aws marketplace

ONE-MINUTE WEBINAR

Next-generation firewalls: A critical part of your security stack

Key Topics

1. Understanding Next-Generation Firewall (NGFW) Basics
2. NGFW Implementation
3. NGFW Use Cases
4. See it in Action: Barrett Steel Turns Information Security Into a Business Enabler
5. Summing it Up

#1

Understanding Next-Generation Firewall (NGFW) Basics

Using traditional firewalls to protect today's hybrid environments—with complex cloud operations and systems scattered around the globe—can make a security team feel lost or constantly behind.

Next-generation firewalls (NGFWs) are a core technology to include in every security stack. NGFWs provide more advanced and comprehensive security capabilities than traditional firewalls, including:

- **Advanced threat protection:** Traditional firewall rules based on network protocol basics, such as traffic protocol, IP address, and/or ports, are easily evaded by today's malware authors. NGFWs often incorporate signature- and behavior-based analytics to identify malicious traffic.
- **Application control:** Unlike traditional firewalls, NGFWs are application aware. They can often inspect and categorize traffic at the application layer, including traffic to/from specific applications or application programming interfaces (APIs).
- **Improved visibility:** With deeper insight and profiling of network traffic, NGFWs can provide additional visibility into real-time network traffic analysis.
- **Streamlined regulatory compliance:** With their advanced visibility and detection capabilities, NGFWs can enforce security controls to help keep organizations compliant with regulatory requirements.
- **Cost savings and simplified deployments:** NGFWs can reduce security overhead—particularly in cloud environments—allowing an organization to gain NGFW benefits with a few mouse clicks.
- **Business continuity:** NGFWs lower the risk of business impact simply by being more capable and integrated. Unified and integrated platforms make it harder for successful intrusions, and this can minimize downtime due to cyberattacks.

#2

NGFW Implementation

Implementing an NGFW into your security stack, especially within a cloud environment, is a straightforward process. The steps below use the AWS Marketplace curated digital catalog as an example:

1. Research NGFW solutions to determine one that can integrate with your current stack or offers the benefits you most value.
2. Plan for an NGFW implementation. This may include defining your cloud footprint/network topology and defining security policies.
3. If needed, schedule proof-of-concepts to test NGFW solutions against what your security team requires. Make sure to evaluate support options in addition to technological capabilities.
4. Once you select a vendor, opt to subscribe within the AWS Marketplace or work through another resource you may have established in an earlier step.

Snippet of NGFW Solutions available in AWS Marketplace.

#3

NGFW Use Cases

Use case 1: Securing enterprise applications
To protect cloud assets, teams can deploy cloud-first NGFWs with a few clicks to inspect traffic at the application level, offering protection that traditional firewalls can't. Cloud-based NGFWs scale easily, integrate with cloud provider APIs—allowing for automatic policy configuration based on the current cloud environment—and centralize management across all cloud applications, regardless of "where" they are deployed.

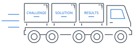
Use case 2: Unified management
Implementing NGFWs as a single appliance at physical locations and at key cloud junctions provides a unified platform for network security management, eliminating the need to maintain multiple security devices at each location. An NGFW offers enhanced features—including intrusion prevention, application awareness, and deep packet inspection—and can implement policies based on specific users, applications, and devices, all while monitoring network traffic in real-time.

Use case 3: Defending against the unknown
All organizations need to consider defenses against novel attacks without known detection mechanisms. For these attacks, the NGFW's onboard behavioral analysis is useful for detecting suspicious activity without knowing exactly what it is. Analysis of patterns of anomalous activity that falls outside typical user activity, and potentially other metadata, may conclude that an attack is ongoing and implement preventative measures. If behavioral analysis alone cannot identify an unknown attack, many NGFWs also utilize machine learning to detect patterns and identify suspicious behavior. Teams can use sandboxing to isolate and analyze suspicious network traffic in a secure environment.

#4

paloalto NETWORKS | BARRETT STEEL LIMITED

See it in Action: Barrett Steel Turns Information Security Into a Business Enabler



Challenge
Maintain strong information security across on-premises and cloud assets and simplify administration for a lean IT team that faced performance limitations in its hard-to-manage legacy security infrastructure.

Solution
The Palo Alto Networks NGFW suite and the Prisma Cloud platform centralize all network security management for Barrett Steel, as well as intelligently detect and disrupt cyberthreats. The company can now control traffic based on application type and user role while enabling secure remote work.

Results
Barrett Steel automatically detects and prevents phishing attacks on-premises and in the cloud and has simplified security management for its IT team. The company has assured that its cloud applications conform with security policies as it supported a 10x increase in remote workers.

> *The fact that we have been able to run and grow our business without any major issues is in large part because of the strong security posture we've taken by investing in solutions from Palo Alto Networks.*
>
> —Sam Ainscow
> Head of IT Operations and
> Chief Information Security Officer
> Barrett Steel

#5

Summing it Up

In a rapidly evolving development, deployment, and threat environment, today's organizations can't expect older security technologies to keep up with modern threats. NGFWs help solve this challenge. Analysts can use NGFWs to perform packet inspection, automatically detect anomalous behavior, and help the security team become application aware. All in all, NGFWs are multi-capability devices that offer network inspection and detection capabilities that traditional firewalls simply can't match.

Next Steps

Explore the role of NGFWs with these AWS Partners

AWS Security Partners have NGFW solutions to help protect your workloads from malicious or unauthorized traffic.

paloalto NETWORKS — Learn more

Check Point SOFTWARE TECHNOLOGIES LTD. — Learn more

FORTINET — Learn more

VALTIX — Learn more

Additional Resources

Watch the webinar
What is a next-generation firewall (and why does it matter)?
View on-demand

Read the whitepaper
NGFWs: A critical part of your security stack
Download now

Discover solutions
Find the tools you need to implement next-generation firewalls (NGFWs) in AWS and protect your assets.
Visit AWS Marketplace

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