Relazione Tecnica: Implementazione delle Policy di Firewall e Segmentazione DMZ

---

1. Obiettivo dell'Architettura

L'obiettivo della configurazione è simulare un ambiente "Enterprise" realistico, abbandonando la logica permissiva tipica dei laboratori di test ("Playground"). La topologia prevede la separazione netta tra la rete interna (LAN/Inside), la zona demilitarizzata (DMZ) e l'esterno (WAN), in conformità con le best practice di sicurezza perimetrale .

Nello specifico, le regole implementate sull'interfaccia **LAN** di pfSense regolano il traffico in uscita dalla rete fidata verso la DMZ e verso Internet, applicando rigorosamente il **Principio del Privilegio Minimo (Least Privilege)**.

---

2. Analisi Dettagliata delle Regole (LAN Interface)

Il motore di filtraggio di pfSense opera in modalità **sequenziale (Top-Down)**: i pacchetti vengono confrontati con le regole dall'alto verso il basso e la prima regola che corrisponde ("match") determina l'azione. Di seguito l'analisi tecnica delle regole attive, in ordine di priorità.

Regola 1: Anti-Lockout Rule

- **Azione:** PASS (Consenti)
- **Descrizione:** Regola di sistema automatica.
- **Funzione Tecnica:** Garantisce che l'amministratore non perda mai l'accesso all'interfaccia di gestione web del firewall (porte 80/443) o SSH (porta 22) provenendo dalla LAN. È una misura di sicurezza operativa (Fail-safe).

Regola 2: Gestione Sistemistica (Admin SSH to DMZ)

- **Sorgente:** 192.168.50.151 (Host Kali - Postazione Amministratore)
- **Destinazione:** 192.168.51.10 (Server DMZ - Metasploitable)
- **Porta/Protocollo:** TCP 22 (SSH)
- Analisi Tecnica:
  Questa regola implementa un accesso privilegiato granulare. Invece di permettere a tutta la LAN di amministrare il server, l'accesso SSH è ristretto esclusivamente all'indirizzo IP della postazione amministrativa (Kali).
- **Giustificazione di Sicurezza:** Previene tentativi di *Brute Force* o accesso non autorizzato alla shell del server DMZ da parte di utenti standard o dispositivi compromessi all'interno della LAN. Rispecchia la necessità di separare il traffico di gestione (Management Plane) dal traffico utente.

Regola 3: Accesso Servizi Corporate (Corporate Web Access)

- **Sorgente:** LAN Subnets (Intera rete aziendale)
- **Destinazione:** 192.168.51.10 (Server DMZ)
- **Porta/Protocollo:** TCP 80 (HTTP)
- Analisi Tecnica:
  Permette a qualsiasi host della rete interna di visualizzare il sito web ospitato nella DMZ. È fondamentale notare che la regola è limitata strettamente alla porta 80.
- **Giustificazione di Sicurezza:** Simula l'accesso legittimo ai servizi aziendali. Poiché la regola specifica solo la porta 80, impedisce implicitamente l'accesso ad altri servizi potenzialmente vulnerabili (es. porte database, RPC) sullo stesso server.

Regola 4: Segmentazione e Isolamento (Reject all other LAN to DMZ)

- **Azione:** REJECT (Rifiuta con notifica)
- **Sorgente:** LAN Subnets
- **Destinazione:** OPT1 Subnets (Intera sottorete DMZ)
- **Protocollo:** ANY (Qualsiasi)
- Analisi Tecnica:
  Questa è la regola cardine della sicurezza interna. Intercetta qualsiasi pacchetto diretto dalla LAN alla DMZ che non sia stato già gestito dalle Regole 2 o 3. L'azione "Reject" invia un pacchetto TCP RST o ICMP Unreachable al mittente, terminando immediatamente la connessione.
- Giustificazione di Sicurezza:
  Impedisce il Movimento Laterale e la ricognizione (Network Scanning). Se un PC nella LAN viene infettato da un malware, questo cercherà di scansionare altre reti (come la DMZ) per propagarsi. Questa regola blocca tali tentativi (es. scansioni Nmap, exploit su SMB porta 445, Telnet porta 23), isolando efficacemente la DMZ dal resto del traffico interno non necessario. Questo riflette la logica Cisco ASA dove il traffico da livello di sicurezza alto (100) a basso (50) deve essere controllato .

Regola 5: Accesso Internet (Default Allow LAN to Any)

- **Azione:** PASS
- **Sorgente:** LAN Subnets
- **Destinazione:** ANY (*)
- Analisi Tecnica:
  Permette alla LAN di accedere a qualsiasi destinazione.

---

3. Conclusioni

La configurazione attuale trasforma un semplice router in un **Firewall Stateful** avanzato.

L'architettura raggiunta offre:

1. **Isolamento dei Ruoli:** Solo l'IT Admin (Kali) può gestire i server.
2. **Continuità Operativa:** Gli utenti accedono al servizio Web.
3. **Contenimento delle Minacce:** La DMZ è protetta da scansioni interne non autorizzate.

Questa impostazione soddisfa i requisiti di progettazione Enterprise delineati nella documentazione di riferimento, garantendo che la DMZ ospiti servizi pubblici senza diventare un punto di vulnerabilità per la rete interna.