Zener

Saving costs, improving flexibility and hardening security with Software Defined Firewalls

An executive brief from Zener

Software Defined Firewalls (SDF)

As software plays a larger role in the digitization of the enterprise, so has the need for efficient IT operations and IT security has grown accordingly. New agile development processes, the flattening of the datacenter, and the increased usage of the public cloud infrastructure calls for new best practices within IT security.

This briefing describes the benefits of Software Defined Firewalls based on a centralized policy with decentralized enforcement.

Having centralized firewalls is like thinking about the skin as the only protection humans are equipped with. In reality, the skin is only the first layer of defense. When bad actors/bacteria enter the body, white blood cells quickly come to the rescue. Zener is the equivalent of the white blood cells in your network.

This white paper outlines how Zener can help improve security while operating at the speed of the business.

DevOps, Cloud and Agile development change the security axiom

To keep pace with the modern security threat profile and to efficiently protect business applications and data, new security measures are needed. The move from a hierarchical network topology to the flattened datacenter, from on-premises to hybrid operations, monolithic to distributed applications, all require an approach to IT security that can match these new complexities. Enter SDF.

The need for distributed SDF

Statistics show up to 80% of IT security budgets go to perimeter intrusion prevention. Previously the locations of business assets were static and placed inside an easy-to-understand perimeter. With single entry-points and hierarchical network paths, it made sense to focus on border control. Not anymore.

Monolithic networks and services will rapidly become a thing of the past. In the world of BYOD (Bring Your Own Device) and cloud, security perimeters pop up and down continuously, around shrink-wrapped deployments, all defined within infrastructure automation at high speed.

To match the complex threat surface of IT assets, we need to embrace the complexity and distribution of the assets with a new kind of firewall across all endpoints of the network.

Generally, the best way to protect a moving target is to stay close to the target. This is also the case in IT. Any asset from high-level servers to low-level API-calls can wear its own protection, just like the white blood cells in our body.

Zener offers a cost-effective way to achieve this kind of protection.

Distributed SDFs promise protection at all system levels

Firewalls, traditionally thought of as border control for the broader network perimeter, can be used at all levels of a system, from individual host protection down to individual API-call filtering. Host and API-call filtering are examples of local protection. Using technologies like **netfilter** and **BPF** makes it possible to add protection without impacting the overall performance of the network.

A Zero Trust model enabled

John Kindervag, Principal Analyst at Forrester Research has advocated for a "Zero Trust Model"[(1)], a model without implicit trust. SDFs allows for designing a network with "deny all" as the default. By only allowing access to assets that have been explicitly defined by a human, one is one big step closer to a Zero Trust model.

The implementation of this can range from a very simple, two-tier system, to a highly fragmented and segmented network with many groups or security zones.

A Win-Win: Many more firewalls, far less complexity

Perimeter-only protection leads to different firewall device types and the proliferation of firewall rules. The complexity of these rule-sets leads to bottlenecks for operations, hindering the speed of development. Network teams struggle to understand the consequences of which ports to open where. Support for protocols and variations like IPv4 and IPv6 makes firewall management even more complex. Complexity means risk.

Zener increases the number of firewalls, while the level of complexity remains as low as managing one. It doesn't matter whether a datacenter has 50,000 or 100,000 machines. Logically the humans only need to administer one single firewall. Automation takes care of

the complexity associated with local enforcement. The humans only need to interface with Zener and can trust Zener automation to handle the complexity.

Zener uses the local OS firewall already in place (for instance, in the form of netfilter for a Linux host). This means no need to purchase additional hardware. Effectively, security measures can increase with 100x or 1000x at no additional cost, while reducing complexity. A unique win-win.

Benefits of SDF

Key benefits of adopting a distributed SDF include:

- Increased **security**
- Increased **speed**
- Significant **cost savings**

Increased security

Zero Trust model. "Deny all" traffic can become a reality. Only traffic explicitly defined will be allowed. All rules can have change control and rule intentions documented with Zener. This reduces misunderstandings between teams and risk for allowance of unnecessary or undesirable traffic.

An additional layer of defense is implemented. Even if the adversaries succeed in getting inside the company perimeter this by itself does not imply access to any asset. This reduces the number of attack vectors.

Zener allows for **Unified firewall rules,** reducing the chance for misconfigurations. This increased simplicity makes the rulesets human readable and understandable. From this follows easier auditing to prove compliance, and reduced risk when making changes

No more big bangs! A traditional setup where new firewall rules need to be applied high up in the hierarchy leads to a big bang change. Phased, incremental rollouts become feasible with distributed SDFs.

Increased speed

The end of TCAM tables. SDF transforms centralized firewall complexity to local simplicity. If the perimeter firewall no longer needs to worry about all potential routes inside the network, what is left are fewer and simpler rules. SDF allows for the use of Linux commodity switches, like the one proven by Linkedin [(3)]. This implies a move away from expensive and closed vendors.

Network teams typically spend 60% or more of their time on port management due to the complexity that follows a traditional and vendor-specific approach. The simplicity offered by SDF in combination with commodity Linux switches and its capability for unified firewall rules will free up valuable time that can be spent on working more proactively, and further reduce the response time spent on port management.

No more surprises. Zener means centralized firewall rules. Combined with change and version control, in known DevOps style, the chances of misconfigured port management is greatly reduced and the team will spend less time on fixing or understanding what has happened. With only explicit traffic allowed change management becomes easier and much less risky.

Support for increased uplink and resiliency. Companies that combine SDF with a flatter network topology the multiple entry points into the datacenter not only greatly increase resiliency as there fewer points of failure, but it also increases the uplink speed. Instead of having one 40 Gigabit uplink, one can now have ten 40 Gigabit, a total of 400 Gigabit uplink.

Increased insight into traffic pattern. Denying all traffic by default and controlling traffic locally makes debugging easier. If a packet is rejected, it is reported by the host, and one can quickly look up the specific rule for this asset to understand why/what rules apply to the asset to understand why and where this rejected traffic came from.

Increased performance and agility. SDF makes it easy to create application-specific quality of service since resources can virtually be moved between environments. Under heavy load, automation can manage and move hosts and resources to best accommodate traffic patterns and performance.

Improved quality of service. Automation can optimize the quality of service by moving resources to where needed the most. A development host, in a flat network topology, can quickly be reconfigured to be a production host. This improves both quality of service and capacity utilization.

Significant cost savings

A distributed SDF solution reduces the complexity found in today's perimeter firewall approach. This translates into less need for advanced TCAM table support. Without compromising on performance, this opens the door for commodity Linux switches replacing closed products from vendors like Cisco, Juniper, and Arista. For a large datacenter, this can represent savings of **hundreds of millions of dollars**[4] in hardware costs.

Next steps

To learn more about Zener and how a distributed Software Defined Firewall can help your organization today, read more on www.zener.io, or send an email to zenerwhitepaper@northern.tech.

Resources and links

1. https://www.forrester.com/report/The+Eight+Business+And+Security+Benefits+Of+Zero+Trust/-/E-RES134863

2. https://code.facebook.com/posts/203733993317833/opening-designs-for-6-pack-and-wedge-100/

3. https://engineering.linkedin.com/blog/2016/06/openswitch

4. http://www.businessinsider.com/how-linkedin-is-shrugging-off-the-175-billion-hardware-industry-2016-10