# Top 5 tips for choosing a firewall

# Contents

Rethink firewall as your flexible, dependable security foundation for a new world of hybrid and distributed environments.

## 1. Think beyond the box

What does the modern firewall look like? Fully integrated with your network infrastructure, but perhaps most importantly: Capable of enforcing policy everywhere from a single pane of glass. The next-gen firewall delivers unified policy across platforms, intel on mobile devices, context and threat intelligence — the visibility you need to handle connections to your network via vulnerable mobile apps and endpoints all over.

## 2. See what's within encrypted traffic

The barrier to really seeing what's going on within encrypted traffic has always been full decryption. An expensive process that's both impractical on a legal and operational level, it leaves your network and infrastructure highly vulnerable to everything from data exfiltration (breaches) to ransomware attacks.

The real challenge has been finding a way to detect malicious activities inside encrypted traffic. Your new firewall should prioritize this as a capability, with the aim of delivering maximum visibility using minimal decryption lift — and cost.

## 3. Demand threat intelligence immediately

With an expanding attack surface combined with ever-more-sophisticated threats against networks, branch offices, and (often) vulnerable and outdated infrastructure, any intelligence framework should be one step ahead of cybercriminals. It should identify incoming threats as exactly what they are — spam, malware, or other types of attacks.

This information should serve as foundational knowledge for what your firewall should do: Give you dynamic context about devices, locations, and users across your network.

## 4. Build in security resilience

Hybrid environments, often made up of users routinely accessing your network with vulnerable devices and apps, give hackers any number of enticing ways to infiltrate your network — making outdated infrastructure especially vulnerable and appealing. The answer to this is building security resilience.

Security resilience means securing the core of your highly available security infrastructure — your firewall — so you can prioritize alerts and tasks based on risk, anticipate what's next, and automate hourly security updates and your responses to unforeseen attacks, ultimately saving time, frustration, and cost.

## 5. Take a holistic approach

Why stop with just a firewall, when you can leverage any number of tools to deliver more visibility, more context, and a unified way to manage traffic and intelligence? With a suite of tools to enhance your firewall performance, you should be able to see more and understand context better without paying more.

Disconnection between services, multiple dashboards, and architecture makes threat management extraordinarily complex. Seek out a firewall and enhancements that help you make faster decisions, reduce your dwell time, and deliver meaningful, actionable metrics.

**See how Cisco Secure Firewall can improve your security posture and defend your organization against increasingly sophisticated threats:**

Learn more about Cisco Secure Firewall


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 **https://www.cisco.com/go/offices**.





Printed in USA C95-3416352-00 01/23