It's time to upgrade:

Why should I buy a next-generation firewall?

INTERNETWORK ENGINEERING

cisco Partner

Gold Certified

Will you be ready for the next big security breach?

In a recent survey, 56% of respondents[1] said that they experienced a significant security event in the past year. If your organization experienced one, were you completely prepared?

We're living in a time where both cybercriminals and the tactics they use are constantly evolving – so much that they can outsmart even the best preventative measures. Couple that with an increasingly distributed network perimeter and it's easy to see why relying on outdated architectures and technology not only make you less efficient and effective from a security perspective, it also makes your organization **more vulnerable to a security breach.**

Areas of the business impacted by a major security breach

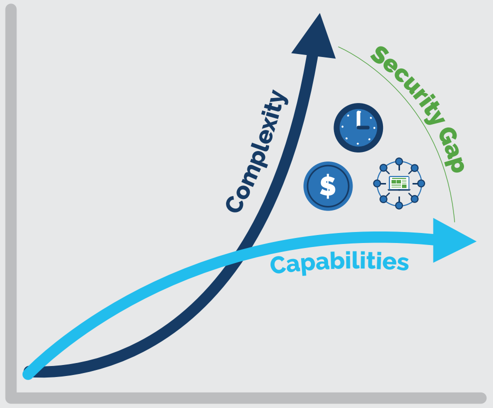
Cisco's 2020 CISO Benchmark Survey found that operations and brand reputation were the most affected areas.

36%	Operations
33%	Brand reputation
28%	Finances
27%	Intellectual property
27%	Customer retention
26%	Supplier relationship
23%	Business partnership
23%	Regulatory scrutiny
18%	Legal engagements

Are you relying on multiple point products?

In hopes of improving security, organizations will often try to address shortfalls by implementing multiple point products. In fact, Cisco's annual security report found that 55% of their customers[2] rely on **more than 5 vendors** to secure their network.

Multiple point products add unnecessary complexity



This approach may work for a while – but when you have a mixed bag of point products that all have different interfaces and don't communicate with each other, it only increases complexity and actually makes you less secure. That's because the more point solutions you have, the more difficult it is to correlate information, gain a clear picture of what's actually going on across your business, and focus on the highest-priority threats. **By reading a report conducted by ESG,** you can gain more insight into why relying on multiple point products for security is a "broken strategy."

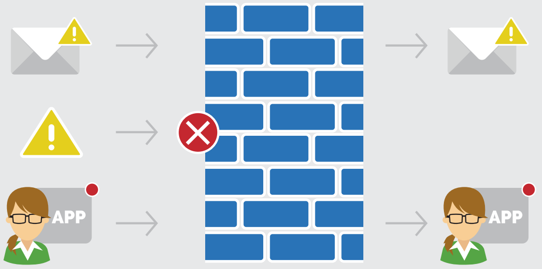
Today's advanced threat landscape calls for an integrated system of security tools that work in concert to combat threats and simplify security operations. In this eBook, you'll learn why a next-generation firewall (NGFW) that provides capabilities beyond threat protection must be at the heart of that integrated system.

Let's begin by discussing the intrinsic differences between legacy and NGFWs.

[1] Cisco, The Security Bottom Line (2019) [2] Cisco, Annual Cybersecurity Report (2017)

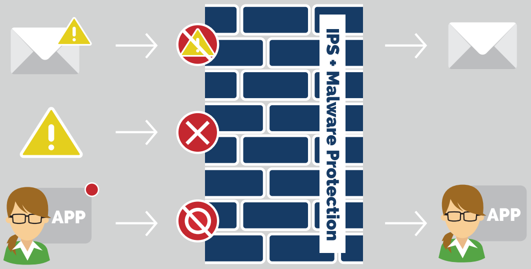
Legacy firewalls vs. NGFWs

A firewall's basic mission is to create a hardened perimeter that prevents certain traffic from entering your network and accessing data or resources. Legacy firewalls do this by blocking specific IP addresses and ports, but many of today's attacks are launched at the application layer and through new attack vectors – requiring additional security products and ultimately more manual processes. In addition to controlling traffic like legacy firewalls, NGFWs also provide additional security functions like anti-malware and intrusion prevention systems (IPS) that make it easier to inspect complicated application/web traffic and protect against modern threats.



Traditional firewalls only monitor specific ports and protocols

- Monitors traffic from network layers 2 through 4
- Threats can get through buried in approved traffic
- Offers no control over specific application functionality
- Other security functions must be deployed and managed separately

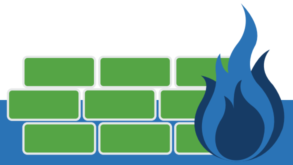


NGFWs enable deeper inspection plus application control

- Allows for deep application-level inspection (layer 7)
- Actively inspects and identifies threats in all traffic
- Enables granular control over application functionality
- Security functions like IPS and anti-malware are integrated and managed together

Is it time to consider an upgrade?

Given that time and budget are always limited, most organizations are reluctant to upgrade IT infrastructure that seems to be "working fine." But the fact that something just appears to be working isn't enough in today's threat landscape, especially when you're considering a core component of your overall security infrastructure. Still unsure of the need to upgrade your current firewall? **Ask yourself these questions:**



1 **Are we able to fully protect ourselves from traffic that our current firewall doesn't see?**

2 **Is our firewall able to keep up with our growing bandwidth requirements and future plans?**

3 **Can our firewall communicate with our security ecosystem and work with other security technologies?**

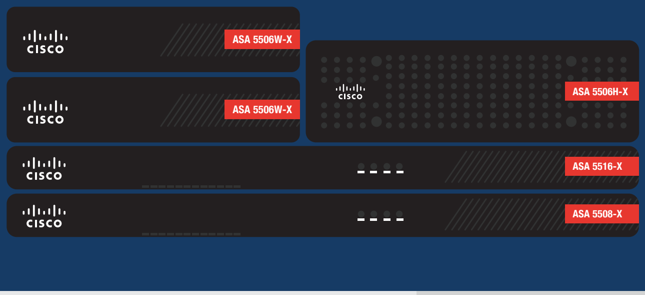
4 **Can we monitor and control what remote users are doing?**

5 **Would we benefit from more security automation and visibility beyond our perimeter?**

If your organization is relying on a traditional firewall and multiple point products for network security, **there's never been a better time to consider transitioning to a NGFW from an industry leader like Cisco.**

Cisco is a leader in Gartner's Magic Quadrant for firewalls

Cisco's family of NGFWs go way beyond protection and access control. In fact, they are foundational to the industry's most complete security platform – providing intelligent control points everywhere with consistent policy and integrated threat visibility. The latest generation of Firepower NGFWs give you the deepest set of integrations between core networking functions and network security to turn your entire network into an extension of your security infrastructure.



Cisco Next-Generation Firewalls

Firewall + Next-gen IPS (NGIPS) + Advanced Malware Protection + Identity Services Engine + Flexible management and deployment options

Prevent breaches automatically to keep your business moving

Talos (Cisco's threat intelligence team) analyzes millions of malware samples daily and automatically shares threat intelligence with their NGFWs to protect your organization 24/7 against known, unknown, and emerging threats.

Get deep network and security visibility

Cisco NGFWs go beyond protection by providing advanced security capabilities like NGIPS and anti-malware to give you deep visibility into telemetry and malicious activity across your applications, users, hosts, networks, and infrastructure.

Automate operations to save time and money

Along with prioritizing threats and making it simple to create/enforce policies, Cisco NGFWs work with the rest of their security portfolio to provide complete visibility and contextual awareness from the edge to your endpoints.

Let Internetwork Engineering help with your transition

Whether you need to transition from a legacy firewall or move to a more modern Cisco appliance, Internetwork Engineering offers the perfect balance of people, process, and technology to make it a seamless journey. We strongly believe that security is not a one-time event and will help you to take advantage of Cisco's industry-leading security architecture to detect, contain, and control security threats so you can better manage risk.

Real-world perspective and practicality from decades of experience across multiple industries

Threat-focused approach to security that keeps your data, business, and reputation safe

Expertise across Cisco's entire security portfolio and many success stories

Solutions to enhance your security posture regardless of your security capabilities

INTERNETWORK ENGINEERING

Additional resources

Download a checklist for choosing a NGFW

Download an infographic or watch a video to better understand what you should look for when choosing a NGFW.

NGFW Checklist

See why Cisco is a leader for NGFWs

Download a Gartner report to learn why Cisco was named a leader in the 2019 Magic Quadrant for Network Firewalls.

Gartner Report

Book a personalized NGFW demo

See how NGFWs go way behind protection and access control.

Schedule a Demo

About Internetwork Engineering (IE)

At IE, we are people connecting people. Since 1996, IE has been connecting people to their customers, coworkers, suppliers, patients, citizens, and students throughout the Southeast, creating more meaningful interactions with the people you care about most. Our mission is to provide technology solutions that inspire innovation and achievement, knowing that the right technology at the right time has the power to transform industries, countries, and lives.