Konfigurieren von Bedrohungserkennung für Remotezugriff-VPN-Services im Cisco FirePOWER Gerätemanager

Inhalt

Einleitung

In diesem Dokument wird der Prozess der Konfiguration der Bedrohungserkennung für Remote Access VPN-Services im Cisco FirePOWER Device Manager (FDM) beschrieben.

Voraussetzungen

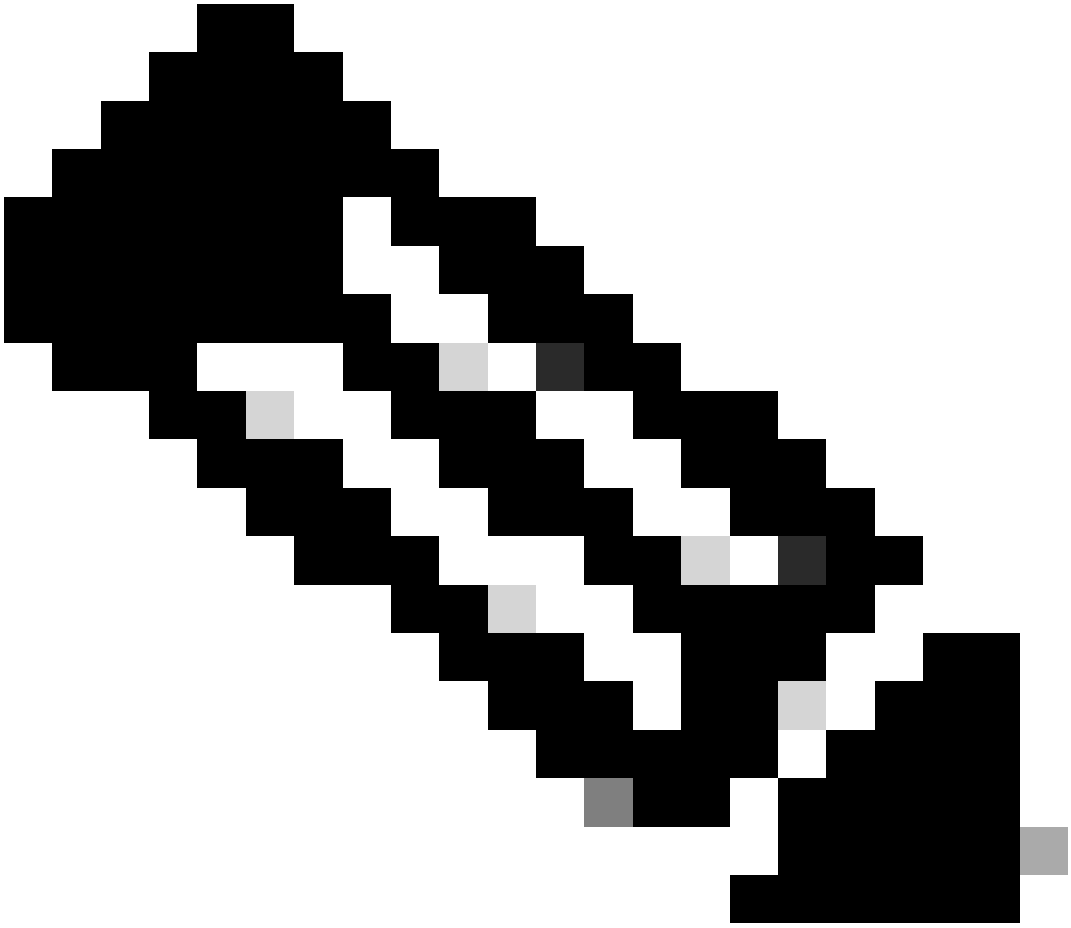
Cisco empfiehlt Ihnen, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco FirePOWER Device Manager (FDM)
- Remote Access VPN (RAVPN) auf FTD

Anforderungen

Diese Funktionen zur Erkennung von Sicherheitsrisiken werden von den nachfolgend aufgeführten Cisco Secure Firewall Threat Defense-Versionen unterstützt:

- Version 7.0 train-> wird von Version 7.0.6.3 und neueren Versionen innerhalb dieses Zuges unterstützt.
- Version 7.2 train-> wird von Version 7.2.9 und neueren Versionen in diesem spezifischen Zug unterstützt.
- Version 7.4 train-> wird von Version 7.4.2.1 und neueren Versionen in diesem spezifischen Zug unterstützt.
- Version 7.6 train-> wird von 7.6.0 und allen neueren Versionen unterstützt.



Hinweis: Diese Funktionen werden derzeit in Version 7.1 oder 7.3 nicht unterstützt.

Verwendete Komponenten

Die in diesem Dokument beschriebenen Informationen basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco Secure Firewall Threat Defense - virtuelle Version 7.4.2.1

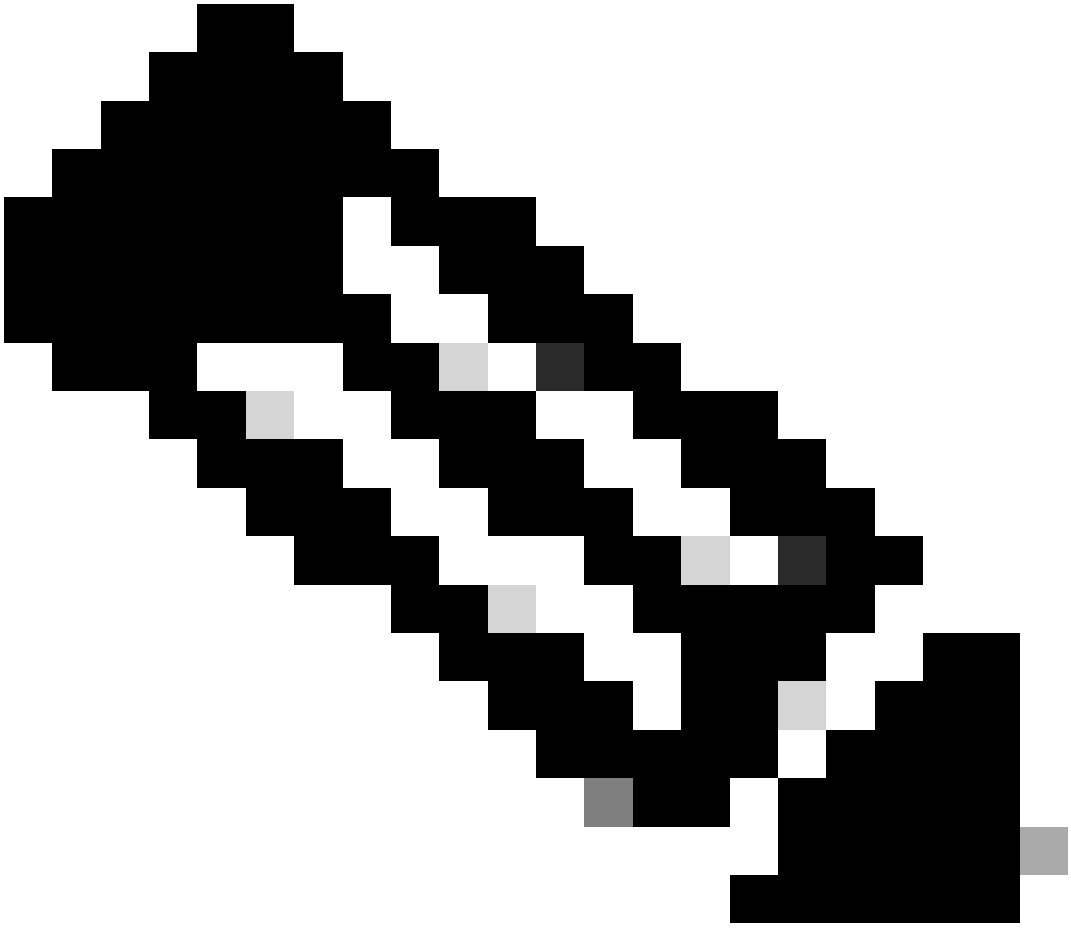
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Funktionen zur Erkennung von Bedrohungen für VPN-Dienste mit Remote-Zugriff tragen dazu bei, Denial-of-Service (DoS)-Angriffe von IPv4-Adressen zu verhindern, indem der Host (die IP-Adresse), der die konfigurierten Schwellenwerte überschreitet, automatisch blockiert wird, um weitere Versuche zu verhindern, bis Sie die Verknüpfung der IP-Adresse manuell entfernen. Für die nächsten Angriffstypen stehen separate Services zur Verfügung:

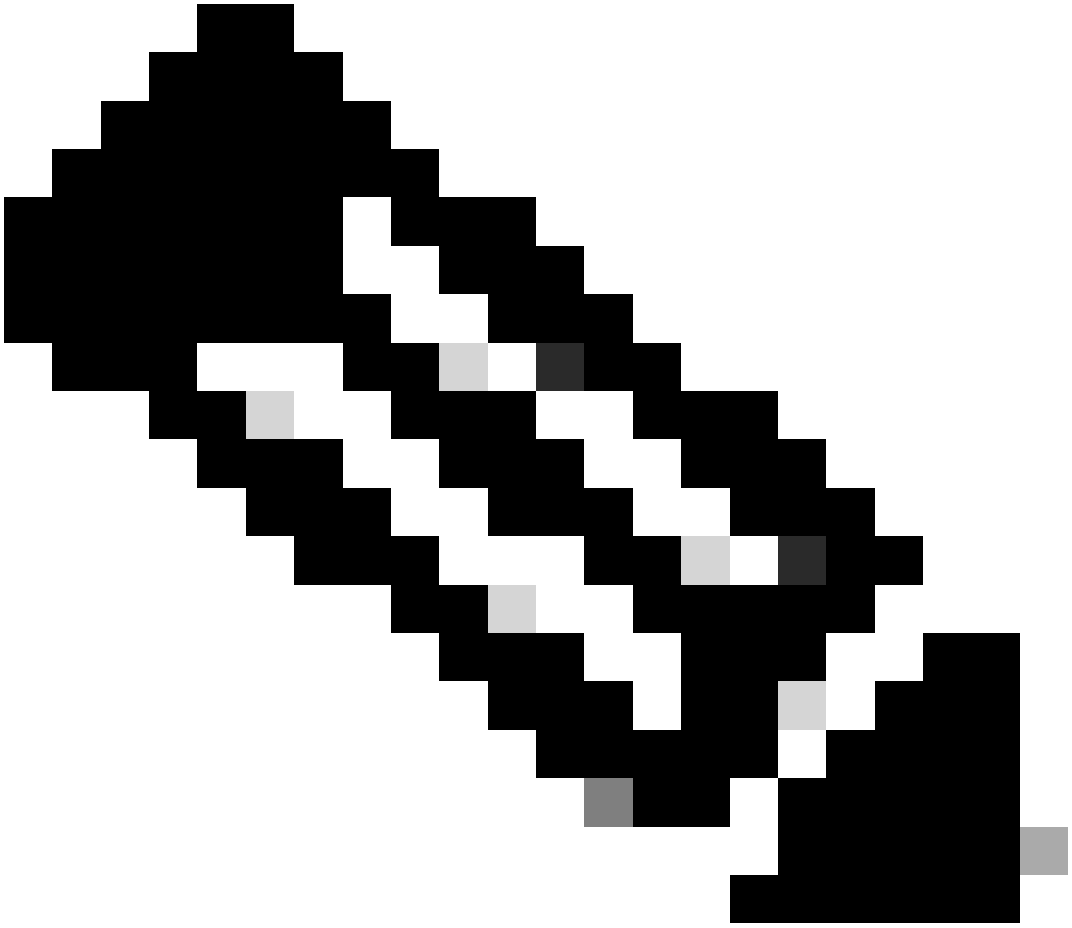
- Wiederholte fehlgeschlagene Authentifizierungsversuche: Wiederholte fehlgeschlagene Authentifizierungsversuche für Remotezugriff-VPN-Dienste (Brute-Force-Angriffe durch Benutzername/Kennwort-Scanning).
- Client-Initiation-Angriffe: Hierbei startet der Angreifer die Verbindung zu einem VPN-Headend für Remote-Zugriff mehrmals von einem Host aus, schließt sie jedoch nicht ab.
- Verbindungsversuche für ungültige Remotezugriff-VPN-Dienste: Wenn Angreifer versuchen, eine Verbindung zu bestimmten integrierten Tunnelgruppen herzustellen, die ausschließlich für den internen Betrieb des Geräts bestimmt sind. Legitime Endpunkte versuchen nicht, eine Verbindung zu diesen Tunnelgruppen herzustellen.

Diese Angriffe können selbst dann, wenn sie keinen Zugriff erhalten, Rechenressourcen belegen und verhindern, dass gültige Benutzer eine Verbindung zu den Remotezugriffs-VPN-Diensten herstellen. Wenn Sie diese Dienste aktivieren, schaltet die Firewall automatisch den Host (die IP-Adresse) ab, der die konfigurierten Schwellenwerte überschreitet. Dies verhindert weitere Versuche, bis Sie die Shun-Anweisung der IP-Adresse manuell entfernen.



Hinweis: Standardmäßig sind alle Dienste zur Erkennung von Sicherheitsrisiken für das Remotezugriffs-VPN deaktiviert.

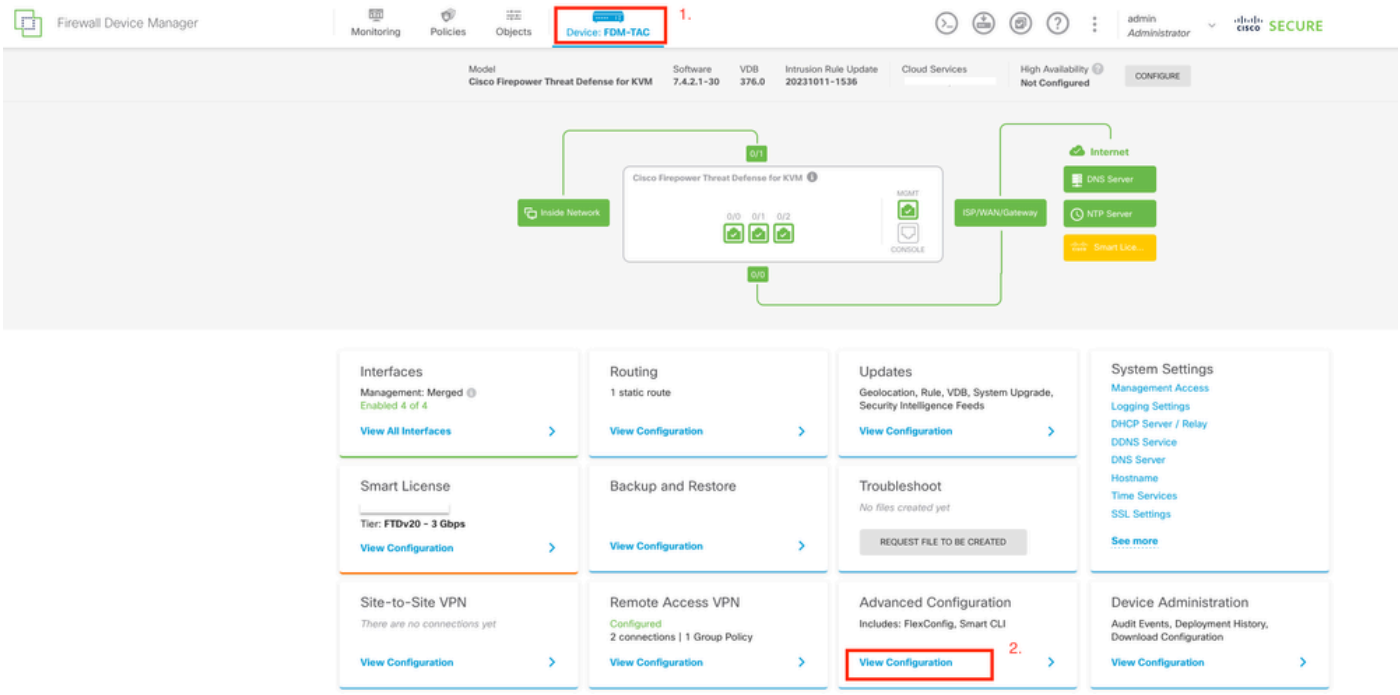
Konfigurieren



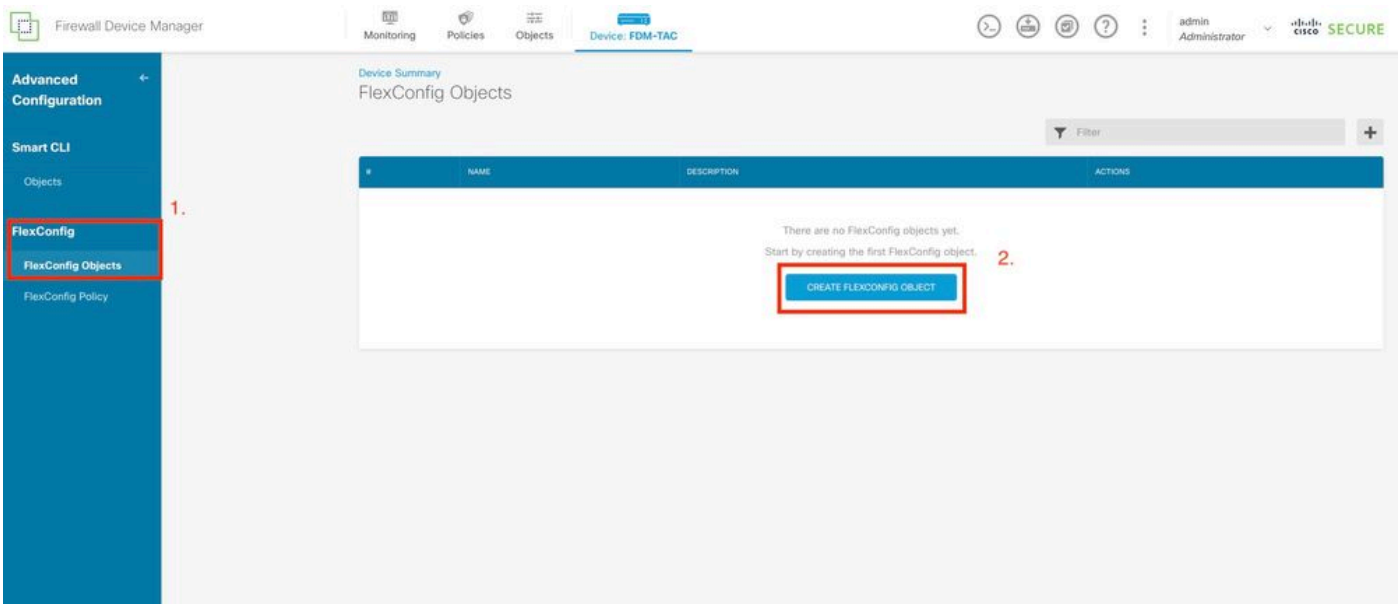
Hinweis: Die Konfiguration dieser Funktionen auf Secure Firewall Threat Defense wird derzeit nur über FlexConfig unterstützt.

1. Melden Sie sich beim Firepower-Geräte-Manager an.

2. Um das FlexConfig-Objekt zu konfigurieren, navigieren Sie zu Device > Advanced Configuration > FlexConfig > FlexConfig Objects, und klicken Sie dann auf Create FlexConfig-Objekt.



Bearbeiten Sie die erweiterte Konfiguration auf der FDM-Startseite.



Erstellen eines FlexConfig-Objekts

3. Fügen Sie nach dem Öffnen des FlexConfig-Objektfensters die erforderliche Konfiguration hinzu, um die Funktionen zur Erkennung von Sicherheitsrisiken für das Remote Access-VPN zu aktivieren:

Funktion 1: Erkennung von Sicherheitsrisiken bei Verbindungsversuchen mit rein internen (ungültigen) VPN-Services

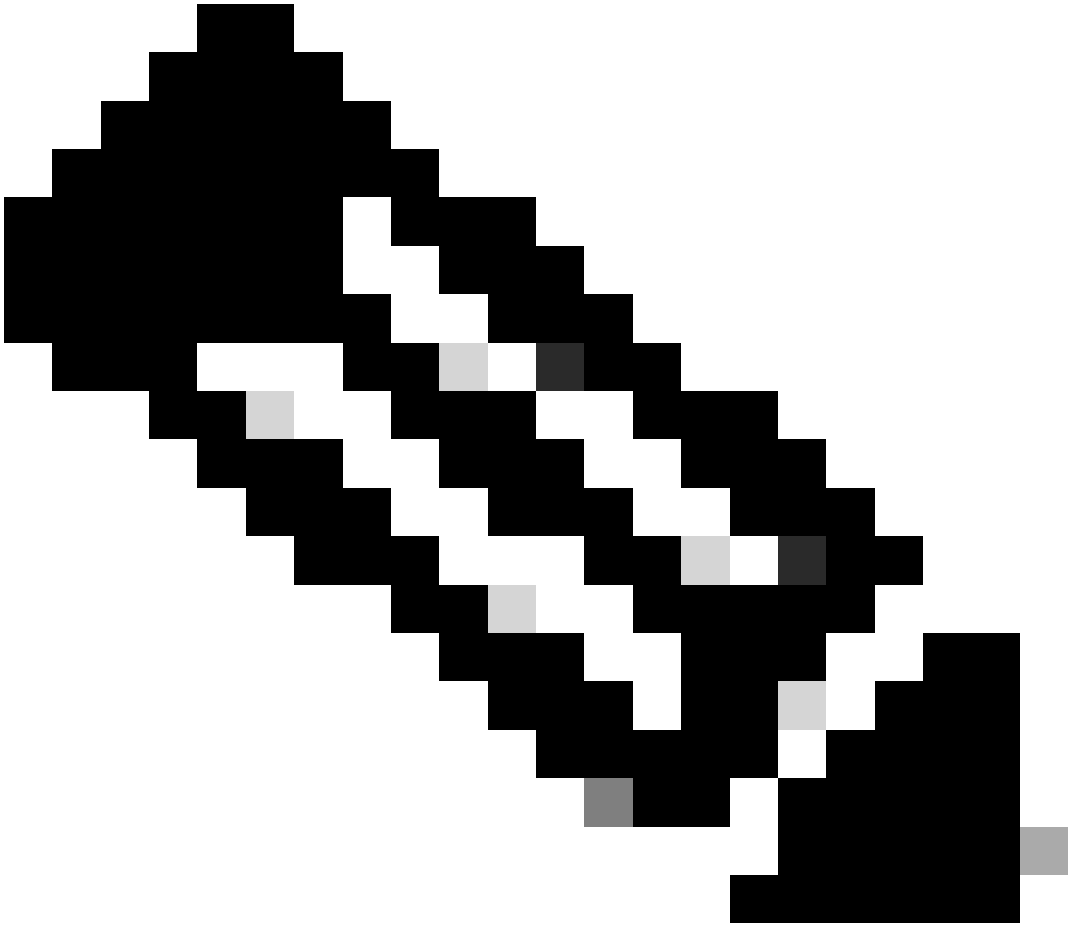
Um diesen Dienst zu aktivieren, fügen Sie den Befehl invalid-vpn-access des Bedrohungserkennungsdiensts in das Textfeld für das FlexConfig-Objekt ein.

Funktion 2: Erkennung von Sicherheitsrisiken bei Angriffen auf VPN-Clients für den Remote-Zugriff

Um diesen Service zu aktivieren, fügen Sie den Befehl service remote-access-client-initiations hold-down <minutes> threshold <count> im Textfeld für das FlexConfig-Objekt hinzu, wobei Folgendes gilt:

- hold-down <Minuten> definiert den Zeitraum nach dem letzten Initiierungsversuch, in dem aufeinander folgende Verbindungsversuche gezählt werden. Wenn die Anzahl der aufeinander folgenden Verbindungsversuche den konfigurierten Grenzwert innerhalb dieses Zeitraums erreicht, wird die IPv4-Adresse des Angreifers ignoriert. Sie können diesen Zeitraum zwischen 1 und 1440 Minuten einstellen.
- threshold <count> ist die Anzahl der Verbindungsversuche, die innerhalb der Haltezeit erforderlich sind, um einen Shun auszulösen. Sie können einen Schwellenwert zwischen 5 und 100 festlegen.

Beträgt die Haltezeit beispielsweise 10 Minuten und der Grenzwert 20 Minuten, wird die IPv4-Adresse automatisch ignoriert, wenn innerhalb von 10 Minuten 20 aufeinander folgende Verbindungsversuche unternommen werden.



Hinweis: Bei der Festlegung der Hold-Down- und Schwellenwerte ist die NAT-Nutzung zu berücksichtigen. Wenn Sie PAT verwenden, wodurch viele Anfragen von derselben IP-Adresse möglich sind, sollten Sie höhere Werte in Betracht ziehen. Dadurch wird sichergestellt, dass gültigen Benutzern genügend Zeit für eine Verbindung zur Verfügung steht. In einem Hotel können beispielsweise zahlreiche Benutzer in kurzer Zeit versuchen, eine Verbindung herzustellen.

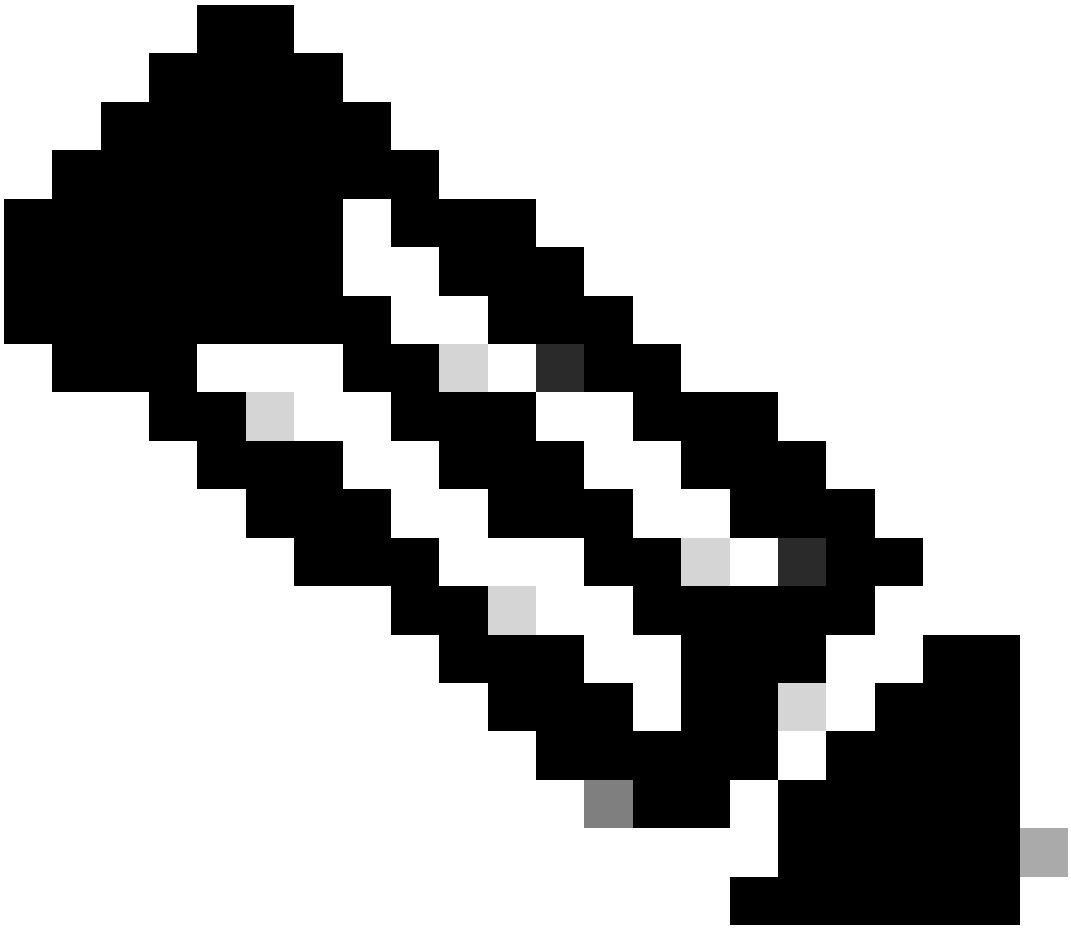
Funktion 3: Erkennung von Sicherheitsrisiken bei VPN-Authentifizierungsfehlern für den Remote-Zugriff

Um diesen Service zu aktivieren, fügen Sie den Befehl service remote-access-authentication hold-down<minutes> threshold <count> im Textfeld für das FlexConfig-Objekt hinzu, wobei Folgendes gilt:

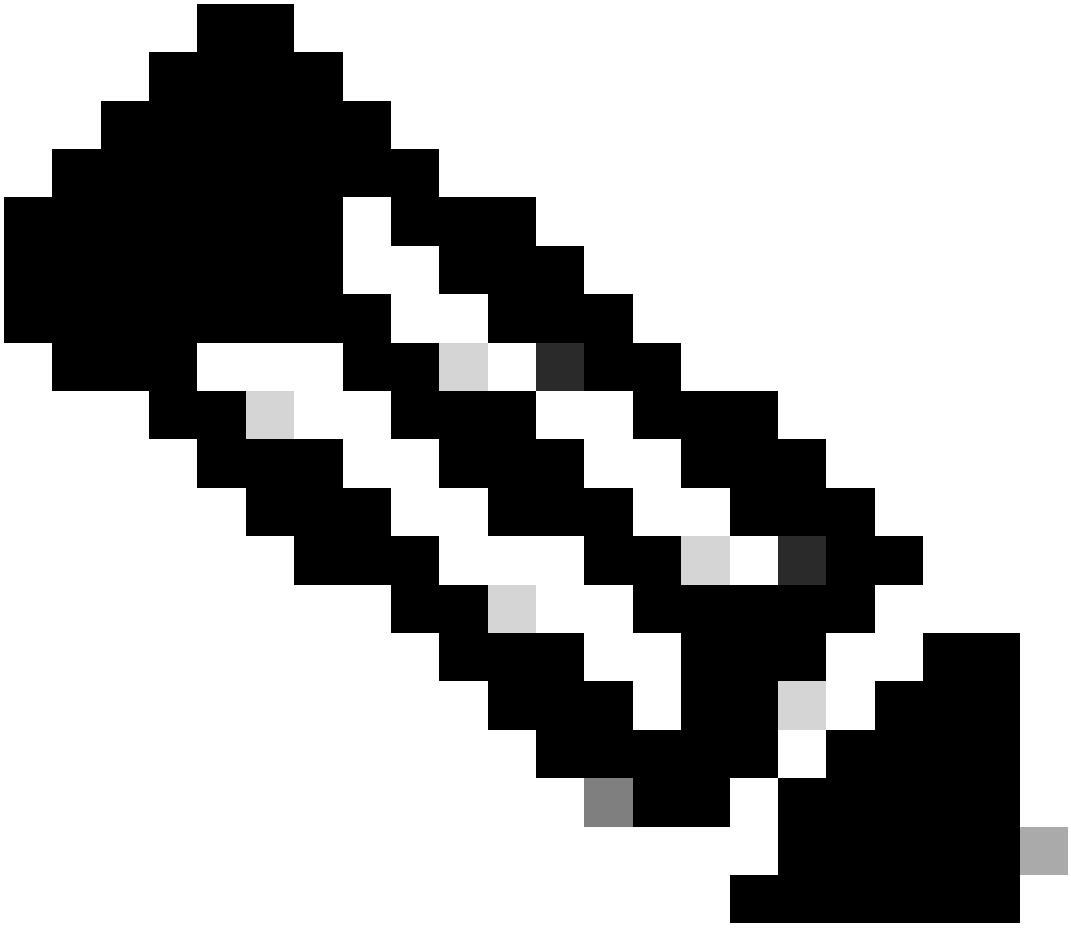
- hold-down <Minuten> definiert den Zeitraum nach dem letzten fehlgeschlagenen Versuch, in dem aufeinander folgende Fehler gezählt werden. Wenn die Anzahl der aufeinander folgenden Authentifizierungsfehler den konfigurierten Grenzwert innerhalb dieses Zeitraums

erreicht, wird die IPv4-Adresse des Angreifers ignoriert. Sie können diesen Zeitraum zwischen 1 und 1440 Minuten einstellen.
- threshold <count> ist die Anzahl der fehlgeschlagenen Authentifizierungsversuche, die innerhalb der Haltezeit erforderlich sind, um einen Shun auszulösen. Sie können einen Schwellenwert zwischen 1 und 100 festlegen.

Beträgt die Haltezeit beispielsweise 10 Minuten und der Schwellenwert 20, wird die IPv4-Adresse automatisch ignoriert, wenn innerhalb von 10 Minuten 20 aufeinander folgende Authentifizierungsfehler auftreten.



Hinweis: Bei der Festlegung der Hold-Down- und Schwellenwerte ist die NAT-Nutzung zu berücksichtigen. Wenn Sie PAT verwenden, wodurch viele Anfragen von derselben IP-Adresse möglich sind, sollten Sie höhere Werte in Betracht ziehen. Dadurch wird sichergestellt, dass gültigen Benutzern genügend Zeit für eine Verbindung zur Verfügung steht. In einem Hotel können beispielsweise zahlreiche Benutzer in kurzer Zeit versuchen, eine Verbindung herzustellen.

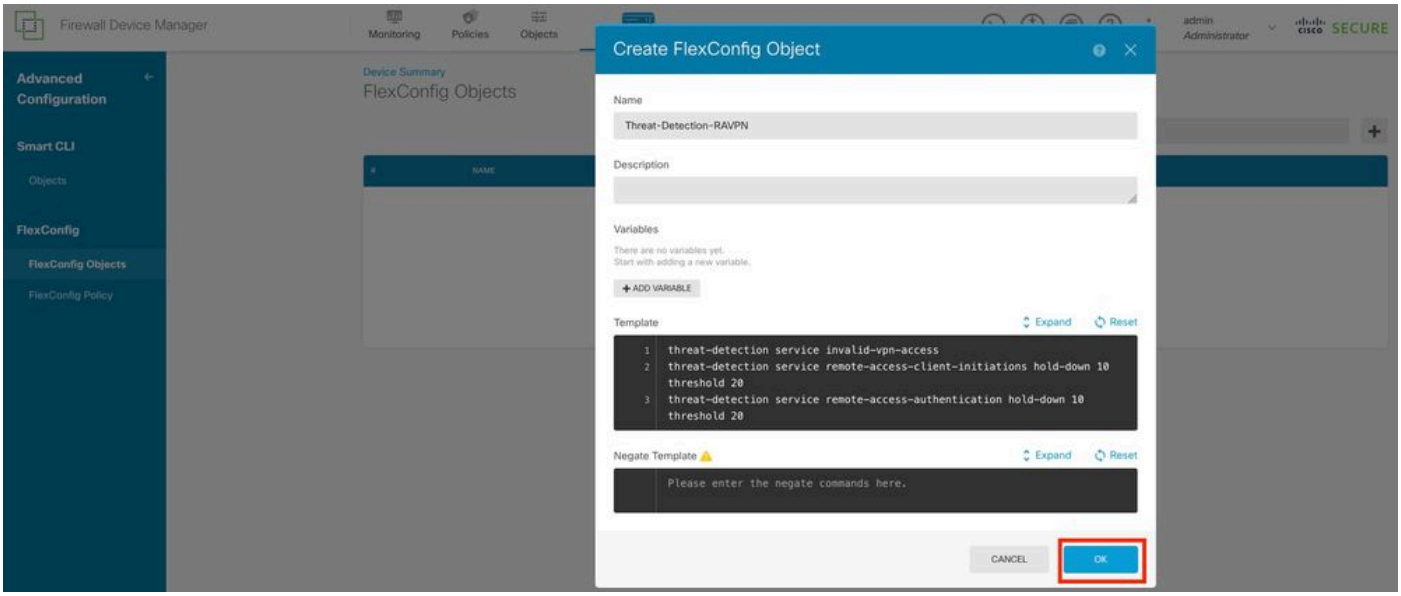


Hinweis: Authentifizierungsfehler über SAML werden noch nicht unterstützt.

Diese Beispielkonfiguration aktiviert die drei verfügbaren Dienste zur Erkennung von Sicherheitsrisiken für das VPN mit Remotezugriff mit einer Haltezeit von 10 Minuten und einem Schwellenwert von 20 für Clientinitiierungsversuche und fehlgeschlagene Authentifizierungsversuche. Konfigurieren Sie die Halte- und Schwellenwerte entsprechend Ihren Anforderungen an die Umgebung.

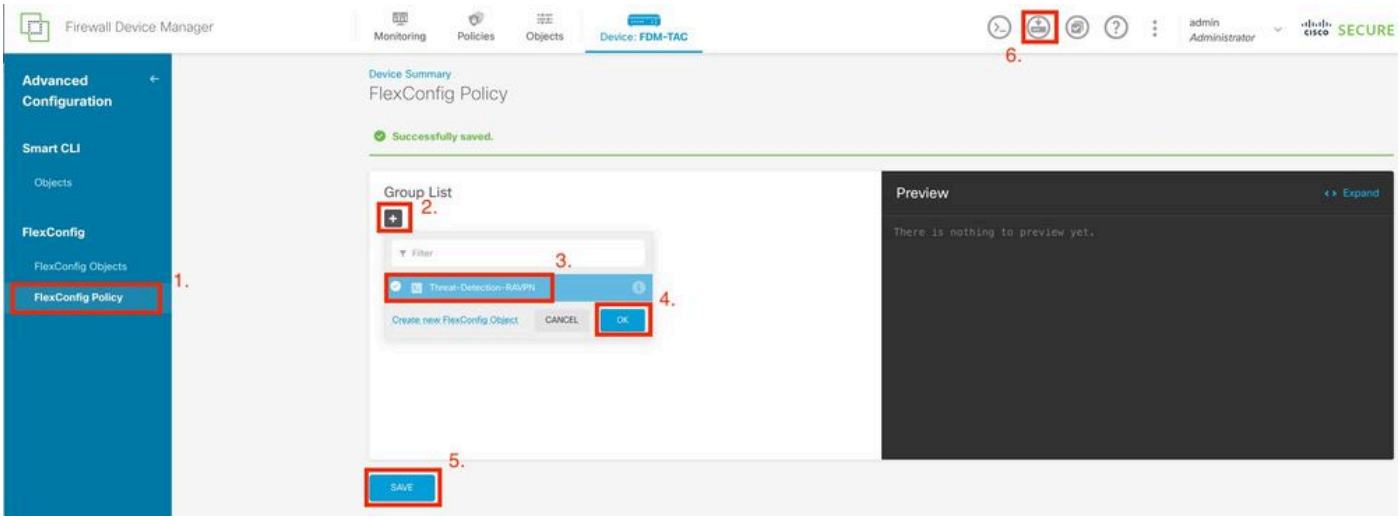
In diesem Beispiel wird ein einzelnes FlexConfig-Objekt verwendet, um die drei verfügbaren Funktionen zu aktivieren.

```
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
```



Definieren Sie die FlexConfig-Objektkriterien.

4. Sobald das FlexConfig-Objekt erstellt wurde, navigieren Sie zu FlexConfig > FlexConfig Policy, und suchen Sie das Pluszeichen unter Group List (Gruppenliste). Wählen Sie das für die RAVPN-Bedrohungserkennung erstellte FlexConfig-Objekt aus, und klicken Sie auf OK, um das Objekt der Gruppenliste hinzuzufügen. Dadurch wird eine CLI-Vorschau der Befehle angezeigt. Überprüfen Sie diese Vorschau, um die Genauigkeit sicherzustellen. Wählen Sie SPEICHERN, und stellen Sie die Änderungen in Firepower Threat Defense (FTD) bereit.



Bearbeiten Sie die FlexConfig-Richtlinie, und weisen Sie das FlexConfig-Objekt zu.

Überprüfung

Um Statistiken für RAVPN-Dienste zur Erkennung von Bedrohungen anzuzeigen, melden Sie sich bei der CLI des FTD an, und führen Sie den Befehl show threat-detection service [service] [entries|details] aus. Dabei kann es sich um folgenden Dienst handeln: remote-access-authentication, remote-access-client-initiations oder invalid-vpn-access.

Sie können die Ansicht weiter einschränken, indem Sie die folgenden Parameter hinzufügen:

- Einträge - Zeigt nur die Einträge an, die vom Bedrohungserkennungsdienst verfolgt werden. Beispielsweise die IP-Adressen, bei denen die Authentifizierung fehlgeschlagen ist.
- details - Zeigt sowohl Servicedetails als auch Serviceeinträge an.

Führen Sie den Befehl show threat-detection service aus, um Statistiken aller aktivierten Dienste zur Erkennung von Bedrohungen anzuzeigen.

<#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
```

Um weitere Details zu potenziellen Angreifern anzuzeigen, die für den Authentifizierungsdienst für den Remote-Zugriff verfolgt werden, führen Sie den Befehl show threat-detection service <service> entries aus.

<#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.
```

Um die allgemeinen Statistiken und Details eines bestimmten Remotezugriffs-VPN-Diensts zur Erkennung von Bedrohungen anzuzeigen, führen Sie den Befehl show threat-detection service <service> details aus.

<#root>

FDM-TAC#

show threat-detection service remote-access-authentication details

Service:

remote-access-authentication

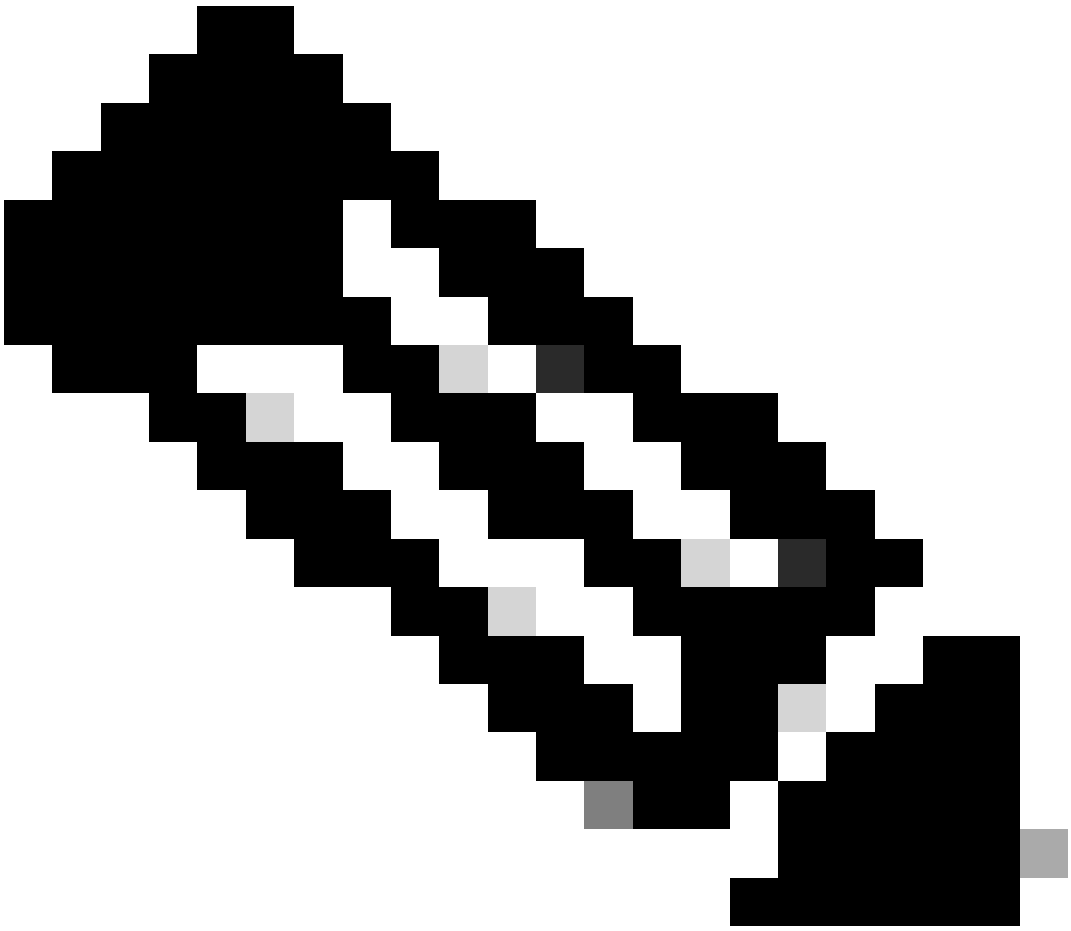
State :

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.
```



Hinweis: In den Einträgen werden nur die IP-Adressen angezeigt, die vom Bedrohungserkennungsdienst verfolgt werden. Wenn eine IP-Adresse die Bedingungen erfüllt, die vermieden werden sollen, erhöht sich die Blockierungsanzahl, und die IP-Adresse wird nicht mehr als Eintrag angezeigt.

Darüber hinaus können Sie Shuns überwachen, die von den VPN-Diensten angewendet werden, und Shuns für eine einzelne IP-Adresse oder alle IP-Adressen entfernen, indem Sie die folgenden Befehle ausführen:

- show shun [ip_address]

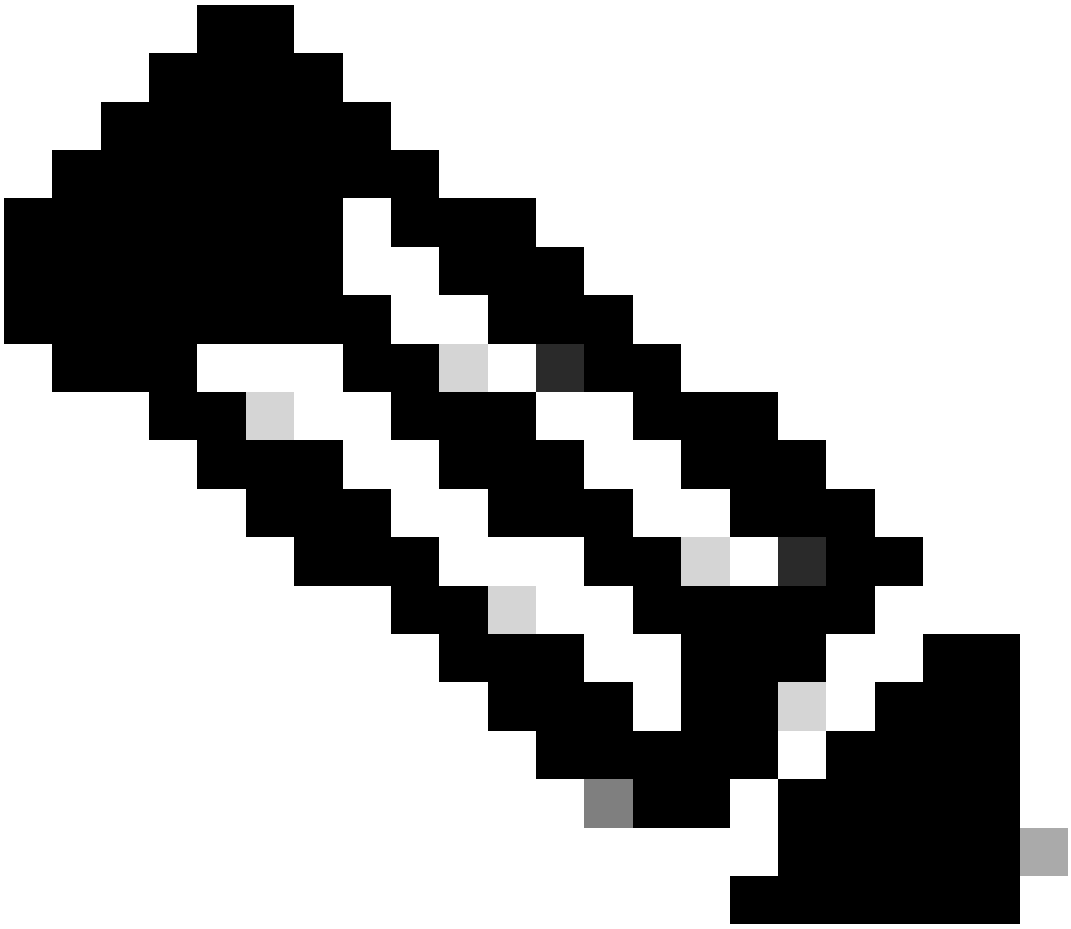
Zeigt nicht autorisierte Hosts an, einschließlich Hosts, die automatisch durch die Erkennung von Sicherheitsrisiken für VPN-Services oder manuell mithilfe des Befehls "shun" ausgeschlossen werden. Optional können Sie die Ansicht auf eine bestimmte IP-Adresse beschränken.

- no shun ip_address [interface if_name]

Entfernt den Shun nur von der angegebenen IP-Adresse. Sie können optional den Schnittstellennamen für die Weiterleitung angeben, wenn die Adresse auf mehr als einer Schnittstelle weitergeleitet wird und Sie die Weiterleitung auf einigen Schnittstellen beibehalten möchten.

- Klarsichtzeichen

Entfernt den Shun von allen IP-Adressen und allen Schnittstellen.



> Hinweis: IP-Adressen, die von der Erkennung von Sicherheitsrisiken für VPN-Services ausgeschlossen wurden, werden nicht im Befehl show threat-detection shun angezeigt, der nur für die Überprüfung der Erkennung von Sicherheitsrisiken gilt.

Weitere Informationen zu den einzelnen Befehlsausgaben und den verfügbaren Syslog-Meldungen zu den Erkennungsdiensten für Remote-Access-VPNs finden Sie im Dokument zur Befehlsreferenz.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Weltweiter Kontakt für den Cisco Support.
- Besuchen Sie auch die Cisco VPN Community hier.
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.