

PRESENTAZIONE PROGETTO DEL VENERDÌ

S3/L5

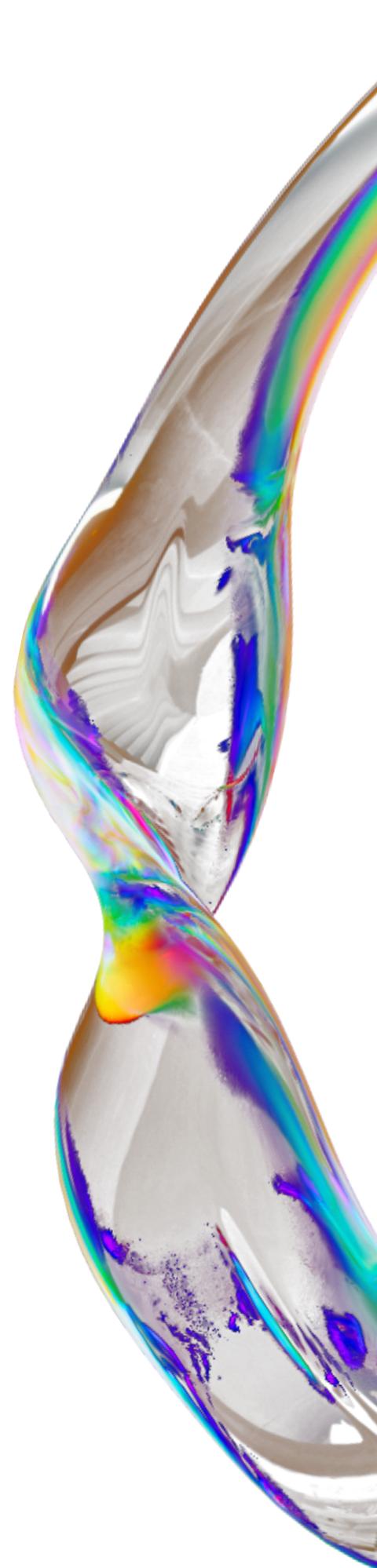
Mirka Febbo



Introduzione alla Configurazione di Rete con pfSense, Metasploitable2 e Kali Linux

Benvienuti a questa presentazione dettagliata sulla configurazione di una rete segmentata utilizzando pfSense come firewall centrale, affiancato da Metasploitable2 e Kali Linux su reti separate. L'obiettivo principale è dimostrare come segmentare il traffico e applicare regole di firewall precise per controllare la comunicazione tra le macchine virtuali.

Iniziamo con l'impostazione degli indirizzi IP per le nostre macchine virtuali, che risiederanno su subnet distinte per garantire una chiara separazione del traffico.



Assegnazione degli Indirizzi IP per Metasploitable2 e Kali Linux

Per stabilire l'architettura di rete, ho assegnato i seguenti indirizzi IP alle macchine Metasploitable2 e Kali Linux:

Metasploitable2 (Nome: Meta):

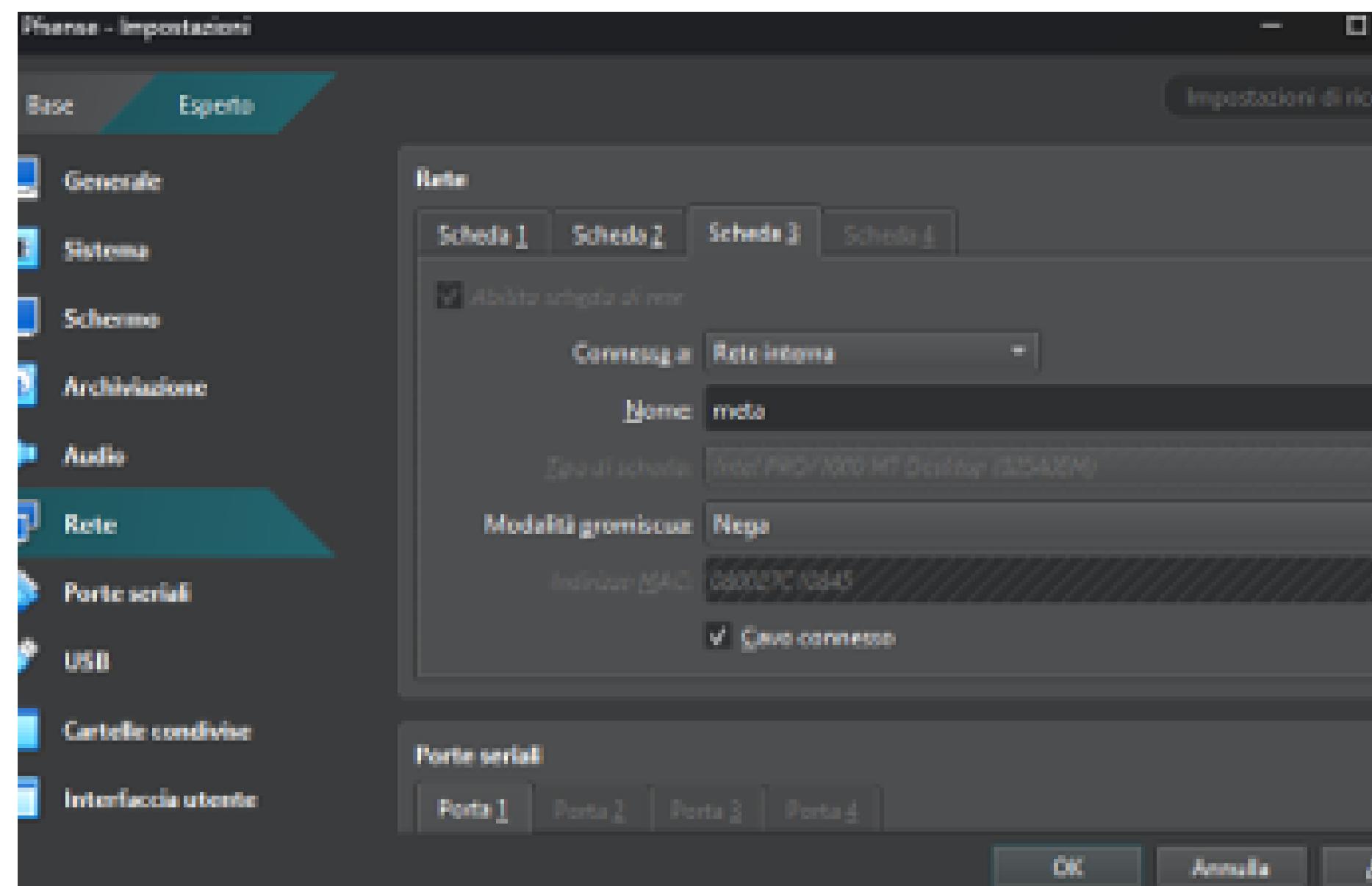
- Indirizzo IP: 192.168.10.100
- Gateway: 192.168.10.1

Kali Linux (Nome: intnet):

- Indirizzo IP: 192.168.50.100
- Gateway: 192.168.50.1

Come potete notare, Metasploitable2 e Kali Linux operano su due reti completamente separate.

Questa segmentazione iniziale è fondamentale per implementare un controllo granulare del traffico tramite pfSense.



Una volta definite le reti per Metasploitable2 e Kali Linux, il passo successivo è l'introduzione di pfSense. Ho creato una terza rete dedicata esclusivamente a pfSense, che fungerà da punto centrale per il routing e il filtraggio del traffico (vedere immagine sopra).

Dopo l'avvio della macchina virtuale pfSense, ho proceduto alla sua configurazione iniziale. Tramite il browser di Kali Linux, ci siamo connessi all'interfaccia web di pfSense. Da qui, abbiamo aggiunto l'interfaccia di rete che si conserverà alla rete di Metasploitable2, denominandola OPT1Meta. Questa interfaccia è stata configurata con il gateway appropriato (192.168.10.1) per garantire la corretta comunicazione con la subnet di Metasploitable2.

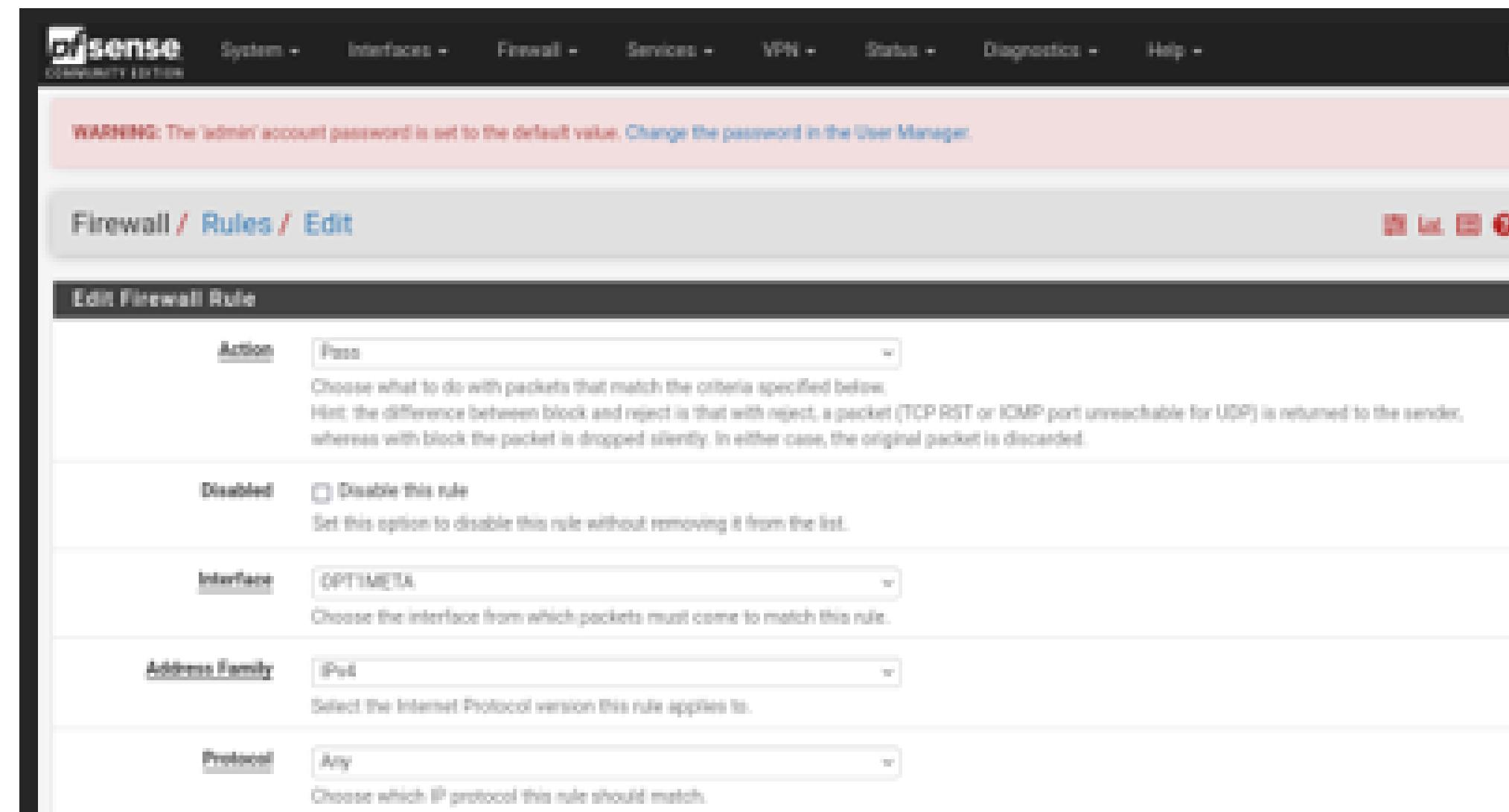


Configurazione Iniziale delle Regole su pfSense: Permesso di Traffico

Con le interfacce configurate e attive, il passo successivo è definire le regole del firewall su pfSense per gestire il flusso di pacchetti tra le reti. La nostra prima regola, configurata tramite la tab "Rules" di pfSense, ha lo scopo di permettere un passaggio specifico di traffico:

- Azione: Pass (permette il passaggio dei pacchetti).
- Interfaccia: OPT1META (si applica al traffico in arrivo o in partenza dall'interfaccia collegata alla rete di Metasploitable2).
- Sorgente (Source): 192.168.10.100 (il nuovo indirizzo IP di Metasploitable2).

Questa regola consente a Metasploitable2 di avviare o ricevere connessioni sull'interfaccia OPT1META, stabilendo una base per la comunicazione nella nostra architettura.



Implementazione di una Regola di Blocco Specifica: Prevenire l'Accesso HTTP

Per dimostrare l'efficacia del filtraggio di pfSense, abbiamo implementato una regola di blocco mirata a prevenire l'accesso al servizio HTTP (porta 80) su Metasploitable2 da parte di Kali Linux. Questa regola è cruciale per la sicurezza e la segmentazione della rete.

Ecco le configurazioni dettagliate di questa regola firewall:

- Azione: Block (i pacchetti che corrispondono a questi criteri verranno scartati).
- Interfaccia: LAN (questa regola si applica ai pacchetti che arrivano sull'interfaccia LAN di pfSense, che in questo scenario rappresenta la rete di Kali Linux).
- Indirizzo di Origine (Source): 192.168.50.100 (l'indirizzo IP di Kali Linux).
- Indirizzo di Destinazione (Destination): 192.168.10.100 (il nuovo indirizzo IP di Metasploitable2).
- Protocollo: TCP (la regola si applica specificamente ai pacchetti TCP).
- Porta di Destinazione: HTTP (porta 80) (la regola blocca il traffico diretto verso il servizio HTTP sulla macchina di destinazione).

Questa regola impedisce efficacemente a Kali Linux di accedere al servizio HTTP sulla macchina Metasploitable2, nonostante le due macchine siano connesse tramite pfSense.

The screenshot shows the pfSense Firewall Rules configuration interface. The main title is "Firewall / Rules / Edit". Below it, the sub-section is "Edit Firewall Rule". The configuration details are as follows:

- Action:** Block
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP

Below the protocol section, there is a note: "Choose which IP protocol this rule should match."

Verifica dell'Obiettivo Raggiunto e Prossimi Passi

Con l'implementazione delle regole di permesso e blocco su pfSense, il nostro obiettivo di segmentare le reti e controllare il traffico tra Metasploitable2 e Kali Linux è stato raggiunto.

Abbiamo dimostrato come:

- Assegnare indirizzi IP su subnet separate.
- Configurare pfSense con più interfacce.
- Implementare regole di firewall per permettere e bloccare il traffico in modo selettivo.

Il passo finale, e più importante, è testare l'efficienza di queste regole. Proveremo a connetterci via HTTP da Kali a Metasploitable2 per verificare che la regola di blocco funzioni come previsto e che l'accesso venga negato. Questo tipo di configurazione è fondamentale per la sicurezza di qualsiasi infrastruttura di rete, permettendo un controllo preciso su chi può comunicare con cosa.

In conclusione:

In conclusione, Creare un firewall è stata una grande sfida,
ma la soddisfazione di esserci riuscita ripaga molto.



Mirka Febbo