IPS Device Manager 5.1 - Firma di sintonizzazione

Sommario

Introduzione

Intrusion Prevention System (IPS) 5.1 contiene oltre 1000 firme predefinite incorporate. Non è possibile rinominare o eliminare firme dall'elenco delle firme incorporate, ma è possibile ritirare le firme per rimuoverle dal motore di rilevamento. In seguito sarà possibile attivare le firme ritirate. Tuttavia, questo processo richiede ai motori di rilevamento di ricostruire la loro configurazione, il che richiede tempo e potrebbe ritardare l'elaborazione del traffico. È possibile ottimizzare le firme incorporate quando si modificano diversi parametri di firma. Le firme incorporate modificate sono denominate *firme ottimizzate*.

In questo documento viene descritto come ottimizzare la firma utilizzando Gestione dispositivi IPS. IDM è un'applicazione Java basata sul Web che consente di configurare e gestire il sensore. Il server Web per IDM risiede sul sensore. È possibile accedervi tramite Internet Explorer, Netscape o Mozilla.

Nota: è possibile creare firme, denominate *firme personalizzate*. Gli ID di firma personalizzati iniziano con 60000. È possibile configurarli in base a diversi fattori, ad esempio la corrispondenza delle stringhe nelle connessioni UDP, la registrazione dei problemi di rete e le analisi. Ogni firma viene creata utilizzando un motore di firma appositamente progettato per il tipo di traffico monitorato.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Intrusion Prevention System Device Manager 5.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Per configurare un sensore per il monitoraggio del traffico di rete per una firma specifica, è necessario attivare la firma. Per impostazione predefinita, quando si installa l'aggiornamento della firma vengono attivate le firme più importanti. Quando viene rilevato un attacco che corrisponde a una firma attivata, il sensore genera un avviso, che viene archiviato nell'archivio eventi del sensore. I client basati sul Web possono recuperare gli avvisi e altri eventi dall'archivio eventi. Per impostazione predefinita, il sensore registra tutti gli avvisi informativi o superiore.

Per alcune firme sono disponibili firme secondarie. In altre parole, la firma è divisa in sottocategorie. Quando si configura una firma secondaria, le modifiche apportate ai parametri di una firma secondaria vengono applicate solo a tale firma. Ad esempio, se si modifica la firma secondaria 3050 1 e si modifica la gravità, la modifica della gravità verrà applicata solo alla firma secondaria 1 e non a 3050 2, 3050 3 e 3050 4.

Ottimizza firme

Un'icona + indica che sono disponibili altre opzioni per questo parametro. Fate clic sull'icona **+** per espandere la sezione e visualizzare gli altri parametri.

Un'icona verde indica che il parametro utilizza attualmente il valore predefinito. Fare clic sull'icona verde per modificarla in rosso, attivando il campo dei parametri in modo da poter modificare il valore.

Procedura dettagliata

Per ottimizzare le firme, completare i seguenti passaggi:

1. Accedere a IDM utilizzando un account con privilegi di amministratore o di operatore.
2. Scegliere **Configurazione > Definizione firma > Configurazione firma**.Verrà visualizzato il riquadro Configurazione firma.
3. Per individuare una firma, scegliere un'opzione di ordinamento dall'elenco **Seleziona per**.Ad esempio, se si cerca una firma UDP Flood, scegliere **Protocollo L2/L3/L4** e quindi **UDP Floods**.Il riquadro Configurazione firme viene aggiornato e vengono visualizzate solo le firme che corrispondono ai criteri di ordinamento specificati.
4. Per ottimizzare una firma esistente, selezionarla e completare i seguenti passaggi:Fare clic

su **Modifica** per aprire la finestra di dialogo Modifica firma.Esaminate i valori dei parametri e modificate il valore di tutti i parametri che desiderate regolare.**Nota:** per scegliere più di un'azione evento, tenere premuto il tasto **Ctrl**.In Stato scegliere **Sì** per abilitare la firma.**Nota:** affinché il sensore rilevi attivamente l'attacco specificato dalla firma, è necessario abilitare la firma.In Stato specificare se la firma viene ritirata. Fare clic su **No** per attivare la firma. La firma verrà inserita nel motore.**Nota:** affinché il sensore rilevi attivamente l'attacco specificato dalla firma, è necessario attivare una firma.**Nota:** fare clic su **Annulla** per annullare le modifiche e chiudere la finestra di dialogo Modifica firma.Fare clic su **OK**.La firma modificata verrà visualizzata nell'elenco con Tipo impostato su Ottimizzato.**Nota:** se si desidera annullare le modifiche, fare clic su **Reimposta**.

5. Fare clic su **Applica** per applicare le modifiche e salvare la configurazione modificata.

Informazioni correlate

- Cisco Intrusion Prevention System
- Documentazione e supporto tecnico – Cisco Systems