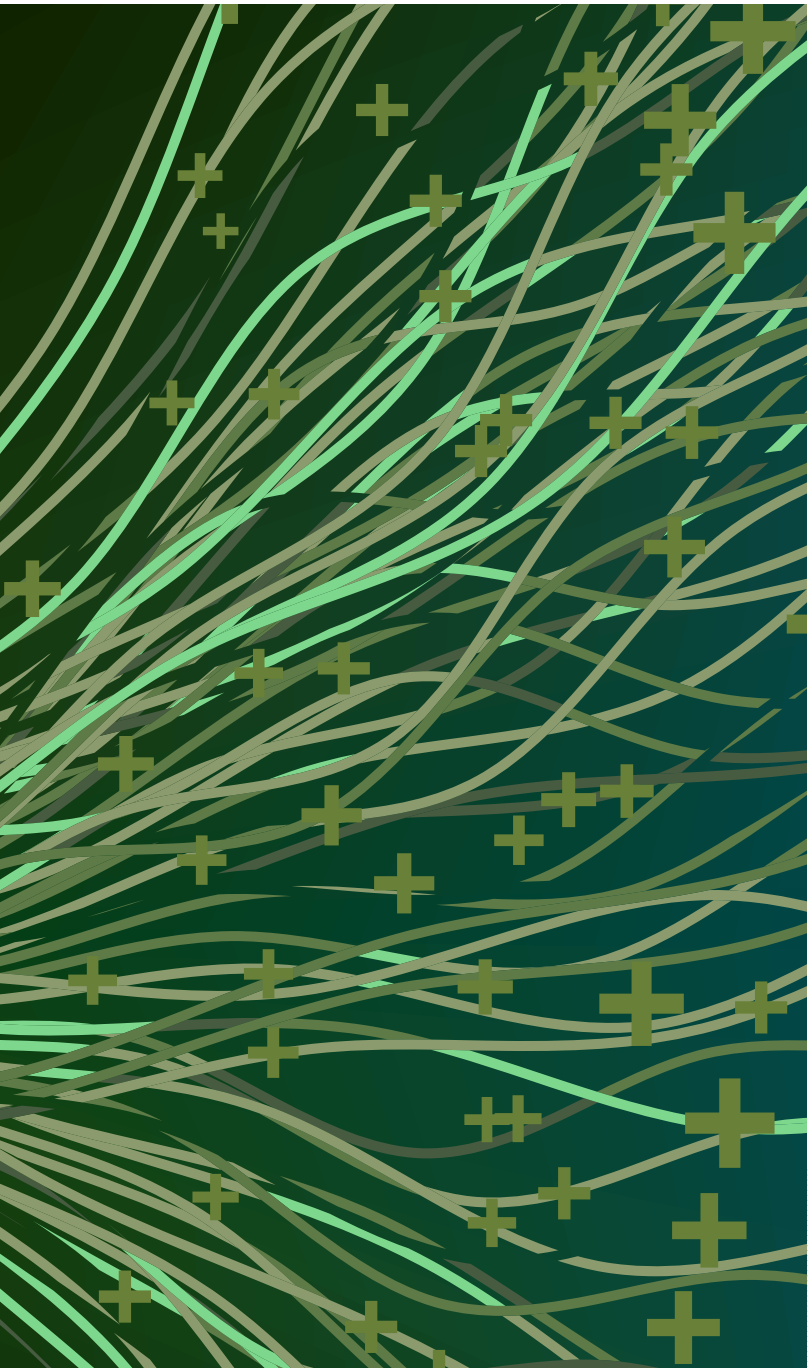
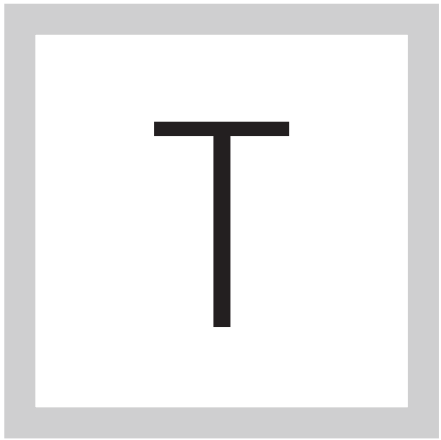


E-Guide

LEARN THE ADVANCED CAPABILITIES YOUR NEXT FIREWALL MUST HAVE

TechTarget | SearchSecurity



O BE ABLE to call your new firewall ‘next generation,’ it must have certain advanced firewall capabilities. Learn what these are in this tip.

LEARN THE ADVANCED CAPABILITIES YOUR NEXT FIREWALL MUST HAVE

John Burke

The term next-generation firewall, as originally conceived, referred to a combination of traditional firewall, application firewall, and intrusion detection/intrusion prevention technologies. It's now so old that it encompasses most firewalls on the maarket. So to say you are looking for something "next generation" when you are in the market to update your firewall doesn't do much to narrow the field.

Given all the other changes going on in enterprise IT -- from the adoption of scale-out architectures and containers to the aggressive shift to integrated hybrid service delivery environments -- firewall shoppers should look for a similarly advanced firewall features: centralized management, distributed enforcement, appropriate scaling, and integration with threat/risk/compliance (TRC) networks.

Centralized management with distributed enforcement is a natural evolutionary change for advanced firewalls in the age of microservices-oriented architectures and scale-out systems. By moving multiple enforcement points in the form of virtual appliances, containers or embedded agents out into an environment, such systems distribute the work of filtering traffic, making security scale-out instead of scale-up. Compute and network resources can be assigned to each enforcement point, as required by the traffic, to and from the parts of the environment they are protecting; more instances can be spun up to meet rising needs, just as more application containers or VMs might be spun up to meet user demand for the service being protected.

Such advanced firewall technologies allow enforcement of policy to follow virtual or containerized workloads even if they move around. They are critical in the emerging private cloud environment (or even any heavily virtualized one) as well as for increased use of public cloud for mission-critical workloads.

The endpoint of distribution is a microsegmentation environment, centered on close control of which users and services can communicate with applications or service components (as well as when and under what circumstances). Anything not directly in the user-facing layer of function is essentially blocked from all but a predefined set of allowable communications

partners. This kind of fine-grained whitelisting greatly improves security against lateral attacks inside an environment, launched from compromised systems against whatever other systems they can reach.

WHAT'S A TRULY ADVANCED FIREWALL?

The issue of scaling is critical. A truly next-generation firewall product should be able to scale as the need for its services scales, with distributed firewalls as just one option. In an age of virtual appliances and containerized virtual network functions, even if you are forced into choke-point firewalls tied to a single place in the network, your next firewall should not be one where you have to decisively over-provision at acquisition in order to meet the needs of your three-years-in-the-future selves. You should be able to buy at the size you need now and grow by adding resources to instances, or spinning up additional containers or VMs to create load-balanced clusters of service nodes, and (possibly) paying to license new tiers of function.

To be sure, there are still scales at which custom silicon and hardware assists are necessary for top performance; there are just fewer of them over time. For these situations, though, long-range overprovisioning can still be a key strategy.

Cloud-based firewalling will be increasingly important as a first line of filtering for enterprises of all sorts. They do not eliminate the need for on-premises defenses, but cloud firewalls do reduce the load on and change the role and scale of that technology.

The cloud will be crucial to robust defense in another way as well: It will allow you to leverage your peers. A truly advanced firewall should have a global TRC network behind it helping identify key threats as soon as they emerge. This TRC network can attach risk and mitigation intelligence to those identifications, to assist you in maintaining auditable compliance.

Many firewalls on the market today that are termed next-generation firewalls do not possess truly advanced firewall features worthy of being termed "next generation." To be truly deemed next gen, a firewall must be tuned up and refactored to meet the needs of the emerging enterprise environment. Your next firewall should be forward looking on questions of control, distribution, scale and cloud capability so it doesn't get in the way of that evolutionary shift.

JOHN BURKE is CIO and principal research analyst with Nemertes Research. With nearly two decades of technology experience, he has worked at all levels of IT, including end-user support specialist, programmer, system administrator, database specialist, network administrator, network architect and systems architect. He has worked at The Johns Hopkins University, The College of St.

Catherine, and the University of St. Thomas.

Home

Learn the advanced capabilities your next firewall must have

Home

Learn the advanced capabilities your next firewall must have

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.