Barracuda

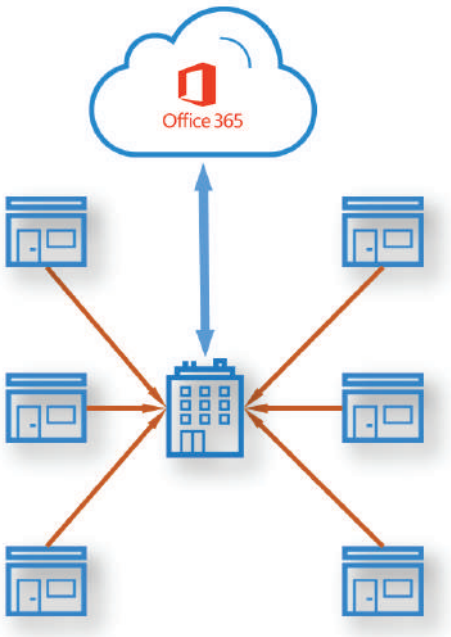
SD-WAN: When the Internet becomes the new network

The evolution of enterprise networking for the Cloud Generation

Most corporate Wide Area Networks (WAN) still have the same basic architecture that was considered state-of-the-art more than a decade ago. Traffic is still backhauled via expensive MPLS lines to a central hub, for security policy enforcement. But as digital transformation drives increasing adoption of, and dependence on, cloud-hosted applications and data, that traditional architecture is growing burdensome

It creates latency, makes bandwidth upgrades very costly, requires weeks of planning for a new location to be connected, and makes critical, cloud-hosted applications slow and unreliable.

Any usage of cloud-hosted applications or services – Microsoft Office 365 is one of the fastest-growing examples – runs up against the limitations of a pre-cloud WAN architecture.



Data previously held in the company network's core is now accessible only via the cloud. Thus the entire backhaul infrastructure, including the leased MPLS lines in support, is becoming a costly relic of a bygone day.

It needlessly introduces latency that can severely degrade performance of cloud apps. What's more, spending vast amounts of funds to scale a MPLS-based network won't work. That's because of the inherently induced latency of the backhauling architecture.

Digital Transformation and demand for Cloud Connectivity marks a strategic inflection point

As the above challenges illustrate, we're reaching a 'strategic inflection point', a term highlighted in Andy S. Grove's seminal business book 'Only The Paranoid Survive'. It's the moment where businesses need to recognise and implement 'full-scale changes in the way business is conduced'.

As an unavoidable fact of moving business functions to the cloud, this affects hardwired service providers, as well as customers shifting their business from traditional on-premises data centres. The company network has to therefore adapt to support this change, to benefit from cloud-hosted networks or even outsource to Software-as-a-Service (SaaS) offerings (e.g., Salesforce.com).

SD-WAN technology to enable cloud adoption:

A new set of products including Software Defined WAN, (SD-WAN) technology emerged during the last few years to facilitate network performance and cloud adoption.

First widespread use of the term SD-WAN occurred when Gartner coined the term in its report "Technology Overview for SD-WAN" as far back in 2015.

To help replace traditional WAN based on MPLS and improve traffic flow, the industry analysts say SD-WAN products must provide the following functions at the minimum:

Be able to replace traditional WAN routers and provide multiple connectivity methods.

Provide Load Sharing across multiple WAN connections. Measure WAN connection quality and select the most appropriate WAN connection based on application type.

Dramatically simplify complexity, management, configuration and orchestration(rollout) of SD-WANs, with "Central Management at the source".

Provide secure VPN connections and additional network services.

SD-WAN market to reach $8 billion by 2021 (CAGR: 69.6%)*

*https://www.idc.com/getdoc.jsp?containerId=prUS42925117

Barracuda

From SD-WAN to Secure SD-WAN

More and more businesses have been adopting Software-Defined Wide Area Networks (SD-WAN). The benefits such as dramatic improvements in application performance, significant reduction of cost for MPLS connectivity and at the time substantially simpler and more agile management are just simply too good to be dismissed.

As it turns out, SD-WAN is the de facto standard for companies leveraging any type of cloud -hosted workloads, especially SaaS services such as Office 365 and Salesforce.com. For the most common and important SaaS use cases, high performance SD-WAN networks require a local direct internet break out to the cloud – at every branch location. This also implies every branch location is as secure as the previous headquarters firewall – otherwise the entire effort is fruitless.

Without full-scale firewall security, the initial SD-WAN products solved the challenge in several ways. For example, service chaining with existing next-generation security solutions, outsourcing security enforcement to the cloud, or even providing basic firewall and IPS security internally. However, these approaches were either "not secure enough" or went against the essential "central management at source" requirement.

To overcome these challenges, a new breed of SD-WAN product appeared during 2017 and 2018. This was commonly referred to as Secure SD-WAN.

These new products bring all the benefits of full SD-WAN connectivity, and combine full next-generation firewall security levels, including Control for thousands of commonly used applications and Advanced Threat Protection. As a side benefit, these products combine central management for all networking, routing and security settings, further simplifying WAN Network management.

The Office 365 question (and answer)

Combining advanced security and SD-WAN into one solution has major benefits for cloud-based applications like Office 365.
As Microsoft explicitly recommends, it's not enough to have fast & direct-to-cloud access. Devices must ensure special handling for the Office 365 protocol.

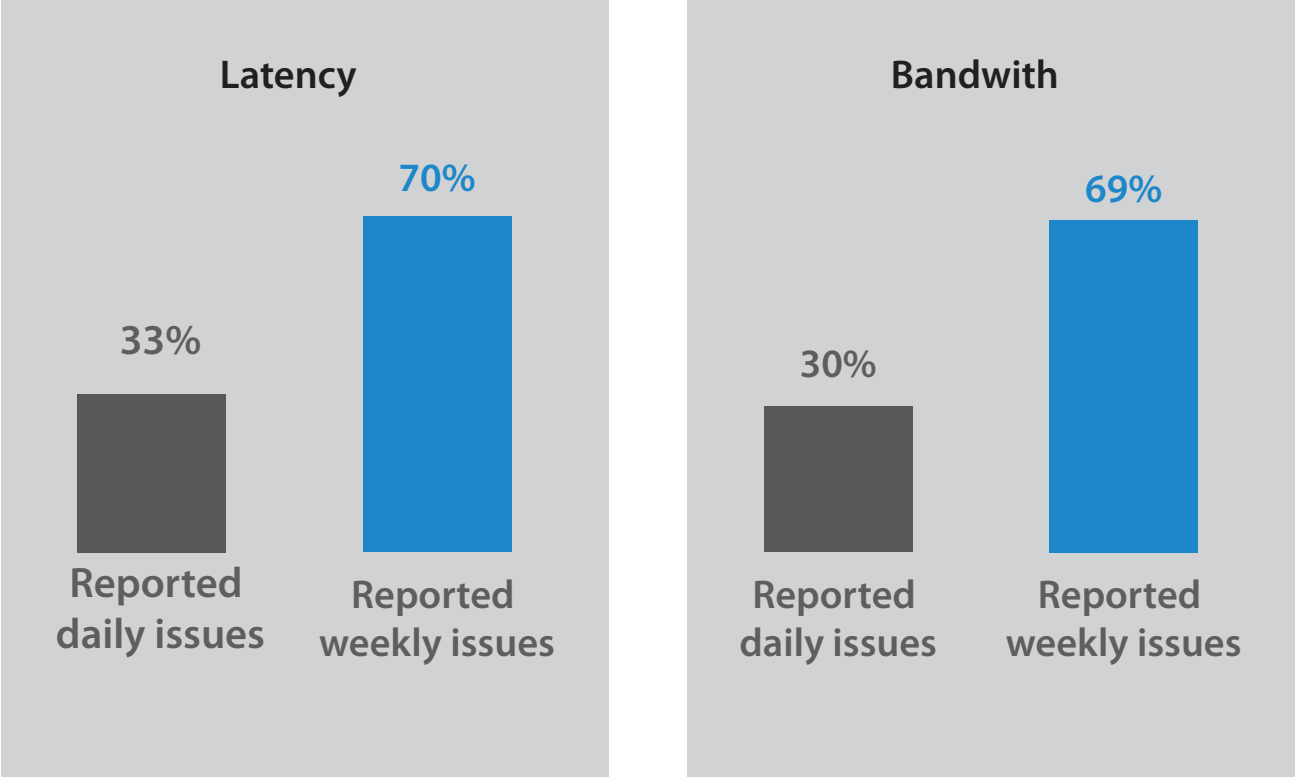
> **"Microsoft strongly recommends that SSL interception is not performed on Office 365 traffic"**
>
> **"AV/anti malware scanning is also done by Office 365 so isn't required inline"**

Source: Microsoft

Secure SD-WAN solutions need to be able to reliably distinguish between Office 365 and other types of traffic. They must then selectively disable antivirus and SSL Interception for these sessions. Otherwise Office 365 would become unusable.

On the other hand, downloading attachments from a entry should be always scanned for viruses, even if the session runs across a seemingly secure HTTPS connection. After all, who can ever be 100% sure that emailed purchase order attachment doesn't contain a macro virus? Particularly because Salesforce customers have reported there is no virus scanning for uploaded attachments.

MPLS backhauling issues with O365



> **"Challenges with Office 365 Deployment" Survey Q1 2017 found a high percentage of problematic Office 365 implementations with MPLS backhauling**

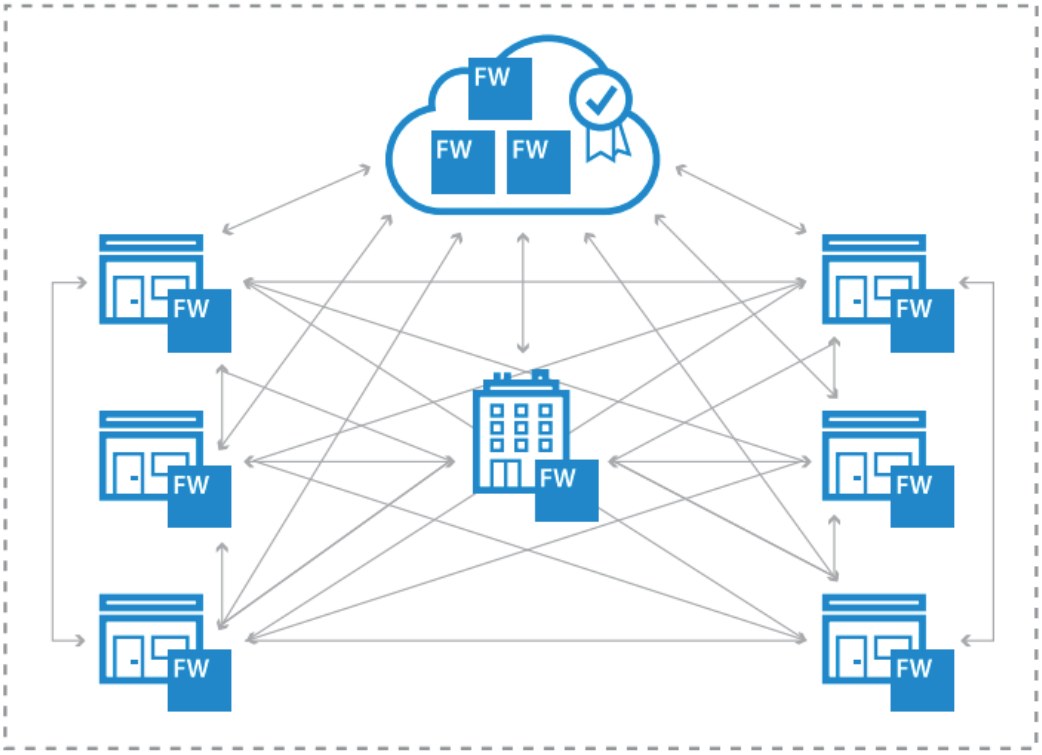
Source: TechValidate and Zscaler

It's clear that access to cloud applications today requires Secure SD-WAN solutions. Specifically, those that combine SD-WAN's technological benefits and apply the same levels of security as would be expected from any headquarters-based high end firewall solution. At the same time, the Secure SD-WAN solution must not only select the best suitable internet uplink to guarantee best performance and user experience, but it must also reliably detect the type of application and adjust security policies accordingly.

Plane sailing with Secure SD-WAN

A crucial aspect of Secure SD-WAN is that it decouples the data plane from the control plane and the management plane.

This simplifies network management, enables dynamic path steering, and minimises the need for managing individual gateways and routers.



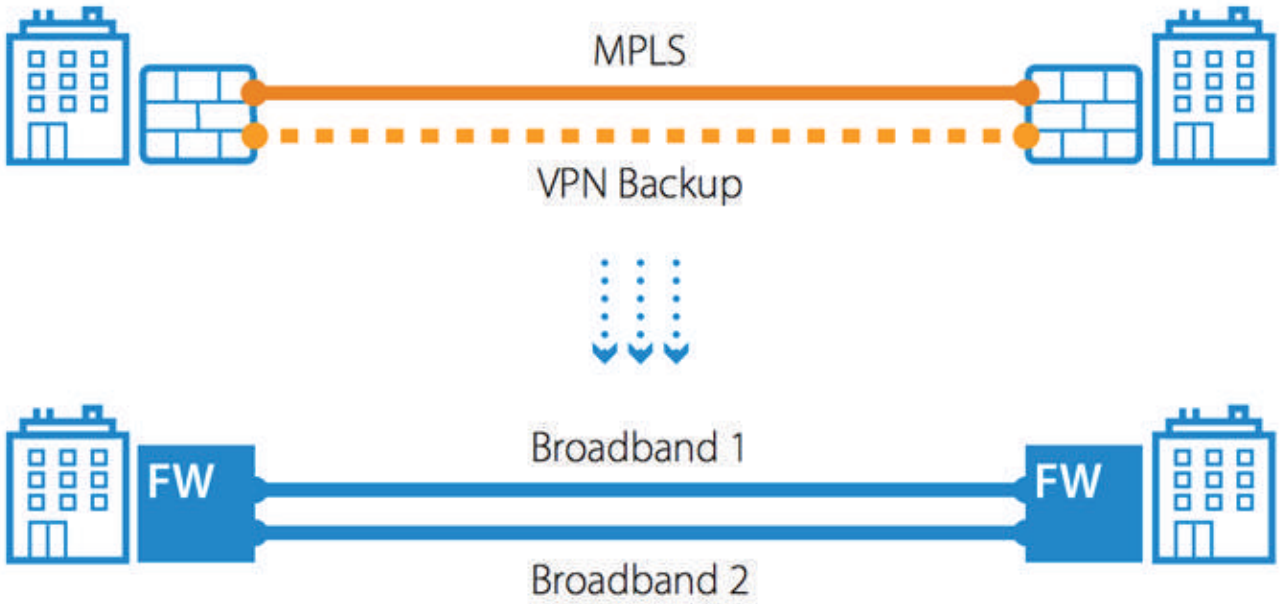
Managing SD-WAN from a central single pane then results in control across the network, no matter how dispersed. In the event of a breach, you can limit the number of potential attack surfaces, set granular rules for users and applications, while maintaining Quality of Service. This network systems unification also results in end-to-end encryption, further increasing security.

Hare vs. Tortoise

Of course, traditional WAN technology has its place. It may be that your business priorities are more about robust connections, than moving fast. Maybe it's more important that your customers simply get to where they need to be.

What's more, MPLS and Secure SD-WAN will run side-by-side, at least for the next few years.

However, maybe you're trying to do this across complex distributed networks, where security needs to be equivalent to headquarters-level. Perhaps you want to avoid bandwidth penalties at times of high demand. Your organisation may be competing with agile industry disrupters. In other words, you want your business to survive and thrive in the modern era. That's when it's time to look at Secure SD-WAN.



Barracuda

Comparing traditional WAN to SD-WAN

Traditional WAN	SD-WAN
Connects multiple Local Area Networks (LAN) using routers provider provided semi-private Multi-Protocol Label Switching (MPLS).	Direct cloud access from every WAN location.
VPN is only used as a backup, and most of the time the secondary line is unused.	Security policies centrally managed and enforced at every WAN location.
Not available at every location.	Combines multiple MPLS, Broadband and Cellullar/LTE.
Hub-and-Spoke architecture with security enforcement at the central break-out point.	Automatically measures all uplinks and selects best method of connectivity based on application demands.
High packet availability, low latency, minimal risks around loss of signal or quality when using virtual desktops or VoIP applications.	All Network, Routing and Security management is done centrally via a single pane dashboard, without the need to deploy personnel.
More complex management and set-up of connectivity, long roll-out time for new locations.	Quick roll-out of new WAN locations.
Medium CapEx, very high OpEx.	Higher CapEx for equipment, low OpEx cost for internet lines. Overall much lower combined WAN cost.

Barracuda

Questions to ask an every SD-WAN provider

Does your SD-WAN solution include ICSA Enterprise certified security levels for direct Internet break out?

Can your solution protect critical traffic by dynamically shifting less important traffic to different uplinks?

Is there a monthly or bandwidth-dependent charge for the SD-WAN features?

Is the full security routing and networking feature set available across all appliances, cloud and VM images?

Do you provide full privacy Zero-Touch Deployment or are we expected to disclose any type of credentials to the provider?

How Barracuda Networks can help

If you have branch offices and remote locations that need to run SaaS applications or connect to your network, Barracuda can dramatically improve application performance and reduce your WAN costs. The traditional approach of backhauling traffic to a main office, via costly MPLS leased lines, just can't deliver on price and performance in the cloud era.

Barracuda Networks' CloudGen Firewalls establish direct internet breakouts for optimised cloud accessibility. Secure SD-WAN maintains a fully-meshed VPN using any type of uplink – including multiple, less expensive, broadband connections.

When you need more than SD-WAN

Secure SD-WANs are an increasingly popular and cost-effective alternative to hardwired network connections and MPLS infrastructures. However, they still require firewalls to secure network connections.

With other vendors, this means buying, managing, and maintaining two boxes at each location – an SD-WAN appliance to connect to the WAN and a network firewall to provide security controls. Only Barracuda CloudGen Firewalls combine SD-WAN connectivity and advanced security into a single product. One that can be physically deployed on-premises, or as a virtual appliance in the cloud.

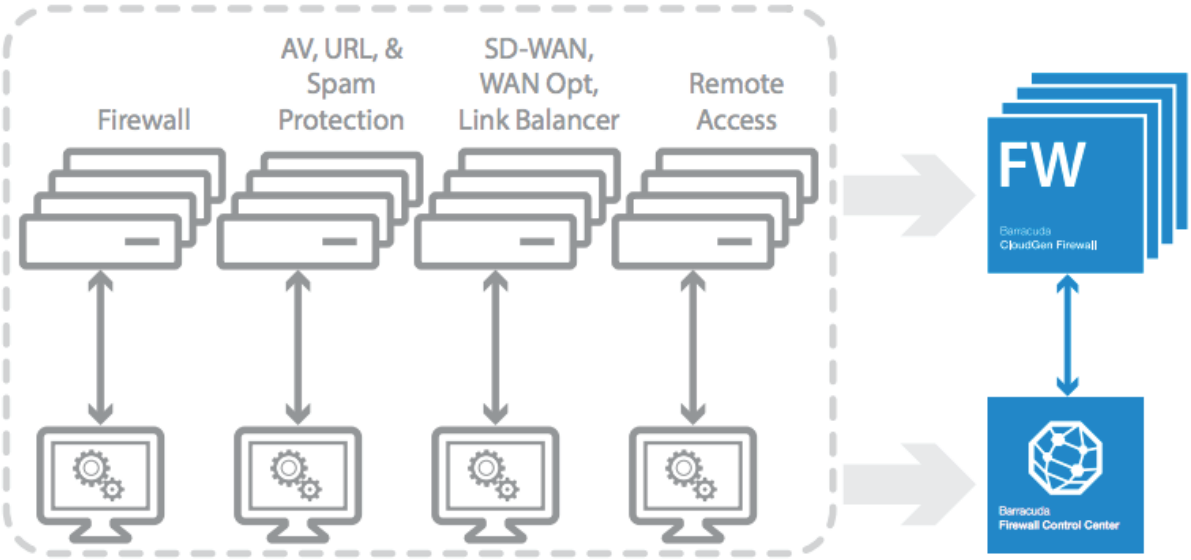
Barracuda CloudGen Firewalls redefine the role of the firewall from a pure perimeter security solution to a distributed network optimisation solution:

- scales across any number of locations and applications

- regulates traffic flows

- provides SD-WAN features to economically route traffic across the extended network while improving performance

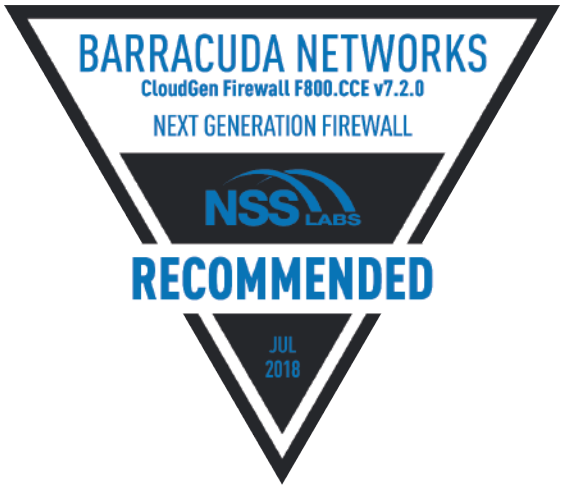
- significantly minimises WAN cost by replacing expensive, leased MPLS lines with inexpensive broadband and smart VPN tunnels, providing traffic compression across multiple uplinks



Validated Security

NSS Labs Inc., recognized globally as the most trusted source for independent, fact-based cybersecurity guidance, independently tested the Security- and SD-WAN capabilities of Barracuda CloudGen Firewalls.

Details are available with NSS Labs: www.research.nsslabs.com/reports



Summary

The Barracuda CloudGen Firewall combines a comprehensive set of advanced security features with capabilities that support and optimise SD-WAN. Traditional SD-WAN devices only deal with network routing and require you to purchase separate firewalls, often from different vendors, in order to provide network security. Barracuda CloudGen Firewalls are all-in-one devices that combine both products into a single package. This gives you a cloud-generation network firewall to provide security, and an SD-WAN controller to provide cost-effective connectivity.

Barracuda CloudGen Firewalls make it easy to create secure pathways across multiple WAN connections and multiple carriers. You can then minimise administrative overheads while optimising your cost structures. Advanced load sharing also lets you distribute encrypted VPN tunnels across multiple WAN connections simultaneously. Built-in compression, caching, and WAN optimisation technologies significantly increase your available bandwidth. These capabilities reduce your need for expensive leased lines, consolidate multiple security functions into a single device, and create a unified management framework. Altogether this results in significant cost savings for your organisation.