Fortifying Your Branch Security

Let's look at some data from a recent Ernst and Young security survey[1], where 89% of respondents state their cybersecurity function does not fully meet their organizational needs. More than half of those same respondents then stated they only have an informal threat intelligence program, if they have one at all. Those numbers coupled with the findings of Frost & Sullivan[2] that estimate a shortage of one million cyber security professionals worldwide by 2020, indicate that security is, and will continue to be a critical part of any organization.

Key Findings

Source: Ernst and Young Global Information Security Survey 2017-18

With each passing day, security breaches and attacks are getting more sophisticated and frequent. Due to the rise of cloud-based applications and IoT (e.g. cloud managed HVAC or production line network sensor), the branch office is emerging as a point of concern that can potentially open the entire enterprise to a host of vulnerabilities from the outside.

Securing a branch office is not easy and it doesn't make sense to backhaul all branch traffic through a centrally deployed firewall in the data center; correspondingly, the resulting latency impacts to application performance generally frustrate both IT and the end-users.

Enterprise IT can either manage network security in-house or consume it as a fully managed security service. Regardless of in-house or outside management, there are various challenges to address when multiple security technologies are deployed as separate resources in the branch.

KEY HIGHLIGHTS

The Why, What and How of Enterprise Network Security

- **Why** digital transformations, cloud and IoT are compelling enterprises to transform their existing edge-network security
- **What** are some of the challenges faced by enterprises making the transition to a digital business
- **How** Versa's SD-WAN helps enterprises resolve mission critical challenges with automated soluitions

[1] https://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18
[2] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Enterprise Challenges with Legacy WAN

The legacy branch office network is increasingly becoming the most plausible target for cyber-criminals. The typical branch has evolved to become the hub of major digital services for both business productivity and customer services. Businesses across multiple industries are adopting direct Internet access to facilitate their multi-cloud services and are offering local guest network-based services, such as guest Wi-Fi. Branch offices are hubs of activity, especially in the banking, financial services, retail and manufacturing industries.

While disruptive technologies, like the cloud and IoT, have broadened and diversified the attack surface, branch security architectures have not evolved at a similar pace. Juggling between users demanding faster and more effective ways to access business applications, and legacy WAN architectures that are unable to keep pace with real-time enterprise demands, IT teams are battling a broad set of challenges:

1. **Cloud, IoT and the Public Internet:** The use of cloud-based services, SaaS app adoption and IoT devices have increased dependence on public Internet connectivity. Backhauling branch traffic to the corporate data center is counter-productive, and the latency impacts application performance. Additionally, different branch office locations, or office sizes and the type of applications the users work with, may require different connectivity types (e.g. purely Internet vs. MPLS vs. hybrid).

   The public Internet is not secure enough for mission critical business applications. There are different security requirements per application, depending on where they are being accessed, and over what type of connectivity. This adds significant complexity when using traditional security appliances to create a standard branch security model.

2. **Complexity and Cost:** The branch office network landscape is complex. There are diverse systems and platforms mixed with bits and pieces of technology that, over time, have made their way into the landscape. Cloud and IoT have added yet another layer of complexity.

   Creating and implementing a security strategy for disparate systems and multiple hardware devices is expensive and requires a lot of time and resources. Procuring, deploying and managing point devices for different layers of security at locations without IT/security expertise, often results in very high Capex and Opex. Not to mention – the more complex the system, the more difficult it becomes to monitor, update, manage, maintain and secure all possible loopholes.

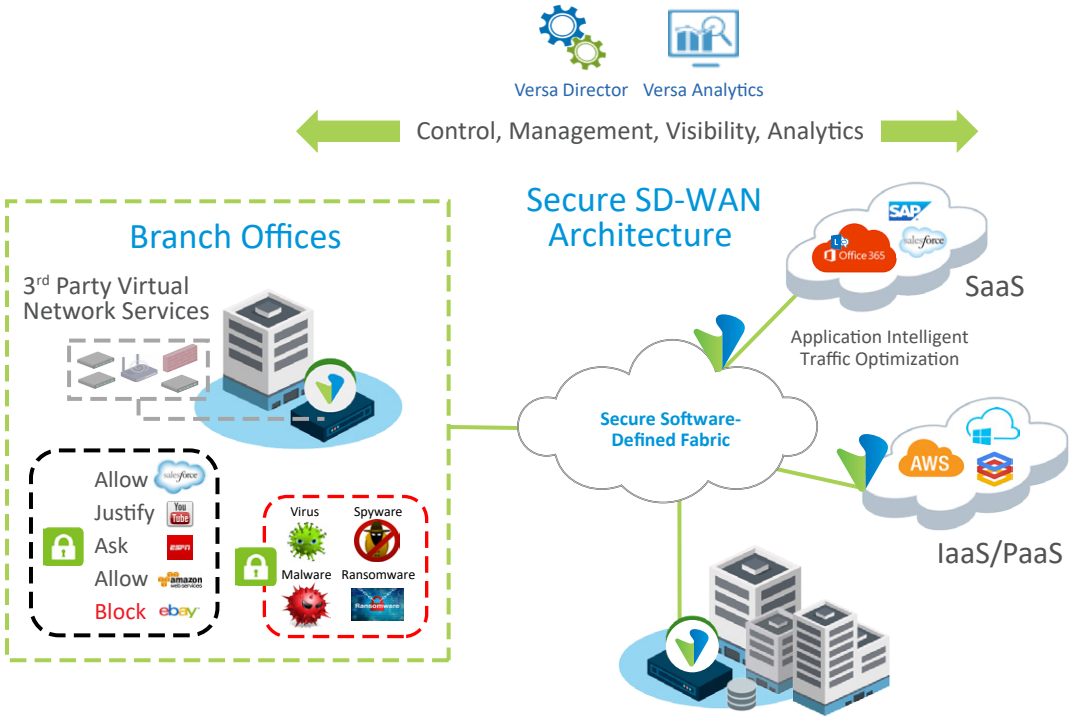
3. **Lack of Visibility:** Most branches currently use a range of connectivity solutions (MPLS, LTE, broadband). Then there is an array of hardware and software components sitting atop this carrier layer. Due to this diversity, third-party network monitoring tools often run into the danger of providing a unified and coherent picture of the networks in real-time. As a result, most organizations end up discovering a breach or an anomaly way after its onslaught. And as most security experts will testify, timely detection and remedial action is critical to minimize the impact of a security breach.

4. **Decentralized Architecture:** Time-to-remediate is critical in the event of a security breach. Every minute lost gives the invader an edge and advantage to strengthen their attack. A centralized management console enables IT teams to dynamically apply role-based access and enforce security policies and configurations per application and centrally manage the security configurations around its applications and networks.

Leveraging Versa's Software-Defined Security

While the above issues with branch security are very real, new technology advances can offset many of these challenges. Software-defined technology can significantly improve the deployment and management of security at the branch.

A core element of Versa Secure SD-WAN is the ability to "software-define" security in terms of form-factor and operations (e.g. policy creation and enforcement). A software-defined security platform separates security functions from proprietary hardware, enabling the use of security functions in software running on commodity x86 servers and white box appliances.



Here are the key features of Versa Operating System (VOS™), enabled by Versa Secure SD-WAN, that helps enhance the enterprise's line of defense:

- **Flexible and Distributed Service Architecture:** IT teams can decide where to run each layer of required security – either on-premises in the branch office, or centrally in the data center or co-location point-of-presence (PoP). For example, compute-intensive services such as malware sandboxing, intrusion prevention (IPS) and AV filtering can be run centrally, while key branch services like firewall and secure web gateway, can be run locally, with the overall set of layered security services defined with a simple policy template.
- **Contextually Aware Security Fabric:** A key aspect of Versa's software-defined security is the contextual intelligence and awareness of users, devices, sites, circuits and clouds; enabling robust and dynamic policies to achieve a multi-layered security posture. For example, IT teams can deploy contextual network and security policies for specific users and specific devices, like anti-virus and URL-filtering, when utilizing certain site-to-site or Internet links. IT security teams can even set unique security policies, differentiated services or security service-chains for guest access, corporate access and partner access networks at the branch. This enables the enterprise to meet business security and compliance policies - all with a single unified software platform.
- **Elasticity:** With a software-based model, IT teams can easily and dynamically scale capacity without having to replace proprietary security appliances. For example, a branch firewall can be doubled in capacity in minutes either automatically or using commands from the central provisioning portal, without a truck roll or firewall appliance swap-out.
- **Centralize, Automated Operations:** One of the biggest benefits of software-defined security is that it delivers services from a single point of control, avoiding the need for on-site skilled personnel. Services can be deployed, and capacity can be increased and enhanced with additional functions automatically, without any on-site presence, hardware refreshes or manual provisioning. Also, if a site(s) requires a different set of security functions, it can be serviced individually from a single management portal within a few minutes instead of hours or days.
- **Monitoring and 24/7 Support:** Versa's SD-WAN solutions are backed by a world-class support team, continuously looking for new security threats, combing various sources to identify and eliminate potential vulnerabilities. The threat research lab at Versa collects intelligence from multiple sources (Internet resources, commercial feeds such as TELUS and internal research) that help the support teams keep track of the latest viral outbreaks and emerging threats. By continuously updating the threat libraries and automating the update through a complimentary subscription service update, Versa insulates its customers from attacks.

Versa's SD-WAN solution was built from the ground up, fully programmable and automated, with a cloud-native architecture and with integrated security, not as just another added feature or external bolt-on service. Security is an intrinsic part of the Versa's software technology – embedded from the ground up. To learn how Versa Networks can help you fortify your organization and accelerate your digital transformation, e-mail us at info@versa-networks.com or request a demo.

Versa Security Functions- A Quick Glance	
Stateful Firewall	Zone-based Firewall, support Address Objects, Address Groups, Services, Geo-Location, Time-Of-Day, Rules, Policies, Zone Protection, DDoS (TCP/UDP/ICMP Flood), Syn-cookies, Port-scans, ALG support, SIP, FTP, PPTP, TFTP, ICMP, QAT support.
Application Visibility	Identifies more than 3000 applications and protocols, Supports Application groups, Application filters, Application visibility and log.
Next-Generation Firewall	Policy Match Triggers: Applications, App Filters, App Groups, URL Categories, Geo Location, Application Identity based (AppID) policy rules, Application Group and Filters, Packet Capture on AppID, IP Blacklisting, Whitelisting, Custom App-ID signatures, SSL Certificate-based protection, Expired certificates, Untrusted Cas, Unsupported cyphers and key lengths, Unsupported Versions, NSSLabs Recommended Rating.
IP Filtering	Filtering of traffic based on Geo-Location, DNS name, Reputation of Source/Destination IP Addresses – support for both IPv4 and IPv6. Automatic updates of IP Reputation database.
URL Categorization and Filtering	URL categories and reputation including customer-defined, Cloud-based lookups, Policy trigger based on URL category, URL profile (blacklist, whitelist, category reputation), Captive portal response including customer defined, Actions include block, inform, ask, justify, and override.
Anti-Virus	Network/Flow based protection with auto signature updates, HTTP, FTP, MTP, POP3, IMAP, MAPI support, 35+ file types supported (exe, dll, office, pdf & flash file types), Decompression support, Storage profile support, Auto signature updates.
IDS/IPS	Default and customer defined signatures and profiles, Versa and Snort rule formats, L7 DDoS, Layer7 Anomaly detection, Support for JavaScript attacks, Security package with incremental updates, Full incremental (daily) and real-time threat (every hour), Lateral movement detection.

About Versa Networks

Versa Networks, the leader in Secure SD-WAN, combines full-featured SD-WAN, complete integrated security, advanced scalable routing, genuine multi-tenancy, and sophisticated analytics to meet WAN Edge requirements for small to extremely large enterprises and Service Providers. Versa Secure SD-WAN is available on-premises, hosted through Versa-powered Service Providers, cloud-delivered, and via the simplified Versa Titan cloud service designed for Lean IT. The company has transacted hundreds of thousands of software licenses globally through its global Service Providers, partners, and enterprises. The company is backed by premier venture investors Sequoia, Mayfield, Artis Ventures and Verizon Ventures.

For more information, visit http://www.versanetworks.com or follow Versa Networks on Twitter @versanetworks.

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com