Risoluzione dei problemi relativi alla mancata applicazione dell'identità SAML per il traffico Secure Web Gateway

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle identità SAML che non vengono applicate al traffico di Gateway Web della sezione.

Identità SAML non applicata per QUALSIASI traffico Web

Se l'identità SAML non viene applicata per QUALSIASI traffico Web, consultare la documentazione Umbrella per verificare che l'impostazione sia stata completata correttamente. Questi elementi di configurazione devono essere completati.

- Impostazioni IdP configurate e testate in 'Distribuzioni > Configurazione SAML'
- Elenco di utenti/gruppi di cui è stato eseguito il provisioning in 'Distribuzioni > Utenti e gruppi Web'
- SAML deve essere abilitato nel criterio pertinente* in 'Criteri > Criteri Web'.
- La decrittografia HTTPS deve essere abilitata nel criterio pertinente in 'Criteri > Criteri Web'

Abilitazione di SAML nei criteri Web

La decrittografia SAML e HTTPS deve essere abilitata nei criteri applicabili all'identità di rete o tunnel interessata. Queste funzionalità vengono applicate prima dell'identificazione di un utente, pertanto il criterio importante è quello applicato al "metodo di connessione".

I criteri SAML devono essere ordinati come segue:

1. Priorità PIÙ ALTA: la policy si applica a utenti/gruppi. Questo criterio determina le impostazioni di protezione/contenuto per gli utenti autenticati.

2. Priorità PIÙ BASSA - Il criterio si applica alla rete/al tunnel. Questo criterio ha SAML abilitato e attiva l'autenticazione iniziale.

Identità SAML non applicata per il traffico Web specifico

Surrogati IP (comportamento predefinito)

Per migliorare l'uniformità dell'identificazione degli utenti, si consiglia di abilitare la nuova funzione dei surrogati IP. Questa funzione è attivata automaticamente per tutti i nuovi clienti Umbrella SAML ma deve essere attivata manualmente per i clienti Umbrella esistenti.

I surrogati IP utilizzano una cache di informazioni IP interno > Nome utente che consente di applicare l'identificazione SAML a tutti i tipi di richieste: anche il traffico non proveniente dal browser Web, il traffico che non supporta i cookie e il traffico non soggetto alla decrittografia SSL.

I surrogati IP possono migliorare notevolmente la coerenza dell'identificazione degli utenti e ridurre il carico amministrativo.

I surrogati IP hanno i seguenti requisiti:

- La visibilità IP interna deve essere fornita utilizzando un'installazione Umbrella Network Tunnel o Proxy-Chain e le intestazioni X-Forwarded-For. Non funziona con il file PAC ospitato da Umbrella
- I surrogati IP non possono essere utilizzati in scenari di indirizzi IP condivisi (Terminal Server, Cambio rapido utente)
- I cookie devono essere attivati nel browser. I cookie sono ancora necessari per la fase di autenticazione iniziale.

Surrogati cookie (surrogati IP disabilitati)

Se i surrogati IP sono disattivati, l'identità dell'utente viene applicata solo alle richieste provenienti dai browser Web supportati e il browser WEB DEVE supportare i cookie. SWG richiede che il browser supporti i cookie per ogni richiesta al fine di tenere traccia della sessione degli utenti in un cookie. Purtroppo ciò significa che non è previsto che ogni richiesta Web venga associata a un utente in questa modalità.

SAML non viene applicato in queste circostanze e viene utilizzato il criterio predefinito assegnato all'identità Rete/Tunnel:

- Traffico non basato su browser
- Browser Web con cookie disabilitati o Protezione avanzata di Internet Explorer
- Controlli OCSP/Revoca certificato che non supportano i cookie
- Richieste Web individuali che non supportano i cookie. In alcuni casi i cookie vengono bloccati per richieste individuali a causa dei criteri di protezione del contenuto del sito Web. Questa restrizione si applica a molte reti di distribuzione dei contenuti più diffuse.
- Quando il dominio o la categoria di destinazione è stata ignorata da SAML utilizzando un elenco di esclusione SAML

- Quando il dominio/categoria di destinazione è stato ignorato dalla decrittografia HTTPS utilizzando un elenco di decrittografia selettiva Umbrella.

A causa di queste restrizioni, è importante configurare un livello minimo di accesso appropriato nella policy di rete/tunnel pertinente. I criteri predefiniti devono consentire l'utilizzo di applicazioni, domini e categorie business critical e di reti di distribuzione dei contenuti.

In alternativa, utilizzare il sistema IP Surrogates per migliorare la compatibilità.

Bypass SAML

In rari casi sono necessarie eccezioni. Questo è necessario quando SWG sottopone una richiesta di autenticazione SAML ma l'app o il sito Web non lo supporta. Ciò si verifica quando:

- Un'app non basata su browser utilizza un agente utente simile a un browser Web
- Uno script non è in grado di gestire i reindirizzamenti HTTP eseguiti dai nostri test sui cookie
- La prima richiesta in una sessione di esplorazione è una richiesta POST (es. URL Single Sign-On) che non può essere reindirizzato correttamente per SAML

L'elenco di esclusione SAML è il modo migliore per escludere un dominio dall'autenticazione pur mantenendo la protezione (ispezione dei file).

- L'eccezione SAML Bypass List deve essere applicata al criterio corretto che interessa la rete o il tunnel utilizzato per la connessione
- L'elenco di esclusione SAML non consente automaticamente il traffico. Il dominio o i domini devono essere ancora consentiti dagli elenchi di categoria o di destinazione nel criterio pertinente.

Bypass SAML - Considerazioni

Quando si aggiungono esclusioni per siti popolari e "home page" è importante considerare l'impatto su SAML. SAML offre risultati ottimali quando la prima richiesta in una sessione di esplorazione è una richiesta GET a una pagina HTML. Esempio: http://www.myhomepage.tld. Questa richiesta viene reindirizzata per l'autenticazione SAML e le richieste successive assumono la stessa identità utilizzando i surrogati IP o i cookie.

L'esclusione delle pagine iniziali da SAML può causare un problema quando la prima richiesta rilevata dal sistema SAML riguarda il contenuto in background. Ad esempio, http://homepage-content.tld/script.js. Questo è un problema perché il reindirizzamento SAML a una pagina di accesso SAML non è possibile quando il browser carica il contenuto incorporato (come i file JS). Ciò significa che la pagina sembra essere visualizzata o funzionare in modo non corretto finché l'utente non accede a un sito diverso per attivare l'accesso.

Se si considerano i siti e le pagine iniziali più popolari, prendere in considerazione le seguenti opzioni:

- Non escludere home page e siti popolari dalla decrittografia SAML o HTTPS se non necessario

- Se si esclude una home page, tutti i domini utilizzati da tale sito (incluso il contenuto di sfondo) devono essere esclusi per evitare incompatibilità SAML

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).