PC2 – Firewall/IDS (OPNsense com Interface Cabeada e Wireless)

2.1. Função e Objetivos

O PC2 atua como a barreira de segurança da rede, utilizando o OPNsense para filtrar o tráfego, realizar NAT e monitorar possíveis intrusões (com módulos como Suricata). Ele dispõe de interfaces cabeada e wireless – sendo esta última útil para conectar dispositivos sem fio ou como WAN secundária.

2.2. Possibilidades de Implementação

- **Instalação Física:** O OPNsense é instalado diretamente no hardware.
- **Máquina Virtual:** Pode ser executado como uma VM usando plataformas como VMware ESXi ou VirtualBox (se a performance permitir).
- **Dual Boot:** Se o PC2 tiver outra função em outros momentos, pode ser configurado para dual boot com OPNsense e outro sistema.

2.3. Passo a Passo para Execução

Passo 1: Preparação do Ambiente

- Verifique que o hardware (processador, memória, HD) e a placa de rede wireless estão funcionando.
- Conecte o PC2 à rede interna através da interface cabeada.

Passo 2: Instalação do OPNsense

- **Em Hardware Físico ou Dual Boot:**
    - Baixe a ISO do OPNsense e grave-a em um pendrive.
    - Configure a BIOS para boot e instale o sistema, definindo as interfaces (cabeada e wireless).
- **Em Máquina Virtual:**
    - Crie uma VM com recursos mínimos (por exemplo, 1–2 GB de RAM, 1 CPU).
    - Monte a ISO do OPNsense e proceda com a instalação, configurando as interfaces virtuais.

Passo 3: Configuração Inicial do OPNsense

- Acesse a interface web do OPNsense via IP configurado na interface LAN.
- Configure a conta de administrador.
- Defina as interfaces:
    - **WAN:** Conectada ao roteador ou modem (pode ser obtida via DHCP ou IP fixo).
    - **LAN:** Conectada ao switch, defina um IP fixo (ex.: 192.168.1.1).

Passo 4: Configuração da Interface Wireless

- Verifique se a placa wireless é reconhecida pelo OPNsense.
- Ative a interface wireless, configure o SSID e defina o tipo de segurança (WPA2/WPA3).
- Atribua um IP para a interface wireless (por exemplo, 192.168.2.1) se ela atuar em rede separada ou para failover.

Passo 5: Configuração das Regras de Firewall e IDS/IPS

- Crie regras de firewall que permitam o tráfego da rede interna e bloqueiem acessos indesejados.
- Configure o NAT para que os dispositivos internos acessem a Internet apenas pelo firewall.
- Ative e configure o módulo IDS/IPS (ex.: Suricata) e defina as assinaturas e alertas desejados.

Passo 6: Testes e Validação

- Realize testes de conectividade (ping, traceroute) usando tanto as interfaces cabeada quanto wireless.
- Utilize ferramentas (como Nmap) para simular ataques e verificar se as regras estão bloqueando acessos não autorizados.
- Confirme que os logs do IDS estão sendo gerados e podem ser acessados via SSH.

Passo 7: Documentação e Manutenção

- Registre todas as configurações (IPs, regras de firewall, configurações do IDS, detalhes da interface wireless).
- Defina procedimentos de atualização e verificação periódica das assinaturas do IDS.
