Risoluzione dei problemi di penalizzazione DNS in MacOS e di accesso con i domini interni

Sommario

Introduzione

Questo documento descrive come risolvere un problema con le versioni più recenti di MacOS Big Sur che influisce sulla risoluzione DNS.

Premesse

Ambito

- AnyConnect Roaming Security Module o Umbrella in rete (ad esempio, VA o inoltro)
  - Client roaming Umbrella standalone non interessato. L'ambiente DNS singolo è presente dove tutti i DNS vengono sovrascritti con 127.0.0.1).
- Si verifica in ambienti con più interfacce di rete, ma solo una può risolvere indirizzi interni. Ad esempio:
  - VPN e off-VPN
  - Più schede NIC: una aziendale e una non aziendale

Sintomi

- Impossibilità (o capacità intermittente) di accedere ai domini locali mantenendo la possibilità di accedere ai domini pubblici
  - nslookup non è influenzato in modo specifico e continua a funzionare
    - il comando ping, traceroute e così via risolve i problemi in modo errato o non trova il dominio interno

Problema

Questo problema è causato dal codice in MacOS che gestisce la modalità di gestione delle

risoluzioni DNS in presenza di più server DNS. Può trattarsi di più resolver su un singolo adattatore di rete o di più resolver su diversi adattatori di rete. Un server DNS che risponde con REFUSED viene "penalizzato" per 60 secondi. In questo caso, qualsiasi ulteriore query DNS eseguita in questo periodo di tempo verrà tentata su server DNS alternativi non penalizzati.

Ad esempio, se DHCP annuncia due server DNS per una rete, A e B, e A risponde con REFUSED, B viene preferito ad A per 60 secondi, a condizione che B non venga penalizzato.

Se tutti i server DNS vengono penalizzati, MacOS preferisce il server penalizzato meno di recente. Ad esempio, se B viene penalizzato mentre A è già penalizzato, MacOS preferisce A rispetto a B.

A questo si aggiunge il modo in cui MacOS 11 e versioni successive tentano di affermare il DoH (DNS su HTTPS). MacOS è programmato per preferire un provider DoH impostato dall'utente quando possibile. Ciò eluderebbe la sicurezza Umbrella DNS, il che significa che restituiremo una risposta RIFIUTATA (come da RFC) quando MacOS avvia una richiesta DoH. A causa della penalizzazione DNS, ciò può causare la risoluzione non corretta dei domini interni. Per ulteriori informazioni su questo problema, vedere questo articolo: Selezione del resolver DNS in iOS 14 e macOS 11.

Soluzione

Non siamo ancora a conoscenza del fatto che Apple intenda modificare questo comportamento o che Umbrella sia in grado di modificare il proprio comportamento per risolvere il problema. Per il momento, ci sono due opzioni che servono come alternative:

Opzione 1

Abilitare split-DNS nei Criteri di gruppo e aggiungere in modo specifico i domini interni alla configurazione split-DNS in modo che siano risolvibili solo tramite tunnel. In questo modo, tali domini possono essere risolti solo tramite tunnel dal resolver del sistema operativo nativo, mentre gli altri domini possono essere risolti solo all'esterno del tunnel.

Opzione 2

Abilitare tunnel-all-DNS nei Criteri di gruppo per impedire al traffico DNS di uscire dal tunnel.

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).