Choosing a firewall-friendly SD-WAN

Three questions to ask before choosing a vendor

If you're looking for an SD-WAN that works with your existing firewall, you're not alone. Your team has invested valuable time into an auditable best-practice security architecture, and that top-of-the-line firewall wasn't cheap. Most of all, your firewall represents a solution that your team is comfortable managing. You and your company have confidence that it works. So why change it?

Before choosing a solution, it's important to understand how different SD-WAN technologies will work with your firewall and what those differences will mean for your company. Choosing an SD-WAN that "kind-of" works with your firewall could add hours to your installation time. It will also likely require poking holes in your network perimeter — potentially compromising your security, compliance, and network stability. Worse, it could fail in a significant way, breaking your on-prem applications or SIP trunks.

Use this guide to learn the different solutions that work with your existing firewall, questions you can ask to evaluate an SD-WAN's firewall-friendliness, and how Bigleaf was built to be the most firewall-friendly SD-WAN out there.

1 Which firewall features will the SD-WAN require me to disable?

We designed Bigleaf's SD-WAN to work with all your firewall's features, but many solutions require that you disable specific features in your firewall and hand them over to the SD-WAN device. So when you're choosing an SD-WAN technology, make sure you ask which of your firewall's essential features you'll need to disable for it to work fully.

Here are some of the more common features you might need to disable or significantly modify:

DHCP – Assigns IP addresses to the computers on a network. Many SD-WAN devices need to act as your LAN's DHCP server to provide full functionality.

NAT – Allows the devices on your clients' network to share a single public IP address and provides a small element of security

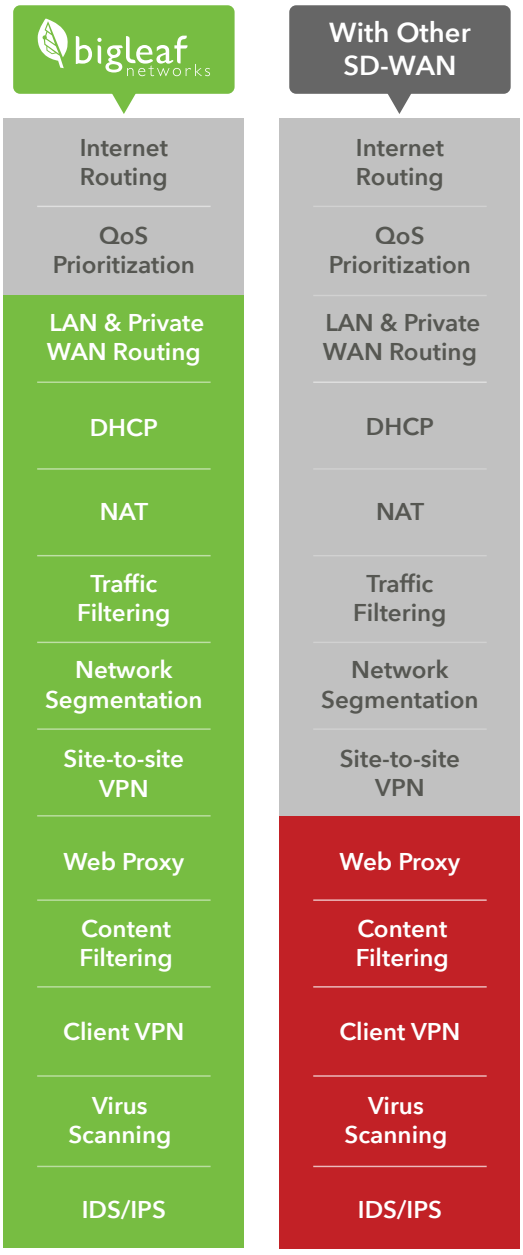
LAN and Private WAN Routing – Determines what path the client's data will take in and between their private network(s)

Site to Site VPN – Establishes secure connections between your clients' sites

Network Segmentation – Limits access to areas of the client's network to improve security

Traffic Filters – Controls what kind of traffic can enter or traverse the client's network

By confirming which of these features would need to be disabled or modified, you'll avoid any surprises when it comes time for installation.



Bigleaf allows your firewall to keep more of its key functionality. *With Bigleaf, your firewall keeps control of more of its critical security and admin features. Other SD-WANs make you disable key functionality..*

2 How long will the SD-WAN install take with an existing firewall?

Bigleaf is known for our firewall-friendly, 90-second install. That's because our SD-WAN sits outside the firewall and doesn't require any firewall features to be disabled.

But some vendors' installation times are longer due to the number and severity of firewall changes required to work with their technology. Installation times can be even longer for multi-site deployments depending on the availability of highly-skilled network engineers needed to configure the new security integration correctly.

So keep in mind that other SD-WAN vendors' "zero-touch" installation can become an hours-long ordeal when you're installing it alongside your existing firewall. Those hours are expensive, so be sure to clarify how long an SD-WAN's install typically takes with an existing firewall in place, including initial policy configuration, device configuration, and firewall reconfiguration.

You should be sure to spend time digging into how the implementation will impact each of the features listed above, and what the integration steps will be.

3 What changes will I need to make for inbound traffic?

If you're running a web, email, VPN, or application server, you'll need to make sure that your inbound traffic is routed correctly and not blocked. You'll also need to deal with any NAT and ensure that any proxying doesn't break your applications. Since your firewall handles that today, it's essential that you understand all of the impacts on this inbound traffic from the SD-WAN solution.

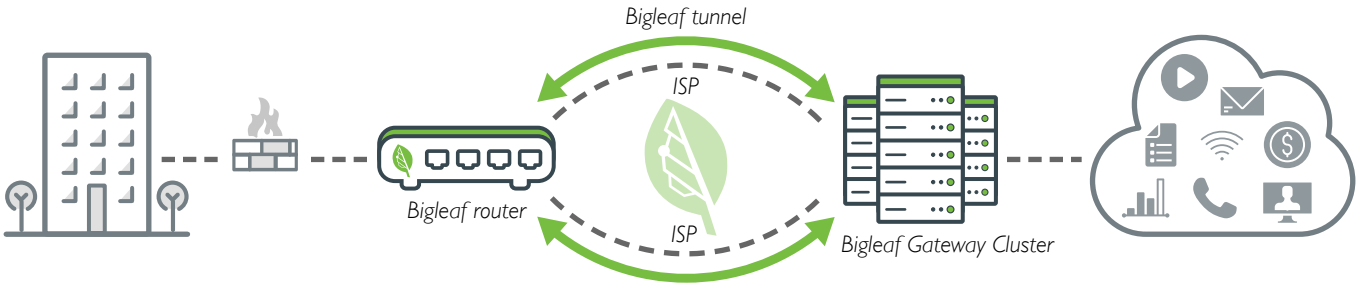
Many SD-WAN solutions are seemingly built only for branch use. They can connect outwards to remote resources, but don't have reliable solutions for inbound connectivity to local servers.

Bigleaf works with your firewall right out of the box

We built Bigleaf from day one to work with your firewall without compromising any of its functionality. To your firewall, Bigleaf looks like an internet connection. To install Bigleaf all you do is update your firewall's WAN IP address — no compromises to your security or compliance. If you have site-to-site VPNs, you may need to update the IP addresses that they connect to. If you're hosting servers internally, simply update the DNS records for those to point at the Bigleaf-provided IP addresses.

We believe in best-of-breed solutions for your critical business applications, and security is high on that list. If you'd like to learn how Bigleaf would work with your existing firewall, contact us today.

BIGLEAF'S SITE-TO-CLOUD ARCHITECTURE



The Bigleaf router installs outside the firewall, prioritizing application traffic in and out of the customer's LAN

Multiple broadband circuits are tunneled together as one pathway, providing bidirectional control and visibility of all traffic

Bigleaf's Gateway Cluster connects this streamlined Enterprise-grade connection to any Cloud application

About Bigleaf Networks

Bigleaf provides a software-defined WAN solution built with a Cloud Access Network that enables you to ensure performant uptime for any Cloud-based technologies across all sites and users. Unlike policy-based solutions, Bigleaf auto-detects application needs and network conditions and intelligently adapts traffic in real time. With Bigleaf, you can easily provide Enterprise-grade connectivity for all of your Cloud applications, improve visibility into your internet usage, and simplify your network.