

Configurazione per il download dei file ZIP protetti da password

Sommario

Problema

Dopo la migrazione a Cisco Secure Access, gli utenti non possono scaricare file ZIP protetti da password (crittografati). I download hanno sempre esito negativo quando tentano di accedere al contenuto dei file crittografati tramite il servizio Secure Access. Questo problema si verifica nonostante siano stati configurati criteri di traffico con connessione Internet su un dispositivo C8200 con più regole di sicurezza, tra cui il blocco basato su categorie, i controlli di ispezione SSL e la funzionalità sandbox.

Si verificano errori di download completi durante il tentativo di accedere a file ZIP protetti da password precedentemente accessibili prima della migrazione di Secure Access. Il problema persiste in più gruppi di tunnel e interessa tutti e 15 i percorsi configurati.

Ambiente

- Cisco Secure Access (ID organizzazione accesso sicuro: 8320925)
- Dispositivo C8200 che gestisce i criteri di traffico associati a Internet
- Gruppi di tunnel multipli su 15 siti (TK-TG e altri)
- Criteri di ispezione SSL con configurazioni abilitate e disabilitate
- Profili di sicurezza sandbox abilitati in determinati criteri
- Profili IPS configurati su regole di accesso specifiche

Risoluzione

La risoluzione per consentire i download di file ZIP protetti da password in Cisco Secure Access implica la configurazione dell'impostazione Consenti accesso a file crittografati e l'implementazione di soluzioni appropriate quando necessario.

Metodo di configurazione principale

Passaggio 1: Accedere alla configurazione dei criteri di accesso sicuro Cisco

Passare al criterio di accesso specifico che gestisce il traffico interessato nel dashboard Cisco Secure Access.

Passaggio 2: Abilitazione dell'accesso ai file crittografati

Nel criterio Impostazioni avanzate, individuare e attivare l'opzione Consenti accesso ai file crittografati. Questa impostazione è configurata in base alle regole e controlla se è possibile accedere al contenuto crittografato tramite il criterio specifico.

Passaggio 3: Applicazione della configurazione

Salvare e applicare le modifiche ai criteri per renderle attive per il traffico degli utenti.

Metodo alternativo per la soluzione

Se il metodo primario non risolve il problema, implementare la soluzione descritta nelle sezioni seguenti.

Passaggio 1: Identificazione degli URL interessati

Determinare gli URL o i domini specifici in cui sono ospitati i file ZIP protetti da password che causano errori di download.

Passaggio 2: Configura elenco indirizzi non decrittografati

Aggiungere gli URL identificati all'elenco Do Not Decrypt nella configurazione di Cisco Secure Access. In questo modo si impedisce l'ispezione SSL su questi URL specifici.

Passaggio 3: Crea criterio di bypass ispezione SSL

Verificare che un criterio di accesso con ispezione SSL disabilitata sia configurato per gestire il traffico verso questi URL.

Questo criterio deve avere:

- Ispezione SSL disabilitata
- Tutti i profili di sicurezza disattivati
- Priorità più alta rispetto ai criteri SSL abilitati per l'ispezione

Riferimento alla configurazione dei criteri

L'ordine delle policy delineato nelle sottosezioni seguenti e le relative configurazioni possono essere utilizzate come riferimento per una corretta gestione del traffico.

Politica 1: Regola di blocco basata su categorie

- Nome criterio: IA-To-InternetContentBlock
- Profilo IPS: Nessuna

- Scopo: Blocca categorie di contenuto specifiche
- Destinazione: Tutti i gruppi di tunnel

Politica 2: Regola disabilitata per l'ispezione SSL

- Nome criterio: IA-SSL-Inspection-MUKOU
- Profilo IPS: Disabled
- Profili di protezione: Tutti disabilitati
- Destinazione: Tutti i gruppi di tunnel

Politica 3: Regola abilitata per l'ispezione SSL

- Nome criterio: Ispezione IA-SSL
- Profilo IPS: Attivato
- Profili di protezione: Funzionalità sandbox abilitata
- Destinazione: Tutti i gruppi di tunnel

Note importanti sulla configurazione

Non esiste un equivalente delle impostazioni globali per la funzionalità Consenti accesso ai file crittografati. Questa impostazione deve essere configurata sui singoli criteri di accesso in base alle esigenze. Per ogni criterio che richiede l'accesso ai file crittografati, questa impostazione deve essere attivata in modo esplicito nella configurazione delle impostazioni avanzate.

Durante il test delle modifiche alla configurazione, attendere il tempo necessario per la propagazione delle policy nell'infrastruttura Cisco Secure Access prima di convalidare la funzionalità. Gli incidenti relativi all'assistenza o le finestre di manutenzione possono influire sui risultati dei test e devono essere presi in considerazione durante la risoluzione dei problemi.

Causa

Il problema si verifica perché Cisco Secure Access, per impostazione predefinita, blocca l'accesso ai file crittografati come misura di sicurezza. Quando l'ispezione SSL è abilitata e rileva contenuto crittografato o protetto da password, il servizio impedisce il download a meno che non sia configurato esplicitamente per consentire tale accesso. L'impostazione Consenti accesso ai file crittografati nelle Impostazioni avanzate dei criteri di accesso controlla questo comportamento e, senza questa impostazione attivata, i file ZIP crittografati e il contenuto simile vengono bloccati durante il processo di download.

Inoltre, i criteri di ispezione SSL possono interferire con i download di file crittografati quando il processo di ispezione non è in grado di gestire correttamente il contenuto crittografato, richiedendo l'impostazione di accesso ai file crittografati o il bypass dell'ispezione SSL per gli URL interessati.

Contenuto correlato

- [Controlli di sicurezza avanzati](#)
- [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).