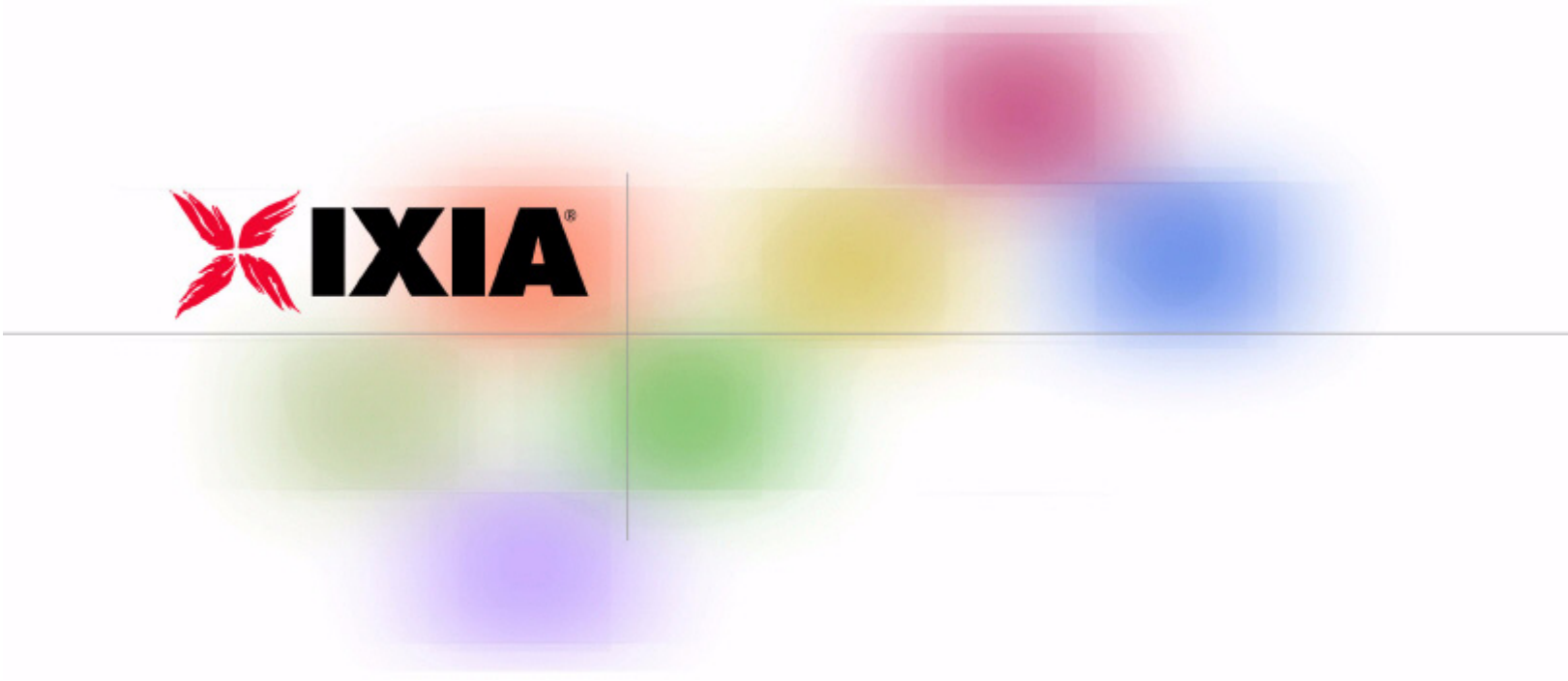
whitepaper

IPSec Virtual Private Networks
Conformance and Performance Testing



Contents

Ixia
26601 W. Agoura Road
Calabasas, CA 91302
Phone: (818) 871-1800
Fax: (818) 871-1805
Email: info@ixiacom.com
Internet: www.ixiacom.com

IPSec Virtual Private Networks: Conformance and Performance Testing

Abstract

With IPSec VPN technology, organizations can use the public Internet as the backbone for their communications network infrastructure, achieving global reach and significant cost savings, while maintaining the security of internal communications. However, successful IPSec product development and implementation present specific challenges: maintaining IPSec protocol conformance and managing the effect of IPSec VPNs on network performance. These challenges are best addressed by an appropriate testing methodology, as demonstrated by Ixia's approach to IPSec conformance and performance testing.

Introduction

Organizations invest significantly in their communications and information infrastructures, and for good reason. Advanced network applications and globalization now enable, and require, these infrastructures to support complex world-wide networks for enterprise businesses, governments, and the military. The cost of maintaining and upgrading these infrastructures continues to grow, driven by:

- The need for pervasiveness: world-wide organizations require global access to their networks.
- The need to maintain the security, privacy, and reliable performance of communications across the growing network.

This accelerating cost has fueled the search for an alternative to privately owned communications infrastructures. At the same time, the Internet's rapid growth offers tantalizing potential as the backbone of such an alternative. Organizations that have traditionally maintained private, closed systems, have begun to look at the potential of the Internet as a ready made resource. The Internet is inexpensive, and globally pervasive: every phone jack on earth is a potential terminus. What the Internet has lacked as a business network is security.

IPSec virtual private network technology surmounts that obstacle, and has proved an increasingly popular way for organizations to leverage the Internet infrastructure, and to use that resource securely.

VPNs and IPSec Technology

For an organization, internal communication must be private—reliably and demonstrably so. The Internet is, of course, anything but private.

Virtual private networks, or VPNs, create secure connections, called tunnels, through public shared communication infrastructures like the Internet. These tunnels are not physical entities, but logical constructs, created using encryption, security standards, and protocols.

As these standards and protocols have continued to evolve, various VPN technologies have emerged. IPSec VPNs are at the forefront of current secure VPN technologies.

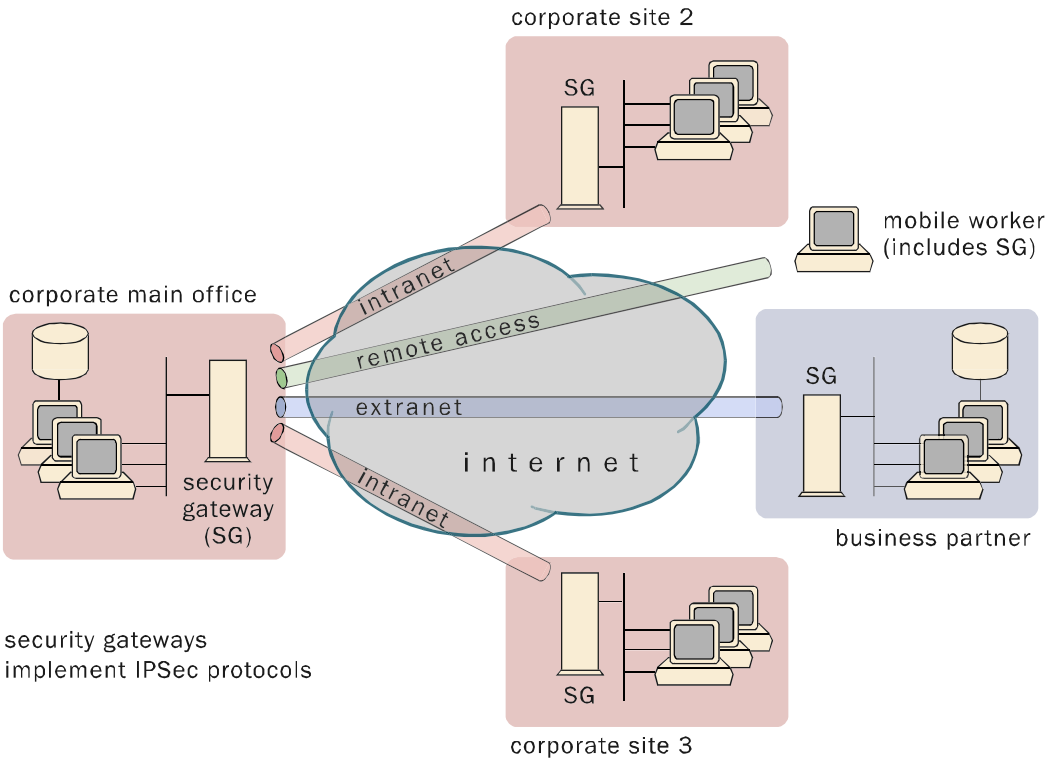


Figure 1. IPSec VPNs establish secure tunnels through the public Internet.

Benefits of IPSec VPN technology

Secure IPSec VPN connections through the Internet result in tremendous savings over the cost of a private WAN connection, leased lines, or long distance phone charges. IPSec VPNs can also increase an organization's productivity.

- Through an IPSec VPN, an organization can grant restricted network access to business partners, customers, or vendors, dramatically increasing the efficiency and speed of business-to-business communications, sales and order processing, and customer service management.
- Home-office workers, telecommuters, and in-the-field sales and service workers can access the corporate network resources securely and economically with IPSec VPN remote access through the public Internet.
- Global, economical access to an organization's network extends the organization's reach to markets formerly too remote or small to target or service profitably.

These benefits have made IPSec VPN solutions increasingly popular with global organizations. This represents a growing, and potentially huge market for manufacturers and providers of VPN-related products and services.

What is IPSec?

IPSec is a set of open standards and protocols for creating and maintaining secure communications over IP networks. IPSec VPNs use these standards and protocols to ensure the privacy and integrity of data transmission and communications across public networks like the Internet.

IPSec security services

IPSec establishes standards for a range of services to address security risks for all IP traffic across the public network:

- **Confidentiality.** Encryption protects the privacy of communications even if they are intercepted.
- **Access control.** Access to IPSec VPN private communications is restricted to authorized users.
- **Authentication.** Authentication verifies the source of received data (data origin authentication), and confirms that the original IP packet was not modified in transit (connectionless data integrity).
- **Rejection of replayed packets.** An anti-replay service counters a replay attack based on an attacker's intercepting a series of packets and then replaying them.
- **Limited traffic flow confidentiality.** Inner IP headers can be encrypted to conceal the identities of the traffic source and destination (beyond the security gateways).

How IPSec works

Before two devices can establish an IPSec VPN tunnel and communicate securely through it, they must agree on the security parameters to use during communication, establishing what is called a security association (SA). The SA specifies the authentication and encryption algorithms to be used, the encryption keys to be used during the session, and how long the keys and the security association itself are maintained. The Internet Key Exchange (IKE) protocol is used to set up the security associations needed for secure communication through an IPSec VPN.

In the negotiation process, one IPSec endpoint acts as an initiator and the other as a responder. The initiator offers the set of authentication, encryption and other parameters that it is ready to use with the other endpoint. The responder tries to match this list against its own list of supported techniques. If there is any overlap, it responds with the common subset. The initiator chooses one combination of techniques from the responder and they proceed with the negotiated setting. IKE negotiation has two phases:

- Phase 1 allows two security gateways to authenticate each other and establish communication parameters for Phase 2 communications. At the end of Phase 1, a Phase 1 Security Association (IKE SA) is established.
- Phase 2 allows two security gateways to agree on IPSec communications parameters on behalf of their respective hosts. At the end of Phase 2, an IPSec SA is established.

IPSec uses two protocols to establish security services -- the Authentication Header (AH) and Encapsulating Security Payload (ESP).

AH. The Authentication Header provides connectionless data integrity and data origin authentication for IP packets. It includes a cryptographic checksum over the entire packet. The receiver uses this checksum to verify that the packet has not been tampered with.

ESP. The Encapsulating Security Payload provides confidentiality for IP traffic through encryption. Current standard IPSec encryption algorithms include the *Triple Data Encryption Standard* (3DES), and the *Advanced Encryption Standard* (AES).

Besides confidentiality, ESP also provides authentication and anti-replay capabilities. Unlike AH, the authentication services of ESP do not protect the IP header of the packet. Most IPSec VPN implementations today use ESP.

AH and ESP may be used separately or together. How they are used depends on the IPSec mode: Transport mode or Tunnel mode. Client-to-LAN connections typically use Transport mode, while LAN-to-LAN connections typically use Tunnel mode.

IPSec VPN Challenges

As discussed earlier, cost savings and ubiquitous access make a compelling case for IPSec VPNs. The IPSec market has grown rapidly in the last few years and promises to grow even more rapidly. However, for the vendors of IPSec VPN equipment, for service providers, and for organizations deploying IPSec VPNs, significant technical issues remain.

To begin with, the dynamic nature of IPSec implementations requires IPSec gateway vendors to continually verify their implementations' compliance with standards to ensure correctness and interoperability. Performance and scalability must also be constantly upgraded and verified to satisfy the growing needs of the IPSec VPN industry.

Managed service providers and network managers must deal with the impact of IPSec VPNs on the performance of applications across the network, and with the interoperability of network elements and services in a multi-vendor environment.

These issues need to be adequately addressed by the IPSec community to ensure rapid growth. The IETF is in the process of updating some of the protocols used with IPSec VPNs (for instance, a newer version of IKE — called IKEv2). These present new and ongoing challenges to the IPSec community.

Why Test for IPSec Conformance?

While the IETF has specified the IPSec protocol standards for several years, early implementations were not completely standards-based and did not interoperate. For implementers of IPSec VPN services this is no longer acceptable.

From the IPSec gateway vendor's perspective, service providers and network managers require conformance to standards, often verifying this themselves to ensure interoperability. In a competitive market, vendors cannot afford to be proven wrong by their customers. Beyond ensuring interoperability, conformance testing provides vendors with significant benefits that are often overlooked. Conformance testing not only ensures the quality of the product, but also accelerates the product development — catching a bug, or correcting a design upstream in the development cycle, can have a huge effect on the product's ultimate profitability.

For service providers and network managers, a multi-vendor environment is the reality, a reality that is unmanageable without standards-based implementations. Since they also upgrade their IPSec VPNs periodically, ensuring that upgrades don't break an existing service becomes very important.

Not all conformance requirements are specific to IPSec, but the addition of IPSec protocols to the network increases the complexity of conformance testing, and the need for it.

Why Test for Scalability and Performance?

Scalability: IPSec requires that tunnels be set up between sites or clients and gateways before data can be sent. The number of users or sites the IPSec VPN service can scale to depends on how many of these tunnels the gateway can support. The maximum number of tunnels supported, or *tunnel capacity*, is a crucial metric vendors use to differentiate their products from the competition. A related, but often-overlooked metric, is *tunnel setup rate,* or the number of tunnels per second a device can establish. Tunnel capacity and setup rate are particularly important for large carrier-grade IPSec gateways with many sites or users.

Performance: Increased security comes at a performance cost, and security and performance are often traded off in IPSec implementations. IPSec can add latency and reduce throughput.

After the tunnels are set up, the IPSec gateways encrypt outbound traffic and decrypt traffic coming into the network. Encryption and decryption are by nature computationally intensive — this is partly why encrypted data stays secure. However, computational overhead means that the throughput through an IPSec tunnel is limited by the encryption and decryption capabilities of the gateways. In addition, encryption and decryption can add significant latency.

For IPSec gateway vendors, scalability and performance are competitive advantages that need to be measured. The move toward hardware-based, high performance systems makes these metrics more important than ever.

For service providers and network managers, scalability and performance top the list of vendor selection criteria, because they directly affect the quality of service. The increased latencies and decreased throughput resulting from IPSec implementation may disrupt a network's current applications and reduce network performance in general.

To summarize, the key metrics derived from performance testing of IPSec systems are tunnel capacity and setup rates, latency, and throughput.

IPSec Testing Challenges

As noted in the previous two sections, conformance, scalability, and performance testing are important for IPSec gateway vendors and users alike. For development test and quality assurance groups, this presents difficult challenges.

Conformance testing challenges

IPSec implementations are dynamic. Several vendors are upgrading their early software-based implementations for higher performance and scalability. At the same time, they are updating their feature set to the latest standards and protocol options. This, combined with aggressive project schedules, means that development test and quality assurance groups need an efficient way to verify the correctness of implementations on an almost daily basis.

Multiple RFCs define the IPSec protocol suite, including IKE, AH, and ESP and several associated protocols and options. To achieve adequate test coverage, a conformance test needs to create several hundred test cases, and these test cases need to be updated constantly. Since the test cycles are very frequent (daily in some cases), they need to be completely automated with a scripting interface. And because the device under test (DUT) needs to be re-configured for each of the hundreds of test cases, there is also a need to script the configuration of the DUT and batch the tests.

To address these challenges, most vendors use a third-party product that is maintained and supported by a dedicated third-party team.

Scalability and performance testing challenges

First generation IPSec gateways were not designed for scalability or high performance, so basic functional testing and small-scale emulation — often with a PC — was adequate. However, as the scale of the testing has increased, performance testing with a PC has become both unmanageable and too expensive.

Another testing approach is to have two IPSec gateways back-to-back and use traffic generators on either side. This approach also suffers from a number of inadequacies. With a back-to-back setup or with PC-based testing, accurate latency measurements are difficult, especially when the testing involves per-tunnel, per-stage timing information. Back-to-back tests do not point out interoperability and timing problems that may exist with respect to other IPSec gateways.

To address these issues, an IPSec-aware testing solution is required. To be really useful, this test tool needs the following characteristics.

Test solution requirements

Basic requirements. The test tool should be able to emulate gateways and hosts, act as the IPSec initiator, and establish tunnels with the device under test (DUT). It should be able to measure capacity and rates accurately.

The test solution should be highly scalable. The higher end of the current generation IPSec gateways require a single test system to scale to hundreds to thousands of tunnels, establish hundreds of tunnels per second, and send Gigabits of encrypted data per second.

It should support all important IPSec options. Algorithms like AES 256 are increasingly becoming important. The test tool should support these new IPSec options.

It should create a mixture of IPSec options easily. Most IPSec gateways support a variety of encryption algorithms (3DES, AES), several Diffie-Hellman algorithms (DH2, DH5, etc.) and several hash algorithms (MD5, SHA-1). The test tool should allow the user to easily configure tunnels with a mix of all these algorithms to test for border conditions. For example, the user may want to create 100,000 tunnels — say, 50 different combinations, with 2,000 tunnels for each combination.

It should provide detailed per-phase and per-tunnel statistics. A key issue in performance testing is the granularity of the results. Aggregate statistics do not provide adequate information to isolate a problem. Latencies should be reported on a per-phase basis: latency for IKE SA creation as well as latency for IPSec SA creation. Similarly, statistics need to be collected on a per-tunnel basis to isolate problems with certain tunnels.

It should be able to send stateful traffic over the tunnels. Once the tunnels are created, encryption and decryption latency need to be measured separately to verify that each is within acceptable limits: the encryption and decryption performance of a DUT may differ. To measure this, the testing solution should be able to both encrypt and decrypt the data. For enterprise users of IPSec VPNs, the testing solution needs to emulate the various enterprise applications over the IPSec tunnels, to ensure that the additional overhead is not disrupting the applications.

It should be automated. Because complex test scenarios need to be repeated frequently, with every update to the DUT, automation is extremely important. Of course, in a manufacturing environment, automation is a must.

Ixia's Approach to IPSec Testing

IPSec conformance

Ixia has addressed the challenges of protocol conformance testing by developing the industry standard conformance test suite, IxANVL (Ixia Automated Network Validation Library). The IxANVL IPSec suite contains over 500 test cases that include tests for IKE, AH and ESP, and supports a wide range of encryption and authentication algorithms, including 3DES, AES, Blowfish, MD5, and SHA. IxANVL provides positive as well as negative test cases.

IxANVL performs its tests as a dialog: it sends packets to the device being tested, receives the packets sent in response, and analyzes the response to determine the next action to take. This allows IxANVL to test complicated situations or reactions in a much more intelligent and flexible way than can be done by simple packet generation and capture devices.

IxANVL can be completely automated using a command-line interface. IxANVL source code is also available to users for customization allowing for greater flexibility.

IPSec scalability and performance

Ixia developed its IxVPN product as a solution for VPN performance testing. IxVPN uses Ixia's purpose-built hardware and provides an extremely extensible solution for validating the scalability and performance of the next generation of IPSec devices and networks.

IxVPN emulates IPSec gateways initiating tunnels on one side of the DUT and hosts on the other side, as shown in Figure 2. Each Ixia port can emulate thousands of IPSec secure gateways — each with unique Source IP and MAC addresses — creating realistic scenarios.

IxVPN makes it very easy to configure a large number of tunnels with varying IPSec parameters. Users can assign a percentage distribution to each option, and the application will automatically create the corresponding mix of IPSec tunnels.

Tunnel capacity testing methodology

To measure the tunnel capacity, the IxVPN initiator ports request tunnels sequentially until a user-defined number of tunnels fail.

Tunnel setup rate testing methodology

Tunnel setup rate is measured by sending a user-definable number of simultaneous tunnel requests. As more tunnels are set up, the rate is measured as a function of the number of tunnels already established.

All statistics, including capacity and tunnel setup rates, are presented in real-time at a fine granularity. Performance statistics are measured on a per-phase per tunnel basis. To assist users in initial troubleshooting, IxVPN also provides protocol message level debug information — again, on a per-tunnel basis.

Data performance testing methodology

Once the tunnels are established, stateful application data is sent over the tunnels using Chariot. The Chariot software mimics the traffic patterns of over 125 popular enterprise transactions. This gives a definitive assessment of how the deployment of IPSec will affect mission-critical applications.

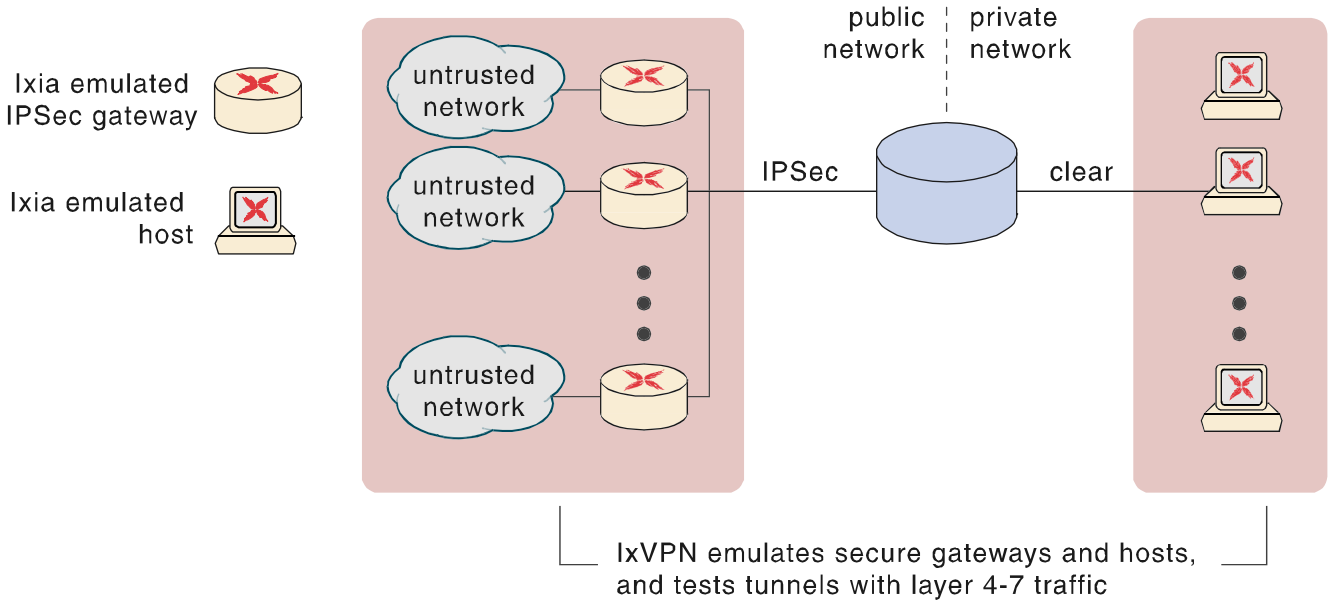


Figure 2. IxVPN network model.

Conclusion

With IPSec VPN technology, the public Internet can serve as the backbone of an organization's communications infrastructure, enabling the organization to realize significant savings and productivity gains. The growing popularity of IPSec VPNs establishes an important market for vendors of IPSec-related products and services.

However, in practice, IPSec technology is successful only if the impact of IPSec on network performance is managed. IPSec affects network throughput and adds latencies that can disrupt networked applications. IPSec implementations must also conform to standards, to ensure that IPSec network elements and applications interoperate in a multivendor environment.

To manage the impact of IPSec, the impact must be measured. For network managers and for vendors of IPSec-related products and services, a comprehensive and well designed conformance and performance testing solution is crucial to the success of IPSec VPN technology.

Appendix: IPSec Testing—an Example Test Plan

This appendix contains a brief plan for IPSec testing with specific examples showing how Ixia's solutions address the challenges of IPSec testing.

1. IPSec conformance test

Objective: To characterize the DUT's compliance to IETF standards

Test setup: IxANVL IPSec test suite running a set of positive and negative test cases against the DUT.

Methodology: IxANVL tests interpret the IPSec RFCs and present a number of scenarios to test the DUT.

1. Select a set of test cases to run in IxANVL.
2. Configure the DUT with the corresponding IPSec parameters and IP addressing using a set of scripts.
3. Run IxANVL in a batch mode with the scripts re-configuring the DUT between tests to match the IxANVL test setup.

Results: Number of tests passed/failed.

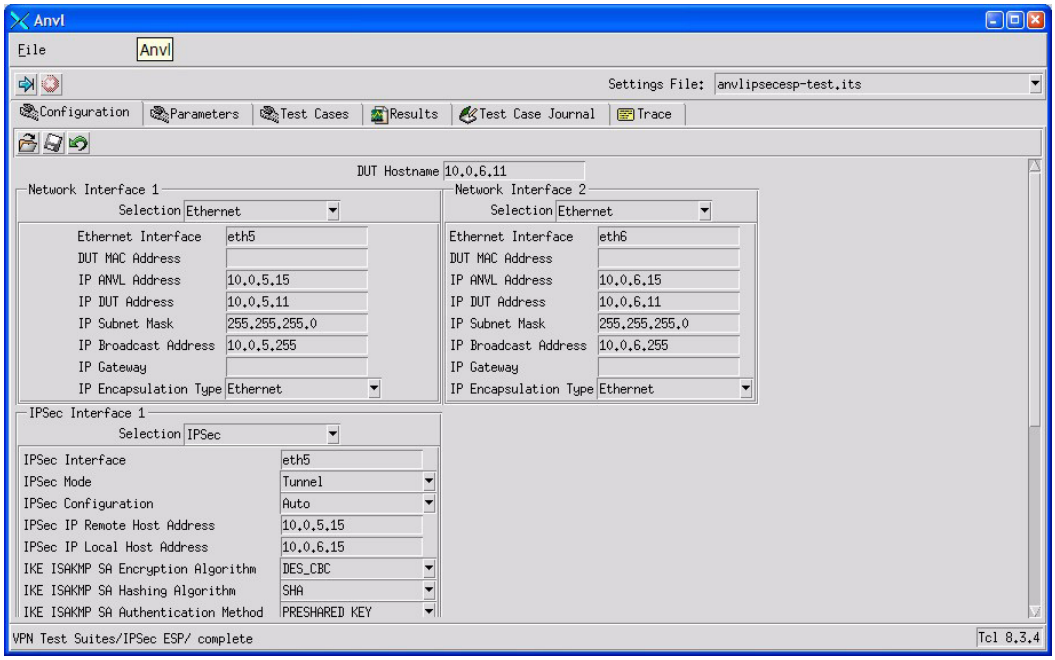


Figure 3. IxANVL — configuring the device under test for conformance testing.

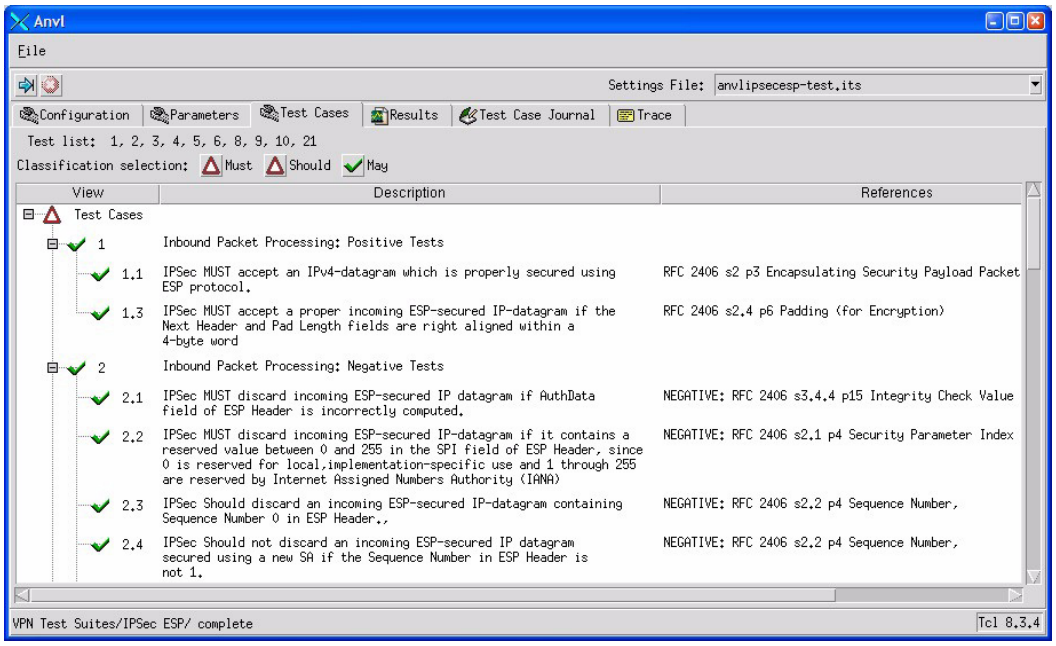


Figure 4. IPSec conformance testing in IxANVL — test cases.

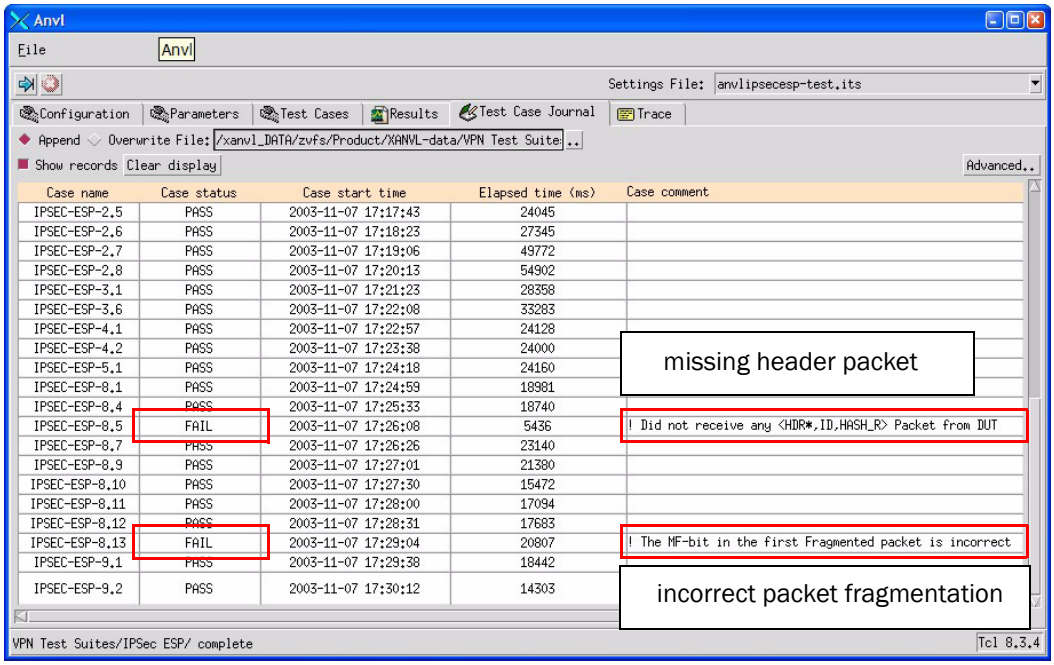


Figure 5. IPSec conformance testing in IxANVL — journal.

2. Tunnel scalability test

Objective: To determine the maximum number of tunnels a DUT can set up.

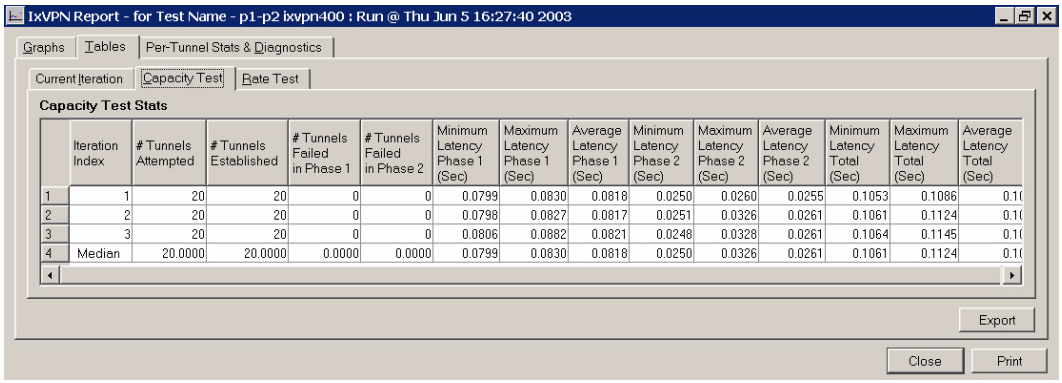
Test setup: Ixia's IxVPN product emulates secure gateways setting up IPSec tunnels against the DUT (as shown in Figure 2.)

Parameters: Varying IKE and IPSec protocols including different modes (tunnel mode and transport mode), varying Diffie-Hellman (dh1, dh2, dh5) and encryption protocols (3DES, AES 128 and AES 256).

Methodology:

1. Configure the DUT to accept tunnel requests from a number of peers.
2. In IxVPN, create a mix of IPSec tunnel parameters. Configure the DUT to match the crypto-parameters for each tunnel that IxVPN will initiate.
3. Set up tunnels sequentially against the DUT until a user-specified number of tunnels fail.
4. Repeat the test for multiple iterations
5. Repeat the test with various mixes.

Result: Maximum number of tunnels that can be set up by the DUT with varying parameters (Figure 6 and Figure 7).



	Iteration Index	# Tunnels Attempted	# Tunnels Established	# Tunnels Failed in Phase 1	# Tunnels Failed in Phase 2	Minimum Latency Phase 1 (Sec)	Maximum Latency Phase 1 (Sec)	Average Latency Phase 1 (Sec)	Minimum Latency Phase 2 (Sec)	Maximum Latency Phase 2 (Sec)	Average Latency Phase 2 (Sec)	Minimum Latency Total (Sec)	Maximum Latency Total (Sec)	Average Latency Total (Sec)
1	1	20	20	0	0	0.0799	0.0830	0.0818	0.0250	0.0260	0.0255	0.1053	0.1086	0.10
2	2	20	20	0	0	0.0798	0.0827	0.0817	0.0251	0.0326	0.0261	0.1061	0.1124	0.10
3	3	20	20	0	0	0.0806	0.0882	0.0821	0.0248	0.0328	0.0261	0.1064	0.1145	0.10
4	Median	20.0000	20.0000	0.0000	0.0000	0.0799	0.0830	0.0818	0.0250	0.0326	0.0261	0.1061	0.1124	0.10

Figure 6. Tunnel capacity test results.

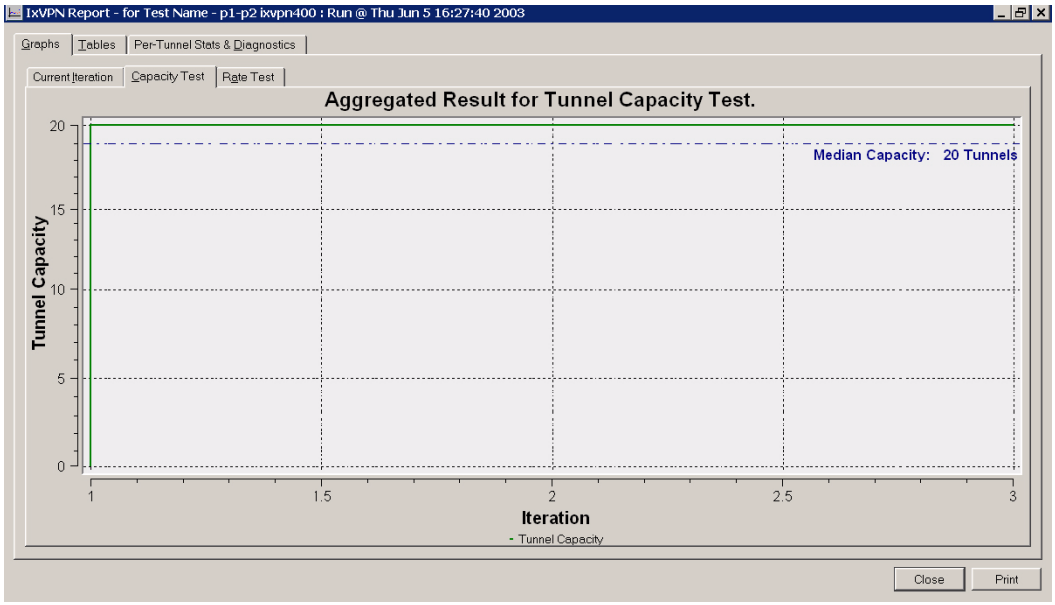


Figure 7. Tunnel capacity test results, graph view.

Creating mixes: example. As shown in Figure 8, the user can test a DUT with various combinations of IPSec tunnel parameters very quickly with IxVPN. While all combinations may not be used for a given deployment, the ability to create mixes quickly will be important to test border conditions.

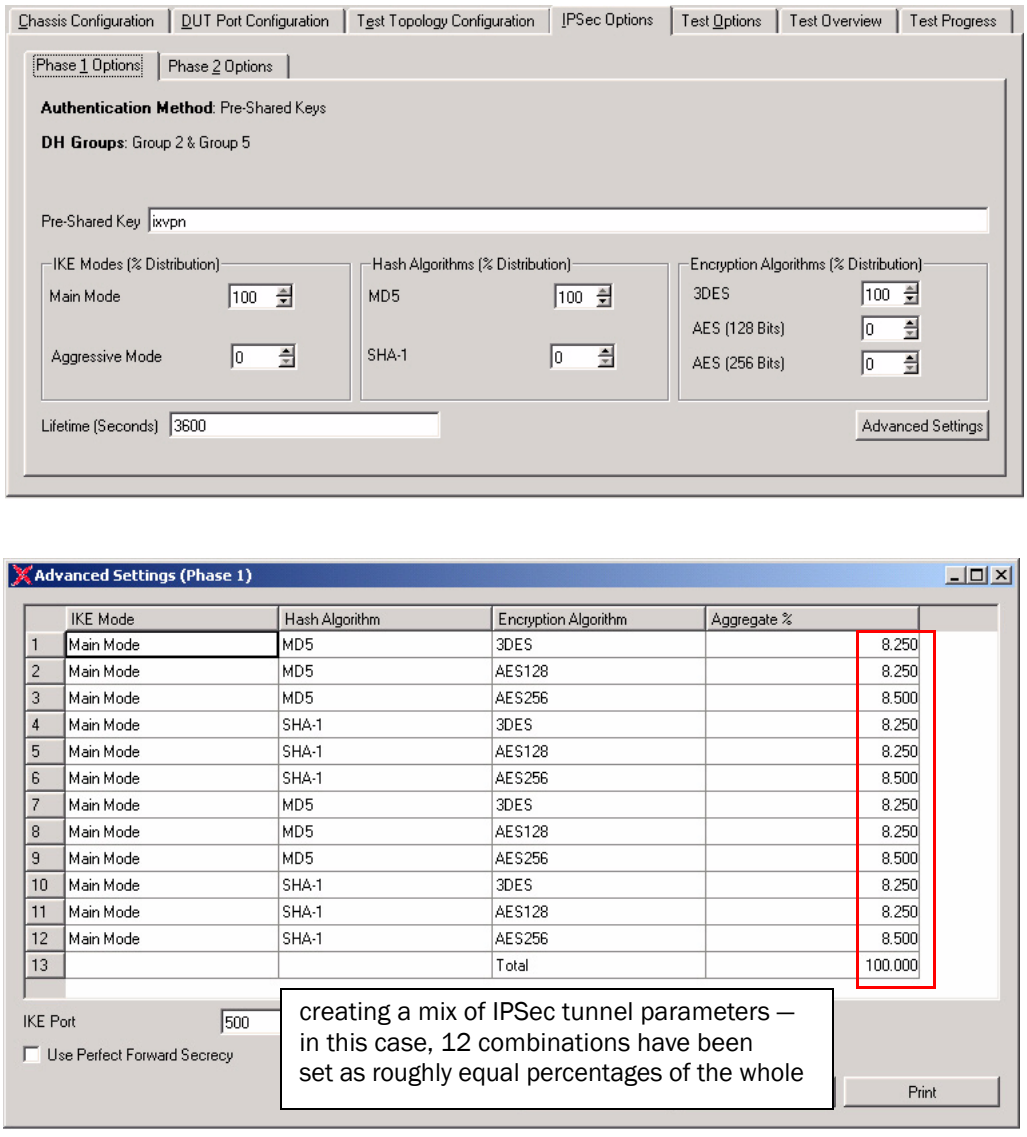


Figure 8. Using IxVPN to set combinations of IPSec parameters for testing.

3. Tunnel setup rate test

Objective: To determine the rate at which the DUT can set up IPSec tunnels under varying conditions.

Test setup: Ixia's IxVPN product emulates secure gateways setting up IPSec tunnels against the DUT (as shown in Figure 2).

Parameters: Varying IKE and IPSec protocols (as in the tunnel scalability test), as well as varying numbers of simultaneous requests to determine behavior under real-world conditions.

Methodology:

1. Configure the DUT to accept tunnels requests from a number of peers.
2. In IxVPN, create a mix of IPSec tunnel parameters. Configure the DUT to match the crypto-parameters for each tunnel IxVPN will initiate.
3. Initiate a number of simultaneous tunnel requests from IxVPN and measure setup rates with each set of requests.
4. Continue to set up new tunnels with varying number of simultaneous tunnel requests until a user specified number of tunnels fail (as the DUT reaches capacity).
5. Repeat the test for multiple iterations and with varying mixes.

Result: Tunnel setup rate as a function of established tunnels on the DUT. As shown in Figure 9, the rate drops significantly as the number of established tunnels increases.

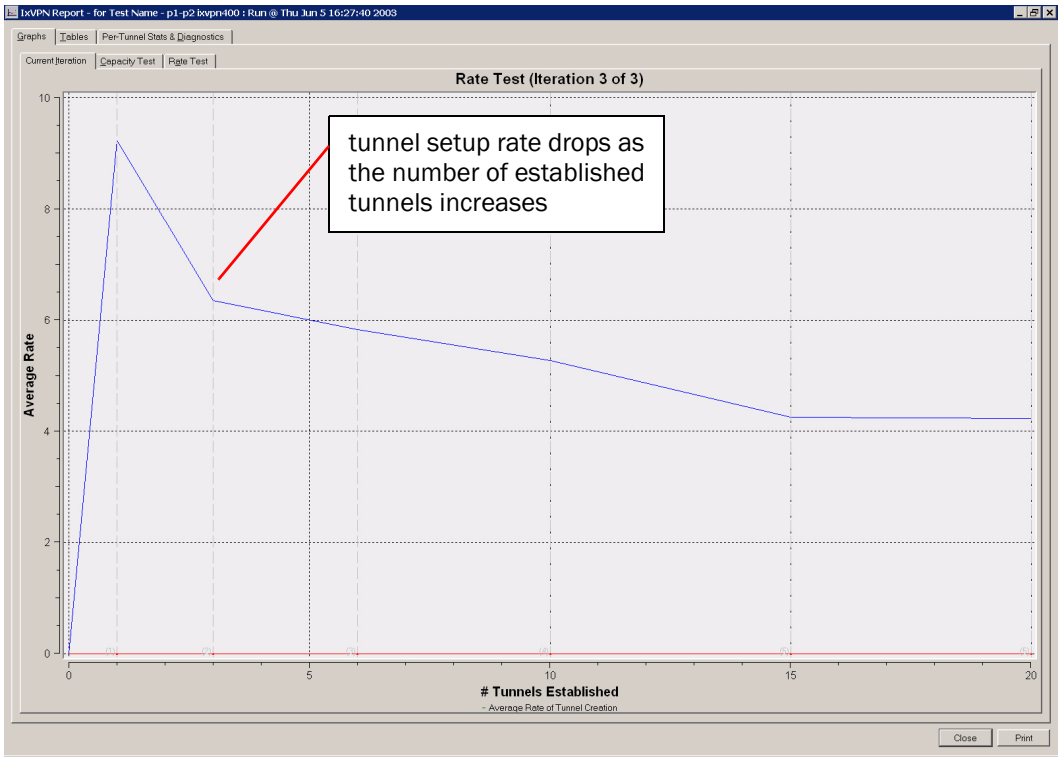


Figure 9. IxVPN tunnel setup rate test, single iteration.

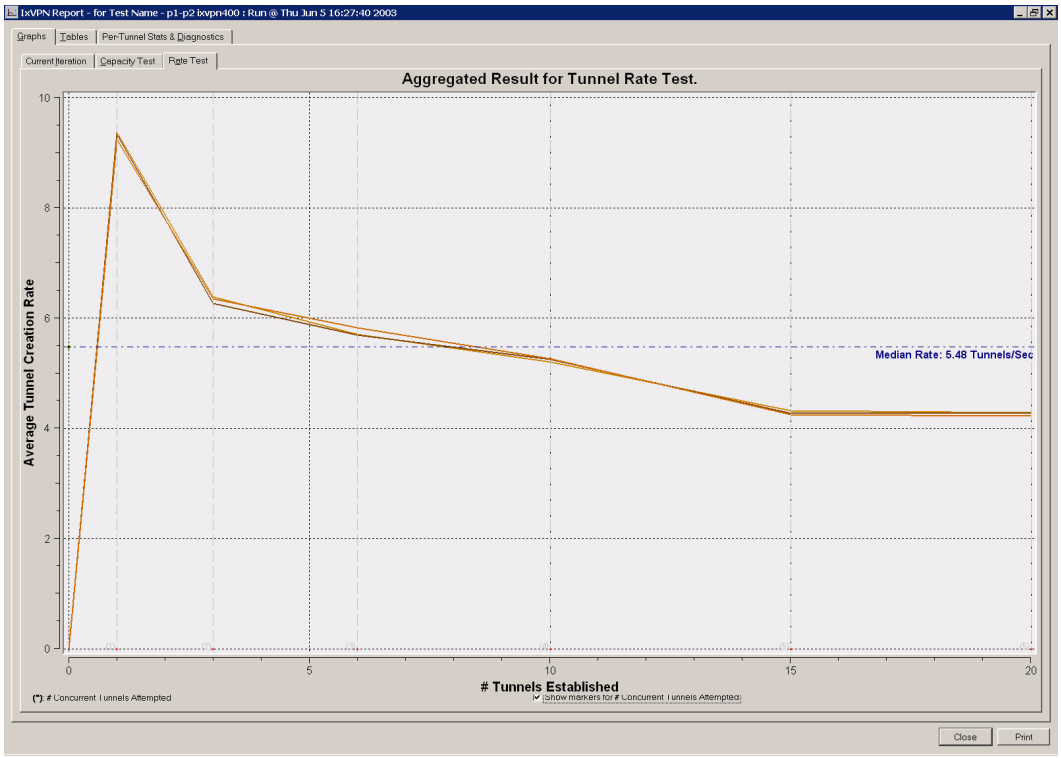


Figure 10. IxVPN tunnel setup rate test, aggregated results.

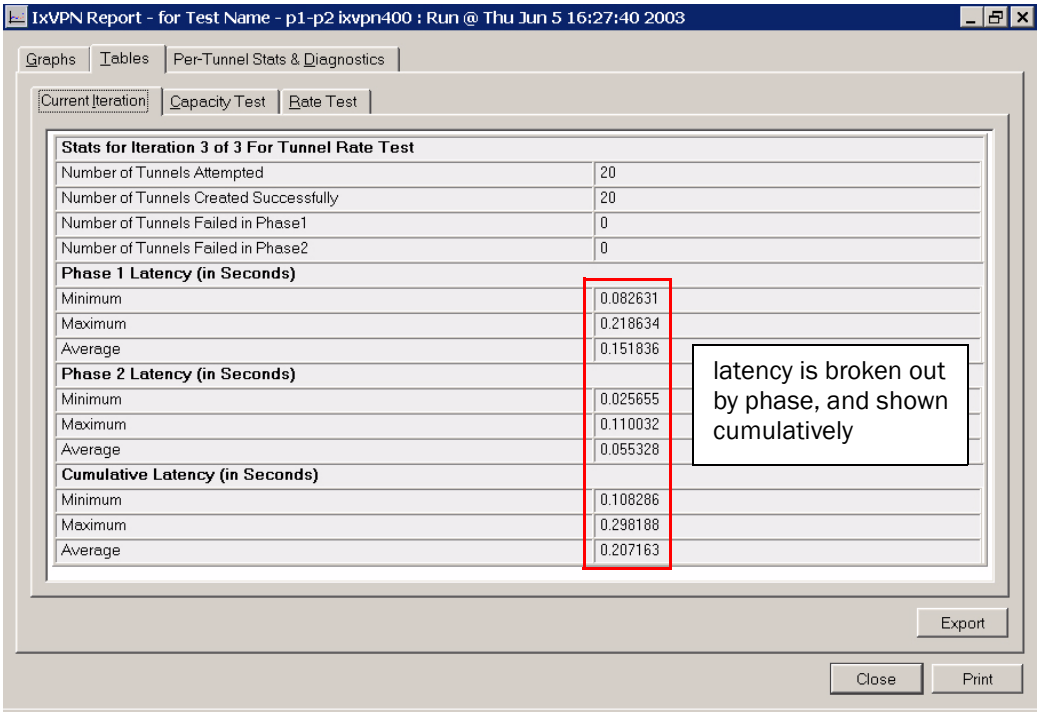


Figure 11. IxVPN setup rate test, statistics.

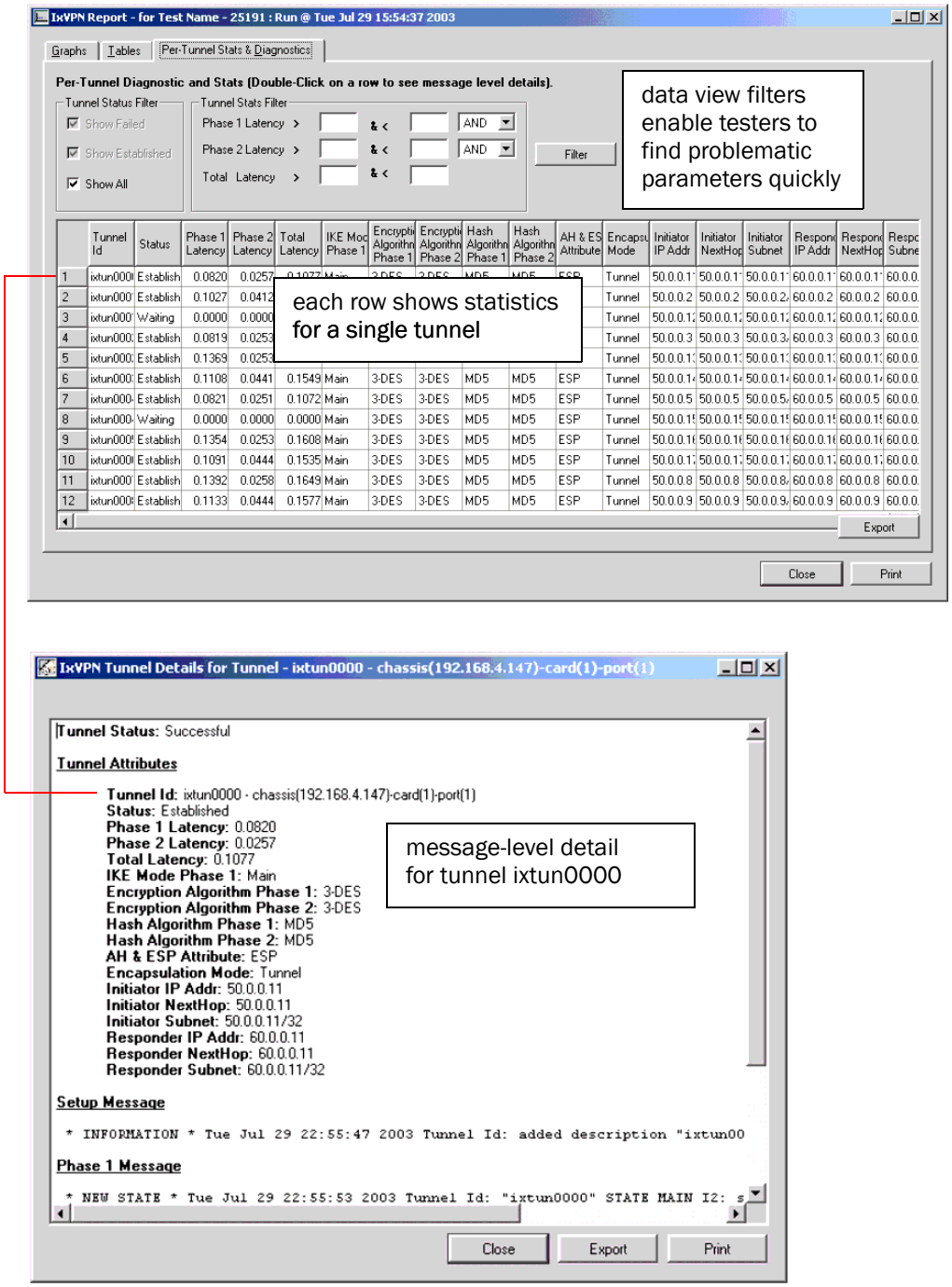


Figure 12. IxVPN per-phase, per-tunnel statistics.

Figure 12 shows statistics on a per-phase, per-tunnel basis. By using the data view filters, users can quickly see if certain tunnel parameters are causing performance problems.

4. Re-key tests

Objective: To determine the long-term stability of the DUT with re-keying, and the rate at which the DUT can re-key.

Test setup: Ixia's IxVPN product emulates secure gateways setting up IPSec tunnels against the DUT (as shown in Figure 2).

Parameters: Varying tunnel lifetimes and re-key intervals with various IKE and IPSec protocol.

Methodology:

1. Establish a number of tunnels against the DUT using IxVPN.
2. In IxVPN, configure the lifetime and re-key intervals to initiate re-keying.
3. At the specified re-key interval, IxVPN will initiate the re-key and measure any failures and also the rate at which the re-key is done by the DUT.
4. Repeat the test for multiple iterations and varying re-key intervals and parameters

Results: Number of re-key failures and re-key rate.

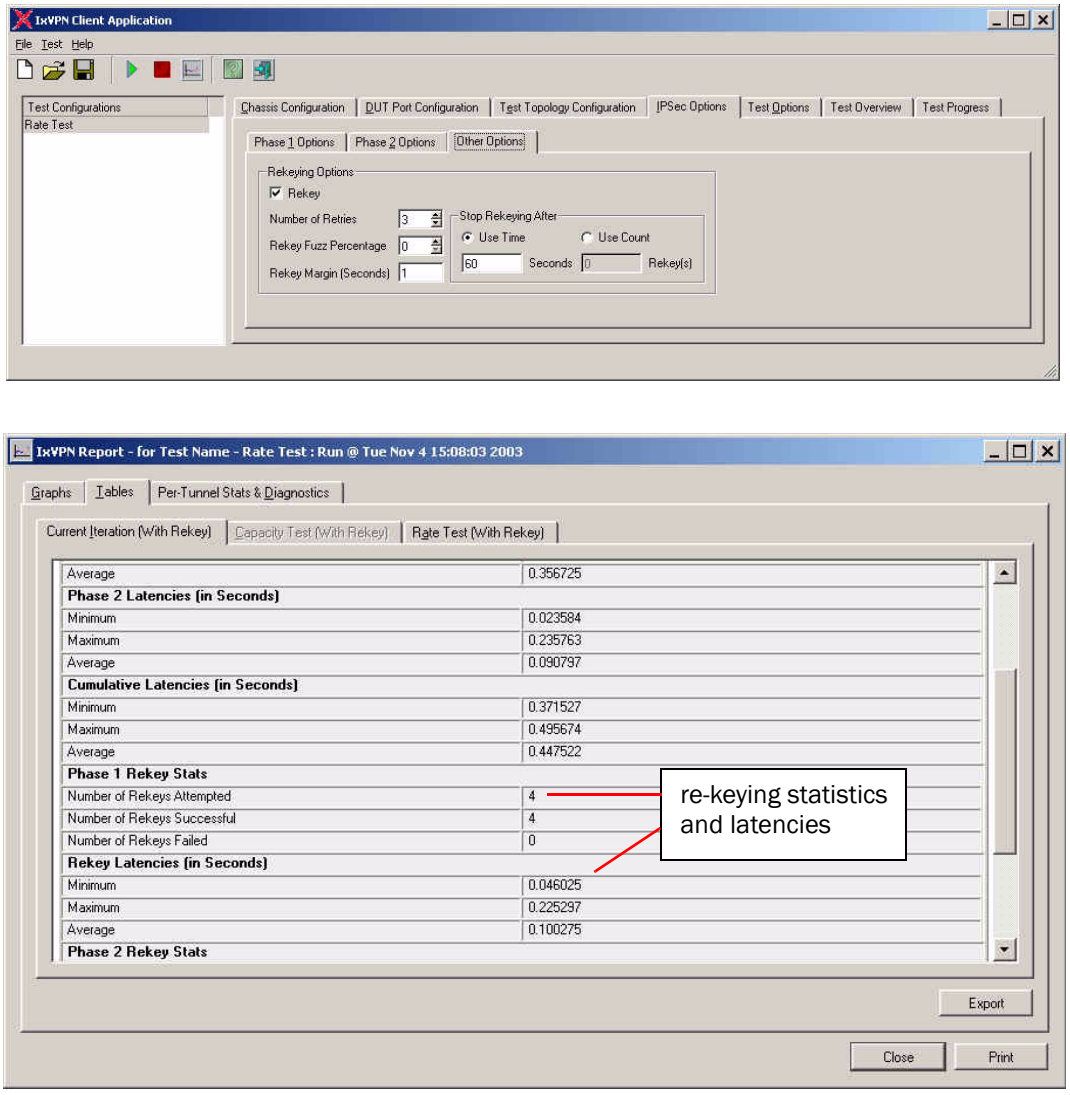


Figure 13. IxVPN re-keying test options and report.

5. Data performance test

Objective: To determine encryption and decryption performance of the DUT so that the impact of IPSec on application performance can be assessed. Key metrics are encryption and decryption throughput, latency, and loss.

Test setup: Once the tunnels are set up using IxVPN, the Chariot product is used to send data over the tunnels in a variety of traffic types.

Parameters: Varying application and transport protocols and packet sizes.

Methodology:

1. Set up a number of tunnels against the DUT using IxVPN with various parameters.
2. Set up Chariot end points on both the public and private side of the DUT.
3. Using the Chariot console, send data over each of the tunnels from the emulated gateway side as well as from the host side to measure encryption and decryption performance.
4. Repeat the test with varying packet sizes and IPSec parameters.

Results: Encryption and decryption throughput, latency, and loss. Chariot reports before and after establishment of IPSec tunnels, showing the impact of IPSec overhead on application traffic (Figure 14).

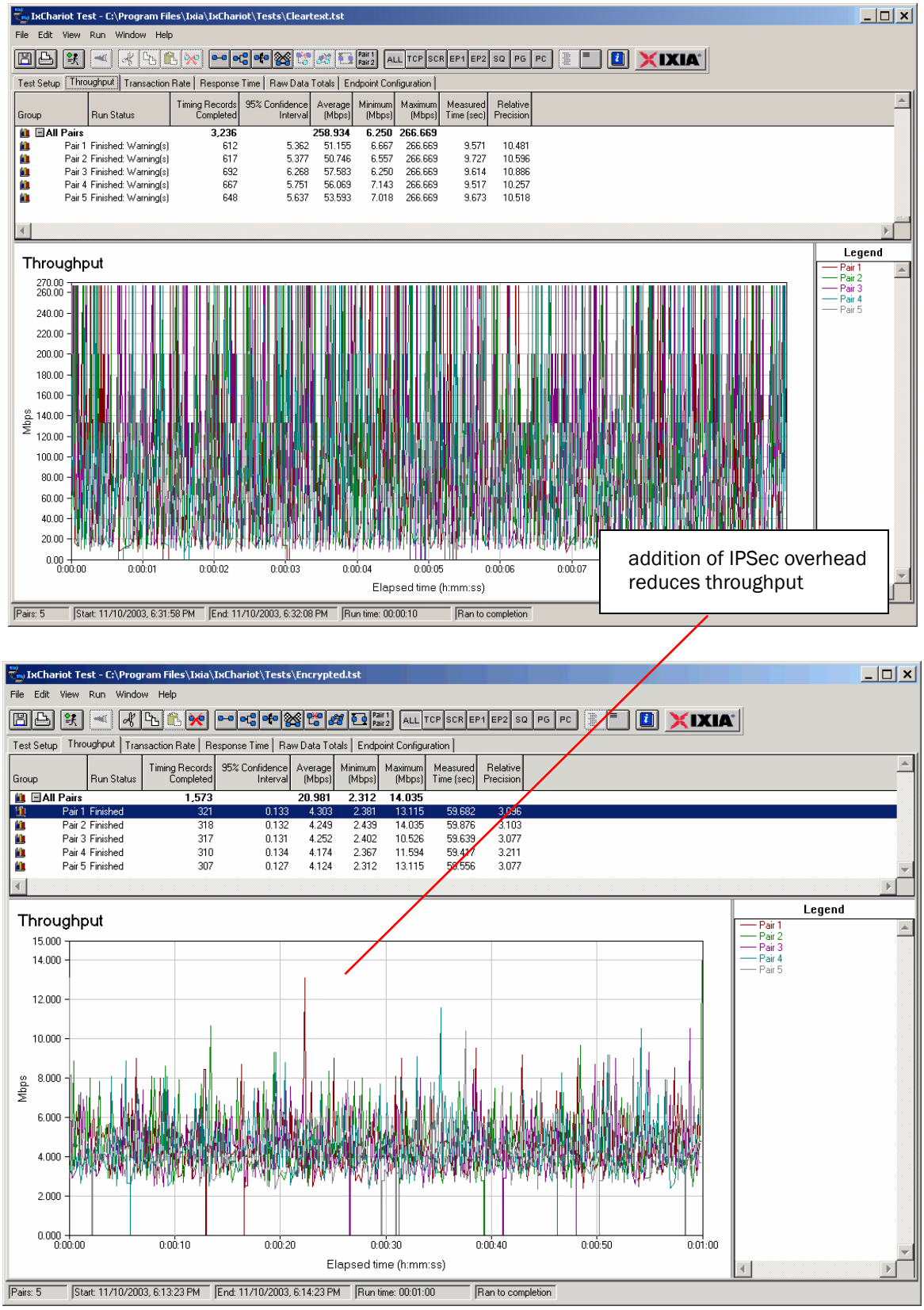


Figure 14. Chariot data performance test: before and after addition of IPSec traffic.

Glossary

Advanced Encryption Standard (AES) A new, faster, and more secure standard encryption algorithm, defined by the National Institute of Standards and Technology (NIST).

Authentication Header (AH) IPSec uses two protocols to establish security services -- the Authentication Header (AH) and Encapsulating Security Payload (ESP). The AH is security protocol, defined in RFC 2402, which provides data authentication and optional anti-replay services. AH ensures the integrity and data origin authentication of the IP datagram as well as the invariant fields in the outer IP header.
see also Encapsulating Security Payload (ESP).

Data Encryption Standard (DES) The Data Encryption Standard (DES) is a standard for a 56-bit encryption key; an older standard, it can be susceptible to brute force attacks.
see also Triple Data Encryption Standard, Advanced Encryption Standard.

Diffie-Hellman Developed by two mathematicians (Diffie and Hellman), this is a class of algorithms that implements public-private key cryptography.

Encapsulating Security Payload (ESP) IPSec uses two protocols to establish security services -- the Authentication Header (AH) and Encapsulating Security Payload (ESP). The ESP is a security protocol, defined in RFC 2406, which provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of security association (SA) establishment and on the location of the implementation in a network topology. ESP authenticates only headers and data after the IP header.
see also Authentication Header, Security Association.

Hash Algorithm A hash algorithm produces a unique fixed-length value from a variable-length message. Used to calculate a checksum as part of IPSec encryption process.

Internet Key Exchange (IKE)	The Internet Key Exchange (IKE) protocol is used to set up the security associations needed for secure communication through an IPSec VPN. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys. Note that IKE is an optional protocol within the IPsec framework and keys can also be manually configured.
Security Association (SA)	Before two machines can establish an IPSec VPN tunnel and communicate securely through it, they must agree on the security parameters to use during communication, establishing what is called a security association (SA).
Security Gateway	An intermediate system, such as a router or firewall, that implements IPSec protocols for a device or network.
Triple Data Encryption Standard (Triple DES, or 3DES)	The current encryption key standard for most business use, 3DES encrypts data three times with up to three different keys.

Acknowledgements

Authors: Sunil Kalidindi, Elliott Stewart