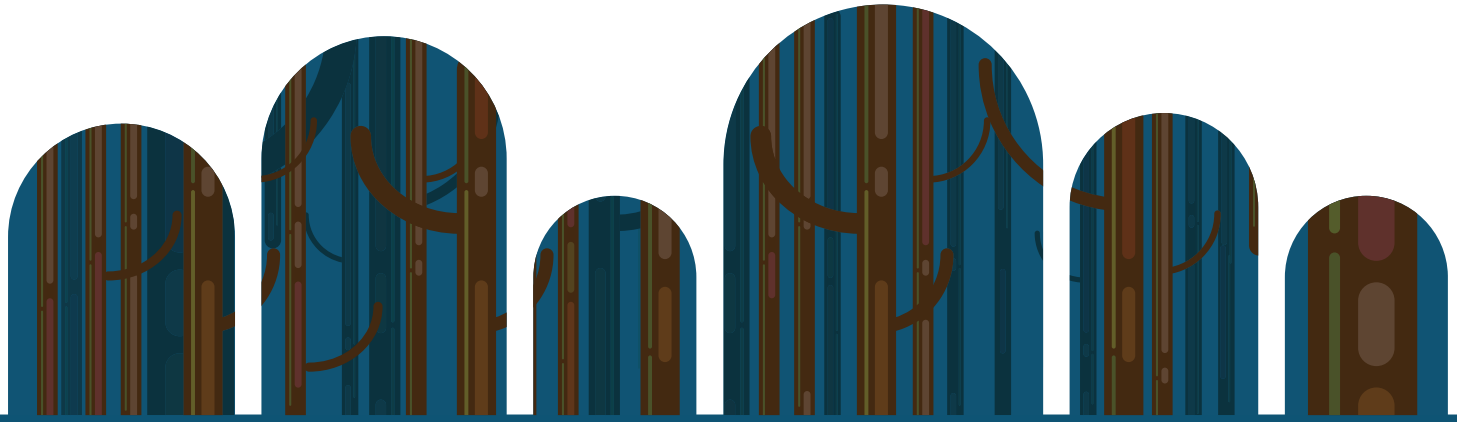


NGFW. See the woods from the trees

You've heard of it, but what does the **Next Generation Firewall** actually do? Get all the details on how it protects your business from cyber threats.

Traditional Firewall vs. Next Generation Firewall

The 'More hawk. Less mole' way to secure your network

A traditional firewall is able to control the traffic at the point of entry or exit within the network. In other words, it's the drawbridge between your own business and the 'great unwashed' of the rest of the internet.

This was perfect for those simple times – back when you used to be able to see everything that was latching onto your network. Now, businesses are increasingly playing host to a myriad of unknown devices, and a deep dark sea of cloud applications which are downloaded by employees.

The main difference with a next generation firewall is that you can set application controls and policies. For example, if a member of your staff downloads some file sharing software that may be unsecure, this will be automatically be made visible and you can do something about it instantly.

Plus, overall you will gain far more visibility and control over the users, devices, threats, and vulnerabilities in your network. So when your board asks you, "Are we secure?" you can provide a much more comprehensive answer than if you have a traditional firewall that only controls traffic.

Find the best Next Generation Firewall for you

While still motivated by profit, a new strategy – destruction of service – is emerging, with the IoT and systems with security weaknesses ripe for exploitation.

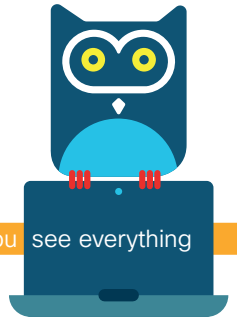
Intelligence knows where to look

Choose your next generation firewall

Different NGFWs are appropriate for different sized businesses, but essentially anyone who wants to control access policy, gain more visibility into what's going on in their next, as well as protect and remediate sophisticated cyber attacks quickly, should consider an NGFW. We've tailored ones specifically for each size of business.

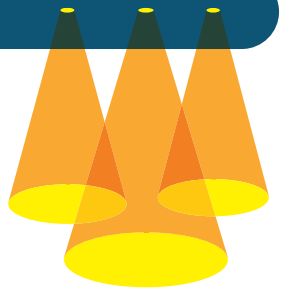
Your ecosystem is changing fast. Adapt quickly.

You can't protect what you can't see. So make sure you see everything



Shed some light on the problem

What's the best approach to installing a next generation firewall?



Some NGFWs can lose visibility and are unable to protect users if they're outside the traditional network perimeter, or when they bypass the VPN to access the Internet. To try and solve this problem, they have added first-generation intrusion prevention and an assortment of unintegrated products.

However, these solutions do little to protect against the risks posed by sophisticated attackers and advanced malware. Nor can they protect roaming users simply and cost-effectively. Furthermore, these NGFWs offer little assistance after an infection occurs. They can't help scope the infection, contain it, or remediate quickly.

You need best-in-class security technologies that work together transparently, follow the user, and mitigate risk when an attack penetrates the network.

The firewall should provide a holistic view of the network and analyse real-time threats and network traffic – effectively, and with scale. Properly installed, it should help your organisation defend against targeted and persistent malware attacks, including emerging threats. Reducing complexity so you see your ecosystem more clearly.

TOP TIPS:

BE STRATEGIC

Work with a vendor who can completely understand how a next generation firewall fits into your existing infrastructure, and can make sure it's helping to stop the threats that your business is most susceptible to.

BE AUTOMATED

A next generation firewall automates routine security tasks such as impact assessment, policy tuning, and user identi¬fication. Make sure you know what to do with this information so it can really be effective.

SHARE INTELLIGENCE

You need to be able to share intelligence and better leverage existing security technologies so that you can consolidate and streamline your response. Look for an NGFW that is open and integrates smoothly with an ecosystem of third-party security solutions. That way you can maximise your existing security investments; such as vulnerability management systems, network visualisation and SIEM systems, workflow remediation, ticketing systems, and network access control.

Read Next-Generation Firewalls: An Investment Checklist

For protection against increasingly advanced threats, you could consider a threat-focussed next generation firewall. Which means you can, among many other things:

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies
- Ease administration and reduce complexity with unified policies

Learn about our threat-focused next-generation firewalls (NGFWs)

Anything to watch out for?

Some next generation firewalls create more problems than they solve. For example, they can become a network bottleneck and slow down your performance.

Some next generation firewalls also lose effectiveness with threat inspection is turned on, i.e. when you need it the most.

Don't let your next generation firewall only work in certain instances. Check out these 5 tips for choosing a next generation firewall.

How the experts see us

NSS Labs performed an independent test of the Cisco Firepower 8120 with NGIPS v6.0 and Advanced Malware Protection v5.3.2016071117.

The Cisco Firepower 8120 with NGIPS and Advanced Malware Protection received a breach detection rating of 100.0%. The Firepower 8120 proved effective against all evasion techniques tested. The solution also passed all stability and reliability tests. Get the full NSS Labs test report

You can also learn more about NGFW features and see how Cisco stacks up against competitors, for example on Security automation and adaptive threat management, User, network, and endpoint awareness, and integrated advanced threat protection. Compare industry next generation firewalls

The Cisco NGFW is designed for a new era of threat and advanced malware protection. Head to our website for more details.