

Agilent NetworkTester

## IPsec Test Software

N4194A

Technical Datasheet



The Agilent NetworkTester IPsec Test Software provides the most scalable and feature-rich IPsec test solution available to test and qualify the performance of your IPsec network security device.



Agilent Technologies

## Key Features

- **Stateful application traffic over IPsec tunnels - determine real-world performance and scalability limits**
- **Configurable IPsec and IKE parameters - rapidly measure performance differences**
- **IPsec hardware acceleration available - increase encryption throughput**
- **Integrated IPsecv6 option - test next-generation IPv6 devices**

## Product Overview

The Agilent NetworkTester is the industry's most powerful test solution for performance testing of connection-aware and content-aware (Layer 4-7) devices and networks.

NetworkTester offers Internet-scale, multi-protocol, multi-port client/server traffic emulation capabilities, delivering unprecedented realism, flexibility and control for your most complex test challenges.

Being an integral part of the Network Tester solution, the IPsec test software meets all of the needs for testing IPsec performance and scalability.

Network equipment manufacturers, service providers and enterprise network operators can measure the IPsec performance metrics of network security devices and validate IPsec VPN network design and capacity before deployment.

Agilent NetworkTester IPsec Test Software can be easily configured to emulate thousands of IPsec clients and gateways, each initiating and establishing IPsec tunnels against a device under test (DUT). A variety of application traffic can then be generated over one of more IPsec tunnels to accurately simulate realistic VPN traffic profiles.

Security services such as VPN support, firewalls, spam/virus filtering and intrusion detection are converging onto integrated security gateways. The Agilent NetworkTester provides the capability to verify simultaneous operation of all security functions.

Agilent NetworkTester also provides access to many IKE and IPsec parameters to comprehensively test your IPsec implementation and help troubleshoot interoperability issues.

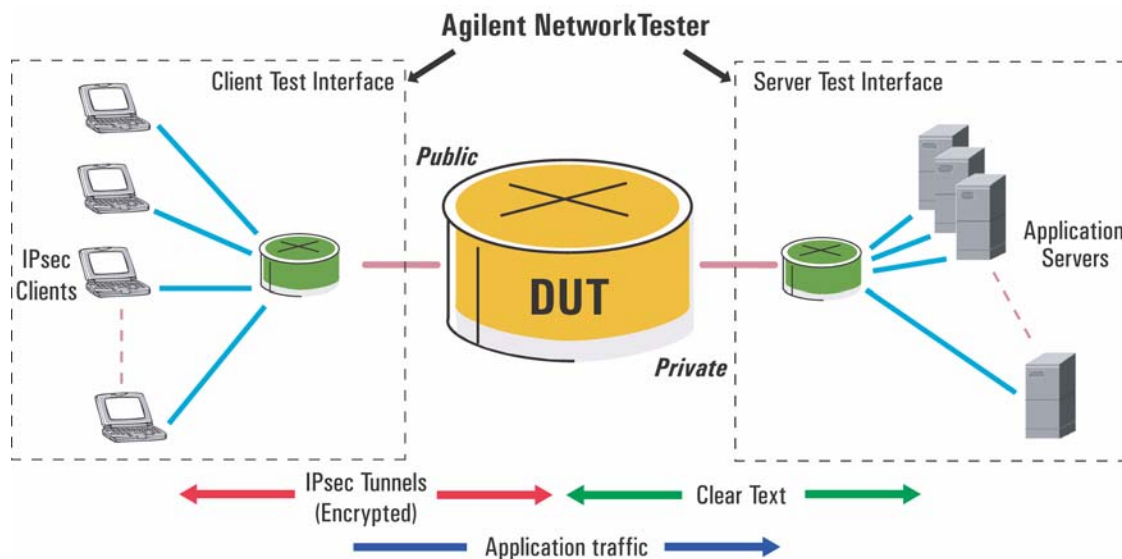


Figure 1: IPsec Test Configuration

## Product Features

### IPsec Performance and Scalability Benchmarking

The IPsec test software can emulate many IPsec clients and gateways, providing the capability to establish IPsec device performance benchmarks, such as:

- Maximum active IPsec tunnels
- IPsec tunnel setup rate and time
- IPsec stateful traffic throughput

### IPsec & SSL Hardware Acceleration

For high performance requirements, Agilent Network Tester supports dedicated hardware acceleration of the DES and 3DES IPsec encryption algorithms, and of the SSL encryption algorithm, for each test interface. Establish a higher number of IPsec

tunnels, faster tunnel setup rates and generate increased IPsec encrypted throughput against the device under test. Both IPsec and SSL can be accelerated simultaneously, enabling high-speed emulation of HTTPS traffic over IPsec tunnels.

### Stateful Application Traffic over IPsec

Client and server emulation of a broad range of application protocols is available to create real, stateful transactions over one or more IPsec tunnels. Generate a mix of application traffic including HTTP, FTP, SMTP, Instant Messaging (Jabber) and NFS, to realistically simulate VPN users. Measure the performance impact of IPsec processing on different applications.

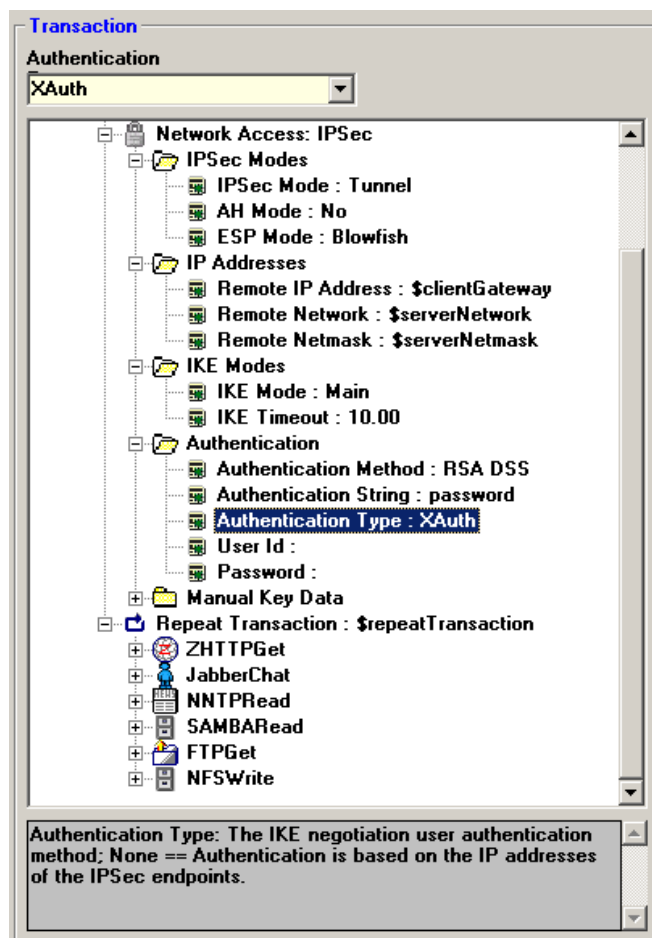


Figure 2: Rapidly configure stateful traffic over IPsec tunnels to measure real-world performance

### Verify IPsec Functionality

The IPsec test software provides a comprehensive IPsec and IKE implementation. Support for today's most important encryption algorithms, such as 3DES and AES, allows essential IPsec throughput measurements to be collected. The impact of protocol settings on IPsec tunnel setup rates can be verified by modifying the numerous IKE parameters.

### Flexible and Integrated User Interface

The NetPressure software application allows complex and large-scale IPsec test scenarios to be created quickly and easily through a single integrated user interface. Powerful test plans can be developed interactively with a few GUI operations in minutes (without the need for scripting) and easily saved for later use. Duplicate and adapt the supplied sample test plans to quickly build new test cases. In addition, this same flexibility is available through a Tcl/Tk application programming interface (API) for automated test environments.

### Applicable IPsec Standards

**RFC 2401:** Security Architecture for the Internet Protocol

**RFC 2402:** IP Authentication Header

**RFC 2403:** The Use of HMAC-MD5 within ESP and AH

**RFC 2404:** The Use of HMAC-SHA-1 within ESP and AH

**RFC 2405:** The ESP DES-CBC Cipher Algorithm With Explicit IV

**RFC 2406:** IP Encapsulating Security Payload (ESP)

**RFC 2407:** The Internet IP Security Domain of Interpretation for ISAKMP

**RFC 2408:** Internet Security Association and Key Management Protocol (ISAKMP)

**RFC 2409:** The Internet Key Exchange (IKE)

**RFC 2410:** The NULL Encryption Algorithm and Its Use With IPsec

**RFC 2411:** IP Security Document Roadmap

**RFC 2412:** The OAKLEY Key Determination Protocol

**Draft-beaulieu-ike-xauth-02.txt:** Extended Authentication within IKE (XAUTH)

## Technical Specifications

### IPsec Parameters

The following IPsec parameters and associated options are supported:

IPsec Protocols	ESP AH with ESP Both
Protocol Mode	Tunnel Transport
Encryption Algorithms	DES* 3DES* AES (128) Blowfish (128)
Authentication Algorithms	MD5 SHA1
Authentication Methods	Preshared keys RSA Digital Signatures
IKE Modes	Main Mode (Phase I) Aggressive Mode (Phase I) Quick Mode (Phase II) Manual Keying
Manual Keying	Yes
Diffie-Hellman Groups	1 2 5
Extended Authentication (XAuth)	Simple (User/Password)

### Statistics

IPsec statistics collected during a test can be displayed numerically, graphically or saved to a file. When IPsec is applied, application statistics refer to the application traffic secured by IPsec.

Statistic	Description	Units
Total IPsec Tunnels	Number of IPsec tunnels established	Tunnels
Cumulative IPsec Tunnels	Number of IPsec tunnels established since the start of the test	Tunnels
IPsec Tunnel Setup Rate	Number of IPsec tunnels established per second	Tunnels/sec
Minimum IPsec Tunnel Setup Time	Minimum time taken to establish an IPsec tunnel	Seconds
Maximum IPsec Tunnel Setup Time	Maximum time taken to establish an IPsec tunnel	Seconds

Average IPsec Tunnel Setup Time	Average time taken to establish an IPsec tunnel	Seconds
L4-7 Throughput	Application throughput (TCP payload) transported over IPsec tunnels	Kilobytes/second Megabits/second Megabytes/second
Interface Throughput	Interface (Ethernet frame) throughput	Packets/second Kilobytes/second Megabits/second Megabytes/second
Application Transfer Rate	Number of object (URL, file, MPEG, mail message, etc.) transfers per second	Transfers/second
Application Transfer Time (Clients)	Time taken to complete an object (URL, file, MPEG, mail message, etc.) transfer	Seconds
Application Transfer Time (Servers)	Time taken from writing first block of object data (URL, file, MPEG, mail message, etc.) to writing last block of object data	Seconds
Total Sessions	Number of TCP socket connections opened	Sessions
Session Rate	Number of TCP socket connections opened per second	Sessions/second
Minimum Connect Time	Minimum time taken to open a TCP socket connection	Seconds
Maximum Connect Time	Maximum time taken to open a TCP socket connection	Seconds
Average Connect Time	Average time taken to open a TCP socket connection	Seconds

\* Hardware acceleration supported with N4190B and N4191B traffic modules

**Application Traffic**

The following application traffic can be secured using IPsec:

DNS	Clients and Servers
FTP	Clients and Servers
H.323	Clients (for client-to-client emulation) For further information please refer to the N4195A VoIP Test Software Technical Datasheet
HTTP	Clients and Servers (1.0, 1.1)
HTTPS	Clients and Servers (SSLv2, SSLv3, TLSv1)
JABBER	Clients and Servers
NFS	Clients
NNTP	Clients
PING	Clients
POP3	Clients and Servers
RTP	Clients (send, receive, and bidirectional for client-to-client emulation) RTCP emulation optional; configurable rate
RTSP	Clients and Servers (MPEG-II, MPEG-III, MOV)
SAMBA	Clients
SIP	CClients (for client-to-client emulation) For further information please refer to the N4195A VoIP Test Software Technical Datasheet
SNMP	Clients
SMTP	Clients and Servers
TELNET	Clients and Servers
TRACEROUTE	Clients

**Miscellaneous**

Diagnostics	Per Tunnel Per Phase
IP Addressing	Same IP/MAC Unique IP/Same MAC Unique IP/MAC

**Configuration**

Please see the NetworkTester Configuration and Ordering Guide for more information.

**Product Numbers**

**N4194A NetworkTester IPsec Software License for IPv4/v6**

Adds IPsec protocol emulation to the NetworkTester system. When combined with the IPv6 software license, IPsecv6 is also provided.

**N4193A NetPressure IPv6 Software License**

Adds IPv6 protocol emulation to the NetworkTester system.

**N4195A NetworkTester VoIP Software License**

Adds VoIP protocol emulation to the NetworkTester system. When combined with the IPv6 software license, VoIPv6 is also provided. When combined with the IPsec software license, VoIPsec (VoIP over IPsec) is also provided. When combined with both the IPv6 and IPsecv6 software licenses, VoIPsecv6 (VoIP over IPsecv6) is also provided.

**N4190B - NetworkTester 10/100/1000 Base-T Ethernet Traffic Module with IPsec & SSL Hardware Acceleration**

Stackable 2-port multi-rate test module with hardware-accelerated IPsec and SSL performance. Includes NetPressure software license for this module.

**N4191B - NetworkTester 1000 Base-SX Ethernet Traffic Module with IPsec & SSL Hardware Acceleration**

Stackable 2-port test module with optical interfaces and hardware-accelerated IPsec and SSL performance. Includes NetPressure software license for this module.

This page intentionally left blank.

## Agilent's NetworkTester Solution

Agilent's NetworkTester solution offers a powerful and versatile test platform to address the evolving test needs of connection and content aware devices and networks. NetworkTester provides Network Equipment Manufacturers, Public Network Operators and Private Enterprise Network Managers with the industry's leading solution for multi-protocol, multi-port traffic emulation for performance analysis of today's L4-7 networking devices.

## Warranty and Support

### Hardware Warranty

Agilent warrants all NetworkTester hardware against defects in materials and workmanship for a period of 1 year from the date of delivery. Agilent further warrants that the NetworkTester will conform to specifications. During the warranty period, Agilent will, at its option, repair or replace the defective hardware. Services provided under this warranty will normally require return of the hardware to Agilent.

### Software Warranty

Agilent warrants all NetworkTester software for a period of 90 days. Agilent warrants that the software will not fail to execute its programming instructions due to defects in materials and workmanship when properly installed and used on the hardware designated by Agilent. This warranty only covers physical defects in the media, whereby the media is replaced at no charge during the warranty period.

### Software Updates

With the purchase of any new system controller Agilent will provide 1 year of complimentary software updates. At the end of the first year you can enroll into the Software Enhancement Service (SES) for continuing software product enhancements.

### Support

Technical support is available throughout the support life of the product. Support is available to verify that the equipment works properly, to help with product operation, and to provide basic measurement assistance for the use of the specified capabilities, at no extra cost, upon request.

### Ordering Information

To order and configure the test solution consult your local Agilent field engineer.

### United States:

Agilent Technologies  
Test and Measurement Call Center  
P.O. Box 4026  
Englewood, CO 80155-4026  
1-800-452-4844

### Canada:

Agilent Technologies Canada Inc.  
5150 Spectrum Way  
Mississauga, Ontario  
L4W 5G1  
1-877-894-4414

### Europe:

Agilent Technologies  
European Marketing Organisation  
P.O. Box 999  
1180 AZ Amstelveen  
The Netherlands  
(31 20) 547-2323  
  
United Kingdom  
07004 666666

### Japan:

Agilent Technologies Japan Ltd.  
Measurement Assistance Center  
9-1, Takakura-Cho, Hachioji-Shi,  
Tokyo 192-8510, Japan  
Tel: (81) 426-56-7832  
Fax: (81) 426-56-7840

### Latin America:

Agilent Technologies  
Latin American Region Headquarters  
5200 Blue Lagoon Drive, Suite #950  
Miami, Florida 33126  
U.S.A.  
Tel: (305) 269-7500  
Fax: (305) 267-4286

### Asia Pacific:

Agilent Technologies  
19/F, Cityplaza One, 1111 King's Road,  
Taikoo Shing, Hong Kong, SAR  
Tel: (852) 3197-7777  
Fax: (852) 2506-9233

### Australia/New Zealand:

Agilent Technologies Australia Pty Ltd  
347 Burwood Highway  
Forest Hill, Victoria 3131  
Tel: 1-800-629-485 (Australia)  
Fax: (61-3) 9272-0749  
Tel: 0-800-738-378 (New Zealand)  
Fax: (64-4) 802-6881

[www.agilent.com/comms/networktester](http://www.agilent.com/comms/networktester)

