5 Tips for Choosing a Next-Generation Firewall

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

1 Integrated Threat Defense

Get actionable, multi-layered protection.

Today's multi-vector and persistent threats slip through gaps in protection and evade detection. A threat-focused NGFW provides best-in-class security technologies that work together across the network and endpoints and are managed through a central console. Built on a comprehensive stateful firewall foundation, threat-focused NGFW technologies should include:

- Next-Generation IPS
- Advanced Malware Protection
- Application Visibility and Control
- Reputation-based URL filtering
- Application-level VPN

▸ With integrated threat and advanced malware protection that continuously correlates threat intelligence across security layers, you can identify and protect against sophisticated attacks.

2 Actionable Indicators of Compromise

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. An NGFW should provide actionable indicators of compromise (IoCs) that:

- Correlate network and endpoint security intelligence
- Provide highly accurate visibility into suspect and malicious file and host behavior
- Prioritize infected hosts for rapid remediation

▸ Actionable IoCs let you see malware activity on hosts and endpoints, understand the impact, and quickly contain and remediate.

3 Comprehensive Network Visibility

Increase security effectiveness with a holistic view.

You can't protect what you can't see. You need to monitor what's happening on your network at all times.
An NGFW should provide full contextual awareness of:

- Users, operating systems, and devices
- Communications between virtual machines
- Threats and vulnerabilities
- Applications and website access
- File transfers, and more

▸ This level of insight helps you identify and address security gaps and fine-tune policies so as to reduce the number of significant events requiring additional action.

4 Reduced Complexity and Costs

Unify security layers and automate for efficiencies.

A combination of advanced threats and a shortage of skilled IT security professionals is stretching IT departments to the max.
Look for an NGFW that:

- Consolidates multiple layers of defenses on a single platform
- Delivers consistent and robust security at scale
- Automates routine security tasks like impact assessment, policy tuning, and user identification

▸ By reducing complexity and costs your team is freed up to focus on events that matter most.

5 Integration with Third-Party Solutions

Maximize existing security investments.

You need to be able to share intelligence and better leverage existing security technologies to consolidate and streamline response.
Look for an NGFW that is open and integrates smoothly with an ecosystem of third-party security solutions like:

- Vulnerability management systems
- Network visualization and SIEM systems
- Workflow remediation and ticketing systems
- Network access control (NAC), and more

▸ Third-party solution integration reduces your IT burden and total cost of ownership (TCO) and strengthens multi-layered protection.

Resources

Requirements When Considering a Next-Generation Firewall

White Paper - Get the full checklist to protect your business from attacks.
Read Now.

Cisco ASA Excels in Firewall Tests

NSS Labs ranks Cisco highest in the most rigorous NGFW testing to date.
Watch the video.

Cisco ASA NGFW Website

Stay up-to-date on the latest trends and see what's new in security from Cisco.
Learn More.

Attacks will continue to evolve as will the IT environment you need to protect. Make sure the NGFW you select provides **tightly integrated, multi-layered threat protection.** By sharing context and intelligence among security functions you accelerate threat detection and response across your organization, and get the most from your investments.

cisco

It's not what we make;
it's what we make possible.

Making security everywhere a reality.

Visit www.cisco.com/go/ngfw

Follow us on Twitter @CiscoSecurity