Legacy vs. Cloud Native Firewall

5 reasons to consider migrating now

67% of network admins strongly agree traditional firewalls can't effectively provide fast, secure access for remote users.[1] Let's look at the difference migrating to a cloud native firewall makes.

Legacy Firewall **VS.** **Cloud Native Firewall**

1 Access and Security

Legacy firewalls create business risk with unrestricted access

Implicit trust can lead to unrestricted access and risk of **lateral movement**

90% of IT and security admins admit they've applied highly permissive policies[2]

Cloud native firewalls securely connect* without disruption

*With a zero trust approach

Easy to understand, centralized policy management reduces misconfigurations and makes them easier to fix

Cloud-delivered protection ensures policies follow users on and off the network, with seamless connections

2 User Experience and Scalability

Legacy firewalls slow end user experience, and there's no native TLS/SSL inspection

Inspecting all traffic can **throttle performance by up to 50%**

High traffic volume requires **higher capacity or more appliances** in your data center—virtual firewalls have the same capacity limitations as physical boxes

Cloud native firewalls have latency-free, unlimited inspection

True cloud-delivered local internet breakouts for direct-to-internet connections

Zscaler Single-Scan, Multi-Action™ (SSMA) engine analyzes all data and traffic, including SSL/TLS, to apply inline, best-in-class-security without compromising performance

3 Cost[3]

Legacy firewalls have expensive upfront and ongoing costs

$30K–$250K+ per enterprise-grade device—typically 2 devices are deployed per location

$50K+ annually in management upkeep, plus hardware, software, and signature support costs

Cloud native firewalls provide significant cost savings

No hardware or software to manage, only licenses

Zscaler reduces appliances **by 90%** and frees up FTE support **by 74%**[4]

4 Zero Trust

Legacy firewalls are unfit for zero trust

- Dynamically establish strict user authentication
- Ensure integrity and security posture of assets
- Change policies in real time if behavior or the environment shifts

Cloud native firewalls have zero trust options available

- Strict and continuous user authentication and policy checks
- Verify context and determine device and user posture and risk
- Establishes direct, secure user-to-application connections

5 Management

Legacy firewalls are resource-heavy

75% of network admins say it's challenging to manage firewall hardware, upgrades, and deployments[5]

More time spent on patches and updates, deployment, research, remediation, and monitoring

Cloud native firewalls allow more time for critical work

No patching, upgrading, deploying, or excessive IPS fine-tuning with FWaaS

Up to 74% of time spent on maintenance can be **freed to focus on strategic goals**

Ready to take action and route your traffic to a cloud native firewall? Read the IDC report, *Why True Security Transformation Requires Cloud Firewalls*, to get started.

Read the Report

1. Virtual Intelligence Briefing (VIB), Networks Security Survey 2021
2. Zscaler, 7 Symptoms Your Legacy Firewall Isn't Zero Trust Compatible
3. Reported by Zscaler customers
4. Zscaler and IDG, Economic Validation Report, 2023
5. Source: Virtual Intelligence Briefing (VIB), Networks Security Survey 2021

zscaler | Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com