Zener

EXECUTIVE BRIEFING

Zener - Software Defined Firewalls

Software Defined Firewalls (SDF)

As software plays a larger role in the digitisation of the enterprise, so the need for efficient IT-operations and security have grown accordingly. New agile development processes, the flattening of the datacenter, and public cloud call for new best-practises within IT-security. In this briefing, we describe the benefits of taking an approach to security based on centralized policy, with decentralized enforcement, in the form of a distributed Software Defined Firewall (SDF) solution.

Zener is a scalable distributed SDF solution.

Traditionally, having only a single centralized firewall is like thinking about the skin as the only protection humans are equipped with. We all know that the skin is only the first layer of defense. If something bad enters the body our white blood cells will come to the rescue. Zener will be the equivalent of the white blood cells in your network.

DevOps, Cloud and Agile development will change the Security axiom.

To keep pace with the modern security threat profile, and to efficiently protect business applications and data, updated security measures are needed. The move from a hierarchical network topology to the flatter datacenter pioneered by Facebook[(2)], from on-premise to hybrid operations spearheaded by AWS, and from monolithic to distributed applications made easy by containers requires an approach to IT-security that can match the complexities of deployment with continuous updating.

The Need For Distributed SDF

80% of IT-security budgets typically go to perimeter intrusion prevention. Previously the locations of business assets were static and easily placed inside an easy-to-understand perimeter. With single entry points and hierarchical network paths, it made sense to focus on border control.

However, monolithic networks and services are rapidly becoming 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 more complex threat surface of IT assets, we need to match the complexity and distribution of the assets with a new kind of firewall, across all the endpoints of the network.

The best way to protect a moving target is to stay close to the target. So also in IT. Each Asset from high-level servers to low-level api-calls can wear its own protection, just like the white blood cells in your body.

A cost-effective way to achieve this kind of protection is through Zener and the concept of distributed Software Defined Firewalls (SDF).

Distributed SDFs as local 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** it is possible to add protection without impacting the overall performance of the network and application performance by optimizing stateful and stateless connectivity, and only filter on inbound traffic.

Enables a Zero Trust Model

John Kindervag, Principal Analyst at Forrester Research has advocated for a “Zero Trust Model[(1)], a model in which there is no implicit trust. With SDF one can design a network with “deny all” as the default. By only allowing access to assets that have been explicitly defined by a human in the IT-organization, one is one step closer to a zero trust model.

A Win-in: Many More Firewalls, Less Complexity

Perimeter-only protection easily leads to various firewall devices and thousands of firewall rules. The complex of these rulesets lead to bottlenecks for change and operations, hindering speed of development, as the network team must spend time understanding the consequences and which ports to open where. Supporting for protocols and variations like ipv4 and ipv6, makes firewall management more complex. Complexity means risk.

With Zener SDF one can dramatically increase the number of firewalls, while the level of complexity goes to just 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 will take care of the complexity assumed with local enforcement for you. The humans only need to interface with Zener, and allow Zener to manage the complexity.

SDF means the firewall is already in place (for instance in form of netfilter for a Linux host). There is no additional hardware to purchase. In effect this means security measures can increase with 100x or 1000x at no additional cost, while reducing complexity. A unique win-win.

Benefits of SDF

Key benefits from adopting a distributed SDF include:

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

Increased security

“Deny all” traffic as the new default can become a reality. Only traffic approved by a human administrator will be allowed. By using Zener, all rules will have change control and rule intentions explained. This reduces misunderstandings between teams and also reduces the change 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 they still don’t have access to any asset.

Zener allows for **Unified firewall rules,** reducing the chance for misconfigurations. The increased simplicity also makes the rulesets human readable and understandable. From this follows easier auditing to prove compliance.

No more big bangs! Phased, incremental roll outs become feasible with distributed SDFs. As opposed to traditional setup where new firewall rules need to be applied high up in the hierarchy leading to a big bang change, new rules can now be rolled out in a phased way.

Increased speed

The end of TCAM tables. SDF transforms centralized complexity to local simplicity. If the perimeter firewall no longer need 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 as proven by Linkedin [(3)] and a move away from expensive and closed vendors.

Network teams may spend 60% or more of their time on port management due to the complexity that follows a centralized 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 reducing the response time spent on port management.

No more surprises. With Zener, all firewall rules are in one place. Combined with change and version control, in known DevOps style, the chances of unintended port management is greatly reduced and the team will spend less time on fixing or understanding what has happened. Only explicit traffic is allowed.

Support for increased uplink and resiliency. For 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 increase the uplink speed. Instead of having one 40g/bit uplink, one can now have ten 40gbit, a total of 400g/bit uplink.

Increased insight into traffic pattern. By denying all traffic by default and controlling traffic locally, debugging becomes easier. If a packet drops, it is reported at local level, and one can quickly look up the specific rule for this asset to understand why / what rules apply to the asset to see 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, one can, with automation easily manage and move hosts and resources to best accommodate traffic patterns and performance.

Improved quality of service. Automation allows for optimizing quality of service by moving resources where they are needed the most. A development host, in a flat network topology, can quickly be reconfigured to become a production host. This improves both quality of service and capacity planning.

Significant cost savings

A distributed SDF solution greatly 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 open the doors for commodity Linux switches replacing closed 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 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