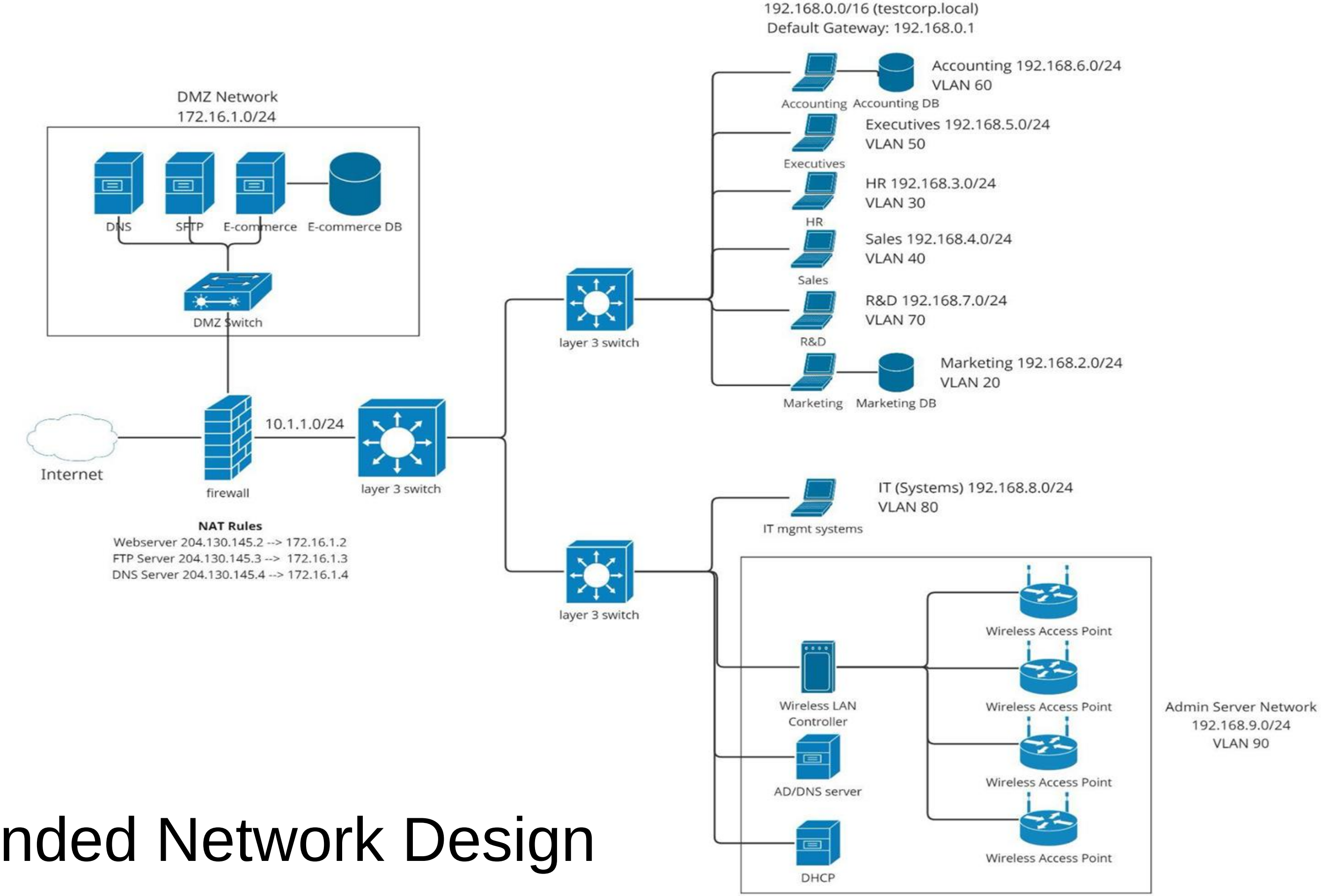
Network Design Recommendations



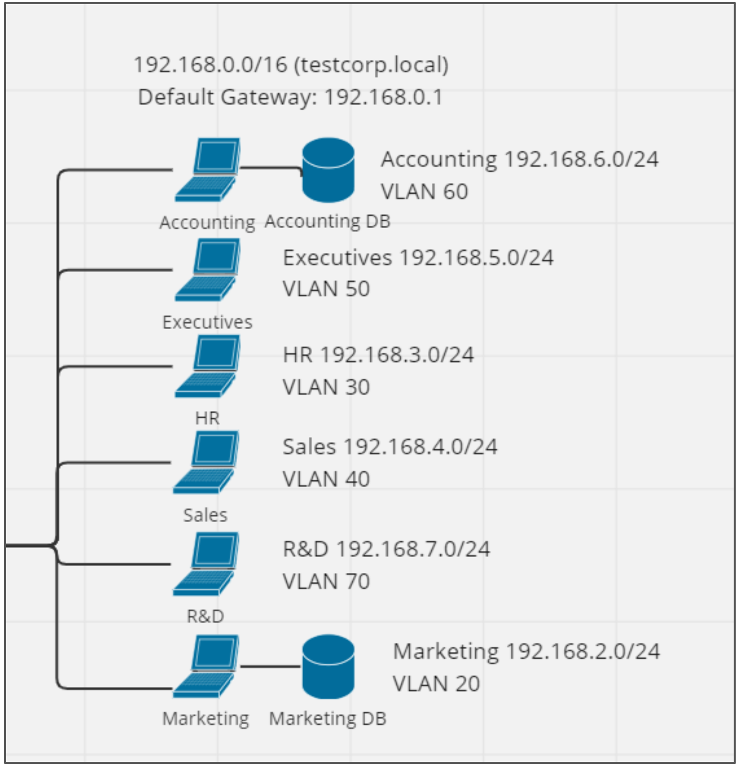
Recommended Network Design

Critical Components

- Firewall
  - Next-Generation firewall provides the best network edge security
  - Filter incoming and outgoing traffic, monitor network activity
- Routing/switching
  - Versatility of layer 3 switches
  - Stackable design allows easy expansion as required
  - Provide for network segmentation
- Wireless LAN
  - Wireless infrastructure allows wireless devices
- Intrusion Prevention System
  - IDS/IPS systems provide monitoring and security across the network
  - Identify and react to threats as they occur

VLAN Segmentation

Department	IP Address	VLAN
Marketing	192.168.2.0	VLAN20
Sales	192.168.4.0	VLAN40
HR	192.168.3.0	VLAN30
Executives	192.168.5.0	VLAN50
Accounting	192.168.6.0	VLAN60
IT (Systems) – Privileged users	192.168.8.0	VLAN80
R&D	192.168.7.0	VLAN70
Admin Server Network	192.168.9.0	VLAN 90



VLANs

IP Addressing Scheme

Public facing:

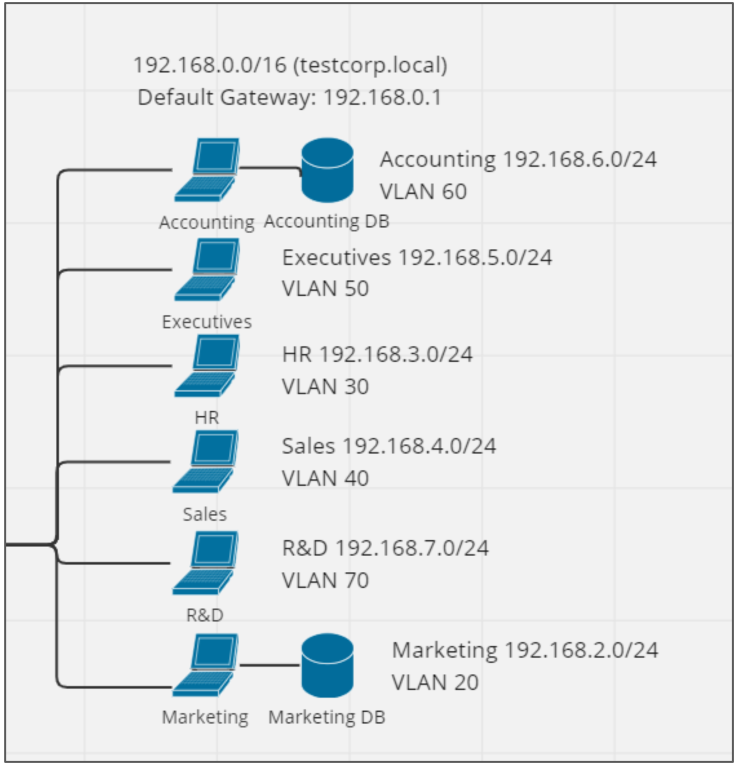
Webserver 204.130.145.2
FTP Server 204.130.145.3
DNS Server 204.130.145.4

DMZ: 172.16.1.0/24.

NAT will translate public IP's to the following:

Webserver 172.16.1.2
FTP Server 172.16.1.3
DNS Server 172.16.1.4
EcommerceDB 172.16.1.5 (No public-facing IP)

Internal address space: 192.168.0.0/16



Internal addresses

NAT Rules

Static

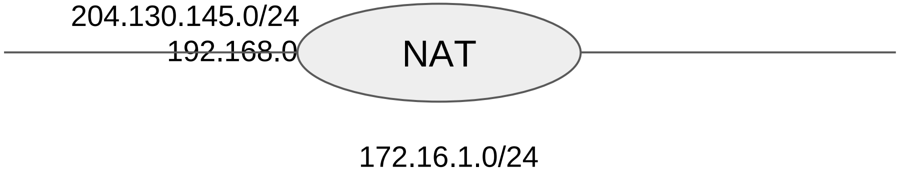
Webserver 204.130.145.2 --> 172.16.1.2

FTP Server 204.130.145.3 --> 172.16.1.3

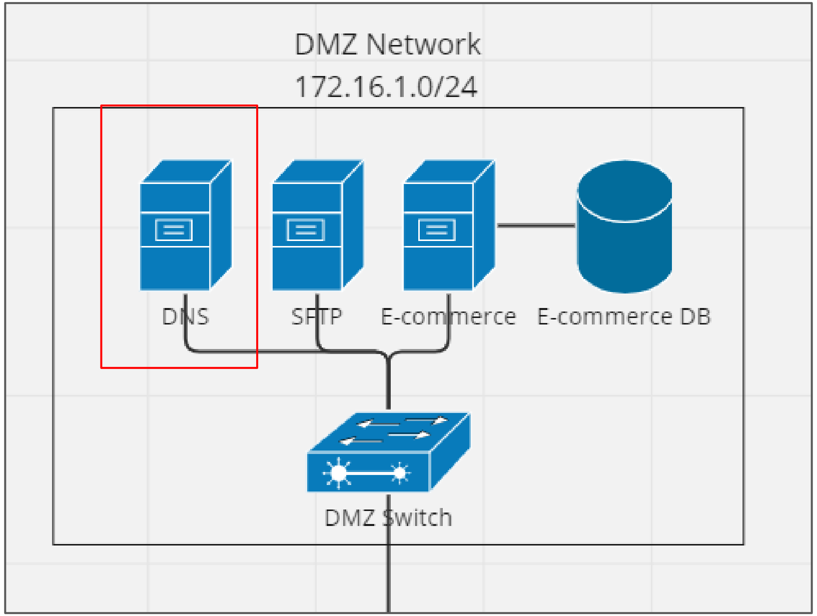
DNS Server 204.130.145.4 --> 172.16.1.4

Dynamic

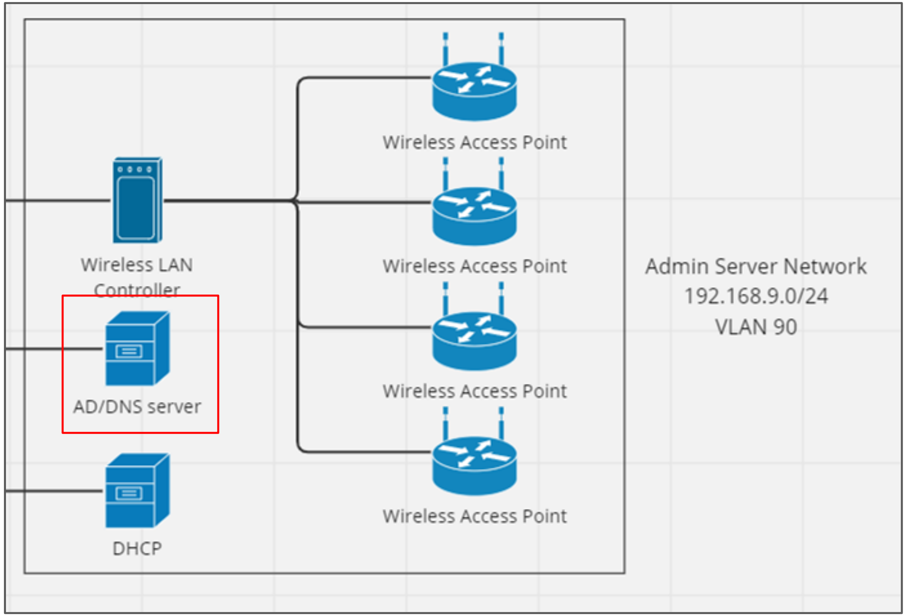
204.130.145.10 <--> 192.168.0.0/16



DNS Architecture



External DNS
testcorp.com



Internal DNS
testcorp.local

DNS Configurations

Internal

DNS Server Name: dc.testcorp.local

Domain: testcorp.local

Name	Type	Data
dc.testcorp.local	A	192.168.9.2
dhcp.testcorp.local	A	192.168.9.3
marketing.testcorp.local	A	192.168.2.100
accounting.testcorp.local	A	192.168.6.100
rnd.testcorp.local	A	192.168.7.100

External

DNS Server Name: dc.testcorp.com

Domain: testcorp.com

Name	Type	Data
testcorp.com	A	204.130.145.2
ftp.testcorp.com	A	204.130.145.3

DHCP

- VLAN20: Marketing
  - DHCP enabled
- VLAN30: HR
  - DHCP enabled
- VLAN40: Sales
  - DHCP enabled
- VLAN50: Executives
  - DHCP enabled
- VLAN60: Accounting
  - DHCP enabled
- VLAN70: R&D
  - DHCP enabled
- VLAN80: IT systems, administration systems, wireless, etc.
  - No DHCP, static addressing

Firewall Rules

1. Allow HTTP (port 80) and HTTPS (port 443) traffic from all VLANs to the internet for general web browsing.
   - Reason: To enable users to access the internet for work-related tasks.
1. Allow DNS (port 53) traffic from all VLANs to the internet.
   - Reason: To allow users to resolve domain names.
1. Allow SSH (port 22) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.
   - Reason: To enable IT administrators to remotely manage and troubleshoot network devices.
1. Allow RDP (port 3389) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.
   - Reason: To enable IT administrators to remotely access and manage user workstations.
1. Allow SMB (port 445) traffic within the Marketing (VLAN20), Sales (VLAN40), HR(VLAN30), Executives (VLAN50), Accounting (VLAN60), and R&D (VLAN70) VLANs.
   - Reason: To enable file sharing within each department.
1. Allow SMB (port 445) traffic from the IT (Systems) VLAN (VLAN80) to all other VLANs.
   - Reason: To enable IT administrators to manage shared files and resources.

Firewall Rules cont.

7. Allow access to an intranet web server on port 8080 from all VLANs.
   - Reason: To provide access to an internal company portal or knowledge base.
7. Allow VoIP (port range 5060-5061) traffic within and between all VLANs.
   - Reason: To enable voice communication within the organization.
7. Allow access to a VPN server on port 1194 from all VLANs to the IT (Systems) VLAN(VLAN80).
   - Reason: To enable secure remote access for authorized users.
7. Allow access to a network monitoring tool on port 3000 from the IT (Systems) VLAN (VLAN80) to all other VLANs.
   - Reason: To enable IT administrators to monitor network performance and troubleshoot issues.
7. Allow traffic from wireless access points (WAPs) to the internet on TCP ports 80, 443, and 53.
   - Reason: This rule allows WAPs to access the internet for legitimate business purposes, such as providing wireless connectivity for employees and guests. Restricting access to only necessary ports (HTTP, HTTPS, DNS) helps to minimize the attack surface and reduce the risk of unauthorized access.
7. Deny all other traffic not mentioned above.
   - Reason: To secure network by preventing any other communication that does not fall under given firewall rules

New Devices/Purchases

- Firewall
  - Cost: $4,014.99
  - Benefit: Enhance network security by filtering traffic from the Internet
- Layer 3 Switches
  - Cost: 24 port - $5319.99 each (purchasing 2) / 48 port - $6939.99 each (purchasing 2)
  - Benefit: Provide faster routing, scalability, flexibility and cost-effectiveness compared to router
- Wireless Access Points/ Wireless Controller
  - Cost: $369.99 each (purchasing 4) / $6076.99
  - Benefit: Allows hosts to connect wirelessly
- Intrusion Prevention System
  - Cost: $772.99
  - Benefit: Layer of security that will help protect against malicious content entering the network
- Warranty/Service Agreements/Licenses
  - Cost: $8,366.77

Total : **$46,777.64**

Secure Network Management and Help Desk Workstation

- Strong Authentication: Use complex passwords, multi-factor authentication to access servers and resources
- Privileged Management: Implement RBAC and ABAC to ensure privileged users can access to the specific resources they are allowed and monitor and audit their activities
- Limit Access: Limit access to servers and resources to the necessary users and provide access on need-to-know basis
- Security Audits: Perform regular audits to identify vulnerabilities to address them
- User Awareness Training: Provide training to all users and especially users who have privileged access to educate them on security best practices and the importance of secure network
- Patching: Keep all software and systems up-to-date with latest security patches and to keep them secure
- Encryption: Implement TLS or SSL to secure data at transit and at rest to protect against data from unauthorized access