Configurare il rilevamento delle minacce per i servizi VPN di accesso remoto in Cisco Firepower Device Manager

Sommario

Introduzione

Questo documento descrive il processo di configurazione del rilevamento delle minacce per i servizi VPN ad accesso remoto su Cisco Firepower Device Manager (FDM).

Prerequisiti

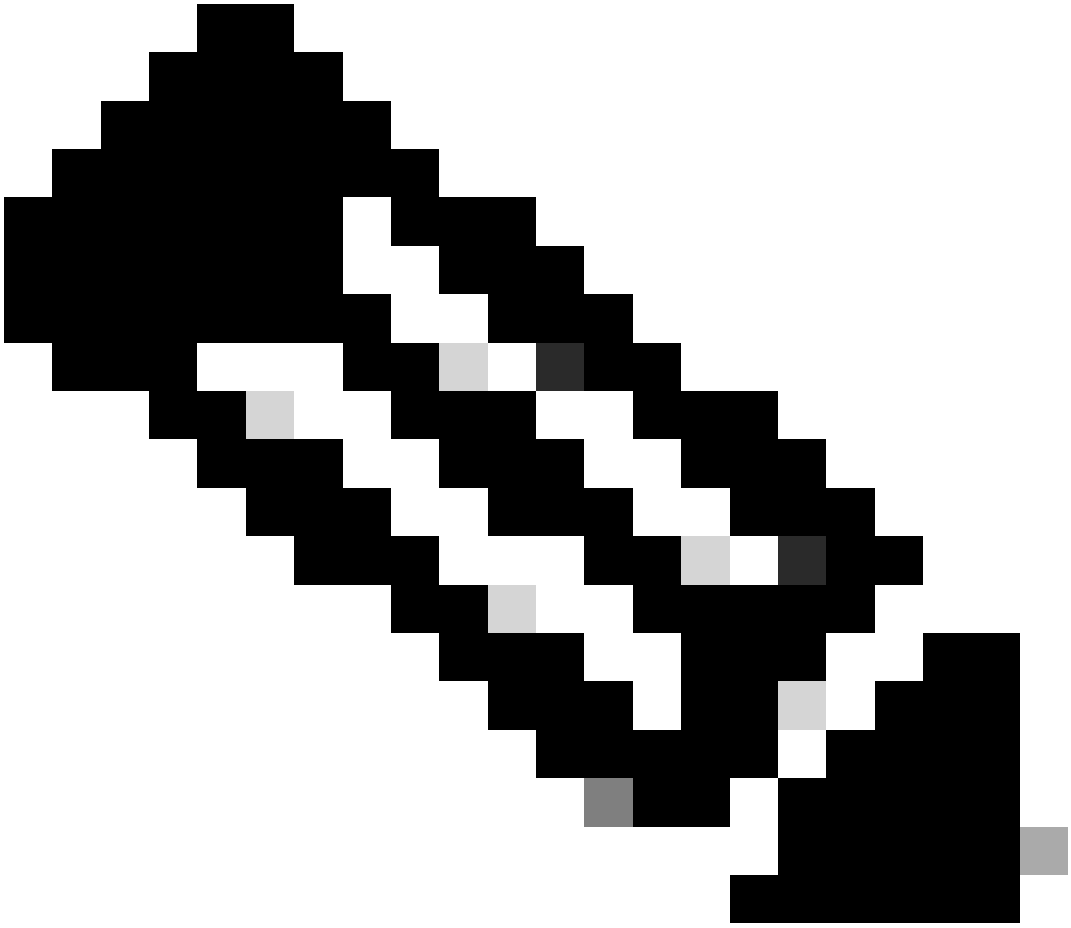
Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Threat Defense (FTD).
- Cisco Firepower Device Manager (FDM).
- RAVPN (Remote Access VPN) su FTD.

Requisiti

Queste funzionalità di rilevamento minacce sono supportate nelle versioni di Cisco Secure Firewall Threat Defense elencate di seguito:

- versione 7.0 treno-> supportato da 7.0.6.3 e versioni più recenti all'interno di questo treno specifico.
- 7.2 versione treno-> supportato da 7.2.9 e versioni più recenti all'interno di questo treno specifico.
- 7.4 versione treno-> supportato da 7.4.2.1 e versioni più recenti all'interno di questo treno specifico.
- 7.6 versione train-> supportata dalla 7.6.0 e da tutte le versioni più recenti.



Nota: queste funzioni non sono attualmente supportate nei treni versione 7.1 o 7.3.

Componenti usati

Le informazioni descritte in questo documento si basano sulle seguenti versioni hardware e software:

- Cisco Secure Firewall Threat Defense Virtual versione 7.4.2.1

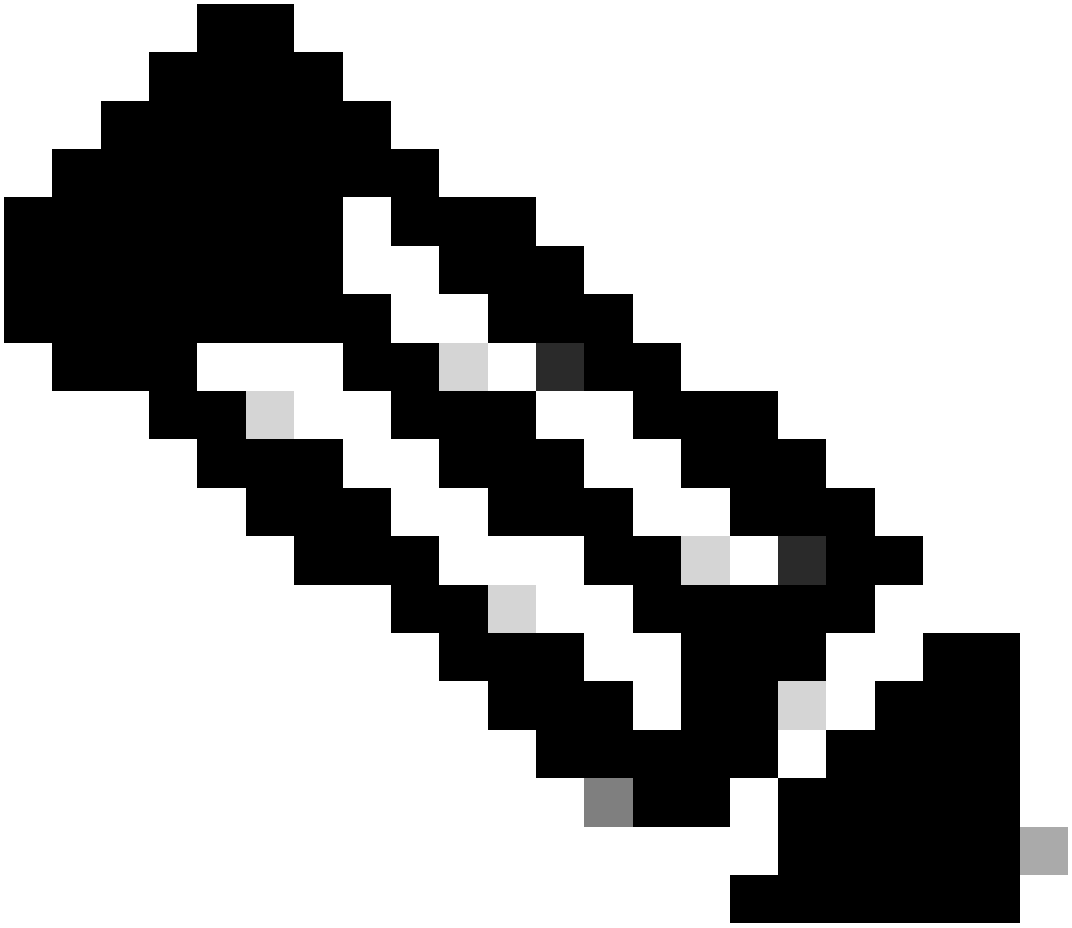
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

Le funzionalità di rilevamento delle minacce per i servizi VPN ad accesso remoto impediscono attacchi Denial of Service (DoS) da indirizzi IPv4 bloccando automaticamente l'host (indirizzo IP) che supera le soglie configurate per impedire ulteriori tentativi finché non si rimuove manualmente la condivisione dell'indirizzo IP. Per i successivi tipi di attacco sono disponibili servizi distinti:

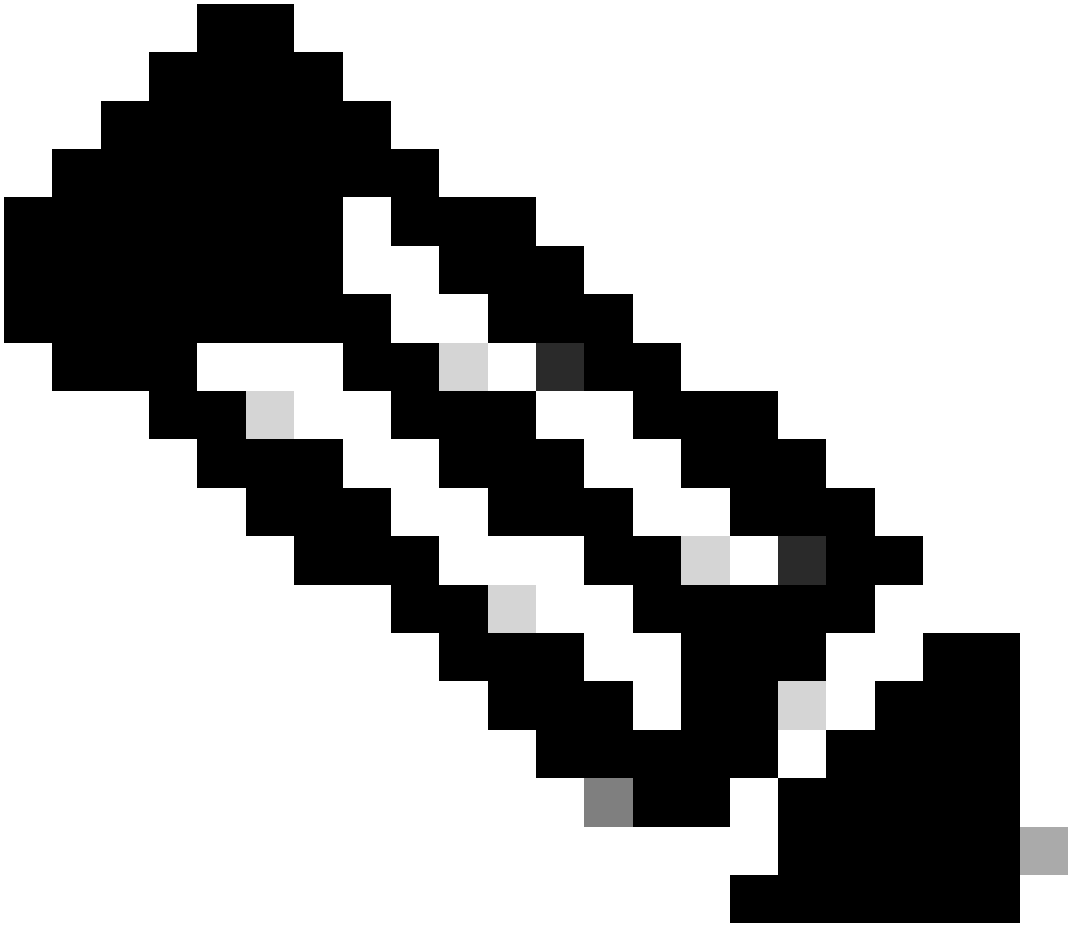
- Tentativi ripetuti di autenticazione non riusciti: Tentativi ripetuti non riusciti di autenticazione per i servizi VPN ad accesso remoto (attacchi brute-force di scansione di nome utente/password).
- Attacchi di avvio client: quando l'autore dell'attacco si avvia ma non completa più volte i tentativi di connessione a un headend VPN ad accesso remoto da un singolo host.
- Tentativi di connessione a servizi VPN ad accesso remoto non validi: quando gli autori di attacchi tentano di connettersi a gruppi di tunnel predefiniti destinati esclusivamente al funzionamento interno del dispositivo. Gli endpoint legittimi non tentano di connettersi a questi gruppi di tunnel.

Questi attacchi, anche quando non riescono a ottenere l'accesso, possono consumare risorse di calcolo e impedire agli utenti validi di connettersi ai servizi VPN di accesso remoto. Quando si attivano questi servizi, il firewall ignora automaticamente l'host (indirizzo IP) che supera le soglie configurate. In questo modo si evitano ulteriori tentativi fino a quando non si rimuove manualmente la sequenza dell'indirizzo IP.



Nota: per impostazione predefinita, tutti i servizi di rilevamento minacce per VPN ad accesso remoto sono disabilitati.

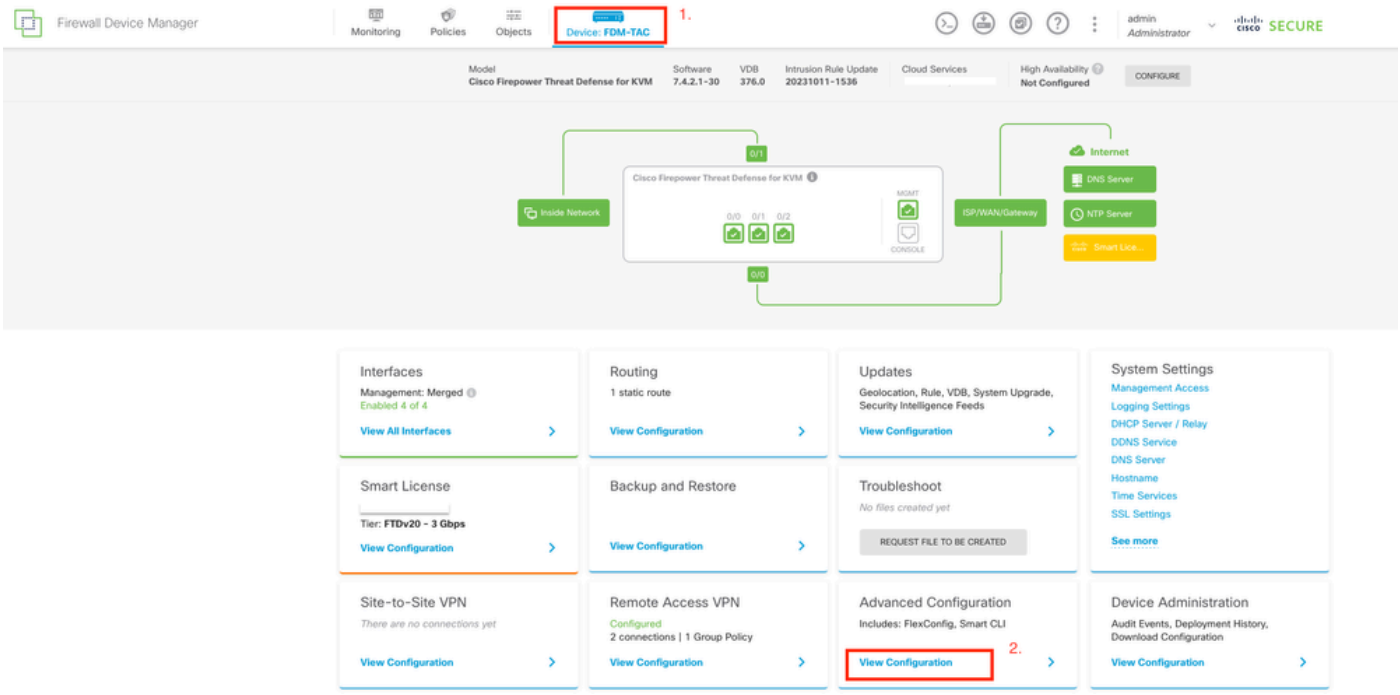
Configurazione



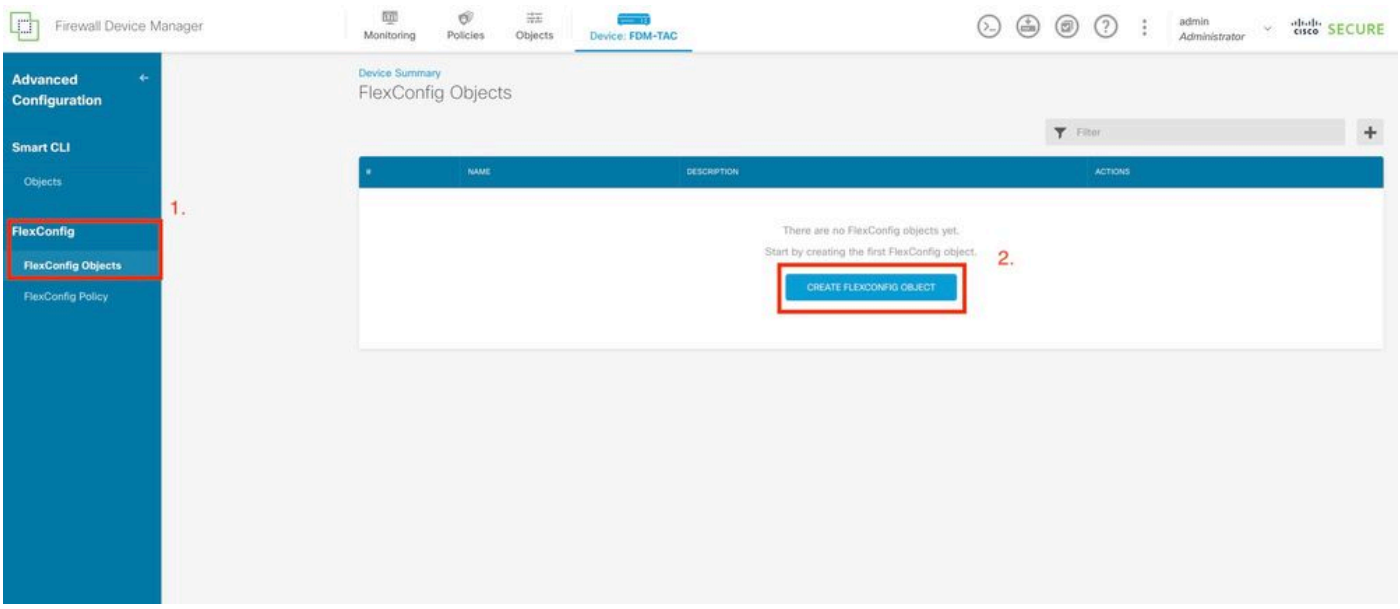
Nota: la configurazione di queste funzionalità in Secure Firewall Threat Defense è attualmente supportata solo tramite FlexConfig.

1. Accedere a Firepower Device Manager.

2. Per configurare l'oggetto FlexConfig, selezionare Dispositivo > Configurazione avanzata > FlexConfig > Oggetti FlexConfig, quindi fare clic su Crea oggetto FlexConfig.



Modificare 'Configurazione avanzata' dalla home page di FDM.



Creare un oggetto FlexConfig.

3. Una volta aperta la finestra oggetto FlexConfig, aggiungere la configurazione necessaria per abilitare le funzionalità di rilevamento minacce per la VPN ad accesso remoto:

Funzionalità 1: rilevamento minacce per tentativi di connessione a servizi VPN di solo interno (non validi)

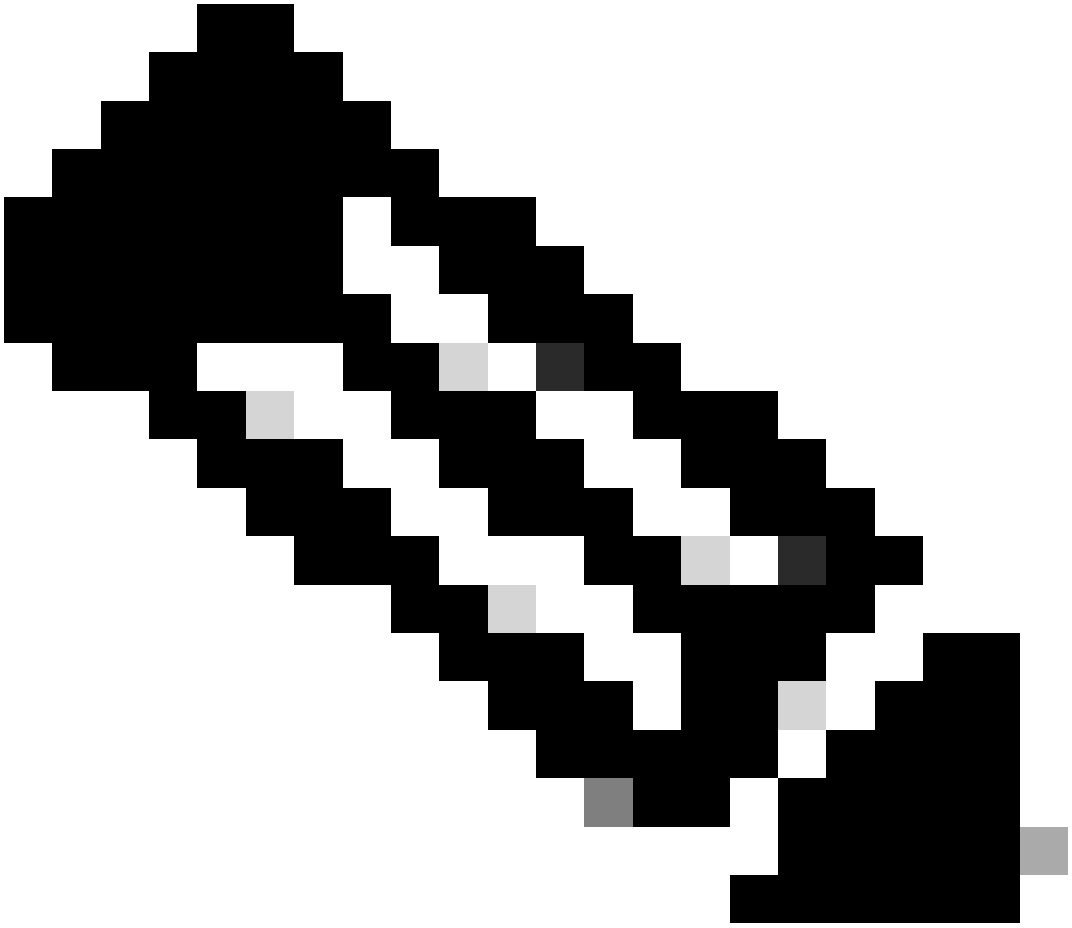
Per abilitare questo servizio, aggiungere il comando threat-detection service invalid-vpn-access nella casella di testo dell'oggetto FlexConfig.

Funzionalità 2: rilevamento minacce per attacchi di inizializzazione client VPN ad accesso remoto

Per abilitare questo servizio, aggiungere il comando threat-detection service remote-access-client-initiations hold-down <minuti> threshold <count> nella casella di testo dell'oggetto FlexConfig, dove:

- hold-down <minuti> definisce il periodo successivo all'ultimo tentativo di avvio durante il quale vengono conteggiati i tentativi di connessione consecutivi. Se il numero di tentativi di connessione consecutivi raggiunge la soglia configurata in questo periodo, l'indirizzo IPv4 dell'autore dell'attacco viene ignorato. È possibile impostare un periodo compreso tra 1 e 1440 minuti.
- threshold <count> è il numero di tentativi di connessione necessari nel periodo di attesa per attivare una deviazione. È possibile impostare un valore di soglia compreso tra 5 e 100.

Ad esempio, se il periodo di attesa è di 10 minuti e la soglia è di 20, l'indirizzo IPv4 viene automaticamente ignorato se vi sono 20 tentativi di connessione consecutivi in un intervallo di 10 minuti.



Nota: quando si impostano i valori di blocco e soglia, tenere in considerazione l'utilizzo NAT. Se si utilizza PAT, che consente molte richieste dallo stesso indirizzo IP, prendere in considerazione valori più alti. In questo modo gli utenti validi avranno tempo sufficiente per connettersi. Ad esempio, in un hotel, numerosi utenti possono tentare di connettersi in breve tempo.

Funzionalità 3: rilevamento minacce per errori di autenticazione VPN ad accesso remoto

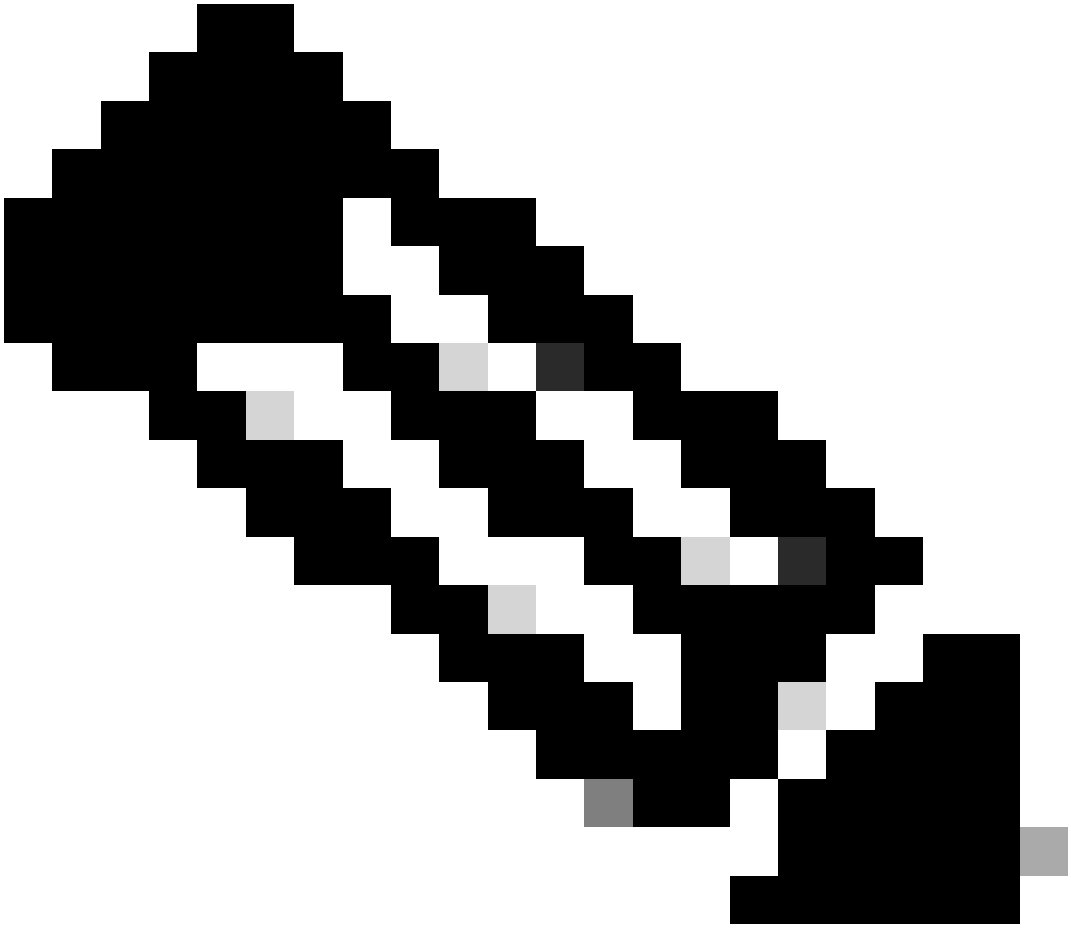
Per abilitare questo servizio, aggiungere il comando threat-detection service remote-access-authentication hold-down<minutes> threshold <count> nella casella di testo dell'oggetto FlexConfig, dove:

- hold-down <minuti> definisce il periodo successivo all'ultimo tentativo non riuscito durante il quale vengono conteggiati gli errori consecutivi. Se il numero di errori di autenticazione consecutivi raggiunge la soglia configurata in questo periodo, l'indirizzo IPv4 dell'autore dell'attacco verrà ignorato. È possibile impostare un periodo compreso tra 1 e 1440 minuti.

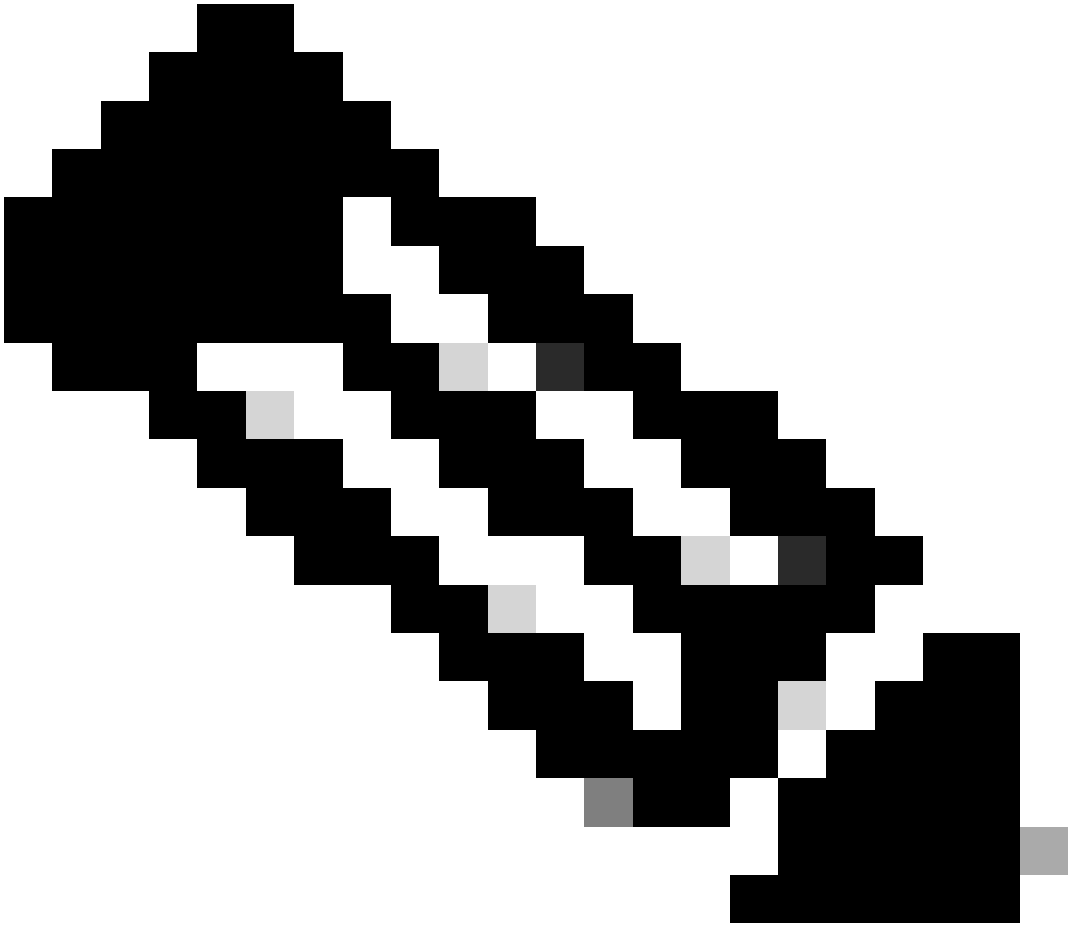
- threshold <count> è il numero di tentativi di autenticazione non riusciti richiesti entro il periodo di attesa per attivare una riattivazione. È possibile impostare un valore di soglia compreso tra 1 e 100.

Ad esempio, se il periodo di attesa è di 10 minuti e la soglia è di 20, l'indirizzo IPv4 viene automaticamente ignorato in caso di 20 errori di autenticazione consecutivi in un intervallo di 10 minuti

---



Nota: quando si impostano i valori di blocco e soglia, tenere in considerazione l'utilizzo NAT. Se si utilizza PAT, che consente molte richieste dallo stesso indirizzo IP, prendere in considerazione valori più alti. In questo modo gli utenti validi avranno tempo sufficiente per connettersi. Ad esempio, in un hotel, numerosi utenti possono tentare di connettersi in breve tempo.

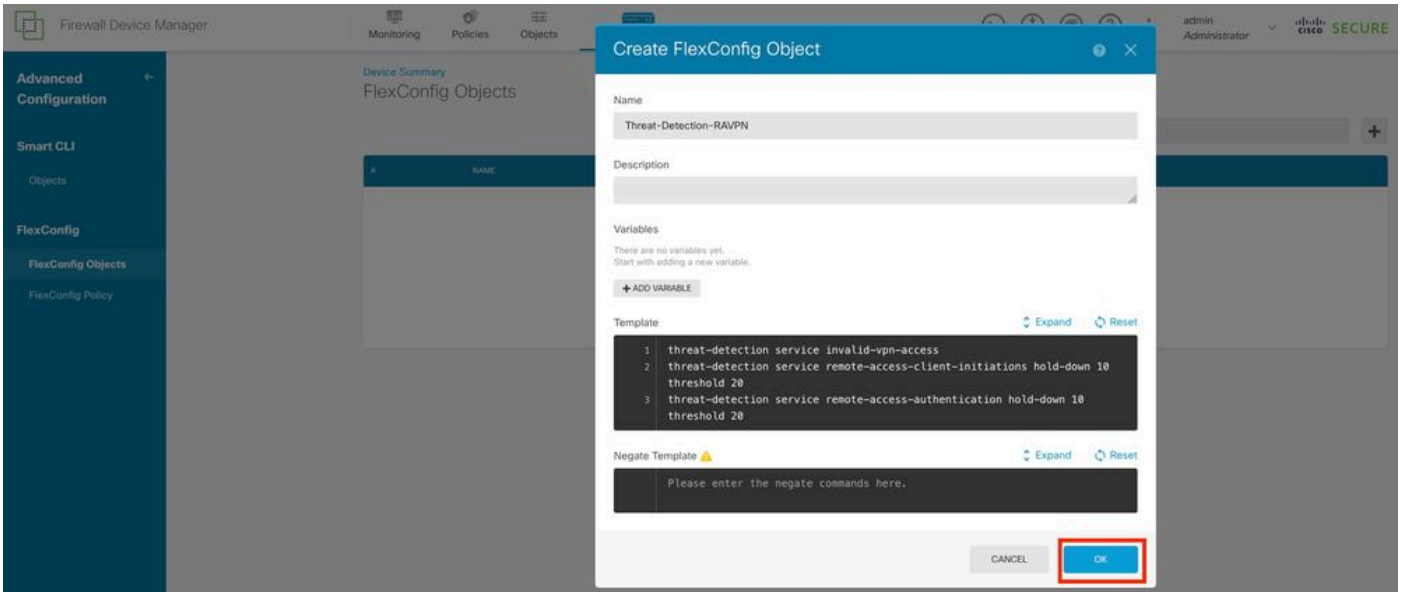


Nota: gli errori di autenticazione tramite SAML non sono ancora supportati.

Questa configurazione di esempio abilita i tre servizi di rilevamento delle minacce disponibili per la VPN ad accesso remoto con un periodo di attesa di 10 minuti e una soglia di 20 per l'avvio del client e i tentativi di autenticazione non riusciti. Configurare i valori di blocco e soglia in base ai requisiti dell'ambiente.

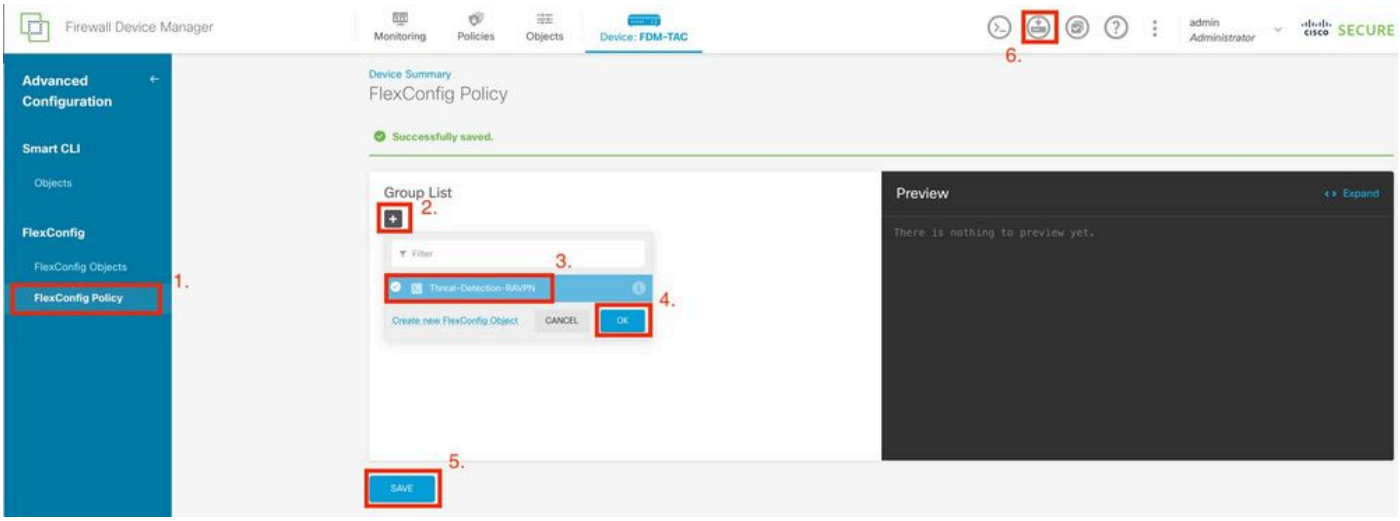
In questo esempio viene utilizzato un singolo oggetto FlexConfig per abilitare le tre funzionalità disponibili.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



Definire i criteri dell'oggetto FlexConfig.

4. Una volta creato l'oggetto FlexConfig, passare a FlexConfig > FlexConfig Policy e individuare il segno più sotto Group List. Selezionare l'oggetto FlexConfig creato per il rilevamento delle minacce RAVPN e fare clic su OK per aggiungere l'oggetto all'elenco dei gruppi. In questo modo viene compilata un'anteprima CLI dei comandi. Esaminare l'anteprima per verificarne la precisione. Selezionare SAVE e distribuire le modifiche in Firepower Threat Defense (FTD).



Modificare il criterio FlexConfig e assegnare l'oggetto FlexConfig.

Verifica

Per visualizzare le statistiche per i servizi RAVPN di rilevamento minacce, accedere alla CLI dell'FTD ed eseguire il comando show threat-detection service [servizio] [voci|dettagli]. Dove il servizio può essere: autenticazione-accesso-remoto, inizializzazione-client-accesso-remoto o accesso-vpn-non valido.

È possibile limitare ulteriormente la vista aggiungendo i seguenti parametri:

- voci: visualizza solo le voci registrate dal servizio di rilevamento delle minacce. Ad esempio, gli indirizzi IP per i quali sono stati eseguiti tentativi di autenticazione non riusciti.
- dettagli: visualizza sia i dettagli che le voci di servizio.

Eseguire il comando show threat-detection service per visualizzare le statistiche di tutti i servizi di rilevamento minacce abilitati.

<#root>

```
FDM-TAC#

show threat-detection service


Service: invalid-vpn-access State : Enabled

    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0

Service: remote-access-authentication State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2

Name: remote-access-client-initiations State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

Per visualizzare ulteriori dettagli sui potenziali attacchi rilevati per il servizio di autenticazione ad accesso remoto, eseguire il comando show threat-detection service <service>.

<#root>

```
FDM-TAC#
```

show threat-detection service remote-access-authentication entries

```
Service:
```

remote-access-authentication

```
    Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Per visualizzare le statistiche generali e i dettagli di un servizio VPN di accesso remoto per il rilevamento delle minacce specifico, eseguire il comando show threat-detection service<service> details.

<#root>

```
FDM-TAC#
```

show threat-detection service remote-access-authentication details

```
Service:
```

remote-access-authentication

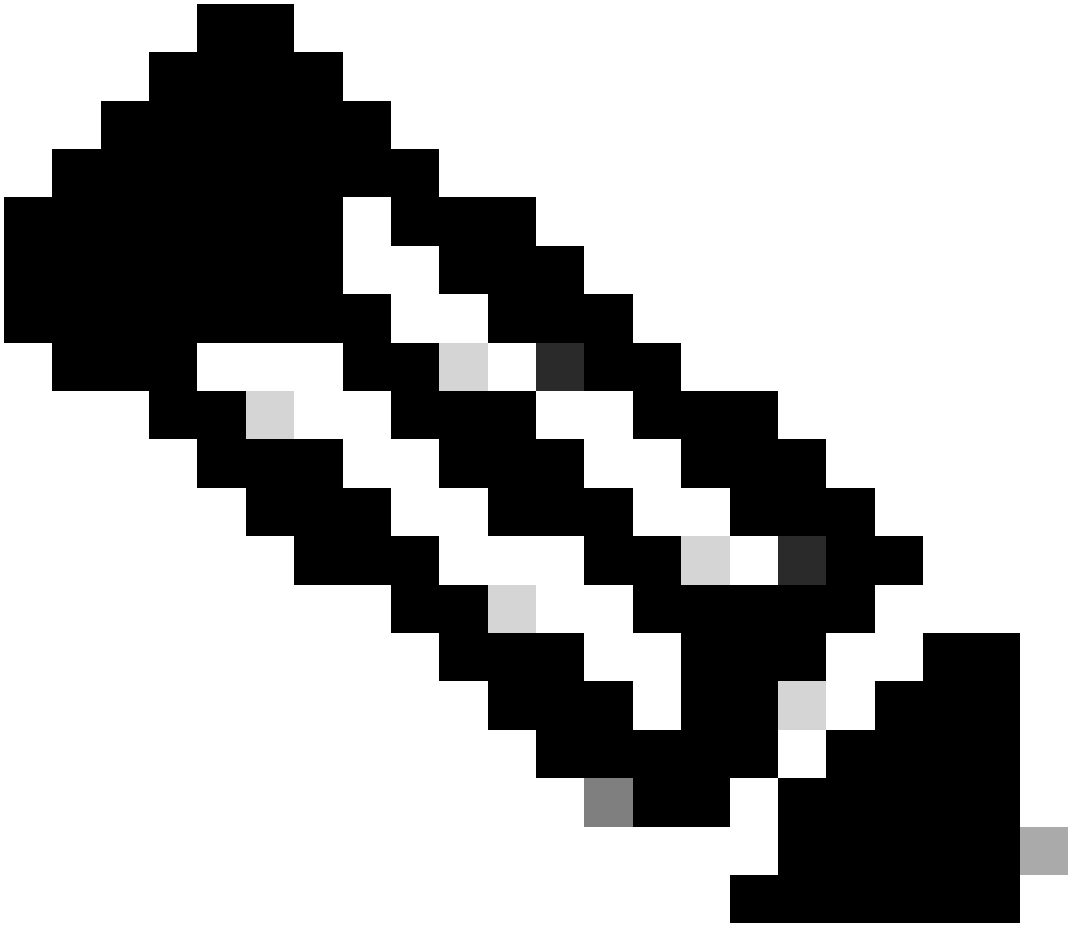
State :

Enabled

```
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```



Nota: le voci visualizzano solo gli indirizzi IP rilevati dal servizio di rilevamento delle minacce. Se un indirizzo IP soddisfa le condizioni da evitare, il numero di blocchi aumenta e l'indirizzo IP non viene più visualizzato come voce.

È inoltre possibile monitorare gli shun applicati dai servizi VPN e rimuovere gli shun per un singolo indirizzo IP o per tutti gli indirizzi IP con i comandi successivi:

- show shun [indirizzo_ip]

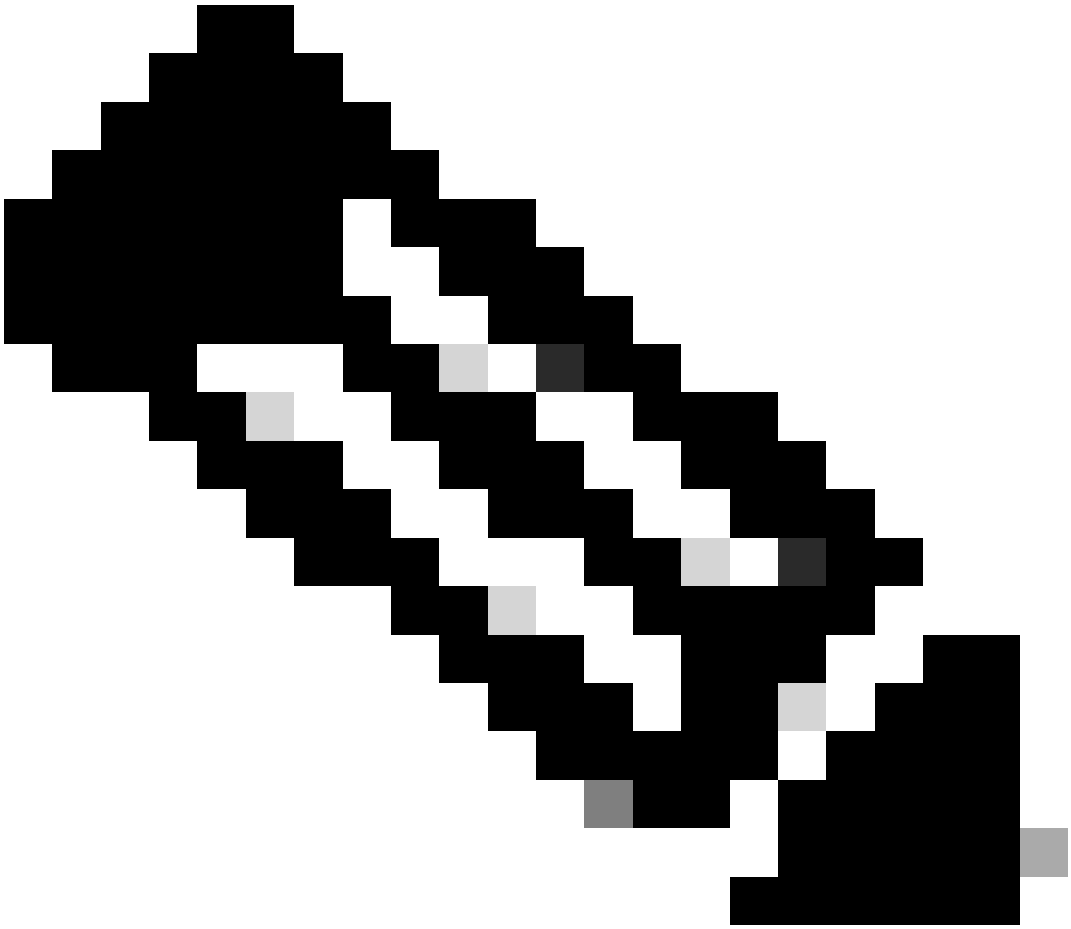
Mostra gli host disattivati, inclusi quelli disattivati automaticamente dal rilevamento delle minacce per i servizi VPN, o manualmente utilizzando il comando shun. Se lo si desidera, è possibile limitare la visualizzazione a un indirizzo IP specificato.

- no shun ip_address [interface if_name]

Rimuove la sequenza solo dall'indirizzo IP specificato. Se si desidera, è possibile specificare il nome dell'interfaccia per lo shun, se l'indirizzo viene ignorato su più interfacce e si desidera lasciare lo shun in posizione su alcune interfacce.

- clear shun

Rimuove la sequenza da tutti gli indirizzi IP e da tutte le interfacce.



Nota: gli indirizzi IP ignorati dal rilevamento delle minacce per i servizi VPN non vengono visualizzati nel comando show threat-detection shun, valido solo per il rilevamento delle minacce di analisi.

Per tutti i dettagli di ciascun output del comando e dei messaggi syslog disponibili relativi ai servizi di rilevamento delle minacce per la VPN ad accesso remoto, consultare il documento di riferimento dei comandi.

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido:Contatti del supporto Cisco internazionali.
- Qui è possibile anche visitare la Cisco VPN Community.

- 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).