

Secure Access VPN - impossibile accedere a Jabber

Sommario

Problema

Gli utenti Secure Client non sono stati in grado di accedere ad applicazioni interne e private, quali Jabber ed Epic, tramite il tunnel VPN ad accesso sicuro quando si utilizzano criteri di accesso privato. Si sono verificati errori di connettività durante il tentativo di raggiungere queste applicazioni aziendali critiche tramite la connessione VPN. Durante la risoluzione dei problemi, è stato osservato il traffico unidirezionale per le risorse Epic in cui il traffico ping e TCP SYN è stato rilevato in uscita dal tunnel VPN di accesso sicuro, ma sono stati identificati problemi di convalida del traffico di ritorno sul firewall di Palo Alto. Inoltre, sono stati documentati i problemi di raggiungibilità di Jabber in cui gli FQDN CUCM venivano risolti tramite DNS interno mentre la direzione del traffico era configurata per il routing basato su IP, causando una mancata corrispondenza nel flusso del traffico.

Ambiente

- Cisco Secure Access con configurazione tunnel VPN
- Secure Client per connettività VPN
- Implementazione criteri di accesso privato
- Cisco Unified Communications Manager (CUCM) per servizi Jabber
- Risorse per applicazioni Epic
- Firewall di Palo Alto per la sicurezza della rete
- Risoluzione DNS interna per FQDN CUCM

Risoluzione

La risoluzione ha richiesto più modifiche alla configurazione e passaggi per la risoluzione dei problemi al fine di ripristinare la connettività alle applicazioni interne tramite il tunnel VPN ad

accesso sicuro:

Configurazione della subnet e modifiche del tunnel

Passaggio 1: Aggiungi altre subnet al tunnel VPN

Sono state aggiunte subnet aggiuntive alla configurazione del tunnel VPN per le risorse interessate. Dopo l'implementazione di questa modifica, il caricamento delle risorse precedentemente inaccessibili è stato completato.

Configurazione controllo indirizzo IP CUCM

Passaggio 2: Configurazione di CUCM IP Steering

Per risolvere il problema di connettività Jabber in cui gli FQDN di CUCM venivano risolti tramite DNS interno mentre la direzione del traffico era basata su IP, gli indirizzi IP di CUCM venivano indirizzati in Secure Client. Questa modifica alla configurazione ha allineato la risoluzione DNS con il meccanismo di gestione del traffico.

Passaggio 3: Crea regola dei criteri di accesso

È stata creata una regola dei criteri di accesso per consentire la raggiungibilità degli indirizzi IP CUCM. Questa regola ripristina la corretta connettività all'infrastruttura CUCM, abilitando la funzionalità Jabber sul tunnel VPN.

Configurazione del routing statico

Passaggio 4: Configura routing statico per subnet CUCM

Verificare che gli indirizzi IP CUCM e la subnet CUCM complessiva siano inclusi nella tabella di routing statica per il tunnel di rete. Questa configurazione garantisce il corretto routing del traffico tra il pool di utenti Secure Client e l'infrastruttura CUCM.

Convalida traffico di ritorno

Passaggio 5: Convalida flusso di pacchetti e traffico di ritorno

Convalidare la configurazione del flusso di pacchetto per verificare che il traffico di ritorno possa raggiungere il pool di utenti Secure Client. Ciò include la revisione della configurazione del firewall di Palo Alto per garantire la corretta convalida del percorso di ritorno per tutte le risorse interne, in particolare per la connettività Epic in cui è stato osservato il traffico unidirezionale.

Causa

I problemi di connettività sono stati causati da più gap di configurazione nell'implementazione della VPN ad accesso sicuro:

- La mancanza di configurazioni di subnet nel tunnel VPN ha impedito il corretto routing alle risorse interne dell'applicazione
- La mancata corrispondenza tra la risoluzione DNS (basata su FQDN) e la configurazione della direzione del traffico (basata su IP) per i servizi CUCM ha causato errori di connettività Jabber
- Regole dei criteri di accesso incomplete che non consentivano il traffico verso gli indirizzi IP CUCM
- Voci di routing statico mancanti per le subnet CUCM nella configurazione del tunnel di rete
- Restituire problemi di convalida del percorso del traffico sul firewall di Palo Alto che influiscono sulla comunicazione bidirezionale

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).