For: Security & Risk Professionals

Market Overview: Network Segmentation Gateways, Q4 2013

by John Kindervag, December 12, 2013

KEY TAKEAWAYS

Forrester's Zero Trust Model Builds Security Into Networks By Default

Current security designs often feature a multitude of security controls overlaid on top of the network, resulting in a poorly managed, poorly operated, and outdated security program. A Zero Trust network architecture allows infrastructure and security pros to improve the management and optimization of the network.

Network Segmentation Gateways Sit At The Center Of The Network

Forrester envisions the development of a new product category called a network segmentation gateway, which takes all of the features and functionality of individual, standalone security products and embeds them into a single solution. These are gateways whose purpose is to segment modern networks securely based upon data type and toxicity.

The SG Market Is Evolving With No True Solution

Not every functionality Forrester envisions for the segmentation gateway is here today, but many vendors are developing products that are delivering on key aspects of the vision. Today's market landscape features large vendors with acquired technology, established security standalones, and disruptive startups and new entrants.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 | Fax: +1 617.613.5000 | www.forrester.com

Market Overview: Network Segmentation Gateways, Q4 2013

Tools And Technology: The Security Architecture And Operations Playbook

by John Kindervag
with Stephanie Balaouras, Rick Holland, Heidi Shey, and Kelley Mak

WHY READ THIS REPORT

Because of the increasing demand for Zero Trust networks, Forrester envisions the development of a new product category called a network segmentation gateway, a product category that is much more than a “next-generation firewall.” A segmentation gateway (SG) takes all of the features and functionality of individual, standalone security products and embeds them into a single solution. By embedding a packet-forwarding engine, a network SG becomes a device that can sit at the center of a Zero Trust network — a streamlined network that segments and protects sensitive data in microperimeters, enables the secure adoption of mobile technology and cloud services, and ensures continuous network analysis and visibility for situational awareness. This report helps S&R professionals understand how network segmentation gateways have matured, what benefits they offer, and details the vendor and solution landscape.

Table Of Contents

Notes & Resources

Forrester interviewed 15 vendor companies, including BAE Systems Applied Intelligence, Barracuda Networks, Check Point, Cisco Systems, Dell SonicWall, F5 Networks, Fortinet, HP TippingPoint, Huawei, IBM, McAfee, Palo Alto Networks, Sourcefire (Cisco), Unisys, and WatchGuard.

Related Research Documents

Transform Your Security Architecture And Operations For The Zero Trust Ecosystem
September 12, 2013

Build Security Into Your Network’s DNA: The Zero Trust Network Architecture
November 15, 2012

No More Chewy Centers: Introducing The Zero Trust Model Of Information Security
November 15, 2012

ZERO TRUST DEMANDS SECURE NETWORKING

In the traditional hierarchical network, security is an afterthought. Current designs merely overlay existing networks with more and more security controls in an attempt to create a semblance of a secure network. The result? Haphazardly deployed security controls have become a management nightmare made even worse by the fact that they don't do much to address the security issues presented by today's threat landscape and your organization's demand to support disruptive technologies like cloud and mobile. In addition, it's likely that your network and security teams operate in independent silos with goals that are often in conflict.

Justified by the concept of "defense in depth (DiD)," the push to proliferate controls makes good business sense for security technology vendors — there is always a place for a new control in a DiD environment — but demonstrates little benefit to end users. This proliferation has led to an operational nightmare whose ongoing costs are difficult to justify each year given the seeming ease in which these controls are breached by modern attackers. Perhaps a better term for this concept is "expense in depth."

Forrester's Zero Trust Model of information security can embolden infrastructure and security professionals to build security into networks by default. In a Zero Trust network architecture, there is no longer: 1) a trusted and untrusted interface on our security devices; 2) a trusted and an untrusted network; and 3) trusted and untrusted users.[1] A Zero Trust network architecture also has very specific traits; infrastructure and security pros can:

- **Easily manage and segment the network for security and compliance.** Leveraging a network SG builds compliance into the fabric of the network. For example, PCI DSS requires a firewall between a wired and wireless network. Using an SG in a Zero Trust network achieves this by default.

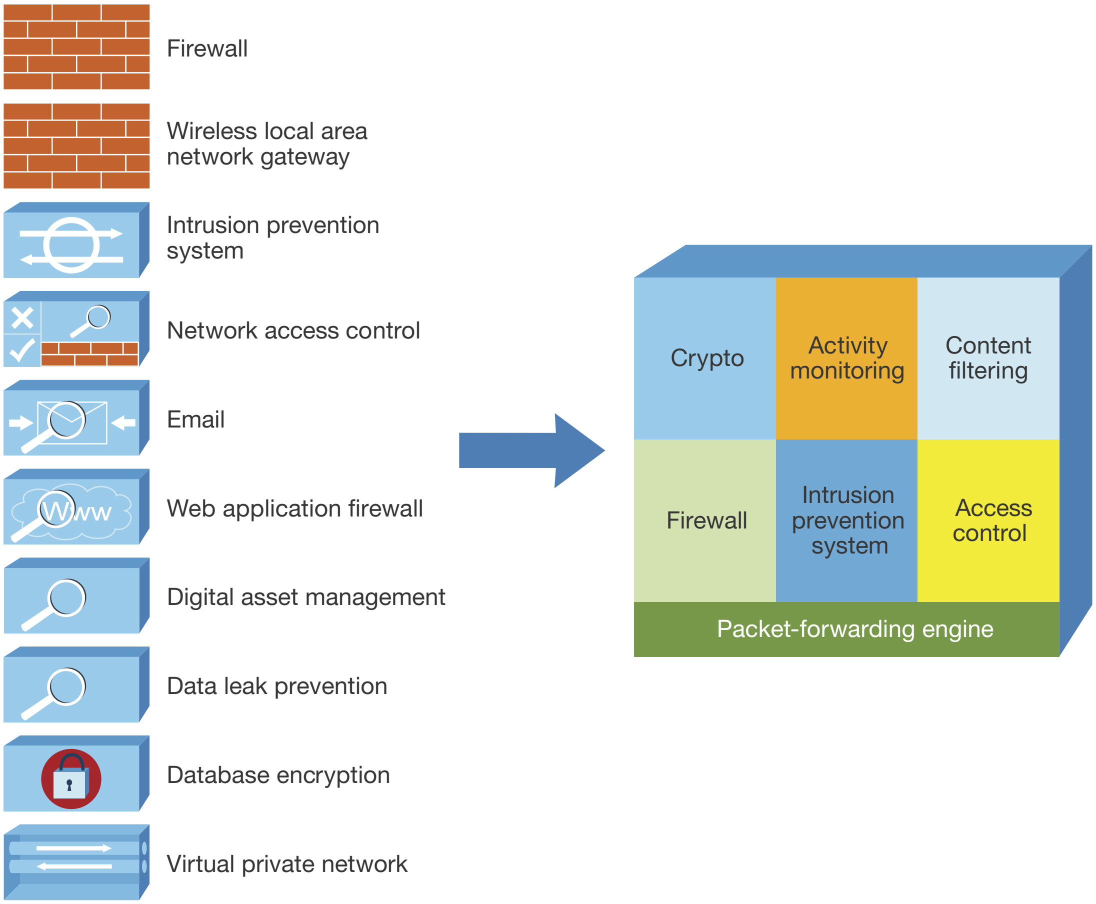
- **Build the network with multiple parallelized switching cores.** The rise of virtualized infrastructure and software-defined networking means that segmented, individualized switching cores are an easily enabled reality. By parallelizing traffic into individual microcore switching infrastructure, improvements in performance can be realized on the network, much in the same manner that multiple core CPUs have improved performance of laptop and server computing.

- **Centrally manage the network from a single console.** Management is the new backplane, and a segmentation gateway eases the control management burden by reducing complexity and consolidating management consoles. Fewer devices equates to improved management.

The Emergence Of Network Segmentation Gateways

Current networks rely on numerous security devices and controls to protect the network and its data. These include firewalls, intrusion prevention systems (IPS's), Web application firewalls (WAFs), content-filtering gateways, network access control, VPN gateways, and other encryption products. For the future-state Zero Trust network, Forrester envisions the development of a new product category called a network SG. This takes all of the features and functionality of individual, standalone security products and embeds them into the very fabric of the SG (see Figure 1). By embedding a packet-forwarding engine, we have a device that can sit at the very center of the network.[2] The SG's larger value lies in its ability to properly segment networks in a secure manner and build security into the very DNA of the network. Presaged by the rise of unified threat management (UTM) and next-generation firewall (NGFW) appliances, the Zero Trust segmentation gateway vision is well on its way to reality.

Figure 1 Zero Trust Network Segmentation Gateway



Source: November 15, 2012, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" Forrester report

61552 Source: Forrester Research, Inc.

Key Features Of Network Segmentation Gateways

Today, Forrester uses next-generation firewalls as segmentation gateways in the Zero Trust networks we help design for our clients. We have chosen not to use the term "next-generation firewall," however, for several reasons. First, the term does these devices a disservice. They are much more than a firewall, next generation or otherwise. In fact, technologically, they are much closer to an IPS with firewall capabilities. At Forrester, we consider NGFW appliances the "next generation" of IPS solutions. Second, we find that applying the moniker "firewall" to these controls encourages security and risk (S&R) pros to deploy them on the perimeter, which is precisely the wrong place for them in an era of deperimeterization and mobility. Because in Zero Trust you place the controls in the center of the network, closer to the data, the devices need a new name to signify their usage, hence the term segmentation gateway. These are gateways whose purpose is to segment modern networks securely based upon data type and toxicity. Using segmentation gateways in combination with the Zero Trust principles, we can now create more robust networks designed to protect our critical data and stand up to modern threats.

To be successful, a segmentation gateway needs to be very high-speed, support multiple high-speed interfaces — 10 Gig today — and have the ability to provide quality of service (QoS) or packet shaping to maintain performance. More specifically, it must have:

- **Integrated inspection and action streams.** Early integrated devices, such as some UTMs, bolted together separate firewall, IPS, or WAF functions to create a sense of integration without its power. This type of management-only consolidation provided operational uplift but didn't provide the speed and efficiency needed in modern networks. In an SG, the vendor integrates all security control functions so that it manipulates the packet once, thereby increasing performance. Additionally, the modern SG must have world-class feature sets for each function in order to provide the efficacy enterprises demand today.

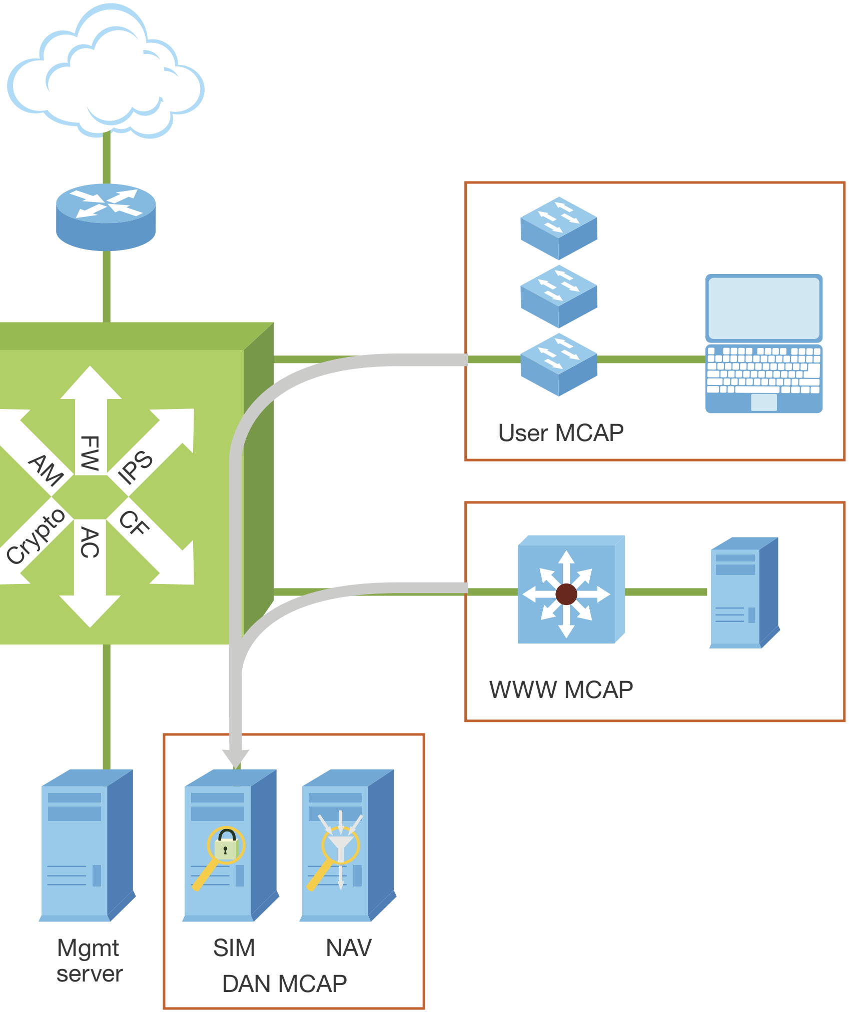
- **A single pane of glass.** Centralized management is fundamental to Zero Trust networking. The abstraction of the management layer into a simple, intuitive, and usable interface is one of the most significant benefits of the maturation of the industry. In Zero Trust, there is functionally one segmentation gateway, regardless of the number of SG appliances that one deploys.

- **Support for software-defined networking.** Software-defined networking (SDN) is the new management paradigm for providing the "single pane of glass" to network device management. In this new age of networks, centralized software — not individual devices — will define how the network functions.[3] Segmentation gateways must be able to interface with SDN controllers to determine how network traffic should flow from a security perspective as well as to automate the creation and enforcement of various microcores and perimeters (MCAPs).

- **Integration with virtual network infrastructure.** Servers were the first part of the IT world to become virtualized. As this type of traditional virtualization reaches critical mass, there will be a need to shift from an old delivery-oriented set of network principles to new orchestration-oriented principles — virtual network infrastructure (VNI). The massive deployment of virtual servers means there is also a significant amount of virtual switching available for the enterprise to leverage. Since each virtual machine has a built-in virtual switch, vendors can create software that will use these unused resources to form the basis for a virtual and highly configurable network, hence the development of VNI.[4] Since VNI is the intelligence in the network transport and the SG is the intelligence in network security, these two solutions must talk so that the network can be securely scalable, securely dynamic, and securely agile to meet the challenges of as-yet-unseen security threats.

- **Lossless packet mirroring.** Inspecting and logging all traffic is one of the primary mandates of Zero Trust. Because the SG sits in the middle of the network, the idea of internal and external networks doesn't exist. Therefore, by sending all the traffic that runs through the SG to a data acquisition network (DAN) where a security analytics (SA) tool can analyze the traffic, Zero Trust can provide the visibility necessary to see potential threat traffic before data can be compromised (see Figure 2). The ability of the SG to send a copy of all the traffic (mirroring) is fundamental to efficiently gaining this visibility.

Figure 2 All Traffic Is Inspected And Logged



Source: November 15, 2012, “Build Security Into Your Network's DNA: The Zero Trust Network Architecture” Forrester report

61552 Source: Forrester Research, Inc.

THE VENDOR LANDSCAPE

The market is still evolving; not every feature Forrester envisions for the SG is here today, but many vendors are developing products that are delivering on key aspects of the SG vision (see Figure 3). Today, we find a market landscape in which:

- **The large vendors bought — not built — technology.** The biggest brands entered this market via acquisition. Saddled with existing technology and old code, most of the majors went outside their shops and opened their pocketbooks to become players in the NGFW — and therefore SG — market. Notably, McAfee acquired Stonesoft, HP purchased TippingPoint (via the 3Com acquisition), Cisco spent big on Sourcefire, and Dell bought SonicWall.[5] Acquisitions seem easier than integration and execution. Only time will tell how these acquisitions will fare.

- **Established security standalones fought to stay relevant.** All the talk about next-generation this and next-generation that left the established standalone security appliance vendors fighting to remain on enterprise buyers' radar. Initially caught unawares by their upstart competitors, these benchmark brands were forced to jump on the bandwagon, much to the relief and benefit of their customers. Check Point Software Technologies champions its Software Blade Architecture; Juniper Networks (who declined to participate in this report) has its SRX product line; and IBM defibrillated its seven-year-old Internet Security Systems (ISS) acquisition to create a product that may compete as a Zero Trust SG.

- **Startups and new entrants disrupted the marketplace.** The trajectory of the firewall market was originally disrupted by the expansion of the idea of a traditional stateful packet-filtering firewall to a more integrated device by early UTM vendors such as Fortinet. This integrated approach was expanded by startups such as Palo Alto Networks, who invigorated a stagnant space with its NGFW positioning. This disruption led to new, unexpected entrants into the space from networking specialists such as the Chinese-based networking powerhouse Huawei Technologies and F5 Networks, a dominant force in the load-balancing sector.[6]

Figure 3 Network Segmentation Gateway Vendor Comparison

Vendor	10 Gig capacity and interfaces	Multiple interfaces	FW features	IPS features	Application awareness	Active Directory integration	User awareness	Autosignature updates	Content filtering	Activity monitoring	Central management console	Web-based management	Compliance reporting capability	VPN gateway	DLP	Inspect encrypted traffic	Purpose-built hardware	Third-party testing	Anti-DDoS mitigation	Advance malware capabilities	Virtual form factor
BAE Systems Applied Intelligence	■	■	■	□	■	■	■	■	□	■	□	■	■		■						■
Barracuda Networks	■	■	■	■	■	■	■	■	■	■	■	□	■	■	□	■	■	■	■	■	■
Check Point	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Cisco Systems	■	■	■	■	■	■	■	■	■		■	■	■	■		□	■	■	■	■	□
Dell SonicWall	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	
F5 Networks	■	■	■	□	□	■	■	■	□	■	■	□	■	■	□	■	□	■	■	□	■
Fortinet	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
HP Tipping Point	■	■	■	■	■	■	■	■	□	■	■	■	■	■			■		■	□	
Huawei	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
IBM	■	■	□	■	■	■	■	■	■	□	■	■	■		□	■	■	■	□	□	■
McAfee	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	□
Palo Alto	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■
Sourcefire (Cisco)	■	■	■	■	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	■
Unisys	■	■	□	□	□	■	■	□		■	■	□	□	■	□	□		■	■		■
Watch Guard	■	■	■	■	■	■	■	■	■	□	■	■	■	■	■	■	□		■	□	■

■ Fully meets criteria □ Partially meets criteria

61552 Source: Forrester Research, Inc.

Vendor Profiles

There are a number of companies that build next-generation firewalls that can be used as segmentation gateways. Currently, the following companies have NGFWs that are being evaluated by Forrester customers to function as SGs:

- **Barracuda Networks.** Barracuda Networks is perhaps best known for its seemingly omnipresent airport advertisements. Traditionally, it has excelled in the small and medium-size business (SMB) content-filtering space. In 2009, Barracuda acquired the Austrian company Phion, a relatively small European-focused enterprise firewall vendor. Since that time, Barracuda Networks has used that technology to create its next-generation firewall. This move has allowed it to begin playing in the enterprise space, especially in European markets.

- **Check Point Software Technologies.** Check Point is one of the originators in network security. Known for creating the stateful firewall, it has entered into the NGFW firewall market with the acquisition of NFR, an early IDS player. This allowed it to create an IPS that would integrate with the existing firewall solutions to create an NGFW. Check Point features are known as "software blades" and allow customers to pick and choose features à la carte that they need for any particular environment. Traditionally a software solution that ran on multiple hardware platforms, Check Point now offers its own integrated hardware/software solution.

  Additionally, Check Point purchased the security appliance assets of Nokia, as the Nokia appliances had become de facto for enterprise Check Point deployments. One of Check Point's acknowledged strengths is an intuitive and scalable management interface. Also, as an early entrant into the marketplace, there are a large number of trained engineers for the platform.

- **Cisco Systems.** Cisco has been a dominant player in the network and security space for many years. It built its ASA CX product on legacy technology, and it has struggled for several years to create a competitive NGFW. Cisco has recently thrown in the proverbial towel and purchased competitor Sourcefire.[7] While insisting it will continue to support the ASA CX product line in parallel with the Sourcefire products, it is difficult to imagine a scenario where these two competitive products thrive within a single entity such as Cisco.

- **Dell SonicWall.** In 2012, Dell purchased SonicWall. Founded in the 1990s and known primarily as a vendor to the SMB market, Dell SonicWall should see a new lease on life. Given the brand recognition and marketing prowess of Dell, the SonicWall products are poised to grab a chunk of the enterprise. Dell SonicWall has very fast high-capacity boxes that hold significant promise within Zero Trust networks. Considering that Dell has acquired complementary companies such as SecureWorks (SIM and managed security services) and Perot Systems (consulting), Dell SonicWall is well positioned as a keystone for future Zero Trust networks.

- **F5 Networks.** F5 Networks is perhaps the world's best known load-balancer company. Leveraging its brand power of its BIG-IP platform, F5 Networks has introduced a firewall module that can reside on the same hardware as its local load-balancing WAF and other assorted modules, allowing it to enter the NGFW and SG markets.

- **Fortinet.** Fortinet was created by the founders of NetScreen (now Juniper Networks), which was the first firewall product to challenge the hegemony of the Check Point/Cisco dominance at the turn of the century. Known primarily as a UTM, Fortinet has been seeing more upmarket traction recently. With the addition of a switch product line, Fortinet is positioning itself to move deeper into the enterprise.

- **HP TippingPoint.** TippingPoint essentially created the IPS market. It was the first major security vendor to create a hardware platform robust enough to be used confidently in-line. HP acquired TippingPoint through the 3Com acquisition. Since that time, there has been some highly publicized turmoil with HP that appears to have contributed to the stunting of TippingPoint's growth curve. With the introduction of TippingPoint's NGFW, an upswing of TippingPoint adoption will become dependent upon HP's sales and marketing execution.

- **Huawei Technologies.** Huawei is a Chinese-based company that has been making waves in the networking space recently. It has deep marketing pockets and is generally more budget friendly than US-based security companies. With the release of an NGFW, Huawei signals its entry into the network security space. Look for it to see growth in this area in Asia Pacific, including Japan (APJ) and among cost-conscious European companies.

- **IBM.** IBM acquired the pioneering security company ISS in 2006 and faced significant challenges when several individuals from ISS's management team quickly left, leading to significant discontent in the installed base. With the acquisition of Q1 Labs in 2011, IBM formed a dedicated security division, IBM Security Systems, and, during this time, it has rebuilt and broadened its security portfolio. IBM has injected new life into the ISS product portfolio (known as the IPS GX), and its reputation is on the mend. IBM has a powerful brand, with an experienced and extensive sales force. If it can continue to execute on its security vision, it stands to become one of the most relevant players in security.

- **McAfee (powered by Stonesoft).** Now owned by Intel, McAfee recently acquired the Finnish company Stonesoft to provide it a well-bred horse for racing in the NGFW sweepstakes. While not well known globally, Stonesoft's offerings are well respected and have an excellent pedigree. Additionally, this will not necessarily overlap with McAfee's existing firewall product, which is proxy-based and of interest mostly to government entities.

- **Palo Alto Networks.** Clearly the disrupter in network security, Palo Alto Networks changed the entire space when it came out with its first next-generation firewall in 2007. Now publicly traded, Palo Alto Networks has seen its market share and reputation expand, and many early Zero Trust adopters choose Palo Alto Networks as their SG.

- **Sourcefire (Cisco).** Sourcefire was founded by the creators of Snort, the most widely used open-source IDS software tool. Now part of Cisco, Sourcefire and Snort are especially popular in the public sector but haven't been as successful in the private sector. Sourcefire should benefit greatly as part of the Cisco family. Cisco knows how to sell to large enterprises and to both IT operations and security pros.

- **WatchGuard Technologies.** WatchGuard is another traditional SMB vendor working to reinvent itself with a broader portfolio. It has significant traction in the midmarket and has the install base and horsepower to become a force in creating SMB Zero Trust networks.

There's More Than One Way To Segment A Network

As enterprises move toward deploying Zero Trust networks, they are choosing to use NGFW appliances as segmentation gateways. But the SG is a concept, not a product. It is any type of gateway that segments traffic, inspects it and limits access, and provides an easy way to support logging and security analytics. There are some interesting technologies that show promise in broadening the current definition of a segmentation gateway. Examples include:

- **BAE Systems Applied Intelligence (formerly BAE Systems Detica).** Detica was acquired by BAE Systems and is now part of a massive global defense contractor. The BAE Systems Applied Intelligence Interactive Content Gateway (ICG) platform provides a gateway to control the flow of various types of content instead of segmenting via traffic alone. More data-centric than network-centric, BAE Systems Applied Intelligence signals the rise of innovative research into how to secure data and content in new ways that can support Zero Trust network architectures.

- **Unisys.** The Stealth product from Unisys is another offering that takes a unique approach to enforcing Zero Trust principles. Stealth conceals protected endpoints and encrypts data as it moves across Stealth-protected networks. As a data-centric offering, the product is not topologically dependent and can work on many types of networks, potentially opening up opportunities in mobility and cloud security.

WHAT IT MEANS

TECHNOLOGICAL ADVANCES PAVE THE WAY FOR MORE ZERO TRUST ADOPTION

As the existing perimeter continues to contract and more and more services are consumed by mobile devices and offered by cloud services, Zero Trust adoption will continue to grow. Mature advanced multifunction security gateways serve as a foundational technology for companies looking to build Zero Trust networks. The development of security gateways gives organizations looking to upgrade their network security capabilities new choices in technology and ultimately topology and paves the way for more widespread adoption of Zero Trust networks.

SUPPLEMENTAL MATERIAL

Companies Interviewed For This Report

BAE Systems Applied Intelligence

Barracuda Networks

Check Point Software Technologies

Cisco Systems

Dell SonicWall

F5 Networks

Fortinet

HP TippingPoint

Huawei Technologies

IBM

McAfee

Palo Alto Networks

Sourcefire (Cisco)

Unisys

WatchGuard Technologies

ENDNOTES

[1] The Zero Trust model is simple: Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted. Thus, security professionals must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic. See the November 15, 2012, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

[2] For more information on building a Zero Trust network, see the November 15, 2012, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture" report.

[3] For more information on software-defined networks, see the November 8, 2012, "Workload-Centric Infrastructure Ignites Software-Defined Networking" report.

[4] For more information on virtual network infrastructure, see the December 12, 2011, "Virtual Network Infrastructure" report.

[5] For more information on the Sourcefire acquisition, see the July 24, 2013, "Cisco's Acquisition Of Sourcefire Has Significant Potential" report.

[6] On September 17, F5 Networks announced its acquisition of web security and antifraud vendor Versafe for an undisclosed sum. With this acquisition, F5 Networks expands its burgeoning security portfolio beyond network layer solutions and into application layer solutions. For more information, see the September 18, 2013, "Moving On Up The Security Stack, F5 Acquires Versafe" report.

[7] For more information on the Sourcefire acquisition, see the July 24, 2013, "Cisco's Acquisition Of Sourcefire Has Significant Potential" report.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 13 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 29 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com. 61552