



VPN Site-to-Site

Connessione Sicura tra Reti

Una VPN site-to-site protegge i dati cifrandoli prima di inviarli su Internet.

Una volta raggiunta la destinazione, i dati vengono decifrati, garantendo una comunicazione sicura tra le reti.

Questo tipo di VPN è ideale per aziende con più sedi o per chi necessita di un accesso remoto sicuro.

BARUFFOLO NOEMI e RINALDI DANILO 5^ AROB

Tipologie di VPN: Quale Scegliere?

VPN Site-to-Site

Connette sedi aziendali creando un'infrastruttura sicura per la comunicazione e la condivisione di risorse interne.

- Ideale per aziende con filiali
- Condivisione sicura di file

VPN di Accesso Remoto

Consente agli utenti di connettersi in modo sicuro alla rete aziendale da qualsiasi luogo, ideale per lo smart working.

- Perfetta per lavoratori remoti
- Accesso sicuro alle risorse

Altri Tipi di VPN: Trusted e Secure

VPN Affidabile (Trusted)

Fornita da un provider esterno, ideale per aziende senza un team IT dedicato, garantendo sicurezza senza gestione interna.

- Adatta ad aziende senza IT dedicato
- Sicurezza gestita esternamente

VPN Sicura (Secure)

Utilizza protocolli avanzati di crittografia per proteggere i dati trasmessi, assicurando un elevato livello di protezione.

- Elevata protezione dei dati
- Sicurezza per informazioni riservate



Vantaggi Chiave di una VPN



Maggiore Sicurezza

Crypta i dati, impedendo intercettazioni e proteggendo le informazioni sensibili da accessi non autorizzati.



Accesso Remoto Protetto

Consente di connettersi in modo sicuro da qualsiasi luogo, proteggendo anche su reti pubbliche.



Superamento Restrizioni

Permette di accedere a contenuti e servizi bloccati in base alla posizione geografica.



Ulteriori Vantaggi: Privacy e Anonimato



Tutela della Privacy

Nasconde l'indirizzo IP e la posizione dell'utente, impedendo il tracciamento durante la navigazione.



Maggiore Anonimato

Garantisce maggiore anonimato online, proteggendo l'identità dell'utente.

L'utilizzo di una VPN non solo aumenta la sicurezza e l'accessibilità, ma offre anche un livello superiore di privacy e anonimato, proteggendo la tua identità digitale da occhi indiscreti.

Configurazione VPN Site-to-Site con pfSense

Obiettivo e Setup

L'obiettivo è creare un tunnel VPN tra due firewall pfSense per consentire la comunicazione tra le LAN. I firewall sono configurati in modalità bridge per non bloccare il traffico.

pfSense 1 (Noemi)

- WAN: 192.168.229.134/24
- LAN: 192.168.1.1/24

pfSense 2 (Danilo)

- WAN: 192.168.144.140/24
- LAN: 192.168.2.1/24

Il tunnel VPN utilizza la rete 10.200.0.0/24, collegando le due LAN.

Configurazione Server OpenVPN e Client OpenVPN

1

Server (pfSense Noemi)

Configurare i parametri del server OpenVPN su pfSense di Noemi: Server Mode, Protocol, Interface, Tunnel Network, ecc.

2

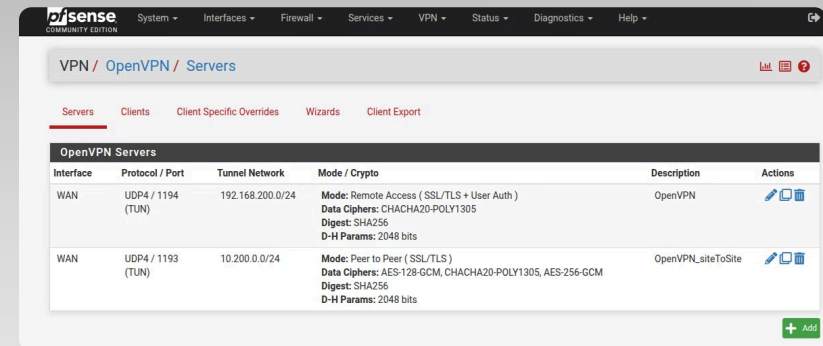
Certificati

Creare un CA interno e un certificato server tramite il Certificate Manager.

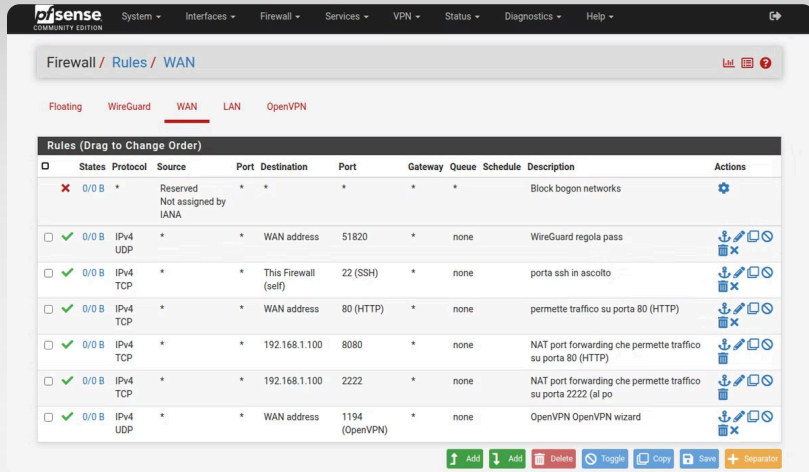
3

Client (pfSense Danilo)

Configurare i parametri del client OpenVPN su pfSense di Danilo e caricare i certificati generati.



Configurazione Firewall, Rotte e Test di Connessione



Firewall

Aggiungere una regola sul firewall per permettere tutto il traffico OpenVPN.

Rotte

Aggiungere una nuova rotta su entrambi i pfSense per indirizzare il traffico.

Test

Eseguire ping tra le LAN per verificare la connessione e controllare eventuali problemi.

Dopo aver completato questi passaggi, le LAN potranno comunicare tramite il tunnel VPN. Verificare le configurazioni e correggere eventuali problemi di connessione.

Problemi Riscontrati

Abbiamo tentato di implementare la configurazione VPN, ma abbiamo incontrato delle difficoltà.

OpenVPN e WireGuard sulla macchina virtuale di Danilo non hanno funzionato con pfSense.

Di conseguenza, non è stato possibile completare tutti i passaggi inizialmente previsti.

Entrando in una rete comune risultava impossibile accedere a pfSense perché l'IP 192.168.1.1 dirottava alla pagina di configurazione del nostro router fisico

Origine Tutorial

Il tutorial seguito è stato preso da risorse online e YouTube.

Configurazione

Abbiamo seguito tutti i passaggi per la macchina virtuale di Noemi solamente.

