Sfide relative all'identificazione per utente e all'applicazione delle policy in Secure Web Gateway (SWG) per ambienti di computer condivisi con autenticazione SAML e inoltro del traffico basato sulla PAC

Sommario

Problema

Nelle distribuzioni Cisco Secure Web Gateway (SWG) che utilizzano l'accesso sicuro con autenticazione SAML e l'inoltro del traffico basato su PAC o Branch to Internet, solo il primo utente ha eseguito l'accesso a un computer condiviso viene identificato correttamente per il traffico Web e l'applicazione dei criteri. Dopo il passaggio a un altro utente, il traffico Web successivo continua a essere attribuito all'utente iniziale, anche quando l'opzione Sostitutivo IP è disabilitata e viene utilizzato un file PAC. Le query DNS riflettono l'utente attivo corretto tramite Umbrella Virtual Appliance, ma i registri Web e firewall mappano in modo permanente l'attività all'utente precedente. La richiesta consente di determinare se SWG supporta l'identificazione e l'applicazione dei criteri negli ambienti di computer condivisi.

Ambiente

- Appliance virtuale per la risoluzione DNS.
- Autenticazione SAML per l'identità utente.
- Combinazione di inoltro del traffico con PAC e senza file PAC.
- Opzione IP surrogate abilitata, con subnet e host specifici ignorati per il surrogato del cookie.
- Dispositivi locali; nessun endpoint o utente remoto.

Risoluzione

Il problema è stato risolto grazie alla formazione degli utenti e alle linee guida per la configurazione, tenendo presenti i seguenti punti:

- Usa identificazione surrogato cookie con file PAC. Il traffico può essere indirizzato verso o da un tunnel di rete.
- Usare l'identificazione del surrogato del cookie senza i file PAC, ma il traffico deve passare attraverso un tunnel di rete.
- Per i criteri di accesso che si desidera applicare al surrogato del cookie è necessario che nel

profilo di sicurezza sia abilitata l'autenticazione SAML.
- Il traffico sostitutivo dei cookie è solo per il traffico basato sul browser. È necessaria una regola separata per identificare il traffico diverso dai cookie proveniente dal computer (ad esempio, traffico dei team o Webex) con l'identità di origine come rete.
- Il modulo SWG non deve essere in uso per consentire il funzionamento del surrogato del cookie.
- Quando è abilitato anche il surrogato IP, è necessario aggiungere gli indirizzi/le subnet IP private che intendono utilizzare il surrogato del cookie nell'elenco di esclusione (Utenti e gruppi - Gestione configurazione - Impostazioni avanzate).
- Anche l'elenco di esclusione per il surrogato dei cookie corrisponde a prefissi più brevi. Ad esempio, se si aggiunge 10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- Il surrogato del cookie supporta il passaggio dell'utente da un computer senza la necessità di disconnettersi per mantenere più identità.

Gran parte della risoluzione dei problemi è stata costituita da test delle policy e da ricerche di attività.

Causa

La causa principale di un'errata identificazione dell'utente in ambienti con computer condivisi è principalmente dovuta all'istruzione dell'utente.

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).