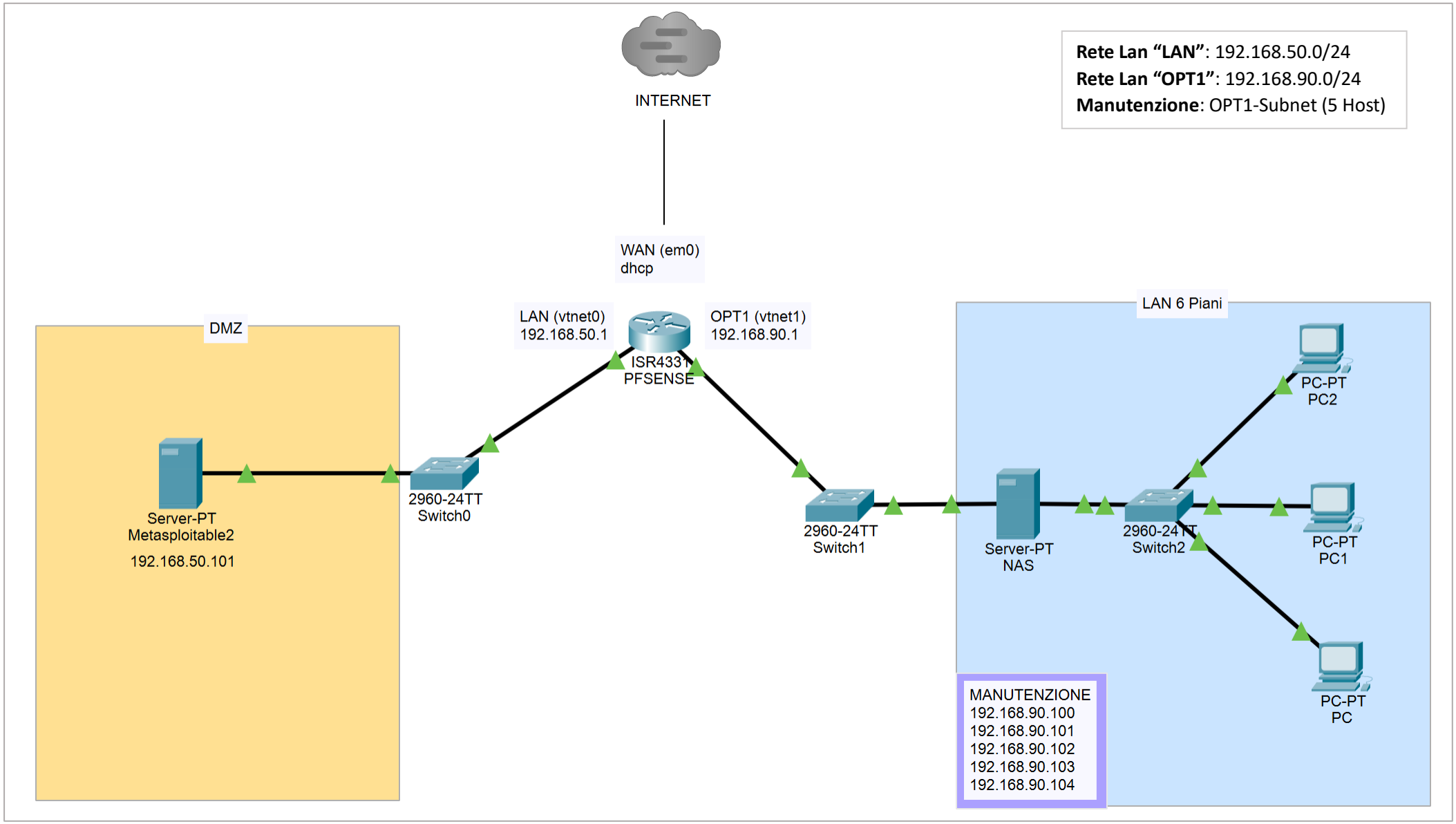
Relazione sulle Regole di Sicurezza e il Funzionamento del Traffico di Rete



Panoramica

La configurazione comprende una rete suddivisa in tre segmenti principali e una connessione WAN per il traffico esterno:

1. **Rete Lan "LAN"**: Zona demilitarizzata contenente il Web Server **Metasploitable2** (IP: 192.168.50.101), con traffico regolamentato per motivi di sicurezza.
2. **Rete Lan "OPT1"**: Rete principale connessa a Internet, all'interno della quale è configurato il gruppo di manutenzione.
3. **Manutenzione (subnet di OPT1)**: Gruppo di 5 indirizzi IP dedicati alla gestione della DMZ, del firewall e di tutti i dispositivi della rete OPT1.
4. **WAN**: Connessione Internet con restrizioni per evitare traffico non desiderato.

ZONA DMZ (LAN) – WEB SERVER

- **Accesso consentito**:
  - Solo agli indirizzi IP del gruppo di **Manutenzione (192.168.90.100 - 192.168.90.104)** per la gestione del Web Server **Metasploitable2**.
  - Il traffico DNS/HTTP verso WAN è consentito per garantire il funzionamento del server.
- **Accesso bloccato**:
  - Tutto il traffico non autorizzato da e verso OPT1, WAN o altri dispositivi della rete è bloccato.
  - Qualsiasi connessione non proveniente dal gruppo di manutenzione.

RETE OPT1

- **Accesso consentito**:
  - I dispositivi all'interno della rete possono accedere a Internet tramite regole di instradamento predefinite.
  - Il gruppo di **Manutenzione (192.168.90.100 - 192.168.90.104)** ha accesso al firewall per la configurazione.
- **Accesso bloccato**:
  - Tutto il traffico diretto verso la zona DMZ è bloccato, eccetto per gli IP del gruppo di Manutenzione.
  - Qualsiasi traffico non autorizzato verso altre subnet.

GRUPPO MANUTENZIONE (SUBSET OPT1)

- **Accesso consentito**:
  - Accesso alla zona DMZ per la gestione del Web Server Metasploitable2.
  - Accesso completo ai dispositivi della rete OPT1.
  - Accesso al firewall per scopi di configurazione amministrativa.
  - Accesso a Internet per attività di aggiornamento o manutenzione software.
- **Accesso bloccato**:
  - Nessuna limitazione specifica, purché le connessioni siano legittime.

CONNESSIONE WAN

- **Accesso consentito**:
  - Il traffico DNS/HTTP è consentito per garantire la funzionalità del Web Server e della rete.
  - La rete OPT1 può accedere a Internet secondo le regole configurate.
- **Accesso bloccato**:
  - Tutto il traffico non autorizzato verso reti interne (DMZ o OPT1).
  - Traffico proveniente da indirizzi privati o non assegnati.

Considerazioni finali sulla Sicurezza

1. **Segmentazione della rete**: La separazione della DMZ dalla rete OPT1 e il controllo degli accessi tramite regole firewall minimizzano i rischi di compromissione.
2. **Accesso amministrativo limitato**: Solo il gruppo di Manutenzione ha privilegi per accedere al firewall e gestire il server nella DMZ.
3. **Blocchi rigorosi**: Il traffico non autorizzato tra reti è bloccato, riducendo il rischio di movimenti laterali in caso di compromissione.