

Configureer bedreigingsdetectie voor VPN-services voor externe toegang op beveiligde firewall-bedreigingsverdediging

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Functie 1: detectie van bedreigingen voor pogingen om verbinding te maken met uitsluitend interne \(ongeldige\) VPN-services](#)

[Functie 2: Threat Detection for Remote Access VPN Client Initiation Attacks](#)

[Functie 3: Bedreigingsdetectie voor fouten in VPN-verificatie van externe toegang](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces van het configureren van bedreigingsdetectie voor Remote Access VPN-services op Cisco Secure Firewall Threat Defence (FTD).

Voorwaarden

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Secure Firewall Threat Defence (FTD).
- Cisco Secure Firewall Management Center (FMC).
- Remote Access VPN (RAVPN) op FTD.

Vereisten

Deze functies voor bedreigingsdetectie worden ondersteund in de volgende versies van Cisco Secure Firewall Threat Defence:

- 7.0 versie trein -> ondersteund in 7.0.6.3

Gebruikte componenten

De informatie die in dit document wordt beschreven, is gebaseerd op deze hardware- en

softwareversies:

- Cisco Secure Firewall Threat Defense virtuele versie 7.0.6.3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Met de functies voor detectie van bedreigingen voor externe VPN-services kunt u beschermen tegen een van de volgende scenario's:

1. Verbinding probeert externe VPN-services ongeldig te maken. Dat wil zeggen, pogingen om verbinding te maken met diensten die alleen bedoeld zijn voor intern gebruik.
2. De initiatie van de cliënt aanvallen, waar de aanvaller begint maar niet de verbindingspogingen aan een verre uiteinde van toegangsVPN voltooit herhaalde tijden van één enkele gastheer.
3. Herhaalde mislukte verificatiepogingen om externe VPN-services te gebruiken (brute-force gebruikersnaam/wachtwoord scannen).

Deze aanvallen, zelfs wanneer zij niet succesvol zijn in hun poging om toegang te krijgen, kunnen computerbronnen verbruiken en voorkomen dat geldige gebruikers verbinding maken met de VPN-services voor externe toegang.

Wanneer u deze services inschakelt, wordt de host (IP-adres) die de ingestelde drempels overschrijdt automatisch door de Secure Firewall omgedraaid om verdere pogingen te voorkomen totdat u het omdraaien van het IP-adres handmatig verwijdert.

 Opmerking: alle services voor bedreigingsdetectie voor externe toegang VPN zijn standaard uitgeschakeld.

Configureren


 Opmerking: de configuratie van deze functies in Secure Firewall Threat Defence wordt momenteel alleen ondersteund via FlexConfig.

1. Log in op het Secure Firewall Management Center.
2. Als u het FlexConfig-object wilt configureren, navigeert u naar Objecten > Objectbeheer > FlexConfig > FlexConfig-object en klikt u vervolgens op Add FlexConfig Object.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects' (highlighted with a red box), and 'Integration'. The 'Objects' tab is active, and the 'Add FlexConfig Object' button is highlighted with a red box. The main content area displays the 'FlexConfig Object' configuration page, which includes a table of objects and a search filter.

3. Zodra het venster Add FlexConfig Object is geopend, voegt u de vereiste configuratie toe om de bedreigingsdetectiefuncties voor Remote Access VPN in te schakelen:

- FlexConfig-objectnaam: activeert-bedreigingsdetectie-omleiding
- FlexConfig-objectbeschrijving: bedreigingsdetectie voor VPN-services voor externe toegang inschakelen.
- Implementatie: eens
- Type: toevoegen.
- Tekstvak: voeg de opdrachten "Threat Detection Service" toe op basis van de beschikbare functies die hieronder worden beschreven.

 **Opmerking:** u kunt de 3 beschikbare bedreigingsdetectiefuncties voor externe toegang VPN inschakelen met hetzelfde FlexConfig-object, of u kunt één FlexConfig-object afzonderlijk maken voor elke functie die wordt ingeschakeld.

Functie 1: detectie van bedreigingen voor pogingen om verbinding te maken met uitsluitend interne (ongeldige) VPN-services


Om deze service in te schakelen, voegt u de opdracht voor de bedreigingsdetectieservice ongeldig-vpn-access toe in het tekstvak van het FlexConfig-object.

Functie 2: Threat Detection for Remote Access VPN Client Initiation Attacks

Om deze service in te schakelen, voegt u de opdracht voor de detectie van bedreigingen op afstand-toegang-client-initiaties ingedrukt <minuten> drempel <count> toe in het tekstvak van FlexConfig-objecten, waarin:

- hold-down <minuten> definieert de periode na de laatste initiatiepoging waarin opeenvolgende verbindingspogingen worden geteld. Als het aantal opeenvolgende verbindingspogingen binnen deze periode de ingestelde drempelwaarde bereikt, wordt het IPv4-adres van de aanvaller gewist. U kunt deze periode instellen op 1 tot 140 minuten.
- drempelwaarde <count> is het aantal verbindingspogingen dat tijdens de onderhoudsperiode is vereist om een melding te activeren. U kunt de drempelwaarde tussen 5 en 100 instellen.

Als de wachttijd bijvoorbeeld 10 minuten is en de drempelwaarde 20 minuten is, wordt het IPv4-adres automatisch geblokkeerd als er 20 opeenvolgende verbindingspogingen zijn binnen een periode van 10 minuten.


 Opmerking: wanneer u de waarden voor hold-down en drempelwaarden instelt, dient u rekening te houden met NAT-gebruik. Als u PAT gebruikt, dat veel verzoeken van hetzelfde IP-adres toestaat, overweeg dan hogere waarden. Dit zorgt ervoor dat geldige gebruikers voldoende tijd hebben om verbinding te maken. Zo kunnen in een hotel talrijke gebruikers proberen in een korte periode verbinding te maken.

Functie 3: Bedreigingsdetectie voor fouten in VPN-verificatie van externe toegang

Om deze service in te schakelen, voegt u de opdracht voor het detecteren van bedreigingen op afstand via externe toegang en verificatie toe `<minuten> <count>` in het tekstvak van FlexConfig-objecten, waarin:

- hold-down `<minuten>` definieert de periode na de laatste mislukte poging tijdens welke opeenvolgende stringen worden geteld. Als het aantal opeenvolgende verificatiefouten binnen deze periode voldoet aan de ingestelde drempel, wordt het IPv4-adres van de aanvaller gewist. U kunt deze periode instellen op 1 tot 140 minuten.
- drempelwaarde `<count>` is het aantal mislukte verificatiepogingen dat tijdens de wachtperiode vereist is om een schuintrekken te activeren. U kunt de drempelwaarde tussen 1 en 100 instellen.

Als de wachttijd bijvoorbeeld 10 minuten is en de drempelwaarde 20 minuten is, wordt het IPv4-adres automatisch geblokkeerd als er 20 opeenvolgende verificatiefouten zijn binnen een periode van 10 minuten.

 Opmerking: wanneer u de waarden voor hold-down en drempelwaarden instelt, dient u rekening te houden met NAT-gebruik. Als u PAT gebruikt, dat veel verzoeken van hetzelfde IP-adres toestaat, overweeg dan hogere waarden. Dit zorgt ervoor dat geldige gebruikers voldoende tijd hebben om verbinding te maken. Zo kunnen in een hotel talrijke gebruikers proberen in een korte periode verbinding te maken.

 Opmerking: verificatiefouten via SAML worden nog niet ondersteund.

Deze voorbeeldconfiguratie maakt de drie beschikbare bedreigingsdetectieservices voor externe toegang tot VPN met een wachttijd van 10 minuten en een drempelwaarde van 20 voor client initiatie en mislukte verificatiepogingen mogelijk. Configureer de waarden voor het vasthouden en de drempelwaarden volgens uw omgevingsvereisten.

In dit voorbeeld wordt één FlexConfig-object gebruikt om de 3 beschikbare functies in te schakelen.

```
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
```

Add FlexConfig Object ?

Name:

Description:

▲ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert 🔗 | Deployment: | Type:

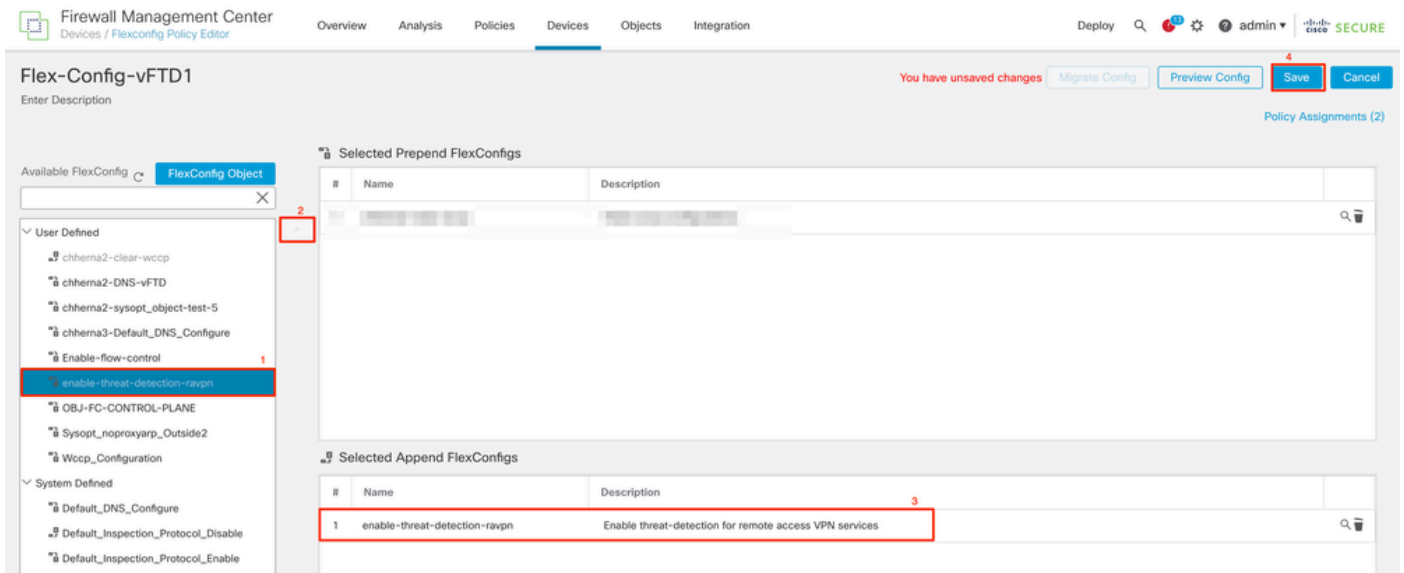
```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

▸ Variables

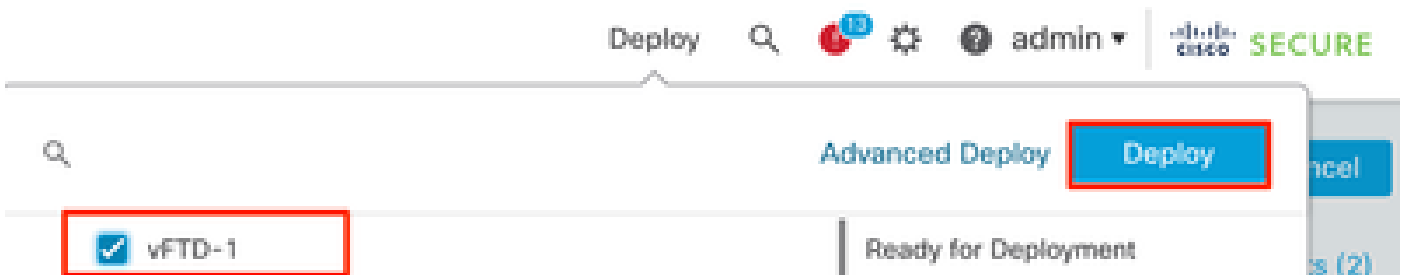
4. Sla het object FlexConfig op.

5. Navigeer naar Apparaten > FlexConfig en selecteer het FlexConfig-beleid dat aan uw beveiligde firewall is toegewezen.

6. Selecteer uit de beschikbare FlexConfig-objecten in het linkerdeelvenster het FlexConfig-object dat u in stap 3 hebt geconfigureerd, klik op ">" en sla de wijzigingen op.



7. Voer de wijzigingen in en controleer deze.



Verifiëren

Om statistieken voor bedreigingsopsporing RAVPN-diensten weer te geven, meldt u zich aan bij de CLI van het FTD en voert u de opdracht `show threat-discovery service [service] [ingangen|details]` uit. Waar de dienst kan zijn: `ver-toegang-authenticatie`, `ver-toegang-cliënt-initiaties`, of `ongeldig-vpn-toegang`.

U kunt de weergave verder beperken door deze parameters toe te voegen:

- `ingangen` — Alleen de ingangen weergeven die door de bedreigingsopsporingdienst worden bijgehouden. Bijvoorbeeld de IP-adressen waar de verificatiepogingen zijn mislukt.
- `details` — Geef zowel de servicedetails als de servicevermeldingen weer.

Draai het bevel van de `show` bedreigingsopsporing om statistieken van alle diensten van de bedreigingsopsporing te tonen die worden toegelaten.

```
<#root>
```

```
ciscoftd# 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

Om meer details van potentiële aanvallers te bekijken die voor de ver-toegang-authenticatie dienst worden gevolgd, stel het bevel van de dienst van de showbedreigingsopsporing <service> ingangen in werking.

```
ciscoftd# 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.


Om de algemene statistieken en de details van een specifieke dienst van VPN van de bedreigingsopsporing de verre toegang in werking te stellen de dienst van de showbedreigingsopsporing <service> detailsbevel.

```
ciscoftd# 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.

 **Opmerking:** de vermeldingen geven alleen de IP-adressen weer die door de bedreigingsdetectiedienst worden bijgehouden. Als een IP-adres aan de voorwaarden om te worden geweerd voldoet, wordt het blokkerende aantal verhoogd en wordt het IP-adres niet langer als invoer weergegeven.

Bovendien kunt u shuns die door de VPN-services worden toegepast, bewaken en shuns voor één IP-adres of alle IP-adressen verwijderen met de volgende opdrachten:

- `toon shun [ip_address]`


Toont geshunde hosts, inclusief de hosts die automatisch worden geshuned door bedreigingsdetectie voor VPN-services, of door handmatig de opdracht `shun` te gebruiken. U kunt de weergave naar keuze beperken tot een bepaald IP-adres.

- `geen shun ip_address [interface if_name]`

Verwijdert de mijden alleen van het opgegeven IP-adres. U kunt de interfacenaam voor de shun naar keuze specificeren, als het adres op meer dan één interface wordt gemeden en u wilt de shun op sommige interfaces op zijn plaats verlaten.

- `clear shun`

Verwijdert de shun van alle IP-adressen en alle interfaces.

 **Opmerking:** IP-adressen die niet worden gedetecteerd door bedreigingsdetectie voor VPN-services, worden niet weergegeven in de opdracht voor detectie van bedreigingen van de `show`, die alleen van toepassing is op detectie van scanbedreigingen.

Raadpleeg het [Command Reference](#) document om alle details van elke opdrachtoutput en beschikbare syslog-berichten met betrekking tot de bedreigingsopsporingsdiensten voor externe toegang VPN te lezen.

Gerelateerde informatie

- Voor extra assistentie kunt u contact opnemen met het Technical Assistance Center (TAC). Er is een geldig ondersteuningscontract vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).
- U kunt [hier](#) ook de Cisco VPN-community bezoeken.
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.