Blocca URL nei messaggi di posta elettronica basati su TLD in Secure Email

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

- Passaggio 1. Creazione di un filtro
- Passaggio 2. Utilizzare Espressioni Regolari
- Passaggio 3. Test in modalità Monitor
- Considerazioni sulle prestazioni

Conclusioni

Introduzione

In questo documento viene descritto come bloccare gli URL nei messaggi di posta elettronica protetti di Cisco in base a domini di primo livello (TLD) specifici.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su Cisco Secure Email.

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.

Premesse

Il blocco di URL basati su domini di primo livello (TLD) specifici può essere un modo efficace per proteggere il sistema di posta elettronica da potenziali minacce. Cisco Email Security Gateway (CES/ESA) analizza la reputazione degli URL e li esegue in base a vari criteri.

Tuttavia, se la politica aziendale richiede il blocco di alcuni TLD, in questa procedura viene illustrato come ottenere questo risultato utilizzando filtri e dizionari nel sistema di posta elettronica.

Passaggio 1. Creazione di un filtro

Per bloccare un intero TLD, devi prima creare un filtro contenuti nel tuo sistema e-mail. Questo filtro identifica e blocca gli URL contenenti i TLD che si desidera limitare. È possibile migliorare questo processo utilizzando i dizionari per gestire gli elenchi di domini di dominio trusted e incorporare le espressioni regolari rilevanti. Aggiungendo queste espressioni regolari a un dizionario, è possibile gestire e applicare in modo efficiente i criteri di filtro.

Passaggio 2. Utilizzare Espressioni Regolari

Le espressioni regolari (regex) sono uno strumento potente per identificare modelli specifici negli URL.

Per bloccare in modo efficace gli URL basati su TLD, è possibile aggiungere queste espressioni regolari a un dizionario. Questo approccio consente una gestione e un aggiornamento semplificati dei criteri di filtraggio:

1. Espressione regolare per il blocco degli URL che inizia con http o https, incluso il supporto per i domini Punycode:

```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. Espressione regolare per bloccare gli URL in formato e-mail, che supporta anche Punycode:

```
(?i)https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)
```

Aggiungendo queste espressioni regolari a un dizionario, è possibile semplificare il processo di filtraggio degli URL, assicurandosi che il sistema di posta elettronica blocchi in modo efficiente i TLD specificati.

Dictionary Properties

Name: URL_TLD

Advanced Matching: ☐ Match whole words ☐ Case Sensitive

▷ Smart Identifiers: *Match specific patterns such as social security numbers and credit card numbers.*

Dictionary Number of terms: 2

Add Terms:

Separate multiple entries with line breaks.

Weight: 1

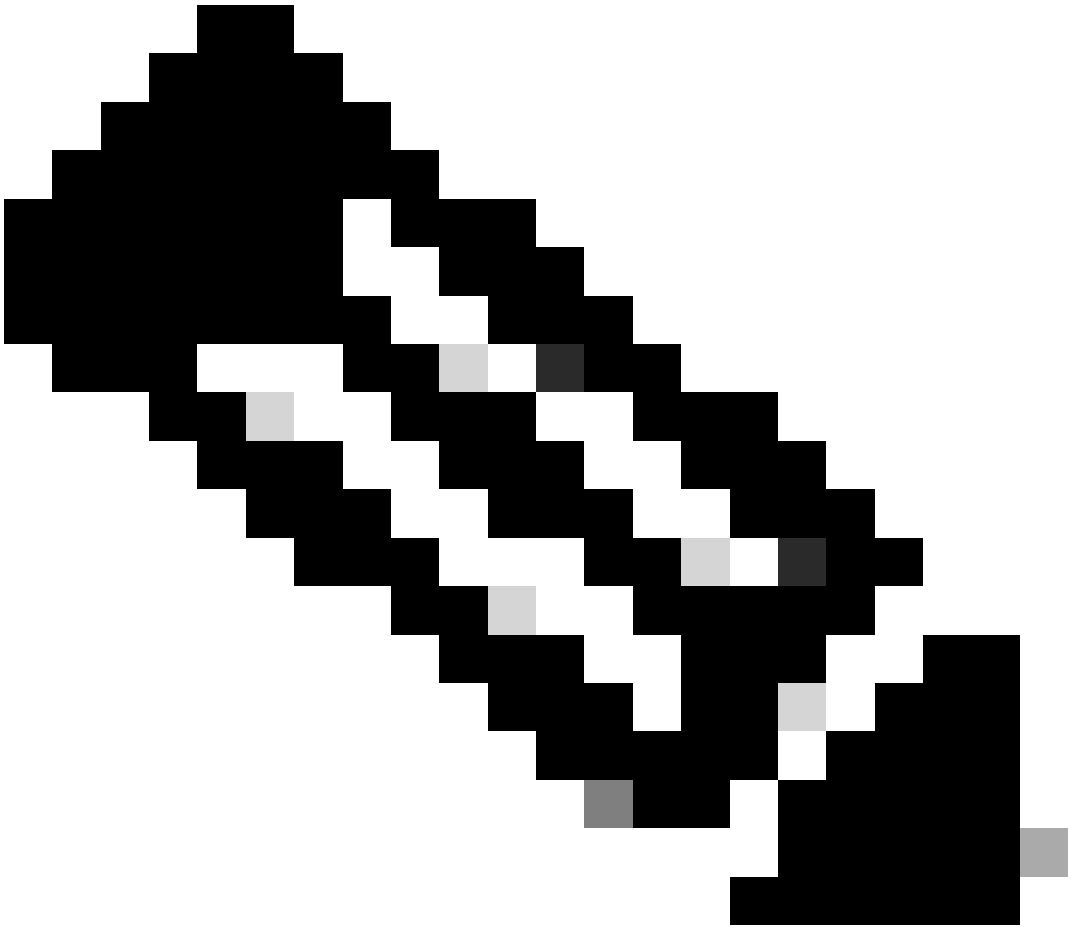
Add

Displaying 1 - 2 of 2 items
Page 1 of 1

<< Previous 1 Next >> 10

Term	Weight	Delete
https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)	1	
https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)	1	

Cancel Submit



Nota: Se è necessario considerare i caratteri Unicode, ad esempio U+2215 (⁄) e U+2044 (/), potrebbero essere necessarie ulteriori modifiche all'espressione regolare.

Passaggio 3. Test in modalità Monitor

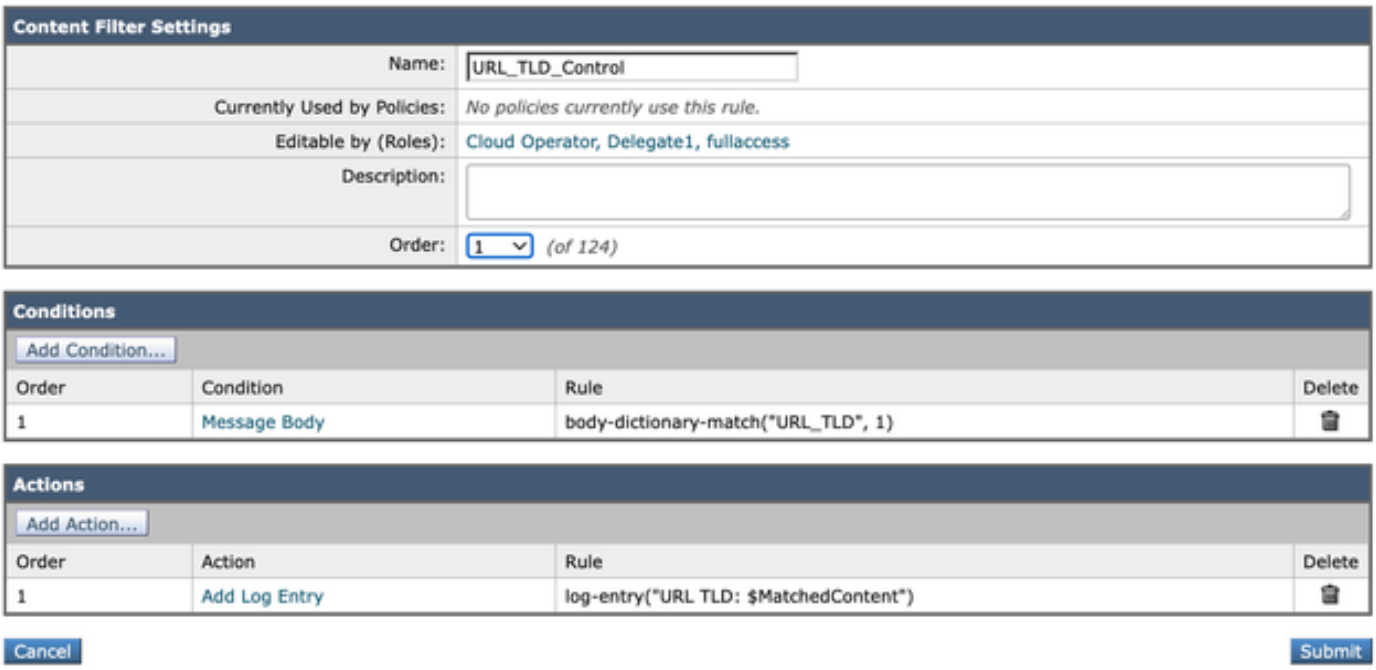
Prima di implementare questi filtri in un ambiente di produzione, si consiglia di utilizzarli in modalità di monitoraggio. Questo approccio consente di valutare l'efficacia dei filtri senza bloccare immediatamente le e-mail, evitando così interruzioni non intenzionali del sistema e-mail.

In modalità di monitoraggio, il sistema registra le istanze in cui gli URL corrispondono ai criteri specificati, consentendo all'utente di osservare i risultati e apportare le modifiche necessarie. A tale scopo, è possibile configurare un'azione della voce del log che acquisisca informazioni rilevanti sugli URL corrispondenti. Ad esempio, è possibile utilizzare l'azione seguente:

```
log-entry("URL TLD: $MatchedContent")
```

Questa azione consente di registrare il contenuto specifico che corrisponde ai criteri del filtro, fornendo informazioni utili sugli URL che verrebbero bloccati se il filtro fosse attivo. Esaminando questi log, è possibile perfezionare le espressioni regolari e le voci del dizionario per assicurarsi che acquisiscano accuratamente gli URL desiderati senza influire sulle e-mail legittime.

Inoltre, il monitoraggio dei log in un periodo di tempo consente di valutare l'impatto dei filtri sulle prestazioni e di apportare le ottimizzazioni necessarie. Dopo aver verificato che i filtri funzionano correttamente, è possibile passare dalla modalità monitor alla modalità blocco attivo:



Considerazioni sulle prestazioni

L'utilizzo esteso di espressioni regolari può avere un impatto negativo sulle prestazioni del sistema di posta elettronica. Pertanto, è essenziale testare e ottimizzare in base alle necessità.

Conclusioni

Il blocco di URL basati su TLD specifici può migliorare la sicurezza del sistema di posta elettronica. In particolare, i nuovi TLD introdotti da Google, come .zip e .mov, hanno sollevato problemi di sicurezza a causa della loro somiglianza con le estensioni di file più diffuse. Testare attentamente i filtri e considerare l'impatto sulle prestazioni consente di mantenere un sistema efficiente e sicuro.

Il registro di Google ha annunciato otto nuovi TLD: .dad, .phd, .prof, .esq, .foo, .zip, .mov e .nexus. Tuttavia, .zip e .mov hanno attirato particolarmente l'attenzione per la loro somiglianza alle estensioni di file ampiamente utilizzate, il che rende cruciale affrontare questi problemi nelle tue misure di sicurezza.

Per ulteriori informazioni sulle implicazioni di sicurezza del TLD .zip, si può consultare il post del blog Talos Intelligence: Perdita di informazioni TLD ZIP. Questa risorsa fornisce un contesto aggiuntivo sui rischi potenziali associati a questi domini di primo livello e sottolinea l'importanza di implementare strategie di filtraggio appropriate.

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).