cisco SECURE

3 tips for growing organizations choosing a firewall

Reimagine the firewall, and stop the madness.

Tip 1

Stop buying firewalls (the traditional way) and start investing in firewalling.

So … you're looking for a firewall with less complexity, that gets out of the way? Then you'll want to understand our unique security vision and differentiated concept of *firewalling*. Years ago, *firewalls* were only *appliances*. But today, they're so much more. Simplified control and visibility, everywhere you need it—that's *firewalling*.

> "Simplified control and visibility everywhere you need it—that's *firewalling*."

Cisco's 2020 survey of almost 500 SMBs reveals small organizations take security seriously: 87% agree that it's a high priority.[1] That's only three percentage points less than larger businesses.

Imagine, stronger security and saving time and money—no matter where your security journey leads you. All because you'll have common firewalling policies, logging, and threat intelligence across your environments. **You'll be prepared because we deliver firewalling with physical and virtualized appliances, cloud-delivered firewall (SASE), and even control for apps and workloads.** You'll be ready to protect:

- Traditional, cloud, micro-segmented, and de-perimeterized networks
- Endpoints, with class-leading DNS, EDR, and VPN security
- Cloud applications, microservices, and containers

1. *Big Security in a Small Business World*, Cisco, 2020.

We call our flexible and comprehensive vision—for what's now, and what's next—*the future of firewalling.* We popularized the firewall, and are a Gartner Magic Quadrant for Network Firewalls leader. We have invested heavily in simplifying firewall management the past several years. You'll find routine access control tasks and rapid threat containment simpler than ever. Also, unlike competing solutions, our firewalls sustain performance in real-world conditions—even with advanced threat prevention functions enabled.

But before considering firewall management, threat defense, throughput, port density, cloud-readiness, vendor support, and cost, please consider our counterintuitive advice: **Stop.** Stop buying firewalls. For that matter, stop buying endpoint EDR. Stop buying VPN. Stop buying sandboxing. In short, stop the madness of buying point solutions that fail to integrate and enhance your security posture. Before you purchase your next firewall, determine how the elements of your security stack should work together. When you have questions, Cisco and our authorized partners are here to help!

Automated threat protection

Security must limit threats, not your business.
Select a firewall that provides:

- **Superior visibility**: You can't protect against what you can't see. See threats across users, hosts, networks, and infrastructure, and stop them faster.
- **Advanced malware protection**: Go beyond point-in-time detection. Use continuous analysis and integration with endpoint security tooling to detect, track, and analyze threats before they become liabilities.
- **World-class threat intelligence**: Security technologies are only as good as the intelligence that powers them. Make sure that your firewall is backed by a world-class threat intelligence organization, like Cisco Talos.

> "Stop. Stop buying firewalls … Stop the madness of buying point solutions that fail to integrate and enhance your security posture."

You're helping your organization grow, and you must protect it. So avoid being mired in the cost and complexity of planning your security a single point solution at a time. **Instead, consider our open platform approach. Understand, when we talk security platform, we're not suggesting that you rip-and-replace your entire security stack as you refresh your firewalls. Further, we're not saying that your security tooling must be entirely Cisco.** But as you plan, understand our unique firewall vision and open platform approach. It will empower you to do more with less because we've taken care of integrations across endpoint, network, and workload sensors.

Tip 2
Leverage Cisco SecureX,
your open security platform.

Get more, without paying more. Firewalling is central to Cisco SecureX™, our open platform for security. SecureX™ is included with every Cisco® Secure Firewall. It integrates Cisco and third-party security tools. SecureX further reduces security complexity and shrinks administration time. For instance, based on load, SecureX can automate virtual firewall provisioning to grow remote access VPN capacity on demand. SecureX can even automate ticketing workflows for others in your organization.

Reduce costs

Small organizations face many of the same threats as enterprises, with less budget and staff. Accomplish more with less.

- **Prevent breaches**: The best cure is prevention. Stopping more threats reduces the time needed for investigations.
- **Automation**: Automated IPS tuning, threat correlation, and Cisco SecureX playbooks reduce manual operations.
- **Prioritize alerts**: Focus on actions, not alerts. Prioritized alerts focus your efforts and save you time.

Reduce cost and administration time with platform-based firewalling. Control and visibility where you need it, unified by consistent policies and threat correlation between networks, workloads, and endpoints.

The SecureX platform also enhances your security posture and effectiveness. It aggregates threat data from across your organization and our global network of sensors, enriched by the Cisco Talos threat intelligence team. The end result of SecureX and Talos is that your security tools are integrated, tuned, and automatically updated throughout the day.

> “SecureX … reduces security complexity and shrinks administration time. For instance, based on load, SecureX can automate virtual firewall provisioning to grow remote access VPN capacity on demand.”

Tip 3
Simplify management,
even AWS VPC security group rules.

Tired of manually updating firewalls? Or managing policies across incompatible firewalls? Wish you had a firewall "easy" button? Spend less time on firewall administration and more driving business outcomes. Cisco Defense Orchestrator (CDO) takes the SecureX platform further. Save days of administration time with CDO's automated identification and deconfliction of overlapping and shadow security policies. CDO also updates every firewall's firmware with the push of a button. CDO manages it all, whether you're using ASA, Firepower, Meraki, or a combination of all three. It even manages AWS® VPC security group rules.

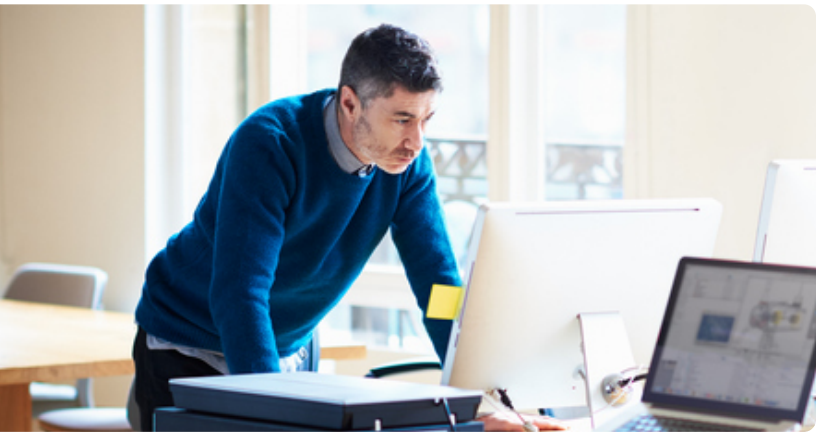
What's more, CDO can consolidate logging across your organization with our data lake capability.

Ease of use

Make sure your firewall saves you time.
Cisco cloud firewall management enables:

- **Simplified management**: Quickly understand access rules with simple visual representations. Rapidly make policy changes. View summaries of risks.
- **Simplified deployment**: No-touch and low–touch options.
- **Easy updates**: Get automated daily threat intelligence, and update all your firewalls with the single press of a button.

> "Spend less time on firewall administration and more driving business outcomes."



Take the next step:
Firewall selection guidance.

Firewall	 Meraki	 Cisco Secure Firewall: Firepower NGFW (FTD)	 Cisco Secure Firewall: ASA	 Cloud-Delivered Firewall Cisco Umbrella
Selection guidance	Integrated SD-WAN and simplest provisioning and management; integrated with Meraki switches, access points, and more. Best for organizations without dedicated NetOps and SecOps personnel.	Threat-focused with highly configurable security policies. Best for actively managed threat defense. Best for organizations with dedicated NetOps and SecOps personnel.	Rugged firewall with advanced routing and VPN. Best for L3/L4-exclusive use cases. Best for organizations with dedicated NetOps personnel.	Fully cloud-delivered security service. Best for when no appliance is desired.
Appliance	Meraki MX	Firepower Threat Defense (FTD) runs on every Firepower 1000, 2100, 4100, and 9300 Series appliance. Also available as a virtual appliance, NGFWv.	Cisco ASA runs on every Firepower 1000, 2100, 4100, and 9300 Series appliance. Also available as a virtual appliance, ASAv.	None required (cloud-delivered)
Cloud manager	CDO (when also using ASA/FTD) and/or Meraki	CDO	CDO	CDO* or Cisco Umbrella® Dashboard

* Expected in 2021.

CISCO DESIGNED