Configure Threat Detection for Remote Access VPN Services on Secure Firewall Threat Defense

Contents

Introduction

This document describes the process of configuring threat detection for Remote Access VPN services on Cisco Secure Firewall Threat Defense (FTD).

Prerequisites

Cisco recommends you to have knowledge of these topics:

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

Requirements

These threat detection features are supported in the Cisco Secure Firewall Threat Defense versions listed next:

- 7.0 version train -> supported in 7.0.6.3

Components Used

The information described in this document is based on these hardware and software versions:

- Cisco Secure Firewall Threat Defense Virtual version 7.0.6.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Threat detection features for remote access VPN services allow you to protect against any of the next scenarios:

1. **Connection attempts to invalidate remote access VPN services.** That is, attempts to connect to services that are intended for internal use only.
2. **Client initiation attacks**, where the attacker starts but does not complete the connection attempts to a remote access VPN headend repeated times from a single host.
3. **Repeated failed authentication attempts to remote access VPN services** (brute-force username/password scanning attacks).

These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and prevent valid users from connecting to the remote access VPN services.

When you enable these services, the Secure Firewall automatically shuns the host (IP address) that exceeds the configured thresholds, to prevent further attempts until you manually remove the shun of the IP address.

Note: All the threat detection services for remote access VPN are disabled by default.

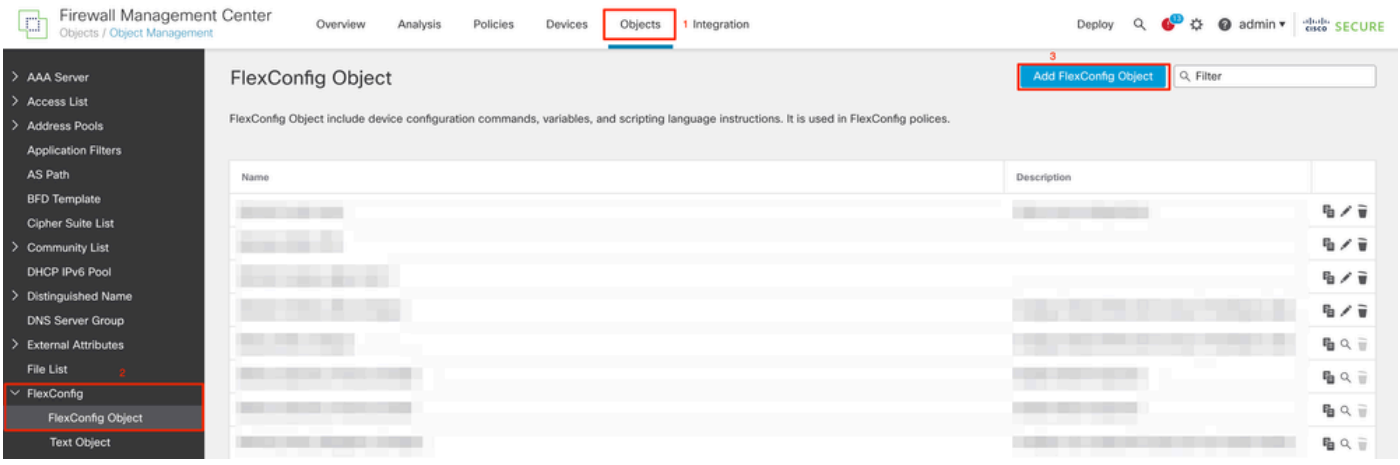
Configure

Note: The configuration of these features on Secure Firewall Threat Defense is currently supported only via FlexConfig.

---

1. Log in to the Secure Firewall Management Center.

2. In order to configure the FlexConfig Object, navigate to **Objects > Object Management > FlexConfig > FlexConfig Object**, then click **Add FlexConfig Object**.



3. Once the **Add FlexConfig Object** window is opened, add the required configuration to enable the threat-detection features for Remote Access VPN:

- **FlexConfig Object Name:** enable-threat-detection-ravpn
- **FlexConfig Object description:** Enable Threat Detection for Remote Access VPN services.

- **Deployment:** Once
- **Type:** Append.
- **Text box:** add the "threat detection service" commands based on the available features described next.

Note: You can enable the 3 available threat-detection features for Remote Access VPN using the same FlexConfig object, or you can create one FlexConfig object individually for each feature to be enabled.

Feature 1: Threat Detection for Attempts to Connect to Internal-Only (Invalid) VPN Services

In order to enable this service, add the **threat detection service invalid-vpn-access** command in the FlexConfig object text box.

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

In order to enable this service, add the **threat detection service remote-access-client-initiations hold-down <*minutes*> threshold <*count*>** command in the FlexConfig object text box, where:

- **hold-down** <minutes> defines the period after the last initiation attempt during which consecutive connection attempts are counted. If the number of consecutive connection attempts meets the configured threshold within this period, the attacker's IPv4 address is shunned. You can set this period between 1 and 1440 minutes.
- **threshold** <count> is the number of connection attempts required within the hold-down period to trigger a shun. You can set the threshold between 5 and 100.

For example, if the hold-down period is 10 minutes and the threshold is 20, the IPv4 address is automatically shunned if there are 20 consecutive connection attempts within any 10-minute span.

Note: When setting the hold-down and threshold values, take NAT usage into account. If you use PAT, which allows many requests from the same IP address, consider higher values. This ensures valid users have enough time to connect. For instance, in a hotel, numerous users can attempt to connect in a short period.

Feature 3: Threat Detection for Remote Access VPN Authentication Failures

In order to enable this service, add the **threat detection service remote-access-authentication hold-down<*minutes*> threshold <*count*>** command in the FlexConfig object text box, where:

- **hold-down** <minutes> defines the period after the last failed attempt during which consecutive failures are counted. If the number of consecutive authentication failures meets the configured threshold within this period, the attacker's IPv4 address is shunned. You can set this period between 1 and 1440 minutes.
- **threshold** <count> is the number of failed authentication attempts required within the hold-down period to trigger a shun. You can set the threshold between 1 and 100.

For example, if the hold-down period is 10 minutes and the threshold is 20, the IPv4 address is automatically shunned if there are 20 consecutive authentication failures within any 10-minute span.

Note: When setting the hold-down and threshold values, take NAT usage into account. If you use

---

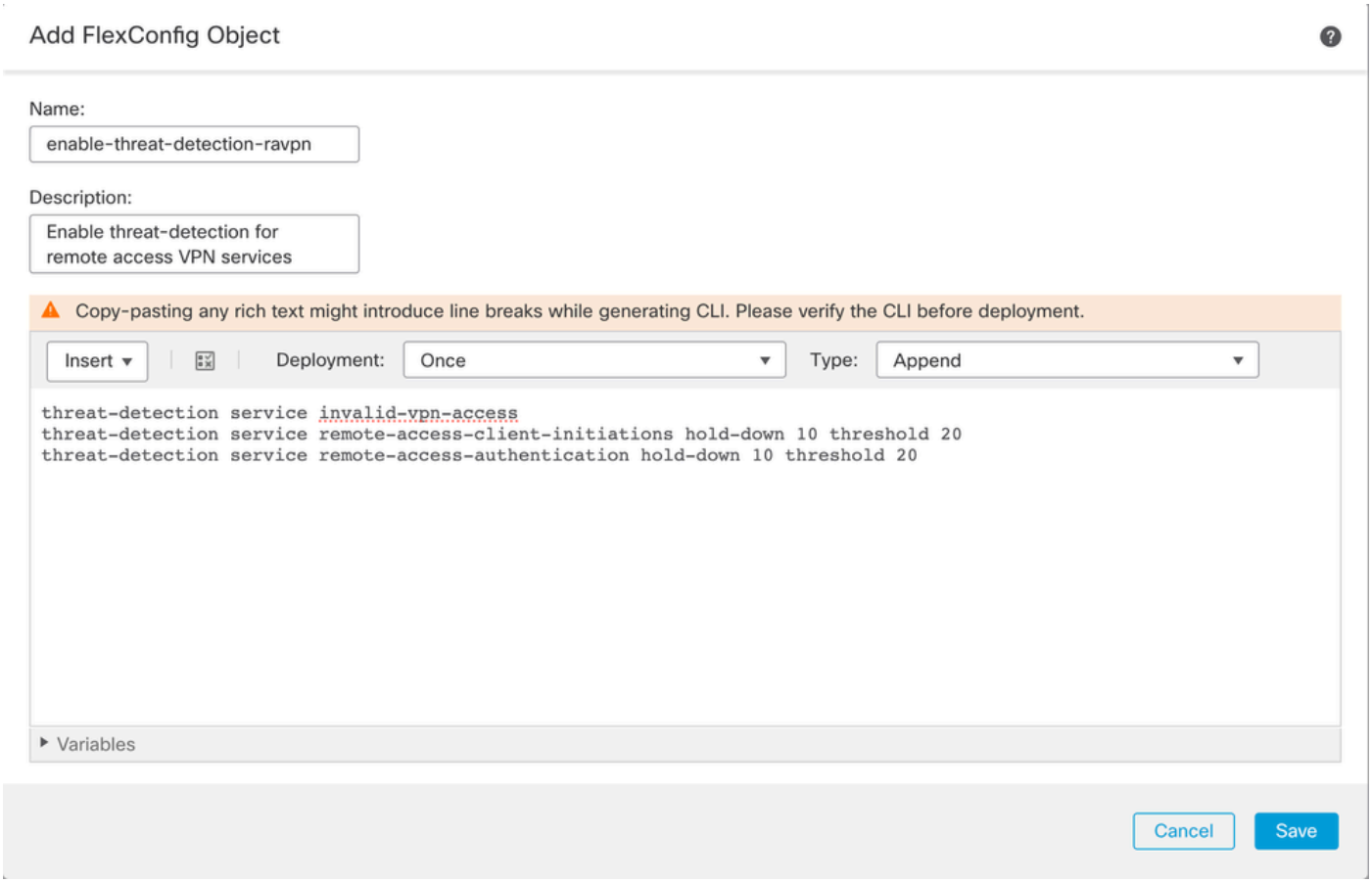
PAT, which allows many requests from the same IP address, consider higher values. This ensures valid users have enough time to connect. For instance, in a hotel, numerous users can attempt to connect in a short period.

Note: Authentication failures via SAML are not supported yet.

This example configuration enables the three available threat detection services for remote access VPN with a hold-down period of 10 minutes and a threshold of 20 for client initiation and failed authentication attempts. Configure the **hold-down** and **threshold** values according to your environment requirements.

This example uses a single FlexConfig object to enable the 3 available features.

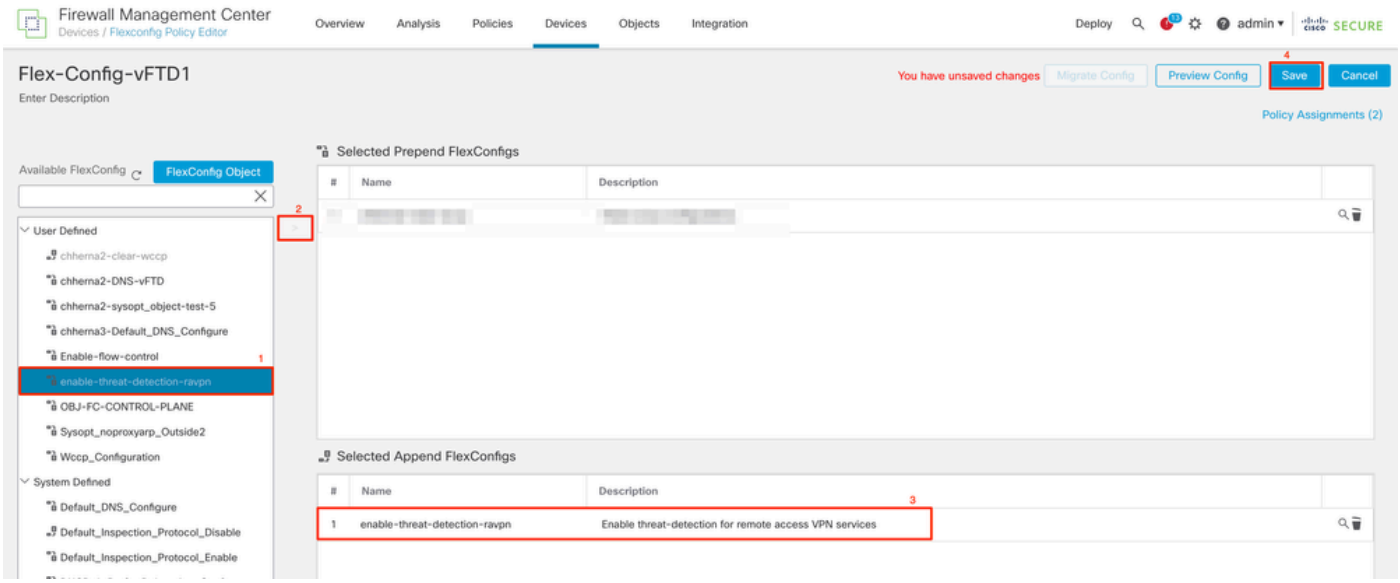
```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



4. Save the FlexConfig Object.

5. Navigate to **Devices > FlexConfig** and select the FlexConfig Policy assigned to your Secure Firewall.

6. From the available FlexConfig Objects displayed on the left pane, **select the FlexConfig object** you configured in step 3, **click** ">", and **save** the changes.



7. Deploy the changes and verify.

Verify

In order to display statistics for threat detection RAVPN services, log in to the CLI of the FTD and run the **show threat-detection service [service] [entries|details]** command. Where the service can be: **remote-access-authentication, remote-access-client-initiations, or invalid-vpn-access**.

You can limit the view further by adding these parameters:

- **entries** — Display only the entries being tracked by the threat detection service. For example, the IP addresses that have had failed authentication attempts.
- **details** — Display both service details and service entries.

Run the **show threat-detection servic**e command to display statistics of all the threat detection services that are enabled.

<#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
```

In order to view more details of potential attackers that are being tracked for the remote-access-authentication service, run the **show threat-detection service <service> entries** command.

```
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.
```

In order to view the general statistics and details of a specific threat detection remote access VPN service run the **show threat-detection service <service> details** command.

```
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.
```

Note: The **entries** display only the IP addresses being tracked by the threat-detection service. If an IP address has met the conditions to be shunned, the **blocking** count increases and the IP address is no longer displayed as an entry.

Additionally, you can monitor shuns applied by the VPN services, and remove shuns for a single IP address or all the IP addresses with the next commands:

- **show shun [*ip_address*]**

Shows shunned hosts, including those shunned automatically by threat detection for VPN services, or manually using the shun command. You can optionally limit the view to a specified IP address.

- **no shun ip_address [interface *if_name*]**

Removes the shun from the specified IP address only. You can optionally specify the interface name for the shun, if the address is shunned on more than one interface and you want to leave the shun in place on some interfaces.

- **clear shun**

Removes the shun from all IP addresses and all interfaces.

Note: IP addresses shunned by threat detection for VPN services do not appear in the **show threat-detection shun** command, which applies to scanning threat detection only.

In order to read all the details for each command output and available syslog messages related to the threat detection services for remote access VPN, please refer to the Command Reference document.

Related Information

- For additional assistance, please contact Technical Assistance Center (TAC). A valid support contract is required:Cisco Worldwide Support Contacts.

- You can also visit the Cisco VPN Community here.
- **Cisco Technical Support & Downloads**