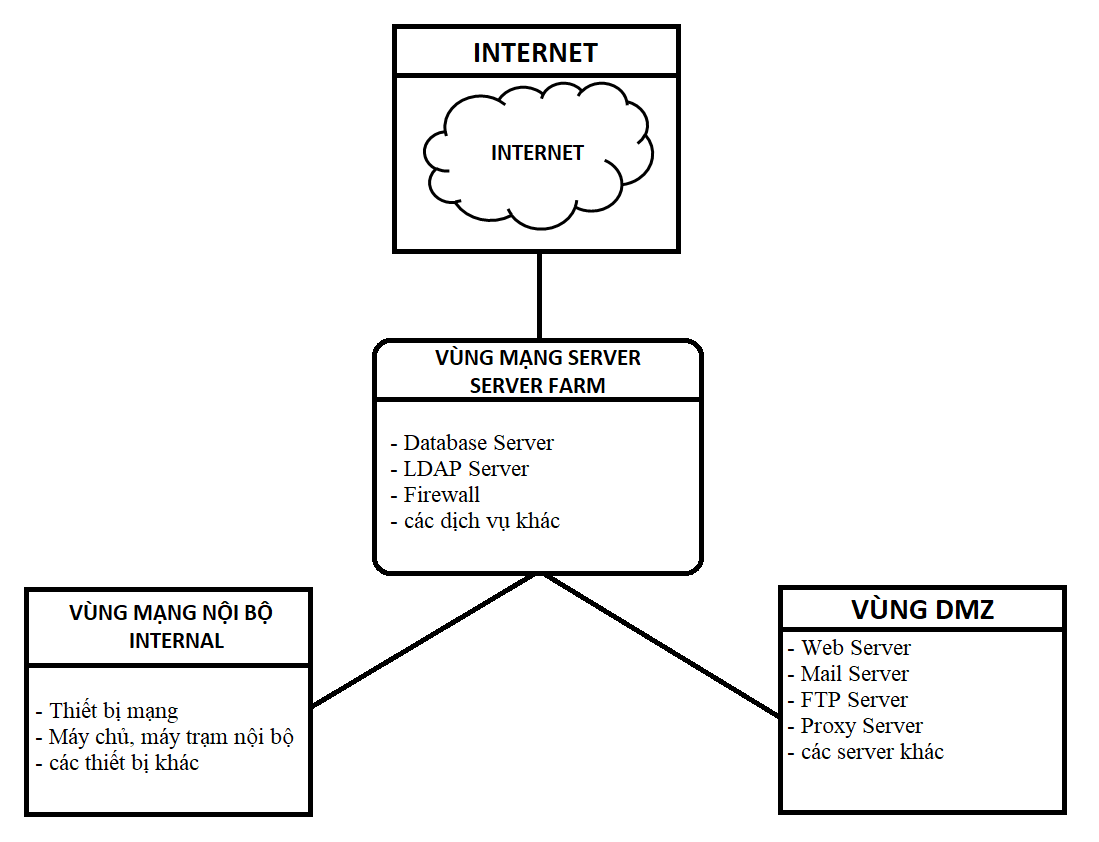
# Tổng quát về mô hình mạng bảo mật cho doanh nghiệp

**Một mô hình mạng bảo mật là cần thiết cho mỗi tổ chức để phân biệt giữa các vùng theo chức năng và thiết lập các chính sách an toan thông tin riêng cho mỗi vùng mạng theo yêu cầu.**

## Các thành phần trong mô hình mạng bảo mật

1. **Vùng mạng internet (External):** kết nối hệ thống mạng doanh nghiệp với mạng internet toàn cầu.
2. **Vùng mạng nội bộ (Internal):** hệ thống mạng LAN (Local area network), đặt các thiết bị mạng, máy chủ, máy trạm trong một nội bộ của công ty. Một công ty có thể có nhiều vùng mạng nội bộ.
3. **Vùng DMZ (Demilitarized Zone):** là vùng mạng trung lập phân biệt giữa người dùng bên ngoài (internet) và máy chủ riêng (mạng cục bộ hoặc mạng diện rộng), chứa các thông tin cho phép người dùng từ internet truy xuất vào và chấp nhận rủi ro tấn công từ internet. Các dịch vụ được triển khai trong vùng DMZ như máy chủ Web, máy chủ Mail, máy chủ FTP, Proxy….
4. **Vùng mạng Server (Server Farm):** đặt các máy chủ không trực tiếp cung cấp dịch vụ cho mạng internet, các dịch vụ được triển khai trong vùng Server Farm như Database Server, LDAP Server, Firewall…



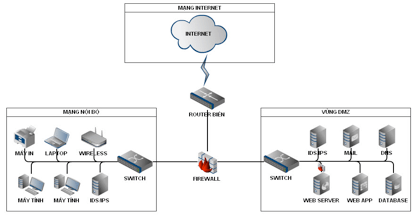
Hình 1‑1: Các thành phần trong mạng lưới bảo mật doanh nghiệp

**Việc tổ chức mô hình mạng bảo mật doanh nghiệp có ảnh hưởng đến sự an toàn thông tin của hệ thống mạng và các cổng thông tin điện tử. Đây là nền tảng cho việc xây dựng hệ thống phòng thủ và bảo vệ an toàn cho các thành phần trước những cuộc tấn công từ bên trong và bên ngoài một cách hiệu quả.**

## Một số mô hình mạng phổ biến

1. **Mô hình 1**

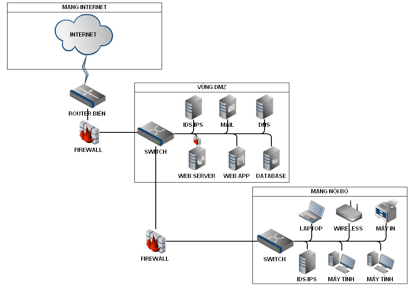
Trong mô hình này, vùng mạng Internet, vùng mạng nội bộ và vùng mạng DMZ được thiết kế tách biệt nhau. Ngoài ra, ta đặt một firewall giữa các vùng mạng nhằm kiểm soát luồng thông tin giữa các vùng mạng với nhau và bảo vệ các vùng mạng khỏi các tấn công trái phép. Đây là mô hình cơ bản trong việc thiết kế mô hình bảo mật doanh nghiệp.



Hình 1‑2: Mô hình 1

1. **Mô hình 2**

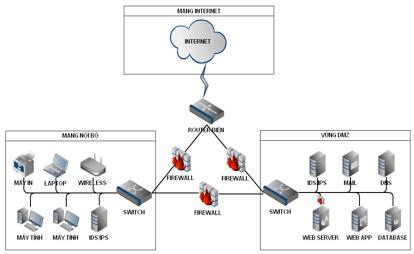
Trong mô hình này, ta đặt một firewall giữa vùng mạng Internet và vùng mạng DMZ và một firewall giữa vùng mạng DMZ và vùng mạng nội bộ. Như vậy, vùng mạng nội bộ nằm sâu bên trong và cách vùng mạng Internet bằng 2 lớp firewall sẽ tăng tính bảo mật hơn.



Hình 1‑3: Mô hình 2

1. **Mô hình 3**

Trong mô hình này, ta đặt một firewall giữa vùng mạng Internet và vùng mạng DMZ , một firewall giữa vùng mạng DMZ và vùng mạng nội bộ và một firewall giữa vùng mạng nội bộ và vùng mạng Internet. Như vậy, mỗi sự truy cập giữa các vùng với nhau đều được kiểm soát bởi một firewall như hình vẽ. Bên cạnh đó, khi tăng số lượng firewall cũng cần tăng chi phí hệ thống, nhưng sẽ mang lại hiệu quả bảo mật tốt nhất.

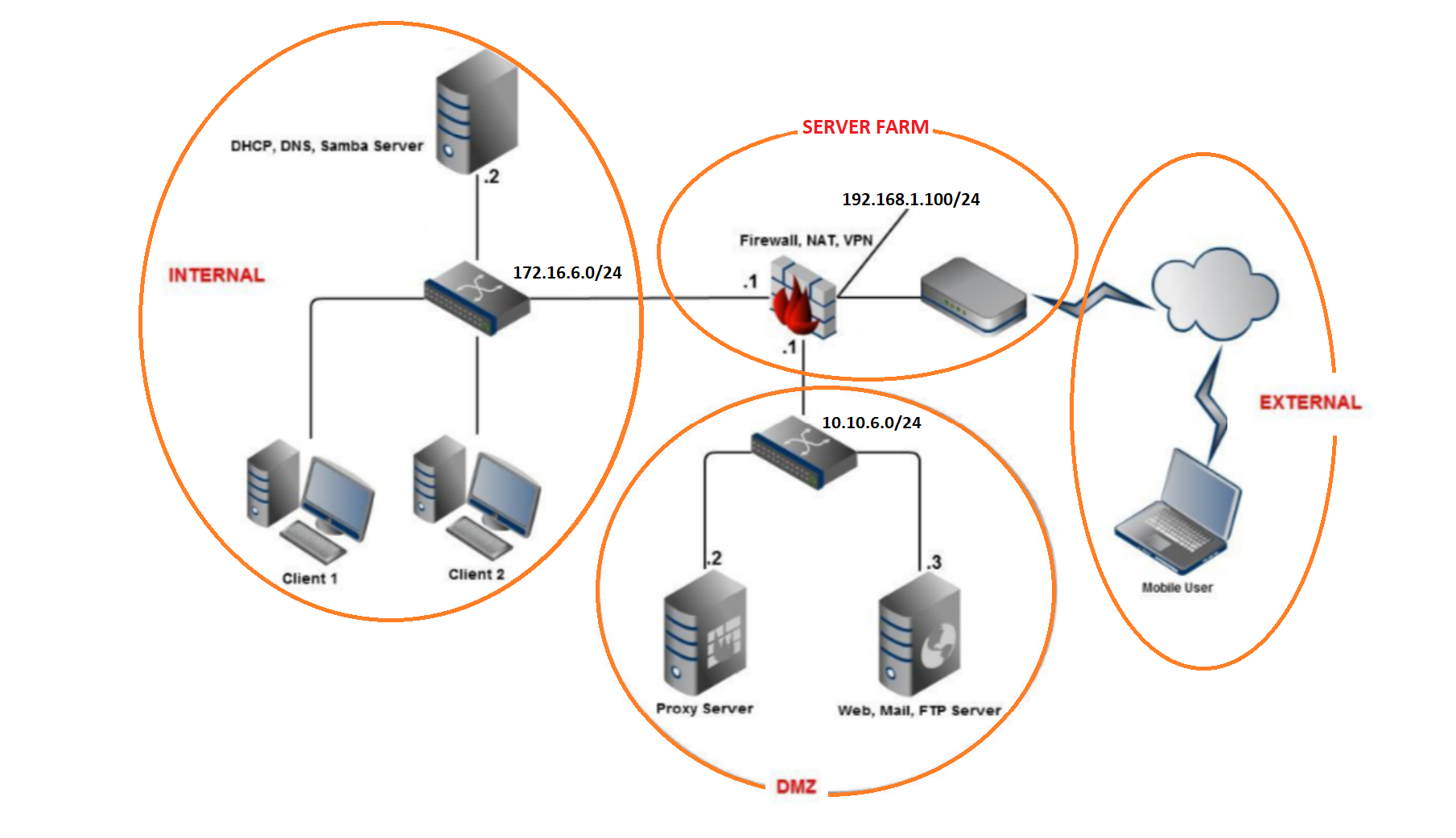


Hình 1‑4: Mô hình 3

## Tiêu chí thiết kế mô hình mạng bảo mật

1. Đặt các máy chủ web (web server), máy chủ thư điện tử (mail server)… cung cấp dịch vụ ra mạng internet nằm trong vùng DMZ. Tránh các tấn công từ mạng nội bộ hoặc gây ảnh hướng tới an toàn mạng nội bộ nếu các máy chủ này bị tấn công và chiếm quyền kiểm soát. Chú ý không đặt máy chủ web, mail server hoặc các máy chủ chỉ cung cấp dịch vụ cho nội bộ trong vùng mạng này.
2. Các máy chủ không trực tiếp cung cấp dịch vụ ra mạng ngoài như máy chủ ứng dụng, máy chủ cơ sở dữ liệu, máy chủ xác thực… Nên đặt trong vùng mạng server network để tránh các tấn công trực diện từ Internet và từ mạng nội bộ. Đối với các hệ thống thông tin yêu cầu có mức bảo mật cao, hoặc có nhiều cụm máy chủ khác nhau có thể chia vùng server network thành các vùng nhỏ hơn độc lập để nâng cao tính bảo mật.
3. Nên thiết lập các hệ thống phòng thủ như tường lửa (firewall) và thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) để bảo vệ hệ thống, chống tấn công và xâm nhập trái phép. Khuyến cáo đặt firewall và IDS/IPS ở các vị trí như sau: đặt firewall giữa đường nối mạng Internet với các vùng mạng khác nhằm hạn chế các tấn công từ mạng từ bên ngoài vào; đặt firewall giữa các vùng mạng nội bộ và mạng DMZ nhằm hạn chế các tấn công giữa các vùng đó; đặt IDS/IPS tại vùng cần theo dõi và bảo vệ.
4. Nên đặt một Router ngoài cùng (Router biên) trước khi kết nối đến nhà cung cấp dịch vụ internet (ISP) để lọc một số lưu lượng không mong muốn và chặn những gói tin đến từ những địa chỉ IP không hợp lệ.

# Mô hình bảo mật mạng doanh nghiệp cơ bản

Báo cáo sẽ trình bày tập trung vào thiết lập một mô hình bảo mật doanh nghiệp cơ bản. Cụ thể mô hình như sau (yêu cầu trong file đính kèm)

1. Vùng INTERNAL

* Gồm các máy client và một số server cung cấp dịch vụ cho mạng nội bộ như DHCP Server, DNS Server, Samba Server.
* Sử dụng đường mạng 172.16.6.0/24, dùng card mạng vmnet1.

1. Vùng DMZ

* Gồm các server quan trọng được truy xuất ra ngoài internet như Web Server, Mail Server, FTP Server, Proxy Server.
* Sử dụng đường mạng 10.10.6.0/24, dùng card mạng vmnet2.

1. Vùng EXTERNAL

* Là mạng internet.
* Công ty sở hữu địa chỉ IP Public, sử dụng địa chỉ private 192.168.1.100, dùng card mạng bridge.

1. Vùng Server Farm

* Đặt máy chủ không trực tiếp như Firewall, NAT, VPN…

1. Công ty sở hữu domain có tên duybinh.com
2. Các server, client có thể là Linux hoặc Windows, trong khuôn khổ project này sẽ sử dụng Linux để tiến hành cài đặt, cấu hình và kiểm tra

Báo cáo sẽ tách ra 4 phần tương ứng 4 vùng trong mô hình hệ thống trên

# Cài đặt và cấu hình

## Vùng mạng nội bộ (Internal)

## Vùng DMZ

## Vùng mạng Server (Server Farm)

# Công cụ thực hiện

Dưới đây là danh sách liệt kê các công cụ thực hiện trong project này.

|  |  |  |
| --- | --- | --- |
| **STT** | **Công cụ** | **Link download** |
| 1 | VMWare workstation pro 15.5 | <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html> |
| 2 | Ubuntu Server 18.04.3 LTS | <https://ubuntu.com/download/server> |
| 3 |  |  |
|  |  |  |

# Tham khảo

1. <https://cystack.net/vi/resource/cybersecurity-framework/>
2. <https://travelgear.vn/blog/dmz-la-gi/>
3. <https://securitydaily.net/network-mo-hinh-mang-hop-ly/>
4. Cấu hình DHCP trên linux: <https://anninhmang.edu.vn/cai-dat-va-cau-hinh-dich-vu-dhcp-server-tren-linux/>