Verifica della decrittografia IPS in Cisco Secure Access

Sommario

Problema

Quando si utilizza Cisco Secure Access con VPN (Remote Access VPN) tramite Secure Client, le organizzazioni devono verificare se la decrittografia e l'ispezione IPS (Intrusion Prevention System) vengono eseguite correttamente per il traffico verso siti Web specifici. La sfida principale consiste nel verificare che i processi di decrittografia e ispezione TLS funzionino correttamente tramite metodi diversi dai registri standard dell'interfaccia utente di gestione, ad esempio Ricerca attività. I requisiti di verifica specifici includono l'identificazione dei controlli dei certificati lato client o dei meccanismi di debug/reporting in grado di supportare la convalida dei test e fornire ulteriore conferma del funzionamento dell'IPS oltre l'interfaccia di gestione.

Ambiente

- Cisco Secure Access (CSA) con funzionalità RAVPN
- Cisco Secure Client per connessioni VPN ad accesso remoto
- Funzionalità di decrittografia e ispezione IPS abilitate
- Traffico TLS/SSL che richiede la decrittografia per l'ispezione della sicurezza
- Traffico Web da client RAVPN a siti Web esterni

Risoluzione

Per verificare che la decrittografia e l'ispezione IPS funzionino correttamente per il traffico VPN ad accesso remoto in Cisco Secure Access, è possibile procedere in due modi:

Metodo 1: Ricerca attività interfaccia utente di gestione (metodo primario)

La funzione Activity Search nell'interfaccia di gestione Cisco Secure Access rappresenta il metodo più affidabile per confermare le operazioni di decrittografia e ispezione IPS. Questa interfaccia visualizza registri e analisi dettagliati che mostrano quando il traffico è stato decrittografato e ispezionato dai servizi di sicurezza.

Per accedere a Ricerca attività:

Passare al dashboard di gestione Cisco Secure Access e individuare la funzionalità Ricerca attività per esaminare i log di ispezione del traffico e lo stato di decrittografia per sessioni utente e siti Web di destinazione specifici.

Per attivare i registri di decrittografia, è possibile attivare questa impostazione nelle impostazioni globali:

Dashboard -> Protetto -> Criteri di accesso -> Impostazioni predefinite regole e impostazioni globali -> Impostazioni globali -> Registrazione decrittografia.

Metodo 2: Verifica dei certificati lato client

Come ulteriore metodo di verifica, è possibile eseguire controlli dei certificati lato client per verificare che il traffico sia stato decrittografato.

Quando Cisco Secure Access decrittografa e ispeziona correttamente il traffico TLS, presenta il proprio certificato al client anziché il certificato del sito Web originale.

Per verificare la decrittografia mediante l'ispezione del certificato:

1. Controlla il certificato del sito Web
Aprire i dettagli del certificato nel browser ed esaminare l'emittente e il periodo di validità.

Se il certificato è rilasciato da una CA radice di Cisco Secure Access con un periodo di validità di circa 10 giorni, indica che il sistema di prevenzione delle intrusioni è stato decriptato a livello di firewall.

Se la validità del certificato è di circa 5 giorni, indica la decrittografia basata su Secure Web Gateway.

2. Convalida l'autorità di certificazione (denominazione controller di dominio)

Questo metodo di verifica dei certificati lato client funge da tecnica di conferma supplementare insieme al metodo di ricerca delle attività principali, fornendo ulteriore garanzia che i processi di decrittografia IPS funzionino come previsto.

Sistema di prevenzione delle intrusioni Non decrittografare:

La decrittazione per il sistema di prevenzione delle intrusioni verrà eseguita se:

· È abilitato con le impostazioni globali E

· Intrusion Prevention System è abilitato per almeno una delle regole dei criteri di accesso (credo che anche se la regola è disabilitata, questa condizione sia ancora valida)

Si desidera ignorare un dominio dalla decrittografia Intrusion Prevention System

Utilizzare l'elenco Do not decrypt fornito dal sistema e aggiungere il dominio nell'elenco Do not decrypt fornito dal sistema.

o

Utilizza la decrittografia basata sull'origine in Impostazioni globali per Cisco Secure Access -

NOTA: questa operazione funzionerà se NON è configurato ALCUN NAT in uscita nella configurazione del tunnel di rete su Secure Access.

Causa

La necessità di utilizzare più metodi di verifica deriva dalla necessità di convalidare l'applicazione delle policy di sicurezza negli ambienti aziendali. Sebbene i registri dell'interfaccia utente di gestione offrano una visibilità completa, i metodi di verifica lato client offrono punti di conferma aggiuntivi che possono essere utili per test di conformità, risoluzione dei problemi e scenari di convalida in cui l'accesso diretto alle interfacce di gestione può essere limitato o in cui sono necessari più punti di verifica per procedure di test approfondite.

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).