

Limitazione geografica di accesso per connessioni VPN e accesso con trust pari a zero

Sommario

Problema

Le organizzazioni che richiedono restrizioni di accesso geografiche per le connessioni ZTA (Zero Trust Access) e VPN possono trovare che i criteri ZTA e VPN esistenti devono essere disabilitati quando tentano di implementare controlli di accesso basati sul paese. Quando i criteri sono disabilitati a causa dell'impossibilità di individuare le opzioni di restrizione geografica native all'interno dell'interfaccia del prodotto Secure SSE, gli utenti non possono più accedere alle risorse necessarie. Il requisito specifico di limitare l'accesso alle connessioni che hanno origine solo all'interno di un determinato paese non può essere configurato utilizzando funzionalità di prodotto incorporate, con un conseguente impatto diffuso sugli utenti quando le policy esistenti vengono disattivate nel tentativo di implementare tali restrizioni.

Ambiente

- Prodotto Cisco Secure Access Service Edge (SASE) / Secure SSE
- Implementazione ZTNA (Zero Trust Access)
- Servizi VPN che richiedono il controllo dell'accesso geografico
- Criteri di accesso alle risorse private
- Organizzazione che richiede restrizioni di accesso specifiche per paese

Risoluzione

Il prodotto Cisco Secure SSE non fornisce attualmente funzionalità native per limitare l'accesso alle risorse private in base alla posizione geografica o al paese dell'utente. Si può ritenere che gli

approcci descritti nelle sezioni successive consentano di risolvere questo problema.

Invio richiesta funzionalità

È necessario inviare una richiesta a Cisco per aggiungere funzionalità di restrizione geografica per l'accesso ZTA e VPN. Questa richiesta di miglioramento viene valutata dal team del prodotto per un'eventuale inclusione nelle versioni future. Le organizzazioni possono collaborare con il proprio Cisco Account Manager per assegnare le priorità a tali richieste di funzionalità in base ai requisiti aziendali.

Considerazioni sulla soluzione manuale

Una possibile soluzione manuale implica l'aggiunta di intervalli di indirizzi IP pubblici specifici del paese come gruppi di oggetti di rete nei criteri di accesso.

Passaggio 1: Ottenere gli intervalli di indirizzi IP pubblici del paese dal Registro Internet regionale (RIR) appropriato.

Passaggio 2: Creare gruppi di oggetti di rete contenenti gli intervalli IP identificati. Configurare i gruppi di oggetti di rete nella configurazione dei criteri di accesso in modo da includere gli intervalli di indirizzi IP specifici allocati al paese di destinazione.

Passaggio 3: Applicare i gruppi di oggetti di rete ai criteri di accesso. Modificare i criteri di accesso esistenti per fare riferimento ai gruppi di oggetti di rete creati, limitando in modo efficace l'accesso alle connessioni originate dagli intervalli IP specificati.

Limitazioni importanti

Questo approccio manuale presenta limitazioni significative in quanto si basa su definizioni di intervalli IP statici e non può tenere conto di allocazioni IP dinamiche, utenti mobili o servizi VPN che potrebbero ignorare le restrizioni geografiche. Inoltre, questo metodo richiede una manutenzione continua per garantire l'accuratezza del range IP.

Gestione temporanea dei criteri

Finché non sarà disponibile una soluzione permanente, le organizzazioni devono evitare di disabilitare contemporaneamente tutte le policy ZTA e VPN. È preferibile implementare un approccio a fasi in cui le policy di accesso critiche rimangono attive mentre i requisiti di restrizione geografica vengono affrontati attraverso mezzi alternativi o in attesa di miglioramenti del prodotto.

Causa

L'architettura del prodotto Cisco Secure SSE non include funzionalità native di controllo dell'accesso geografico per l'accesso alle risorse private. La struttura dei criteri di accesso ai prodotti è progettata in base all'identità dell'utente, alla postura del dispositivo e ai controlli basati sulla rete, ma non include la posizione geografica come parametro di applicazione dei criteri. Ciò rappresenta una lacuna nella capacità del prodotto piuttosto che un problema di configurazione o un difetto del software.

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).