

L'accesso a Internet non riesce quando è attivo il servizio Secure Client Umbrella SWG Agent

Sommario

Problema

Quando il servizio Cisco Secure Client - Umbrella SWG Agent è in esecuzione su un notebook Dell Windows, gli utenti non sono in grado di accedere ai siti Web. Una volta arrestato il servizio Umbrella SWG Agent, viene ripristinato il normale accesso al Web. Il problema si verifica con Cisco Secure Client versione 5.1.14.145, che include sia i moduli AnyConnect VPN che Umbrella. Il file OrgInfo.json è presente nella directory prevista e il certificato CA radice di accesso sicuro Cisco è installato nell'archivio certificati radice attendibili.

Ambiente

- Prodotto: Cisco Secure Client (moduli AnyConnect VPN e Umbrella)
- Versione del software: 5.1.14.145
- Sistema operativo: Windows (notebook Dell)
- Servizio agente SWG Umbrella abilitato/disabilitato
- OrgInfo.json presente in %ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
- CA radice di accesso sicuro Cisco installata nell'archivio Autorità di certificazione radice attendibili
- DNS/sicurezza Web abilitata nel dashboard di accesso sicuro
- Profilo di sicurezza assegnato con decrittografia abilitata

Risoluzione

Il problema è stato risolto identificando e correggendo un errore di sincronizzazione NTP (Network Time Protocol) sul dispositivo client. L'impossibilità di sincronizzare l'ora ha impedito la comunicazione protetta richiesta dall'agente SWG Umbrella per il trasferimento del traffico Web, con conseguenti pacchetti RST (TCP reset) e perdita dell'accesso Web. Una volta ripristinata la sincronizzazione NTP, l'accesso Web funzionava normalmente con l'agente SWG attivo.

Seguire questo flusso di lavoro completo per la risoluzione dei problemi.

Passaggio 1: Verificare la configurazione e i prerequisiti

- Verificare che OrgInfo.json si trovi in
%ProgramData%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json.
- Verificare che la CA radice di accesso sicuro Cisco sia presente nell'archivio Autorità di

certificazione radice attendibili.

- Verificare che DNS/Web Security sia abilitato nel dashboard Accesso sicuro.
- Verificare che nel profilo di sicurezza assegnato sia abilitata la decrittografia.

Fase 2: Acquisire e analizzare il traffico di rete

Acquisire un pacchetto del traffico client diretto al proxy SWG per identificare comportamenti anomali, ad esempio pacchetti di reset TCP imprevisti.

Descrizione dell'acquisizione del pacchetto che mostra il problema:

The packet capture revealed that TCP reset (RST) packets were being sent to the client, disrupting the

Passaggio 4: Convalidare le regole del firewall perimetrale

- Ispezionare le regole del firewall perimetrale per garantire che il traffico da e verso i server SWG sia consentito sull'interfaccia in entrata.

Passaggio 5: Eseguire Diagnostica di sistema e protocollo

Eseguire questo comando sul client per verificare la presenza di errori di sincronizzazione NTP:

```
curl ipinfo.io
```

Descrizione del risultato diagnostico:

The output indicated NTP timing was out of sync on the client device.

Causa

La causa principale è un errore nella sincronizzazione NTP (Network Time Protocol) sul dispositivo client. Questo problema di temporizzazione impediva la comunicazione sicura tra il client e il servizio proxy SWG Umbrella, provocando la reimpostazione dei pacchetti TCP e la perdita dell'accesso Web quando il servizio agente SWG era attivo. La risoluzione del problema di sincronizzazione NTP ha ripristinato il corretto funzionamento dell'agente SWG Umbrella, consentendo la trasmissione del traffico Web in modalità protetta.

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).