Software-based Segmentation
An Inside-out Approach to Achieving Security Bliss
# Contents

## PART ONE

- **Say Goodbye** to the Legacy Firewall Graveyard 03
- **Solved!** 3 Problems with Legacy Firewalls 04
- **4 Segmentation** Basics 10
- **Myth vs Reality:** 5 Segmentation Myths Debunked 11

## PART TWO

- **Reduce Risk** on the Inside 12
- **Your Zero Trust Checklist:** 6 Ways to Gain Explicit Control 16

## THE BOTTOM LINE 17
We get it. You are tired of your old, on-prem firewalls. IT environments and security requirements have evolved lightyears ahead of what they were originally built for. And the cybersecurity landscape has evolved, too - attack methods have grown more sophisticated and cybercriminals are more tricky. A decades-old appliance architecture simply can’t stand up to the latest malware, botnet attacks, phishing schemes, social engineering and data extortion.

Did you know? 60% of security experts say their legacy firewalls don’t prevent cyberattacks against critical business and cloud-based applications.

But even with their myriad of problems - they are expensive, immobile and lack visibility, to name just a few - the reality is, legacy firewalls are not going away anytime soon. They serve an important function at the perimeter handling north-south traffic, and provide a hardshell around the organization.

But firewalls cannot manage east-west traffic in on-premises datacenters and in the cloud.

This is a job for software-based segmentation.
Solved!  
3 Problems with Legacy Firewalls

THE PROBLEM: LACK OF VISIBILITY IS A KILLER

The lack of visibility into the flow of data makes implementing and maintaining rules hard. Because of this, firewalls often have extremely long rulesets, and they have a lot of rules that are overly permissive or not even necessary.

THE SOLUTION

Look for solutions that integrate a visual map, asset classification and application dependency mapping with policy creation and management.
Solved!

3 Problems with Legacy Firewalls

THE PROBLEM: FIREWALLS ARE HARD TO MAINTAIN

Application owners and firewall admins rarely know the appropriate IP ports and protocols that need to communicate. So, managing firewalls becomes an iterative, troubleshooting process.

THE SOLUTION

Instead of framing policies around the fixed network “plumbing” like IPs and ports, base them on meaningful attributes like the process an application uses, fully qualified domain names (FQDN) and user identity. This way, the attributes remain the same and your policies will keep working, even if you make a change to your datacenter or move your workload to the cloud.
THE PROBLEM: FIREWALLS LACK AGILITY

Any changes you make to a firewall usually require scheduled downtime. This means when an application owner needs to make a change, they may wait a week or more for the change to be reviewed and implemented during a maintenance window.

THE SOLUTION

Modern IT organizations have moved away from change windows to DevOps models where applications are appearing and updating continuously. Find a technology solution that can be automated using the same DevOps tools that you’re using for the applications themselves. This way, as applications continuously evolve, the security approach adapts along with it.
Let’s talk about the traditional way of doing things. It is complicated. And it is not adaptable. The old-school approach to managing legacy firewalls bases segmentation on location - and that location cannot be easily changed. It is usually based on a hard-coded IP address or routed to a datacenter. This means you physically have to move whatever it is you want to secure behind the firewall, a process that is resource-intensive, risk averse and slow. Cloud migration? Visibility? Adequate security? Forget about it.

Leave your legacy firewalls where they are. Take a deep breath and embrace the new. Software-based segmentation can be easily implemented alongside your existing firewalls, and it is adaptable. With software-based segmentation, you can actually make changes to your environment, datacenter and network, and set policies, based on what you see. And the workload and policies can show up anywhere - in the cloud, datacenter, wherever. Plus, you can apply and adapt your security policy without making changes to the network and with zero system downtime.

YOU CAN TAKE IT WITH YOU.
Would you trust something you cannot actually see? We did not think so. But this is precisely what you are doing when it comes to establishing security policies behind a firewall. You cannot actually see what’s inside. It is like looking at the building without being able to see the people inside.

Software-based segmentation is not based on chance. It breaks up the pieces so you’re totally aware of all activity that your workloads are involved in. Once you know what is inside your environment, you can form a plan and break up the segments into something meaningful and effective based on your specific use cases.
Legacy firewalls simply were not built for change. While they serve an important purpose at the perimeter, like DDoS protection and traffic filtering and inspection, security inside the network is hard to pull off with firewalls. Why? They were deployed as natural choke points, which means every segmentation effort comes with operational roadblocks, like the need to change and remove networks and applications. This is tedious and resource-intensive.

Software-based segmentation can help you overcome these operational challenges and allow you to continue your security practices beyond endpoints and perimeters. First, it features a distributed firewall approach (versus a choke point). Second, it is workload-centric, which means it can collect data from the host system and then apply it to asset classification and a more granular approach to rules, like process-level content and policies. Overall, software-based segmentation is a more adaptable, granular way to protect critical assets inside your network, and requires less effort and resources than firewalls.
Segmentation Basics

Segmentation is more important than ever before. Attack surfaces are bigger, sophisticated attacks, like ransomware, move laterally after a breach, and you have to think about application dependencies beyond the perimeter. But segmentation is not a one-and-done approach.

Here is a look at four common types of segmentation, how they’re different and why you need them:

01 **ENVIRONMENT SEGMENTATION**

separates systems in different development environments, such as Development, QA, Staging and Production. This is a broad version of segmentation where the end goal is to separate systems in different environments to ensure access is limited to only the necessary users and applications. A lot of compliance initiatives require the assurance that non-production systems cannot access production systems.

02 **NETWORK SEGMENTATION**

is an architecture practice of splitting a network into multiple subnetworks, each being its own smaller network segment. Network Segmentation gives IT operators a tool to better control network traffic, boost performance and improve security.

03 **MICROSEGMENTATION**

is a more granular form of segmentation that’s used to isolate workloads from one another and secure them individually. This includes the ability to set segmentation rules for elements such as processes, containers, users, domain names and devices. This approach is superior at controlling east-west traffic and protecting against lateral movement.

04 **IDENTITY-BASED SEGMENTATION**

expands beyond microsegmentation’s ability to protect a single endpoint, device, workload or container by enabling dynamic rules that assess identity - can be the user, device or context - as part of determining whether or not to allow communication. Identity-based segmentation policies can be based on granular settings - not just IP or port - such as tags, OS type or application characteristics.
Myth vs Reality:
5 Segmentation Myths Debunked

**MYTH 01**
Segmentation projects are too difficult and take too long to complete.

**REALITY ::** Starting with visibility and a clear understanding of what is happening inside your environment takes segmentation from months to weeks or even days to complete. Modern segmentation technologies can also use AI to accelerate the process even further.

**MYTH 02**
Segmentation projects require network infrastructure changes and downtime.

**REALITY ::** Software-based segmentation decouples security from infrastructure, so segmentation can be performed independently from the underlying infrastructure without changes or downtime.

**MYTH 03**
Segmentation blocks legitimate traffic in my network.

**REALITY ::** Visualizing your environment and using software-based segmentation policies makes it possible to see the effect that these policies will have on your business activities before real-time enforcement is activated.

**MYTH 04**
Segmentation inhibits user access and introduces unnecessary latency.

**REALITY ::** Using distributed, software-based segmentation policies instead of forcing all traffic through specific firewall chokepoints eliminates network bottlenecks. And more precise policies that are application- and identity-aware reduce the risk of inadvertent user-access issues.

**MYTH 05**
I can’t use the same segmentation tools in the cloud as I use on-premises.

**REALITY ::** If you decouple segmentation policies from infrastructure, the same policies used in the datacenter can also work in the cloud.
Breaches will happen. And they can cripple your business, compromise your data, damage your brand and cost you millions.

For instance, cybercrime is up 600% this year due to Covid-19, with attackers posing as public health organizations through sophisticated phishing schemes.
Companies spent an average of $2.4 million in 2020 defending against an onslaught of malware and web-based attacks.

Still think firewalls can do it all? Think again. Once an attacker has breached a network, environment or datacenter, it will use lateral movement to steal data and wreak havoc, like taking control of application servers or accessing database servers.

In fact, 70% of all attacks now involve attempts at lateral movement.

While firewalls see lateral movement as legitimate traffic happening within a network, software-based segmentation stops it dead in its tracks. A critical component to your security program, software-based segmentation allows you to restrict lateral movement, and, in the event of a breach, make it harder for an attacker to navigate the environment. You get a fighting chance at protecting data and critical applications, decreasing dwell time and even detecting the attacker. This approach is more scalable, easy to use and allows you to quickly implement segmentation without making changes to your network or systems.
Zero Trust is all about who does what to whom, and how they do it. In other words, having explicit control over who does what inside your network. According to Forrester Research, Zero Trust is not one product or platform; it is a security framework built around the concept of “never trust, always verify” and “assuming breach.”

By giving a user access to anything inside the network, you’re automatically granting too much trust, and as a result, putting your entire organization at risk. First, employees often make mistakes, which could have serious security implications. Some even have malicious intent.

Plus, outside of VPN networks and devices, there are a lot of entry points to the datacenter you should consider. Attackers can get inside a network through the production server (like in the case of the SolarWinds breach), an internet-facing application that’s vulnerable, or a vulnerable VPN, to name just a few. In this case, you trust a server just because it’s within the network, but in practice, the attacker can access anything and move laterally without constraint.

**ZERO TRUST DOESN’T HAVE TO BE COMPLICATED.**
In order to achieve Zero Trust in your production network, you have to block all activity that is not explicitly allowed.

This is something that legacy firewalls simply cannot do at a granular level, because it requires identifying attributes at a level deeper than IP addresses and ports.

On the contrary, software-based segmentation allows you to actually see what is happening in detail and create precise, human-understandable policies that include identity.

**Voila. Explicit control.**
Your Zero Trust Checklist: 6 Ways to Gain Explicit Control

Let’s keep it simple. Trust should be based on the size of the segment - and the smaller the segment, the better when it comes to protecting critical data, assets and applications. Here are six steps to Zero Trust without the operational complexity:

01. **IDENTIFY YOUR SENSITIVE DATA**
   using visualization labels.

02. **MAP THE FLOWS OF YOUR SENSITIVE DATA**
   using automated flow and dependency mapping.

03. **ARCHITECT YOUR ZERO TRUST MICRO-PERIMETERS**
   using the right tools for the rapid definition of any segmentation or microsegmentation policy.

04. **CONTINUOUSLY MONITOR YOUR ZERO TRUST ECOSYSTEM**
   through real-time monitoring and analysis.

05. **EMBRACE SECURITY AUTOMATION AND ORCHESTRATION**
   with APIs and technology integrations.

06. **HAVE CAPABILITIES IN PLACE TO UNTRUST SOMEONE OR SOMETHING**
   so if you are under attack, you can easily untrust any machine with pre-set attributes, regardless of the user or segment.
By now, you are probably wondering how you can break-up with your old-school solutions to strengthen your security posture inside your network.

No problem.

Leave your legacy firewalls where they are - they are good at protecting the network perimeter. But the benefits really stop there.

What matters most lives at the core of your organization, the digital assets, data and applications that exist beyond the perimeter - the guts of your corporate infrastructure. Shifting your focus from the inside-out, and implementing software-based segmentation and a Zero Trust framework will give you the visibility and control you need to detect and stop lateral movement, apply granular and adaptable policies, and stop cyberattacks, like ransomware, from propagating your network.

Visit the Guardicore Segmentopedia to learn more about how segmentation can help with ransomware, Zero Trust, cloud security and more.

Learn More →
About Guardicore
Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint.

Guardicore.com | © 2021 Guardicore Ltd. All rights reserved.