Configurazione di Umbrella con il blade software anti-bot Check Point

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Panoramica

Funzionalità

Procedura di configurazione

- Prevenzione di interruzioni del servizio
- Passaggio 1: Generazione token API e script Umbrella
- Passaggio 2: distribuire lo script personalizzato sull'accessorio Check Point
- Passaggio 3. Creare o modificare un avviso per il punto di controllo da inviare al nuovo script
- Passaggio 4: Verifica dell'integrazione e impostazione degli eventi del punto di controllo da bloccare

Osservazione degli eventi aggiunti alla categoria di protezione dei punti di controllo in "Modalità di controllo"

- Esamina elenco di destinazione
- Rivedere le impostazioni di protezione per un criterio

Applicazione delle impostazioni di protezione del punto di controllo in "Modalità blocco" a un criterio per client gestiti

Creazione di report in Umbrella per gli eventi dei punti di controllo

- Creazione di report sugli eventi di sicurezza dei punti di controllo
- Segnalazione dell'aggiunta di domini all'elenco di destinazione del punto di controllo

Gestione di rilevamenti indesiderati o falsi positivi

- Gestione di un elenco di indirizzi consentiti per il rilevamento di elementi indesiderati
- Eliminazione di domini dall'elenco di destinazione del punto di controllo

Introduzione

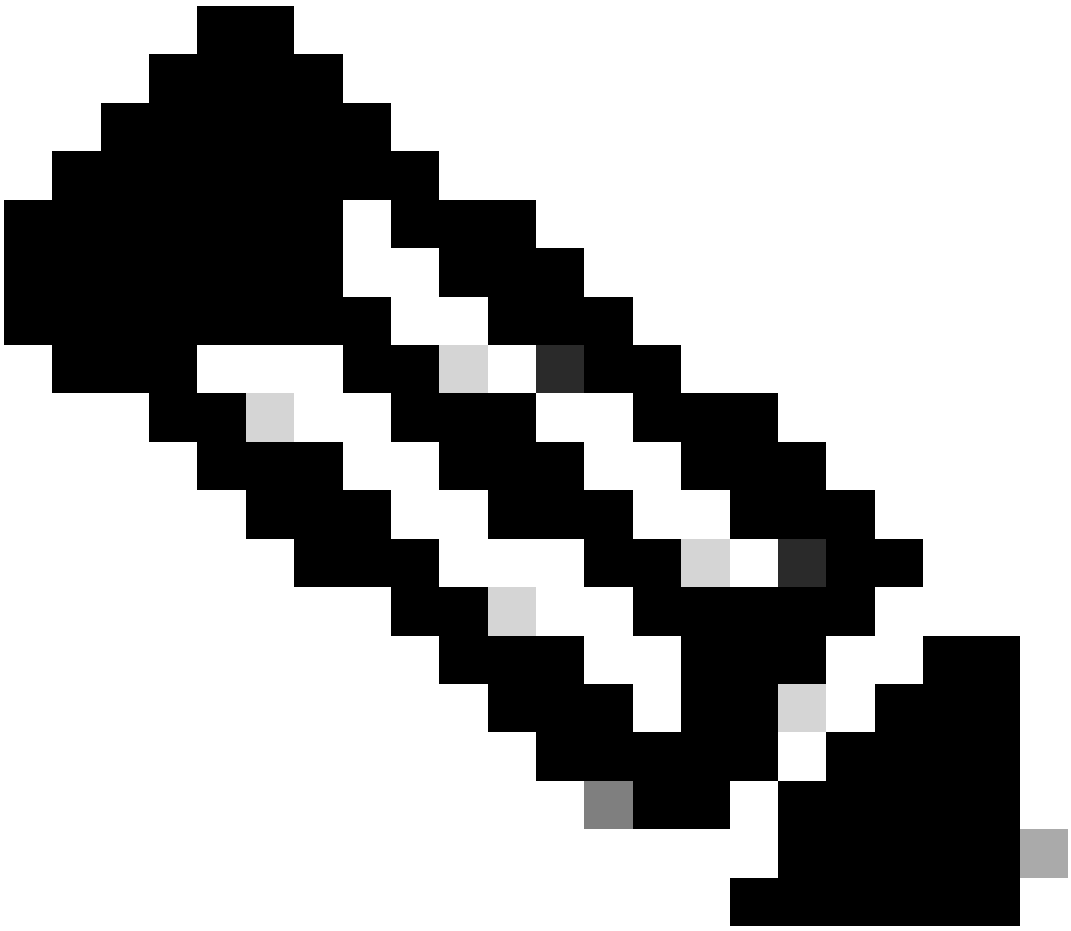
Questo documento descrive come integrare Cisco Umbrella con Check Point Anti-Bot Software Blade.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Un dispositivo Check Point con il blade software anti-boot
- Software Check Point versione R80.40 o successiva
- Verificare che il dispositivo del punto di controllo possa eseguire richieste HTTP in uscita su "https://s-platform.api.opendns.com".
- Un pacchetto Cisco Umbrella come DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage
- Diritti amministrativi di Cisco Umbrella Dashboard



Nota: L'integrazione Check Point è inclusa solo nei pacchetti Cisco Umbrella come DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Se non disponi di uno di questi pacchetti e desideri integrare Check Point, contatta il tuo Cisco Umbrella Account Manager. Se disponi del pacchetto Cisco Umbrella corretto ma non vedi Check Point come integrazione per il tuo dashboard, contatta il supporto Cisco Umbrella.

Componenti usati

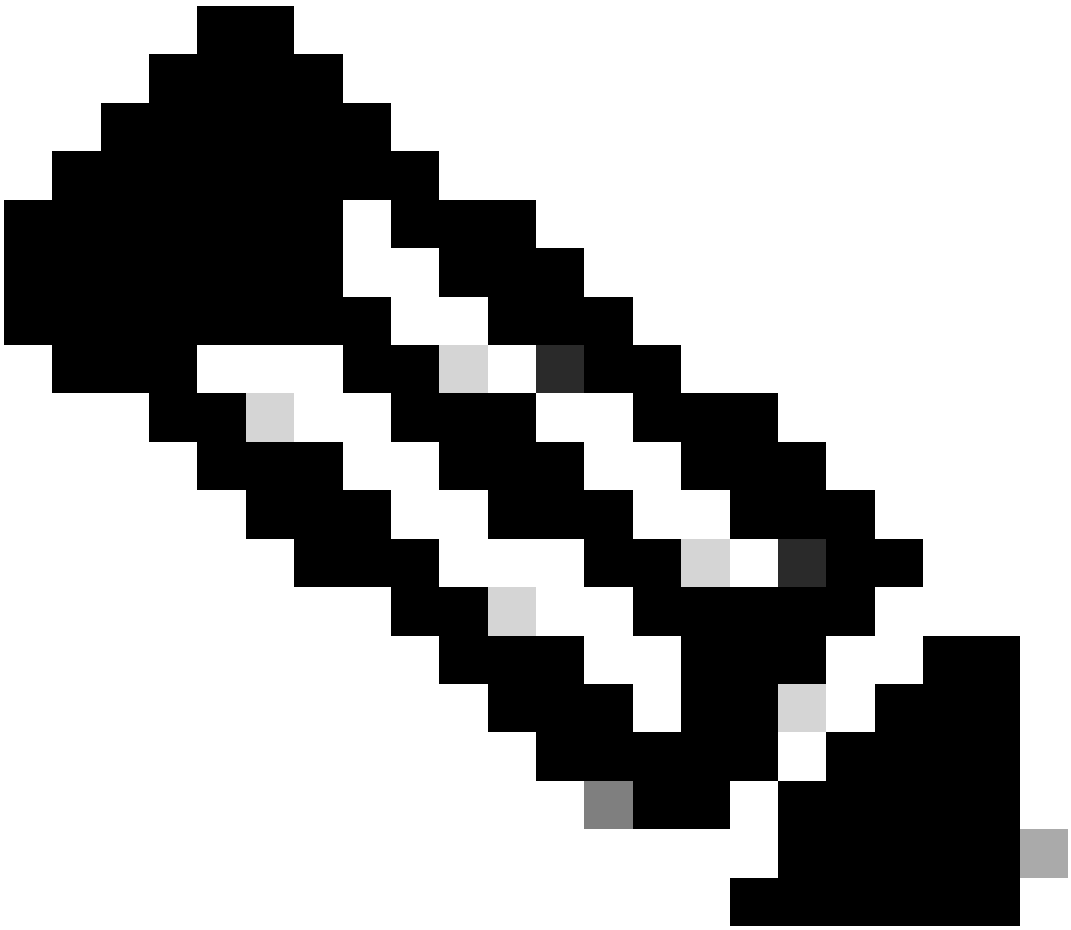
Le informazioni fornite in questo documento si basano su Cisco Umbrella.

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.

Panoramica

L'integrazione di Cisco Umbrella con il software anti-boot blade Check Point consente a un dispositivo Check Point di inviare a Cisco Umbrella gli avvisi del blade software anti-boot quando il blade rileva minacce nel traffico di rete che controlla. Gli avvisi ricevuti da Cisco Umbrella creano un elenco di blocchi che può proteggere notebook, tablet e telefoni in roaming su reti non protette dal blade software anti-boot Check Point.

In questo documento viene spiegato come configurare un dispositivo Check Point per inviare gli avvisi di blade con software anti-boot a Cisco Umbrella.



Nota: Questa integrazione è stata deprecata da Check Point nella versione R81.20 dopo che è stata inizialmente rilasciata in R80.40.

Funzionalità

L'integrazione di Cisco Umbrella con l'appliance blade software anti-bot Check Point invia le minacce rilevate (ad esempio, domini che ospitano malware, comandi e controllo di botnet o siti di phishing) a Cisco Umbrella per l'imposizione globale.

Cisco Umbrella convalida quindi la minaccia per verificare che possa essere aggiunta a una policy. Se viene confermato che le informazioni provenienti dal software anti-bot Check Point sono una minaccia, l'indirizzo di dominio viene aggiunto all'elenco di destinazione del check point come parte di un'impostazione di sicurezza che può essere applicata a qualsiasi criterio Cisco Umbrella. Tale criterio viene applicato immediatamente a qualsiasi richiesta effettuata dai dispositivi assegnati a tale criterio.

In futuro, Cisco Umbrella analizza automaticamente gli avvisi relativi ai punti di controllo e aggiunge siti dannosi all'elenco di destinazione dei punti di controllo. In questo modo la protezione tramite Check Point viene estesa a tutti gli utenti e i dispositivi remoti e viene fornito un altro livello di applicazione alla rete aziendale.

Procedura di configurazione

La configurazione dell'integrazione prevede i passi riportati di seguito.

1. Abilitare l'integrazione in Cisco Umbrella per generare un token API con uno script personalizzato.
2. Distribuire il token API e lo script personalizzato nell'accessorio Check Point.
3. Generare/modificare un avviso per il punto di controllo da inserire in questo nuovo script.
4. Imposta il blocco degli eventi del punto di controllo in Cisco Umbrella.

Prevenzione di interruzioni del servizio

Per evitare interruzioni indesiderate del servizio, Cisco Umbrella consiglia di aggiungere nomi di dominio mission-critical che non possono mai essere bloccati (ad esempio, google.com o salesforce.com) all'elenco globale degli indirizzi consentiti (o ad altri elenchi di destinazioni in base ai criteri dell'utente) prima di configurare l'integrazione.

I domini mission-critical possono includere:

- Home page dell'organizzazione
- Domini che rappresentano i servizi forniti e che possono avere record interni ed esterni. Ad esempio, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Le applicazioni basate su cloud meno note da cui dipende Cisco Umbrella non possono essere incluse nella convalida automatica del dominio. Ad esempio, "localcloudservice.com".

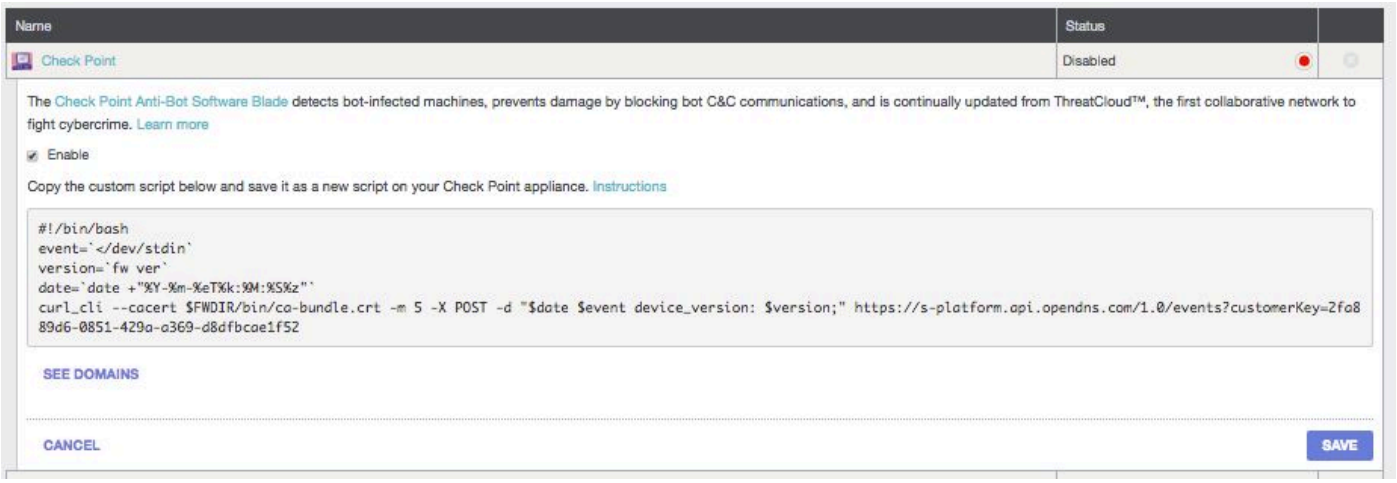
Questi domini devono essere aggiunti all'elenco globale degli oggetti autorizzati, che si trova in Criteri > Elenchi di destinazione in Cisco Umbrella.

Passaggio 1: Generazione token API e script Umbrella

1. Accedere a Cisco Umbrella Dashboard come amministratore.

2. Passare a Criteri > Componenti criterio > Integrazioni e selezionare Punto di controllo nella tabella per espanderlo.

3. Selezionare l'opzione Abilita.



4. Copiare l'intero script, a partire dalla riga con:

```
#!/bin/bash
```

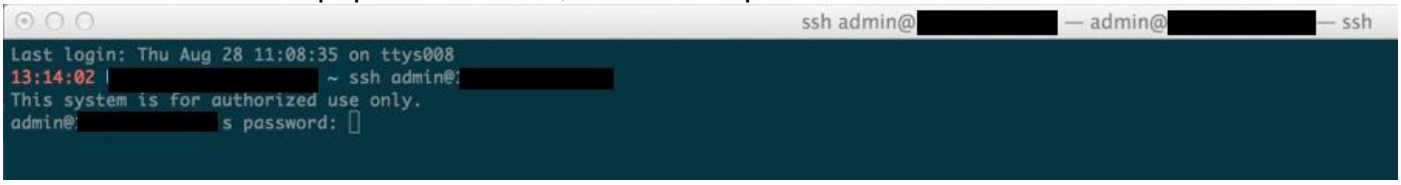
Lo script potrà quindi essere utilizzato nei passaggi successivi.

5. Selezionare Salva per abilitare l'integrazione.

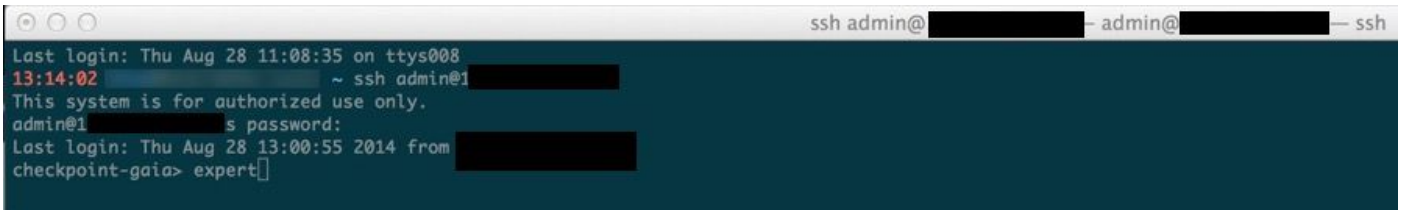
Passaggio 2: distribuire lo script personalizzato sull'accessorio Check Point

I passaggi successivi consistono nell'installare lo script Cisco Umbrella personalizzato sull'accessorio Check Point e quindi abilitarlo in SmartDashboard.

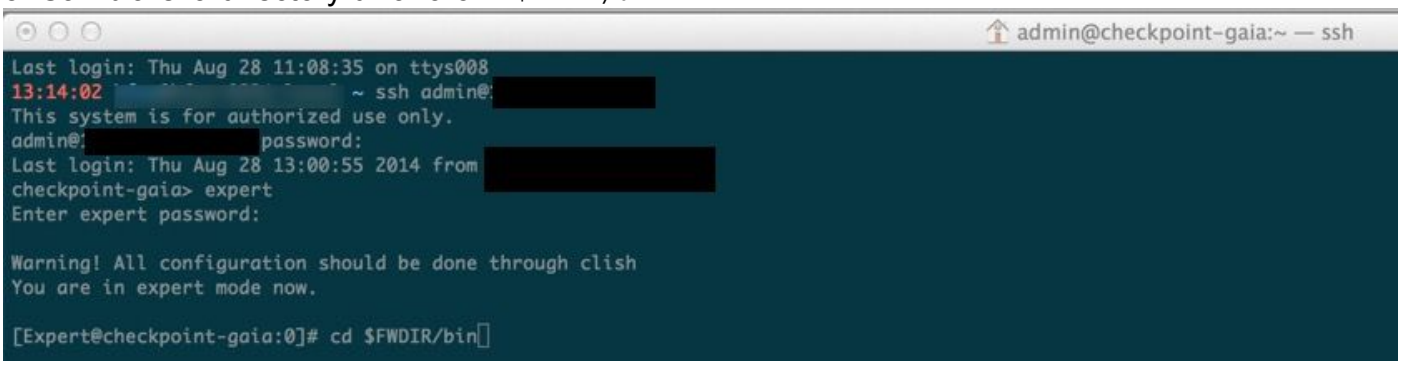
1. Per installare lo script personalizzato, SSH nel dispositivo Check Point come amministratore:



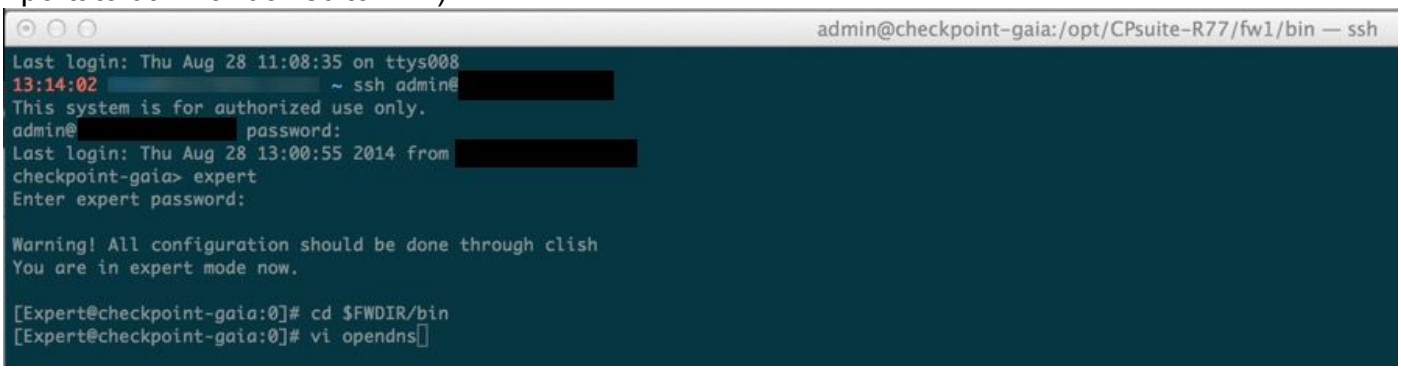
2. Quindi, avviare "Expert Mode" digitando "expert" nella riga di comando:



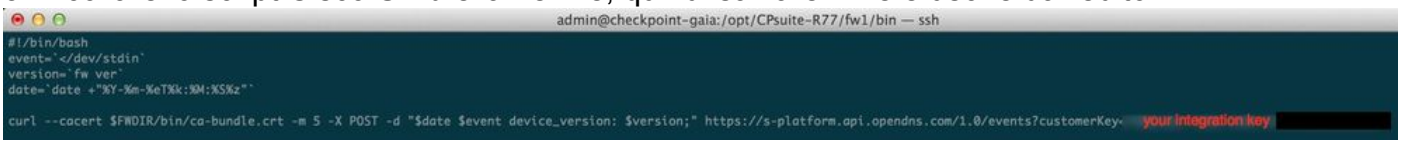
3. Cambiare la directory di lavoro in `$FWDIR/bin`:



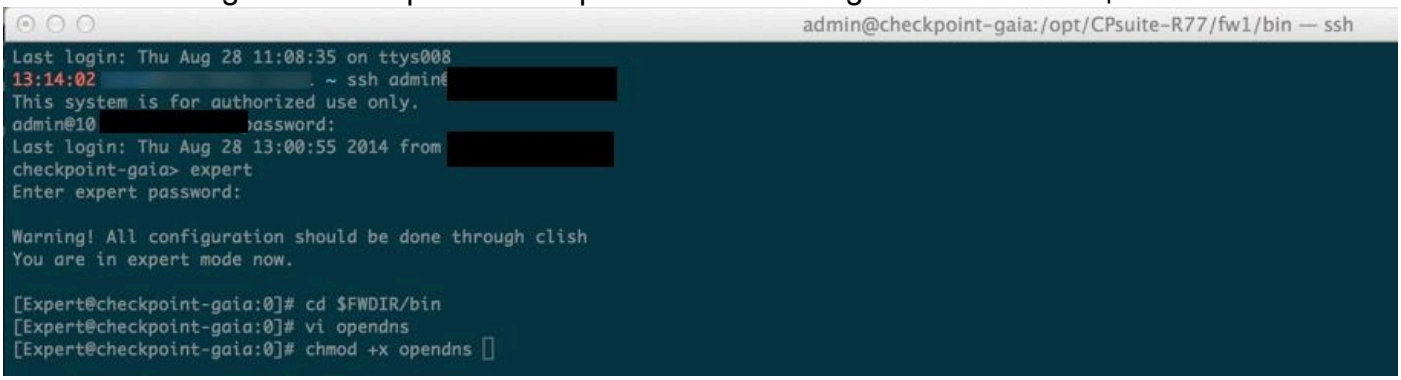
4. Aprire un nuovo file denominato "open" utilizzando un editor di testo (come nell'esempio riportato utilizzando l'editor "vi"):

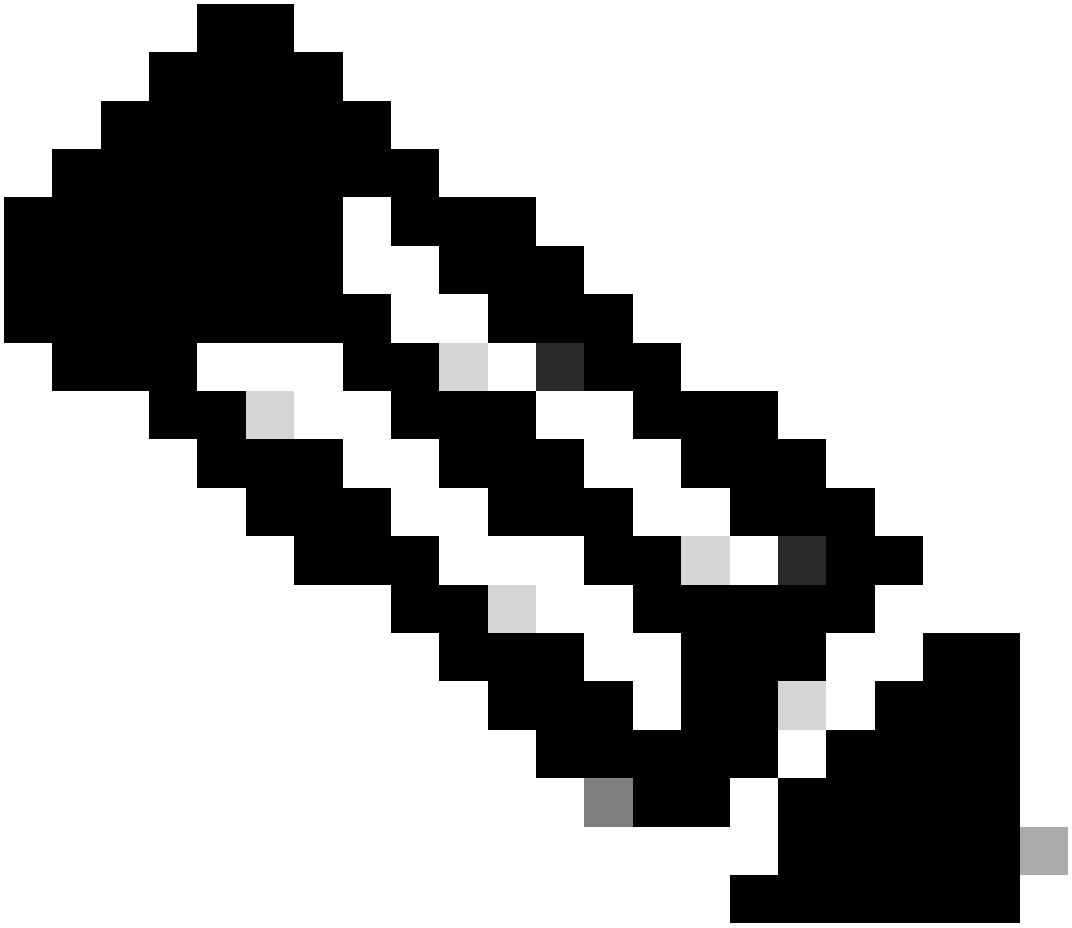


5. Incollare lo script Cisco Umbrella nel file, quindi salvare il file e uscire dall'editor:



6. Rendere eseguibile lo script Umbrella personalizzato eseguendo `chmod +x open`:



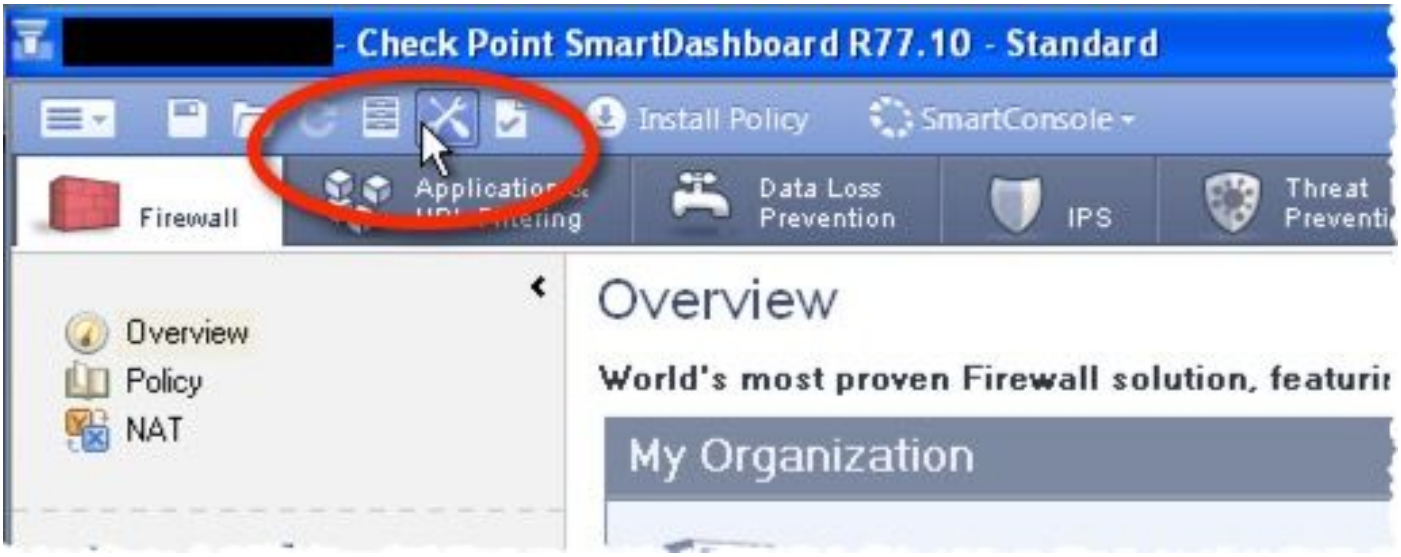


Nota: Se si aggiornano o si modificano le versioni di Blade, è necessario ripetere questi passaggi nella nuova versione.

Passaggio 3. Creare o modificare un avviso per il punto di controllo da inviare al nuovo script

1. Abilitare SmartDashboard per pubblicare il nuovo script eseguendo l'accesso e avviando SmartDashboard:

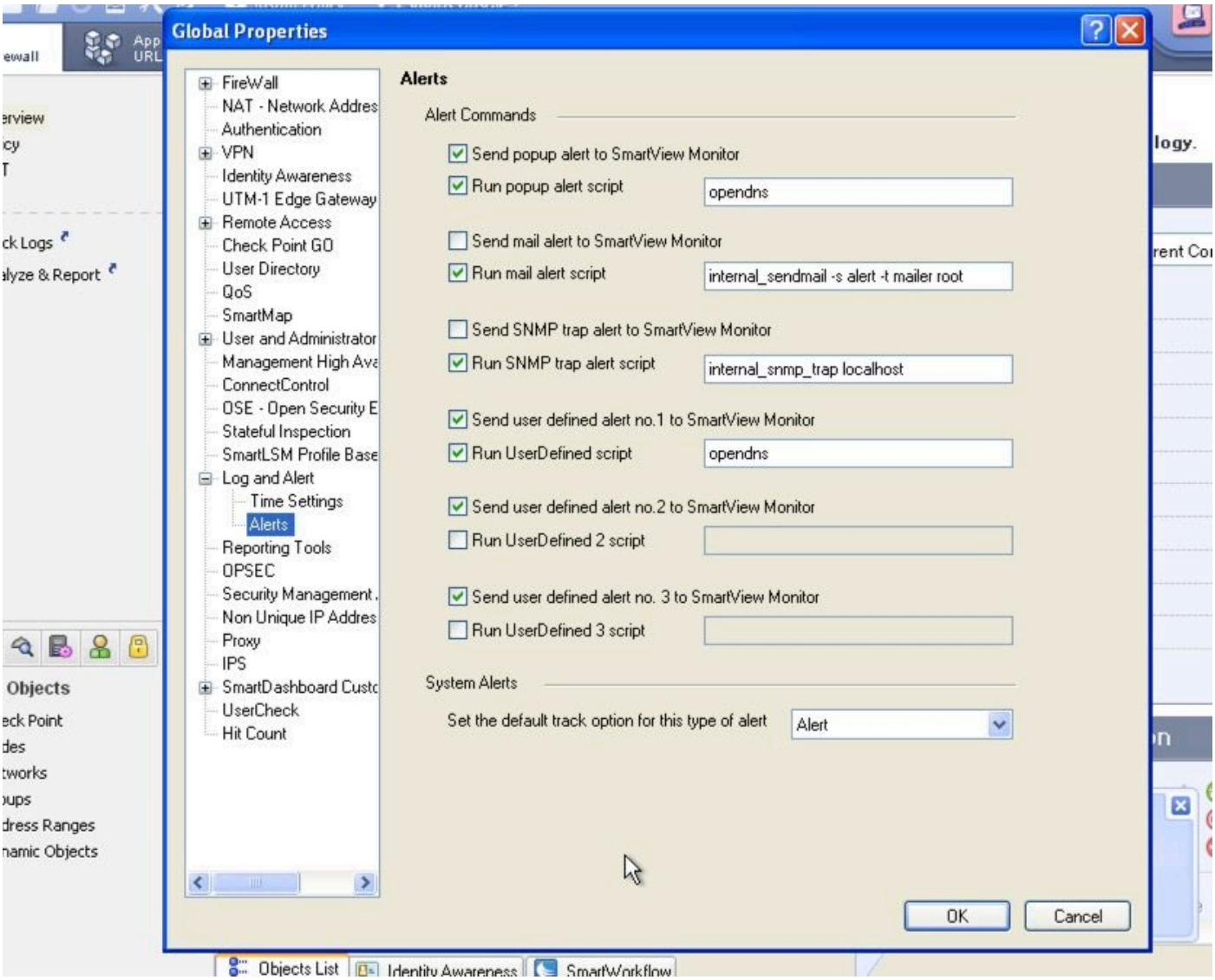
2. Aprire Proprietà globali:



3. In Proprietà globali, aprire Log and Alert > Alert e completare i passi riportati di seguito.

- Selezionare Invia script di avviso popup ed Esegui script definito dall'utente.
- Definire "open" nei campi di script per entrambi.

4. Selezionare OK. Da SmartDashboard, salvare e installare il criterio aggiornato.



Passaggio 4: Verifica dell'integrazione e impostazione degli eventi del punto di controllo da bloccare

In primo luogo, generare un evento blade di test anti-bot da visualizzare in Cisco Umbrella Dashboard:

1. Da qualsiasi dispositivo della rete protetto dall'accessorio Check Point, caricare questo URL nel browser:

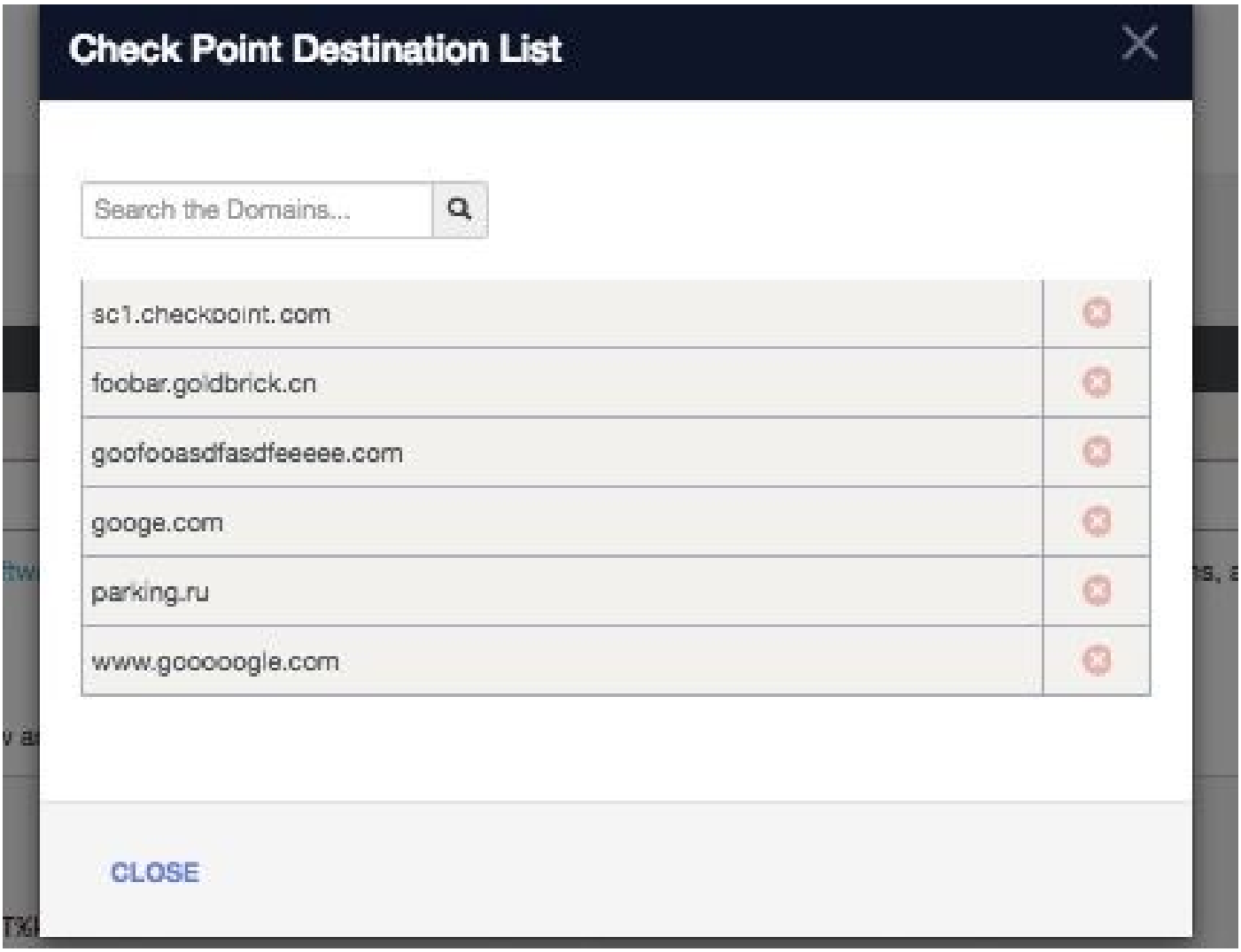
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

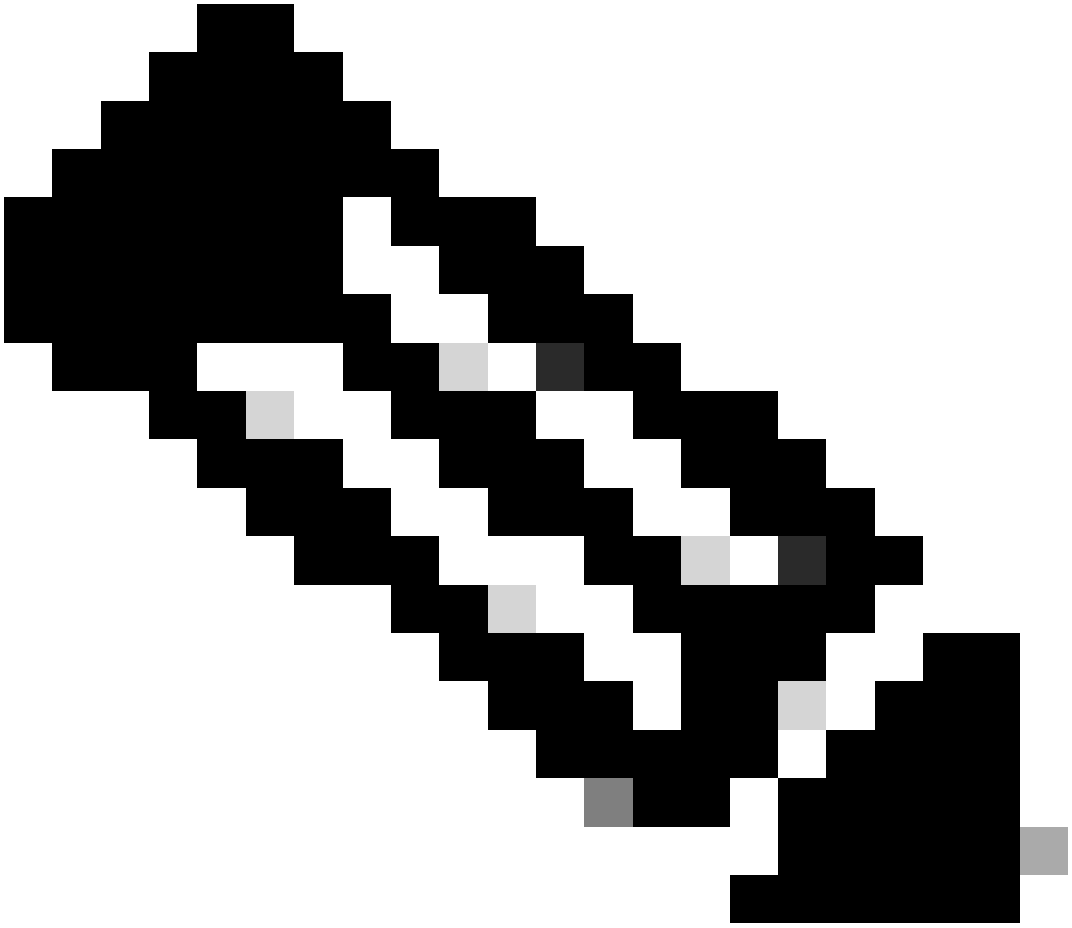
2. Accedi al dashboard di Cisco Umbrella come amministratore.

3. Passare a Criteri > Componenti criterio > Integrazioni e selezionare Punto di controllo nella tabella per espanderlo.

4. Selezionare Vedere Domini. Viene visualizzata una finestra che mostra l'elenco di destinazione

del punto di controllo che può includere "sc1.checkpoint.com". Da quel momento in poi, un elenco ricercabile inizia a essere popolato e a crescere.



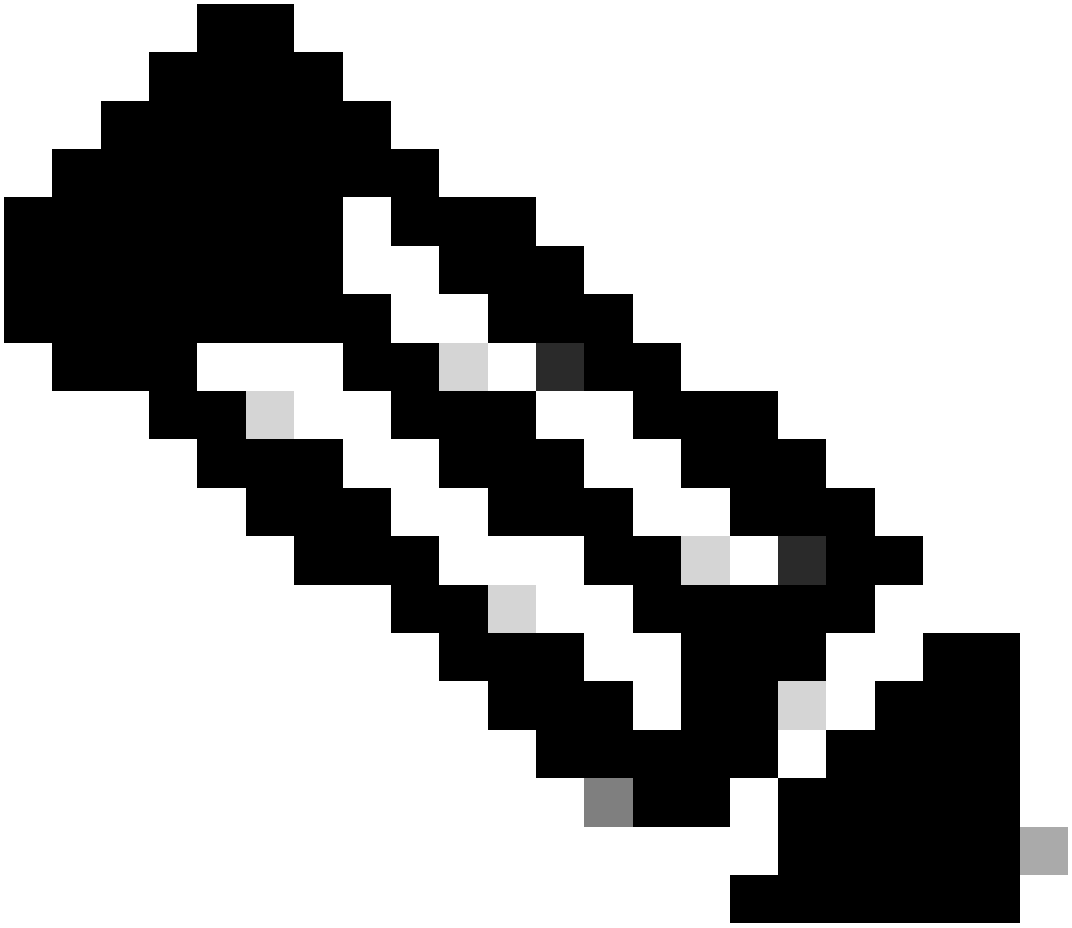


Nota: È inoltre possibile modificare l'elenco di destinazione se in questa posizione è visualizzato un dominio che non si desidera applicare in. Selezionare l'icona Elimina per rimuovere il dominio.

Osservazione degli eventi aggiunti alla categoria di protezione dei punti di controllo in "Modalità di controllo"

Il passaggio successivo consiste nell'osservare e controllare gli eventi aggiunti alla nuova categoria di protezione Punto di controllo.

Gli eventi generati dall'accessorio Check Point iniziano a compilare un elenco di destinazioni specifico che può essere applicato ai criteri come categoria di protezione Check Point. Per impostazione predefinita, l'elenco di destinazione e la categoria di sicurezza sono in "modalità di controllo" e non vengono applicati ad alcun criterio. Pertanto, non è possibile modificare i criteri Cisco Umbrella esistenti.



Nota: La "modalità di controllo" può essere attivata per il tempo necessario in base al profilo di distribuzione e alla configurazione di rete.

Esamina elenco di destinazione

È possibile consultare l'elenco delle destinazioni dei punti di controllo in qualsiasi momento in Cisco Umbrella:

1. Passare a Criteri > Componenti dei criteri > Integrazioni.

2. Espandere Check Point nella tabella e selezionare Vedere Domini.

Rivedere le impostazioni di protezione per un criterio

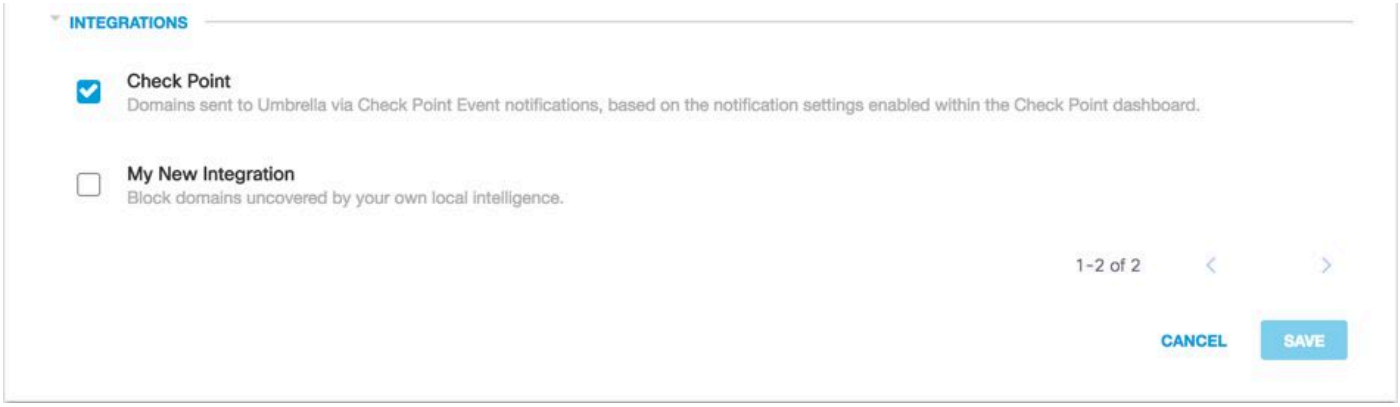
È possibile rivedere le impostazioni di sicurezza che possono essere abilitate per un criterio in qualsiasi momento in Cisco Umbrella:

1. Passare a Criteri > Componenti criterio > Impostazioni protezione.

2. Selezionare un'impostazione di protezione nella tabella per espanderla.

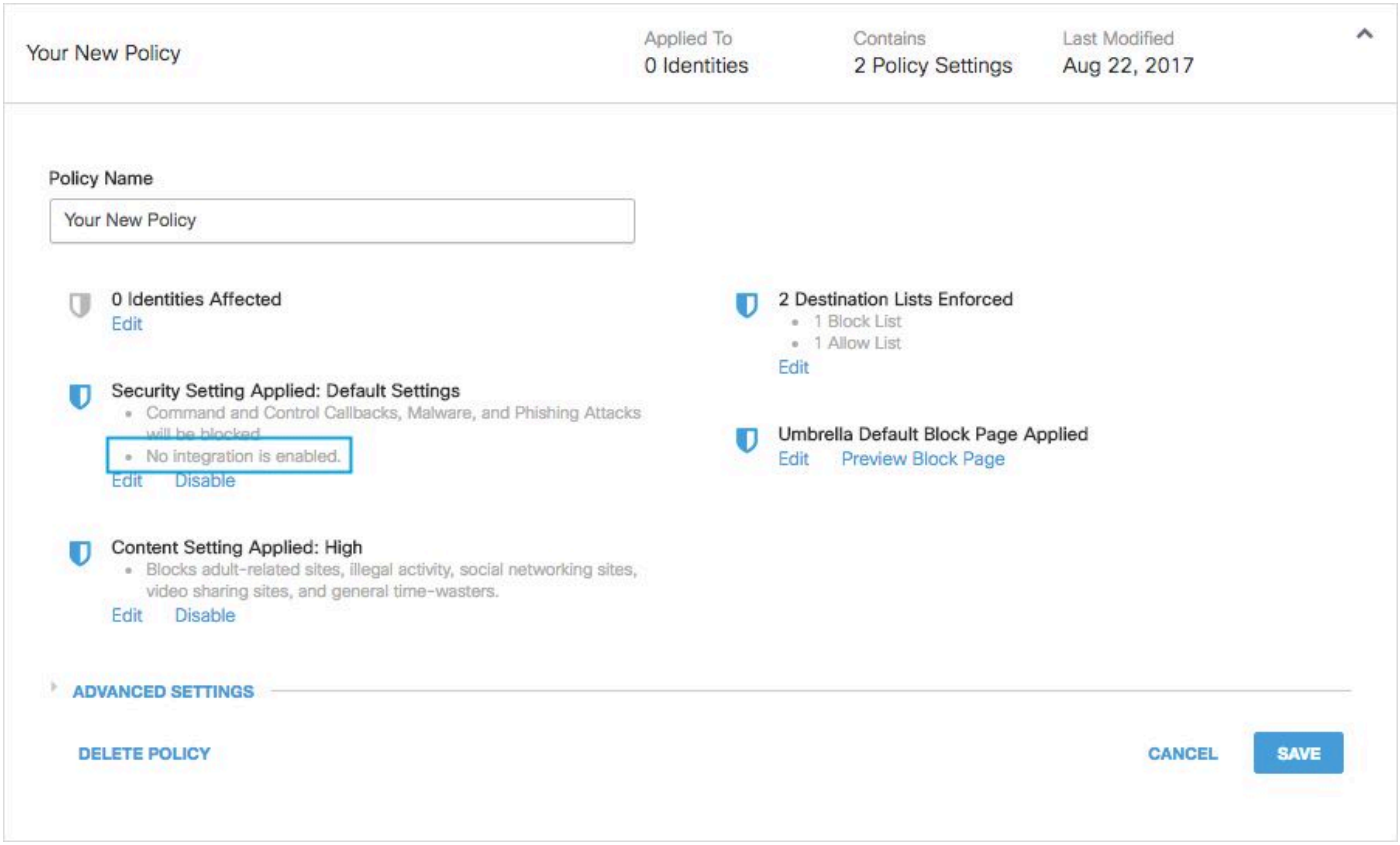
3. Scorrere fino alla sezione Integrazioni ed espandere la sezione per visualizzare l'integrazione Check Point.

4. Selezionare l'opzione per l'integrazione Check Point, quindi selezionare Salva.



115013984226

È inoltre possibile esaminare le informazioni sull'integrazione tramite la pagina Riepilogo impostazioni di protezione:



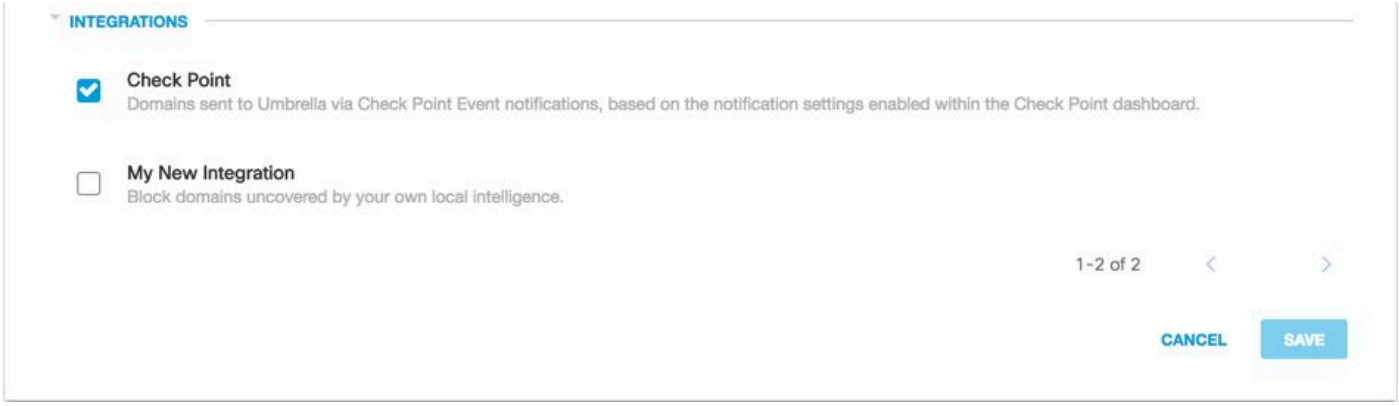
19916943300244

Applicazione delle impostazioni di protezione del punto di controllo in "Modalità blocco" a un criterio per client gestiti

Quando sei pronto a far applicare queste minacce alla sicurezza aggiuntive dai client gestiti da Cisco Umbrella, modifica le impostazioni di sicurezza su un criterio esistente o crea un nuovo criterio che si trovi al di sopra del tuo criterio predefinito per assicurarti che venga applicato per primo:

1. Assicurarsi che l'integrazione Check Point sia ancora abilitata come nella sezione precedente. Passare a Criteri > Componenti criterio > Impostazioni protezione e aprire l'impostazione appropriata.

2. In Integrazioni, verificare che l'opzione Punto di controllo sia selezionata. In caso contrario, selezionare l'opzione e scegliere Salva.



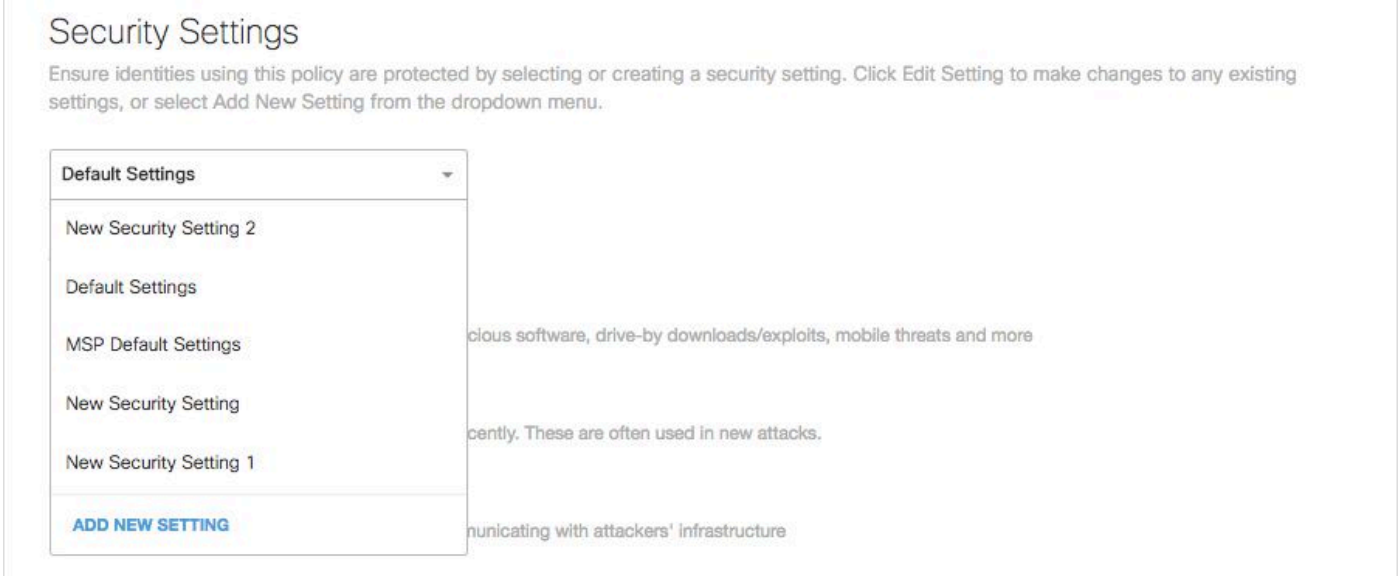
115013984226

Successivamente, nella procedura guidata Criteri Cisco Umbrella, aggiungere questa impostazione di protezione a un criterio che si sta modificando:

1. Passare a un criterio: o Criteri > Criteri DNS o Criteri > Criteri Web.

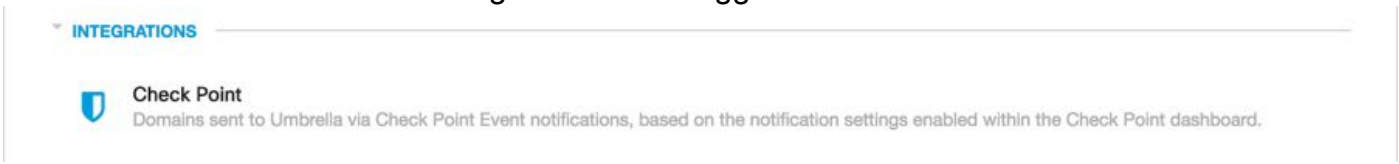
2. Espandere un criterio e in Impostazioni di protezione applicate (Criteri DNS) o Impostazioni di protezione (Criteri Web) selezionare Modifica.

3. Nell'elenco a discesa Impostazioni protezione, selezionare un'impostazione di protezione che includa l'impostazione Punto di controllo.



19916943316884

L'icona a forma di scudo sotto Integrations viene aggiornata in blu.



115014149783

4. Selezionare Set & Return (Criteri DNS) o Save (Criteri Web).

I domini del punto di controllo contenuti nell'impostazione di protezione per il punto di controllo possono quindi essere bloccati per le identità che utilizzano il criterio.

Creazione di report in Umbrella per gli eventi dei punti di controllo

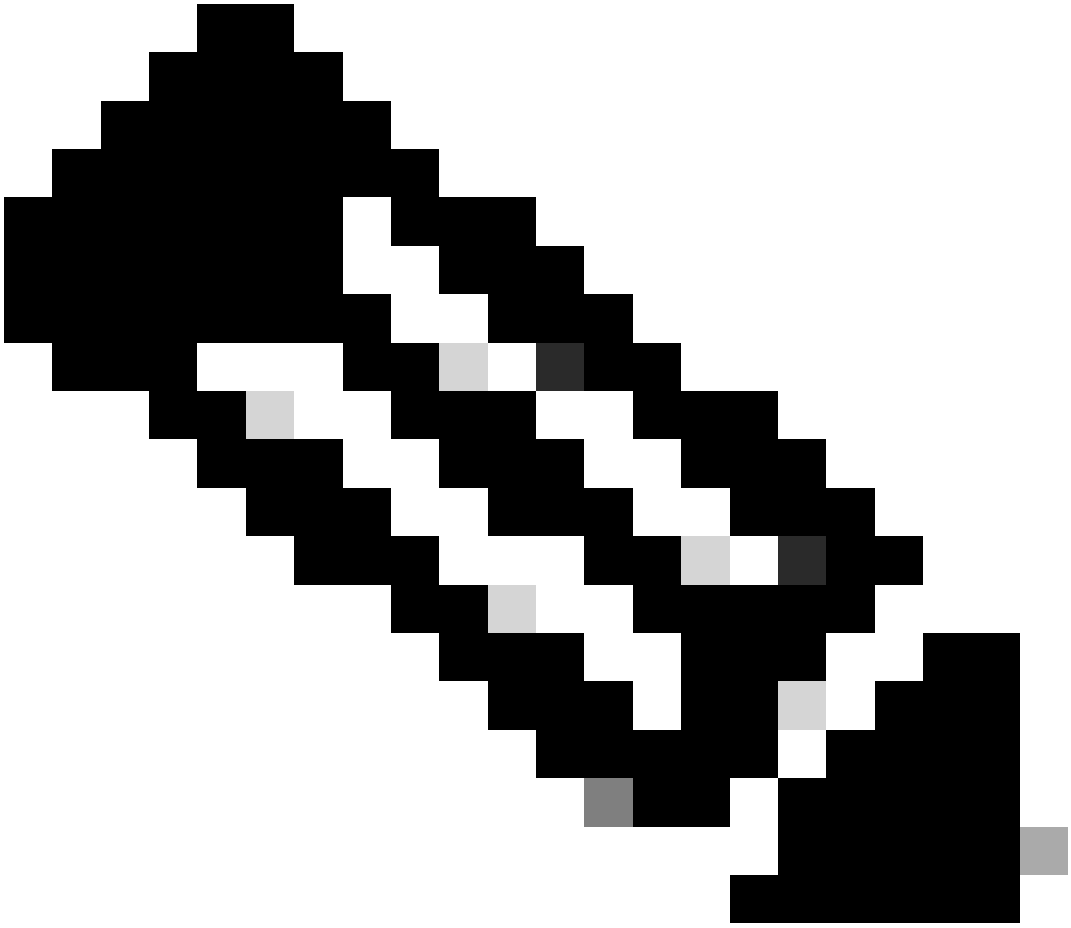
Creazione di report sugli eventi di sicurezza dei punti di controllo

L'elenco di destinazione del punto di controllo è una delle categorie di protezione disponibili per i report. La maggior parte o tutti i report utilizzano le categorie di protezione come filtro. Ad esempio, è possibile filtrare le categorie di protezione per visualizzare solo l'attività correlata al punto di controllo:

1. Passare a Rapporti > Rapporti principali > Ricerca attività.

2. In Categorie di protezione, selezionare Punto di controllo per filtrare il report in modo da visualizzare solo la categoria di protezione per il punto di controllo.

115014197623



Nota: Se l'integrazione Check Point è disattivata, non può essere visualizzata nel filtro Categorie di protezione.

3. Selezionare Applica per visualizzare l'attività relativa al punto di controllo per il periodo selezionato nel rapporto.

Segnalazione dell'aggiunta di domini all'elenco di destinazione del punto di controllo

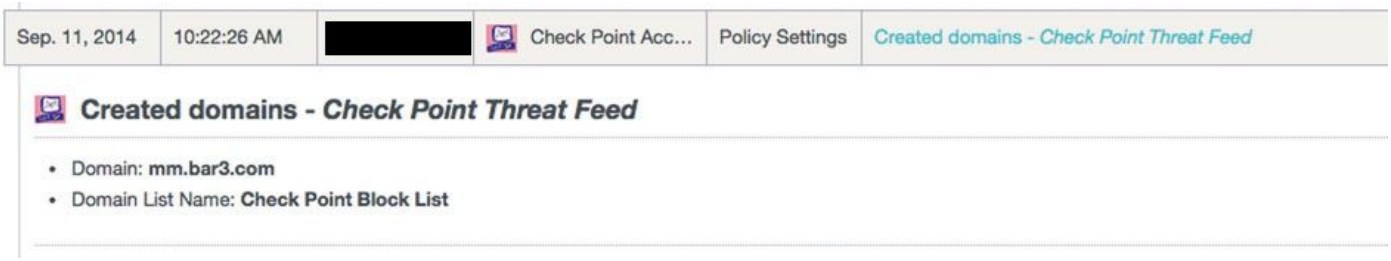
Il registro di controllo Cisco Umbrella Admin include gli eventi generati dall'accessorio Check Point durante l'aggiunta di domini all'elenco di destinazione. Questi domini sembrano essere aggiunti da un'etichetta "Account del punto di controllo", sotto la colonna Utente del registro di controllo.

Per trovare il log di controllo di amministrazione Umbrella, passare a Report > Log di controllo di amministrazione.

Per segnalare quando è stato aggiunto un dominio, applicare un filtro che includa solo le modifiche apportate al punto di controllo applicando un filtro Filtro in base a identità e impostazioni

per l'elenco di blocco del punto di controllo.

Una volta eseguito il report, sarà possibile visualizzare un elenco di domini aggiunti all'elenco di destinazione del punto di controllo.



Gestione di rilevamenti indesiderati o falsi positivi

Gestione di un elenco di indirizzi consentiti per il rilevamento di elementi indesiderati

Benché improbabile, è possibile che i domini aggiunti automaticamente dall'accessorio Check Point attivino un blocco indesiderato che può impedire agli utenti di accedere a determinati siti Web. In una situazione come questa, Cisco Umbrella consiglia di aggiungere il dominio o i domini a un elenco di indirizzi consentiti, che ha la precedenza su tutti gli altri tipi di elenchi di indirizzi, incluse le impostazioni di sicurezza. Un elenco Consenti ha la precedenza su un elenco Blocca quando un dominio è presente in entrambi.

Vi sono due motivi per cui questo approccio è preferito:

- In primo luogo, nel caso in cui l'accessorio Check Point dovesse aggiungere di nuovo il dominio dopo la rimozione, l'elenco Consenti impedisce che ciò provochi ulteriori problemi.
- In secondo luogo, l'elenco Consenti mostra una registrazione cronologica di domini problematici per analisi legali o rapporti di audit successivi.

Per impostazione predefinita, esiste un elenco di indirizzi consentiti globale che viene applicato a tutti i criteri. L'aggiunta di un dominio all'elenco globale degli indirizzi consentiti comporta che il dominio sia consentito in tutti i criteri.

Se l'impostazione di sicurezza Check Point in modalità di blocco viene applicata solo a un sottoinsieme delle identità Cisco Umbrella gestite, ad esempio solo a computer mobili e dispositivi mobili mobili, è possibile creare un elenco Consenti specifico per tali identità o criteri.

Per creare un elenco Consenti:

1. Passare a Criteri > Elenchi di destinazione e selezionare l'icona Aggiungi.

2. Selezionare Allow (Consenti), quindi aggiungere il dominio all'elenco.

3. Selezionare Salva.

Una volta salvato l'elenco, è possibile aggiungerlo a un criterio esistente relativo ai client interessati dal blocco indesiderato.

Eliminazione di domini dall'elenco di destinazione del punto di controllo

Accanto a ogni nome di dominio nell'elenco di destinazione del punto di controllo è presente un'icona Elimina. L'eliminazione dei domini consente di pulire l'elenco di destinazione del punto di controllo in caso di rilevamento indesiderato.

Tuttavia, l'eliminazione non è definitiva se il dispositivo Check Point invia nuovamente il dominio a Cisco Umbrella.

Per eliminare un dominio:

1. Passare a Impostazioni > Integrazioni, quindi selezionare Punto di controllo per espanderlo.

2. Selezionare Vedere Domini.

3. Cercare il nome di dominio che si desidera eliminare.

4. Selezionare l'icona Elimina.

5. Selezionare Chiudi.

6. Selezionare Salva.

In caso di rilevamento indesiderato o di falso positivo, Cisco Umbrella consiglia di creare immediatamente un elenco degli accessi consentiti in Cisco Umbrella e quindi di correggere il falso positivo all'interno di Check Point Appliance. In seguito, è possibile rimuovere il dominio dall'elenco di destinazione del punto di controllo.

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).