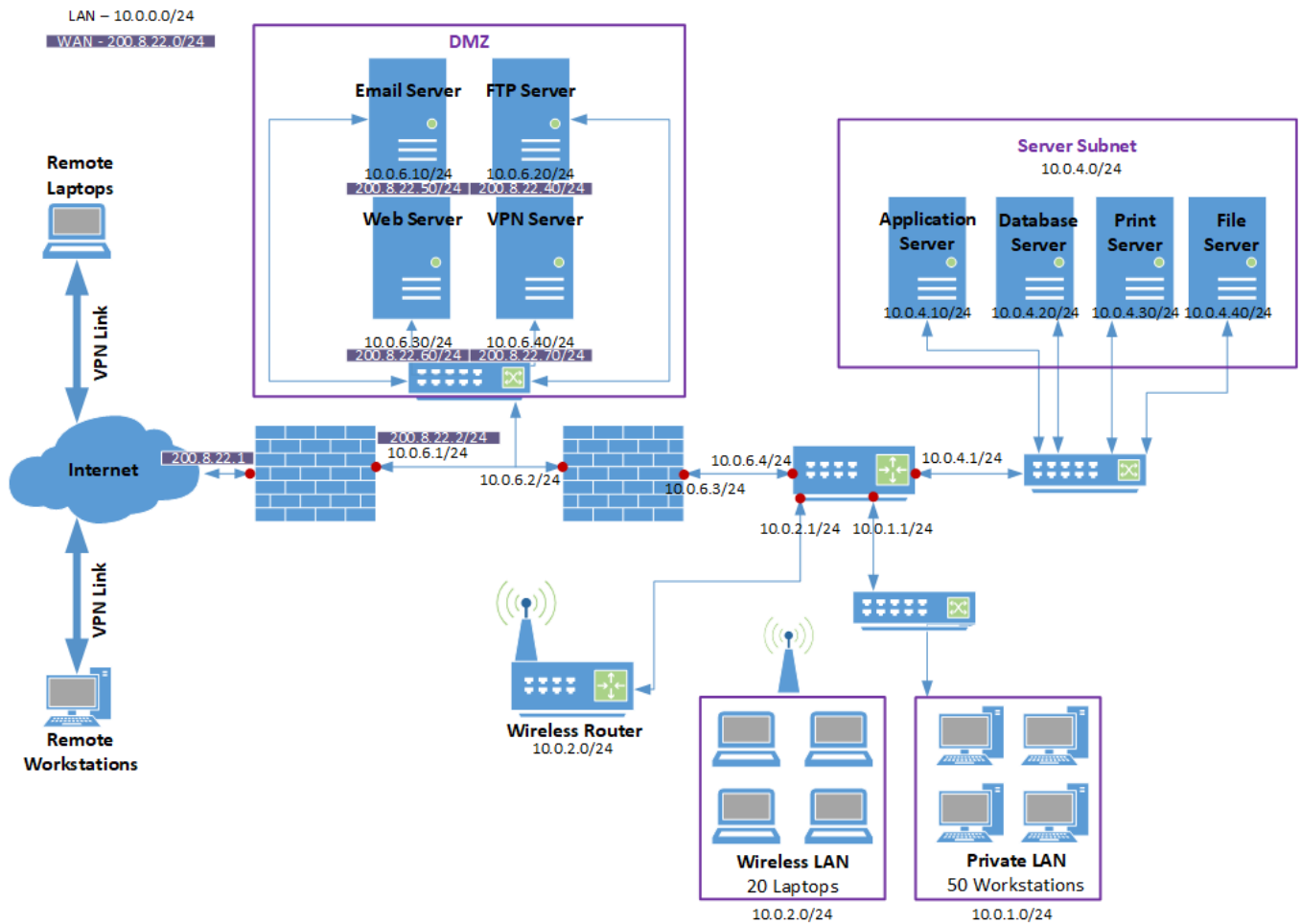


Network Security Design
May 2021

Task 1: Create a new network diagram clearly identifying and labeling all components of the network and their corresponding locations (with respect to each other). This should include existing and new components.



Task 2: Clearly show the location of the new components such as any web-facing servers and firewall/s. List all the new components, their role, dummy IPs and ports being used.

New Components	Role	Dummy IP/range		Ports Being Used (if any)	Comments
		WAN IP	LAN IP		
1 web-server	Hosts website	200.8.22.4	10.0.6.30	22, 80, 443	located in DMZ
1 email server	Manage email services	200.8.22.6	10.0.6.10	587, 465, 110	located in DMZ
1 web-facing secure FTP server	Uploading and downloading files	200.8.22.7	10.0.6.20	20, 21	located in DMZ
1 vpn server	Manage VPN services; needed for secure remote access	200.8.22.5	10.0.6.40	500, 5500, 1723	located in DMZ
1 internal wireless switch	Provides wireless network access for laptops		10.0.2.1		
20 laptops to be connected via wireless switch	Used for portable network connectivity		10.0.2.0/24		

Do the same for existing components:

Existing Components	Role	Dummy IP/range		Ports Being Used (if any)	Comments
		LAN IP			
50 workstations	n/a	10.0.1.0/24			
1 database server	Manages database	10.0.4.20/24		TCP 1433, 4022, 135, & TCP/UDP 1434	Typical ports to open for SQL server and associated database services
1 application server	Manages applications	10.0.4.10/24		389, 636, 15216200, 9401	Ports to open for Oracle application server
1 print server	Manages all printers on network	10.0.4.30/24		2501, 5001, 9100, 9101, 9102, 9600	Covers ports for typical printer manufacturers
1 file server	Manages files	10.0.4.40/24		TCP/UDP 135-139 & 445	Ports for file sharing and SMB communications

Task 3: Clearly define the firewall rule list using the format found in the pfSense Firewall Rules tab in the Excel file provided.

EXTERNAL FILTERING FIREWALL

Firewall Rules					Source IP Address				Destination IP Address				Port Range		Extra Options	
Action	Disabled	Interface	Address Family	Protocol	Invert	Type	Address	Subnet Mask	Invert	Type	Address	Subnet Mask	From	To	Log	Description
Deny		WAN	IPv4	TCP/UDP		any	200.8.22.0			any	any					Spoof prevention
Deny		WAN	IPv4	TCP/UDP		any	any			any	200.8.22.1					Blocks direct communication to firewall
Deny		WAN	IPv4	TCP/UDP		any	any			any	200.8.22.2					Blocks direct communication to firewall
Deny		WAN	IPv4	TCP/UDP		any	200.8.22.1			any	any					Blocks direct communication to firewall
Deny		WAN	IPv4	TCP/UDP		any	200.8.22.2			any	any					Blocks direct communication to firewall
Allow		WAN	IPv4	TCP/UDP		any	any			>1023	200.8.22.0		24			Allows for multiple web sessions
Allow		WAN	IPv4	TCP/UDP		any	any			25	200.8.22.8					Allows SMTP traffic to email server
Deny		WAN	IPv4	TCP/UDP		any	any			7	200.8.22.0		24			Blocks network pings
Deny		WAN	IPv4	TCP/UDP		any	any			23	200.8.22.0		24			Blocks Telnet access to all internal servers from public networks
Allow		WAN	IPv4	TCP/UDP		any	any			80	200.8.22.4					Allow HTTP to access web server
Allow		WAN	IPv4	TCP/UDP		any	any			443	200.8.22.4					Allow HTTPS to access web server
Allow		WAN	IPv4	TCP/UDP		any	any			21	200.8.22.7					Allow FTP traffic on FTP server
Allow		WAN	IPv4	TCP/UDP		any	any			21	200.8.22.7					Allow FTP traffic on FTP server
Allow		WAN	IPv4	UDP		any	any			500	200.8.22.5					Allow IKE on VPN server
Allow		WAN	IPv4	UDP		any	any			5500	200.8.22.5					Allow NAT-T to VPN server
Allow		WAN	IPv4	UDP		any	any			1701	200.8.22.5					Allow L2TP traffic
Deny		WAN	IPv4	TCP/UDP		any	any			any	any					Deny all else
Allow		DMZ	IPv4	TCP/UDP		any	200.8.22.11			any	200.8.22.0		24			Administrator access to any device
Deny		DMZ	IPv4	TCP/UDP		any	any			any	200.8.22.1					Deny access to by firewall
Deny		DMZ	IPv4	TCP/UDP		any	any			any	200.8.22.2					Deny access to by firewall
Deny		DMZ	IPv4	TCP/UDP		any	200.8.22.1			any	any					Deny access to by firewall
Deny		DMZ	IPv4	TCP/UDP		any	200.8.22.2			any	any					Deny access to by firewall
Allow		DMZ	IPv4	TCP/UDP		any	200.8.22.0			any	any					Allow outbound communication
Deny		DMZ	IPv4	TCP/UDP		any	any			any	any					Deny all

INTERNAL FILTERING FIREWALL

Firewall Rules					Source IP Address				Destination IP Address				Port Range		Extra Options	
Action	Disabled	Interface	Address Family	Protocol	Invert	Type	Address	Subnet Mask	Invert	Type	Address	Subnet Mask	From	To	Log	Description
Deny		DMZ2	IPv4	TCP/UDP		any	any			any	200.8.22.3					Block all internet from accessing firewall
Deny		DMZ2	IPv4	TCP/UDP		any	200.8.22.3			any	any					Blocks firewall from accessing internet
Allow		DMZ2	IPv4	TCP/UDP		any	any			>1023	200.8.22.0		24			Allows return traffic from multiple web sessions
Deny		DMZ2	IPv4	TCP/UDP		any	any			any	any					Deny all else
Deny		LAN	IPv4	TCP/UDP		any	any			any	200.8.22.3					Deny access to firewall
Deny		LAN	IPv4	TCP/UDP		any	200.8.22.3			any	any					Deny access from firewall
Allow		LAN	IPv4	TCP/UDP		any	any			>1023	10.0.4.0		24			Allow web multiple web sessions on 10.0.4.0
Allow		LAN	IPv4	TCP/UDP		any	any			>1023	10.0.2.0		24			Allow web multiple web sessions on 10.0.2.0
Allow		LAN	IPv4	TCP/UDP		any	any			>1023	10.0.1.0		24			Allow web multiple web sessions on 10.0.1.0
Allow		LAN	IPv4	TCP/UDP		any	10.0.0.0	24		any	any					Allow all outbound traffic from internal network
Deny		LAN	IPv4	TCP/UDP		any	any			any	any					Deny all else

Task 4: Create a few NAT rules. Clearly document the NAT rules required for any of the internet-facing servers.

Interface	Ext. Address	Protocol	Ext. Port Range	NAT IP	Local Port	Description
WAN	interface address	TCP/UDP	FROM: SMTP TO: SMTP	10.0.6.10	25	NAT allow SMTP to email server
WAN	interface address	TCP/UDP	FROM: HTTP TO: HTTP	10.0.6.30	80	NAT allow HTTP to web server
WAN	interface address	TCP/UDP	FROM: HTTPS TO: HTTPS	10.0.6.30	443	NAT allow HTTPS to web server
WAN	interface address	TCP/UDP	FROM: FTP TO: FTP	10.0.6.20	20	NAT allow FTP to FTP server
WAN	interface address	TCP/UDP	FROM: FTP TO: FTP	10.0.6.20	21	NAT allow FTP to FTP server
WAN	interface address	TCP/UDP	FROM: IKE TO: IKE	10.0.6.40	500	NAT allow IKE to VPN server
WAN	interface address	TCP/UDP	FROM: NAT-T TO: NAT-T	10.0.6.40	5500	NAT allow NAT-T to VPN server
WAN	interface address	TCP/UDP	FROM: L2TP TO: L2TP	10.0.6.40	1701	NAT allow L2TP to VPN server

Task 5: Once you have the network design figured out, list in detail how you would assess the security of the network.

- Conduct a simulated firewall test.
- Create a virtualized network environment using a virtualizing tool such as VMWare and test out different scenarios.
- Use fuzzing tools such as Honggfuzz to see how the security handles the stress of an attack and reveal any vulnerabilities.
- Run a vulnerability assessment using a tool such as OpenVAS.
- Conduct a penetration test.

Task 6: Identify at least three (3) possible network security threats.

1. Malware/ransomware
2. Botnets
3. Viruses and worms
4. DDoS attacks
5. Phishing attacks

Task 7: Explain at least three (3) security countermeasures you have implemented in your design and their purpose.

1. A DMZ has been created to protect the private network from web-facing servers.
2. An internal server subnet has been created to create separation from the private and wireless LAN access. The router can be configured to restrict access to only those hosts requiring it.
3. Firewall is set as an edge router to filter internet traffic.