**VPN (Virtual Private Network)**

**Che cos’è una Vpn?**

È una delle implementazioni più usate dell’IPSec ed è una **rete** **privata** che si **appoggia su una rete pubblica**. **Garantisce** la **confidenzialità**, **l'integrità** e **l'autenticazione** delle informazioni scambiate su quella rete.

**Vantaggi e svantaggi di utilizzare una rete privata (non è Vpn):**

**Vantaggi:**

* Larghezza di banda sempre disponibile
* Nessun problema di accesso
* Nessuna congestione del traffico (almeno non al livello di rete)
* Prestazioni e sicurezza garantite

**Svantaggi:**

* Mancanza di scalabilità e si deve contattare col provider per avere una banda maggiore
* Rischio del blocco della rete in casi di guasto su un canale (non c’è ridondanza)
* Alti costi di installazione
* Tempi lunghi per la configurazione e la riconfigurazione

**Vantaggi e svantaggi di una Vpn:**

**Vantaggi:**

* Facile configurazione e riconfigurazione
* È scalabile
* Valido rapporto tra costi e funzionalità
* Il rischio di blocco di rete è nullo

**Svantaggi:**

* La variabilità del tempo di trasferimento
* Il controllo degli accessi
* La sicurezza delle trasmissioni

Gli ultimi due svantaggi vengono affrontati impiegando una combinazione di 3 fattori: **autenticazione, cifratura** e **tunneling.**

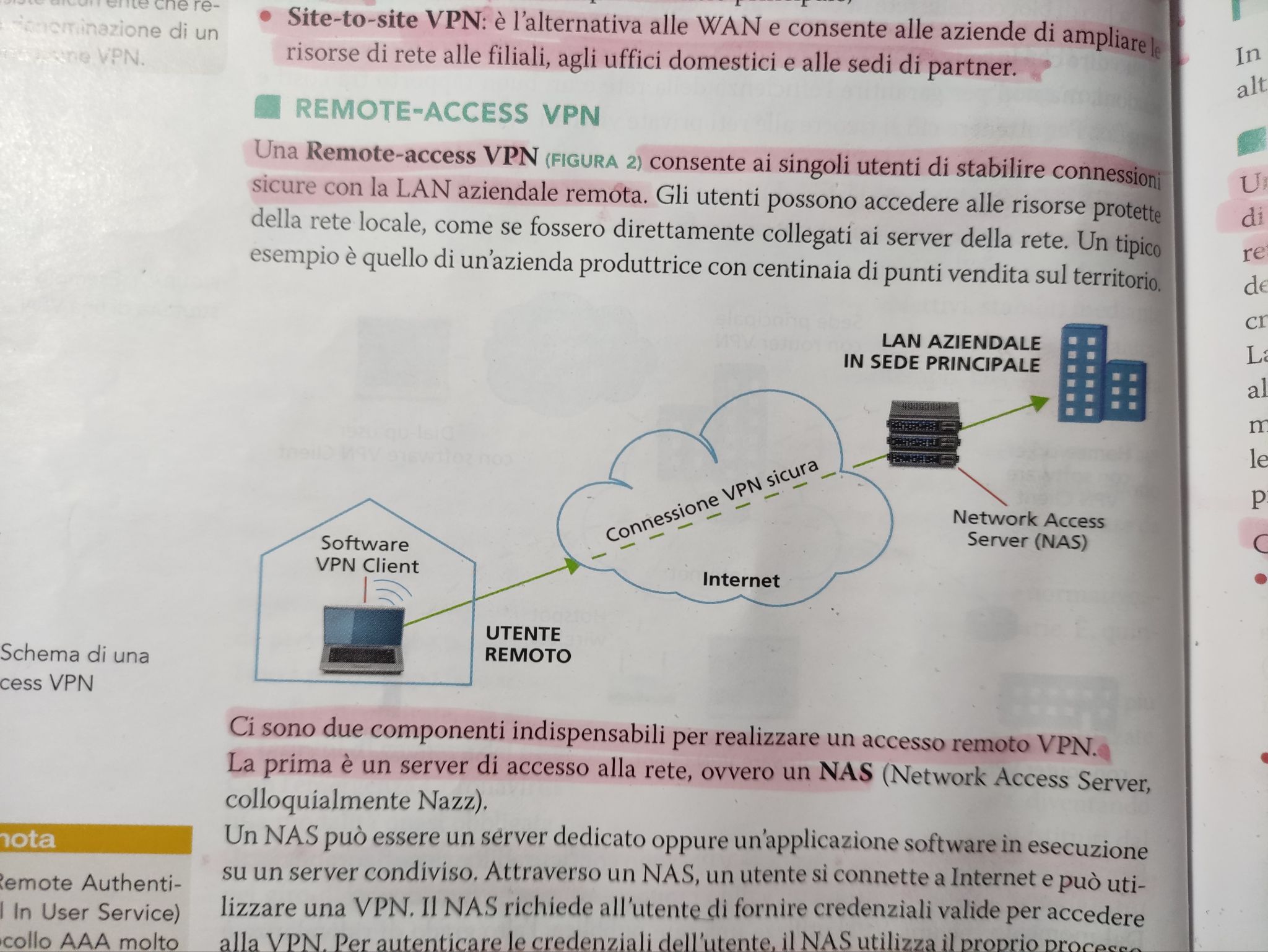
**Tipi di VPN in ambito commerciale:**

**Remote access VPN:**

Consente ai singoli utenti di stabilire connessioni sicure con la LAN aziendale remota. Ci sono **due** **componenti** **essenziali** per realizzare un accesso remoto VPN:

* **NAS**: con questo l’utente si connette a Internet e può utilizzare una VPN. Per autenticare le credenziali dell’utente, il NAS ha il proprio processo di autenticazione o si può usare un server di autenticazione separato come **RADIUS AAA** (**Authentication** **Authorization** **Accounting**) **Server**.
* **Software VPN Client**

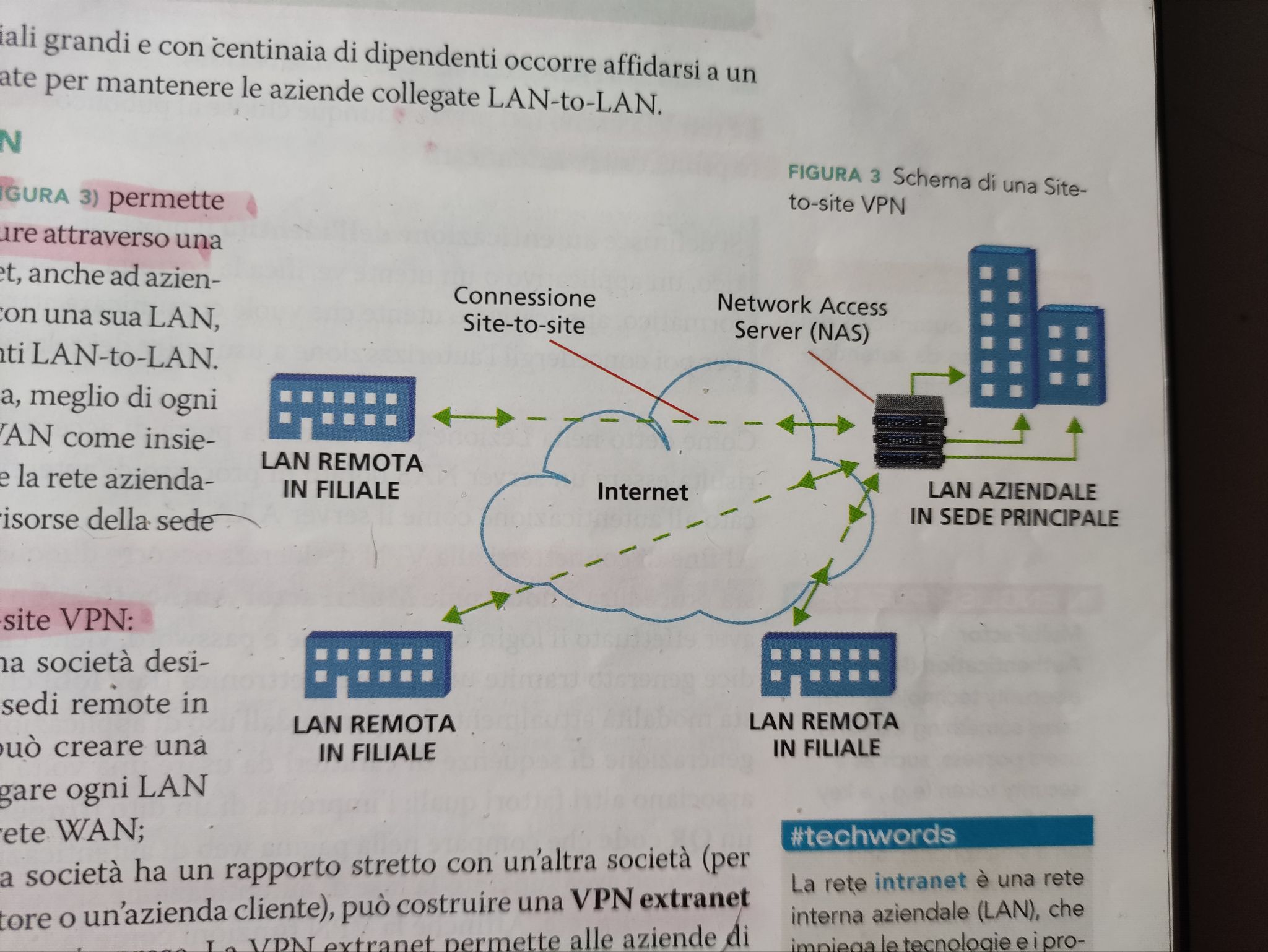
Inoltre è necessario anche un firewall che fornisce una barriera tra la LAN privata e Internet.



**Site-to-site VPN:**

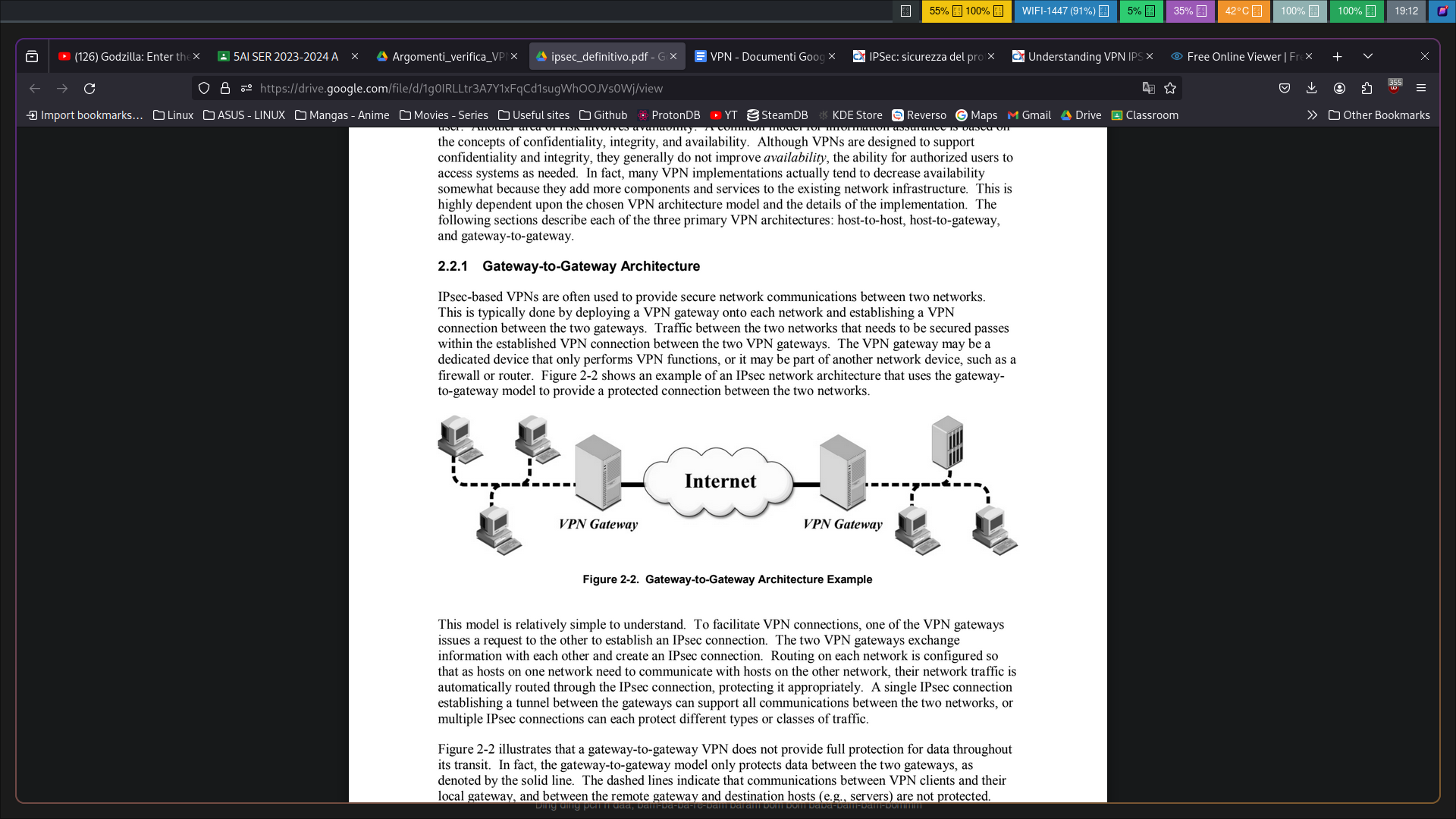
Permette di stabilire connessioni sicure attraverso una rete pubblica. Ci sono due tipi :

* **Intranet-based**: una società decide di unire le reti delle sedi remote in un'unica rete privata, quindi creare una **VPN** **intranet** per collegare ogni LAN separata in una singola rete WAN.
* **Extranet-based**: un’azienda crea una **VPN** **extranet** per permettere di collegarsi con le LAN di altre aziende o clienti o fornitori.



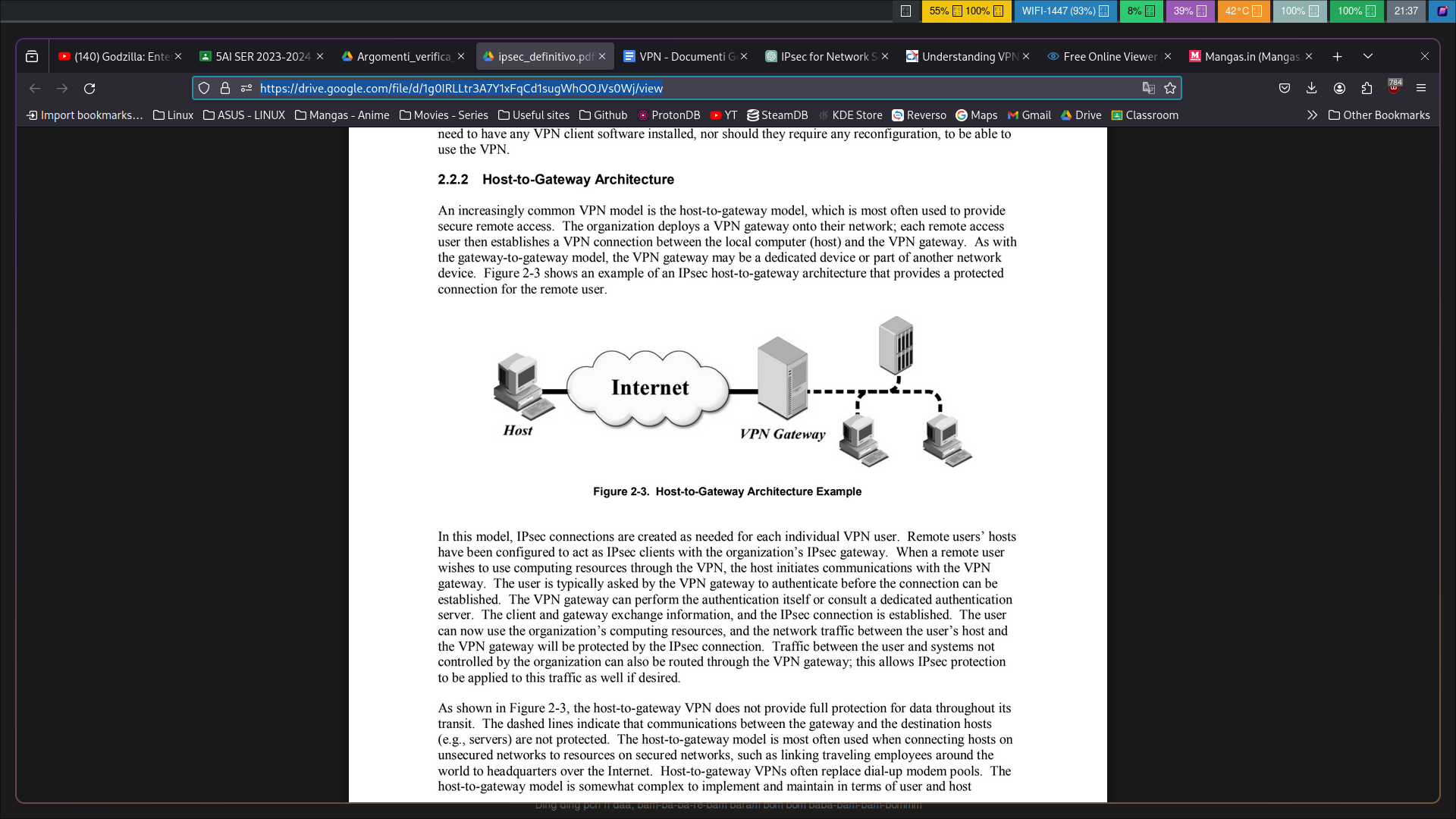
**Le 3 principali architetture di VPN:**

**Gateway-Gateway architecture:**



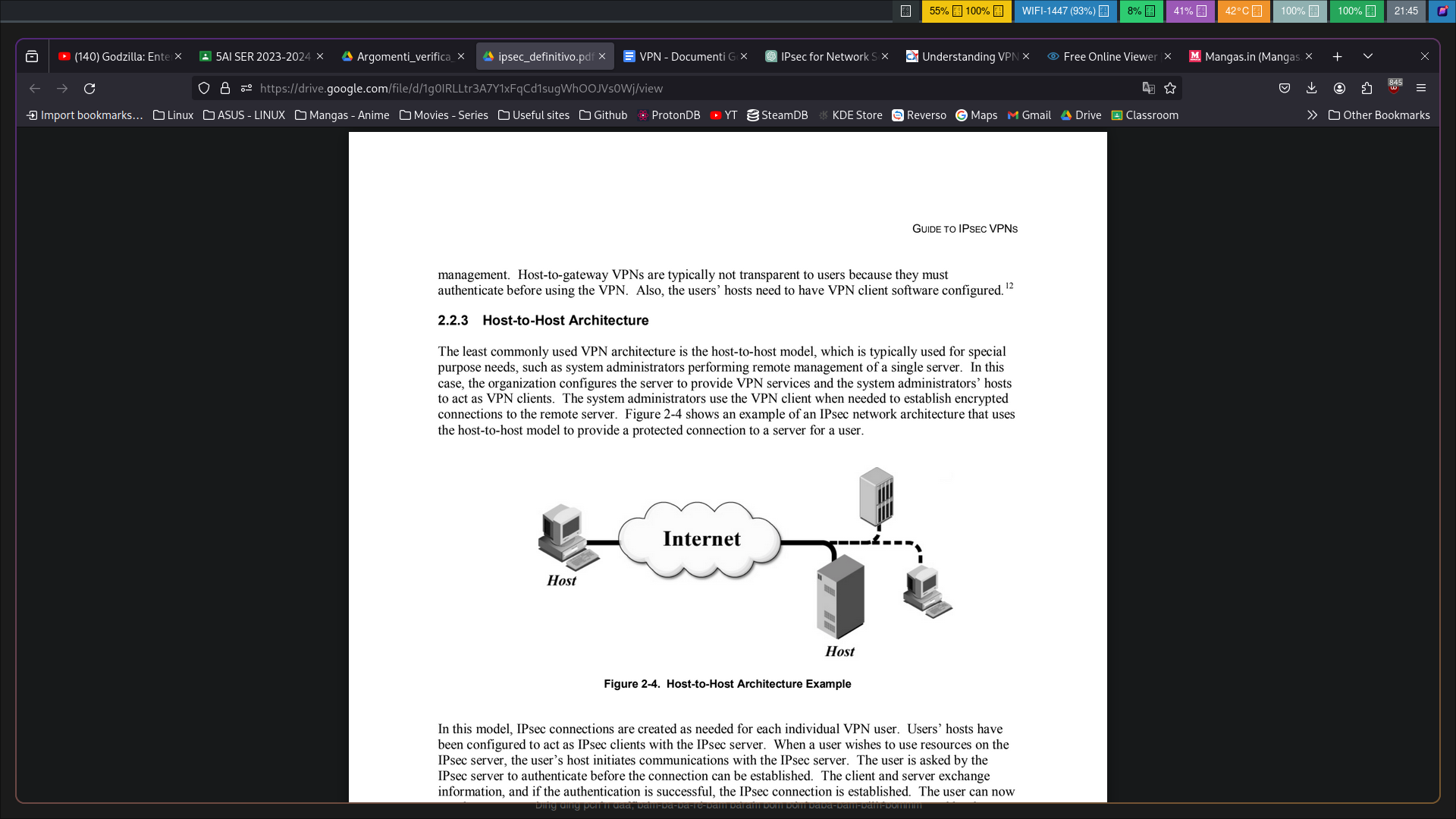
I gateway di due reti stabiliscono una rete sicura attraverso una rete pubblica di solito Internet. Questa configurazione consente alle reti aziendali di comunicare tra loro in modo sicuro e privato. Si deve tener conto che le linee tratteggiate indicano che non sono protette.

**Host-to-Gateway architecture:**



Un host da remoto stabilisce una connessione sicura con il gateway di una rete. Prima che venga stabilita la connessione, la VPN Gateway chiede all’host l’autenticazione. L’autenticazione può essere gestita dalla stessa VPN gateway o da un server dedicato.

**Host-to-Host architecture:**

****

Si stabilisce una connessione sicura tra host specifici e ovviamente prima di stabilire la connessione, deve essere gestita l’autenticazione.

**Sicurezza nei livelli TCP/IP**

**Application layer:**

La sicurezza viene gestita singolarmente da ogni programma.

**Transport layer:**

La sicurezza può essere garantita in una singola connessione da host a host, le informazioni IP non sono nascoste. Il protocollo più comune in questo layer è la sicurezza per HTTP (TLS).

**Network layer:**

Qui la sicurezza viene applicata su ogni applicazione, la connessione tra due host può essere completamente protetto, visto che vengono criptate le informazioni dell’IP.

**Data Link layer:**

La sicurezza viene applicata fisicamente, criptando tutto quello che passa per quella strada. Il problema per fare questo sono i costi che sono alti.