**SETTIMANA 3 LEZIONE 5 MONTIS MATTIA**

**CONFIGURAZIONE RETE CON USO DI FIREWALL**

Rappresentare una rete con i seguenti componenti:

● Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).

● Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.

● Una rete interna con almeno un server o nas.

● Un firewall perimetrale posizionato tra le tre zone.

● Spiegare le scelte.

Il diagramma di rete illustra una configurazione di una rete locale con vari componenti di rete e dispositivi di sicurezza, ciascuno con un ruolo specifico.

**Immagine che contiene diagramma, Piano, linea, Disegno tecnico

Descrizione generata automaticamente**

Il diagramma di rete illustra una configurazione di una rete locale con vari componenti di rete e dispositivi di sicurezza, ciascuno con un ruolo specifico.

1. Internet: rappresenta la connessione alla rete globale WAN;
2. Firewall a filtraggio dinamico: Un firewall a filtraggio dinamico (FFD) è un dispositivo di sicurezza della rete con la funzione di monitorare e controllare il traffico di rete in base a una serie di regole predefinite.

A differenza del firewall a filtraggio statico, che si basa su regole statiche, l’FFD è in grado di adattarsi alle minacce in tempo reale.

Il firewall a filtraggio dinamico impedisce l’accesso dall’esterno alla rete ma interno, ma consentendo solo l’invio di pacchetti da connessioni già autorizzate. Utilizza una lista di controllo degli accessi per verificare gli indirizzi IP dei pacchetti in arrivo e blocca quelli non presenti nella lista predefinita.

1. DMZ (zona demilitarizzata): È una sottorete che contiene servizi accessibili dall'esterno, come i server HTTP e SMTP. La DMZ è separata dalla rete interna per aumentare la sicurezza, in modo che eventuali compromissioni dei server nella DMZ non mettano a rischio la rete interna.
2. HTTP e SMTP: Sono server che gestiscono rispettivamente il traffico web (HTTP) e la posta elettronica (SMTP). Sono posizionati nella DMZ per essere accessibili dall'esterno senza compromettere la sicurezza della rete interna.
3. IPS (Intrusion Prevention System): Ho deciso di posizionare il dispositivo tra la DMZ e il router. La sua funzione è quella di monitorare il traffico di rete per rilevare e prevenire intrusioni e attacchi. Un IPS può bloccare il traffico di rete considerato pericoloso.
4. Router: Il router collega la DMZ alla rete interna. Gestisce il traffico tra le diverse sottoreti e instrada i pacchetti di dati verso le destinazioni corrette, è ciò che permette di comunicare verso reti esterne.
5. Switch: Lo switch è collegato al router e gestisce il traffico di rete ai vari dispositivi nella rete interna. Permette la comunicazione tra i dispositivi collegati nella stessa rete.
6. PC1, PC2, PC3, PC4: Questi sono computer collegati alla rete interna tramite lo switch. Possono comunicare tra loro.
7. IDS (Intrusion Detection System): Questo dispositivo è collegato allo switch e al NAS. La sua funzione è quella di monitorare il traffico di rete per rilevare attività sospette o non autorizzate. L’IDS non ha una funzionalità attiva come l’IPS ma si limita a segnalare le attività sospette. Ho posizionato l’IDS tra lo switch e il NAS come misura preventiva di attività sospetta, così da avere una risposta in tempo reale.
8. NAS (Network Attached Storage): Nella parte più interna della rete locale è posizionato il NAS, “sorvegliato” da un IDS.  
   Il NAS è essenziale per la gestione e l’archiviazione dei dati. È un dispositivo di archiviazione collegato alla rete che consente a più utenti di accedere ai dati archiviati, ciò facilita la condivisione di file e il backup dei dati.

In conclusione, la configurazione descritta offre un buon equilibrio tra sicurezza e funzionalità. Ogni componente ha un ruolo chiaro: il firewall gestisce il traffico in entrata, la DMZ protegge i servizi esposti al pubblico, e l’IPS/IDS rilevano e bloccano minacce.