ebook

Guide to cloud connectivity and security in distributed networks

How to respond to the new imperatives facing your distributed organization

Jim Fulton, *Solution Marketing Director*
Mary Blackowiak, *Senior Product Marketing Manager, NGFW*

January 29, 2019

FORCEPOINT

Table of contents

Distributed networks are the new normal

Distributed networks are the new reality of today's mobile, global workforce. Transforming cloud connectivity and security within these networks is the new challenge.

Digital transformation initiatives mean that organizations are rapidly shifting the way they do business. Often beginning with cloud application adoption, effective digital transformation requires the ability to fully secure the IT environment, including organizations' most sensitive data, while employing new technologies at the speed of cloud.

In addition, organizations are becoming more dispersed, moving from having a few large offices or locations, to having many smaller locations. This hyper-connected global environment requires the ability to bring up new offices quickly while providing reliable, location-independent access to services and data.

How can distributed organizations achieve the reliable connectivity and holistic security they need to leverage the latest advances in IT and adopt cloud-based applications while reducing cost and supporting greater user productivity?

The new imperatives of distributed organizations

In the face of digital transformation, more is expected of security teams than ever before. To unlock productivity of the cloud in distributed environments and mitigate risks that arise from increased access, organizations must find a way to:

- Adopt SaaS/cloud applications to boost user productivity and lower costs
- Increase agility and reliability of networks to support distributed connectivity, on premises and in the cloud
- Protect enterprise data and intellectual property against advanced threats originating from all directions
- Unleash workforce productivity while having the ability to detect and intervene in risky activity

Why traditional distributed networks can't keep up

The traditional approach of backhauling traffic from remote branches to a central location then out to the internet just isn't feasible anymore. Unfortunately, organizations often find this out the hard way. As they begin to roll out company-wide access to cloud-based applications, they discover a multitude of problems.

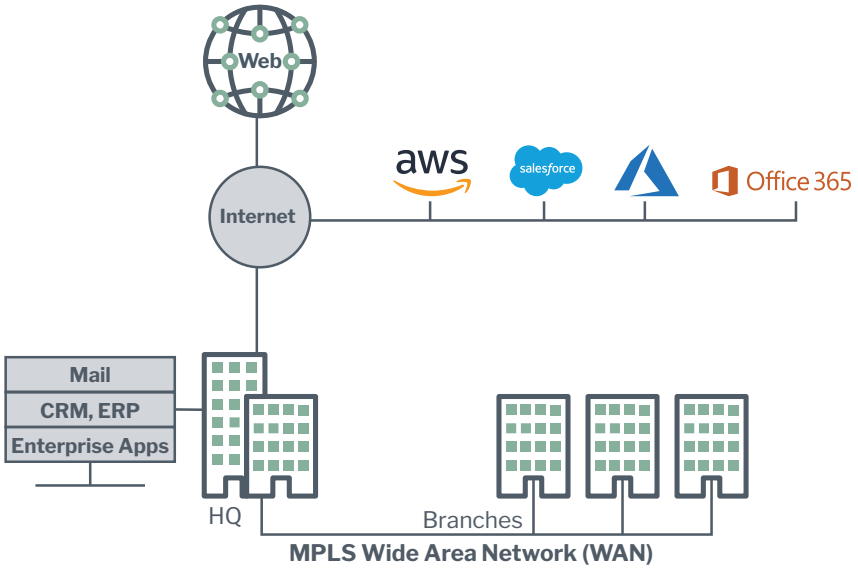
Poor performance
MPLS cannot handle the additional network traffic created by users connecting to cloud applications, causing latency and poor user experience.

Single points of failure
Networks can become suddenly unavailable due to multiple external factors (example: construction crews accidentally severing a buried cable).

Costly and time-consuming upgrades
Adding dedicated lease lines to handle the increased traffic can take months to install and come at an exorbitant price.

Manual administration
Often, each connection must be managed and maintained independently, adding to the complexity and cost of this type of infrastructure.

But, there is good news. There are ways for organizations to reduce costs while increasing agility and productivity.



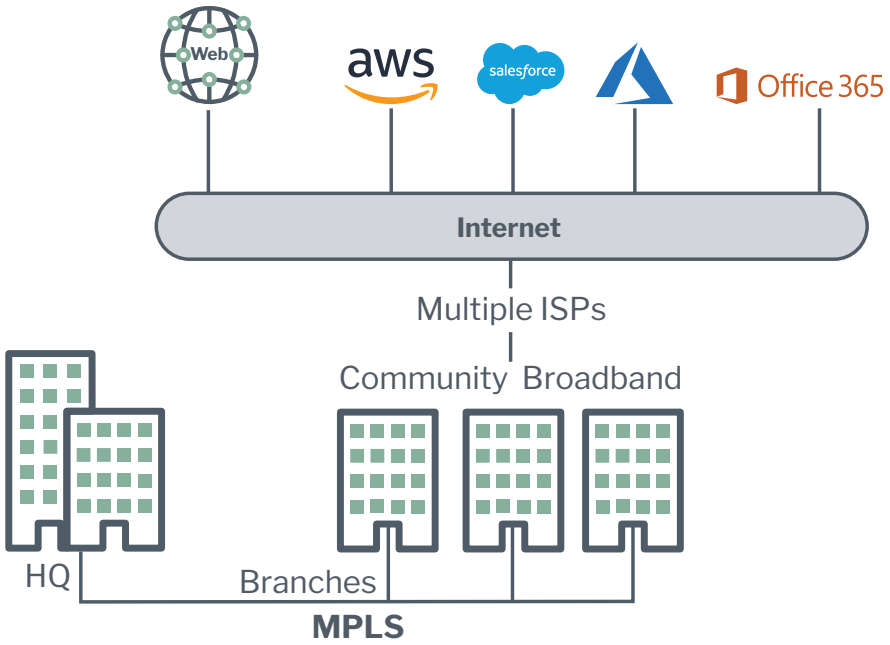
A more effective approach to connecting your networks

Augment or replace MPLS with local internet breakouts

Reduce use of MPLS to reduce cost
A growing number of organizations are addressing the connectivity issue by replacing the old MPLS technology, known for slow performance and difficult, expensive upgrades.

Use commodity broadband links to increase agility
An alternative to replacing MPLS lines altogether is to augment connectivity with lower cost commodity broadband links such as fiber, commercial DSL, and mobile carrier technologies.

Use multiple ISPs to increase productivity
Utilizing multiple links ensures continuous connectivity, even in the event of a single link failure.



Dynamically connect direct-to-cloud and site-to-site

Distributed organizations looking to increase productivity need two kinds of connectivity: direct-to-cloud and site-to-site.

Eliminate backhauling for cloud application traffic

With direct-to-cloud connectivity, traffic accessing cloud-based applications would no longer go through central headquarters but directly to the cloud instead.

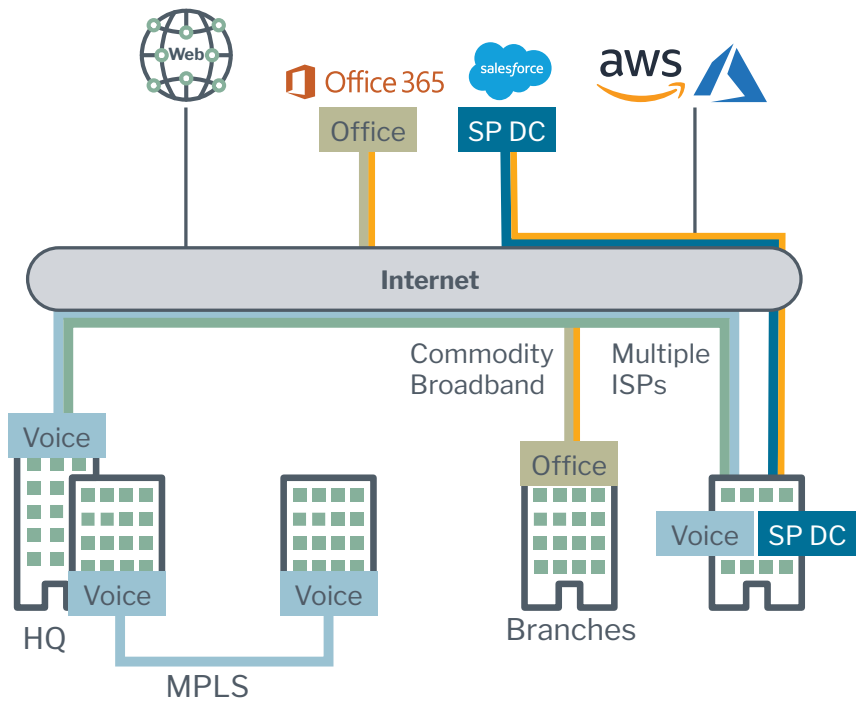
Reserve site-to-site connectivity for internal traffic

Site-to-site connectivity ensures that legacy applications and other internal applications, notably VoIP, can still go over internal links when they need to.

Optimize use of most appropriate links

Instead of IT staff trying to cobble together ways of connecting and hard-coding what applications go where, traffic is sent dynamically over the most efficient links.

Ultimately, this approach is about optimizing each location's available resources to increase productivity and route traffic most efficiently.



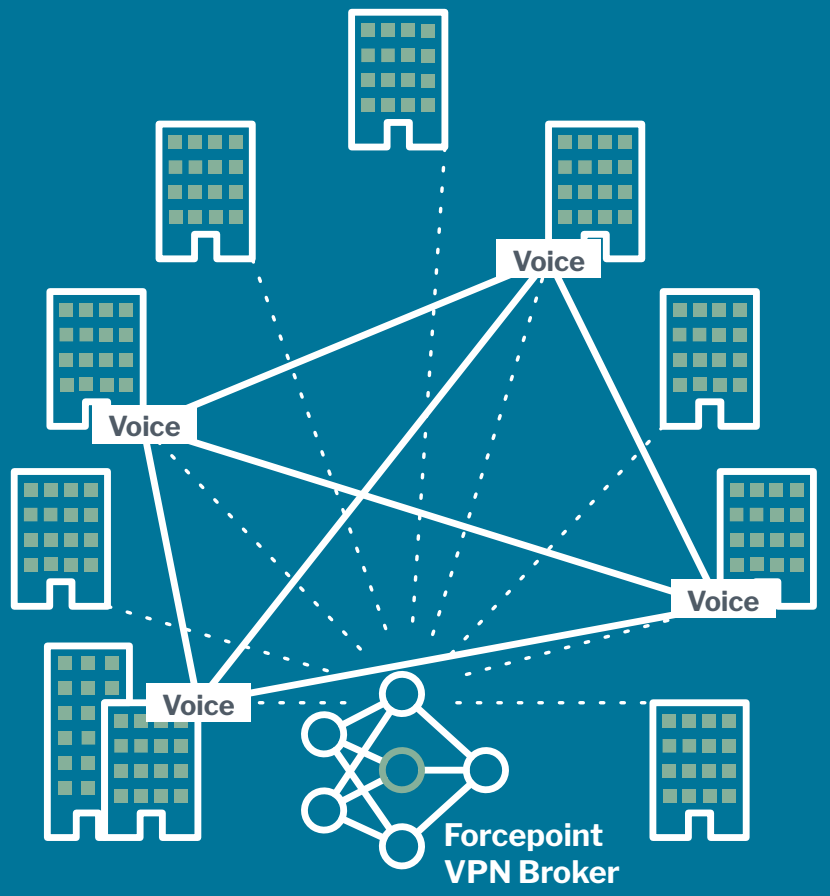
Scale site-to-site connectivity with on-demand VPNs

For organizations with site-to-site connectivity, connecting all of the sites together is called a mesh and at scale it can be expensive, time consuming, and difficult to administer.

New architectures built for this kind of scale are reinventing how VPNs are set up. The connectivity among the sites is designed so they can dynamically determine how to connect to each other. With on-demand VPNs, organizations can:

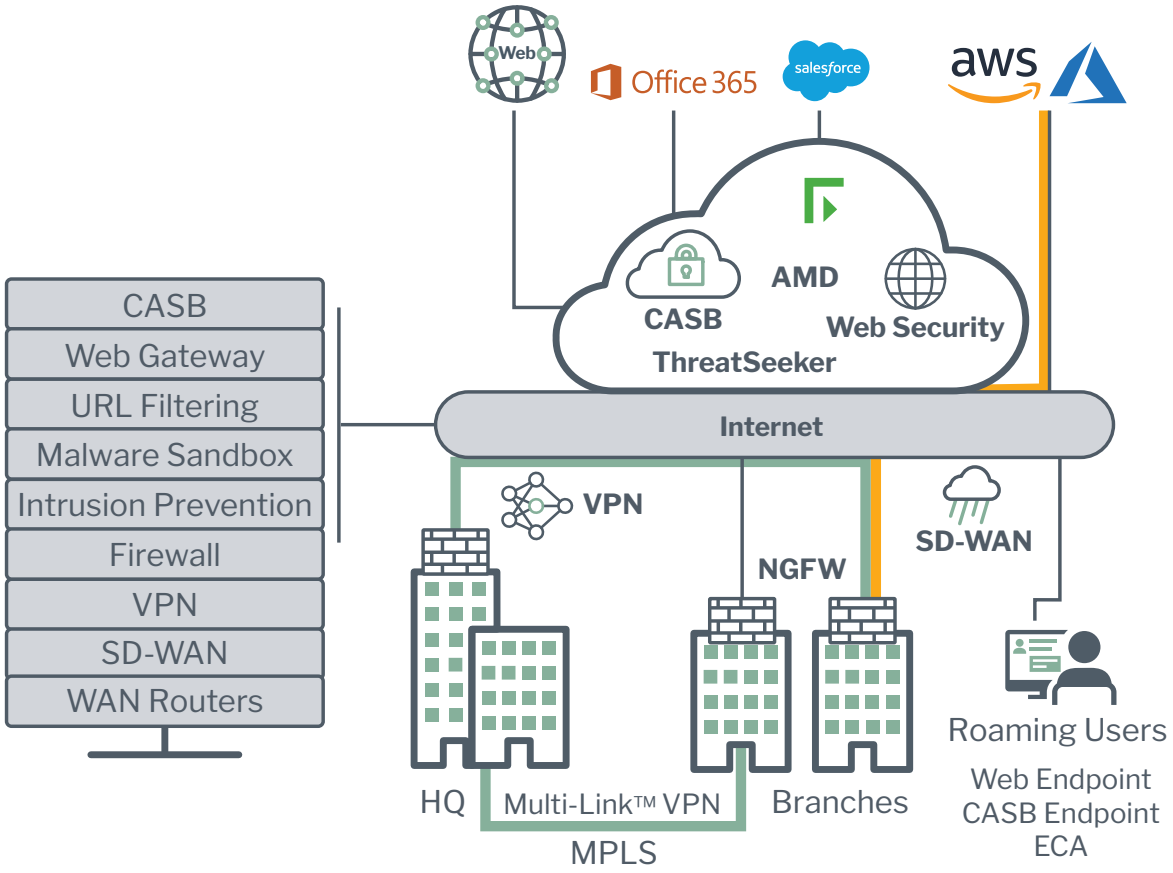
- Configure VPNs centrally and update dynamically
- Connect sites directly without creating bottlenecks due to backhauling
- Scale to thousands of sites
- Use public and private links seamlessly

This is important because it allows neighboring organizations to communicate more effectively. Instead of manually configuring every location, connectivity becomes dynamic. This allows a smaller equipment footprint at each site, with less complexity. Overall, this reduces cost as well as risk of network outages.



Move from a patchwork of products to an integrated solution

As organizations look to transform their IT to the cloud, the industry is moving toward consolidation—the traditional patchwork landscape of point products is evolving into an integrated approach in which pieces all work together to provide consistent security that removes gaps and redundancies.



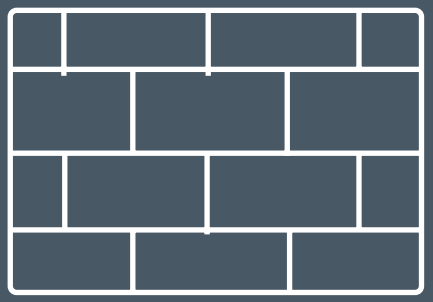
Three types of security that all internet-connected sites should have

Changing the way each branch site connects also influences other things, most notably, security. Gartner specifically advises clients that branch office firewalls must offer the same level of security as primary internet gateways. Once a branch connects directly to the internet, it has essentially become a primary internet gateway.

> "Branch-office firewalls need to … offer the same levels of security efficacy as the primary gateway does.[1]"

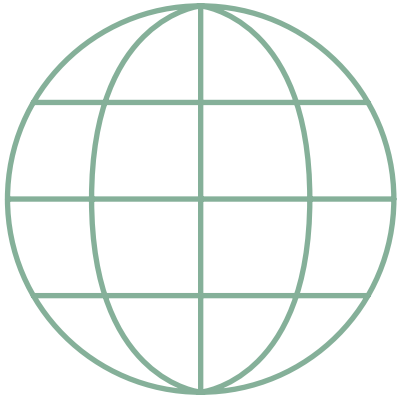
[1]2017 Gartner Magic Quadrant for Enterprise Network Firewalls

Access Control and Intrusion Prevention



Web Threats and Content Security

Cloud Application Data Protection



Access control and intrusion prevention

Keep intruders and advanced threats out

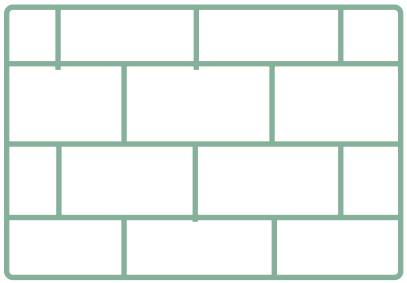
Distributing security out to every location helps to ensure intruders remain locked out. It is very common for attackers to attempt to gain access to the enterprise network via branch locations. They no longer go to the main internet portal to knock on the front door. They're looking to see what windows were left open out back.

Limit unauthorized access

The organization also needs control over what assets and resources a user can access from the branch locations. This becomes important if something gets in through some other means, like a USB stick. Having the ability to quickly cut off access to a command and control site is extremely important.

Centrally deploy, monitor, and manage

Distributed security, however, does not necessarily mean distributed management. Policy setting, monitoring, and control should be centralized. In fact, that is the direction that the industry is going: making sure that solutions provide centralized control with distributed enforcement.



Protection against advanced threats and undesirable web content

Prevent drive-by downloads and block acceptable use violations

This type of security is about protecting people when they're using the web—keeping advanced threats out and preventing access to content that violates acceptable use policy.

Offload SSL/TLS inspection from firewalls

In two years, it's projected that more than 80% of the traffic will be encrypted.[1] Moving SSL/TLS inspection to the cloud provides some distinct advantages:

- Smaller firewalls can be used at each location
- The risk of overloading core infrastructure as processing requirements increase at each location is eliminated

Enforce consistent policies everywhere

When security is in the cloud, it's much easier to ensure that the same security polices apply to every device and every user—from central locations to branches connecting directly to the cloud and even remote workers.

Discover unsanctioned shadow IT SaaS applications

Get visibility into use of unauthorized SaaS cloud applications and insight into the level of organizational risk they might present.

[1] Gartner, "Predicts 2017: Network and Gateway Security," Lawrence Orans et al, 13 December 2016.

Safeguards for data in cloud-based applications

The third part of the security, complementing web security in the cloud, is using a cloud access security broker (CASB) to:

- Ensure security of data stored in cloud applications
- Monitor for possibly compromised accounts
- Control sharing of sensitive files
- Enforce consistent policies everywhere

Forcepoint provides one of the most flexible CASB systems out there. It supports a very large number of existing commercial applications and also enables organizations to add support for their own applications very quickly to provide consistent enforcement—not only for Office 365 and enterprise applications, but for proprietary systems as well.

How cloud web gateways complement firewalls

People often wonder why they can't just secure web use with firewalls, as many provide URL filtering and content security. Forcepoint NGFW, in fact, is built for that deep kind of inspection—but most don't have that ability. However, putting security up in a cloud web gateway gives you several interesting advantages.

Deeper web security
Using technologies such as proxies prevent direct access to the network. Dynamic classifications can block or allow sites based on content rather than hard-coding each of them individually.

Controlled access or usage
Rather than simply blocking or allowing a site, organizations can find a middle ground with controlled access and usage or by providing overrides for legitimate exceptions.

Other integrated technologies
Applying data loss prevention will scan data as it transmits across the internet to detect regulated data or intellectual property. Using cloud application control maintains controlled access to cloud applications, looks for anomalies, and performs auditing.

Visibility and control
The operational benefits of pairing a cloud web gateway with a firewall include consistent visibility and enforcement across users and locations, including policy enforcement and control of shadow IT.

Operational costs and reliability
Operational efficiency of the overall infrastructure can be improved by offloading the rapidly growing computational burden of SSL and TLS inspection. Ultimately, the life of infrastructure can be extended and the risk avoided of overload or having to over-provision and buy more than needed.

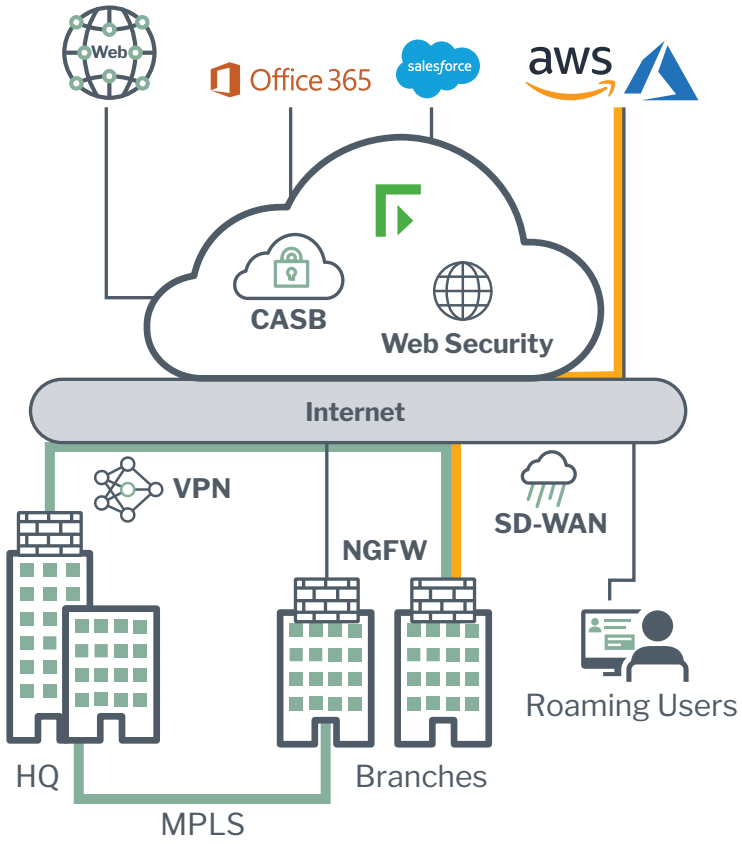
Transforming connectivity and security for moving to the cloud

Following these steps for connectivity and security through digital transformation can provide important benefits to an organization, including increased productivity and improved user experience at a much lower cost, whether it's for accessing cloud applications or internal legacy applications.

Using the same policies and tools for visualizing what's happening on a network, and extending that seamlessly into the cloud will help security teams understand use and manage risk of deploying cloud applications.

The right connectivity and security also make compliance a lot easier. Auditors can see that acceptable use policies are being enforced consistently and seamlessly, and that an organization has the ability to segment networks and services to control access.

Consolidating point products allows for consistency in defining and enforcing policies and provides a seamless and consistent user interface. Ultimately, this ensures greater productivity as workers can access the data they need, safely, from across the globe.



About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: people's behavior as they interact with critical data and systems. This human-centric approach to cybersecurity frees employees to innovate by understanding the normal rhythm of user behavior and the flow of data in and out of an organization. Forcepoint behavior-based solutions adapt to risk in real time and are delivered via a converged security platform to protect network users and cloud access, prevent confidential data from leaving the corporate network, and eliminate breaches caused by insiders. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

Contact

forcepoint.com/contact

[SECURITYBRANCH-EBOOK-NA-EN-160119-WEB] 800015.011819