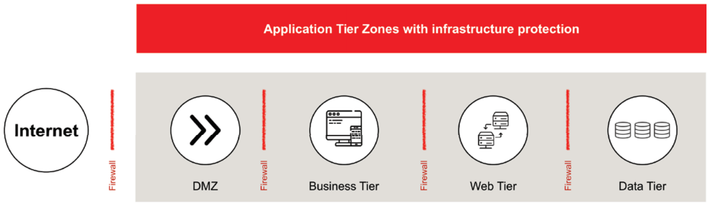
SHIELDX

CISO Guide to Fixing a Flat Network

The cloud is upending infrastructure. But what does that mean exactly?

For more than twenty years, a typical application design comprised of a basic set of four zones:

- Application
- Web
- Middleware
- Database



IT and security teams, concerned about the threat of hackers spreading laterally after initial penetration, separated these zones with firewalls to eliminate a flat network. Or worse, the flat network remained—with nothing more than a single firewall between the world and the internal network—and exposed enterprises to all kinds of security risks.

Suddenly, the plot thickens: your CEO, CFO or CIO mandates you move to the cloud to take advantage of its scale and economics. As great as the cloud may be, this is a moment when you're likely to feel like your cloud security options are limited.

To meet that C-level mandate, you could address the problem with:

- **Traditional firewalls:** yesterday's technology. In truth, a physical firewall is essentially the perfect design to prevent scalability, increase costs and require an army of expensive resources to manage policies.

- **Virtual firewalls:** You'll find that removing the physical chassis doesn't eliminate the scaling issue. For example, if you just need more encryption, you'll need to buy more firewalls just for that capability. Further, like their physical brethren, they come out of the box requiring extensive configuration and ongoing management.

- **Agents:** Some vendors promise to segment your cloud environment with agents. But agents introduce new software and complexity. Do you really want more software running in the background on every machine in the house?

Choose any of these options and you're stuck with:

- No visibility
- No policy automation
- No control automation
- No viable path to support the business as it moves to the cloud

THE LOGIC OF APPLICATION SECURITY

In an April 2019 report, Gartner noted that "Security zones in microsegmentation are determined by application logic." This is a critical insight: decisions about which elements in a network are allowed to interact are driven by business requirements, not hardwiring, equipment choices, or the whims of your cloud provider.

CHECKLIST

What does this mean in practical, technical and business terms for cloud security solutions? You should:

□ Insist on a security solution that understands virtual objects by what they contribute, not along traditional application tiers, ie, not by IP addresses. Even if an object's IP address changes, you know it still belongs to the same virtual group. Further, you know that this group requires a specific security policy or control. By contrast, tools that focus on IP addresses and ACLs condemn security teams to a perpetual cycle of manual policy and ACL updates because they are misaligned from a fundamental, architectural point of view.

□ Deploy a tool that allows you to describe security policy in business terms—not as ACLs or groups of IP addresses. Expressing a policy should be a simple statement of business intent. For example: always restrict reporting workloads from the transaction database. If your rules contain IP addresses, you're a reboot or a tweak away from a potentially disastrous error.

□ Leverage AI/ML for workflow—not just threat detection—to build and maintain policies. Today, many large enterprises employ half a dozen FTEs solely to update firewall rules. Imagine redeploying these employees in more strategic roles.

□ Embrace DevSecOps. If developers can tag workloads by policy and the tags are applied automatically as workloads are spun up downstream, security becomes quickly and easily embedded into the development process. As the DevSecOps name implies, this instantly operationalizes security.

□ Seek a microsegmentation solution that doesn't overlook essential security controls including threat and malware prevention, information loss prevention, URL filtering and more.

THE PROMISE OF MICROSEGMENTATION

To play to cloud's inherent strengths, you'll need to integrate such cloud-native concepts as containerization, microservice application architectures, and microsegmentation.

Microsegmentation is especially relevant to the challenges of shifting security into cloud scenarios, as it's a software-based method for isolating various endpoints on a larger network into smaller segments. While basic segmentation can be achieved using physical networks separated by routers and switches, a software-based approach means that very fine-grained "micro" segments are possible. One container providing a single service as part of an application segmentation scheme can communicate only with other containers that are allowed to call that service. A "micro-perimeter" including deep packet inspection of the sort you'd find in next-gen firewall can add protection between these individual services.

There are, as you'd expect, different ways to build microsegmented architectures. One simple approach is to manipulate the ACLs (Access Control Lists) of servers or containers on the network. The ACL is restricted to only those entities that should sit on a given microsegment.

While there are clear benefits to ACL-based segmentation, considerably more agile and secure microsegmentation is possible using some of the virtual network capabilities of environments such as Cisco (Underlay Networks) and Azure (User-Defined Routes).

THE SHIELDX CLOUD SECURITY ARCHITECTURE

While real cloud security is a must, the road to cloud so far has seen early adopters leave themselves insufficiently protected as traditional protective zones have been collapsed to a single server plane, along with a hope and a prayer that all the traffic reaching the company's servers is funneled through a battery of virtual firewalls.

For a more coherent approach, ShieldX Elastic Cloud Security uses microsegmented connectivity and a container-based, microservices architecture to replace the tiered zones and the monolithic firewalls that protect them. You still have zones, but they are automatically generated and maintained, individually defined for separate business applications, and scaled on the fly on a per-zone basis.

The approach tackles the full breadth of the cloud security problem. ShieldX uses machine learning to automatically discover workloads in an environment, configures microsegments accordingly, then automatically rolls out policies to keep those workloads secure. A full set of API's allow third-party elements such as intrusion protection systems to be incorporated within microsegments.

True to a cloud-native approach, ShieldX implements its components using containers, meaning that scaling up services can occur on a granular level. If deep packet inspection is reaching a maximum load, a new instance of that service alone can be launched, as opposed to a transplanted traditional zone approach, where an entire appliance-based firewall virtual appliance must be spun up. ShieldX can manage segments that tie together disparate workloads, such as physical container hosts, Kubernetes pods (with full label mapping), VXLAN isolation, or container network interfaces (CNI) such as Flannel or Calico.

Finally, ShieldX goes beyond the limitations of ACL-based microsegmentation to provide deep packet inspection, rivaling the capabilities of standard next-gen firewalls, but without the performance penalties that can occur when NGFWs are placed at network choke points.

In short, ShieldX security services are literally embedded in the pathways among application components and these pathways are controlled to provide separation among components. The scaling advantages of the cloud are preserved without sacrificing security. Indeed, If you were designing multi-cloud security from scratch for the next generation of cloud deployments, you'd see soon enough that ShieldX has already done it for you.

SHIELDX

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

November 2018