***BARUFFOLO NOEMI RINALDI DANILO 5^AROB***

**VPN SITE-TO-SITE**

**DEFINIZIONE**

**Una VPN (Virtual Private Network) site-to-site protegge i dati cifrandoli in un punto della rete prima di inviarli attraverso Internet. Una volta raggiunta la destinazione, i dati vengono decifrati e instradati verso il loro obiettivo finale, garantendo una comunicazione sicura tra le due reti.**

**TIPOLOGIE DI VPN**

**Esistono diversi tipi di VPN, ciascuno con caratteristiche specifiche pensate per diversi scenari d’uso:**

**1. VPN Site-to-Site**

* **Descrizione: Connette due o più sedi aziendali attraverso una rete privata virtuale, creando un’infrastruttura sicura per la comunicazione tra le sedi.**
* **Vantaggi: Ideale per aziende con più filiali, permette la condivisione sicura di file e risorse interne.**
* **Esempi di utilizzo: Collegamento tra sede centrale e uffici periferici, creazione di una rete aziendale distribuita.**

**2. VPN di Accesso Remoto (Remote Access VPN)**

* **Descrizione: Consente agli utenti di connettersi in modo sicuro alla rete aziendale da qualsiasi luogo, utilizzando una connessione Internet.**
* **Vantaggi: Perfetta per lavoratori in smart working o in viaggio, garantisce accesso sicuro alle risorse aziendali da qualsiasi dispositivo.**
* **Esempi di utilizzo: Connessione da casa ai server aziendali, accesso a file e software aziendali durante trasferte di lavoro.**

**3. VPN Affidabile (Trusted VPN)**

* **Descrizione: Servizio VPN fornito da un provider esterno, che gestisce l’infrastruttura e garantisce una connessione sicura.**
* **Vantaggi: Adatta alle aziende che non dispongono di un team IT dedicato, offre sicurezza senza necessità di gestione interna.**
* **Esempi di utilizzo: Imprese con esigenze di sicurezza elevate, aziende con risorse IT limitate.**

**4. VPN Sicura (Secure VPN)**

* **Descrizione: Utilizza protocolli avanzati di crittografia e sicurezza per proteggere i dati trasmessi sulla rete.**
* **Vantaggi: Assicura un elevato livello di protezione per la navigazione e l’accesso a risorse sensibili.**
* **Esempi di utilizzo: Protezione dei dati su reti Wi-Fi pubbliche, sicurezza per chi gestisce informazioni riservate online.**

**VANTAGGI DI UNA VPN**

**L’utilizzo di una VPN offre numerosi benefici, migliorando sicurezza, accessibilità e privacy online:**

* **Maggiore sicurezza   
  Una VPN cripta i dati trasmessi, impedendo intercettazioni e proteggendo le informazioni sensibili da accessi non autorizzati.**
* **Accesso remoto protetto   
  Consente di connettersi in modo sicuro a reti aziendali o personali da qualsiasi luogo, garantendo protezione anche su reti pubbliche.**
* **Superamento delle restrizioni geografiche   
  Permette di accedere a contenuti e servizi bloccati in base alla posizione geografica, come siti web, piattaforme di streaming o servizi online.**
* **Tutela della privacy   
  Nasconde l’indirizzo IP e la posizione dell’utente, impedendo il tracciamento durante la navigazione e garantendo maggiore anonimato online.**

**COME DOVREBBE FUNZIONARE**

**Configurazione VPN Site-to-Site con pfSense**

**Obiettivo**

L'obiettivo è creare un tunnel VPN tra due firewall pfSense in modo che le LAN di ciascun sistema possano comunicare tra loro. I firewall sono configurati in modalità bridge per non bloccare il traffico tra le reti.

**Configurazione di rete**

**Setup iniziale**

* **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.

**1. Configurazione del Server OpenVPN su pfSense di Noemi**

1. Andare su **VPN > OpenVPN > Servers**, cliccare su Add.
2. Configurare i seguenti parametri:
   * **Server Mode:** Peer to Peer (SSL/TLS)
   * **Protocol:** UDP
   * **Interface:** WAN
   * **Local Port:** 1194
   * **Tunnel Network:** 10.200.0.0/24
   * **Local Network:** 192.168.1.0/24
   * **Remote Network:** 192.168.2.0/24
   * **TLS Authentication:** Abilitato
   * **Data Cipher:** AES-256-GCM
3. Salvare e applicare le modifiche.

**Creazione dei certificati**

1. Andare su **System > Certificate Manager > CAs**, cliccare Add e creare un CA interno.
2. Andare su **System > Certificate Manager > Certificates**, cliccare Add e creare un certificato server.

**2. Configurazione del Client OpenVPN su pfSense di Danilo**

1. Andare su **VPN > OpenVPN > Clients**, cliccare su Add.
2. Configurare i seguenti parametri:
   * **Server Mode:** Peer to Peer (SSL/TLS)
   * **Protocol:** UDP
   * **Server Address:** 192.168.229.134
   * **Port:** 1194
   * **Tunnel Network:** 10.200.0.0/24
   * **Local Network:** 192.168.2.0/24
   * **Remote Network:** 192.168.1.0/24
3. Caricare i certificati generati su pfSense 1.
4. Salvare e applicare le modifiche.

**3. Configurazione del Firewall su entrambi i pfSense**

Andare su **Firewall > Rules > OpenVPN** e aggiungere una regola per permettere tutto il traffico:

* **Protocol:** Any
* **Source:** Any
* **Destination:** Any
* **Action:** Allow

**4. Configurazione delle Rotte su entrambi i pfSense**

Andare su **System > Routing > Gateways** e aggiungere una nuova rotta.

**Su pfSense di Noemi (192.168.229.134):**

* **Network:** 192.168.2.0/24
* **Gateway:** 10.200.0.2

**Su pfSense di Danilo (192.168.144.140):**

* **Network:** 192.168.1.0/24
* **Gateway:** 10.200.0.1

**5. Test della Connessione**

1. Aprire un terminale su una macchina nella LAN di pfSense di Noemi (192.168.1.100).
2. Eseguire ping 192.168.2.100.
3. Ripetere il test dalla LAN di pfSense di Danilo (192.168.2.100) verso 192.168.1.100.

**Se il ping non funziona:**

* Controllare le regole del firewall.
* Verificare che il tunnel OpenVPN sia attivo in Status > OpenVPN.
* Controllare le rotte statiche.

**Conclusione**

Dopo aver completato questi passaggi, le LAN di entrambe le configurazioni potranno comunicare tra loro tramite il tunnel VPN.

Se necessario, bisogna verifica le configurazioni e correggere eventuali problemi di connessione.