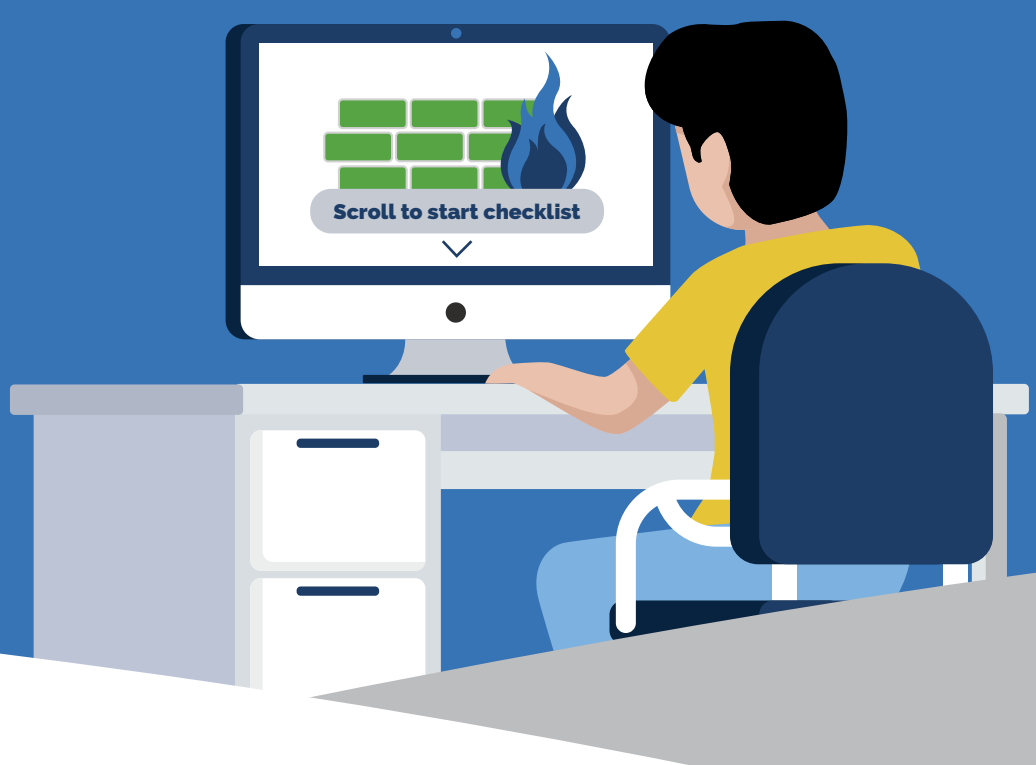
INTERNETWORK ENGINEERING

cisco Partner
Gold Certified

Your checklist for choosing a next-generation firewall (NGFW)

You know your firewall needs a refresh … but what do you do about it? Just like any other technology investment, choosing the right firewall for your organization isn't an easy task. Use this checklist to ensure the ones you're considering can deliver what your organization needs both now and in the future.



1 Does it deliver breach prevention and advanced security?

The first job of a firewall should be to prevent breaches, but since preventative measures will never be 100% effective, make sure the NGFW you choose includes **built-in** advanced capabilities such as:

- An Intrusion Prevention System (IPS) to spot stealthy threats
- URL filtering to enforce your policies
- Malware protection that analyzes behavior
- Real-time threat intelligence that's fed into the platform

2 Does it offer comprehensive network visibility?

Your firewall should provide a holistic view of activity across your entire network and full contextual awareness so you can see:

- Threat activity across users, hosts, networks, and devices
- Where/when threats originated, who it's affected, and what it's doing
- How you can stop threats to limit and contain the damage they're causing

3 Does it provide flexible management and deployment options?

Whether you're transitioning from a traditional firewall or upgrading your appliance, the firewall you choose should meet your unique requirements by offering:

- Options for every use case – including on-box or centralized management
- Ability to deploy on-premises, in the cloud, or for remote employees
- Customizable capabilities that can be easily turned on or off
- A wide range of throughput speeds

4 Does it decrease your time-to-detection?

According to Cisco research, the industry standard time for threat detection is 100 to 200 days which is far too long in today's threat landscape. The NGFW you choose should be able to:

- Detect known, unknown, and emerging threats in seconds
- Detect threats that make it past your perimeter within hours or minutes
- Prioritize alerts so you can focus on those that matter most
- Deploy consistent policy that's automatically enforced and easy to maintain

5 Can it work together with the rest of your security architecture?

The NGFW you choose should not be a siloed tool – it should communicate and work seamlessly with your entire security architecture. Choose a firewall that:

- Seamlessly integrates with other tools from the same vendor
- Automatically shares threat information with email, web, endpoint, and network security tools
- Automates security tasks like threat assessment, policy tuning, and user identification

Get educated on the firewall vendor landscape or schedule a demo

INTERNETWORK ENGINEERING

At Internetwork Engineering, we offer the perfect balance of people, process, and technology to make your transition to an NGFW a seamless journey. If you'd like to learn more about the vendor landscape or see how Cisco's NGFWs check all these boxes and more, reach out today.

Schedule a Demo