Scalable Enterprise Network Security

Considerations for Designing a Secure, Future-Proof Network Architecture

Overview

In the past, an enterprise network's people, places, and things all resided on-site, making a hardware-based architecture and on-premises-focused strategy viable for information security. Today, networks are undergoing a digital transformation: Workloads are shifting to the cloud, workforces are more mobile than ever, and IoT is creating thousands of additional network on-ramps.

Enterprise IT teams are being challenged to deliver LAN-like connectivity and access across the WAN to the entire organization; at the same time, they must make the most of limited budgets and thwart ever-more-sophisticated network attacks.

Many have come to understand that legacy architectures cannot meet the needs of today's distributed enterprises. Given evolving business needs and limited budgets, organizations are looking at the foundation of their security strategy — the network architecture itself — and considering what kinds of changes should be made to deliver both performance and security.

Network Architecture: Foundational Security Strategy

There is no shortage of network security solutions on the market, but as organizations ask their IT teams to keep doing more with less, simply layering more and more security solutions and applications becomes an expensive, complex, and untenable way to combat evolving security threats.

Complex protocols and archaic command-line segmentation scale poorly and expose the company to greater risk of a mistake, especially at the Network's edge, where companies usually lack on-site IT expertise and the visibility required to keep the network secure.

A growing number of distributed enterprises achieve both layered security and scalability by rethinking their network architectures, adopting automation, and centralizing maintenance.

This white paper offers a comparison of security architectures and considerations for choosing the right option for your organization's abilities and needs.

The Traditional Approach: Hub & Spoke

Benefits:

- **Security:** With the proper encryption and authentication, VPNs are a highly secure solution for transmitting data. This is in contrast to MPLS, which is not encrypted[2].
- **Threat detection:** Unencrypted data can be analyzed as it moves through the network and used to identify potential threats or breaches.
- **Governance:** Enterprises charged with transmitting or storing highly sensitive data can be more confident that they are in control of implementation and maintenance of the security architecture.

Risks:

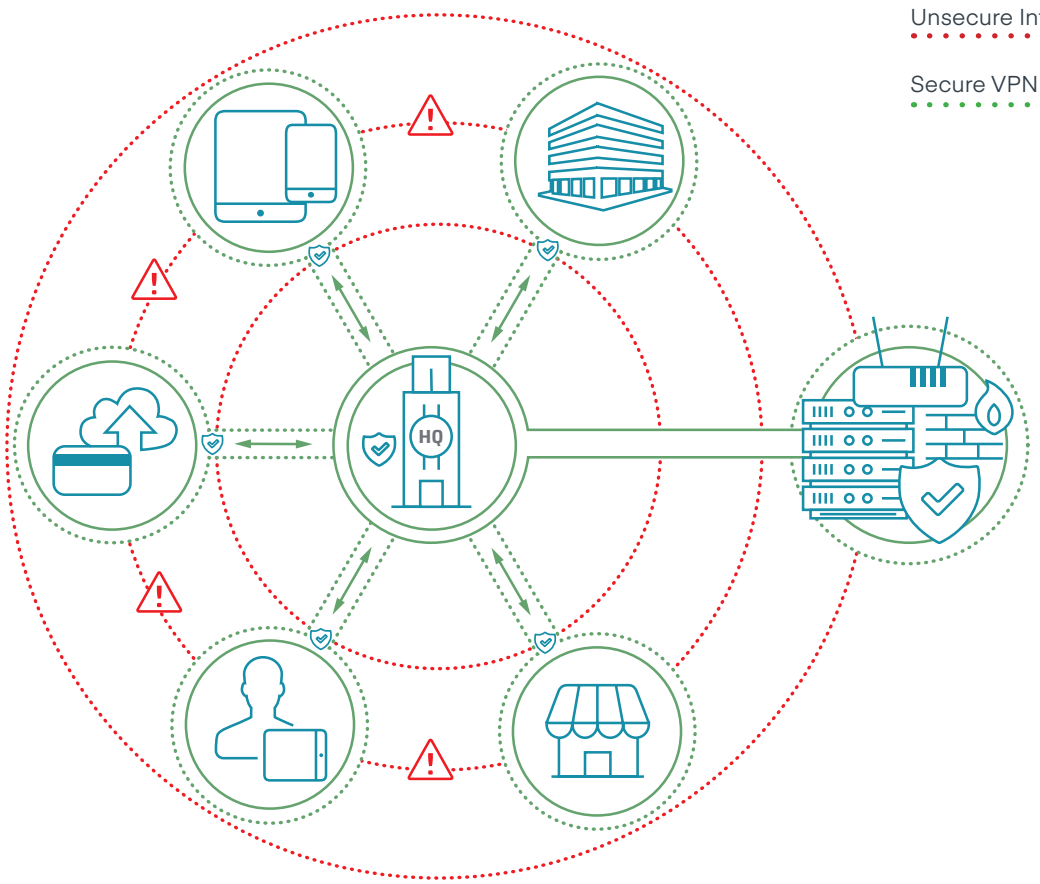
- **Planning and configuration mistakes:** Deploying a VPN requires extensive planning and configuration, along with consistent updating. Improperly configured segments may create security holes within the core network, which hackers can exploit to access sensitive data.
- **Scalability:** A growing company may find the complex configuration requirements of hub-and-spoke difficult or expensive to maintain over hundreds of locations and amid evolving needs.
- **Inefficiencies:** Routing all traffic through headquarters for security scanning creates a network chokepoint, and the more locations routing traffic through HQ, the more users are likely to experience latency, bandwidth issues, and lost productivity. End users may turn to shadow IT practices (like using a nearby public WiFi network), opening the company network up to many risks.

According to Verizon, the top industries affected by data breaches are:[1]

1. **Financial Services**
2. **Healthcare**
3. **Public Sector**
4. **Retail & Accommodation**

1 **Source** Verizon, 2017 Data Breach Investigations Report

2 **Source** http://www.rcrwireless.com/20140513/wireless/mpls-security



Key to Success:

Secure the hub-and-spoke architecture with isolation and segmentation. In the past, many organizations used single- or dual-firewall architectures that divided networks into segments at Layers 3 and 4, as well as limiting IP address ranges, Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) ports that could traverse one segment or another. While this network security architecture remains the most common, more organizations are starting to control traffic at higher layers and use emerging technologies that facilitate traffic capture, analysis, and control.

The New Model: Cloud & Software-Defined Applications for Network Security

Benefits:

- **Scalability & concentration:** Increasing the scale of a cloud-based security architecture can require less planning than traditional hardware-based architectures.
- **Threat management:** Web traffic can be dynamically authenticated, encrypted, and filtered with near-zero latency. External Internet-based attacks can be rejected while detecting and preventing local malware.
- **Threat response:** In contrast to many on-premises solutions, event logs and alerts can be filtered through cloud-based algorithms for more detailed monitoring and actionable analytics.

— **Flexible traffic routing:** Simplified cloud-based tunnels and security protocols to protect data in transit can be configured and deployed between remote sites and corporate headquarters much faster and without the cost of traditional hardware gateways.

— **Built-in security:** Perimeter-secured overly networks that leverage SD-Perimeter technology ensure security is built into all IoT connections, and that policies follow mobile workforces no matter their location.

Risks:

— **Loss of governance:** In a cloud-based model, data and information are stored with a third party. It may be difficult to inspect the provider's data-handling practices.

— **Time-to-resolution:** Problems with on-premises solutions can be addressed by logging on directly to the appliance to engage vendor support faster; with cloud-based solutions, IT has to open a ticket and work externally to resolve issues.

— **Customization:** With cloud-based security offerings, IT can address network vulnerabilities but loses a level of customization as a trade-off for speed and scalability. However, most organizations don't need (or use) the detailed customization features that on-premises vendors offer. They opt for tried-and-true implementations because they typically don't have time for the detailed work of implementing customizations.

— **Resource sharing and isolation failure:** In a cloud-based security model, customers share provider resources with other customers. Cloud providers generally implement isolation measures to prevent "guest-hopping" or pivot attacks — wherein a hacker exploits vulnerabilities of one operating system to obtain access to another hosted on the same hardware — but there is a small risk that these measures will fail.

— **Security compromise from within:** If user permissions and roles are not set up carefully, a user might have the ability to delete or modify their data within the cloud solution, either accidentally or intentionally.

— **Data portability:** It may be difficult, if not impossible, to move data should you ever need to switch cloud providers, unless there is a prior agreement between the provider and the enterprise that the information is owned by the enterprise.

Keys to Success

Maximize and automate cloud services with effective threat management. In addition to implementing isolation techniques and controls, distributed enterprises can reduce costs and network complexity by collapsing their infrastructure to some extent, while still employing multi-layered security throughout their sites.

53%

of IT staff agree that Internet-based WAN is more secure than MPLS.[3]

3 **Source** Enterprise Management Associates, 2016.

Connecting People, Places & Things: Blending On-Premises & Cloud Security

A Secure & Scalable Architecture

Many organizations want the cost savings and efficiencies of the cloud, but they don't want to sacrifice traditional levels of control and security. Legacy network security solutions require expensive and overfeatured hardware, archaic command-line interfaces, intensive multi-day training courses, certification programs, and 400-page manuals. While some organizations place greater trust in appliance-based security because it is proven and familiar, the complexity of on-premises security architecture creates an inherent vulnerability, and sometimes there's nowhere to house security hardware — for example, in the case of mobile workers or IoT devices.

A blended approach offers the immediacy of on-premises management with the simplicity and centralized control of the cloud. IT teams can better keep up with growth at the network's edge, while users benefit from low latency and the convenience of Direct-to-Internet access to cloud applications, and the company's most sensitive and valuable data stays protected by requiring users to access it over an encrypted VPN.

This infrastructure is best implemented using a multi-WAN routing platform — one that can handle wired/MPLS, LTE, and software-defined networking. Software-defined networks deliver the ability to immediately and remotely extend the network to additional people, places, and things.

A blended security approach helps address the growing challenge that enterprises face when attempting to manage access between and among groups of users, applications, locations, servers, and thousands of IoT devices. Relying on access control lists and firewall permissions to manage these sophisticated topologies is becoming increasingly unsustainable. By shifting to a hybrid approach, it is possible to leverage the flexible scalability of the cloud while integrating with existing infrastructure and permissions management systems.

A successful implementation should require no modification of existing network infrastructure.

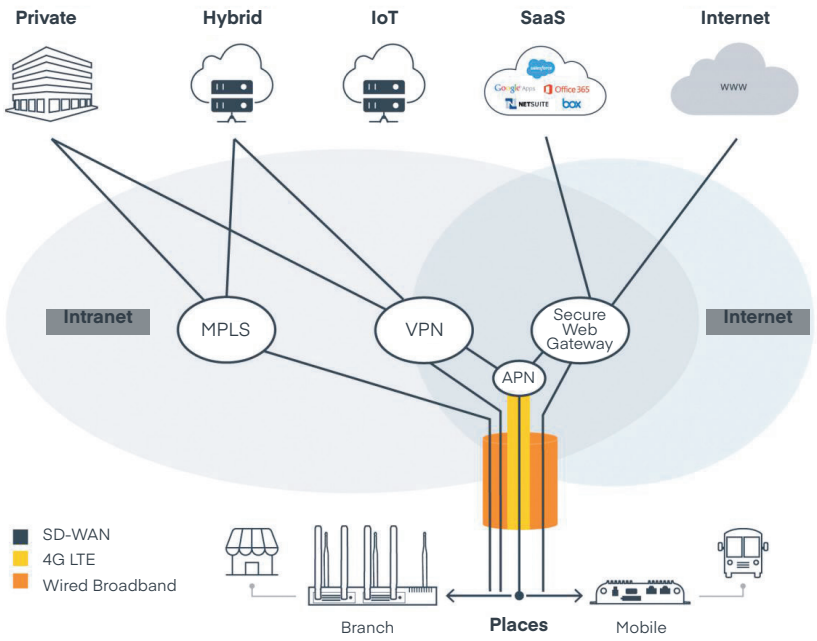
Benefits:

- **Governance:** Because an organization's most sensitive data can be kept on VPN architecture, it can retain governance and ensure compliance with regulatory requirements.
- **Latency:** Organizations that need low-latency access to large files, or have high-volume email needs, can still enjoy the same speedy access to these files while utilizing the cloud for other tasks.

> **"Industries that rely on their Internet presence for doing business or communications seem to suffer larger DDoS attacks."**
>
> Verizon Data Breach Investigations Report, 2017

— **Scalability:** Certain applications, such as those that process big data, only work well at cloud scale. Organizations can take advantage of these tools with Direct-to-Internet access.

— **LAN-like security and connectivity over the WAN:** Organizations need LAN-like security on the WAN, and software-defined technology enables them to achieve that more easily by abstracting the physical network itself. Essentially, SD-Perimeter technology lets organizations build private networks using broadband infrastructure, achieving the security and control of a private LAN with the bandwidth and remote management of broadband.



Risks:

— **Lack of familiarity:** This unique model may be unfamiliar or uncomfortable for many organizations. Historically, similar split-tunnel configurations have not been widely implemented. As is common whenever a change or unfamiliar practice is instituted, there may be risks associated with lack of experience managing such a solution.

Key to Success

Implement well-established controls and choose network solutions that enable a high level of visibility. Network reports and alerting should be granular, and a centrally located IT team should have a very clear picture of what is happening on the network from the edge all the way to the core. Established, documented, and uniform controls are critical to making this architecture work for a distributed enterprise.

Specifically, a successful approach will utilize controls at multiple layers.

In a recent study, 46% of organizations said they have a "problematic shortage" of cybersecurity skills, and one-third of those respondents said their biggest gap was with cloud security specialists.[4]

4 **Source** https://community.spiceworks.com/topic/1668233-making-a-secure-jump-to-the-hybrid-cloud

Network Security Through Cradlepoint's NetCloud Services & Wireless Edge Endpoints

Cradlepoint's NetCloud Services for branch, mobile, and IoT are delivered through purpose-built, LTE-enabled endpoints that include a limited lifetime warranty and comprehensive 24x7 support.

All-in-One Edge Endpoints

Cradlepoint's all-in-one routers include an integrated statefull firewall; support for DMVPN or Auto VPN; and Cradlepoint's CP Secure Web Filter, powered by industry-leading Webroot BrightCloud® Threat Intelligence.

Some organizations leverage separate Cradlepoint routers to move specific applications off the main enterprise network and onto a completely separate Parallel Network dedicated to that application.

NetCloud Manager

NetCloud Manager allows IT managers to rapidly deploy and dynamically manage networks at geographically distributed stores and branch locations. NetCloud Manager's open API allows enterprises to seamlessly integrate other security and big data tools as well. NetCloud Manager is hosted at a third-party storage facility on a secure, enterprise-class server, providing equipment redundancy, perpetual power, multiple Internet channels, and backup and restoration services.

Perimeter-Based IoT Security

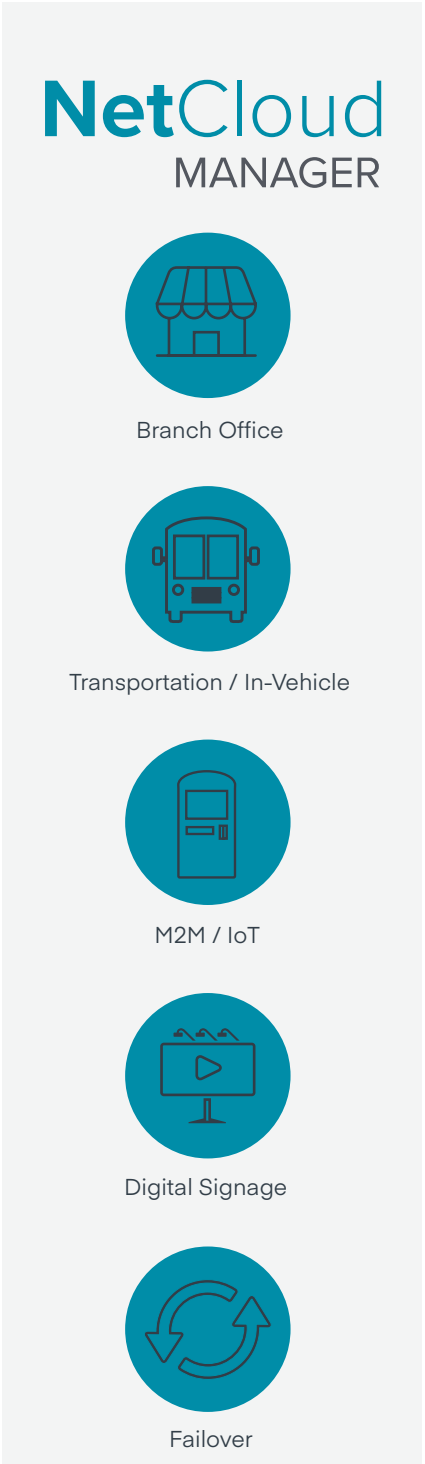
Through SD-Perimeter technology, Cradlepoint's NetCloud Perimeter enables IT professionals to create encrypted and perimeter-secured private overlay networks that protect IoT devices and isolate them from trusted networks. This service enhances visibility and control while simplifying management and security processes.

Third-Party Security Applications

Cradlepoint's Innovation Partners program provides seamless integrations with these industry-leading solutions:

Zscaler Internet Security — Zscaler Internet Security enables enterprises to embrace cloud applications and mobilty, while delivering a superior user experience. Configured in minutes, Zscaler Internet Security leverages the threat intelligence harnessed from the Zscaler cloud.

CP Secure Threat Management — This comprehensive IPS/IDS defends against evasion attacks, improves network availability, and protects sensitive data. CP Secure Threat Management is powered by Trend Micro's industry-leading Deep Packet network, requiring no infrastructure modification to deploy.



About Cradlepoint

Cradlepoint is the global leader in cloud-delivered wireless edge solutions for branch, mobile, and IoT networks. The Cradlepoint Elastic Edge™ vision — powered by NetCloud services — provides a blueprint for agile, pervasive, and software-driven wireless WANs that leverage 4G and 5G services to connect people, places, and things everywhere with resiliency, security, and control.

More than 27,000 enterprise and government organizations around the world, including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and first responders in 10 of the largest U.S. cities, rely on Cradlepoint to keep critical branches, points of commerce, field forces, vehicles, and IoT devices always connected and protected. Major service providers use Cradlepoint wireless solutions as the foundation for innovative managed network services. Founded in 2006, Cradlepoint is a privately held company headquartered in Boise, Idaho, with a development center in Silicon Valley and international offices in the UK and Australia.

Learn more at cradlepoint.com