Conflitti di risoluzione DNS tra Cisco Secure Access e l'app Banyan Security

Sommario

Problema

Quando Cisco Secure Access viene implementato contemporaneamente all'app Banyan Security sugli endpoint Windows, gli utenti riscontrano significativi rallentamenti e timeout della risoluzione DNS. I sintomi specifici includono:

- La risoluzione DNS inizia a scadere quando l'app Banyan Security è connessa.
- Le pagine Web vengono caricate molto lentamente, anche se alla fine vengono risolte.
- L'app Banyan avvia un proxy DNS locale su un'interfaccia di loopback, simile al comportamento di Umbrella.
- Questa configurazione del proxy DNS interferisce con il normale comportamento di risoluzione DNS.

Il problema riguarda in particolare gli utenti che devono accedere ad ambienti esterni mentre Cisco Secure Access è implementato per la sicurezza della rete principale.

Ambiente

- Cisco Secure Access implementato con i componenti di accesso a Internet (modulo roaming, VA, DNS, SWG, PAC, IPS, certificati)
- Banyan Security App in esecuzione sugli endpoint Windows
- Utenti che richiedono l'accesso ad ambienti esterni tramite Banyan mantenendo la connettività Secure Access
- Servizi proxy DNS in esecuzione su interfacce di loopback da entrambe le applicazioni

- Bypass del dominio interno già configurato in Accesso sicuro per la risoluzione FQDN

Risoluzione

Per risolvere i conflitti di risoluzione DNS tra Cisco Secure Access e Banyan Security App, implementare i seguenti approcci:

Passi risoluzione principali

Questo è un ID bug Cisco CSCwr21575 noto che risolve i conflitti noti del proxy DNS tra Cisco Secure Access e le applicazioni di sicurezza di terze parti che implementano i proxy DNS locali.

Sintomo

La risoluzione DNS scade o è ritardata in modo significativo.

Condizioni

- Query DNS intercettata dal modulo Cisco Secure Client Umbrella.
- Il server DNS primario è configurato su un indirizzo IP compreso nell'intervallo di loopback 127.0.0.0/8 e le destinazioni delle query DNS di tale server.
- Sulla stessa scheda o su un'altra scheda è presente almeno un altro server DNS IPv4 senza loopback.

Soluzione alternativa

Impostare il server DNS primario su un indirizzo IP non di loopback. La soluzione definitiva è aggiornare Cisco Secure Client alla versione 5.1.13 e successive.

Verifica e collaudo

Dopo aver implementato le fasi di risoluzione, eseguire la seguente convalida:

- Verifica la velocità di risoluzione DNS con Cisco Secure Access e Banyan Security App attive
- Verificare che i tempi di caricamento delle pagine Web tornino a livelli accettabili
- Confermare che l'accesso agli ambienti esterni tramite Banyan continua a funzionare
- Verifica che la risoluzione del dominio interno tramite bypass Secure Access rimanga operativa

Causa

Il rallentamento della risoluzione DNS è causato da implementazioni di proxy DNS in conflitto tra Cisco Secure Access e l'app Banyan Security. Entrambe le applicazioni stabiliscono proxy DNS locali su interfacce di loopback, creando percorsi di risoluzione DNS concorrenti che determinano timeout e risposte ritardate.

Il comportamento proxy DNS dell'app Banyan Security interferisce con la gestione DNS di Cisco Secure Access, in particolare influendo sull'ordine e sulla priorità dell'elaborazione delle query DNS sugli endpoint Windows.

L'ID bug Cisco CSCwr21575 risolve questo problema specifico di compatibilità.

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).