Configurazione delle porte proxy per il traffico delle porte non standard su WSA 1000V

Sommario

Problema

Un proxy WSA 1000V ospitato su VMware stava elaborando correttamente il traffico client sulle porte 80 e 443, ma non stava elaborando il traffico sulle porte non standard come la porta 8890. Quando l'accesso a una destinazione tramite una porta non standard è stato inizialmente bloccato dai criteri, il server di sicurezza di Windows ha registrato correttamente la richiesta bloccata. Tuttavia, dopo aver aggiunto l'indirizzo IP e l'URL a un criterio di autorizzazione, il traffico non è riuscito e non sono stati generati log corrispondenti sul proxy. Questo comportamento indicava che il traffico non stava raggiungendo o non era in corso di elaborazione da parte del server di servizi di distribuzione Windows dopo la creazione del criterio di autorizzazione, con un impatto sull'accesso client alle applicazioni che utilizzano porte non standard.

Ambiente

- Proxy Cisco WSA 1000V ospitato su VMware
- Software versione 15.0.0
- Il traffico sulle porte 80 e 443 viene elaborato normalmente.
- Traffico su porta non standard (ad esempio, la porta 8890) non elaborato dal proxy.
- Consenti criteri configurati per le destinazioni interessate.

Risoluzione

Il problema è stato risolto configurando WSA in modo da supportare porte non standard nelle impostazioni del profilo di identificazione. La configurazione delle porte proxy deve essere

aggiornata per includere i numeri di porta non standard richiesti.

Procedura di configurazione

Passaggio 1: Accedere all'interfaccia di Web Security Manager.

Passaggio 2: Passare alla configurazione Profili di identificazione.

Passare a Web Security Manager > Profili di identificazione.

Passaggio 3: Selezionare il profilo di identificazione desiderato che richiede il supporto di porte non standard.

Passaggio 4: Espandere le opzioni di configurazione avanzata.

Nella pagina del profilo di identificazione espandere la scheda Avanzate.

Passaggio 5: Configurare l'impostazione Proxy Ports.

Selezionare il collegamento accanto a Porte proxy per accedere alla configurazione della porta.

Passaggio 6: Aggiungere i numeri di porta non standard richiesti.

Aggiungere i numeri di porta specifici utilizzati dai client per le connessioni a porte non standard (ad esempio, 8890).

Passaggio 7: Salvare ed eseguire il commit delle modifiche alla configurazione.

Dopo aver implementato queste modifiche alla configurazione, il server WSA è in grado di elaborare e ispezionare il traffico sulle porte non standard specificate, consentendo al proxy di gestire correttamente le connessioni client e applicare policy al traffico che utilizza queste porte.

Causa

WSA 1000V è stato configurato con impostazioni predefinite della porta proxy che includevano solo porte HTTP (porta 80) e HTTPS (porta 443) standard. La configurazione delle porte proxy del profilo di identificazione non include le porte non standard richieste dalle applicazioni client. Senza la configurazione esplicita di queste porte nelle impostazioni avanzate del profilo di identificazione, WSA non è stata in grado di intercettare, elaborare o applicare i criteri al traffico utilizzando porte non standard, anche quando i criteri di autorizzazione sono stati configurati per le destinazioni.

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).