Spirent **Avalanche**

IPSec Testing

### Application and Security Testing Solutions

Applications

- Compare application performance with and without IPSec
- Test user data, voice, and video over IPSec tunnels
- Determine maximum tunnel capacity of IPSec gateways
- Measure tunnel set-up and tear-down rates
- Test IPSec tunnel set-up, tear-down and encryption inside the cloud with Avalanche Virtual
- Find maximum tunnel throughput
- Test IPSec services over cloud and virtualized environments and devices
- Analyze the effects of aggressive tunnel re-keying
- Measure the user experience through encrypted tunnels
- Support for IKEv1 and IKEv2 for demanding IPSec applications
- Emulate IPSec deployment scenarios for IPv4 and IPv6 networks, including:
    - IPv4 over IPv4
    - IPv4 over IPv6
    - IPv6 over IPv6
- Test site-to-site and remote access tunnels
- Test attack traffic and vulnerabililties over IPSec

Road warriors, telecommuters and business partners all rely on the secure communications capabilities offered by IPSec. Spirent Avalanche enables Network Equipment Manufacturers, Service Providers, and Enterprise customers to realistically test their IPSec VPN gateways and cloud-based IPSec deployments.

Benefits

Spirent Avalanche's IPSec feature provides complete performance assessment of IPSec 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 IPSec 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 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:** IPSec is a fully integrated Avalanche application that supports many use cases, minimizing the number of test applications to learn

- Comprehensive statistics quickly identify problem areas
- Tunnel Control
    - Persistent and non-persistent tunnels
    - IKE Message Retry timers
        - Max Retry
        - Expire timers
    - Commit Bit support
    - Advanced Re-Keying events capabilities
        - Phase 1 Reconnect
        - Phase 2 Re-Key with old key timer
        - SA lifetimes
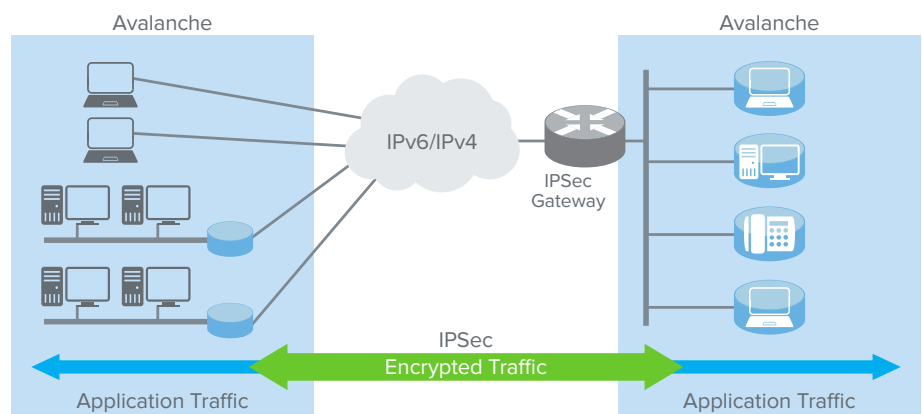
Technical Specifications

IPSec Security Protocols

- AH+ESP
- Tunnel Mode

IPSec Parameters

- Main Mode and Aggressive Mode
- Authentication
  - Pre-Shared Keys
  - X.509 Certificates
  - RSA Digital Signatures/Certificates
- Initial Contact Support
- Configurable Vendor ID
- Extended Authentication (XAuth)
  - ModeConfig address assignment
  - Generic (username and password)
  - RemoteVPN
  - Nortel Contivity
  - Checkpoint Hybrid
- IKE Phase 2
  - Quick Mode
  - Perfect Forward Secrecy (PFS)
  - Dead Peer Detection

- Tunneling and Encryption over IPv4 and IPv6
  - Support for IKEv1 and v2
  - IKEv1 Encryption Support
    DES, 3DES, ESPNULL, AES-128, AES-192, AES-256, AES-128-GCM-8, AES-256-GCM-8, AES-128-GCM-12, AES-256-GCM-12, AES-128-GCM-16, AES-256-GCM-16, AES-128-GMAC, AES-192-GMAC, AES-256-GMAC, HASH: HMAC-MD5 and HMAC SHA -1 Diffe-Hellman Groups: 1, 2, 5, 14, 15, 16, 19, 20, and 24
  - IKEv2 Encryption Support
  - DES, 3DES, ESPNULL, AES-128, AES-192, AES-256, AES-128-GCM-8, AES-256-GCM-8, AES-128-GCM-12, AES-256-GCM-12, AES-128-GCM-16, AES-256-GCM-16, AES-128-GMAC, AES-192-GMAC, AES-256-GMAC, HASH: HMAC-MD5, HMAC SHA -1, AES-XBCB-MAC, SHA-256, SHA-384, SHA-512 Diffe-Hellman Groups: 1, 2, 5, 14, 15, 16, 19, 20, and 24
  - Supports thousands of site-to-site tunnels per-test
  - Persistent and non-persistent tunnels
  - IKE Message Retry timers
    - Max Retry
    - Expire timers
  - Commit Bit Support
  - Re-Keying
    - Phase 1 Reconnect
    - Phase 2 Re-Key with old key timer
    - SA Lifetimes

Ordering Information

Description	Part Number
Avalanche IPSec for CF20	CMP-ASW-IPSEC-CF20
Avalanche IPSec for C100	CMP-ASW-IPSEC
Avalanche IPSec for Compatible Spirent TestCenter Modules (full chassis)	BPK-1204A
Avalanche IPSec for Compatible Spirent TestCenter Modules (2 Modules)	BPK-1204A-2XMOD

Available in license bundles for C1 and Avalanche Virtual.

Supported Modules/Platforms

- Spirent C100 Appliances
- Spirent C1 Appliances
- Spirent mX modules
- Software
  - Avalanche version 4.80 or higher with Avalanche IPSec option
- CF20
- AVR over CF20

Requirements

An IBM® compatible PC must meet the following minimum requirements to run Spirent Avalanche

- One 10/100/1000Base-T unshielded twisted pair (UTP) cable
- One 10 Mbps or 10/100/1000 Mbps Ethernet NIC
- Intel® E6300 Core 2 Duo 4 (or equivalent)
- Minimum of 4 GB of RAM
- Minimum of 50 GB free space on the hard drive
- Windows 7, 32 or 64-bit Operating Systems

Spirent Services

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements. For more information, visit the Global Services website atwww.spirent.com or contact your Spirent sales representative.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com