Ospirent™

Spirent Avalanche
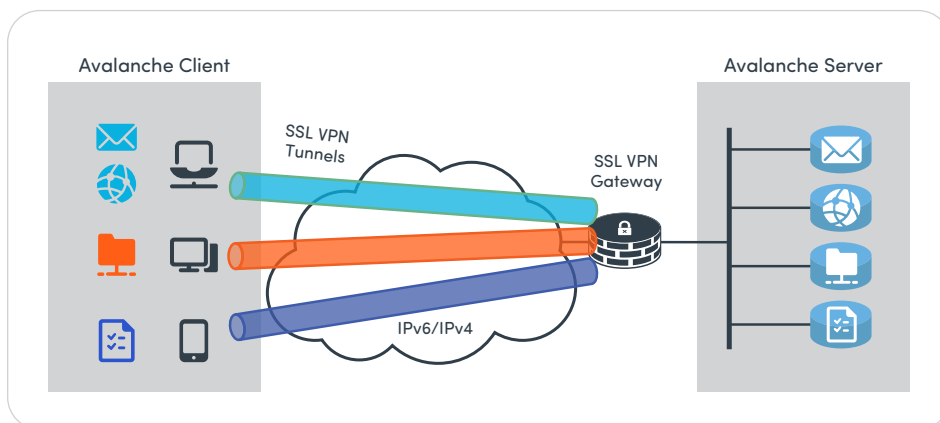
SSL VPN Testing

Application and Security Testing Solutions

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. Spirent 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

Spirent 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 IP4
  - IPv6 over IPv6
- Test automation using FormsDB for creating large numbers of unique user name/password/group names

Avalanche Client — SSL VPN Tunnels — SSL VPN Gateway — IPv6/IPv4 — Avalanche Server

Technical Specifications

SSL VPN Security Protocols	
TLS	DTLS

SSL VPN Parameters	
Validated for use with: Cisco AnyConnect™ v9.x Palo Alto GlobalProtect™ v8.1.15-h3 agent v5.2.0	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

Description	Part Number
SSL VPN support requires the following licenses based on your specific platform.	
Avalanche Application Testing Client for C100-S3 and C200	CMP-ASW-APP
Avalanche SSL Client Server for C100-S3 and C200	CMP-ASW-SSL

Supported Modules/Platforms

- Spirent C200 Appliances
- Spirent C100-S3 Appliances
- Spirent CF20
- CyberFlood Virtual ESXi/KVM/Cloud
- Software
  – Avalanche version 5.11 or higher with Avalanche SSL VPN option

Options are available for other platforms, please contact Spirent for more information.

Spirent™