# Client VPN: impossibile verificare correttamente l'errore di modifica della tabella di inoltro IP su Secure Client RAVPN Split-Tunnel/DNS predefinito

## Sommario

## Problema

Gli utenti Mac riscontrano errori intermittenti durante il tentativo di autenticazione CLI ad applicazioni interne mentre sono connessi a Cisco Secure Client VPN. Gli errori presenti come errori di "host non trovato" durante l'autenticazione CLI e quando si utilizzano comandi come `curl`. Tuttavia, i comandi di risoluzione DNS come `nslookup` e `dig hanno` esito positivo. Il problema si verifica in modo casuale e può essere temporaneamente risolto riconnettendo la VPN, dopo di che la connettività funziona per un breve periodo prima che si verifichi di nuovo il problema. La VPN split-tunnel è in uso e Cisco Umbrella è attiva. Il problema non si verifica quando si utilizza Palo Alto GlobalProtect VPN.

- Messaggio di errore: "host not found" (host non trovato) sull'autenticazione CLI e sui comandi `curl`.
- Messaggio di errore: il client VPN non è in grado di verificare correttamente le modifiche apportate alla tabella di inoltro IP. Problema di risoluzione DNS (Domain Name Server) durante la connessione delle risorse private
- comandi `nslookup` e `dig` riusciti
- Connettività intermittente dopo la riconnessione della VPN
- Accesso remoto con split-tunnel, VPN e modulo Umbrella abilitati
- Problema riproducibile solo con Cisco Secure Client VPN su dispositivi MacOS

## Ambiente

- Prodotto: Cisco Secure Client (CSC) con più moduli
- Piattaforma: dispositivi Mac aziendali
- Configurazione profilo VPN: profilo VPN ad accesso remoto - Ignora accesso sicuro - Modalità split-tunnel e modalità DNS selezionate come "DNS predefinito"
- Filtro DNS: Cisco Umbrella abilitato
- Versioni modulo:
    - Cloud Management v1.0.0.23
    - AnyConnect VPN v5.1.13.17
    - Umbrella v5.1.13.177

    - DART v5.1.13.17
    - Secure Firewall Posture v5.1.13.177
    - Network Visibility Module v5.1.13.177
- Dati diagnostici: bundle DART raccolti per l'analisi
- Osservato solo su Cisco Secure Client VPN (non su Palo Alto GlobalProtect)

# Risoluzione

- Durante il debug della configurazione del profilo VPN (`naic.org`) per lo split-tunnel e della tabella di routing della VPN AnyConnect sul lato client, è stato osservato questo comportamento:
    - Scenario di lavoro: quando si esegue una `ricerca nslookup` per i domini locali non di produzione dell'insieme di credenziali, le richieste DNS gestite dai server DNS configurati nel profilo VPN sono state risolte correttamente in indirizzi 10.x. Di conseguenza, la tabella di routing è stata aggiornata con l'indirizzo IP risolto (ad esempio, 10.59.130.193) in route non protette.
    - Scenario non funzionante - Tuttavia, quando le stesse richieste DNS sono state gestite dal DNS locale del sistema macOS (192.168.x.x) configurato sulle schede untun4 ed en0 anziché sui server DNS definiti nel profilo VPN, questo comportamento è stato chiaramente osservato dall'acquisizione dei pacchetti mentre il problema è stato rilevato.
    - I domini privati sono stati risolti nell'intervallo IP 34.x.x.x, che ha causato il problema di connettività. L'acquisizione di Wireshark ha consentito di identificare la root cause del problema.
- Dal punto di vista della progettazione e della configurazione, con l'impostazione di un profilo VPN con tunnel suddiviso, è consigliabile utilizzare il DNS suddiviso anziché il DNS del sistema locale o il DNS predefinito.
- Inoltre, è stata aggiunta la voce `us-east-eks-amazonaws.com` per garantire che il traffico di questo cluster EKS venga indirizzato correttamente attraverso l'interfaccia del tunnel remoto.
- È stato inoltre discusso che l'interfaccia RAVPN deve avere la precedenza sul modulo Umbrella e non deve essere in conflitto con il file `OrgInfo.json` contenente l'ID organizzazione Umbrella.
- Durante il nostro processo di risoluzione dei problemi, abbiamo fatto una nuova installazione del client CSC senza il modulo Umbrella, con quello scenario non siamo stati in grado di vedere il problema. Sono stato in grado di rivedere dal punto di vista Umbrella anche, il dominio radice naic.org configurato nell'elenco dei domini interni per ignorare Umbrella che significa che le risoluzioni del dominio locale è inoltrato a sistema configurato macOS DNS non intercettato dal modulo Umbrella DNS a livello di kernel interfaccia loopback.

Ciò è in linea con la risoluzione dei problemi quando non è presente alcun modulo Umbrella. Con la corretta configurazione del profilo VPN, inclusi i domini corretti nella regola di gestione del traffico e la configurazione DNS divisa, non dovremmo vedere il problema anche con il modello Umbrella attivato.

L'utente ha confermato che il problema è stato risolto dopo aver modificato la modalità DNS in Split tunnel e modificato la configurazione del profilo VPN.

## Causa

Profilo VPN - Ignora accesso sicuro - La modalità DNS dovrebbe essere impostata su Tunnel suddiviso (le opzioni più comuni degli scenari di utilizzo) e includere tutti i domini applicazione privati/interni nella configurazione DNS suddiviso per risolvere il problema.

## Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).