Informazioni sulle impostazioni di backoff DNS e SWG per CSC

Sommario

Introduzione

In questo documento vengono descritte le impostazioni di backoff di DNS e Secure Web Gateway (SWG) per Cisco Secure Client (CSC).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Secure Client.

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.

Panoramica

Fino a circa il 25 aprile 2024, il comportamento di backoff del modulo SWG di Cisco Secure Client non poteva essere controllato indipendentemente dallo stato del modulo DNS e dipendeva dalle impostazioni di backoff DNS per abilitare/disabilitare la protezione SWG. Per risolvere questo problema, Umbrella ha disaccoppiato il comportamento per il modulo DNS e il modulo SWG, abilitando la gestione indipendente secondo necessità. Questa funzionalità è disponibile per i Cisco Secure Client nella versione 5.1.3.62 e successive, dove Umbrella ha disaccoppiato le

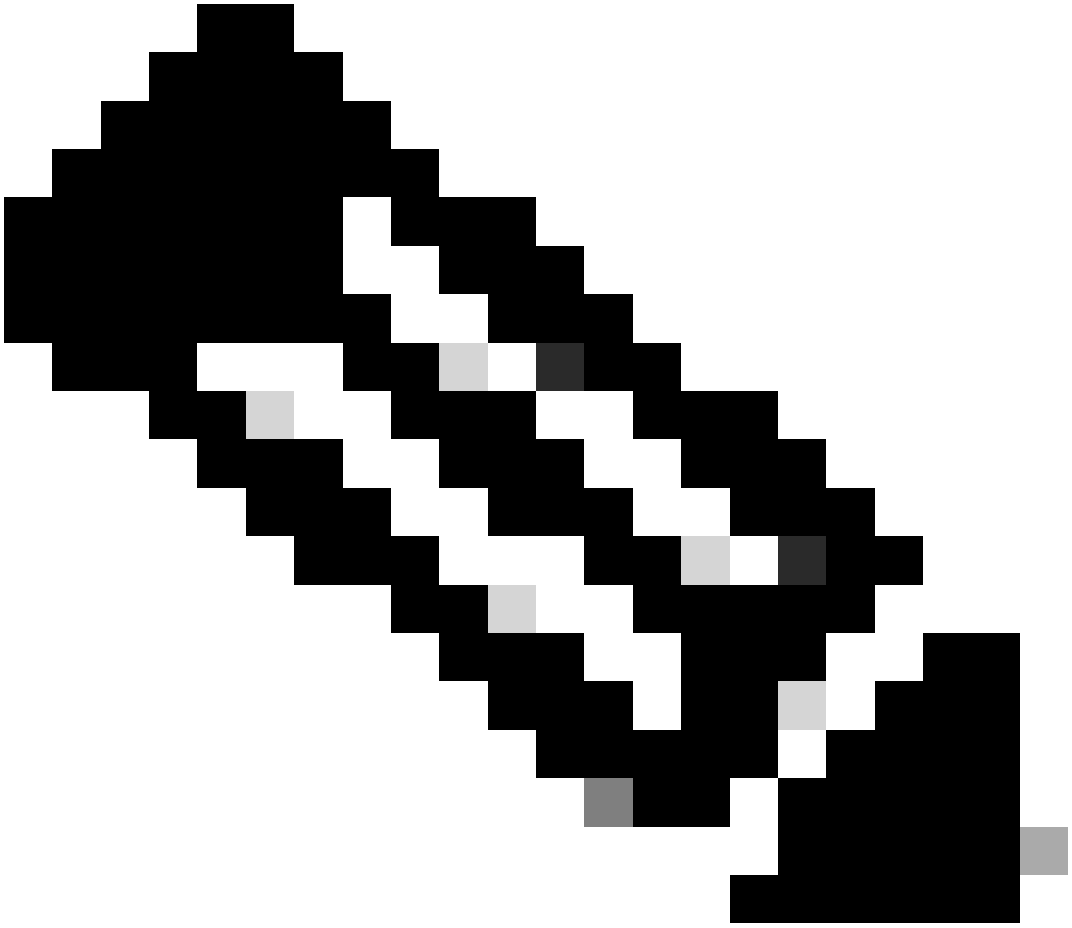
impostazioni di backoff DNS e SWG per consentire un controllo granulare avanzato. I client delle versioni precedenti non hanno seguito il backoff separato del modulo SWG.

Quando la funzionalità di backoff di Secure Web Gateway segue DNS è abilitata, il modulo SWG di CSC segue il comportamento del modulo DNS. Tuttavia, ciò non si verifica con tutte le impostazioni di backoff DNS. Nella sezione successiva vengono descritte in dettaglio le impostazioni di backoff DNS che il modulo SWG esegue o non esegue.

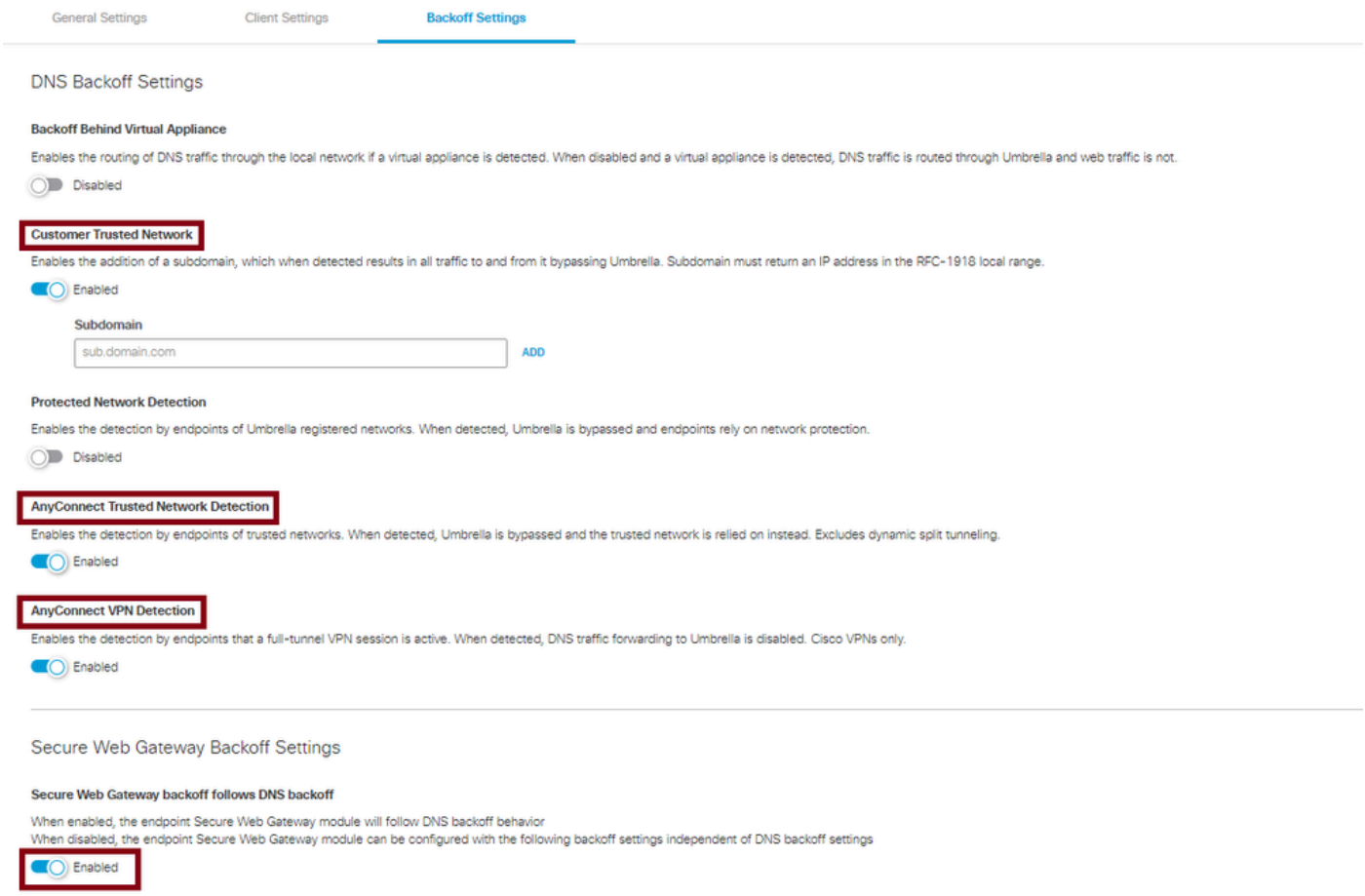
Quali impostazioni di backoff DNS causano il backoff di SWG?

Queste impostazioni di backoff DNS causano il backoff di SWG:

- Rete attendibile cliente: Impostare un dominio Customer Trusted Network nelle impostazioni di backoff DNS è uno dei metodi più semplici. L'hosting di un dominio interno che viene risolto in un indirizzo RFC1918 consente di eseguire contemporaneamente il backoff di DNS e SWG. Il client di Umbrella è codificato per eseguire query su quel dominio. Se il dominio viene risolto in un indirizzo IP privato, il dispositivo viene identificato come connesso a una rete privata e protetta e il modulo DNS viene interrotto. Questo meccanismo di backoff è rispettato anche dal modulo Web, che può analogamente eseguire il backoff quando il modulo DNS risolve correttamente il dominio.
- Rilevamento reti attendibili AnyConnect
- Rilevamento VPN AnyConnect



Nota: Le impostazioni di backoff DNS rimangono funzionali sui client sicuri Cisco che eseguono versioni precedenti alla 5.1.3.62, in quanto sono state implementate prima del disaccoppiamento delle impostazioni di backoff DNS e SWG.

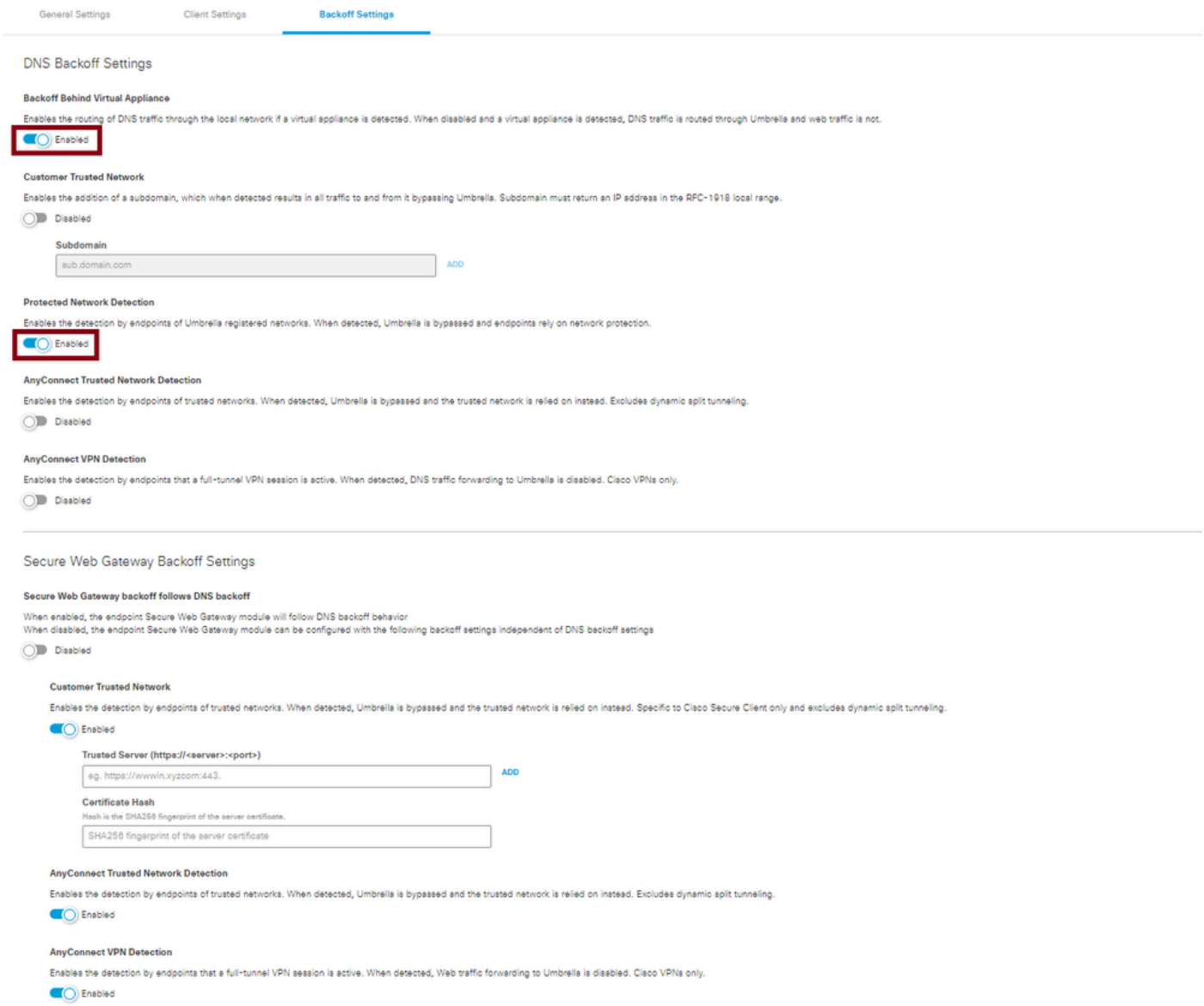


27885424859028

Quali impostazioni di backoff DNS non causano il backoff di SWG?

La configurazione di queste due funzioni di backoff DNS non provoca il backoff di SWG. Pertanto, è necessario configurare le impostazioni di backoff SWG in modo selettivo, indipendentemente dallo stato di configurazione DNS. Questo argomento viene illustrato in dettaglio nella sezione successiva.

- Backoff dietro Virtual Appliance: A partire da AnyConnect 4.10.07061 (MR7) e Secure Client 5.0.02075 (MR2), il modulo SWG può rimanere abilitato sulle reti in cui è presente un'appliance virtuale Umbrella. Se in precedenza ci si affidava alla presenza di un dispositivo virtuale per disabilitare il modulo SWG e il reindirizzamento Web su una determinata rete, è possibile usare Dominio di rete trusted o Rilevamento di reti attendibili AnyConnect.
- Protected Network Detection



27885587178772

Impostazioni di backoff SWG indipendente

Se queste funzioni di backoff DNS non sono abilitate nel proprio ambiente, è possibile utilizzare esclusivamente una delle impostazioni di backoff SWG qui descritte per garantire che SWG rimanga disabilitato:

- Rete attendibile cliente
- Rilevamento reti attendibili AnyConnect
- Rilevamento VPN AnyConnect

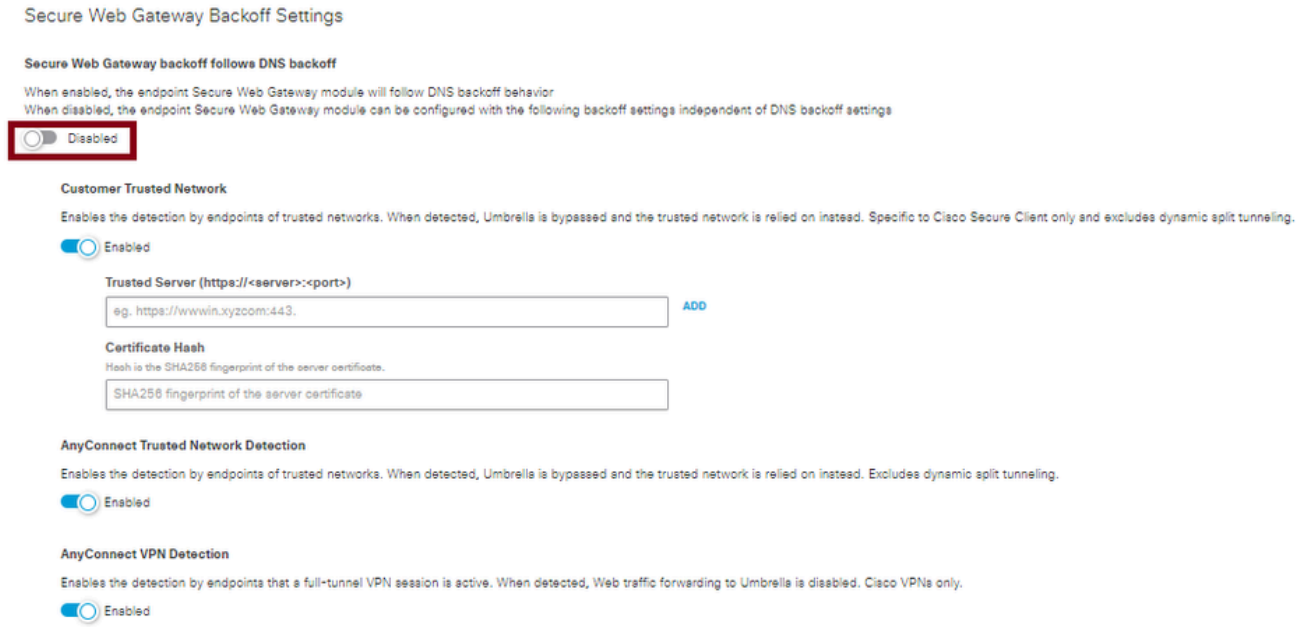
Questa nuova funzionalità consente al modulo SWG di funzionare indipendentemente dal modulo DNS. Questa funzionalità è disponibile per i Cisco Secure Client con versione 5.1.3.62 e successive. Configurate uno degli interruttori espliciti di backoff SWG nel quadro comandi:

- Rete attendibile cliente: Un'opzione consiste nell'utilizzare l'opzione Customer Trusted Network (Rete attendibile cliente) nelle impostazioni di backoff SWG, in cui è possibile

configurare un server interno a cui il client possa accedere per confermare che si trovi sulla rete protetta. È necessario verificare che il server Web sia raggiungibile dal client, ottenere un certificato su tale server e copiare l'hash del certificato nel dashboard Umbrella.

Le altre due opzioni si applicano esclusivamente alle connessioni VPN:

- Rilevamento reti attendibili AnyConnect
- Rilevamento VPN AnyConnect



27886005743764

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).