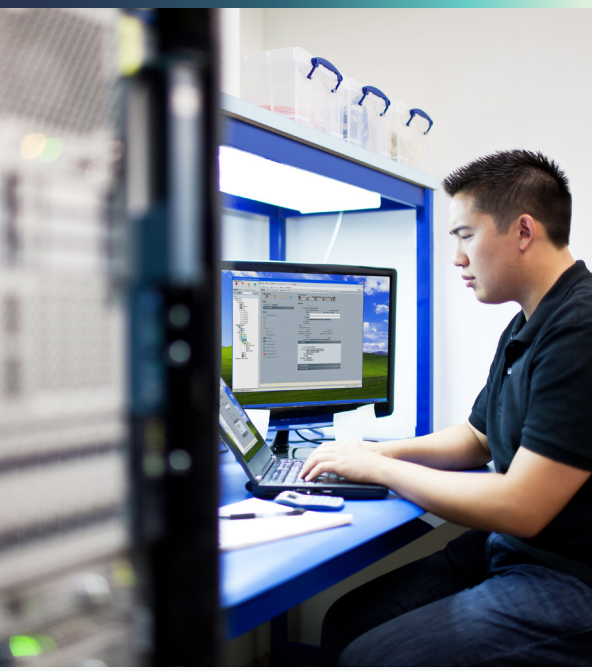
At-a-Glance



Cisco FirePOWER Threat Defense for ISR

Secure Your Branch and Remote Offices

Enterprise-level risks in today's branch offices require enterprise-level security. While you deal with BYOD, compliance requirements, and the increasing use of direct Internet access (DIA) in your distributed sites, you also have to defend them against advanced persistent threats.

You can do that by using Cisco's industry-leading threat protection capabilities, which now run on an additional platform: Cisco Integrated Services Routers (ISRs). Cisco FirePOWER Threat Defense for ISR extends enterprise-level threat protection beyond traditional network edge and data center deployments to help protect your DIA traffic.

Now you can capitalize on the cost savings and improved user experiences of branch DIA, while better protecting devices and hosts against advanced threats wherever they reside: in branches, partner locations, and other remote sites.

Aim for 'Security Everywhere'

Cisco FirePOWER Threat Defense for ISR is a component of the Cisco "security everywhere" strategy. The goal is to give you the continuous visibility and control you need to defeat advanced threats across your environment. A integrated set of security features work together to help keep your remote operations secure:

- **FirePOWER Next-Generation Intrusion Prevention System (NGIPS)** sets the standard for advanced threat protection, integrating real-time contextual awareness, intelligent security automation, and industryleading threat prevention.
- **Application Visibility and Control** shrinks the potential attack surface through precise 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 persistent advanced malware threats.
- **Reputation-based URL Filtering** mitigates sophisticated client-side attacks by controlling access to more than 280 million URLs in more than 80 categories, minimizing risks associated with suspicious and unacceptable domains.
- **FireSIGHT Management Center** provides centralized event and policy management along with visibility into the devices, operating systems, applications, and users running in your network.

Next Steps

Contact your local sales rep to schedule a demo and request for pricing details. For additional information, visit the Cisco FirePOWER Threat Defense for ISR web page.

Benefits

- Take advantage of direct Internet access (DIA) in branches while keeping your connections secure.
- Deliver multilayered threat protection to your branch, partner, and remote offices.
- Free up valuable real estate with router and security technology in one consolidated footprint.
- Implement a clear division of roles and responsibilities using a centralized management console.

"Using a tuned policy, the FirePOWER 8350 blocked 99.5 percent of exploits. The device proved effective against all evasion techniques tested. The device also passed all stability and reliability tests."

NSS Labs 2015 Next Generation Intrusion Prevention System (NGIPS) Test Report

C45-734882-02 08/15