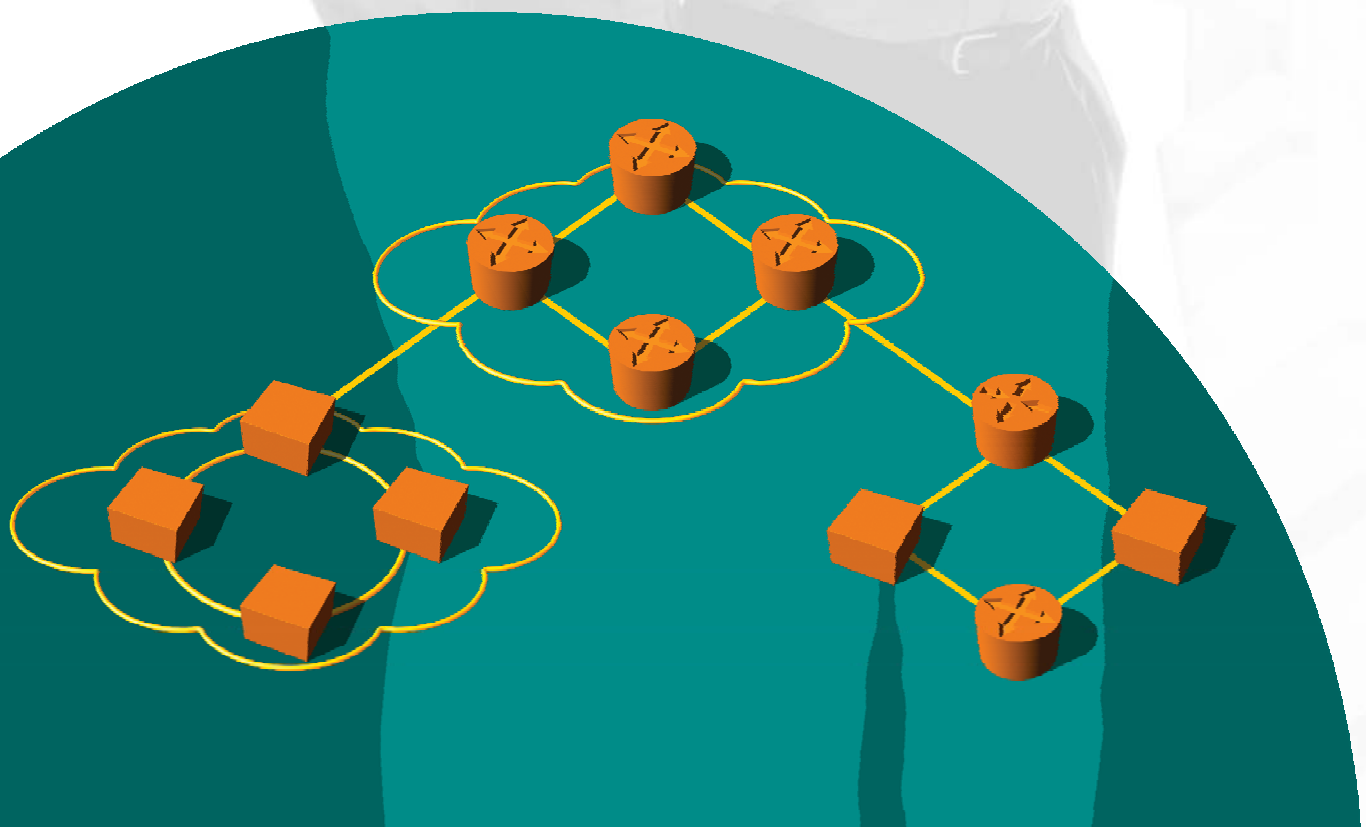


Spirent Communications Test Methodologies

IPSec Edition



Spirent Communications IPSec (IP Security) Edition

Welcome to this informative IPSec Edition of the Spirent Communications Test Methodologies series of journals.

Spirent Communications is a worldwide provider of integrated performance analysis and service assurance systems for next generation network technologies. Spirent is also the leader in comprehensive test methodologies. In this edition, you will find valuable IPSec test methodologies to use in the lab or with deployed networks.

Testing is the only way to understand the diverse conditions that networks and their components will accept and continue to operate efficiently. By testing early and often, your technical staff can monitor the pulse of equipment and determine why systems behave or fail under load.

If you want to review additional test methodologies, visit Spirent Communications Developers Network (SCDN) at <http://scdn.spirentcom.com>. After registering at SCDN, you will be able to download free scripts, share information about developing the scripts and obtain help from a technical community comprising industry members from all over the world.

You will find a list of IPSec test methodologies below. Best wishes with your testing efforts.

Spirent Communications

www.spirentcom.com

Table of Contents

IPSec Tests and Support Documents

IPSec Tunnel Capacity and Successful Sessions (TM-0145).....	1
IPSec Data Performance (TM-0146).....	3
IPSec Setup Rate (TM-0147).....	5
Adjusting IPSec Settings (TM-0148).....	7
Identifying IPSec Problems (TM-0149).....	9

Appendix

Acronyms.....	12
Glossary.....	13
IPSec Diagram — Initiator.....	15
IPSec Diagram — Responder.....	16
Spirent Communications Test Methodologies Information.....	17

IPSec Tunnel Capacity and Successful Sessions

RFC 2401: Security Architecture for the Internet Protocol

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 2409: The Internet Key Exchange (IKE)

Objective

This test measures the number of IPSec tunnels that the device under test (DUT) is capable of establishing (capacity). This test also validates that the tunnel is able to transfer data (Session) immediately after establishment and at end of test.

Overview

IPSec allows for the safe transfer of information through various authentication and encryption algorithms. Before information can be transferred, a "tunnel" is created between two security gateways (SGs) using a two-phase process. Phase 1 establishes communications between the SGs while the Phase 2 establishes the communication for the network behind the SGs. Only after the completion of Phase 2, when a tunnel has been established, can the "session" between the source and destination hosts be validated.

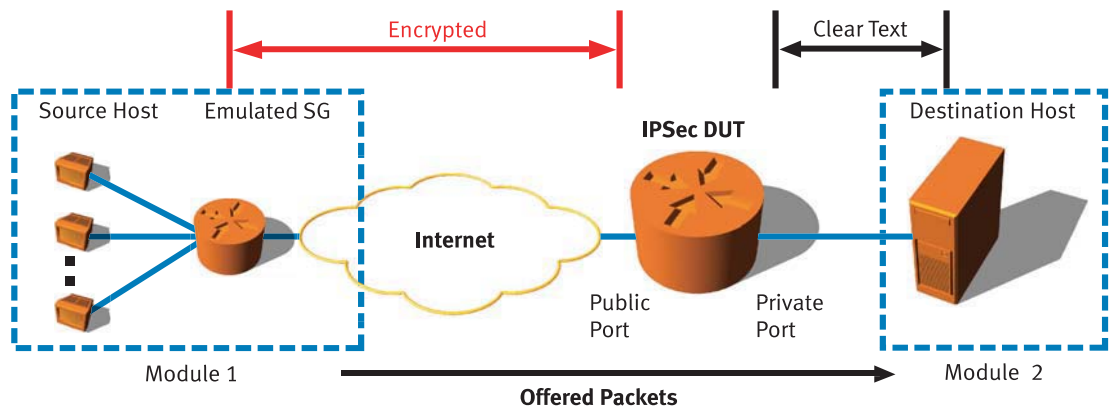
Because of IPSec's design, after two SGs have created a Phase 1, they do not establish additional Phase 1s for new traffic sources. Instead multiple Phase 2s are created for the various networks, all of which use the same Phase 1 information. This potentially hides problems associated with memory allocation and CPU utilization. Although memory is allocated for the Phase 2s, the impact on performance typically is not noticeable since Phase 2s are "quick" to create and not very CPU intensive. Depending on the DUT, no performance impact may be seen when there are hundreds of Phase 2s but be very noticeable with tens of Phase 1s. Also, the DUT may only transmit traffic over one tunnel, leaving the user unsure if there were multiple Phase 2s and if traffic was generated over them.

To determine tunnel capacity and the DUT's ability to validate the session with traffic, a minimum of two modules are required. One module will exchange encrypted information with the DUT while the other module will process unencrypted information in clear text. The module generating the traffic will contain the source host while the other module will contain the destination host. Assuming the DUT will be the IKE responder, the module with source host will also be the module with emulated SGs.

Traffic from the source host will be generated to the emulated SG. The emulated SG will then go through the Phase 1 and Phase 2 processes with the DUT (typically, the IP Address of the Public port). Once a tunnel has been established, the traffic from the source host will be decrypted by the DUT and forwarded from its Private port to the destination host. The destination host will then respond, sending information to the Private port of the DUT. The DUT will then encrypt the information, forward out its Public port for decryption by the emulated SG. Once decrypted, the emulated SG will forward to the source host and the source host will report that the session was successful.

Setup

IPSec Tunnel Capacity and Session Test



Since some DUTs can emulate multiple SGs, this test will assume the DUT's Public port is the SG address for encrypted traffic. The Private port is the interface forwarding unencrypted traffic. It is also assumed the DUT will be the IKE responder (not initiating the tunnel but only responding to tunnel requests).

Test Steps

1. Configure the DUT so the traffic offered from Module 1 can be forward to Module 2.
2. Match the desired number of SGs between Module 1 and DUT.
3. Match the Phase 1 test parameters between Module 1 and DUT:
 - a. Pre-shared Secret.
 - b. D-H Group.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
 - e. IKE mode.
4. Match the Phase 2 test parameters between Module 1 and DUT:
 - a. Transform.
 - b. Perfect Forward Secrecy.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
5. Set SA Lifetimes large enough to prevent rekeys (outside scope of test).
6. Set tunnel setup rate to a low number (<10/sec but DUT dependent).
7. The test stops when the # Sessions has reached user-defined # tunnels or tunnels fail.
8. If tunnels fail, decrease tunnel setup rate and/or decrease # tunnel retries.
9. If sessions fail, decrease tunnel setup rate and/or increase # session retries.

Test Parameters

Different test outcomes can be obtained by modifying any of the following input parameters:

- Tunnel setup rate.
- Number of tunnel retries.
- Number of session retries.
- IKE timers.

Test Outcome

Tunnel capacity, successful sessions and active tunnels at completion of test.

IPSec Data Performance

RFC 2401: Security Architecture for the Internet Protocol

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 2409: The Internet Key Exchange (IKE)

Objective

This test measures the amount of stateful traffic that can be forwarded by the device under test (DUT) over multiple IPSec Tunnels. Please refer to the "IPSec Tunnel Capacity and Successful Session" Test Methodology for additional information on IPSec.

Overview

IPSec allows safe transfer of information through various authentication and encryption algorithms. Before information can be transferred, a "tunnel" is created between two security gateways (SGs) using a two-phase process. Phase 1 establishes communication between the SGs while the Phase 2 establishes the communication for the network behind the SGs. Only after the completion of Phase 2, when a tunnel has been established, can the "session" between the source and destination hosts be validated.

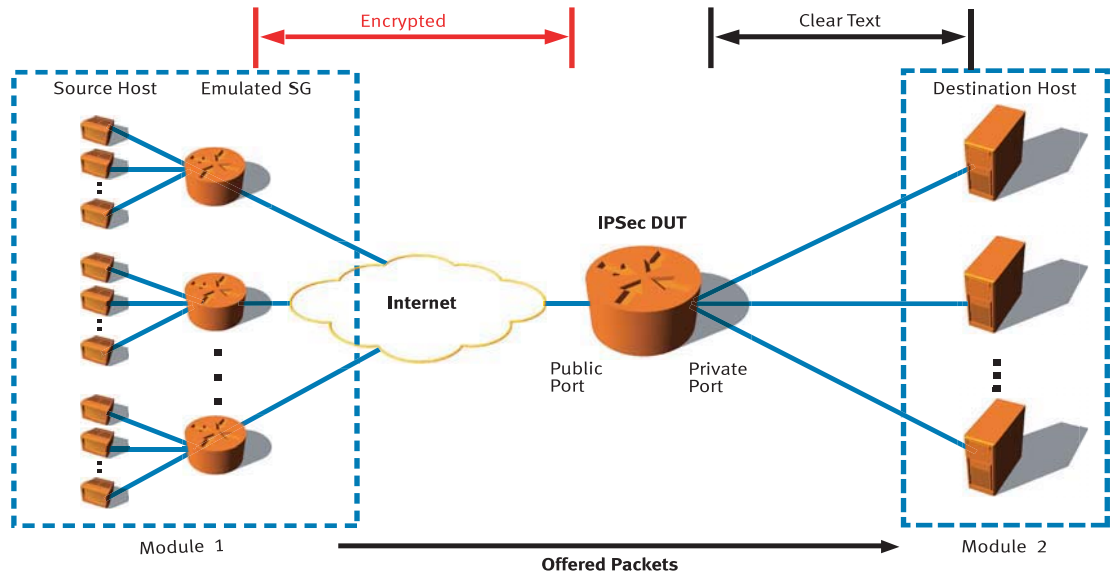
The testing of data performance is typically conducted with two DUTs hooked back to back and with UDP traffic sent across the tunnel. Two fundamental problems exist with this approach: First, because of the way IPSec works, only a single Phase 1 will be created between the devices. Second, IPSec devices also are firewalls that require stateful traffic and UDP is non-stateful. Although this method of testing provides useful information compared with traditional performance tests designed around UDP, it does not test the way the stateful technologies must be tested.

To evaluate IPSec's impact on data performance, multiple tunnels are required with each tunnel generating traffic simultaneously. This is important since each packet has to be matched with the appropriate database entry (i.e., tunnel) before being processed. This lookup time causes delay that impacts performance. Although the traditional tests with UDP can be used, most traffic is TCP based. With TCP, discarded packets are resent with the normal TCP ACKs that creates additional load on the DUT. For this reason, TCP based traffic is necessary with measurements taken from an application perspective (i.e., payload).

The type of stateful TCP traffic determines the type of measurements to be collected. If the desire is to measure the ability to measure data forwarding (Mbps) of specific size payloads, TCP tests should be selected. If the desire is to measure the response time (ms) to retrieve an object, HTTP should be selected. Both measurements have their use in defining the DUT's characteristics.

NOTE: TCP performance results should not be directly compared to UDP results since the measurements are taken from different reference points. TCP has retransmissions and ACKs and does not include the TCP nor IP overhead.

Setup IPSec Data Performance Test



Since some DUTs can emulate multiple SGs, this test will assume the DUT's Public port is the SG address for encrypted traffic and the Private port is the interface forwarding unencrypted traffic. It is also assumed the DUT will be the IKE responder (not initiating the tunnel but only responding to tunnel requests).

Test Steps

1. Configure the DUT so the traffic offered from Module 1 can be forward to Module 2.
2. Match the desired number of SGs between Module 1 and DUT.
3. Match the Phase 1 test parameters between Module 1 and DUT:
 - a. Pre-shared secret.
 - b. D-H Group.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
 - e. IKE mode.
4. Match the Phase 2 test parameters between Module 1 and DUT:
 - a. Transform.
 - b. Perfect Forward Secrecy.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
5. Set SA Lifetimes large enough to prevent rekeys (outside scope of test).
6. Set tunnel setup rate to a low number (<10 /sec but DUT dependent).
7. Determine is running TCP or HTTP test.
8. Define number of packets and packet size (TCP) or object size (HTTP).
9. The test stops when the data has been received.

Test Parameters

Different test outcomes can be obtained by modifying any of the following input parameters:

- Number of tunnels.
- Encryption algorithm.
- Perfect Forward Secrecy.

Test Outcome

TCP data forwarding rate (Mbps) and HTTP response time (ms).

IPSec Setup Rate

RFC 2401: Security Architecture for the Internet Protocol

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 2409: The Internet Key Exchange (IKE)

Objective

This test measures the rate at which the device under test (DUT) is capable of establishing IPSec Tunnels. Please refer to the "IPSec Tunnel Capacity and Successful Session" test methodology for additional information on IPSec.

Overview

IPSec allows for safe transfer of information through various authentication and encryption algorithms. Before information can be transferred, a "tunnel" is created between two security gateways (SGs) using a two-phase process. Phase 1 establishes communication between SGs while the Phase 2 establishes the communication for the network behind the SGs. Only after the completion of Phase 2, when a tunnel has been established, can the "session" between the source and destination hosts be validated.

Testing the IPSec setup rate of a DUT depends primarily on two factors: Number of Phase 2s (aka tunnels) per Phase 1 and total number of tunnels. The general rule of thumb is if you increase either, performance decreases. The performance impact will depend on the CPU, memory and IPSec implementation of the DUT.

Phase 1 and Phase 2

Phase 1s have two modes - Main and Aggressive. Main mode is commonly used since it is more secure and has additional handshakes not required by Aggressive mode. Phase 2s have one mode - Quick. As the name implies, this mode is very fast to establish since it reuses key information from the Phase 1.

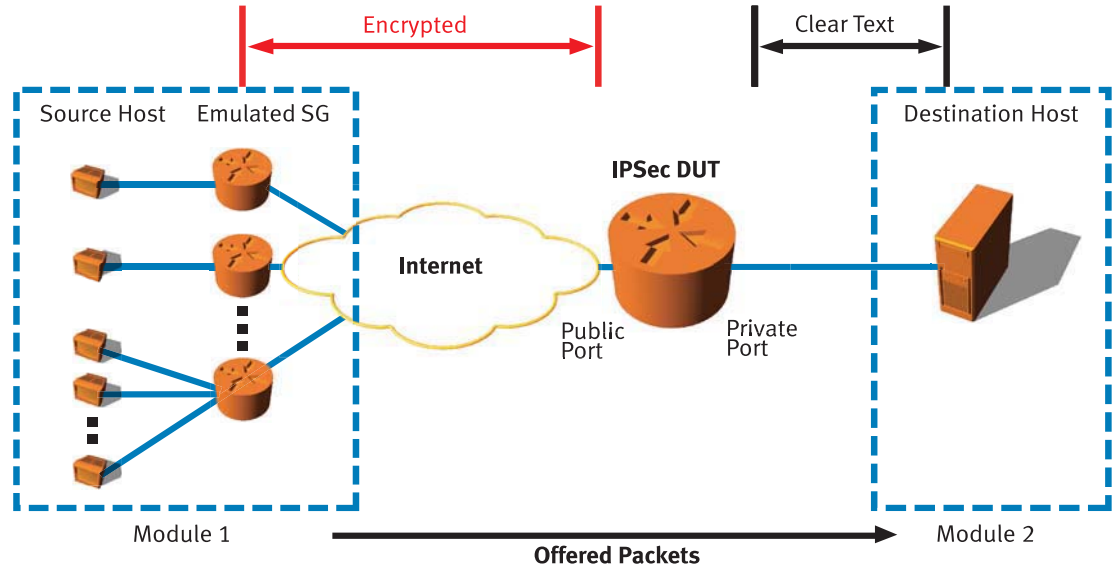
When testing setup rates, it is important to test under realistic scenarios. Most IT departments create a single Phase 2 per Phase 1 for each site, tunneling all traffic over it since it is easier to maintain. However, some locations may require higher levels of encryption per department (accounting, marketing, sales) and multiple Phase 2s may be necessary. Whether using multi-Phase 2s per Phase 1 or one Phase 2 per Phase 1, make sure to compare devices equally since a "tunnel" is always considered a Phase 2.

Total Number of Tunnels

Normally as the number of tunnels to be tested increases, the lower the setup rates will be. This is the result of memory being allocated and the time to look through the database to find the corresponding tunnel. In addition, as tunnels are established there will be thresholds where the setup rate decreases as the DUT processes new tunnel requests. These thresholds will require a retest of the DUT at a lower rate to find the next threshold.

Setup

IPSec Setup Rate Test



Since some DUTs can emulate multiple SGs, this test will assume the DUT's Public port is the SG address for encrypted traffic. The Private port is the interface forwarding unencrypted traffic. It is also assumed the DUT will be the IKE responder (not initiating the tunnel but only responding to tunnel requests).

Test Steps

1. Configure the DUT so the traffic offered from Module 1 can be forward to Module 2.
2. Match the desired number of SGs between Module 1 and DUT.
3. Match the Phase 1 test parameters between Module 1 and DUT:
 - a. Pre-shared Secret.
 - b. D-H Group.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
 - e. IKE mode.
4. Match the Phase 2 test parameters between Module 1 and DUT:
 - a. Transform.
 - b. Perfect Forward Secrecy.
 - c. Authentication algorithm.
 - d. Encryption algorithm.
5. Set SA Lifetimes large enough to prevent rekeys (outside scope of test).
6. Set tunnel setup rate to a low number (<10/sec but DUT dependent).
7. The test stops when the number of sessions has reached user-defined number of tunnels or tunnels fail.
8. Rerun test with higher setup rate.
9. Continue process until setup thresholds have been identified.

Test Parameters

Different test outcomes can be obtained by modifying any of the following input parameters:

- Tunnel setup rate.
- Number of tunnels.
- Number of Phase2s per Phase 1.

Test Outcome

Min, Max and Ave Tunnel establishment time by Phase 1, Phase 2 and complete tunnel negotiation.

Adjusting IPSec Settings

TEST METHODOLOGY REFERENCES

IPSec Tunnel Capacity and Successful Session (TM-0145)

IPSec Data Performance (TM-0146)

IPSec Setup Rate (TM-0147)

Objective

This document discusses key elements of testing IPSec and their impact on the device under test (DUT). For additional information on IPSec, please refer to the references listed above that cover the actual test methodologies.

Overview

Because IPSec is designed for security, understanding how it works can be difficult since most messaging that takes place is encrypted. IPSec is a stateful protocol consisting of two main components called Phase 1 and Phase 2. Phase 1 establishes communication between the security gateways (SGs) while Phase 2 establishes the communication for the networks behind the SGs. Once the Phase 2 is completed (i.e., when a "tunnel" has been established), the actual "session" between the source and destination hosts is validated.

Key Items Affecting Test Results

Hardware Accelerators

Description — Today, most DUTs can achieve rates of 10/100+ Mbps. Even software-based encryption solutions are able to achieve high encryption rates with fast processors. But to achieve these higher encryption rates, in addition to higher setup rates, DUTs are equipped with specialized hardware accelerators. Only with these hardware accelerators will the true upper limits be tested.

Impact — Testing with software encryption may not reach the upper limits of the DUT.

Recommendation — Use hardware accelerators for testing devices beyond 10 Mbps and for setup rates of 100+ tunnels per second.

Number of Tunnels and Setup Rate

Description — The number of tunnels a DUT can support is based on available memory. As tunnels are configured, entries are added to a database consuming memory. This database is referenced for every tunnel request, and the speed of the look-ups will depend on the database size. As the database grows, the rate in which look-ups can occur diminishes.

Impact — The more tunnels configured, the lower the setup rate. In addition, as tunnels are established, the setup will further decrease due to the additional time to cross-reference each packet against existing tunnels.

Recommendation — When performing large-scale tunnel capacity tests, start with low setup rates. Once successful, increase the setup rate slowly until the threshold of the DUT is determined. In most cases, it is best to start with one tunnel per second, then two tunnels per second, then three tunnels per second, etc.

SA Lifetimes

Description — Because encryption algorithms can be broken over time, IPSec is designed where both Phase 1s and Phase 2s create new keys (aka SA Lifetime). SA Lifetime is performed after X kilobytes of data has been exchanged or after Y amount of time. Typically, VPNs are implemented to perform rekeys over Y amount of time to prevent network slowdown during peak business hours. Many implementations use settings 24 hours for Phase 1s and eight hours for Phase 2s.

Impact — Rekeys require CPU cycles similar to those during the creation of a tunnel. If the DUT has to perform a rekey in the middle of a test, identifying which device was the limiting factor will be hard to determine.

Recommendation — Set SA Lifetimes to large values where rekeys do not occur during a test. If a rekey does occur, the results should be carefully analyzed since they potentially could be misleading. Since duration tests are typically for validating that tunnels are still up, and since there were no memory leaks, rekeys are acceptable.

Phase Parameters

Description — One group of items that will have the greatest impact on setup rate and overall tunnel capacity are the Phase parameters of retry attempts, retry timer, max retry timer and expirer timer. Assuming the configuration is correct, these parameters determine whether a tunnel is successful or not.

- **Retry attempts** — the number of times the IPSec protocol stack will attempt to create the tunnel.
- **Retry timer** — the length of time to wait between retries.
- **Max retry timer** — the maximum length of time to wait between retries.
- **Expirer timer** — the maximum amount of time from the initial tunnel request before failing the tunnel.

Impact — Once a DUT starts experiencing problems with establishing tunnels, the retries can potentially cause all new tunnels to fail until it can process the requests in its cache. However, depending on the Expirer timer, the DUT may be able to eventually catch up with requests.

Recommendation — If it is a small tunnel test, let the DUT try to establish the tunnels. If it experiences problems, adjust the Phase parameters until all the tunnels are successful. It is best to let the tunnels timeout (Expirer timer reached) or not to attempt retries to see what the upper limit of the DUT can do.

Session Retries

Description — Tunnels are created for the purpose of transferring traffic (aka session). When measuring tunnel capacity, only those tunnels able to transfer traffic across both directions are considered successful. Even if both Phase 1 and Phase 2 are created, if traffic cannot be sent between the source host and the destination host across the tunnel, the session is considered a failure. This is important to understand since certain DUTs make tunnel creation a priority when sending traffic over existing tunnels.

Impact — Sending a single packet across a tunnel will show if the DUT is able to create tunnels while being able to forward over existing tunnels.

Recommendation — If sessions are failing, reduce the tunnel setup rate and increase the session retry attempts. The combination of these actions should allow the DUT to successfully forward traffic while creating tunnels.

PFS

Description — PFS (Perfect Forward Secrecy) takes place when the Phase 2 obtains new keying information using D-H (Diffie-Hellman). Since D-H requires additional processing, enabling it may decrease the rate in which Phase 2s can be established.

Impact — Increasing the D-H level used (e.g., 1, 2 or 5) will decrease the setup rate and possibly the number of successful tunnels and sessions.

Recommendation — It is best to test with D-H turned on for harder testing. If PFS will not be implemented, then it should be disabled.

Identifying IPSec Problems

TEST METHODOLOGY REFERENCES

IPSec Tunnel Capacity and Successful Session (TM-0145)

IPSec Data Performance (TM-0146)

IPSec Setup Rate (TM-0147)

Objective

This document discusses common items to investigate when troubleshooting IPSec problems with the device under test (DUT). For additional information on IPSec, please refer to the test methodologies listed above that cover the actual test methodologies.

Overview

Setting up two similar DUTs for IPSec is complicated. Setting up two different vendor DUTs to interoperate using IPSec is even harder. For this reason, most IPSec testing today is done with two similar devices with a single tunnel. However, this approach is unrealistic and could lead to incorrect purchasing and deployment decisions. To set up tests, the most common items are discussed. Follow their order when checking for problems.

Check These Problems in the Following Order

Reachability

Make sure that all devices are able to communicate to each other. Check for proper cabling and ensure that any VLANs forward traffic to the right port. Since a lot of Denial of Service attacks are ICMP based, certain DUTs will not respond to pings. Verify that the port IP Address is on the right network.

Default Routes

Because of all the IP addresses used in IPSec, it is common to forget to set default routes. As a rule, verify the DUT has at least three default routes set covering traffic to the security gateway (SG), source host and destination host. If the DUT is designed as a VPN/Firewall device, the SG and the source host are assigned to the Public port while the destination host is assigned to the destination port.

Default Gateways

Not to be confused with SGs, default gateways are the next hop if the device on that subnet can't resolve the IP address. Make sure the default gateway is set to the next physical interface. Some devices can simulate multiple SGs, resulting in a unique SG IP address than the port IP address. Phase 1 and Phase 2 Parameters

Double-check and then triple-check that the Phase 1 and Phase 2 parameters match. Most problems result from wrong configurations, but they are hard to spot since everything is encrypted. The best way to see problems associated with Phase 1 or Phase 2 mismatch is to troubleshoot the tunnel with a bounce diagram so the phase with the problem is easily displayed. A more complicated method is sorting through an IPSec stack trace.

ARPs

Ensure that ARPs are being resolved. If tests end quickly with no results, then chances are high that the IP addresses are set on wrong networks and/or the default route is incorrect. It is best to create a single tunnel using a diagram with all the IP addresses labeled. With the diagram, it should become apparent if there are any IP issues related to ARPs. If still unsure, put the all ports on the same network and start moving off one port at a time to see where the problem is.

Access Lists/Rules

If all the IP addresses and IPSec settings are correct but no tunnel is established or traffic sent across the tunnel, check to see if there is an access list or rule prohibiting the traffic. Each DUT is different. Although one didn't use restrictions like access list or rules as part of IPSec, other DUTs might.

Rerun Tests

Some DUTs load IPSec from flash while others have it always loaded. Depending on the device, a second test may result in better performance and also provide insight into how it works.

Anomalies

Probably the hardest to troubleshoot since the problem is at the IPSec protocol level. When they occur, it is important to collect as much information as possible (see "Additional Help" section below). However, sometimes the culprit is found in the test setup. For example, if tunnels are not torn down between tests some DUTs may establish new tunnels and then use the old tunnels since they are first in their database. This behavior will show that there was twice the number of tunnels compared with the test setup.

Helpful Tools

The following tools are useful when troubleshooting:

- IPSec stack logs — Shows exactly what is happening for an IPSec protocol level.
- Bounce diagrams — Visual diagrams for reducing troubleshooting time.
- Ping — Useful to ensure packets actually reach intended targets.
- Trace route — Useful to find misconfigurations of routes or VLANs.
- Protocol analyzer — For showing which packets are transferred.

Additional Help

Problems sometimes exist with IPSec interoperability. It is important that the test tool use a well known IPSec vendor that has a proven track record of interoperability. If additional help is required to troubleshoot the problem, always send the following items:

- Results file — Results file from the test tool shows what the user is seeing and can help in explaining the cause of the problem.
- Setup files — Setup files from both the DUT and test tool are required. If the DUT is Web-based, send screen shots of pertinent screens.
- IPSec log files — IPSec log files from both the DUT and test tool are required. Without log files, there can be delays in determining if there is a problem with IPSec interoperability or with the configurations.
- Network diagram — A network diagram with all IP address clearly visible is very helpful. Sometimes the problem is with the test network.

Appendix

Acronyms

3DES — Triple Data Encryption Standard
ACK — Acknowledgement
AES — Advanced Encryption Standard
ARP — Address Resolution Protocol
DES — Data Encryption Standard
D-H — Diffie-Hellman
DUT — Device Under Test
ESP — Encapsulating Security Payload
HTTP — Hyper Text Transfer Protocol
IKE — Internet Key Exchange
IP — Internet Protocol
IPSec — IP Security
MD5 — Message Digest 5
PFS — Perfect Forward Secrecy
SA — Security Association
SG — Security Gateway
SHA-1 — Secure Hash Algorithm Version 1
SPI — Security Policy Index
TCP — Transmission Control Protocol
UDP — User Datagram Protocol

Glossary

AES – The Advanced Encryption Standard that is currently being developed as a replacement for DES by the U.S. NIST organization. There are a number of algorithms being considered, and they are all 128-bit block ciphers that support 128, 192, and 256 bit keys.

DES/3DES – Data Encryption Standard, defined by the U.S. government. It was created in the 1970s by IBM assisted by the agency that is now called NSA. Based on Horst Feistel's ideas, the team of scientists at IBM devised a cipher that has influenced the science of cryptology. The controversy around DES key length and design issues has developed many variants of the original algorithm. DES is a symmetric 64-bit block cipher that uses a 56-bit key. The size key is usually not considered long enough to protect (encrypt) valuable data. The 3DES (or triple-DES) is the most accepted and is a variant of DES. 3DES is a combined set of two DES keys totaling 112 bits. Due to its larger size, 3DES is considered much more secure than DES.

Diffie-Hellman (D-H) Key Exchange – A method for key exchange between two parties. This method can be used to generate an unbiased secret key over an insecure medium. The method has many variants.

Initiator – The side of the VPN (can be either Public or Private) that initiates the tunnel setup process.

IKE – The key exchange algorithm used with IPSec. This is a new name for the ISAKMP/Oakley key exchange. In particular, this refers to the resolution draft that specifies which parts of each specification must be implemented for IPSec use. The IKE protocol is defined in RFC 2409, RFC 2408 and RFC 2407.

IPSec – A protocol suite for protecting IP traffic at packet level as defined by the Internet Engineering Task Force (IETF). It can be used for protecting the data transmitted by any service or application based on IP. There are two phases to the creation of a tunnel. Phase 1 refers to the negotiation between security gateway identities. Phase 2 refers to the networks behind the security gateways. IPSec protocols are defined in RFC 2401.

PFS – Perfect Forward Secrecy. Refers to the notion that any single key being compromised will permit access to only data protected by that single key. In order for PFS to exist, the key used to protect transmission of data must not be used to derive any additional keys. If the key used to protect transmission of data was derived from some other keying material, that material must not be used to derive any more keys.

Phase 1 – The first step in the creation of a tunnel. Information is exchanged between security gateways, allowing for more secure communication of the Phase 2.

Phase 2 – Considered as a "tunnel" where information can be transferred. Phase 2s are vital for the communication of devices behind the private/secure side of the security gateways.

Pre-shared Secret – Pre-shared secret is an authentication method in IKE. In this method, two peers have configured a shared password used to authenticate the endpoints by means of encryption (A can decipher packet B has encrypted, therefore A knows B knows the same secret it knows and vice versa). This authentication method scales badly and is usable for very limited number of hosts.

Rekey – The re-establishment of the information used for encrypting data. Rekeys occur based on the SA Lifetime.

Responder – The side of the VPN (Public or Private) that responds to the other side that initiated the tunnel setup process.

SA – Security Association. A unidirectional connection created for security purposes. All traffic traversing an SA is provided the same security processing. In the IPSec context, an SA is an Internet layer abstraction implemented through the use of an AH or ESP. The SA contains data controlling how a transformation is applied to an IP packet. The data is determined using specially defined SA management mechanisms. The data may be a result of an automated SA and key negotiation, or it may be defined manually.

SA Lifetime – The amount of time an SA will exist before trying to rekey. SA Lifetimes can be set by Phase 1 or by Phase 2. The lifetime value can be set either by time or by amount of traffic.

Session – A session is when information can successfully transverse a tunnel. Tunnels can be successful, but sessions can still fail if the proper rules or routing are not enabled.

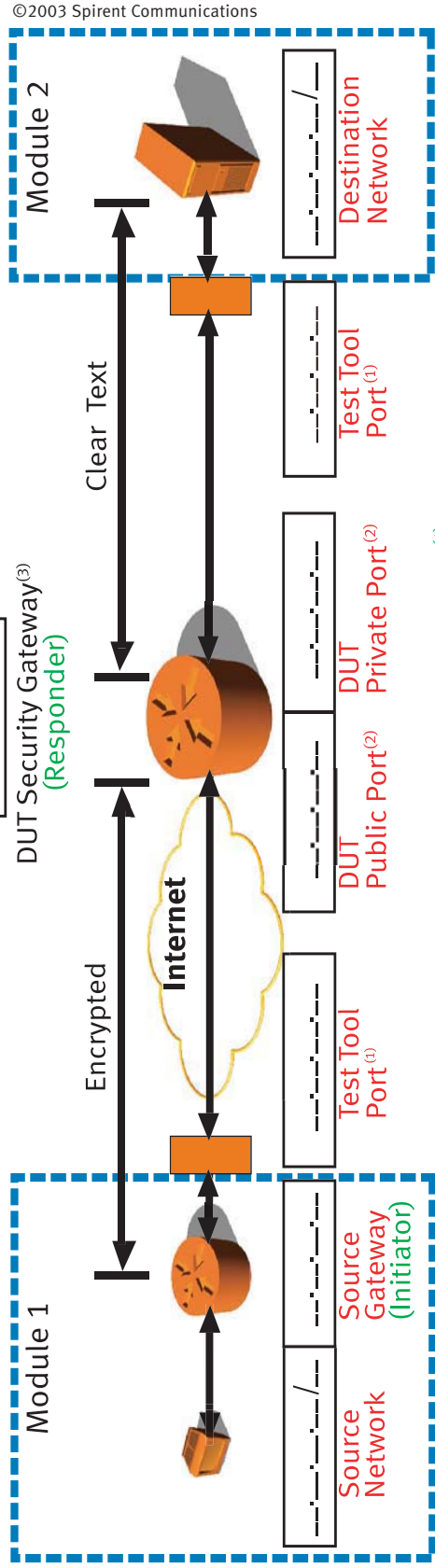
Security Gateway – A security gateway is a device or system that resides between an external untrusted network (such as the Internet) and trusted hosts on a LAN. The security gateway provides security services for the trusted hosts when they communicate with hosts on the untrusted network.

SPI – Security Policy Index. An arbitrary value used in combination with a destination address and a security protocol to uniquely identify an SA. The SPI is carried in AH and ESP protocols to enable the receiving system to select the SA under which a received IP packet will be processed. An SPI has only local significance as it is defined by the creator of the SA, which is usually the receiver of the IP packet carrying the SPI. Thus, an SPI is generally viewed as an opaque bit string. However, the creator of an SA may choose to interpret the bits in an SPI to facilitate local processing. This term is defined in RFC 2401.

Transformation – A particular type of change applied to an IP packet. For example, ESP encryption, AH integrity service and payload compression are transformation types. An SA supplies the keys and other association-specific data to a transformation. IPSec transformations are defined in RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2406 and RFC 2405.

Tunnel – A tunnel is the completion of a Phase 2. Once a tunnel is established, the session can occur. Multiple tunnels per Phase 1 can exist.

Initiator Setup Guide



©2003 Spirent Communications

Pre-shared Key

DUT Security Gateway(3)
 (Responder)

Encrypted

Clear Text

Internet

DUT Public Port(2)

DUT Private Port(2)

Test Tool Port(1)

Destination Network

Module 1

Module 2

Source Network

Source Gateway (Initiator)

Test Tool Port(1)

DUT Public Port(2)

DUT Private Port(2)

Test Tool Port(1)

Destination Network

Phase 2 Policy

PFS (Yes/No)
 AH/ESP
 MD-5/SHA-1
 DES/3DES/AES/None

Phase 1 Policy

Main/Aggressive
 MD-5/SHA-1
 DES/3DES/AES
 D-H Group (1/2/5)



Initial Packet(4)

DUT Model

DUT Firmware

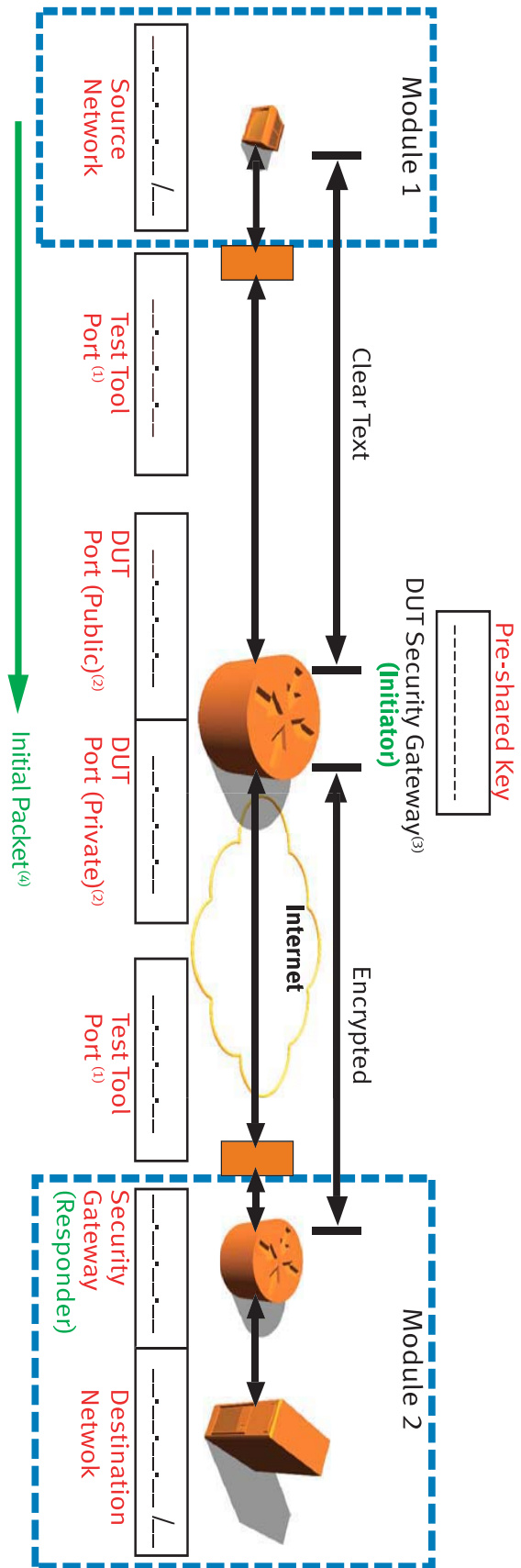
Test Tool Version

Test Name

Username / Date

- Notes:**
- (1) "Default Gateway" typically will be the "DUT Port"
 - (2) "Default Gateway" typically will be the "Test Tool Port"
 - (3) Verify Default Routes are present for the IP Addresses of the "Source Host", "Security Gateway" and "Destination Host"
 - (4) Initial packet to create a Tunnel is always sent from the Source Host to the Destination Host regardless if the DUT is the Initiator or Responder

Responder Setup Guide



©2003 Spirent Communications

Phase 2 Policy
 PFS (Yes/No)
 AH/ESP
 MD-5/SHA-1
 DES/3DES/AES/None

Phase 1 Policy
 Main/Aggressive
 MD-5/SHA-1
 DES/3DES/AES
 D-H Group (1/2/5)

Test Name

Username / Date

DUT Model

DUT Firmware

Test Tool Version

- Notes:**
- (1) "Default Gateway" typically will be the "DUT Port"
 - (2) "Default Gateway" typically will be the "Test Tool Port"
 - (3) Verify Default Routes are present for the IP Addresses of the "Source Host", "Security Gateway" and "Destination Host"
 - (4) Initial packet to create a Tunnel is always sent from the Source Host to the Destination Host regardless if the DUT is the Initiator or Responder

Spirent Communications

Test Methodologies Journals

The Spirent Communications Test Methodologies series of journals has been developed to make network and equipment testing easier. Spirent provides a Web site for scripts and other resources at <http://scdn.spirentcom.com/welcome.asp>. Registration is required to access the scripts and other tools to help you expedite testing.

Spirent offers journals with test methodology documents and support data for the following topics:

- Router Performance Edition — Router Performance Testing
- Volume II — IPv6, Wireless, Edge Router, Metro Optical, VoIP, SS7, QoS
- Layer 4-7 Edition — Network and Application Testing
- IPv6 Edition — IPv6 and IPv4 Test Methodologies
- Optical Edition — Near End Performance Testing
- Edge Router Edition — Edge Router Testing
- MPLS Edition — MPLS Network Testing
- IPSec Edition — IP Security Testing



Analyze | Assure | Accelerate™

Spirent Communications is a worldwide provider of integrated performance analysis and service assurance systems for next-generation network technologies. Our solutions accelerate the profitable development and deployment of network equipment and services by emulating real-world conditions in the lab and assuring end-to-end performance of large-scale networks.

Spirent performance analysis solutions include instruments and systems that measure and analyze the performance of network equipment, particularly the devices that route voice and data messages to their destination. Our service assurance solutions include remote test, fault and performance management systems that let network service providers quickly identify network faults and monitor real-time performance.

Spirent's integrated performance analysis and service assurance solutions enable our customers to more rapidly develop and certify new devices, lowering the cost of widespread deployment and operation of new network services.

Spirent Communications is a wholly owned subsidiary of Spirent plc, an international network technology company.

Spirent Communications

15200 Omega Drive
Rockville, MD USA
20850-3240
Tel: +1 301.417.1224
info@spirentcom.com

Sales and Information

Americas
Tel: +1 800.927.2660
productinfo@spirentcom.com

Europe, Middle East, Africa
Tel: +33 1 6137.2250
salesemea@spirentcom.com

Asia Pacific
Tel: +852.2166.8382
spirentasia@spirentcom.com

Spirent Communications Developers Network
<http://scdn.spirentcom.com>

www.spirentcom.com