Applicazione delle policy di accesso sicuro per alcuni protocolli applicativi

Sommario

Introduzione

In questo documento viene descritta l'applicazione dei criteri di accesso sicuro quando si utilizzano determinati protocolli applicativi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso sicuro
- FTP (File Transfer Protocol)
- Protocollo TCP (Transmission Control Protocol)
- Firewall as a Service (FWaaS)
- SSH (Secure Shell)
- HTTP (Hyper Text Transfer Protocol)
- Connessione Internet UDP rapida (QUICK)
- Protocollo SMTP (Secure Mail Transfer Protocol)

Premesse

Un tipico test FWaaS per valutare l'applicazione di policy basata sul protocollo dell'applicazione è un test di utilizzo improprio del protocollo.

Il test per questo scenario solitamente comporta la creazione di un criterio che blocca un protocollo applicativo specifico, ad esempio FTP/SSH, su una porta non standard. Ad esempio, è possibile consentire l'FTP solo sulla porta TCP 21 e bloccare l'FTP sulla porta TCP 80.

Secure Access utilizza il rilevamento del protocollo OpenAppID per rilevare protocolli di applicazioni quali FTP, SSH, QUIC, SMTP e altri. e utilizza un gateway Web sicuro per proteggere il traffico HTTP(S).

Problema: il test dell'applicazione dei criteri per alcuni protocolli applicativi su TCP 80/443 determina il timeout della connessione e non viene generato alcun log in Secure Access

In alcune circostanze, ad esempio nel tentativo di consentire/bloccare alcuni protocolli come FTP sulla porta TCP 80/443, si verifica una situazione in cui la connessione iniziale tra il client e il server viene intercettata dal motore proxy, l'handshake TCP viene completato e quindi il motore proxy in Secure Access attende sul client di inviare il traffico, ma il protocollo richiede un segnale sul lato server per raggiungere il client.

Questa situazione determina il timeout della connessione a causa dell'attesa del client sul segnale del server e il proxy alla fine interrompe la connessione. Secure Access non genera registri per questo tipo di sessioni.

Soluzione

Si tratta di un comportamento previsto a causa del modo in cui il traffico Web è protetto dall'architettura Secure Access e poiché tale test interessa il traffico non Web (FTP, SSH, Telnet, SMTP, IMAP e altri protocolli che inizialmente si basano su un segnale sul lato server) sulle porte Web, per tale sessione non viene generato alcun log.

Informazioni correlate

- Guida per l'utente di Secure Access
- Pagina Secure Access Community
- Documentazione e supporto tecnico – Cisco Systems

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).