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

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Threat Detection for Attempts to Connect to Internal-Only (Invalid) VPN Services
- Threat Detection for Remote Access VPN Client Initiation Attacks
- Threat Detection for Remote Access VPN Authentication Failures

Verify

Related Information

Introduction

This document describes the process of configuring threat detection capabilities for Remote Access VPN on Cisco Secure Firewall ASA.

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Remote Access VPN (RAVPN) on ASA

These threat detection features are supported in the next Cisco Secure Firewall ASA versions:

- 9.16 version train > supported from 9.16(4)67 and newer versions within this specific train.
- 9.17 version train > supported from 9.17(1)45 and newer versions within this specific train.
- 9.18 version train > supported from 9.18(4)40 and newer versions within this specific train.
- 9.19 version train > supported from 9.19(1).37 and newer versions within this specific train.
- 9.20 version train > supported from 9.20(3) and newer versions within this specific train.

- 9.22 version train > supported from 9.22(1.1) and any newer versions.

Note: 9.22(1) was not released. The first release was 9.22(1.1).

Components Used

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

- Cisco Secure Firewall ASA version 9.20(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 help prevent Denial of Service (DoS) attacks from IPv4 addresses by automatically blocking the host (IP address) that exceeds the configured thresholds, to prevent further attempts until you manually remove the shun of the IP address. There are separate services available for the next types of attack:

- Repeated failed authentication attempts to remote access VPN services (brute-force username/password scanning attacks).
- 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.
- Connection attempts to invalid remote access VPN services. That is, when attackers try to connect to specific built-in tunnel groups intended solely for the internal functioning of the device. Legitimate endpoints can never attempt to connect to these tunnel groups.

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

Log in to the **Secure Firewall Command Line Interface (CLI)** in global configuration mode and enable one or more of the available threat detection services for remote access VPN:

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

To enable this service, run the **threat-detection service invalid-vpn-access** command.

Threat Detection for Remote Access VPN Client Initiation Attacks

To enable this service, run the **threat-detection service remote-access-client-initiations hold-down <minutes> threshold <count>** command, 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.

Threat Detection for Remote Access VPN Authentication Failures

To enable this service, run the **threat-detection service remote-access-authentication hold-down<minutes> threshold <count>** command, 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.

The next 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.

```
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
```

Verify

To display statistics for threat detection RAVPN services, 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.

```
ciscoasa# 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
```

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.

```
ciscoasa# 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.
```

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.

```
ciscoasa# 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 a shun applied to the specified IP address.

If an IP address is shunned on multiple interfaces and no specific interface is mentioned, the command removes the shun from only one interface. The selection of this interface is based on a route lookup for the shunned IP address. To remove the shun from additional interfaces, you must explicitly specify the interface.

- **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.

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 Cisco Secure Firewall ASA Firewall CLI Configuration Guide, 9.20. Chapter: Threat Detection 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 Communityhere.