User Manual for Company Network Design

This user manual provides comprehensive instructions and configuration details for setting up and managing a secure network infrastructure for an IT Consulting Business. It covers network overview, hardware components, topology design, configuration procedures, security policies, monitoring, troubleshooting, and maintenance guidelines.

Introduction and Network Overview

This manual provides instructions and configuration details for setting up and managing the secure network infrastructure for the Company Network Design. This network supports critical functions, such as internet access, inter-departmental communication, and network monitoring, while maintaining strong security protocols.

The network is segmented into multiple VLANs and secured through layered firewalls and managed switches. The key components include an internet router, external and internal firewalls, a DMZ with segregated VLANs, and a structured internal network with VLANs for each department.

Objectives:

- Provide secure internet access and network isolation.
- Set up a DMZ for public-facing services.
- Implement internal VLANs for department-specific networks.
- Use firewalls to control traffic between different zones.

Hardware Components and Roles

Component	Role	Model
Internet Router	Connects to external network (ISP)	Cisco ISR
External Firewall	Protects the network perimeter	Cisco ASA
Business Router	Routes traffic between the DMZ and internal NW	Cisco ISR
DMZ Firewall	Controls access to DMZ VLANs	Cisco ASA
Internal Firewall	Protects internal network from DMZ	Cisco ASA
DMZ Switch	Segments VLANs for public services	Cisco Switch
Internal Switch	Distributes network access to departments	Cisco L3 Switch
Department Switches	Access switches for department VLANs	Cisco Switch

Network Topology & VLAN Design

The network is designed with the following VLANs:

Internal Network VLANs:

- VLAN10 (IT Department): 192.168.1.0/27
- VLAN20 (Executive Management): 192.168.1.32/27
- VLAN30 (HR): 192.168.1.64/27
- VLAN40 (Finance): 192.168.1.96/27
- VLAN50 (Sales): 192.168.1.128/27
- VLAN60 (Customer Support & Marketing): 192.168.1.160/27
- VLAN99 (Data Center Servers): 192.168.1.192/27

Step-by-Step Configuration Procedures

Below are detailed configuration steps for each network device.

Internet Router

1. Access Configuration Mode:
2. Set Hostname and IP Address:

```
Router>enable
Router#configure terminal
```

3. Configure Default Route to External Firewall:

```
Internet(config)#ip route 0.0.0.0 0.0.0.0 222.0.112.2
```

External Firewall

1. Set Hostname and IP Address for Outside Interface:
2. Configure Inside Interface and Routing:
3. Define Access Control for Web and DNS Services:

```
EXTFW(config)#interface g1/2
EXTFW(config-if)#ip address 172.168.0.2 255.255.255.252
EXTFW(config-if)#nameif INSIDE
EXTFW(config-if)#security-level 100
EXTFW(config-if)#exit
EXTFW(config)#route OUTSIDE 0.0.0.0 0.0.0.0 222.0.112.1
```

```
EXTFW(config)#access-list OUTSIDE-TO-INSIDE extended permit tcp any host
EXTFW(config)#access-list OUTSIDE-TO-INSIDE extended permit udp any host
EXTFW(config)#access-group OUTSIDE-TO-INSIDE in interface OUTSIDE
```

Access and Security Policies

Firewall Rules

Implement policies to control inbound and outbound traffic at each firewall.

VLAN Access Control

Each VLAN is segmented to allow only necessary traffic.

User Access Levels

Admin access to network devices should be limited and secured.

Network Monitoring, Troubleshooting, and Maintenance

Monitoring Tools:

- NIDS: Monitors network traffic in the DMZ VLAN for potential intrusions.
- WAF: Protects web applications from attacks in the DMZ.
- Honeypot: Used to detect and deflect unauthorized access attempts.

Troubleshooting Tips:

- Connection Issues: Verify firewall rules and routing configurations.
- VLAN Issues: Ensure VLAN assignments on switches and firewalls are correct.
- Network Logs: Monitor logs for unusual activity; review NIDS alerts for threats.

Backup and Maintenance Guidelines

Backup Configuration:

- Regularly back up router and firewall configurations to prevent data loss.
- Maintain a secure, off-site backup of all configurations.

Regular Maintenance:

- Update firewall and router firmware periodically.
- Review and refine firewall rules to match evolving security requirements.
- Periodic audits of VLAN assignments and access control policies.