

Avalanche

SSL VPN Testing

Application Performance Testing Solution

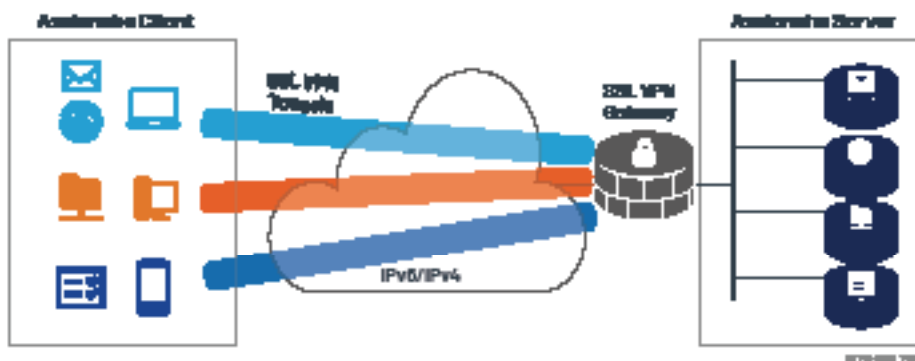
Demand for remote work has been part of enterprise operation for quite some time. Current climate of global and local crisis has also added urgency to deployment of infrastructure that allows business continuity and remote access to corporate resources. SSL VPN provides a highly secure and simple way to access corporate network for remote workers. VIAVI Avalanche SSL VPN testing enables Network Equipment Manufacturers, Enterprises, and Service Providers to realistically validate on-prem and cloud-based SSL VPN gateways and deployments.

Benefits

- VIAVI Avalanche's SSL VPN feature provides complete performance assessment of SSL VPN gateways to quickly understand and correct deficiencies before deployment. The use of real application protocols over encrypted tunnels is the best way to truly understand the gateway's effect on user experience.
- **Quicker Time to Test:** Integrated SSL VPN allows full performance characterization of gateways, leading to faster production roll-outs
 - **Avoiding Downtime:** High-performance testing with real traffic identifies proper sizing for your environment while providing comprehensive statistics to quickly locate problem areas
 - **Investment Protection:** Support for both IPv4 and IPv6 ensures testing needs can be supported now and for future generation testing
 - **Minimizing Cost:** SSL VPN is a fully integrated Avalanche application that supports many use cases, minimizing the number of test applications to learn

Applications

- Compare application performance with and without SSL VPN
- Test user data over SSL VPN tunnels
- Determine maximum tunnel capacity of SSL VPN gateways
- Measure tunnel set-up and tear-down rates
- Find maximum tunnel throughput
- Test SSL VPN services over cloud and virtualized environments and devices
- Measure the user experience through encrypted tunnels
- Emulate SSL VPN deployment scenarios for IPv4 and IPv6 networks, including:
 - IPv4 over IPv4
 - IPv4 over IPv6
 - IPv6 over IPv4
 - IPv6 over IPv6
- Test automation using FormsDB for creating large numbers of unique user name/password/group names



SSL VPN Testing Topology

Technical Specifications

SSL VPN Security Protocols	
TLS	DTLS
SSL VPN Parameters	
Validated for use with: Cisco AnyConnect™ Gateway v9.x and later Palo Alto GlobalProtect™ Gateway v8.x and later	Supports full suite of TLS v1.2 Elliptical Curve, DHE, RSA, AES ciphers including: • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • AES128-SHA256 • AES128-CCM8 • DHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256

Ordering Information

Available in license bundles for CyberFlood appliances.

Part Number	Description
CMP-ASWB-EPK-CF50	Avalanche Expansion Pack License for the CF50 Appliance
CMP-ASWB-EPK-CF400	Avalanche Expansion Pack License for the CF400 Appliance
CMP-ASWB-EPK-CF1000	Avalanche Expansion Pack License for the CF1000 Appliance

- Please contact your VIAVI sales representative for more details, including ordering information for CyberFlood Virtual.



Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2026 VIAVI Solutions Inc. Product specifications and descriptions in this document are subject to change without notice. Patented as described at viavisolutions.com/patents

avalanche-sslvpn-ds-hse-nse-ae
30194837 901 0826

viavisolutions.com