# Procedure consigliate per la pianificazione dell'aggiornamento del contenuto del firewall protetto

## Problema

Le organizzazioni che gestiscono dispositivi Firewall Threat Defense (FTD) con Firewall Management Center (FMC) richiedono linee guida sulle best practice per l'applicazione degli aggiornamenti della sicurezza e del contenuto. In particolare, non è chiaro con quale frequenza debbano essere applicati i diversi tipi di aggiornamento, se gli aggiornamenti possano essere pianificati anziché applicati immediatamente e quali siano gli impatti operativi di tali aggiornamenti. La domanda sorge perché Cisco rilascia spesso aggiornamenti dei contenuti, a volte settimanali, e gli amministratori devono capire se questi devono essere applicati immediatamente al momento del rilascio o se possono essere pianificati in base alle finestre di manutenzione organizzativa e alle policy di gestione delle modifiche.

## Ambiente

- Cisco Secure Firewall Firepower, tutte le versioni
- Firepower Management Center, tutte le versioni

## Risoluzione

Questa tabella mostra lo scopo di ogni tipo di aggiornamento in Firepower.

| Tipo di aggiornamento | Scopo | Note |
|---|---|---|
| SRU/LSP | Aggiornamenti delle regole di | Gestisce le regole di |

| | | |
|---|---|---|
| | intrusione (Snort 2 e Snort 3 rispettivamente) | rilevamento/prevenzione delle intrusioni |
| GeoDB | Dati di geolocalizzazione per indirizzi IP | Utilizzato per il filtraggio del traffico basato sulla geolocalizzazione |
| VDB | Informazioni sulla vulnerabilità e impronte digitali dell'host | Utilizzato per la valutazione della vulnerabilità e l'analisi dei rischi |

Gli aggiornamenti dei contenuti di Cisco Secure Firewall sono suddivisi in tre tipi, ciascuno con frequenze di rilascio diverse e procedure di pianificazione consigliate. In questa tabella vengono descritti i suggerimenti per la pianificazione delle procedure consigliate per ogni tipo di aggiornamento:

| Tipo di aggiornamento | Frequenza di rilascio | Pianificazione consigliata | Pianificazione predefinita FMC | Percorso Di Navigazione (Da Modificare) |
|---|---|---|---|---|
| SRU/LSP | Frequente | Giornaliero | Giornaliero | Sistema > Aggiornamenti contenuti > Aggiornamenti regole |
| GeoDB | ~Settimanale | Settimanale | Settimanale | Sistema > Aggiornamenti contenuti > Aggiornamenti geolocalizzazione |
| VDB | ~Mensile | Settimanale | Settimanale | Sistema > Strumenti: Pianificazione > Download settimanale del software |

Per configurazioni di sicurezza e postura ottimali, la best practice consiste nell'applicare uno qualsiasi di questi aggiornamenti non appena vengono rilasciati da Cisco. Alcuni di questi file di aggiornamento possono essere abbastanza grandi e le allocazioni della larghezza di banda devono essere prese in considerazione. Se si utilizza la stessa rete, si consiglia di installare gli aggiornamenti più grandi al di fuori delle ore di traffico di punta.

## Aggiornamenti SRU/LSP (Intrusion Rules)

Gli aggiornamenti SRU (Snort Rule Updates) e i Lightweight Security Packages (LSP) contengono regole per il rilevamento e la prevenzione delle intrusioni. Tali aggiornamenti devono essere applicati con la massima frequenza possibile dal punto di vista operativo per mantenere la

protezione contro le minacce emergenti.

Per modificare la pianificazione SRU/LSP: Selezionare Sistema > Aggiornamenti contenuti > Aggiornamenti regole nell'interfaccia di FMC per modificare le impostazioni di ora, data e frequenza.

Gli aggiornamenti SRU/LSP supportano l'installazione automatizzata e possono essere pianificati per l'installazione automatica dopo il download e l'installazione.

## Aggiornamenti GeoDB (Geolocation Database)

Gli aggiornamenti del database di georilevazione forniscono i dati sulla posizione geografica corrente per gli indirizzi IP e vengono in genere rilasciati ogni settimana.

Per modificare la pianificazione di GeoDB: Per modificare i parametri di programmazione, selezionare Sistema > Aggiornamenti contenuto > Aggiornamenti geolocalizzazione nell'interfaccia FMC.

Gli aggiornamenti di GeoDB possono essere pianificati per il download e l'installazione, ma l'installazione nei dispositivi gestiti richiede il push manuale e non può essere completamente automatizzata come gli aggiornamenti SRU/LSP.

## Aggiornamenti VDB (Vulnerability Database)

Vulnerabilità Gli aggiornamenti del database vengono pubblicati circa ogni mese e vengono gestiti come aggiornamenti software anziché come aggiornamenti del contenuto.

Per modificare la pianificazione VDB: Selezionare Sistema > Strumenti: Pianificazione e modifica dell'attività Download settimanale del software per regolare la frequenza e i tempi di download.

Gli aggiornamenti VDB rientrano negli aggiornamenti software e non possono essere distribuiti in modo indipendente. Sono inclusi quando si eseguono distribuzioni manuali che compilano tutte le modifiche in sospeso.

## Considerazioni sulla distribuzione

Durante la distribuzione degli aggiornamenti, FMC compila tutte le modifiche di configurazione in sospeso e può includere più tipi di aggiornamenti del contenuto in un'unica operazione di distribuzione. Alcuni aggiornamenti possono causare brevi riavvii del servizio Snort durante la

distribuzione, che devono essere presi in considerazione quando si pianificano gli aggiornamenti durante le ore di produzione.

Le organizzazioni devono allineare le pianificazioni degli aggiornamenti alle politiche di gestione delle modifiche e considerare la possibilità di pianificare gli aggiornamenti durante le finestre di manutenzione se brevi interruzioni del servizio rappresentano un problema per l'ambiente operativo.

## Causa

Si è trattato di una richiesta di assistenza per la configurazione e l'operatività piuttosto che di un malfunzionamento tecnico. La necessità di chiarimenti è sorta a causa dell'incertezza relativa alle procedure di pianificazione degli aggiornamenti, alle funzionalità di automazione e all'impatto operativo dei diversi tipi di aggiornamento dei contenuti negli ambienti Cisco Secure Firewall.

## Contenuto correlato

- Cisco Secure Firewall Management Center Administration Guide, 7.6: Aggiornamenti
- 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).