

Indirizzi di destinazione di accesso sicuro per la configurazione del routing suddiviso

Sommario

Problema

Quando si distribuisce Cisco Secure Access (CSA) con Cisco Secure Client (CSC) sugli endpoint Windows in un'architettura di rete Hub-Spoke, è molto probabile che le organizzazioni abbiano bisogno di configurare il routing suddiviso per consentire al traffico del sito Spoke di connettersi direttamente a CSA sul circuito Internet Spoke locale anziché hairpinning attraverso l'Hub. Questa configurazione richiede la conoscenza di tutti gli indirizzi di destinazione Cisco utilizzati quando si stabilisce il tunnel CSA, in modo che le eccezioni di routing (breakout/split routing) possano essere definite sui dispositivi di rete come i firewall Fortigate.

Il requisito specifico è identificare tutte le informazioni di destinazione (indirizzi IP o URL) per gli endpoint CSA utilizzati da CSC quando si stabiliscono i tunnel TLS/DTLS, consentendo la corretta configurazione delle policy di routing che ignorano il tunnel VPN con hub per il traffico CSA.

Ambiente

- Implementazione di Cisco Secure Access (CSA)
- Cisco Secure Client (CSC) sugli endpoint Windows
- Topologia di rete Hub-Spoke con firewall Fortigate
- Connettività tunnel TLS/DTLS a CSA

Risoluzione

Per configurare il routing di split per le connessioni Cisco Secure Access, le informazioni di

destinazione descritte nelle sezioni seguenti devono essere configurate sul dispositivo Fortigate per consentire la connettività diretta agli endpoint CSA.

Dominio e porte di destinazione CSA

Dominio primario

`*.vpn.sse.cisco.com`

Porte e protocolli richiesti

- TCP/UDP 443: Utilizzato per la definizione del tunnel TLS/DTLS
- UDP 500/4500: Utilizzato per la definizione del tunnel IPsec
- TCP 80: Utilizzato per i controlli di revoca dei certificati VPN

Fortigate Configuration Approach

Configurare i criteri di routing sul dispositivo Fortigate per indirizzare il traffico destinato al dominio CSA (*.vpn.sse.cisco.com) e le porte specificate tramite il circuito Internet Spoke locale anziché tramite il tunnel VPN Hub-Spoke. In questo modo viene attivato il flusso del traffico descritto nei successivi frammenti di codice.

Flusso di traffico desiderato

`Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication`

Al posto del flusso di traffico attraverso il sito hub

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Considerazioni importanti

Le destinazioni della connessione CSA vengono determinate in modo dinamico durante il runtime, pertanto non è possibile predeterminare indirizzi IP specifici per la configurazione del routing statico. L'approccio basato su dominio basato su *.vpn.sse.cisco.com fornisce il metodo più affidabile per la configurazione delle policy di routing suddiviso.

Fare riferimento alla documentazione ufficiale di Cisco Secure Access per i requisiti di porta e destinazione più recenti, in quanto questi sono probabilmente aggiornati con le nuove versioni del software.

Causa

Nelle topologie di rete Hub-Spoke, per impostazione predefinita tutto il traffico in Internet proveniente da siti Spoke passa attraverso il sito Hub. Quando si implementa CSA con CSC, il comportamento predefinito del routing determina il hairpin del traffico del tunnel CSA attraverso il sito hub prima di raggiungere gli endpoint CSA, introducendo potenzialmente inefficienze a livello di latenza e larghezza di banda. La natura dinamica della selezione degli endpoint CSA richiede policy di routing basate su dominio anziché regole statiche basate su IP per garantire la corretta funzionalità di routing in modalità split.

Contenuto correlato

- [Documentazione su Cisco Secure Access - Requisiti di connessione](#)
- [Documentazione di Cisco Secure Access - Configurazione di rete](#)
- [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).