5 Tips for Choosing a Next-Generation Firewall

Invest in a new Next-Generation Firewall (NGFW). Ask if it delivers...

1 Breach Prevention and Advanced Security

Prevent attacks and quickly detect malware if it gets inside

Job #1 of a firewall should be to prevent breaches and keep your organization safe. But since preventive measures will never be 100% effective, your firewall should also have advanced capabilities to quickly detect advanced malware if it evades your front-line defenses. Invest in a firewall with the following capabilities:

- Prevention to stop attacks before they get inside
- A best-of-breed Next-Generation IPS built-in to spot stealthy threats and stop them fast
- URL filtering to enforce policies on hundreds of millions of URLs
- Built-in sandboxing and advanced malware protection that continuously analyzes file behavior to quickly detect and eliminate threats
- A world-class threat intelligence organization that provides the firewall with the latest intelligence to stop emerging threats

2 Comprehensive Network Visibility

See more so you can stop more

You can't protect against what you can't see. You need to monitor what's happening on your network at all times so you can spot bad behavior and stop it fast. Your firewall should provide a holistic view of activity and full contextual awareness to see:

- Threat activity across users, hosts, networks, and devices
- Where and when a threat originated, where else it has been across your extended network, and what it's doing now
- Active applications and websites
- Communications between virtual machines, file transfers, and more

Additional Resources

Demand more from your firewall. Explore Cisco Firepower NGFW.

Cisco NGFW Overview
Cisco NGFW Demo
Customer Testimonial: Downer Group

Visit cisco.com/go/ngfw

3 Flexible Management and Deployment Options

Customization to meet the unique needs of every organization

Whether you are a small to medium-sized business, or a large enterprise, you firewall should meet your unique requirements.

- Management for every use case – choose from an on-box manager or centralized management across all appliances
- Deploy on-premises or in the cloud via a virtual firewall
- Customize with features that meet your needs – simply turn on subscriptions to get advanced capabilities
- Choose from a wide range of throughput speeds

4 Fastest Time to Detection

Accelerate malware detection to mitigate risk

The current industry standard time to detect a threat is between 100 to 200 days; that's far too long. A next-generation firewall should be able to:

- Detect threats in seconds
- Detect the presence of a successful breach within hours or minutes
- Prioritize alerts so you can take swift and precise action to eliminate threats
- Make your life easier by deploying consistent policy that's easy to maintain, with automatic enforcement across all the different facets of your organization

5 Not a lone wolf. A member of the pack.

An integrated security architecture enables automation and reduces complexity

Your next-generation firewall should not be a siloed tool. It should communicate and work together with the rest of your security architecture. Choose a firewall that:

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