Blocco del protocollo dell'applicazione Secure Access che impedisce la connettività Internet

Sommario

- Problema
- Ambiente
- Risoluzione
  - Passaggio 1: Identificare la regola di blocco
  - Passaggio 2: Modifica impostazioni applicazione
  - Passaggio 3: Applicazione e verifica delle modifiche
- Causa
- Contenuto correlato

Problema

Dopo la migrazione a Cisco Secure Access, gli utenti hanno riscontrato un blocco della connettività Internet durante il tentativo di accedere ai servizi Web. Il sintomo specifico è il traffico HTTP bloccato dai criteri di sicurezza, che impedisce l'accesso a siti Web e applicazioni attendibili.

I dettagli dell'evento di blocco mostravano le seguenti caratteristiche:

- Azione: Bloccato
- Motivo blocco evento: AC_RULE_MATCH_BLOCK
- Destinazione: http://www.bing.com/api/shopping/v1/user/shoppingsettings
- Porta di destinazione: 443

- Categorie: Senza categoria
- Categoria applicazione: Cerca
- Protocollo applicazione: Hypertext Transfer Protocol
- Protocollo: TCP

Ambiente

- Distribuzione Cisco Secure Access
- Criterio di sicurezza attivo con restrizioni del protocollo dell'applicazione

Risoluzione

La risoluzione implica la modifica della configurazione delle regole di sicurezza per consentire il traffico del protocollo dell'applicazione HTTP mantenendo la postura di sicurezza per le applicazioni realmente non attendibili.

Passaggio 1: Identificare la regola di blocco

Individuare la regola specifica che causa il blocco nell'interfaccia di gestione Secure Access:

- Nome regola: Test
- Configurazione corrente: Utilizzo del blocco Impostazioni applicazione come destinazione.

Passaggio 2: Modifica impostazioni applicazione

Accedere alla configurazione della regola e controllare il nome delle impostazioni dell'applicazione in Destinazione:

- Passare a Risorse > Risorse Internet e SaaS > Elenchi applicazioni. Quindi, fare clic sull'applicazione.
- Individuare le impostazioni del protocollo applicativo.
- Deselezionare o rimuovere HTTP dall'elenco dei protocolli di applicazione bloccati.
- Garantire la presenza di altri controlli di protezione per le applicazioni non attendibili.

Passaggio 3: Applicazione e verifica delle modifiche

Salvare le modifiche alle regole e verificare la connettività:

1.- Applicare le modifiche della configurazione al criterio attivo.

2.- Verificare la connettività Internet con le destinazioni bloccate in precedenza.

3.- Monitorare i registri di protezione per garantire che il traffico HTTP legittimo sia ora consentito.

4.- Verificare che le altre protezioni di sicurezza restino efficaci.

Causa

La causa principale è una configurazione delle regole di sicurezza troppo restrittiva in Cisco Secure Access. La regola è stata configurata in modo da bloccare tutto il traffico HTTP del protocollo dell'applicazione, impedendo l'esplorazione Web e l'accesso all'applicazione legittimi. L'ampia applicazione del blocco del protocollo HTTP ha influito sulla normale connettività Internet per gli utenti che accedono a servizi Web e applicazioni attendibili che utilizzano i protocolli HTTP/HTTPS.

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).