

A large graphic spanning the middle of the page, featuring a network of blue and orange nodes connected by lines, with a bright blue light streak and a white curved line. The background is split into blue and orange sections.

Security and SD-WAN:

Firewall Options Comparison

Technology Brief

Security and SD-WAN go hand in hand these days, with traditional firewall vendors offering failover and SD-WAN vendors offering firewalls. This technology brief describes options available in the marketplace and industry best practices with regard to these technologies.

How Are These Solutions Different?

Firewalls were designed to create a barrier between your internal network and the outside world. They are an essential component of the modern business network. Over the past two decades, firewalls have evolved to keep up with more complex threats and sophisticated attacks. Improvements include Next Generation Firewalls (NGFW) and intrusion prevention features. These innovations have resulted in highly specialized appliances that are great at inspecting large amounts of data, detecting the latest malware and ransomware threats, alerting against potential Distributed Denial of Service (DDoS) attacks, and helping businesses meet new, stringent compliance requirements.

SD-WAN solutions were purpose-built to connect business to the outside world – the Internet, the Cloud, branch offices, data centers. As more business applications moved to the Cloud (Salesforce, Office 365, Google Apps, Citrix), businesses needed to optimize and guarantee access to the Internet. To support this, solutions like Ecessa combine multiple connections of any types (MPLS, T1, cable, DSL, satellite, wireless) from any combination of providers. These solutions use features such as automatic failover and failback, Quality of Service (QoS), load balancing, performance metrics and alerts, and Software Defined Wide Area Networking (SD-WAN) to optimize the performance of connections and eliminate outages.

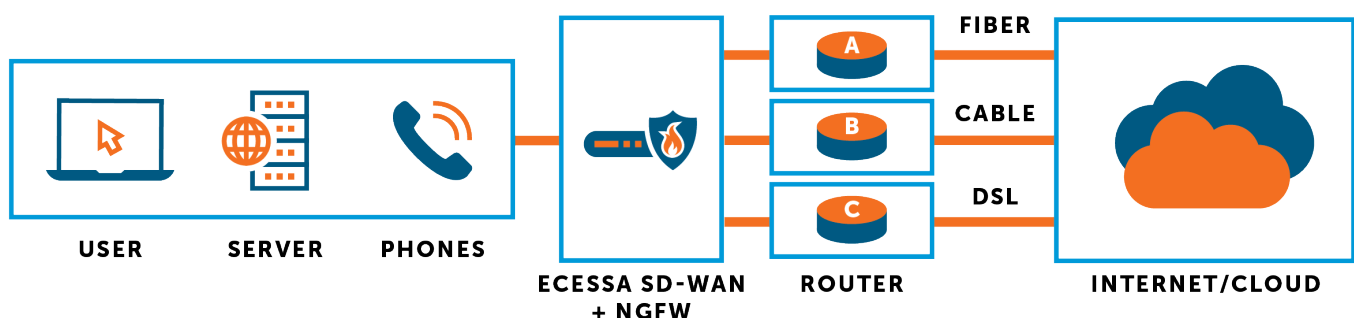
To meet market demands, the feature sets of firewalls and SD-WAN controllers are increasingly converging. Depending on your network architecture, an Ecessa device with an integrated NGFW may meet your needs. Or, you may need both a dedicated firewall and an advanced SD-WAN solution to ensure a resilient, secure network.

Let's examine some popular network architectures to illustrate how these technologies integrate.

Which Solution Is Right For Your Business?

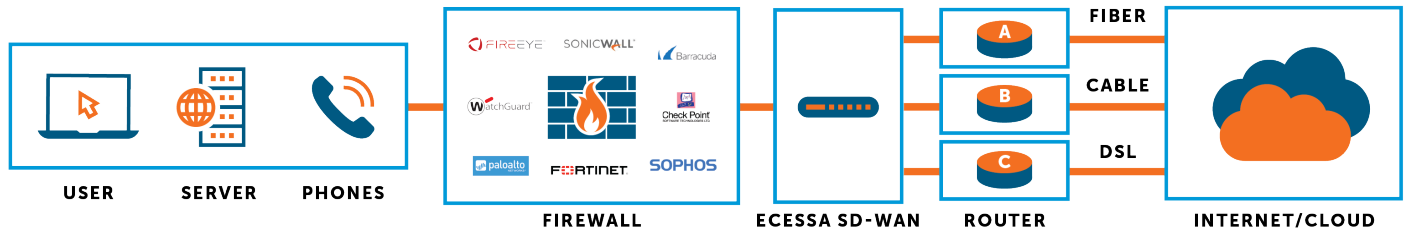
Demands on your network are increasing every day. To get the best performance and protection for your business, you'll need both firewall and SD-WAN capabilities. Whether they reside on one platform or two depends on your needs. They play specific roles and work well together. With Ecessa, you have options.

Option 1: Streamlined all-in-one solution using Ecessa's Integrated NGFW and SD-WAN.



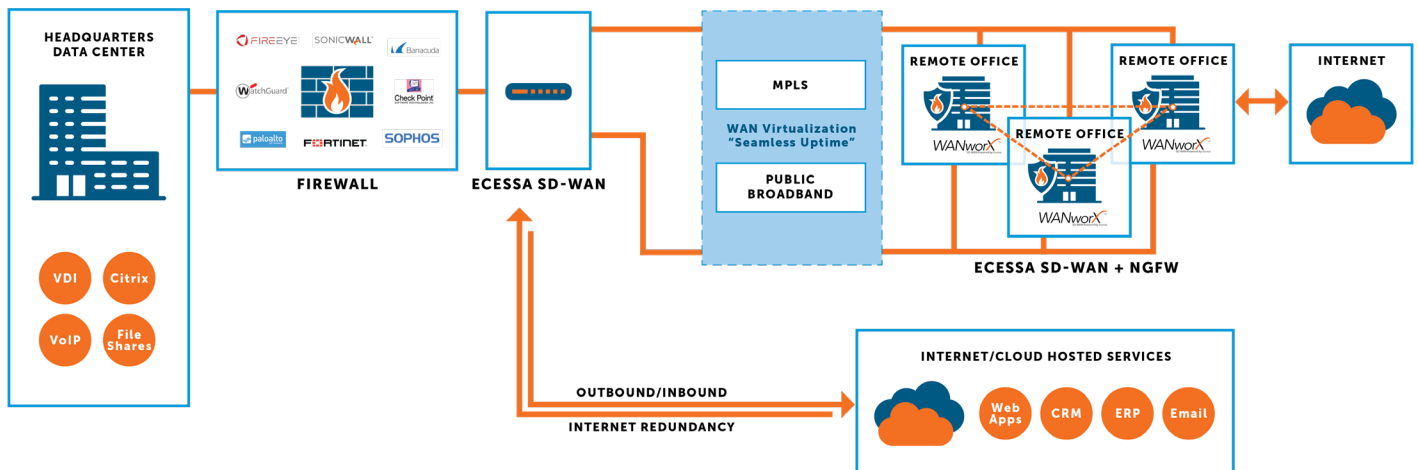
Small and medium businesses adding redundant communication links for failover, load balancing and resiliency may determine all their security needs are met by Ecessa's built-in Next Generation Firewall with intrusion detection and prevention (IDS/IPS) features. Device consolidation can remove administrative complexity and save money for these organizations.

Option 2: Keep your existing firewall and add Ecessa's expert SD-WAN resiliency. Leverage two purpose-built devices.



Best-in-class firewalls with advanced features are essential in today's network. If you have one you love, keep it. To improve access to the Internet, add bandwidth, eliminate outages, and possibly renegotiate ISP contracts to save investment add a best-in-class SD-WAN solution. Ecessa has validated interoperability with leading firewall vendors. Ecessa devices integrate easily into your existing network and do not require you to modify your architecture, change your IP addresses or remove any of your existing equipment.

Option 3: Use an enterprise firewall at HQ and use the combined Ecessa SD-WAN and NGFW at remote locations.












Enterprises with multiple locations may have made a significant investment in a powerful firewall at their headquarters and typically backhaul all branch traffic through that single device. With growing needs to access the Internet from all remote locations, this may lead to increased network congestion and poor application performance. Backhauling traffic may continue to make sense for certain applications and classes of data, ERP, time tracking and virtual desktop sessions. But vast amounts of Internet traffic could be securely and efficiently offloaded at each edge location. Some organizations maintain firewalls at each remote location, with costly investments in ongoing support agreements. A more economical option is to use Ecessa's NGFW features, while also taking advantage of Ecessa's advanced SD-WAN capabilities, like inbound and outbound failover, load balancing, encrypted tunneling, packet-level control and more. A typical configuration for SMEs creating private networks over public broadband connections is to keep the enterprise firewall and offload basic web traffic at the network edge and remote offices.

Summary

Security and resilience are at the top of every network's must-have list and this trend will continue. How you provide that depends on your needs. Our advice: Give Ecessa a call and leverage our networking expertise for recommendations on the most efficient and economical devices with the right feature sets to meet your needs.

Ecessa and Firewall Comparison

Below are some details highlighting the differences between leading firewalls and Ecessa secure SD-WAN solutions.

									
Networking: Participate in enterprise network routing, IP assignment (DHCP), traffic management (QoS), DNS, NAT, and server failover features. SNMP compliant alerts.	✓	✓	✓	✓	✓	✓	✓	✓	✓
Basic Security: Provide port based policy rules and ACL for securing the network; deny unauthorized users (DoS, DDoS attacks). DMZ capability for LAN.	✓	✓	✓	✓	✓	✓	✓	✓	✓
NGFW: Web content filtering, intrusion detection and prevention (IDS/IPS), custom rules.	✓	✓	✓	✓	✓	✓	✓	✓	✓
UTM: Spam filtering, Endpoint Security		✓	✓	✓	✓	✓	✓	✓	✓
VPN: IPSec and SSL VPNs with 128 & 256-bit encryption).	✓	✓	✓	✓	✓	✓	✓	✓	✓
Connectivity: Integrate up to 25 connections; works with any service (broadband, MPLS, T1, DSL, 4G/5G/ cellular, microwave, satellite).	✓	✓							
Outage Avoidance: Customizable parameters for automatic failover and fallback, inbound and outbound load balancing, authoritative DNS and more.	✓	✓							
Advanced SD-WAN Features: IPSec encrypted SD-WAN tunnels and packet-level control to eliminate outages and ensure quality of service.	✓	✓			optional		optional		optional
Total Cost of Ownership: Relative cost of solution; hardware plus software licenses and support.	\$	\$\$\$	\$	\$\$	\$\$	\$\$	\$\$	\$\$\$	\$\$\$