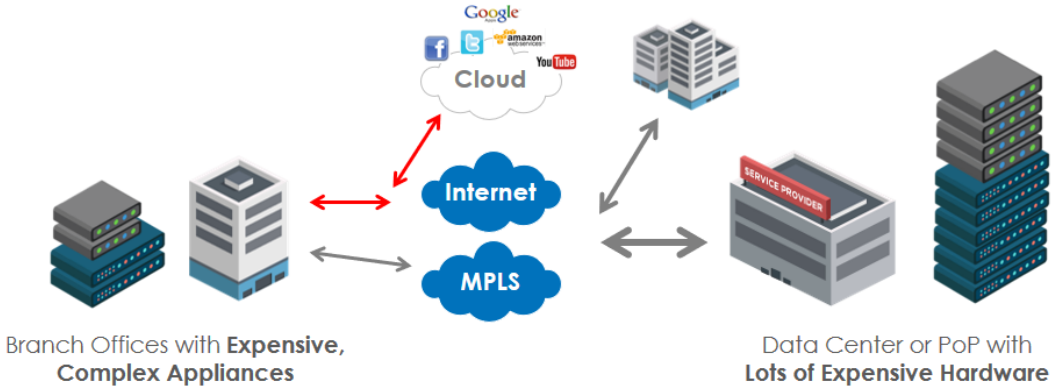
Applying Software-Defined Security to the Branch Office

Branch Security Overview

Increasingly, the branch or remote office is becoming a common entry point for cyber-attacks into the enterprise. Industry analysts noted in 2013 that attack volume for branch offices would grow more than 500 percent by 2016. Fast forward to today, and while the attack landscape has only broadened and become more sophisticated, branch security architectures, and the managed service offerings often used to deploy and operate them, have not significantly evolved. Point security appliances (usually firewalls or unified threat management (UTM) devices) or add-on software in a branch router are used to approximate perimeter data center security at the branch.



Security at the Branch: Enterprise Challenges

Enterprises with multiple branches today either manage their security devices in-house or leverage a managed service provider. Regardless, there are multiple challenges to address when multiple security technologies are deployed as separate resources in the branch:

- **Cloud apps / Internet connectivity** – companies today have apps running both in the cloud and the corporate data center. Additionally, different branch offices locations or sizes have different connectivity types (e.g. purely Internet vs. MPLS vs. hybrid). Thus there are very different security requirements depending on where the apps 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. In addition, if all traffic to/from cloud apps must be routed through the corporate data center for security functions, end user performance will be negatively impacted.

- **Complexity and cost of ownership** – having to purchase, deploy and manage point devices for different layers of security at locations where there is generally not any IT/security expertise available locally, resulting in very high Capex and Opex
- **Complexity and risk of error** – having to integrate different layers of security together without minimizing overall protection
- **Lack of agility** – companies experience long deployment times due to hardware shipping, as well as scheduling of consultants or integrators to install, integrate and test equipment. This occurs both at initial deployments, but also when capacity upgrades are required (e.g. if a new or larger WAN circuit is provisioned to a direct Internet access office, then higher capacity firewall is required)

Security at the Branch: Service Provider Challenges

On top of the enterprise challenges around branch security noted above, service providers have an incremental set of operational difficulties as they build and scale managed security services:

- **Cost of CPE** – as security threats targeting the branch become more advanced, and the range of required security functions grows, CPE costs can soar. For example, a unified threat management (UTM) or next-generation firewall appliance is significantly more costly than a basic stateful firewall
- **Lack of agility** – as noted above, the shipping/deploying/provisioning of advanced security devices is slow and expensive, and it can take weeks to several months to properly launch a branch office from a security perspective. Providers need to be able to rapidly launch new services at a small and cost-effective level (without major hardware inventory costs), and then quickly scale them as business targets are reached.
- **Added complexity at scale** – as a managed security service's customer and site volume grows, providers often find that complexity and operating costs grow radically after certain thresholds are reached – especially when the service is based on basic infrastructure like firewall appliances built for individual enterprises vs. managing 100s or 1000s of customers from a central PoP or data center
- **Change management** – constant changes in the security landscape and the resulting updates to rules on managed CPE devices, rolling out changes in threat feeds (e.g. updates to an IPS engine or anti-malware to mitigate a zero-day vulnerability) or adding new critical services (e.g. adding application visibility & control to a basic firewall solution already in place) remotely and automatically becomes a challenge. Keeping up with regulatory compliance at each location

stipulates additional challenges in keeping the managed service architecture up-to-date and constantly requires skilled professionals to be sent to the customer location.

- **Systems expertise** – as network and security functions become complex, the requirement for service providers to provide technical support to manage these devices either remotely or on-site can quickly erode the margins of a managed service

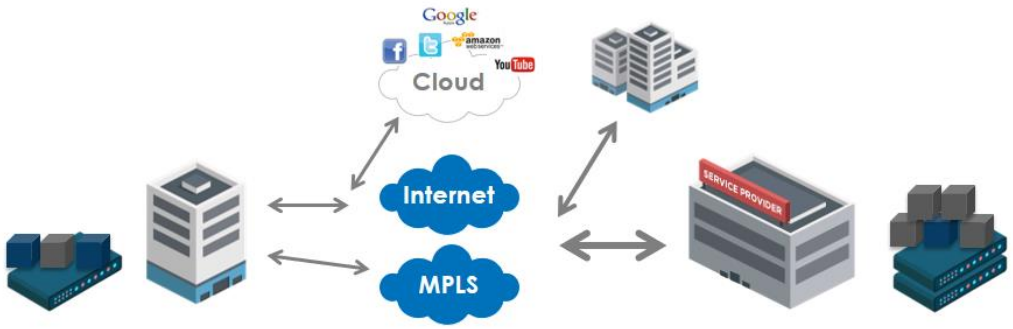
These challenges very often result in extra truck rolls and service calls that result in eroded margins and place significant pressure on the business model of the managed service.

Leveraging Software-Defined Security and NFV

While the above issues with branch security are very real, technology advances in the last few years can offset many of these challenges. Software-defined technology can significantly improve the deployment and management of security at the branch. Specifically, network function virtualization (NFV) is a rapidly growing telecom industry trend of evolving previously hardware-centric network and security technologies into software-based solutions.

A core element of NFV is the virtualized security or network function (VNF), which is a software-based or virtualized version of a specific function like a next-generation (NG) firewall. Much more than just converting from point hardware or appliances to virtualized software instances, VNFs are centrally managed and policy orchestrated, zero-touch provisioned, and service-chained, addressing many of the operational challenges noted earlier.

In essence, applying NFV (and VNFs) to enterprise security and managed security services results in the ability to "software-define" security in terms of both form-factor and operations / policy creation / enforcement. This is compounded by the fact that software-defined security created from NFV de-couples security functions from proprietary hardware, enabling the use of security functions in software running on commodity x86 servers and white box appliances.



Taking an example of branch security, imagine an enterprise with 400 branch offices that needs to refresh or increase its branch security. Instead of scheduling new UTM or NG firewall appliances and shipping them to branch sites at the rate 20 per month (an aggressive schedule, at one installation per business day), and a project schedule of over 1.6 years. The enterprise or managed service provider can ship commodity white box appliances to 100 branches per month, and simultaneously activate and test 25 devices per week remotely, for a total project time of 4 months. The result is far lower cost of deployment, as well as compliance and data protection delivered more than a year earlier.

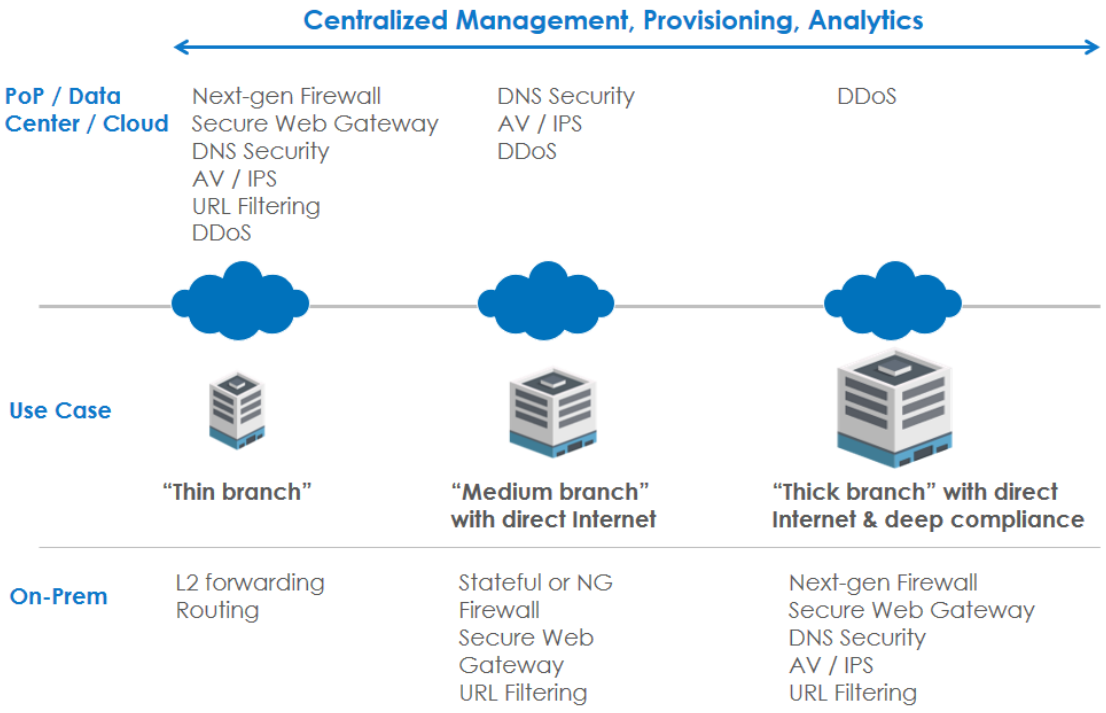
Another key aspect of software-defined security using NFV is the ability to service chain to easily achieve multi-layered security. For example, a service provider can service chain multiple security functions, like a NG firewall and a secure web gateway, to provide security for direct Internet access from the branch. As the service creation, service definition and service-chain rules are created using APIs, centralized orchestration and management tools, each branch office security service is programmed to deploy in hours, instead of days or even months.

Other aspects of creating a software-defined managed security service or enterprise deployment include:

- **Elasticity:** When deploying branch security through a software-defined and NFV-based model, capacity can easily and dynamically be scaled up or down 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, with no truck roll or firewall appliance swap-out required.

- **Flexible and distributed service architecture:** With the advent of NFV, service providers and large enterprise have the capability (and flexibility) to decide where to run each layer of required security – either on-premises in the branch office or centrally in the data center or provider point-of-presence (PoP). For example, compute-intensive services such as malware sandboxing, intrusion prevention (IPS) and AV filtering can be run centrally, while services that are key in the branch, like

firewall and web gateway, can be run locally, while the overall set of layered security functions are service-chained.



- **Centralize, automated operations**: A software-defined and NFV-based approach to security also provides a way to deliver services from a single point of control, avoiding the challenging requirement for skilled personal available on-site whenever needed. Instead, services can be deployed, capacity increased and enhanced with additional functions automatically, all without requiring any on-site presence, hardware refreshes or manual provisioning. Also, if a particular customer 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.

In summary, deploying SD-Security for the branch office involves adding additional layers of security for better defense-in-depth, when and where you need them. Adopting a software-defined and NFV-based approach gives enterprises and managed service providers the flexibility to deploy the right security functions necessary to meet an ever increasing complex threat landscape while reducing deployment times, operation complexity and significantly reducing capex and operating costs.

Learn more at http://www.versa-networks.com and follow us on Twitter *@versanetworks*.
2953 Bunker Hill Lane | Suite 210 | Santa Clara, CA | 95054 | +1-408-385-7660