Configure Branch Threat Defense

Overview of Cisco Branch Threat Defense

Cisco Branch Threat Defense is a router security technology that strengthens protection and saves time and money without having to deploy multiple-point security products. This technology mitigates security vulnerabilities in branch offices with direct Internet connections that bypass your data center, and encrypt communication between enterprise branches, headquarters, and data centers. See Cisco Branch Threat Defense Guide.

You can use to configure Branch Threat Defense starting from Regulatory Compliance use cases, and configure the technologies such as Zone-Based Firewall (ZBFW), Snort Intrusion Prevention System (IPS), Cloud Web Security (CWS) and OpenDNS.

Related Topics

Supported IOS-XE Platforms, on page 1

Supported IOS-XE Versions, on page 1

Prerequisites for Enabling Branch Threat Defense, on page 2

Use the Branch Threat Defense Wizard, on page 2

Supported IOS-XE Platforms

The Branch Threat Defense functionality is supported on Cisco 4000 series Integrated Services Routers (ISR).

Supported IOS-XE Versions

The Branch Threat Defense functionality is available in Cisco IOS-XE Release 15.5(3)S1 (16.3.1 when OpenDNS is configured) and later releases.

Prerequisites for Enabling Branch Threat Defense

- This feature is available only in Security Packages which require a security license. Contact Cisco Support to obtain the license.
- Ensure that the Cisco 4000 series ISR has at least 8 GB of RAM. For more information, see the section "Virtual Service Resource Profile" in the Security Configuration Guide for Branch Threat Defense.
- Each router to be provisioned should already have a Snort IPS OVA present in the same location on its file-system. Use the "Copy OVA to Device" CLI template to distribute a Snort IPS OVA to each device to be provisioned before proceeding.

Related Topics

Use the Branch Threat Defense Wizard

Step 1   Choose Services > Network Services > Branch Threat Defense.

Step 2   Click Next to choose the configuration.

Step 3   Read the description in the Choose Configuration page and choose the required use case from the Select a Use Case drop-down list.

The configuration options vary according to the selected use case.

Step 4   Choose the required configuration options and click Next.

Step 5   Choose the devices you want to configure and click Next.

Step 6   Enter the configuration values or use the import/export icon to configure the ZBFW, Snort IPS CLI, CWS and OpenDNS depending on the chosen use case.

Step 7   Click Apply and click Next to goto CLI Summary tab where you can confirm the device and template configuration values.

Step 8   Schedule the deployment job using Prepare and Schedule tab.

Step 9   Click Next and click Deploy in the Confirmation tab to deploy the Branch Threat Defense.

Step 10   Click Job Status to view the job details in the Job Dashboard.

Related Topics