Configurazione di SWG per evitare conflitti con il traffico VPN SSL

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di incompatibilità tra Secure Web Gateway (SWG) e VPN SSL utilizzando le porte intercettate.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Umbrella SWG per AnyConnect può incontrare problemi di incompatibilità con alcune VPN SSL che usano le porte intercettate dall'agente SWG, come TCP 443. AnyConnect SWG può non essere attivato e applicare la copertura in modo affidabile. L'affidabilità della rete può peggiorare o diventare non disponibile quando SWG è attivo e il traffico VPN passa attraverso SWG. In questo scenario il traffico non Web viene interrotto. Questo problema interessa tutte le VPN SSL che utilizzano le porte 80 e 443.

Soluzione

Per impedire a SWG di intercettare il traffico VPN, configurare un bypass per i domini VPN e gli indirizzi IP:

1. Nel dashboard Umbrella, passare a Distribuzioni di accesso > Gestione domini > Domini esterni.

2. Aggiungere il dominio e l'indirizzo IP dei server headend VPN all'elenco dei domini esterni. La voce IP garantisce che il traffico VPN non venga mai intercettato dall'agente SWG a causa del numero elevato di connessioni.

3. Attendere un'ora prima che la nuova impostazione venga propagata.

Per utilizzare SSL VPN con SWG:

1. Aggiungere il dominio VPN all'elenco dei domini esterni.

2. Se il dominio headend VPN è un suffisso di ricerca DNS, il client aggiunge automaticamente questo dominio per la durata della connessione.

3. Aggiungere gli indirizzi IP o l'intervallo di indirizzi IP dell'headend VPN all'elenco dei domini esterni.

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).