

Scenario

Troubleshooting:

E' un processo di identificazione del problema attraverso una eliminazione progressiva logica e sistematica delle cause che possono averlo generato.

Descrizione Attività:

E' la settimana centrale di Agosto.

L'ufficio è chiuso e chi lavora lo sta facendo in Smart-Working da casa, te compreso.

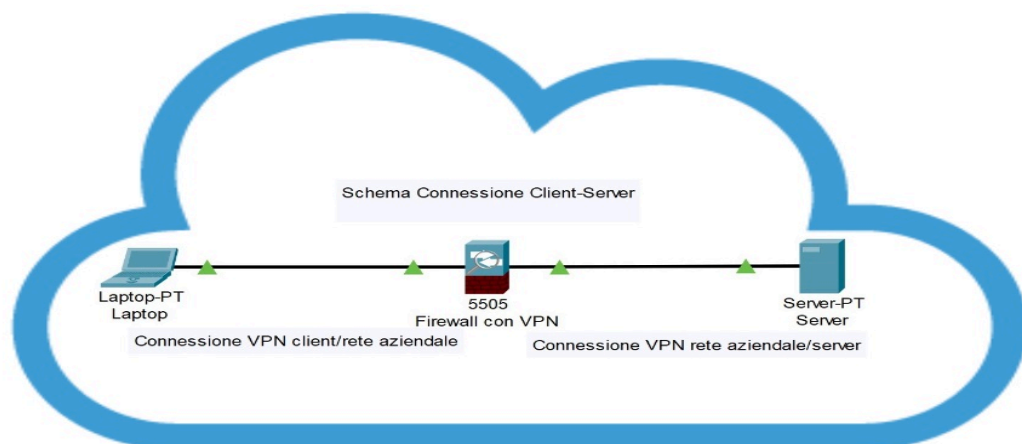
Sono le 8.45 del mattino accendi il computer e noti che nel canale Slack dedicato al supporto tecnico un tuo collega manifesta problemi nel collegarsi ad un server remoto dell'azienda che è in cloud.

Oggetto della sua richiesta è *"non riesco a collegarmi al server dell' [ERP](#)"*

Nessuna descrizione aggiuntiva.

Alle 9.00 altri colleghi iniziano a collegarsi su Slack e ti manifestano lo stesso problema: non riescono a collegarsi al server.

L'infrastruttura di rete della tua aziende è la seguente:



Alcune info sullo schema precedente:

- Client: è considerato l'hardware con il quale si connette alla rete, quindi computer aziendale in dotazione all'utente. N.B.: le impostazioni di un dispositivo aziendale non possono essere modificate in autonomia dall'utente
- VPN: significa, virtual private network: è una rete privata virtuale che garantisce privacy, anonimato e sicurezza attraverso un canale di comunicazione logicamente riservato (tunnel VPN) e creato sopra un'infrastruttura di rete pubblica. Il termine virtuale sta a significare che tutti i dispositivi appartenenti alla rete non devono essere necessariamente collegati ad una stessa LAN locale ma possono essere dislocati in qualsiasi punto geografico del mondo.
- Firewall: può essere fisico o virtuale (WAF) è installato tra la rete aziendale e internet. Immaginate la rete aziendale non come se fosse il vostro ufficio ma potenzialmente distribuita per tutto il pianeta. Il firewall serve a proteggerla grazie alla sua capacità di filtrare le chiamate che arrivano verso i vostri server. Un firewall per funzionare bene necessita di regole che sono impostate solitamente dall' IT Support oppure dal Sistemista. Con le regole si decide quali chiamate sono ammesse verso la nostra infrastruttura e quali no.
- Antivirus: i primi antivirus effettuavano un controllo meccanico, ovvero verificavano se nel proprio data base era presente o meno la firma del virus, signature-based (come se fosse l'impronta digitale). Questo metodo seppure alla base del meccanismo è limitato ed efficace parzialmente. Oggi gli antivirus sono molto più evoluti se vuoi approfondire l'argomento di consiglio la lettura di questo [articolo](#) vedremo anche i dettagli del comportamento di alcune tipologie di virus nel corso: Introduction To Cyber-Security.

Ecco cosa devi fare in questo esercizio:

- Indica che genere di problemi puoi escludere, sulla base delle informazioni fornite.
- Indica le domande che porresti ai tuoi colleghi per fare il Troubleshooting del problema seguendo lo schema:
 1. Identificazione del Problema.
 - Domande a risposta aperta. ...
 - Domande a risposta chiusa. ...
 2. Teoria sulle Probabili Cause. ...
 3. Test sulle Probabili Cause. ...

Nota bene: In questo esercizio non devi trovare qual è la soluzione esatta del problema non hai informazioni a sufficienza per poterla identificare. Devi spiegare che cosa almeno puoi escludere lo stia causando e come raccoglieresti le informazioni che ti servono per l'analisi e in quale parte dell'infrastruttura può essere localizzata se tra: client e firewall o tra firewall e server.

Per raccogliere le informazioni ti suggeriamo di utilizzare sempre una tabella a supporto in modo che tu possa aggregare le informazioni:

Esempio

Domanda	Risposta	Motivazione

Domanda	Risposta	Motivazione
State riscontrando anche problemi di rete domestica?	No, sto solo riscontrando problemi nel connettermi in remoto.	Per capire se il problema riguarda solamente il collegamento in remoto o anche della rete internet.
Vi siete assicurati che il computer sia abilitato in	si.	Per assicurarmi che semplicemente la

remoto con il server dell'azienda?		connessione in remoto non eradisabilitata.
Cosa stavate facendo quando si è verificato il problema?	Mi stavo connettendo al server ERP.	Per capire se il problema si è verificato mentre faceva qualcosa e quindi causato da lui e quando.
Ha provato a vedere se il problema si verifica quando vi connettete alla VPN e verificare se si tratta della VPN?	Si e il problema si verifica quando ci connettiamo alla Per capire se è un problema di VPN..	Per capire se è un problema di VPN.
Che tipo di browser state usando?	Chrome.	Per capire se è un problema di browser.
Avete provato a verificare se con altri browser?	Si.	Per capire se hanno provato ad usare altri browser ed escludere un possibile problema di browser.
Avete provato a verificare se il firewall è attivo?	Si.	Per capire se c'è qualche problema di firewall.
Avete installato qualche tipo di aggiornamento recentemente?	Si.	Per capire se un aggiornamento ha creato conflitti o rallentamenti.
Verificate degli errori quando provate a connettervi?	Si.	Cercare di capire quali tipi di errori ci sono nel caso si verificano nel momento della connessione.
Avete provato a fare una scansione?	Si.	Per verificare se ci sono malware o virus nel computer.

Non avendo informazioni a sufficienza non posso raggiungere una vera e propria conclusione ma penso che una teoria probabile potrebbe essere un problema tra firewall e server.

