by managing their own environment to ensure segmentation and protection. The pfSense firewall will secure the traffic between three different zones: the internet, DMZ, and internal networks. Configuring the pfSense firewall this way ensures the sensitive services on the internal network remain secure while still being able to communicate with external services. The VyOS firewall will isolate the DMZ from the public network. Like the pfSense firewall, the VyOS firewall aims to secure the services on the internal network. These services include but are not limited to HTTP, FTP, and TFTP.

Additionally, centralized authentication will be implemented on the network environments. All hosts will be required to authenticate their users against the active directory located on the domain controller. UNIX systems will be configured to utilize PAM and Kerberos hashes. Having a centralized approach to user management will hopefully enhance the performance and security of Computer Industries infrastructure.

Lastly, a captive portal on the pfSense firewall and web configurator will be implemented. This new login portal will help manage access to the guest network by requiring users to authenticate with credentials provided by the domain controller. Adding a captive portal into the pfSense environment adds even more security which in turn will keep Computer Industries sensitive data protected.

This upgrade to Computer Industries security aligns with the goals and growth strategies implemented at the beginning of the year. By configuring and deploying two firewalls, implementing centralized authentication, and adding a captive portal to pfSense, Computer Industries upholds the standard for security in the IT landscape.

PROCEDURES

This procedure section goes phase by phase for the objectives completed during lab two, Microsoft Windows Administration. The troubleshooting techniques used can be found in Appendix A. In this section, the **buttons** used will be in bold, typed in computer instructions are in `Courier New`, *options* selected/pressed will be italicized, and steps requiring menu navigation will be represented by the pipe symbol. In rare occurrences, there are sometimes *options* interpreted as a **button**, which is represented by both italicized and bolded ***words***.

Table 1. Formatting Key

Representation	Format in Report
Button	**Button**
Options	*Options*
Text Entered in Computer	`Courier Text`
Menu Navigation	*Start* | *Programs* | *MS Office* | *Word*

Configuring Active Directory for VyOS Authentication

The Active Directory Domain Controller needs to be configured to allow the authentication from the VyOS router. This allows domain users to be able to log into the router itself. The following procedures are from start to finish.

1. Opened Private B Domain Controller
2. Opened *Server Manager* | *Tools* | *Network Policy Server* | *RADIUS Clients and Servers*
3. Right clicked *RADIUS Clients* and then selected **New**
4. Entered `VyOS Router` as the friendly name
5. Entered `44.104.28.4` for the IP of the router
6. Typed `group28key` as the shared secret
7. Re-entered the secret key
8. Selected **OK**
9. Repeated steps 2-8 on Private A Domain Controller and entered `PfSense` as the friendly name and an IP address of `44.104.28.5`

Joined Alma Linux Machines to the Domain

The Alma Linux machines were joined to the domain in order to allow for the authentication of domain users. This allows for any user with domain credentials to be able to log into those machines. The following procedures are from start to finish.

1. Opened the Alma Linux machine on the VyOS side of the network
2. Typed `sudo apt update`
3. Typed `sudo apt upgrade`
4. Entered `sudo nano /etc/resolv.conf`

5. Entered the DNS server as `192.168.2.3`
6. Saved the file
7. Typed `sudo dnf install realmd sssd adcli krb5-workstation samba samba-common oddjob oddjob-mkhomedir -y`
8. Entered `y` when prompted
9. Typed `sudo realm join –user=Adminstrator private.lcl` to join the machine to the domain
10. Repeated steps 2-9 on the pfSense Alma Linux machine but entered `192.168.3.2` as the DNS server

Created the Captive Portal Network

The captive portal network allows network administrators to control who is able to access the internet while utilizing those machines. The following procedures are from start to finish.

1. Migrated to vSphere
2. Selected the Port Groups section
3. Right clicked *CNIT455G28 Switch* | *Distributed Port Group* | *New Distributed Port Group*
4. Entered `Captive Guest Network` as the name
5. Selected **Next** | **Next** | **Finish**

Create the Captive Portal

The captive portal was created to allow domain users to connect to allowed sites on the internet while using machines located on that network. The following procedures are from start to finish.

1. Migrated to the pfSense web configurator
2. Selected *Services* | *Captive Portal* | **Add**
3. Entered `Captive Portal` as the name and selected **Save & Continue**
4. Selected *Enable Captive Portal*
5. Selected *OPT2* as the interface, as that is the interface of the captive network
6. Under Authentication, selected *Use an Authentication backend*
7. Entered the RADIUS server located on Private A Domain Controller as the Authentication Server
8. Selected **Save**

RESULTS

The team at Computer Industries has successfully implemented the new network architecture that aims to boost overall security. The new architecture now hosts a safe, efficient, and is also scalable. Centralized authentication, certificate services, and a captive portal are now implemented in the network architecture. Figure 2 below depicts the newly improved network infrastructure after implementing the necessary parts to the enhancement project. The Windows 10 Guest Client is now a separate interface from the pfSense firewall.

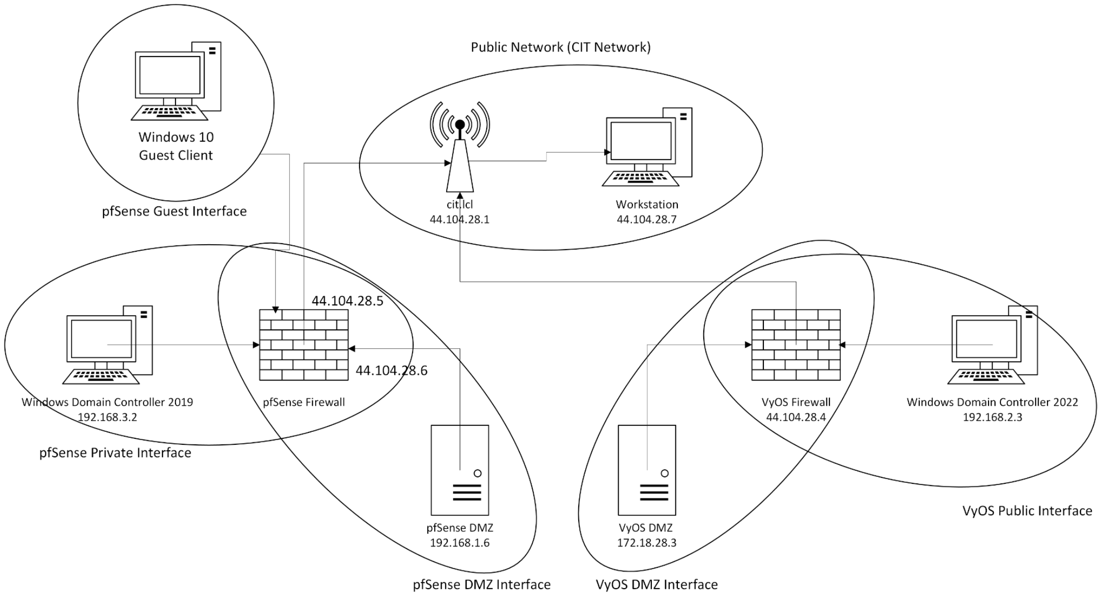

Figure 2: Logical Diagram

The newly implemented Windows 10 guest client serves as a captive portal interface, requiring users to authenticate to the Private A Domain Controller on the pfSense side. This captive portal solution enhances security for the pfSense network segment. The UNIX machines were also set up to use PAM and Kerberos to authenticate to their respective Active Directory domain controllers. By creating the newly improved network infrastructure, the team at Computer Industries now has a more secure and efficient network with robust authentication and access control.

CONCLUSIONS AND RECOMMENDATIONS

All objectives of this new enhancement project were successfully achieved. The network was divided into two environments, like how it was before. One side was managed by a pfSense firewall and the other by VyOS. Each environment was configured to ensure that hosts authenticated users through their respective Active Directory domain controllers. These were Private A and Private B, respectively.

All UNIX machines were successfully configured to use PAM and Kerberos for authentication, integrating them seamlessly with the AD domains. Doing so ensured centralized authentication, thus meeting the project requirements. On the other side, the pfSense firewall was configured to source users directly from the Active Directory domain. Doing so ensured secure access as well as provided centralized user management.

A new network segment was added on the pfSense side which hosted a Windows 10 workstation machine. This segment was secured using a captive portal solution on pfSense. To sign into the captive portal, the end user would have to sign in using valid domain authentication credentials to grant users access to other networks. Implementing a captive portal restricted access to authorized users only.

Recommendations

Recommendation One: Commit to enabling captive portal

To avoid accidentally locking out users, making sure captive portal configuration is all set and ready to go is crucial before you hit the save button. Creating a captive portal wrong can cost you a lot of time trying to fix it, so make sure the captive portal is ready to go. A ready to go captive portal will have Active Directory users readily configured as well as gateways in the captive portal settings.

Recommendation Two: Manage Time Better

The team at Computer Industries was given one week to complete this enhancement project. However, the team was not capable of achieving this in one week and was able to get a one week extension because of a holiday break. The team scrambled to complete this project after the break. This problem could have been mitigated if the team deployed better time management.

Recommendation Three: Test Thoroughly

Before finalizing and deploying any changes, the team at Computer Industries recommends conducting through testing all of the configurations before moving on. More often than not, the network would fail on devices after we moved on from them and started configuring other things. Doing so lead our attention away from the important things of this enhancement project.

BIBLIOGRAPHY

CIT (n.d.). *Lab Report Template*

How to configure captive portal on pfSense software?. Zenarmor. (2024, February 6). https://www.zenarmor.com/docs/network-security-tutorials/how-to-configure-captive-portal-on-pfsense

Join in active directory DOMAIN2023/03/08. *AlmaLinux 9 : Join in Active Directory Domain : Server World.* (n.d.). https://www.server-world.info/en/note?os=AlmaLinux_9&p=realmd

Rawles, P (n.d.). *CNIT 45500 Lab 4 - Additional Network Security Applications*

User management. *User Management - VyOS 1.3.x (equuleus) documentation.* (n.d.). https://docs.vyos.io/en/equuleus/configuration/system/login.html

APPENDIX A: PROBLEM SOLVING

Problem 1: Locked out of pfSense

Problem Description: After enabling the captive portal feature on the pfSEnse firewall, users trying to authenticate to the Active Directory domain encountered authentication failures when attempting to login. The issue persisted despite confirming that the Active Directory domain server was reachable and the configuration for the captive portal appeared to be sufficient. Furthermore, attempts to access the pfSense web interface for troubleshooting were unsuccessful, leaving the system in a locked out state.

Possible Solutions: One potential solution was to verify and reconfigure the captive portal settings to ensure compatibility with the newly implemented AD authentication. A second solution involved testing the connection between pfSense and the Active Directory server to confirm that they can communicate together. A third solution considered restarting the pfSense firewall or the entire device to resolve any temporary issues.

Attempted Solutions: The first solution was attempted by trying to access the pfSense console from other machines to review the captive portal settings. However, the system was locked-out by all attempts. The second solution involved using tools like LDAP testing from the active directory server, but no problems were detected. The final solution attempted was to restart pfSense entirely. However, restarting the firewall did not solve the problem.

Final Solution: None of the above solutions worked. Weirdly enough, disabling the web interface on pfSense and reenabling the web interface bypassed the captive portal for long enough to disable the captive portal. After configuring a proper gateway in the captive portal settings, the feature was turned on again and was fully functional.

Problem 2: Windows 10 network segment connectivity

Problem Description: After deploying a Windows 10 device on the newly implemented network segment from pfSense, network connectivity was proving to be difficult. The new device was unable to access any internet or ping any sort of gateway on the network. This issue was isolated to any device connected to the new network segment.

Possible Solutions: One potential solution was to verify the network configuration of the Windows 10 device. Ensuing that the network adapter was configured correctly is crucial to getting network access. Another solution involved testing browser settings for potential caching issues or misconfigured settings. If configured correctly, the device should be able to access the captive portal without network access. A third solution involved restarting both devices as well as reconfiguring the web interface on pfSense to ensure the settings specified were functional.

Attempted Solutions: The first solution was attempted by releasing and renewing the IP caching address on the Windows 10 device. The commands ran were `ipconfig /release` and `ipcfonfig /renew`. The device still could not access the network or ping anywhere. The second solution also ended in a deadend, as the browser could still not reach the captive portal address. Finally, the pfSense settings were reconfigured and the devices were restarted.

Final Solution: Restarting the pfSense machine fixed the persisting problem. However, this solution was a temporary solution and would not fix the problem permanently. After restarting the pfSense machine and waiting for the device to be on, the Windows 10 workstation on the new network segment would gain internet access for a brief period of time. In that period of time, the captive portal was accessed and signed into.

APPENDIX B: VIRTUAL MACHINE NETWORK SETTINGS CONFIGURATION

Appendix B gives the IP Address, Subnet mask, Default Gateway, Preferred DNS, Alternate DNS settings, and Domain Controller assignments for each VM computer. Appendix B also gives the IP address and Subnet mask of the interfaces attached to pfSense.

Table 1: Virtual Machine Networking Configuration Settings

PC/Interface	IP address	Subnet Mask	Gateway	Pref. DNS	Alt. DNS
pfDMZ	192.168.1.6	255.255.255.0	192.168.1.1	44.2.1.44	44.2.1.45
pfSense	44.104.28.5	255.255.255.0	192.168.1.1	192.168.1.5	192.168.2.2
privA	192.168.3.2	255.255.255.0	192.168.3.1	127.0.0.1	
privB	192.168.2.3	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45
VyOS	44.104.28.4	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45
VYosDMZ	172.18.28.3	255.255.255.0	172.18.28.1	44.2.1.44	44.2.1.45
WINDOWSPublic	44.104.28.7	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45
Metasploit	192.168.1.25	255.255.255.0	192.168.1.1	44.2.1.44	44.2.1.45
KaliVM	192.168.3.7	255.255.255.0	192.168.3.1	44.2.1.44	44.2.1.45

Additional Network Security Applications

UltimateLAMP	192.168.1.200	255.255.255.0	192.168.1.1	44.2.1.44	44.2.1.45
SecOnion	192.168.1.69	255.255.255.0	192.168.1.1	44.2.1.44	44.2.1.45

APPENDIX C: PFSENSE FIREWALL RULE CONFIGURATION

Table 1: WAN Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	IPv4 ICMP	*	*	*	*	*
Pass	IPv4 TCP/UDP	*	*	44.104.28.6	80	*
Pass	IPv4 TCP/UDP	*	*	44.104.28.6	20-21	*
Pass	IPv4 TCP/UDP	*	*	WAN address	80	*
Pass	IPv4 TCP/UDP	*	*	192.168.1.6	80	*
Pass	IPv4 TCP/UDP	*	*	192.168.1.6	20-21	*
Block	IPv4 *	*	*	*	*	*

Table 2: OpenVPN

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	IPv4 *	*	*	*	*	*

Table 3: OPT1 Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	*	*	*	OPT Address		*
Pass	IPv4 TCP	OPT1	*	LAN	*	*
Pass	IPv4 *	OPT1	*	*	*	*
Pass	IPv4 TCP/UDP	*	*	OPT1	21000-21999	*
Pass	IPv4 TCP/UDP	OPT1	*	*	53	*
Pass	IPv4 TCP/UDP	OPT1	*	*	80	*
Pass	IPv4 TCP/UDP	OPT1	*	*	443	*

Pass	IPv4 TCP/UDP	OPT1	*	*	20-21	*
Pass	IPv4 TCP/UDP	OPT1	*	*	*	*
Pass	IPv4 TCP/UDP	OPT1	*	*	123	*
Pass	IPv4 TCP/UDP	OPT1	*	*	25	*
Block	IPv4 *	*	*	*	*	*

Table 4: LAN Interface Rules

Action	Protocol	Source	Port	Destination	Port	Gateway
Pass	IPv4 *	*	*	LAN	*	*
Pass	IPv4 TCP	*	*	*	*	*
Pass	IPv4 *	*	*	*	*	*
Pass	IPv4 *	PRIVATE	*	*	*	*
Pass	IPv6 *	PRIVATE	*	*	*	*
Block	IPv4 *	*	*	*	*	*

Table 5: NAT Outbound Rules

Interface	Source	Port	Destination	Port	NAT Address	Port
WAN	192.168.1.6/32	*	*	*	44.104.28.6/32	*
WAN	192.168.3.0/24	*	WAN	*	WAN	*
WAN	192.168.3.0/24	*	*	*	44.104.28.6	*
WAN	192.168.1.0/24	*	WAN	*	WAN	*
WAN	192.168.1.0/24	*	*	*	44.104.28.6	*

Table 2: IPsec

Action	Protocol	Source	Port	Destination	Port	Gateway

Pass	IPv4	*	*	*	*	*	*

APPENDIX D: VyOS Config

```
group28@Router1# show
 firewall {
     global-options {
         all-ping enable
     }
     ipv4 {
         forward {
             filter {
                 rule 5 {
                     action jump
                     inbound-interface {
                         name eth0
                     }
                     jump-target site2site
                 }
             }
         }
         name one {
             rule 1 {
                 action reject
             }
         }
```

```
name site2site {
    default-action accept
}
name wan2lan {
    default-action drop
    rule 2 {
        action accept
        description "Allow established/related"
        state established
        state related
    }
    rule 10 {
        action accept
        destination {
            address 172.18.28.3
            port 80
        }
        protocol tcp
        source {
            address 44.104.28.0/24
        }
    }
    rule 20 {
```

```
  action accept
  destination {
    address 172.18.28.3
    port 69
  }
  protocol tcp
  source {
    address 44.104.28.0/24
  }
}
rule 30 {
  action accept
  destination {
    address 172.18.28.3
    port 20
  }
  protocol tcp
  source {
    address 44.104.28.0/24
  }
}
rule 40 {
  action accept
```

```
                destination {
                    address 172.18.28.3
                    port 21
                }
                protocol tcp
                source {
                    address 44.104.28.0/24
                }
            }
        }
    }
}
interfaces {
    ethernet eth0 {
        address 44.104.28.4/24
        description External
        hw-id 00:50:56:91:41:7f
    }
    ethernet eth1 {
        address 172.18.28.1/24
        description DMZ
        hw-id 00:50:56:91:2e:64
    }
    ethernet eth2 {
        address 192.168.2.1/24
        description "Private B"
        hw-id 00:50:56:91:81:62
        ip {
            enable-proxy-arp
        }
    }
    loopback lo {
    }
    tunnel tun0 {
        encapsulation gre
        remote 192.168.3.1
        source-address 192.168.2.1
    }
}
nat {
    destination {
        rule 20 {
            description "DNAT for Priv"
            destination {
                address 44.104.28.4
                port 80
            }
            inbound-interface {
                name eth0
            }
            protocol tcp
            translation {
                address 192.168.2.3
                port 80
            }
        }
    }
    source {
        rule 10 {
            outbound-interface {
                name eth0
            }
            source {
                address 172.18.28.0/24
            }
            translation {
                address masquerade
            }
        }
        rule 65 {
            destination {
                address 192.168.3.0/24
            }
            exclude
            outbound-interface {
                name eth0
            }
        }
        rule 110 {
            outbound-interface {
                name eth0
            }
            source {
                address 192.168.2.0/24
            }
            translation {
                address masquerade
            }
        }
    }
}
pki {
}
protocols {
    static {
        route 0.0.0.0/0 {
            next-hop 44.104.28.1 {
            }
        }
        route 192.168.1.0/24 {
            interface vtun0 {
            }
        }
        route 192.168.2.0/24 {
            next-hop 192.168.2.1 {
            }
        }
    }
}
service {
    ntp {
        allow-client {
            address 0.0.0.0/0
            address ::/0
        }
        server time1.vyos.net {
        }
        server time2.vyos.net {
        }
        server time3.vyos.net {
        }
    }
    ssh {
        listen-address 44.104.28.4
        port 22
    }
}
system {
    config-management {
        commit-revisions 100
    }
    conntrack {
        modules {
            ftp
            h323
            nfs
            pptp
            sip
            sqlnet
            tftp
        }
    }
    console {
        device ttyS0 {
            speed 115200
        }
    }
    host-name Router1
    login {
        radius {
            server 192.168.2.3 {
                key group28key
                port 1812
                timeout 5
            }
        }
        user group28 {
            authentication {
                encrypted-password
$6$rounds=656000$K03Cy4G03Ucf9iM8$jQ/EYjPCrGJaPFirFAlp6rdBOhb962ojShJve.x/yknL
MpWmwFBuVf0YDnPqyu49mBTH9DqF4ulS.hR0CkY2m/
```

```
            }
        }
        user vyos {
            authentication {
                encrypted-password
$6$QxPS.uk6mfo$9QBSo8u1FkH16gMyAVhus6fU3LOzvLR9Z9.82m3tiHFAxTtIkhaZSWssSg
zt4v4dGAL8rhVQxTg0oAG9/q11h/
                plaintext-password ""
            }
        }
    }
    name-server 44.2.1.44
    syslog {
        global {
            facility all {
                level info
            }
            facility local7 {
                level debug
            }
        }
    }
}
```

Additional Network Security Applications

[edit]