

White Paper

Validating IPsec Network Security Devices

Realistic Traffic Performance Measurement

A plethora of different connection-aware and content-aware appliances - such as VPN concentrators, content switches, and load balancers - is being deployed in private networks and in data centers to satisfy the security and content switching needs of enterprises. In response, manufacturers are combining the capabilities of this equipment into integrated devices such as IPsec-capable security routers, integrated security gateways, and all-in-one Data Center devices.

Validation of these devices can be complex. Although they may include IPsec, it is no longer adequate to test IPsec capabilities in isolation. Because the devices perform filtering or switching based on layer 4 to 7 information, it is unacceptable to merely test using instrumented layer 2 or 3 packets. The layer 4-7 capabilities must be tested together with IPsec to fully stress the device in a realistic manner.

This paper discusses IPsec test issues and shows you how to measure the latest security devices using a mix of real application traffic over IPsec tunnels. You will learn how to accurately gauge performance from the perspective of the end user's experience.



Agilent Technologies

Introduction

IPsec is a suite of protocols providing security services for data communications over public IP networks. It is one of the technologies used to implement and deploy Virtual Private Networks (VPNs) - a cost-effective alternative to building a private network for internal, corporate communications.

IPsec VPNs have been successfully deployed for remote-access and site-to-site communications for several years. The reasons for the success of IPsec VPNs are many:

- *Cost savings* - Using Internet Service Provider (ISP) connectivity is much less expensive than dedicated WAN circuits and leased lines.
- *Security* - Encryption and authentication algorithms keep enterprise data private and secure as it traverses the public Internet.
- *Scalability* - Adding new users and sites via an IPsec VPN connection is quick and cost-effective.
- *Global access* - With the rapid growth of the Internet and its global reach, it can extend the enterprise network to remote sites and new markets.

These benefits will continue to serve the popularity of IPsec VPNs, and will ensure IPsec remains the dominant VPN technology for years to come. Security at the edge is growing with the need to prevent outside security threats, as well as to accommodate a high corporate rollout of VPN access to remote users and sites. Security within the LAN is also gaining attention to enable secure communications within the enterprise. Both trends are driving the development of high-performance network security devices that support IPsec. These powerful new devices are driving the IPsec test needs beyond those of basic functional and interoperability testing and towards performance and scalability validation.

IPsec Basics

The IPsec suite of protocols was designed to provide authentication, replay protection, integrity and confidentiality services for data running over shared, public networks. It also includes mechanisms for automating the periodic exchange and generation of new keys, which are used by the various encryption and authentication algorithms.

Before secure traffic can pass over a public IP network, an IPsec VPN connection or tunnel must be setup between two peering devices. IPsec tunnel setup can also be automated by using the Internet Key Exchange (IKE) protocol, and it involves two phases of protocol negotiations:

- *Phase I* includes negotiation of the encryption and hash algorithms and the authentication method to be used; a Diffie-Hellman (DH) key exchange; and peer identity verification. Phase I establishes an IKE security association (SA), which provides a secure channel for subsequent protocol exchanges.
- Under the protection of the IKE SA, *Phase II* includes negotiation of the encryption and hash algorithms to be used, and the IPsec protocol to be used for IP traffic encapsulation - Authenticating Header (AH) or Encapsulating Security Payload (ESP). Phase II establishes an IPsec SA for each direction of IP traffic flow.

After Phase II completes, IP traffic can now securely travel over the IPsec tunnel - encrypted and/or authenticated as specified by the IPsec SA just created.

For a more detailed IPsec description, refer to the '*Agilent NetworkTester - IP Security (IPsec)*', technology primer.

Why Test IPsec Performance?

Device Manufacturers

Vendors of IPsec VPN appliances need to validate their IPsec implementations as well as measure the performance and scalability of their devices. The R&D teams need to test their IPsec features and fine tune the performance of their devices, while the system test groups are usually responsible for finding the IPsec performance limits and producing a set of publishable performance results. The security provided by IPsec comes at a performance cost - how well an IPsec device makes the trade-off between security and performance is a required measurement.

Network equipment manufacturers (NEMs) also demonstrate IPsec features and performance to their customers. Sales and marketing personnel are continually involved in product demonstrations, while proof-of-concept labs are required to demonstrate and qualify real IPsec VPN network designs for their customers.

IPsec performance is also a key variable used by device manufacturers to competitively position their products. Having the right test solution and methodology to accurately determine and demonstrate IPsec performance is crucial.

Service Providers

Many service providers offer various types of VPN services - be it fully managed CPE-based VPN solutions, network-based VPN solutions or outsourcing services for customers who manage their own CPE. Since IPsec is the leading VPN technology, IPsec performance is an important metric for service providers evaluating different IPsec VPN devices. With VPN adoption increasing as broadband access grows, service providers are facing challenges in scaling their networks and services to accommodate a growing number of VPN users. Service providers need to accurately benchmark the performance of different vendor devices and test VPN services and applications before deployment. This allows validation of their VPN network design and capacity, consistent with their customers' requirements.

Enterprise Network Operators

As with service providers, enterprise network operators must dimension their networks to handle the expected number of users and sites interconnected through IPsec VPNs. There are many different devices that support IPsec VPNs, each targeted for a specific network size and configuration, and also claiming certain performance figures. IPsec is supported in standalone VPN-only appliances as well as integrated security devices such as firewalls. Network managers need to evaluate all potential VPN devices and determine which performance and configuration combination will provide optimal application and network performance for their organization.

IPsec Test Challenges

With the growing rollout of remote-access and site-to-site IPsec VPNs, greater importance is being placed on testing IPsec performance and scalability. Testing IPsec devices with one or more PCs with limited application support may have been sufficient for simple functional testing, but is inadequate for high performance verification.

Continual improvements are being made to the performance and scalability of IPsec network security devices. These frequent upgrades require repeated verification. IPsec provides encryption and authentication services to IP traffic, but these services impose an overhead on VPN traffic transported between IPsec endpoints. It is important to test how well a device can maximize IPsec throughput and minimize application latencies across VPN connections. An IPsec device also needs to support a large number of concurrent IPsec tunnels and must be able to add new IPsec tunnels quickly. These measurements relate to how well a device will be able to scale to support large numbers of end users and applications.

Applications and services running over IPsec VPNs include email, web browsing, file sharing, application data streaming and various client/server programs. Accurate qualification of an IPsec device requires testing with real, stateful application traffic. As real-time voice and video become more common VPN applications, IPsec performance will also need to be tested with such applications. Many network security devices maintain state of TCP and UDP connections, and make forwarding and filtering decisions based on stateful packet inspection and application layer content. Using stateless traffic generation is insufficient - accurate performance characterization of an IPsec device requires testing with the kind of applications that will be running in a real IPsec VPN environment.

The capabilities of network security devices are also expanding. Initially, many network security devices were standalone systems that performed single functions - such as firewalls, VPN-only appliances and intrusion detection systems (IDSs). These individual systems are being integrated into single-blade or single-module solutions for routers and switches. The development of integrated security appliances is also growing. These appliances integrate multiple security functions such as VPN, firewall, intrusion detection, intrusion prevention and virus scanning onto the one device. This convergence of security functions imposes further test challenges to ensure that all functions can co-exist and operate simultaneously. For example, a firewall must be able to maintain traffic forwarding over IPsec VPN tunnels, while preventing a DoS attack at the same time.

Equipment vendors usually quote IPsec performance in isolation, while integrated security appliances are designed and developed to support multiple functions when deployed in real networks. For such devices, IPsec performance must be evaluated and measured in the presence of other functions.

Governments worldwide are encouraging and even mandating IPv6 support across networking equipment. In response, significant activity surrounding IPv6 testing is occurring, as vendors endeavor to have their devices IPv6-ready. Although originally designed into the IPv6 specification, IPsec was first widely used to protect traffic running over IPv4 networks. As IPv6 adoption grows, the testing of IPsecv6 will become increasingly important.

IPsec Test Scenarios

IPsec Performance Benchmarks

The key metrics and performance benchmarks commonly used for IPsec devices are:

- *IPsec Maximum Active Tunnels* - How many active IPsec VPN users a device can support simultaneously. (An active tunnel is defined as a tunnel that has been established and is actively transporting IP traffic.)
- *IPsec Tunnel Setup Rate and Time* - How quickly an IPsec device will be able to service VPN tunnel requests.
- *IPsec Stateful Traffic Throughput* - The application performance to expect from an IPsec VPN connection.

An important initial step to begin testing is to establish a test environment that simulates the network operating environment as closely as possible. Figure 1 illustrates such a test configuration to use when measuring IPsec performance benchmarks. In this configuration we have emulated IPsec VPN clients and security gateways that are used to initiate and establish one or more IPsec tunnels against the device under test (DUT). Application traffic is then configured for transmission over these IPsec tunnels. Note that it is also valid to execute the first two tests without any application traffic running, as it will measure raw IPsec performance of a device. However, a realistic test scenario is one where stateful application traffic is running.

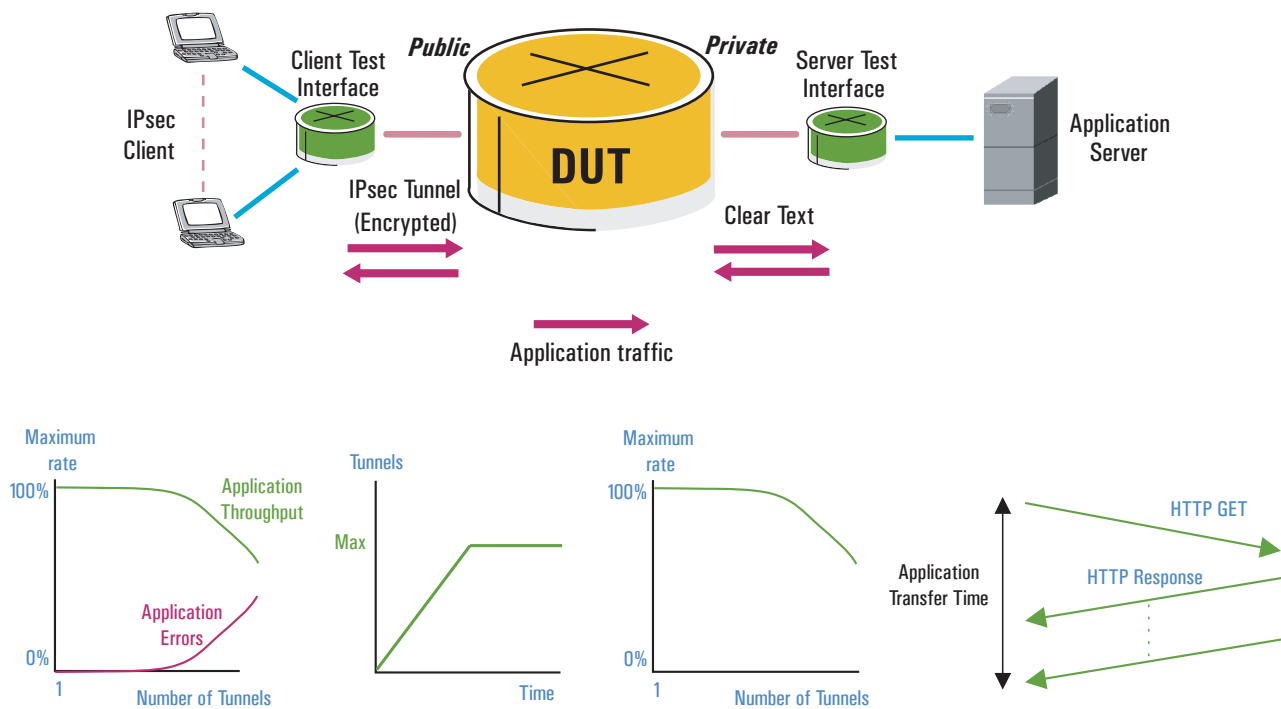


Figure 1: Testing IPsec Performance Benchmarks

There are various factors that will affect the test results or produce different test outcomes.

It is useful to measure IPsec tunnel setup rate as a function of the number of tunnels established. The rate may reduce as the number of established tunnels increases, because an increase in resource usage is required on the DUT to manage the existing IPsec tunnels. Tunnel setup time - the time taken to establish an IPsec tunnel (including both Phase I and Phase II negotiations) - is likely to increase as the number of established tunnels increases.

Validating IPsec Network Security Devices

Total, maximum application throughput will vary depending on the number of active IPsec tunnels. Throughput is usually greater across a smaller number of active tunnels. A limit will be reached beyond which the device cannot sustain error-free throughput over an increasing number of IPsec tunnels. This limit must be measured, and the relationship between application throughput per tunnel and the total number of active tunnels should be determined.

Measuring application transfer times and rates will help predict the application response times that clients should expect when using a specifically configured IPsec VPN connection.

IPsec allows for many different parameters to be negotiated during tunnel setup. All combinations of these different parameters need to be tested, and the way they affect the key performance metrics should be recorded:

- The encryption algorithm chosen will affect IPsec stateful traffic throughput because the processing requirements of each algorithm is different. For example, DES is much faster to compute than 3DES.
- DH group selection (key size) will affect the IPsec tunnel setup rate and time. The larger the key size, the slower the setup rate and the longer the setup time.
- The authentication method chosen can affect the IPsec tunnel setup rate and time. The use of digital signatures requires the exchange of digital certificates during tunnel setup. Lower setup rates and longer setup times may be seen, when compared to the use of preshared secrets.
- The hash algorithm selected can affect IPsec stateful traffic throughput and IPsec tunnel setup rate and time. The two algorithms used with IPsec are MD5 and SHA-1. SHA-1 is more secure, producing a 160-bit message digest, but comes at a performance cost.
- Perfect Forward Secrecy (PFS) is an option available for Phase II negotiations, which allows for an additional DH key exchange. Having PFS enabled may result in lower tunnel setup rates and longer tunnel setup times.
- One IKE SA can be used to secure multiple IPsec SAs and therefore multiple IPsec VPN tunnels. This configuration will affect tunnel setup rate and time because Phase I is not renegotiated for each tunnel request. This setting may also affect the maximum number of tunnels that can be established.

IPsec Realistic Traffic Performance

Figure 2 illustrates a test scenario used to reproduce a realistic user profile by transmitting a mix of application layer traffic over one or more IPsec tunnels. The purpose of the test is to verify the performance characteristics of an IPsec device when it needs to accommodate multiple tunnels, each carrying a mix of applications:

- How does a mix of user application data over one or more tunnels affect IPsec stateful traffic throughput?
- Is the maximum number of active tunnels the same?

Answering these questions will help determine how an IPsec device will perform when deployed in a real network.

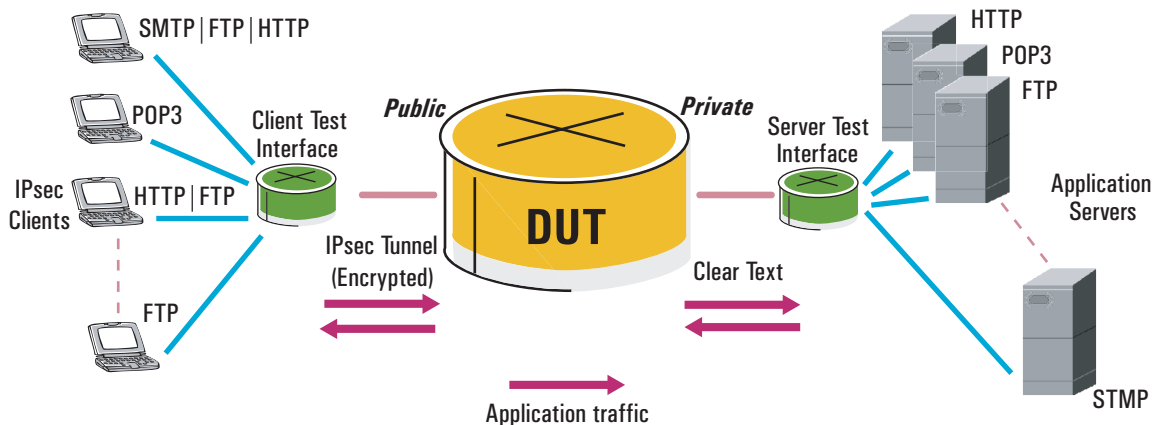


Figure 2: Testing IPsec Realistic Traffic Performance

Tests can also be performed to highlight the performance impact of IPsec processing on application traffic, and how it differs amongst applications. See Figure 3 to see results of such a test. Understanding why IPsec can have a greater performance impact on certain applications is important in evaluating whether an IPsec device will fit the needs of VPN users and their applications.

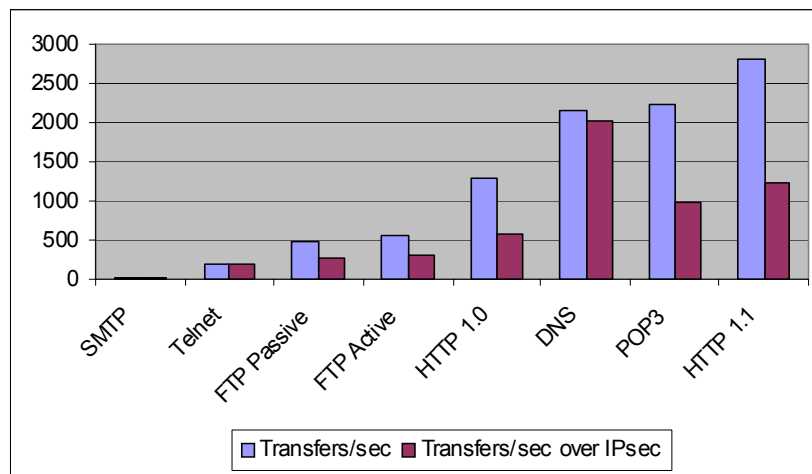


Figure 3: Impact of IPsec on Application Performance

As network security features are converging onto single platforms, testing IPsec performance and scalability becomes more complicated. IPsec VPN support can be found on many different devices:

- VPN and Firewall appliance
- VPN-only appliance
- Router with VPN support
- Router with VPN and Firewall
- VPN software on server
- Integrated security appliance

Testing IPsec performance in isolation is necessary for these devices, but should not be the only form of testing. Supporting IPsec is a computationally intensive task for a device, and validating the impact of this overhead on other device features, such as stateful packet inspection, is important.

Figure 4 illustrates a test scenario that is used to evaluate such a condition. The objective of the test is to measure the impact of a denial of service (DoS) attack on authorized customer traffic and IPsec VPN traffic. VPN/Firewall appliances are very common security devices used at the enterprise network perimeter, and this test depicts a typical scenario that this device has been designed to perform.

This test will answer these questions:

- Can the firewall perform multiple security functions simultaneously?
- How is IPsec VPN traffic affected during a DoS attack?
- Can customers still access an organization's public web server during a DoS attack?

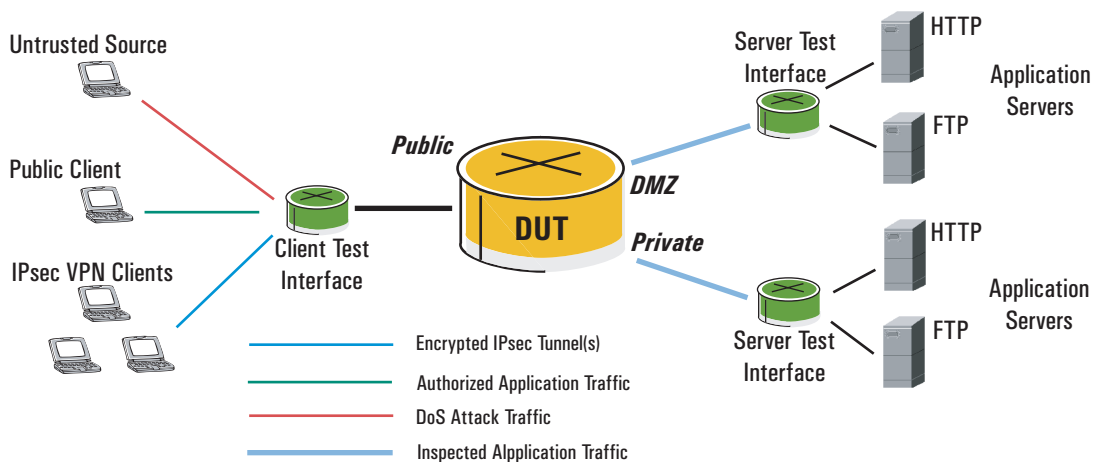


Figure 4: Testing Integrated Security Devices - IPsec VPN and Stateful Packet Inspection

Figure 5 displays typical results of this test. The results indicate degradation in IPsec VPN application performance in the presence of a DoS attack. The performance of some devices may degrade more, some less, and others may drop the tunnel altogether. Validating IPsec performance under realistic network conditions will allow the appropriate IPsec device to be chosen for a VPN deployment.

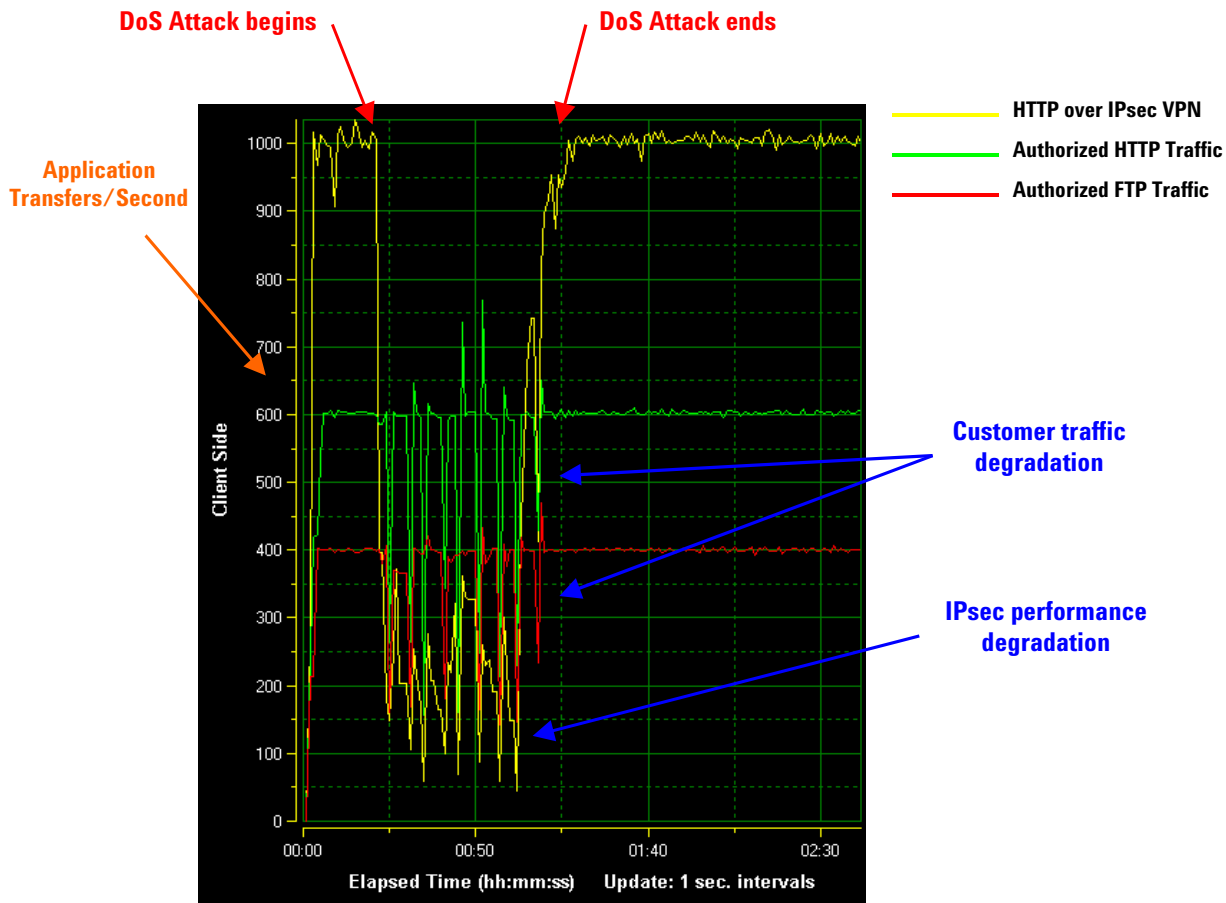


Figure 5: Impact of DoS Attack on IPsec Performance

IPsec Test Solution Requirements

A dedicated test solution with integrated IPsec capabilities is the only way to address these test challenges, execute the required test scenarios, and begin to find the performance limits of an IPsec-capable device. To summarize, an IPsec test solution must include the following capabilities:

- *IPsec Emulation* - As the basic requirement, a test solution must be able to emulate many IPsec clients and gateways. These entities will need to initiate and establish IPsec tunnels against a DUT.
- *Application Support* - Client and server emulation of a wide range of application protocols is necessary. The ability to mix application protocols over a single test interface or single IPsec tunnel, and the ability to send real, stateful application traffic over one or more IPsec tunnels are required.
- *High Performance & Scalability* - Testing the performance limits of an IPsec device can only be accomplished with a test solution capable of supporting up to thousands of IPsec tunnels and many Gigabits per second of stateful application traffic.
- *Flexibility* - The ability to create complex and large-scale IPsec test scenarios quickly and easily through a single integrated application is important. In addition, providing this same flexibility through an application programming interface (API) is necessary for automated test environments.
- *Functionality* - IPsec includes many protocols and processes that work together. Having the ability to configure the various parameters - such as encryption and hash algorithms - is crucial to be able to stress an IPsec implementation and validate the performance impact of different IPsec and IKE parameters.
- *Measurements* - An IPsec test solution would not be complete without comprehensive measurement and reporting capabilities. As a minimum this should include accurate measurement and display of IPsec tunnels, tunnel setup rates, tunnel setup times, and stateful application throughput.

Agilent NetworkTester

The Agilent NetworkTester is a powerful, versatile and integrated solution for accelerating the development and deployment of network security and content-switching devices and networks. NetworkTester's NetPressure software application meets all of the needs for testing IPsecv4 and IPsecv6 performance and scalability. The IPsec protocol suite is an integral part of the NetworkTester solution, providing a complete environment for all layer 4-7 test and measurement needs.

NetworkTester provides for quick and easy emulation of IPsec devices, which can be scaled to test many thousands of IPsec tunnels. Dedicated IPsec hardware acceleration allows the true traffic performance limits of an IPsec device to be found.

NetworkTester supports both client and server emulation of a broad range of application protocols, including HTTP, FTP, SMTP, POP3, RTSP and more. This enables realistic simulation of user and application profiles over IPsec VPN networks.

Integrated into the one, easy-to-use graphical user interface (GUI), NetworkTester also provides comprehensive measurement and graphing capabilities for accurate recording and reporting of all test results.

Conclusion

As VPN adoption continues to grow rapidly and IPsec remains the dominant VPN technology, testing the realistic traffic performance and scalability of IPsec network security devices is becoming ever more vital for the successful design and deployment of scalable VPN deployments.

IPsec VPN features are being integrated with other security services into multifunction security devices. Understanding how these features affect IPsec VPN performance will ensure that enterprise network designs will accommodate all users.

A comprehensive test solution that provides real application traffic integrated with large-scale IPsec VPN emulation is the fastest and most cost-effective solution to testing IPsec performance and scalability.

References

- [1] Kent, Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, 1998
- [2] Kent, Atkinson, "IP Authentication Header", RFC 2402, 1998
- [3] Madson, Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, 1998
- [4] Madson, Glenn, "The Use of HMAC-SHA-1 within ESP and AH", RFC 2404, 1998
- [5] Madson, Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, 1998
- [6] Kent, Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, 1998
- [7] Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, 1998
- [8] Maughan, Schertler, Schneider, Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, 1998
- [9] Harkins, Carrel, "The Internet Key Exchange (IKE)", RFC 2409, 1998
- [10] Glenn, Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, 1998
- [11] Thayer, Doraswamy, Glenn, "IP Security Document Roadmap", RFC 2411, 1998
- [12] Orman, "The OAKLEY Key Determination Protocol", RFC 2412, 1998
- [13] Doraswamy, Harkins, "IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks", 2nd Edition, Prentice Hall, 2003
- [14] Infonetics Research, "VPN and Firewall Appliances and Software, Market Share and Forecasts", Feb 2004

This page intentionally left blank.

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.
2660 Matheson Blvd. E
Mississauga, Ontario
L4W 5M2
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

