Enterprise Strategy Group by TechTarget

SHOWCASE

APRIL 2024

Achieving Simplicity, Scale, and Security With Google Cloud NGFW Enterprise, Powered by Palo Alto Networks

John Grady, Principal Analyst

Abstract: Public cloud infrastructure security remains a persistent challenge for organizations as threat levels escalate in volume and sophistication. As cloud adoption continues to surge, organizations require a firewall solution that offers the benefits of a cloud-native approach while delivering the robust security needed to fully exploit the cloud's potential. Google's Cloud NGFW Enterprise, powered by Palo Alto Networks, combines best-in-class cloud engineering with industry-leading security, enabling organizations to efficiently and effectively apply network security policies at scale.

Many Continue to Struggle With the Disconnect Between IaaS and Network Security

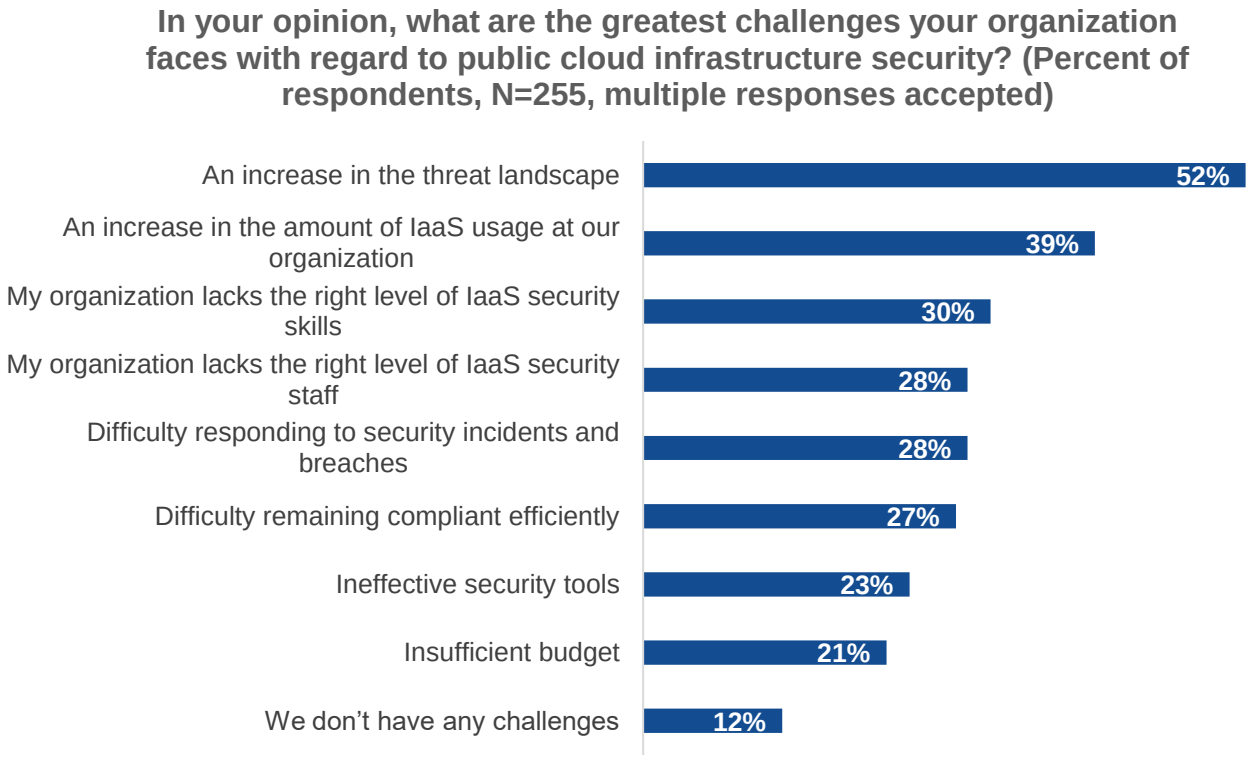
The use of public cloud infrastructure (i.e., IaaS) is ubiquitous, yet many organizations continue to report challenges in securing this part of their environment. According to research from TechTarget's Enterprise Strategy Group, 88% of organizations cite challenges of some kind with regard to securing public cloud infrastructure (see Figure 1).[1] The variety of challenges include ineffective security tools (cited by 23%) and insufficient budget (21%), but the most common challenges are the following:

- **Expanded threat landscape.** More than half of respondents (52%) cited an increase in the threat landscape as a top public cloud infrastructure security challenge. Attackers understand that an increasing amount of sensitive data and business-critical applications have moved to the cloud. As a result, they target these environments with a variety of tactics, including zero-day exploits, targeted penetration attacks, malware, and the opportunistic exploitation of misconfigured infrastructure. Securing these environments is made even more difficult due to the interconnectedness of cloud applications. Specifically, Enterprise Strategy Group research has found that 94% of organizations say at least one production application or elements of an application communicate across regions within a cloud service, while 79% say at least one communicates via open ports exposed to the internet.[2]
- **Greater IaaS usage.** More than one-third of respondents (39%) indicate that the scale of IaaS usage is also a common issue. One of the key benefits of the cloud is its on-demand and elastic nature. Yet, at the same time, this can make ensuring consistent security significantly more difficult. Creating, deploying, and maintaining network security policies in such a highly dynamic environment can be difficult. Further, enforcing these policies typically requires traffic to be routed to centralized inspection points, such as a firewall. This type of hairpinning can negatively affect performance. As a tradeoff, some organizations may choose not to inspect traffic, which increases the risk that an attack will go undetected.
- **Staff and skills shortages.** Finally, a number of respondents noted that their organizations lack the right level of IaaS security skills (30%) and staff (28%). This only exacerbates the issues around deployment and proper

[1] Source: Enterprise Strategy Group Research Report, *Network Security Trends in Hybrid Cloud Environments*, July 2022. All Enterprise Strategy Group research references are from this report, unless otherwise noted.
[2] Source: Enterprise Strategy Group Complete Survey Results, *Cloud Entitlements and Posture Management Trends*, March 2023.

routing, not to mention ongoing configuration management. The organizational dynamics when it comes to securing IaaS also come into play here. Cloud operations teams and the developers they support often move much quicker than their security counterparts. Security teams may be brought in to secure infrastructure after it has already been deployed, leaving a window where network security is not in place.

Figure 1. Public Cloud Infrastructure Challenges



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Protecting Cloud-resident Infrastructure Requires a Security-first, Cloud-native Approach

To address these challenges, security teams need tools that help them more efficiently and effectively protect their organization's IaaS resources. More specifically, they need firewalls that are truly cloud native and that offer simplicity, scalability, and strong security to ensure their organization can take full advantage of cloud infrastructure while simultaneously reducing risk.

[Security teams] need firewalls that are truly cloud native and that offer simplicity, scalability, and strong security to ensure their organization can take full advantage of cloud infrastructure while simultaneously reducing risk.

Traditionally, organizations have had to seek tradeoffs when weighing usability and security capabilities. Often, solutions providing the best security require more experience and higher skillsets, while those providing simplicity didn't offer robust security capabilities. Businesses generally and security teams specifically are no longer willing or able to make that tradeoff; they require solutions that improve efficiency while also offering strong security.

Simplicity

Cloud resources are ephemeral and often brought online without the knowledge of security teams. Network security policies must be automatically applied and enforced. To accomplish this in a dynamic cloud environment, policies must be based on the application characteristics (application type, the region it is deployed in, etc.) rather than IP address. Based on established policy, as workloads come online, security rules should be able to be enforced without having to update network routing to point traffic to a specific firewall instance. Enterprise Strategy Group research highlights the importance of simplicity, with 48% citing ease of management and 46% pointing to ease of deployment as top reasons their organization uses firewalls from cloud service providers.

Scalability

A significant reason for adopting cloud architectures is the scalable nature of the infrastructure. In fact, 41% of Enterprise Strategy Group research respondents cited scalability as a top reason their organization uses firewalls from cloud service providers. Unfortunately, traditional network security approaches limit how quickly capacity can be securely expanded. The need to manually deploy instances and load balancers, in addition to required network routing updates, can all limit scalability. Cloud firewall solutions that are cloud-native and built on a distributed architecture can automatically scale with the environment and put protection closer to the workload to avoid backhauling.

Enterprise Strategy Group research highlights the importance of simplicity, with 48% citing ease of management and 46% pointing to ease of deployment as top reasons their organization uses firewalls from cloud service providers.

The ability to support a variety of use cases is another key aspect of scalability. Many organizations start by filtering inbound and outbound traffic rather than performing east-west inspection. Filtering ingress and egress traffic is a foundational aspect of network security and low-hanging fruit to reduce risk and block threats. However, current architectures make it difficult to scan east-west traffic to prevent threats from moving laterally. Specifically, the need to route intra-virtual private cloud (VPC) traffic back to the VPC perimeter for inspection can negatively impact performance. Solutions that offer support for both inbound/outbound protection and east-west inspection at scale without performance impacts can help organizations enhance their security protections over time.

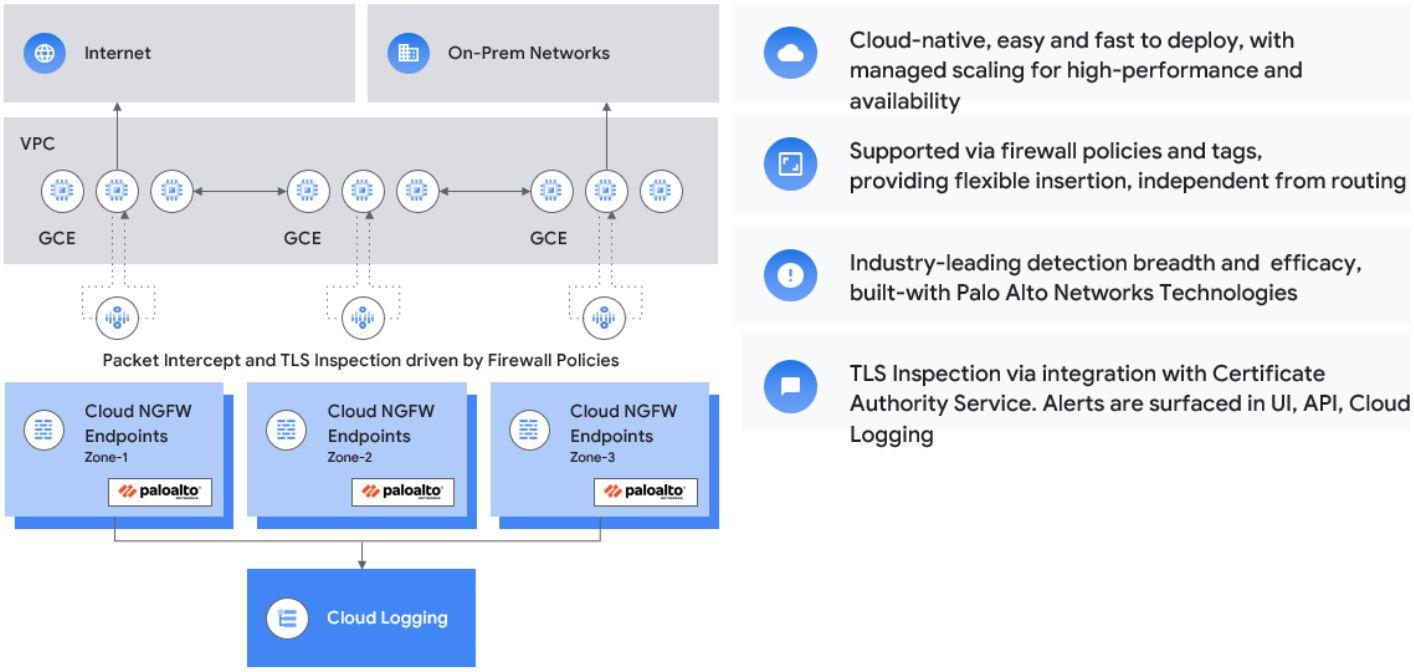
Strong Security

While cloud service firewalls have been prioritized for ease of use and scalability, third-party vendors have often been used to enhance the native security capabilities in these tools. In fact, Enterprise Strategy Group research found that 77% of organizations using intrusion prevention in the cloud do so to augment security group or network firewall security capabilities from CSPs. Yet adding tools to enhance security only contributes to complexity. Cloud firewalls must offer more than just stateful inspection; Layer 7 visibility and advanced threat prevention, supported by robust threat intelligence to block sophisticated threats, are also required.

Google Cloud NGFW Enterprise, Powered by Palo Alto Networks

Google Cloud NGFW Enterprise, powered by Palo Alto Networks, delivers a new approach to network security deployment and administration in the cloud through its distributed architecture, network security posture controls, and best-of-breed threat prevention (see Figure 2). This approach increases ease of deployment and scalability, while improving security effectiveness. Rather than choosing between a CSP or third-party firewall, Cloud NGFW Enterprise gives customers a third choice when considering how best to secure their IaaS environment.

Figure 2. Google Cloud NGFW Enterprise, Powered by Palo Alto Networks



Source: Google and Palo Alto Networks

Google Cloud NGFW Enterprise includes global network firewall policies and regional network firewall policies, identity and access management (IAM)-governed tags combined with network firewall policies for microsegmentation, address groups to simplify rules for ingress and egress control, filtering for incoming or outgoing traffic from or to specific domains, and Google Cloud Threat Intelligence. Critically, it also provides advanced Layer 7 security capabilities that protect Google Cloud workloads from threats and malicious attacks. The intrusion prevention service powered by Palo Alto Networks, together with Transport Layer Security (TLS) interception and decryption provided by Google, offers threat detection and prevention from malware, spyware, and command-and-control attacks for both encrypted and non-encrypted traffic.

The distributed architecture of Cloud NGFW Enterprise provides stateful firewall policy enforcement close to each workload to enable zero-trust security architecture. This enables simplicity, scale, and performance by streamlining deployment with zero routing or network architecture changes. The solution is cloud-native, fully managed by Google, with unified perimeter and microsegmentation protection, and low latency traffic inspection.

Network security posture controls help organizations scale more effectively by enabling them to set a preventative posture that follows the organization. The solution offers machine learning-driven recommendations for posture improvements, as well as frictionless incident response with IAM-provisioned tags. In addition to global firewall policies that enable rules to be grouped into a policy object applicable to all regions, as well as regional network firewall policies that enable rules to be grouped into a policy object applicable to a specific region, Cloud NGFW Enterprise supports hierarchical firewall policies. These policies enable rules to be grouped into a policy object that can apply to Organization and Folder level, protecting many VPC networks in one or more projects, supporting consistency in creating and enforcing firewall policy across the organization. By applying these organization or folder-level policies, security teams can be assured that policy is being deployed and followed across the organization and departments, even moving at cloud speed. Further, firewall rules logging lets security teams audit, verify, and analyze the effects of firewall rules and obtain complete visibility into their cloud environment with both allowed and denied traffic.

Through its partnership with Palo Alto Networks, Google Cloud NGFW Enterprise applies Palo Alto Networks threat prevention to protect networks against high-volume and sophisticated attacks by implementing multiple layers of prevention, confronting threats at each phase of the attack. Palo Alto Networks' threat intelligence comes from 65,000 customer organizations analyzing 8.6 billion transactions daily. The combination of Cloud NGFW Enterprise with Palo Alto Networks enables organizations to protect Google Cloud networks from internet-bound threats, while also providing lateral inspection across cloud workloads. Further, by making it easier for customers to apply east-west protection in their Google environment, Cloud NGFW helps ensure that threat actors attempting to move laterally through the environment are blocked. Whenever a threat is detected, corresponding threat logs are generated and automatically sent to Google Cloud Logging to provide centralized visibility.

Conclusion

Security teams today have an incredibly challenging job: They have to protect their organization from a variety of threats while not impeding business innovation or agility. Tools that make it easier for security teams to accomplish these goals are more important than ever and should be prioritized. The partnership between Google and Palo Alto Networks bridges the gap between the convenience and usability of CSP firewalls and the proven threat prevention of third-party tools. Cloud NGFW Enterprise from Google, powered by Palo Alto Networks, offers simplicity, scalability, and strong security to help organizations take full advantage of cloud infrastructure while minimizing the risk of malicious cyberattacks.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com