Configurazione di SSE Do Not Decrypt per IPS e SWG Decryption Bypass

Sommario

Problema

Il traffico HTTPS verso destinazioni di categoria finanziaria continua a presentare un certificato SSE Cisco anziché il certificato del sito Web di origine, anche dopo l'aggiunta della categoria finanziaria o di domini specifici a un elenco Do Not Decrypt (DND) e l'applicazione della regola di accesso pertinente. Questo comportamento viene osservato quando si accede a siti tramite Zero Trust Access Client (TIA), con un impatto specifico sull'accesso a siti Web correlati al settore finanziario, ad esempio https://onlinesbi.sbi.bank.in/, dove è richiesta la visibilità completa dei certificati.

Quando si aggiunge un sito o una categoria di contenuti all'elenco DND, è possibile presentare il certificato del sito Web di origine al browser anziché il certificato SSE di Cisco. Tuttavia, il certificato SSE di Cisco continua a essere presentato, indicando che la decrittografia del traffico viene ancora eseguita nonostante la configurazione DND.

Ambiente

- SSE (Cisco Secure Service Edge)
- Connettività Zero Trust Access Client (TIA)
- Decrittografia IPS globale abilitata
- IPS attivo sui criteri di accesso
- Categoria finanziaria configurata nell'elenco Non decrittografare nel profilo di sicurezza
- Regole di accesso applicate con i profili di sicurezza corrispondenti

Risoluzione

La risoluzione implica la comprensione che Cisco SSE esegue due tipi distinti di decrittografia e la configurazione delle impostazioni appropriate dell'opzione Non decrittografare per entrambi i tipi di decrittografia.

Informazioni sui tipi di decrittografia SSE

Cisco SSE esegue due processi di decrittografia distinti:

- Decrittografia SWG (Secure Web Gateway) - Decrittografia proxy Web
- Decrittografia IPS - Decrittografia del sistema di prevenzione delle intrusioni

Le voci Do Not Decrypt configurate all'interno di un profilo di sicurezza si applicano solo alla decrittografia SWG e non impediscono la decrittografia IPS. Quando la decrittografia IPS globale è abilitata e IPS è attivo su qualsiasi criterio di accesso, la decrittografia IPS viene comunque eseguita, in modo che il certificato SSE Cisco venga presentato al browser.

Procedura di configurazione

Passaggio 1: Aggiungere siti o categorie di contenuto all'elenco Da non decrittografare fornito dal sistema.

L'elenco Non decrittografare fornito dal sistema viene applicato a tutti i profili IPS. L'aggiunta di un sito o di una categoria di contenuti all'elenco Fornito dal sistema comporta la presentazione del certificato del sito Web di origine, evitando in tal modo la decrittografia IPS.

Passaggio 2: Verificare che non siano necessarie ulteriori modifiche ai criteri.

Non è necessario fare riferimento all'elenco Do Not Decrypt fornito dal sistema nei criteri di accesso. L'elenco viene applicato automaticamente a tutti i profili IPS.

Test di convalida

Per verificare la corretta configurazione, è possibile utilizzare i seguenti metodi di convalida:

Metodo 1: Aggiungi dominio all'elenco Non decrittografare fornito dal sistema

L'aggiunta del dominio specifico all'elenco degli elementi da non decrittografare forniti dal sistema può determinare la presentazione del certificato del sito Web di origine anziché del certificato SSE di Cisco.

Metodo 2: Disabilita temporaneamente la decrittografia IPS globale (solo per il test)

La disattivazione temporanea della decrittografia IPS globale determina inoltre la visualizzazione del certificato di origine per il sito testato, a conferma che la decrittografia IPS è stata la causa della presentazione del certificato SSE di Cisco.

Risultati previsti

Dopo aver eseguito la configurazione corretta:

- I siti o le categorie di contenuti aggiunti all'elenco Non decrittografare fornito dal sistema presentano i certificati dei siti Web di origine.
- La decrittografia SWG e IPS viene ignorata per i siti o le categorie specificati.
- Il browser visualizza il certificato del sito Web effettivo anziché il certificato SSE di Cisco.

Causa

Il problema si verifica perché Cisco SSE esegue due processi di decrittografia distinti: decrittografia SWG e decrittografia IPS. Non decrittografare le voci configurate nei profili di sicurezza ignora solo la decrittografia SWG. Quando la decrittografia IPS globale è abilitata e IPS è attivo sui criteri di accesso, la decrittografia IPS continua a essere eseguita in modo indipendente, causando la presentazione del certificato SSE Cisco al browser anche quando i siti sono inclusi negli elenchi DND dei profili di sicurezza.

Per ignorare completamente entrambi i tipi di decrittografia, i siti o le categorie di contenuto devono essere aggiunti all'elenco Non decrittografare fornito dal sistema, che si applica a tutti i profili IPS e impedisce la decrittografia SWG e IPS.

Contenuto correlato

- Crea elenco indirizzi non decrittografati valido per accesso protetto
- Risoluzione dei problemi e raccolta delle informazioni di base per un accesso sicuro
- 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).