Cisco Firepower Threat Defense for ISRs

Q. What is Cisco Firepower™ Threat Defense for ISRs?

A. Cisco Firepower Threat Defense for ISRs extends industry-leading Cisco® threat protection beyond the network edge and data center to an additional platform in branch offices: the Cisco Integrated Services Router (ISR).

Q. Why would I want or need it?

A. You can now capitalize on the cost savings and improved user experiences of direct Internet access (DIA) in branch sites while better protecting devices and hosts, wherever they reside, against advanced threats.

Q. What are the elements of Cisco Firepower Threat Defense for ISR?

A. There are five components:

- **Firepower Next-Generation Intrusion Prevention System (NGIPS)** sets the standard in advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and industry-leading threat prevention effectiveness.
- **Application Visibility and Control (AVC)** reduces the potential surface area of attacks through detailed control of thousands of applications and by enforcing mobile app, social media app, and acceptable-use policies.
- **Advanced Malware Protection (AMP)** for Networks protects against highly sophisticated, targeted, zero-day attacks, and advanced persistent malware threats. It continuously analyzes files and network traffic for threats that evade first lines of defense, provides deep visibility into the activity and behavior of a threat, and then lets you quickly scope the impact of an active attack and contain it with a few clicks.
- **Reputation-based URL Filtering** mitigates sophisticated client-side attacks - and improves employee productivity - by controlling access to more than 280 million URLs in more than 80 categories and reducing the risk from suspicious or unacceptable domains.
- **Cisco Firepower Management Center** is the centralized point for event and policy management for all of the Firepower Threat Defense for ISR components. It provides visibility into everything on the customer's network: physical and virtual hosts, operating systems, applications, services, protocols, users, geolocation information, content, network behavior, network attacks, and malware. It also reduces customer costs by streamlining operations and automating many recurring security analysis and management tasks.

Q. Which ISR models can run Firepower Threat Defense?

A. The capability is available on both the ISR G2 and ISR 4000 Series platforms. Specifically:

- Cisco ISR G2 Series
  - 1921 ISR
  - 1941 ISR
  - 2901 ISR
  - 2911 ISR
  - 2921 ISR

    - 2951 ISR
    - 3925 ISR
    - 3945 ISR
    - 3925E ISR
    - 3945E ISR
  - Cisco ISR 4000 Series
    - 4321 ISR
    - 4331 ISR
    - 4351 ISR
    - 4431 ISR
    - 4451 ISR

Q. How is Cisco Firepower Threat Defense for ISR managed?

A. It is managed centrally through the Firepower Management Center. The management center is available in both appliance and virtual form factors.

Q. Can the management center simultaneously manage Firepower NGIPS appliances, the threat-defense functions of Cisco ASA with Firepower Services (Cisco's next-generation firewall), and Cisco Firepower Threat Defense for ISR?

A. Yes. Up to 300 Firepower sensors (both virtual and physical) can be managed by a single management center instance.

Q. If the Firepower Management Center does not have Internet access, can signature updates be uploaded offline by removable media such as flash drives and CD-ROMs?

A. Yes. Product updates are available on our Software Download page.

Q. For what situations is Cisco Firepower Threat Defense for ISR well suited?

A. It's particularly valuable to organizations with distributed branch offices or retail stores, where cloud applications, video, and bring-your-own-device (BYOD) policies are driving up bandwidth requirements and costs. Because of these increases, distributed enterprises face pressure from their branch offices for direct Internet access (DIA), an alternative to backhauling traffic through the data center. DIA provides cost savings but forfeits the inherent enterprise-level threat protection the data center provides. Cisco Firepower Threat Defense for ISR fixes that issue.

Q. When should I deploy integrated threat defense capabilities in a router as opposed to a firewall? When should I deploy them in both?

A. When all traffic from the branch will be backhauled to the data center for inspection and content filtering using a secure tunnel, a stateful firewall will meet the security requirements. If the branch's traffic goes onto the Internet directly, then you need both stateful firewall and Firepower Threat Defense for ISR capabilities.

Q. How can Firepower Threat Defense for ISR be deployed to inspect traffic from wireless devices?

A. Firepower Threat Defense for ISR should be deployed just past the wireless network termination point. For added threat protection, there is a Cisco AMP for Endpoints version for mobile devices. Alerts from AMP for Endpoints are sent into the Firepower Management Center as well.

Q. Where can I find technical configuration information about Cisco Firepower Threat Defense for ISR?

A. While the following link does not yet include the “Cisco Firepower Threat Defense for ISR” branding, you can find more technical information here.

Q. How do I order Cisco Firepower Threat Defense for ISR?

A. Contact your Cisco account representative or Cisco partner representative, and they will be able to help you.

Q. Where can I go for more information on Firepower Threat Defense for ISR?

A. You can get more information for this specific product here, and you can get more detailed information on the Firepower Threat Defense solution here.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C67-734837-01 05/17