aws marketplace

NAVIGATE. EVALUATE. ELEVATE.

Your guide to selecting the ideal NGFW solution for your business

aws marketplace

Navigate. Evaluate. Elevate.

Your guide to selecting the ideal NGFW solution for your business

How can an NGFW strengthen my organization's resilience?

A Next Generation Firewall (NGFW) isn't just a "revamped" firewall. It's optimized for the scale and scope of cloud operations that your enterprise needs.

Although all NGFW offerings serve the same broader purpose, there isn't a one-size-fits-all solution. In this document, we'll explore some crucial questions that your team can use to clearly define your security priorities, accelerate your search, and streamline your NGFW deployment.

Discover the benefits of implementing a more sophisticated approach to security

Enhanced visibility and control: Not only does an NGFW observe "typical" ports and protocols, it also provides more intensive protocol examination, application awareness, and deep packet inspection.

Advanced threat detection and prevention: An NGFW often comes equipped with intrusion detection systems (IDS) and intrusion prevention systems (IPS), application awareness, and sandboxing capabilities that can assist in handling advanced threats, including malware, phishing, and zero-day exploits.

Security and compliance best practices: Many organizations are required to comply with various regulations and standards (such as ISO/IEC 27001 or PCI-DSS). An NGFW can be an integral component of your overall security approach, helping to satisfy compliance requirements by providing features such as historical event tracking, logging, and monitoring.

Simplified management: Most NGFW solutions come equipped with centralized management capabilities, which means you can deploy multiple firewalls but manage and configure them from a single location. This helps stretched teams maintain a robust network security presence. Security teams can focus on priority tasks with simplified management.

Cloud visibility: An NGFW in the cloud provides all the above capabilities, with the added benefit of being implemented within your cloud stack. It isn't just cloud-deployed—it's also cloud-visible. Whether you're running serverless functions or a complex network of storage and virtual machines, an NGFW can quickly be implemented in critical observation locations, providing robust network security with less downtime.

Traditional vs. Next Generation Firewall: What's the difference?

Traditional firewall:

- ✓ Recognizes network protocols
- ✓ Filters traffic based on IP address and port
- ✓ Supports routing protocols
- ✓ Increasingly less effective against sophisticated malware

NGFW:

Includes the functionality of a traditional firewall, plus:

- ✓ Incorporates signature- and behavior-based analytics to identify malicious traffic
- ✓ Offers protection at various stack levels and with multiple capabilities
- ✓ Is application-aware
- ✓ Provides improved visibility
- ✓ Helps streamline regulatory compliance
- ✓ Potentially reduces security expenses
- ✓ Enhances business continuity

A direct path to NGFW implementation requires knowing where your business currently stands and where it wants to go, then applying those parameters to the current range of available solutions—to find the best fit for your organization's infrastructure and security goals.

To help get you started, we're going to dive into three key considerations:

1. **Consideration:** Does the product meet our technical requirements?

2. **Consideration:** Which solution aligns with our budget?

3. **Consideration:** How much time are we going to invest in this deployment?

1. Consideration: Does the product meet our technical requirements?

Technical capabilities are a great gatekeeper for deciding on the right firewall for your organization, as these requirements will directly inform your selection of a firewall vendor.

Start by answering a few key technical questions to establish a foundation for your NGFW requirements:

- Can our existing architecture accommodate an NGFW?
- Do we have compliance requirements?
- Do our applications have special requirements?
- Do we need our firewall to be application-aware?
- Do we want our firewall to manage a site-to-site virtual private network (VPN)?

Expert Corner

"We shouldn't ask yesterday's tools to keep up with tomorrow's threats. A fleet of connected and centrally managed NGFWs can improve network security posture, simplify management, reduce costs, and enhance security teams' visibility into network traffic."

Matt Bromiley
SANS Digital Forensics and Incident Response Instructor

How do you want to deploy your NGFW?

This decision will refine your list of potential vendors and provide key information to your vendor. Which of the following best describes your team?

"We know exactly what we need, and we're ready to move forward." 1

Recommended deployment style: **Self-managed**

With little vendor interaction, your security team can spin up and deploy as many cloud-based NGFWs as needed, often with little downtime.

"We want to maintain control over select elements, but would also feel more comfortable with expert guidance." 2

Recommended deployment style: **Partially managed**

Cloud-based firewalls in AWS can be deployed with partial management options, allowing you to work with a trusted vendor on key needs, such as deployment or technical troubleshooting, while still maintaining control over some operational elements, like threat detection and response.

"We want to find a vendor that we can rely on for the entire NGFW implementation and maintenance." 3

Recommended deployment style: **Fully managed**

A fully managed NGFW offers businesses the chance to implement robust network security—without overextending their existing security teams or hiring additional internal personnel.

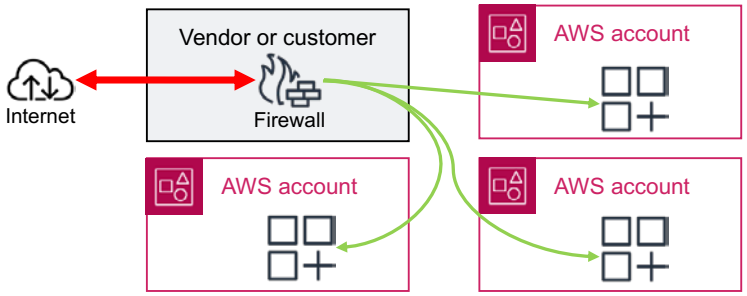
Where do you want to position your NGFW?

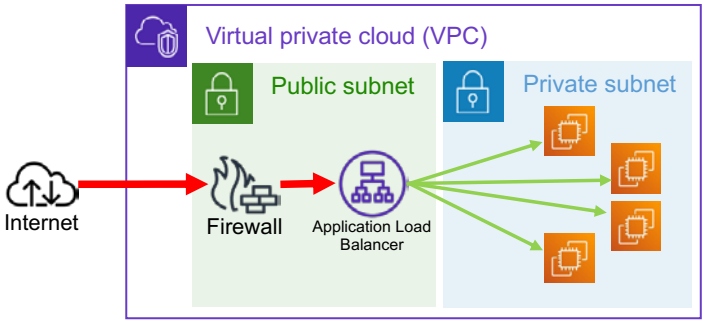
The best placement for your NGFW in your cloud environment depends on many factors, including traffic patterns, bandwidth requirements and availability, and the cloud services you have chosen to use. The NGFW should be placed in a location that provides maximum coverage and protection with little to no impact on performance.

NGFW placement is largely dependent on your cloud network topology and security requirements. Rather than there being a single, correct placement, it's more about asking "What works for my team?"

At your perimeter for Ingress and Egress

This is a traditional home of a firewall. Utilizing a common Ingress and Egress point allows you to fully inspect and control traffic both in and out of your network. This is also a popular architecture when your firewall is managed by a partner even if they aren't in AWS. A partner firewall can be fully managed by the partner and control the traffic destined to your workloads in different accounts. Egress inspection is useful for detecting and preventing malicious traffic, being part of your Data Loss Prevention program, or simply providing control, visibility, and monitoring to the internet from your network.



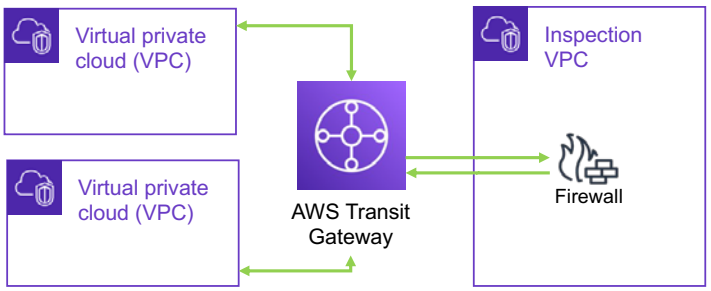


In front of workloads and other gateways

Strategically positioning firewalls in your network in AWS is a common practice. These firewalls can add extra layers of protection by inspecting traffic as it enters your VPC but before it reaches your workload. This can be especially useful for meeting compliance requirements such as PCI and HIPAA, whether it's for a group of virtual servers, a dedicated application, or a load-balancer. The firewall placed in front of it can terminate TLS, inspect traffic for malicious behavior, apply Intrusion Prevention, and forward it on to your workload helping you fulfill both security and compliance requirements.

In your network for east-west inspection

Take control of east-west traffic in your internal network including in AWS Transit Gateway. By placing firewalls in a dedicated Inspection VPC attached to your Transit Gateway, you can inspect some or all of the traffic between VPCs that are also attached to the Transit Gateway. Inter-VPC communications can now be enforced by your security team through your firewall policy. Traffic can be inspected for malicious behavior or logged for forensic analysis. A firewall that supports TLS termination can be leveraged to get deeper layer-7 visibility.



If you're unsure of the ideal placement of your NGFW, this will be an important discussion to have with your potential vendor.

2. Consideration: Which solution aligns with our budget?

Budget considerations are complex and can require long evaluations to ensure you've covered every aspect of the project. They might also influence whether you reconsider a firewall option that includes all the technical requirements on your initial wish list.

In addition to licensing costs, consider the following:

- Do we have any blind spots in our cost estimate for implementing the solution?
- Will we need to pay for staff training?
- How much input will we need from a consultant, and at what cost?
- Will there be data-processing costs involved for the traffic we'll need to inspect?
- Will other cloud services be required for your implementation, and will they have associated data-processing costs?

Expert Corner

"During my career I've learned that budgeting for projects is a bit of an art. Your costs can be more than just licensing. It's also the need to train staff, hire consultants, or even buy additional software. Don't let hidden expenses surprise you!"

Geoff Sweet
Senior Security Solutions Architect, AWS

3. Consideration: How much time are we going to invest in this deployment?

Specific timeline considerations include:

- Although it may be a relatively short turnaround to turn on new firewalls, can the same be said for the architectural work required to begin routing traffic through them?
- Will there be a lot of testing and work needed to put our NGFW in line with our traffic?
- If the changeover requires an outage, will we need to review and adhere to our downtime policies?
- Will our staff need training to get the expertise to operate, maintain, and report on our NGFW?

Once you've estimated these time requirements, consider framing them against the earlier decision over your preferred deployment style. With a clearer idea of the timeline, you can look back to reassess whether this conflicts with what your internal teams can realistically manage.

If your internal teams can fully execute and manage an NGFW implementation, how much bandwidth will that leave them to maintain regular business operations? Or, if your teams require additional training to manage deployment and maintenance, will that investment be more beneficial than passing those tasks along to a third party? These answers may shift your thinking about your preferred deployment style.

Developing a forecast of your expected time-spend ahead of deployment can help to clarify expectations, and save you that time—and more—in the long run.

Expert Corner

Time is the one asset that cannot be gained back. Know your team's bandwidth and capabilities. Let them prioritize time, gaining the most value for their hours—not their dollars.

Matt Bromiley
SANS Digital Forensics and Incident Response Instructor

When there's more than one suitable NGFW solution, how can you decide?

As with most technologies, different products are weighted toward fulfilling different organizational needs. It's not about searching for a 'best' solution—it's about selecting the solution that best aligns with your specific circumstances.

In most instances, this will likely involve a compromise when it comes to your ideal conditions.

Let's consider that you've now reached the end of the evaluation process. You've selected four viable products, available through four separate vendors. No single product satisfies all of your ideal requirements—but each one has certain attributes that you're seeking.

Expert Corner

"Sometimes the right product at the right price is right there in front of you. But sometimes it isn't, and that's OK. In that case, know where you can be flexible in stretching the goals for your project. Don't compromise your security over a project constraint."

Geoff Sweet
Senior Security Solutions Architect, AWS

✓ Meets requirements · — Partially meets requirements · ✗ Doesn't meet requirements	Solution A	Solution B	Solution C	Solution D
What's the next step in your decision-making process? It's time to compare these solutions in detail and apply the priorities that you've established through the considerations presented in this guide.	Fills every technical requirement (and more), but it's relatively expensive and new to the IT team, which will need training. Also, the implementation time involves technical challenges that will take longer than we'd hoped.	Doesn't fill our technical requirements, but we can live with its perceived deficiencies—especially considering that it's well within our budget and fast to implement.	Presents some conflicts for our technical requirements. Plus, it's still on the expensive side. But it does include ample vendor support and provides tools that should make deployment fast and simple.	Fills all our technical requirements—but it's significantly over our budget, and although it's a great product, its deployment presents challenges that will have a longer than desired timeline.
Technical Requirements	✓	—	—	✓
Budget	✗	✓	—	—
Time to Implement	—	✓	✓	✗

Your company's priorities will define your decision about which solution to implement. Determine your organization's key needs and work through the scenario above, selecting the optimal fit based on your immediate and future priorities and limitations.

Now that you know where you're headed, choose the solution that will take you there.

The NGFW solutions available in AWS Marketplace combine multiple integrated security functions, such as IDS/IPS, VPN gateways, antivirus and anti-bot controls, application control, secure sockets layer (SSL), and TLS inspection, and web filtering.

Select a solution that fits your organization's mandate for enhanced security and get started today.

AWS Network Firewall

- Native AWS solution
- ANF handles scaling up based on throughput
- Multiple deployment models
- Stateless and stateful rules to optimize traffic

Video

Learn more

CHECK POINT

- Recognized by analysts as an industry leader in cloud network security
- 99.8% malware prevention as verified by independent test lab
- Manage security consistently across on-prem, AWS, and hybrid-clouds
- Single pane of glass for visibility, policy management, and control

Datasheet | Video

Learn more

FORTINET

- Enforce Zero Trust policies
- Automate deployment and management of security
- Comprehensive scanning of traffic to and from the cloud
- Integrate your Secure SD-WAN with AWS

Datasheet | Video

Learn more

paloalto NETWORKS

- Deep integration with AWS
- Application-based policy enforcement
- Central management with Panorama
- Threat prevention from viruses, worms, malware, and more
- URL filtering to control in and outbound request

Datasheet | Watch a demo

Learn more

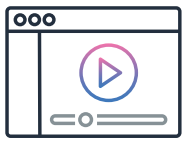
Additional resources

As the shape of the enterprise changes, so should its protection.

When the structure of an enterprise's operations shifts, its security measures need to change shape to stay effective. Hybrid working environments, complex cloud operations, globally distributed physical infrastructure, evolving data sovereignty requirements—these conditions define the modern enterprise, and traditional firewalls weren't designed to handle them.

In this new era for the modern enterprise, maintaining dependability requires the next generation of security approaches. An NGFW is a powerful device that, when correctly implemented, can become a staple of incident detection and response procedures for years to come.

To explore the critical role an NGFW can play in securing your business, or to get started on your implementation journey, click on the links below.



Watch webinar

Join Matt Bromiley and Geoff Sweet for a discussion on "What is a Next Generation Firewall (and why does it matter)?"

View on-demand

Read the whitepaper

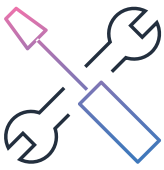
Matt Bromiley shares his industry expertise in "An NGFW: A critical part of your security stack."

Download now

Read the ebook

The value of Next Generation Firewall (NGFW) tools.

Download now



Discover NGFW solutions

Find additional resources and tools to implement an NGFW in AWS and protect your assets.

Learn more

Talk to an expert

Get connected with a solution architect that can share best practices and help solve your business challenges.

Get connected

AWS Marketplace

Find, buy, deploy, and govern software solutions on AWS Marketplace.

Learn more