1. Default Login Credentials

- **Username**: admin
- **Password**: pfsense

2. Network Architecture

- **WAN**: Internet connection
- **DMZ**: Publicly accessible resources
- **DEVELOPMENT**: Developer network
- **WORKER**: Employee network
- **GREEN**: Green team control network

3. Rules and NAT Configuration

General Rules:

- **WAN**: NAT rules apply. NAT is used for incoming traffic. "Any, Any" rule is applied to the network.
- **DMZ, DEVELOPMENT, WORKER, GREEN**: "Any, Any" rules are applied, all traffic is allowed.
- **NAT**: Traffic from the WAN network is NAT-ed to internal networks. NAT + Proxy settings applied.
- **DNS server is active.**

3.1 NAT Rules

- **Mailing System**: Redirect ports 587 and 143 to internal IP 10.49.31.52 on ports 587 and 143.
- **External Range**: External employees have access to the internal Gitea server operated by the organization via the port range 3000-3100. Redirected to the 192.#.160.24 network, where ports 2900-3000 are reserved.
- **Access to Company Website**: With HAProxy, port 8080 is available from the company's public IP, providing access to the web service on port 80 in the DMZ.
- **Mailing System External Access**: In addition to ports 587 and 143 (mail server ports), port 35000 is kept open.
- **Green Team Control**: Port 34000 should be redirected to IP address 10.49.31.10.

3.2 Firewall Rule Examples

I. **DMZ**:

- All traffic from the **GREEN** network to the DMZ network is allowed.
- The DMZ network is only accessible externally.
- The DMZ network cannot see other networks.
- The **DEVELOPMENT** network can access the DMZ network.

II. **DEVELOPMENT**:

- All traffic from the **GREEN** network to the **DEVELOPMENT** network is allowed.
- The **DEVELOPMENT** network has access to all networks behind the firewall and allows outbound traffic.

III. **WORKER**:

- All traffic from the **GREEN** network to the **WORKER** network is allowed.
- The **WORKER** network only allows outbound traffic and does not have access to other networks.

IV. **GREEN**:

- All traffic is allowed.

4. DNS Server Configuration

- The pfSense DNS server feature is enabled with default settings.
- The DNS service is available for internal networks.
- DNS server IPv4 address: 207.#.72.53

5. SSH Key Configuration

- **For the GREEN Team**: SSH key is configured for secure access.
- **For Ansible**: A separate SSH key is configured for automatic management.

6. HAProxy Configuration

- HAProxy is configured with Layer 7 rules.
- Proxy-based load balancing is used for HTTP/HTTPS traffic.
- Different backends are configured for network segments.