Final Project: Small Business Network Design

Joslen Tardencilla  
Summer-2215-CNT2001C-2609-O

Professor Pamela Brauda

August 22, 2021

Assignment Summary

This is a basic network design for a small business of just 18 employees in a one floor office. The design includes a standard Firewall and DMZ Switch that only allows for the employees to access sites that only the company allows. In the DMZ, only the Mail and Web server is public to the employees, the Proxy and Database servers will be private. The office will mostly run on a wireless connection that is secured locally, though there is the option for employees to utilize wall ethernet ports. Access points are deployed in the office area and connected to Access Switch with a Cat6e Cable supporting maximum of 100m cabling. All Ethernet ports and WLAN port working inside a same bridge. Access points deployed inside the ceiling grid and have three 5dbi antennas with 150m Omni-directional range installed on the surface of ceiling to deliver the most wireless signal. Access to the remote command-line for the whole network will be from the secure shell server. The internet connectivity to the employees will come from three main access points. Two of which will be directed at the 14 employees, and one assess point will be directed in the area of the company executives.

Security Summary

For the Public and Private servers there are a few attacks that may occur, but the design has ways to combat that. Connections will be limited to protect your server against DoS attacks, DNS will be activated to block bogus senders, and a DNSBL(DNS Backlist) server will be set up within the Proxy to fight incoming email abuse. All servers have their own Firewall. All operating systems are up-to-date and pulling patches every midnight. The Firewall has self-hardening security rules. The Core Switch is protected by a spanning tree and VTP protection. The DMZ and Access switches are protected by MAC restricted port security, and DHCP Spoofing.

Diagram Summary

The diagram starts with an internet access that is set by the internet provider. That then is access thought the Edge Router that is narrowly focused for company tasks and secured through the layer 7 Transparent Firewall. Firewall is connected to Edge Router and Core Switch, both with fiber optic links. It operates as a transparent IPS and has an IPv4 address on its loopback interface for management. This then feeds the Layer 3 Core Switch that is a VTP Server. It also provides DHCP service, answering requests coming from Internal Segment. The links between Core Switch and other switches contains aggregation of two fiber optic links using LACP. All operating ports (including port-channels) are operating in trunk mode. The Core Switch feeds signal to the DMZ switch and Access switch, this is then bounced back as public and private internet. DMZ Switch is connected to Core Switch with two uplinks aggregated with LACP protocol working in trunk mode. The ports connected to Proxy Server and Database Server are in access mode to VLAN Internal, rest of the used ports are in access mode placing in DMZ VLAN. All unused ports are in shutdown state. Access Switch is connected to Core Switch with two uplinks aggregated with LACP protocol working in trunk mode. All other ports are in access mode to VLAN Internal. This cleaned up and secured internet, for company usage, is then accessed through ethernet or wireless through access points. Access points are deployed in the office area and connected to Access Switch with a Cat6e Cable supporting maximum of 100m cabling. All Ethernet ports and WLAN port working inside a same bridge. Access points deployed inside the ceiling grid and have three 5dbi antennas with 150m Omni-directional range installed on the surface of ceiling to deliver the most wireless signal. To have access points within the acceptable cabling range, the following implementation is recommended. The internet feeds all 18 employee workstations and the 2 server stations. However, there are public and private networks in the diagram. The Web and Mail Servers are public, while the Proxy and Database servers are private. There are also Vlans implemented in the diagram. Web and Mail servers operate though a DMZ Vlan, while the private servers as well as the workstations all operate through internal Vlan. The Network Printers also utilize the internal Valn to operate accordingly. 2 Network Printers are connected to the Wireless Network using static IP address 192.168.1.2-3. Printers also support WPA2-PSK Personal authentication.

Inventory Summary

The inventory includes an Edge Router, Layer 7 Transport Firewall, Layer 3 Core Switch, Layer 3 DMZ Switch, Layer 2 Access Switch, Access Point, Proxy Server, Database Server, Mail Server, Web Server, Workstations, and the Network Printers. I picked this standard hardware because they ease user management and security for such a small scoped network design.

Inventory Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Quantity | Description | Item name | Icon |  |
| 1 | IP address: **192.168.0.15** | Edge Router |  | 1 |
| 1 | Host name: **Company1**  Uses ipv4 corresponding to Edge router | Layer 7 transparent Firewall |  | 2 |
| 1 |  | Layer 3 Core Switch | A picture containing text, clock, gauge  Description automatically generated | 3 |
| 1 |  | Layer 3 DMZ Switch | Icon  Description automatically generated | 4 |
| 1 |  | Layer 2 Access Switch |  | 5 |
| 3 | Each have different address: 192.168.1.4  192.168.1.5  192.168.1.6 | Access Point |  | 6 |
| 1 for each | Will have internal Vlan.  Address for Proxy: 192.168.1.7  Address for Database: 192.168.1.8 | Proxy and Database Server | Icon  Description automatically generated | 7 |
| 1 for each | Will be public. | Web and Mail server | Icon  Description automatically generated | 8 |
| 20 | 14 for employees, 4 for executives, 1 for server room, and 1 for DHCP access pc.  DHCP range: 192.168.1.20-40 | Workstations |  | 9 |
| 2 | Address: 192.168.1.2  192.168.1.3 | Network Printer |  | 10 |

Diagram

Diagram

Description automatically generated

# Logical explanations / With detailed security descriptions for each component

## Edge Router

### Connectivity:

Edge router resides inside the edge segment. By the outside interface, it is connected to the internet provider. On the internal interface, is it physically connected to the transparent firewall with fiber optic link and have tree sub-interfaces with dot1Q encapsulation. Each sub-interface have certain fixed IPv4 address to communicate with appropriate VLAN and Firewall.

### NAT:

There are four NAT rules written in the router.

1. A source NAT, masquerading traffic from public servers to the outside allowing certain ports to pass.
2. A source NAT, masquerading traffic from Proxy server and DNS Server.
3. A Source NAT, masquerading traffic from Firewall.
4. A Destination NAT, forwarding incoming TCP and UDP grouped ports from outside to IP of mail server.
5. A Destination NAT, forwarding incoming TCP and UDP grouped ports from outside to IP of web server.

### Routes:

The default route is toward the ISP. Two static routes for IPs inside DMZ and Internal VLANs will be forwarded to CoreSwitch

### Security:

Router has self-hardening security rules, preventing brute-force logging attacks, SSHv2 only access.

## Layer 7 transparent firewall

### Connectivity:

Firewall is connected to edge router and core switch, both with fiber optic links. It operates as a transparent IPS and has an IPv4 address on its loopback interface for management.

### IPS and firewall:

The firewall gets the signature updates from the official provider. It also has an IP-Blacklist in text format provided by trusted sources, blocking any incoming traffic from IPs with malicious reputation on the internet.

### Security:

Firewall has self-hardening security rules, preventing brute-force logging attacks, SSHv2 only access.

## Layer 3 Core Switch

### Connectivity:

This switch is connected to Firewall, DMZ Switch and access switch. CoreSwitch is VTP Server in the domain and root of the spanning tree topology. It also provides DHCP service, answering requests coming from Internal Segment. The links between CoreSwitch and other switches contains aggregation of two fiber optic links using LACP. All operating ports (including port-channels) are operating in trunk mode.

### Routes:

Beside connected routes, there are two routes rules written in the CoreSwitch.

1. Routing traffic coming from Proxy Server and DNS Server to any destination using Router as Gateway.
2. Routing traffic coming from DMZ to any destination using Router as Gateway.

### DHCP:

There is only one scope defined in the DHCP for internal users. This excludes the first 20 IPs from the range for Static IPs for access points, printers, and Proxy Server. For DHCP peers, Default Gateway for DHCP peers is CoreSwitch and DNS is IP of internal DNS Server.

### Security:

Spanning tree and VTP protection, DHCP Spoofing prevention, Brute-Force prevention, automated version backups.

## Layer 3 DMZ Switch

### Connectivity:

DMZ Switch is connected to CoreSwitch with two uplinks aggregated with LACP protocol working in trunk mode. The ports connected to Proxy Server and Database Server are in access mode to VLAN Internal, rest of the used ports are in access mode placing in DMZ VLAN. All unused ports are in shutdown state.

### Security

MAC restricted port security, DHCP Spoofing.

## Layer 2 Access Switch

### Connectivity:

Access Switch is connected to CoreSwitch with two uplinks aggregated with LACP protocol working in trunk mode. All other ports are in access mode to VLAN Internal.

### Security:

MAC restricted port security, DHCP Spoofing.

## Access points

### Connectivity:

Access points are deployed in the office area and connected to Access Switch with a Cat6e Cable supporting maximum of 100m cabling. All Ethernet ports and WLAN port working inside a same bridge. Access points deployed inside the ceiling grid and have three 5dbi antennas with 150m Omni-directional range installed on the surface of ceiling to deliver the most wireless signal. To have access points within the acceptable cabling range, the following implementation is recommended

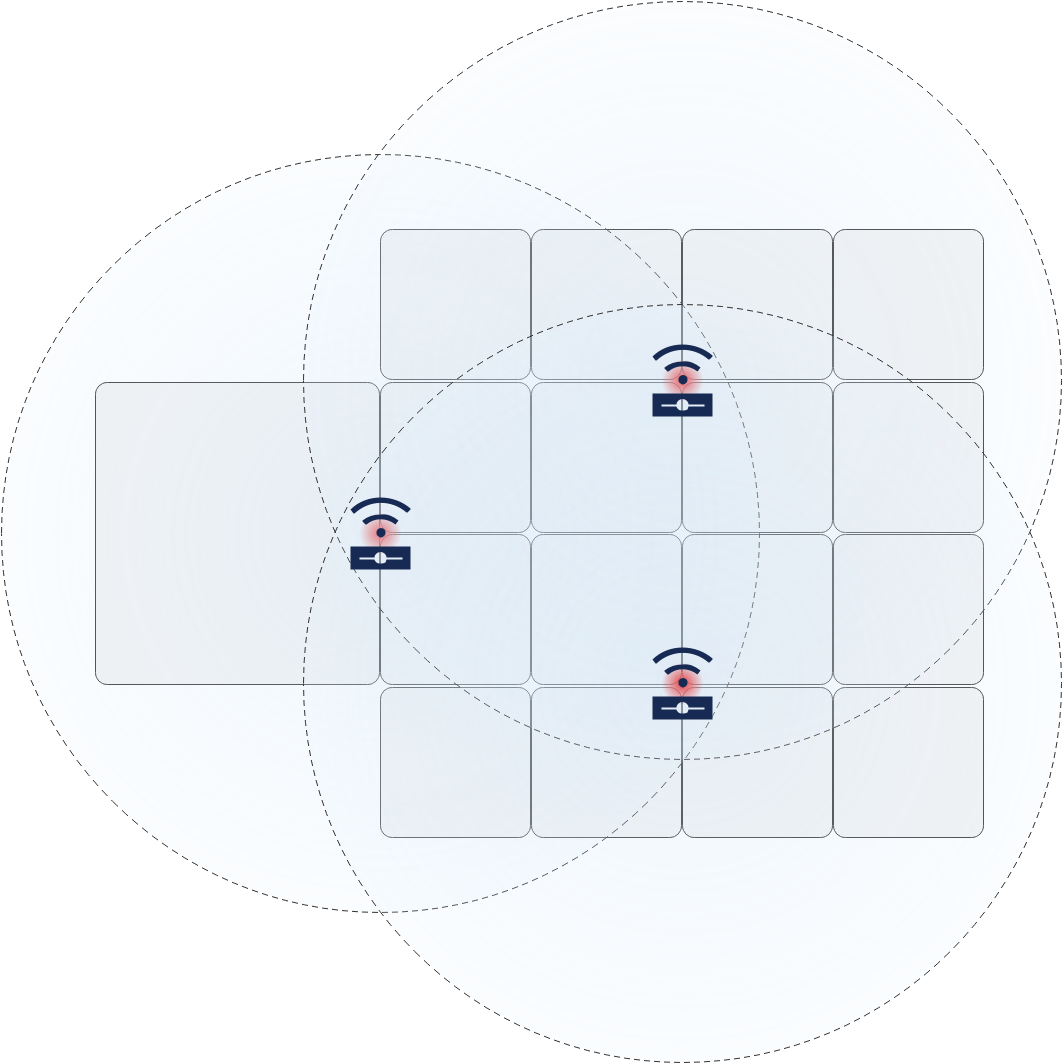


Figure 1 - Effective signal range

### Security:

Connecting to WLAN network requires WPA2-PSK Personal key. For more security, internal MAC Access-list set up on all of the APs allowing only known clients to connect.

## Proxy Server

### Connectivity:

This server is connected to a port on DMZ switch and placed in the Internal VLAN. It has a Proxy service running on port 1080.

### User Management:

Proxy Server has built-in Hotspot service with auto-redirection authentication page. Network Admin creates set of rules, limiting the bandwidth or time of each authenticated user to give them access to the internet. On the first attempt to open an internet page by internal users, they have to authenticate by Hotspot webpage; and their visited pages will remain in the Hotspot dashboard for admins to review if necessary. Proxy service also can restrict any outgoing traffic to certain websites, depending on the corporate policy.

## Network Printer

### Connectivity:

2 Network Printers are connected to the Wireless Network using static IP address 192.168.1.2-3. Printers also support WPA2-PSK Personal authentication.

## Servers Security

All servers have their own firewall, allowing only ports required for running services. Admins only can log in through encrypted SSH connection and have maximum of 3 failed retries. All operating systems are up-to-date and pulling patches every midnight.