GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Understanding and Configuring IPSec between Cisco Routers

Name: Ryan Ettl
Date Submitted: November 12, 2003
Certification: GSEC
Version: 1.4b
Option: 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract....3
Introduction....3
Virtual Private Networking (VPN):....3
VPN Disclaimer....5
Fundamentals behind Security Gateway-to-Security Gateway VPN....6
Terms and Definitions:....7
IPSec Tunneling:....8
Establishing an Inter-company VPN connections (Extranet):....10
Crypto Policy:....11
Transform Set:....12
AH and ESP: (tunnel mode only)....13
Crypto Access List:....15
Crypto Maps:....17
Applying an IPSec tunnel:....17
Recap:....18
Additional Security Parameters to be implemented with IPSec:....18
Extend IP access list:....18
Network Address Translator (NAT)....19
IP accounting:....20
Final Configuration:....21
Conclusion:....21
References....22

© SANS Institute 2004, Author retains full rights.

Abstract:

In today's corporate business network infrastructure there are many needs to securely transfer data across the internet. This can be a company's top secret information regarding product designs, product release dates, patent information, HR employee investigations, ect. In many cases, these examples require a secure means of data transfer to third party companies specializing in a field of engineering or legal subject matter. This paper will provide insight for a secure solution to address this business need using Virtual Private Networking.

All widely used Virtual Private Networks can be classified under three basic categories:

1. Host-to-Security Gateway (a.k.a. Client-to-Server)
2. Host-to-Host (a.k.a. Client-to-Client)
3. Security Gateway-to-Security Gateway (a.k.a. Router-to-Router or Site-to-Site VPN)[1]

Focus will be centered on category three. After reading this paper the reader should understand the fundamentals behind Security Gateway-to-Security Gateway VPN connections, be able to configure a VPN connection across the Internet using IPSec compliant devices as terminating end points, and configure additional security parameters. This paper will exclude any client VPN hardware or software related topics to limit the scope.

Introduction:

Virtual Private Networking (VPN):

> About 65% of the top 3,000 organizations worldwide have implemented VPNs, according to Hurley. A VPN encrypts data transmitted over the public Internet, enabling remote users such as distributors, suppliers, partners, and teleworking employees to securely access a company's network. Combined with firewalls, intrusion detection, proper authentication, and other security tools, VPNs provide robust, scalable, low-cost security.[2]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

---

[1] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 464

[2] James A. Martin. "Securing Business Networks". iQ Magazine, September/October 2003 http://business.cisco.com/prod/tree.taf%3Fasset_id=103850&ID=92781&ListID=44753&public_view=true&kbns=1.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The above quote addresses all 3 classifications of VPN connections, but illustrates the growing presence of all VPN technology in the business community.

Corporate migration to VPN connections across the Internet is beginning to become very attractive because of the tremendous cost savings. Instead of incurring the cost for a point-to-point dedicated lease line, which can span thousands of miles depending on geographic location, corporations can use VPN technology to deliver data over the Internet. This allows a company to purchase a leased line from the local Internet Service provider's (ISP's) first Point of Presence (POP) which spans a minimal geographical distance. A price quote from an undisclosed telecom provider in the UK during spring of 2003 for Intel Corporation illustrates the considerable cost savings. (Note: For confidentiality reasons the below geographic information has been altered, but relative distance and dollar amounts are portrayed accurately.)

Poland

Before: 512k leased line to Denmark has a monthly cost of $19,000 or $228,000 per year.

After: 1024k VPN Connection to England, local tail provided by UK telecom provider in Poland, has a monthly run rate of $5,185 or $62,220 per year.

Total Saving: $165,780 per year[3]

With VPN twice the bandwidth is gained for nearly four times less the cost of the leased line. To back up VPN cost savings claim, below is a publicly available price comparison of converting to a VPN solution from ISDN and frame-relay leased lines.

Typical monthly costs for traditional private WAN connections versus Internet access

	Private WAN Connections			Internet Access (VPN)
	ISDN	ISDN	Frame Relay	
Bandwidth	9 hours/day 5 days/week	24 hours/day 7 days/week	24 hours/day 7 days/week	24 hours/day 7 days/week
64Kbps	$1,884	$6,571	$1,276.50	$673-$888 per link
128Kbps	$3,504	$14,054	$3,168.75	

Explanation of Charges

- ***ISDN*** has a low monthly rate, but charges 1 to 2 cents per minute plus additional long distance rates. For example: GTE in Hillsboro, Oregon, charges $94 for installation and $48 per month for business, plus 1 to 2 cents per minute depending on distance and

[3] Stephen Jones. "Lease Line to VPN" Intel Global Engineering. GER – Senior Network Engineer, October 29th, 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

time of day for a local call. Long distance calls for business-to-business connections cost the same as telephone long distance x 2 for 2 B channels (128Kbps).

So charges for 9 hours/day, 5 days/week are: $48 + (9 hours x 60 = 540 minutes x 20 days = 10800 x $.02 = $216) = $264/month. Add long distance at 15 cents/minute = $1,620 + $264 = $1,884/month to connect two offices at 64Kbps. $3,504 for 128Kbps.

Charges for 24 hours/day, 7 days/week are: $48 + (24 hours x 60 = 1440 minutes x 30 days = 43,200 minutes x $0.02 = $864) = $912/month. Add long distance at 15 cents/minute = $6,480 + $912 = $6,571/month to connect two offices at 64Kbps. $14,054 for 128Kbps.

- ***Internet Access*** charges are also based on charges quoted in Hillsboro, Oregon. They include $123/month for a full time Frame Relay connection plus an Internet access fee of $550/month from an independent ISP or $765/month from GTE, the local Telco.

Prices shown are as of 7/97, valid only in the United States, and quoted in U.S. dollars. Although we make every effort to ensure that this information is accurate, Intel assumes no responsibility for errors of fact or omissions herein. This information is subject to change without notice.

[4]

As shown above, the motivating factor to move from leased lines to VPN solutions is clearly cost saving. However, the question remains, how does a private company transfer data across the internet securely? This introduces the concept commonly referred as passing trusted data over untrusted networks. Traditionally, leased lines were considered secure because a company purchased end-to-end physical connectivity. With a leased line only the purchasing company's network traffic should traverse the leased line. Additionally, this assumes the vendor is keeping their equipment both physically and logically secure. Many companies are content with this level of security, but other security conscientious companies purchase thousands of dollars in hardware encryption devices. Hardware encryption devices provided a means of strong encryption over an already private data communication medium. Both leased lines and hardware encryption devices allow companies to extend their trusted networks over a private Wide Area Network (WAN). Because of the advent of VPN and the inherent cost saving advantages their needs to be a way to provide the same secure functionality over an untrusted network (the internet). VPN can provide this functionality. There are three parts to this paper. The first is being able to understanding the fundamentals of Secure Gateway-to-Secure Gateway VPN with the introduction of IPSec protocol, the second is configuring a VPN connection using Cisco routers as security gateways, and third is how additional security parameters such as NAT, extended IP access lists and IP accounting can be applied to a VPN connection.

VPN Disclaimer:

Converting from a dedicated leased line to a VPN solution must be taken under careful scrutiny. VPN may prove to be too great of a risk to run business critical (real time) applications contributing directly to a corporation's revenue stream. In house terminating VPN connections that are non-ISP-managed can span

[4] "Intel Networking Technologies" Intel Corporation, 2003. http://www.intel.com/network/technologies/vpn.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

multiple Internet Service providers. There is no guaranteed performance or established Service Level Agreement (SLA) stating minimum uptime, millisecond delay or acceptable amount of line errors. An SLA is stated clearly when purchasing a dedicated lease line. There can be a delicate balance between cost savings and guaranteeing delivery of mission critical data. An example was presented by Eric Cole during a Raleigh, NC SANS convention in October, 2003 of a stock brokerage firm losing over 3.5 million dollars in three months due to an inconsistent millisecond delay across a VPN connection. The delay was just enough to throw off buyers and sellers real-time transactions by fractions of a point causing the company to reimburse traders.[5] This is one reason why VPN connectivity solutions are more widely seen connecting non-mission critical hub or Inter-company sites into larger corporate facilities.

Fundamentals behind Security Gateway-to-Security Gateway VPN

> 'VPN' or 'Virtual Private Network,' is probably the most recklessly used term in the networking industry. It is being portrayed as a panacea for a broad set of problems and solutions, when the objectives themselves have not been properly thought out…no matter what definition you choose, the basic idea is to create a private network via tunneling and/or encryption over the public Internet."[6]

The word VPN causes confusion because of the various types of VPN technology available today. VPN? A majority of people immediately associate VPN with a means of remote access using a software application to connect to an organization from client machines (desktops or laptops) through cable or DSL service providers. This type of VPN is commonly used, but is more suited for a topic discussion on Client-to-Server VPN connections. The center of discussion for this paper will focus on site-to-site VPN connections.

SG-to-SG VPNs are established through a network tunnel. Tunnels are logical communication paths transmitting private data over public networks. Secure Tunnels guarantee the privacy and integrity of the transmitted data and the authenticity of the parties communicating[7]. In reference to the OSI model, there are two types of tunnels, layer 2 and layer 3. SG-to-SG VPN technology utilizes layer 3 tunneling, which allows the VPN technology to be independent of any layer 1 physical media and layer 2 data transmission technology. For instance, a large corporation can still deploy a VPN tunnel over their OC3 ATM connection, through the internet and successfully deliver data to a smaller company with T1

[5] Eric Cole. "SANS Security Essentials T1 Conference" October 2003, Raliegh, NC.

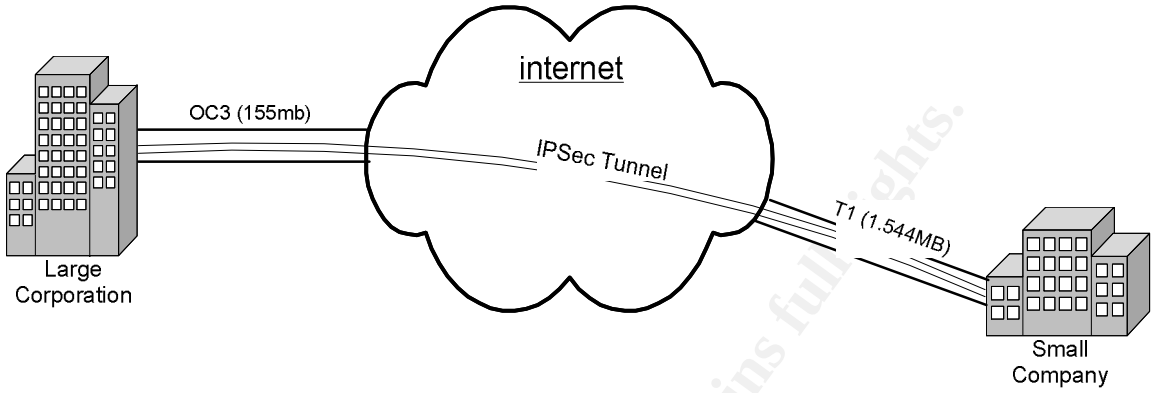
[6] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 208

[7] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 209

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

internet access. The layer 3 tunneling protocol most commonly used today to achieve site-to-site connectivity across the internet is IPSec. This concept is illustrated by the self-created figure 1 below:

Figure 1



Terms and Definitions:

Now that we have discussed the concepts of SG-to-SG VPN connections, we can start addressing the topic in more detail. Here are some definitions and Terms that will be used throughout the remainder of the paper.

Encryption - Provides data confidentiality.

Authentication - Provides data integrity.

Internet Protocol Security (IPSec) - A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between two sites.

Internet Security Association and Key Management Protocol *(ISAKMP)* - This is the framework which defines the mechanics of implementation a key exchange protocol and the negotiation of a security association.

Internet Key exchange protocol (IKE) - Provides authentication of the IPSec peers, negotiates security associations, and establishes IPSec keys.

Hashed Message Authentication Code (HMAC) – Combination of hash algorithm and secret shared key.

DES - Data Encryption Standard used to encrypt packet data. 3DES is no longer the best method of encryption, but is considered reliable and secure.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

MD5 (HMAC variant) - MD5 (Message Digest 5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

Authentication Header (AH) - A security protocol which provides data authentication.

Encapsulating Security Payload (*ESP*) - The protocol which provides data services by encapsulating the data that needs to be protected.

Peer - Refers to the two Cisco routers on either side of the VPN tunnel.

Security association (SA) - IPSec security association which describes how two or more entities will use security services for a particular data flow. This includes the methods which will be used for encryption and authentication.

Security Parameter Index (SPI) -This is a number combined with an IP address and security protocol identifies a SA.

Transform set - Represents a certain combination of security protocols and algorithms that the peers on each end of the tunnel must agree upon before initiating a secure data flow.

Tunnel – A secure communication path between two peers

Intranet – Represents a private network governed by one organization. In SG-to-SG VPN context this would be an IPSec connection between two offices, for one company, in separate geographic locations.

Extranet – Represents two private networks (intranets) connected to one another to exchange data. In SG-to-SG VPN context this would be an IPSec connection between two separate companies.
[8]

IPSec Tunneling:

IPSec technology presents a way to protect sensitive data that travels across untrusted networks. IPSec is the IETF standard for network layer tunneling described in RFC 1825 through 1829.[9] "With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables application such as virtual private networks (VPNs), including

[8] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

[9] R. Atkinson. "Security Architecture for the Internet Protocol" IETF. August 1995
http://www.ietf.org/rfc/rfc1825.txt?number=1825

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

intranets, extranets…."[10] IPSec allows the creation of a secure tunnel between two Security Gateways or IPSec compliant routers. Intranets in separate geographic locations can be created across the internet. This concept is commonly referred to as transferring data from trusted networks across an untrusted network. IPSec was created to provide the following functionality across the internet.

- **Data Confidentiality**—the IPSec sender can encrypt packets before transmitting them across a network.
- **Data Integrity**—the IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication**—the IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- **Anti-Replay**—The IPSec receiver can detect and reject replayed packets.[11]

For IPSec to achieve this functionality it requires an Internet Key Exchange (IKE) methodology. IPSec is established using a higher level protocol called ISAKMP combined with lower level protocols SKEME key exchange and a subset of Oakley key exchange.[12] ISAKMP protocol conducts peer negotiation to provide mutual authentication of tunnel endpoints using a common key exchange. An entire paper can be written on IPSec key exchange and is out of the scope of this paper. Please refer to Chris Gutridge's, March 2003 GSEC paper for additional detail on ISAKMP key exchange.[13] What is important to remember is that IPSec protocol allows you to define a set of security associations. The next section defines these security associations and how to configure them on peering security gateways.

---

[10] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

[11] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

[12] "Internet Key Exchange Security Protocol Commands" Cisco Systems, Inc. 2002, 669-73
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a00800eeaf5.html

[13] Chris Gutrdige, "IPSec Tunnel Creation" March 2003.
http://www.sans.org/rr/papers/index.php?id=1107

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Establishing an Inter-company VPN connections (Extranet):

After reading this section you should be able to configure peering Cisco routers using IPSec and understand the functionality of each command. All configuration presented below is specific to Cisco Hardware running IOS 12.1 or higher. However, it is important to note, "IPSec is standards-based, Cisco devices will be able to interoperate with other IPSec-compliant networking devices…"[14] This allows for a lot of flexibility. All companies do not deploy the same networking hardware in their environment, but as long as they are IPSec compliant, network connectivity can be established via IPSec tunneling protocol.

> When creating IPSec tunnels, the main goal is to protect data flows that carry confidential or sensitive data over an untrusted or public network. Therefore, before planning your IPSec tunnel implementation, you must have a solid understanding of the traffic you want protected by IPSec tunnels, and the sources and destinations of this traffic.[15]

Below a fictional scenario has been created to adhere to the above criteria:

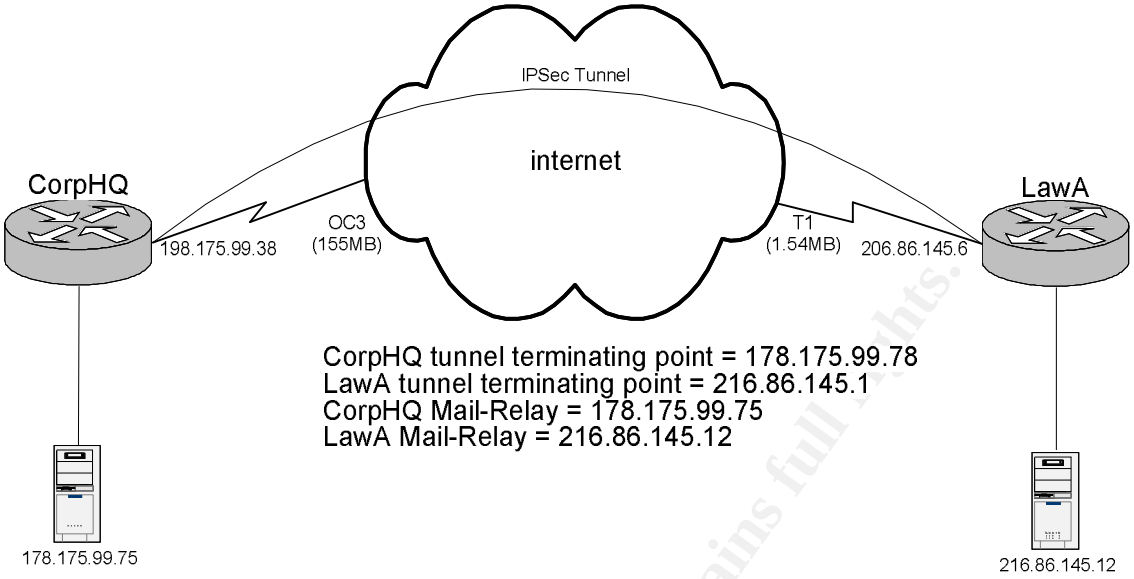
A large corporation (CorpHQ) has a business need to securely send/receive confidential E-mail with a third party law firm (LawA). All forthcoming configurations will be based on self-created figure 2.

© SANS Institute 2004, Author retains full rights.

[14] **"**Defining VPN Tunnel Policies**"** Cisco Systems, Inc. 1992-2003, 9.1-23 http://www.cisco.com/en/US/customer/products/sw/cscowork/ps3994/products_user_guide_chapter09186a008014f5ec.html

[15] **"**Defining VPN Tunnel Policies**"** Cisco Systems, Inc. 1992-2003, 9.1-23 http://www.cisco.com/en/US/customer/products/sw/cscowork/ps3994/products_user_guide_chapter09186a008014f5ec.html

Figure 2



Key Components of creating an IPSec tunnel in chronological order:

- Crypto Policy
- Transform-set
- Access-list
- Defining your crypto map[16]

Crypto Policy:

A crypto policy must be established identically on both the corporate router and the third party corporation's router including the pre-shared key. The only change needed on the third party's peering router is CorpHQ's tunnel terminating IP address. Before configuring a crypto policy five parameters must be decided upon by both ends of the VPN tunnel. If any of these parameters do not match, the VPN tunnel cannot be established.

1. What encryption will be used? DES or 3DES
2. What Authentication? Pre-share, rsa-encr, rsa-sig
3. What Diffie-Hellman group? 1, 2 or 5
4. What Hash? SHA or MD5
5. What lifetime? Between 60-86400[17]

---

[16] Road Runner. "Site-to-Site VPN Using Cisco IOS VPN" NetworkFest.com January/February 2003
http://www.networkfest.com/articles/010103/a010103_08/a010103_08.html

[17] "Internet Key Exchange Protocol" Cisco Systems, Inc. February 2, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113newft/113t/1133t/isakmp.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To configure a policy use global configuration mode as shown below:

```
CorpHQ(config)# crypto isakmp policy 60                 # line 1
CorpHQ(config-isakmp)# encr 3des                        # line 2
CorpHQ(config-isakmp)# hash md5                         # line 3
CorpHQ(config-isakmp)# authentication pre-share         # line 4
CorpHQ(config-isakmp)# group 2                          # line 5
CorpHQ(config-isakmp)# lifetime 3600                    # line 6

CorpHQ(config)# crypto isakmp key [pre-shared key] address 216.86.145.1 # line 7
```

Line 1 – Establish an ISAKMP protection policy with priority. The highest priority is 1 and the lowest priority 10,000.[18] This is the beginning of IKE negotiation process for IPSec.
Line 2 – Specifies Triple DES encryption used with this policy
Line 3 – Specifies MD5 as the hash algorithm
Line 4 – Specifies a pre-shared key must be used to apply the security policy
Line 5 – Specifies which Diffie-Hellman group will be applied.
Line 6 – Specifies when the crypto policy's security associations expire and must be reestablished. 3600 seconds (1 hour) or 4,608,000 kilobytes (10MB per second for one hour) is the default for a Cisco isakmp policy. [19]
Line 7 – The pre-share key must be the same on each peer router. The crypto isakmp shared key also specifies the terminating ends of the IPSEC tunnel.

Transform Set:

Transform sets are a combination of security protocols and algorithms that protect the data flow across the internet. Specifically, the IPSec transform set parameters is a pre-established configuration on peering routers to form another Security Association (SA). The SA configuration must match on each peering router in order to successfully encrypt and authenticate from the sender and decrypt and unauthenticated at the receiver.

Encryption and/or Authentication must be selected out of the below choices:

ah-md5-hmac	AH-HMAC-MD5 transform
ah-sha-hmac	AH-HMAC-SHA transform
esp-3des	ESP transform using 3DES(EDE) cipher (168 bits)

---

[18] "Internet Key Exchange Security Protocol Commands" Cisco Systems, Inc. 2002, 669-73 http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a00800eeaf5.html

[19] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002 http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

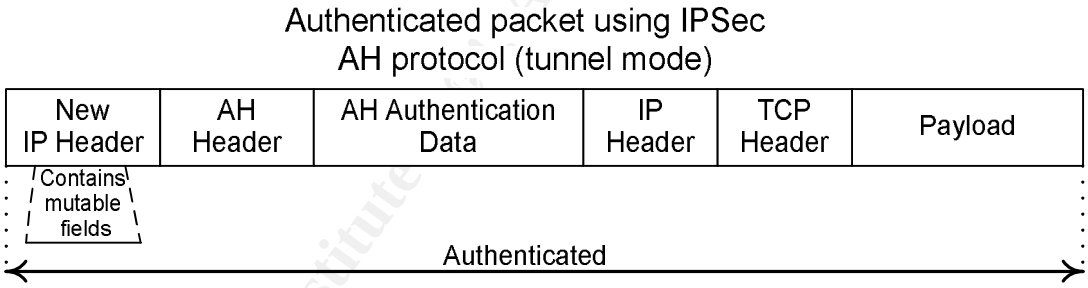
esp-des	ESP transform using DES cipher (56 bits)
esp-md5-hmac	ESP transform using HMAC-MD5 auth
esp-null	ESP transform w/o cipher
esp-sha-hmac	ESP transform using HMAC-SHA auth

The transform set allows the user to configure ESP or AH IPSec security protocols. Each protocol is described below.

AH and ESP: (tunnel mode only)

Authentication Header (AH) protocol ensures data integrity and replay protection for IP data. AH is able to guarantee data integrity by using a hash algorithm (such as MD5) and a secret shared key to produce a Hashed Message Authentication Code (HMAC). (Further detail on hash functions can be found in John Edward Silva's, January 15, 2003 GIAC practical)[20]. The AH protocol protects the complete datagram including the IP header, AH header, IP header, and IP payload. "Any change to any field (except mutable fields)…can be detected".[21] Note: Mutable fields are places in the IP header which must change on the way to their destination. They include the Type of Service, flags, fragment offset, time to live and header checksum. An example of an AH protocol authenticated packet is shown in figure 3.

Figure 3



(based on Mairs, 233)

AH only works with non-fragmented IP packets. When an AH packet reaches its intended destination, the receiver will first reassemble any fragmented packets. Once resembled, the AH process will unauthenticate the packet. If any part of the packet is fragmented or changed it will be discarded. AH discards the packet, because the agreed upon hash value between the sender and receiver will not match.[22] This protects against fragment attacks and anti-replay attacks.

---

[20] John Edward Silva. "An Overview of Cryptographic Hash Functions and Their Uses" January 15, 2003.
http://www.sans.org/rr/papers/index.php?id=879

[21] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 388

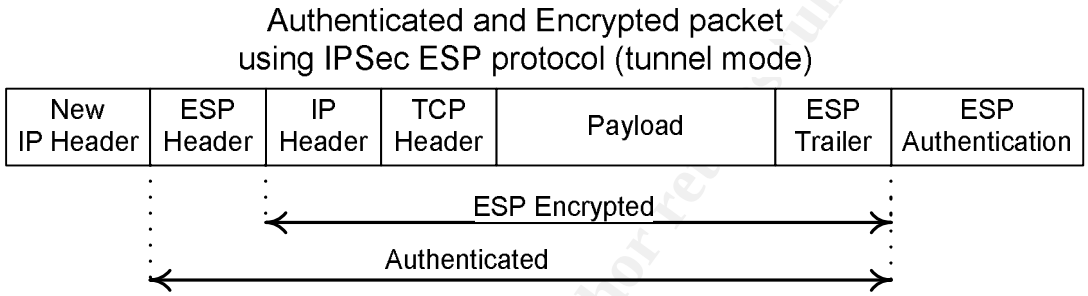
[22] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 386

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Any fake packets that are sent to either end of an IPSec tunnel terminating point will be discarded, because they will not pass the checksum verification. AH provides three of the four functionalities for creating an IPSec tunnel. Data integrity, data authentication, and anti-replay services are all achieved through AH, but not data confidentiality. With AH all data is sent in clear text and this is why ESP is the preferred protocol used with IPSec tunnel creation for Extranets.

Encapsulation Security Payload protocol ensures both data authentication and confidentiality for IP data. ESP is able to guarantee both these services by creating a new IP packet within an ESP header and trailer. An example of an ESP packet is shown in figure 4.

Figure 4



(based on Mairs, 233)

Contained within the ESP header and trailer are the original IP Header, TCP header and payload. These fields are encrypted using a manually specified cryptographic algorithm.[23] This makes the original destination IP address, type of data being sent (TCP header), and the actual data being sent (payload) unreadable while traversing the internet.

The authenticated portion of the ESP packet includes the ESP header and ESP authentication. The ESP header contains two parts (not shown in figure 4), the Security Parameter Index (SPI) and the sequence number. "The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the Security Association for this datagram."[24] The SPI is the destination IP combined with a hash algorithm such as MD5 or SHA. The second part is the sequence number which implements a counter with each packet. For example, when one packet is sent it is given a number of 1, when the next packet is sent it is given a number of 2 and so on. This function prevents replay attacks. If a fake packet is sent to the receiving security gateway, it will be discarded, because it is not part of the increasing

[23] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 394

[24] S. Kent and R. Atkinson. "IP Encapsulating Security Payload" IETF. November 1998 http://www.ietf.org/rfc/rfc2406.txt?number=2406

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

number sequence. Lastly, ESP authentication trailer provides a checksum. If any of the data within the ESP header ESP encrypted information has been altered the packet will be discarded. Since the ESP protocol provides the highest level of security and encrypts data across the internet, it will be used in the above fictional scenario.

CorpHQ(config)# **crypto ipsec transform-set CorpHQ-vpn esp-3des esp-md5-hmac** # line 1
CorpHQ(config)# **mode (tunnel or transport)** # line 2

Line 1 – ESP is selected because it provides both authentication and confidentiality services. There are three parts to line one. "CorpHQ-vpn" is the name of the Transform Set. Essentially, CorpHQ-vpn is the name of a security association and the rest of the configuration establishes the rules of the SA. "esp-3des" encapsulates and encrypts the IP Header, TCP Header and Payload while traversing the internet. "esp-md5-hmac" authenticates the encrypted packet with the destination IP address and an MD5 hash while traversing the internet. Additionally, when NAT is introduced, ESP eliminates conflicts between NAT and AH's checksum verification mechanism. ESP only performs integrity checks on bits in the header that are not altered by NAT devices.[25] This will be covered in more detail in the Additional Securities section.

Line 2 - Tunnel mode is enabled by default on Cisco devices. "Tunnel mode is used whenever either end of a security association is a gateway…..The advantages of Tunnel mode are total protection of the encapsulated IP datagram and ability to use private addresses."[26] IPSec tunnel mode should be utilized with extranet connectivity to a third party company. For reference, transport mode can be used if less overhead processing is required by the security gateway. Additionally, transport mode is often used when IPSec connectivity between intranets needs to be established and every host in one intranet has access to every host in the other.

Crypto Access List:

The crypto access list will specify which data traffic will pass through the IPSec tunnel. Crypto access lists are more like security associations than traditional ip access lists. "…the access lists used for IPSec are used only to determine which traffic should be protected by IPSec, not which traffic should be blocked or permitted…".[27] For example, if outbound data matches one permit statement on

[25] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 470

[26] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 392-3

[27] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CorpHQ and the same permit statement is mirrored on LawA then data is authenticated, encrypted and passed across the IPSec tunnel. As data reaches the tunneling endpoint at LawA or vise versa, the crypto access list will discard out any traffic that does not meet the permit criteria. Essentially, a crypto access list applied to an interface filters both inbound and outbound traffic. This provides the strongest level of security. In addition, since we are configuring ipsec-isakmp crypto maps, IPSec connections will not be accepted unless they meet the criteria of the permit statements.[28]

Reference for below Access list:
CorpHQ interface IP address = 153.183.175.5
CorpHQ tunnel terminating point = 178.175.99.78
LawA tunnel terminating point = 216.86.145.1
CorpHQ Mail-Relay = 197.175.99.75
LawA Mail-Relay = 216.86.145.12
CorpHQ management subnet = 178.175.95.0

CorpHQ(config)# **ip access-list extended LawA-intel** # line 1
CorpHQ(config-ext-nacl)# **permit icmp host 153.183.175.5 host 216.86.145.1** # line 2
CorpHQ(config-ext-nacl)# **permit ip host 178.175.99.75 host 216.86.145.12** # line 3
CorpHQ(config-ext-nacl)# **permit ip host 178.175.99.78 host 216.86.145.12** # line 4
CorpHQ(config-ext-nacl)# **permit icmp 178.175.95.0 0.0.0.255 host 216.86.145.12** # line 5

LawA would contain a mirrored Crypto Access-list.

LawA(config)# **ip access-list extended** (LawA-names-access-list)
LawA(config-ext-nacl)# **permit icmp host 216.86.145.1 host 153.183.175.5**
LawA(config-ext-nacl)# **permit ip host 216.86.145.12 host 178.175.99.75**
LawA(config-ext-nacl)# **permit ip host 216.86.145.12 host 178.175.99.78**
LawA(config-ext-nacl)# **permit icmp 216.86.145.12 host 178.175.95.0 0.0.0.255**

Line 1 – Creating a named extended IP access list
Line 2 – Permits ICMP from the CorpHQ tunnel terminating interface to the LawA tunnel terminating interface. This is used for management testing purposes in order to test layer 3 connectivity and latency across the internet. This allows network personal to run extended pings from tunnel endpoints and prove IPSec is functioning correctly.
Line 3 – Permits IP connectivity between the CorpHQ's and LawA's mail-relay servers.
Line 4 – Permits IP connectivity from CorpHQ's tunnel terminating end-point to LawA's mail-relay server.
Line 5 – Permits every host at CorpHQ on the 178.175.95.0 subnet to send ICMP packets to LawA's mail-relay server. This has been configured to allow network

[28] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

management devices periodically send icmp requests to the mail server to make sure it is still connected to the network.

Crypto Maps:

A crypto map pulls all the pieces together required to create an IPSEC connection. This includes the security associations contained within the access-list and the transform set joined with the peer address. These crypto maps will be applied to interfaces through which IP traffic passing through the interface is evaluated against the applied crypto map set. If a crypto map entry sees outbound IP traffic that should be protected and the crypto map specified the use of IKE, a security association is negotiated with the remote peer according to the security associations in the crypto map. For IPSec to succeed between two IPSec peers, both peers crypto map entries must contain compatible configuration statements (SAs).[29]

```
CorpHQ(config)#crypto map CorpHQ-vpn 60 ipsec-isakmp      #line 1
 CorpHQ(config-crypto-map)#set peer 216.86.145.1          #line 2
 CorpHQ(config-crypto-map)#set transform-set CorpHQ-vpn   #line 3
 CorpHQ(config-crypto-map)#match address LawA-CorpHQ      #line 4
```

Line 1 – Configuring the crypto map with a name CorpHQ-vpn with a sequence number of 60. Ipsec-isakmp specifies that IKE will be used to establish the IPSec tunnel between peers. This command also places the user in crypto map configuration mode allowing the user to specify the below parameters. NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.
Line 2 – Sets the IPSec tunnel's remote terminating end. This tells CorpHQ where it can forward protected traffic.
Line 3 – Configures the named transform-set to be used. The transform-set contains Hash algorithm and Encryption method. Note: Several transform sets can be configured under a single crypto map.
Line 4 – Applies the previously configured named Crypto access list to the crypto map. The crypto access list describes what traffic should be protected.
Note: Optional parameters that specify additional SAs are configurable.[30]

Applying an IPSec tunnel:

Once the crypto map has been established on both peering routers it is time to apply the configuration to an interface. After this configuration, no additional configuration coordination with LawA will need to be completed.

```
CorpHQ(config-if)# crypto map CorpHQ-vpn          #line 1
```

[29] Tyrone Harding. "Configuring IPSec and ISAKMP" White Paper # WP20010117-01, 2003. 5

[30] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Line 1 – Applies crypto map to an interface. All inbound traffic to the interface will be processed against the crypto map. If it does not meet the established security associations of the crypto map the traffic will be dropped or, if specified in the router configuration, routed elsewhere.

Recap:

At this point, there is now an IPSec tunnel created between LawA and CorpHQ VPN concentrator routers. IPSec is providing encryption and authentication which is protecting trusted data across an untrusted network (the internet). The IP traffic destined from CorpHQ to LawA and vise versa must match the established criteria of the crypto map before it will be protected and allowed to traverse the IPSec tunnel. In this case, data from the LawA's mail-relay server (216.86.145.12) and Concentrator terminating point (216.86.145.1) has access into CorpHQ's mail-relay server via the established IPSEC tunnel.

In many cases, corporations are content with this configuration and level of security. However, the IP traffic from LawA's mail-relay server to CorpHQ's mail-relay server is unrestricted. Since CorpHQ does not own or control LawA's mail-relay server, CorpHQ cannot enforce company security policies and ensure physical security of the box. Because of these two vulnerabilities CorpHQ has the need to implement additional security parameters to ensure only e-mail traffic is being passed between the two mail-relay servers.

Additional Security Parameters to be implemented with IPSec:

Three security related parameters that can be configured on a Security Gateway are extended IP Access Control Lists (ACLs), Network Address Translation (NAT) and IP accounting.

Extend IP access list:

"IPSec implementations support machine-based certificates only, rather than user certificates. As a result, any user with access to one of the endpoint machines can use the tunnel."[31] This results in the need for a strict access list with third party companies. Without applying an access-list to CorpHQ's router interface (with an applied crypto map) a wide open door for LawA's mail-relay server has been created into CorpHQ's mail-relay server. In the above scenario, there is only the need to pass e-mail traffic between tunnel endpoints. Any Network traffic not meeting one of the below permit statements will be discarded by the router once traversing the IPSec tunnel from LawA. The below extended

[31] John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002. 219

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ACL configuration will restrict the tunnel to SMTP network traffic. For a complete reference on extended IP access lists please reference Nancy Novato's, July 5, 2001 GIAC practical.[32]

Reference for below Access list:
CorpHQ Mail-Relay = 178.175.99.75
LawA Mail-Relay = 216.86.145.12

CorpHQ(config)# **ip access-list extended 101**
CorpHQ(config-ext-nacl)#
access-list 101 permit tcp host 216.86.145.12 host 178.175.99.75 eq smtp
access-list 101 permit tcp host 216.86.145.12 eq smtp host 178.175.99.75 gt 1023 established

CorpHQ(config)# **ip access-list extended 102**
CorpHQ(config-ext-nacl)#
access-list 102 permit icmp host 178.175.99.35 host 216.86.145.12
access-list 102 permit tcp host 178.175.99.35 host 216.86.145.12 eq smtp

Network Address Translator (NAT)

NAT applies a defense in-depth methodology by adding another layer of security. NAT is a router function defined in RFC 1631 and stemmed from the short term need to conserve public IP address space. To accomplish this, private address space was defined in RFC 1579.[33] Ranges are below:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

These ranges are not routable on the internet only within a private IP address space, such as a company's intranet. Unless a company plans on giving their primary e-mail server a public IP address, NAT will need to be used with the implementation of IPSec.

Caution must be taken when using NAT with IPSec tunnels. NAT device can not be placed in the middle of an IPSec tunnel when using AH because the source and/or destination IP addresses are modified. This causes an AH packet to fail the checksum verification and the router believes the packet has been tampered with, so the packet is discarded.

[32] Nancy Novato. "Easy Steps to Cisco Extended Access List" July 5, 2001 http://www.sans.org/rr/papers/index.php?id=231

[33] K. Egevang and P. Francis. "The IP Network Address Translator (NAT)" May 1994 http://www.ietf.org/rfc/rfc1631.txt?number=1631

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

> If you use Network Address Translation (NAT), you should configure static NAT translations so that IPSec will work properly. In general, NAT translation should occur before the router performs IPSec encapsulation; in other words, IPSec should be working with global addresses.[34]

In our given scenario, NAT is configured for 2 reasons. The first reason is based on functionality. CorpHQ does not want to route LawA's public IP address into its private network. In order to make an e-mail from LawA routable on CorpHQ's private network, NAT must readdress the traffic to be internally routable. The second reason for implementing NAT (which is more of a side benefit) is additional security. Combined with IPSec authentication and encryption NAT provides a privacy mechanism. Machines on the internet backbone cannot monitor which hosts inside a company's intranet are sending and receiving packets.[35]

CorpHQ(config)# **ip nat outside source static 216.86.145.62 192.168.8.215** #line 1

Line 1 - In this case NAT replaces packets with the IP header of 206.86.145.62 with a new internal routable address of 192.168.8.225.

IP accounting:

After the above configuration is put into place, CorpHQ has done all they can at the network layer to secure their Extranet VPN connection with LawA. IP accounting can be enabled on CorpHQ to monitor all network traffic and see if any unwanted network traffic is traversing the IPSec tunnel terminating interface. IP accounting output-packets configuration statement allows you view the source and destination IP addresses traversing each ip accounting enabled interface. Any unwanted network traffic can be detected.

CorpHQ(config-if)# **ip accounting output-packets** #line 1

Line 1 – This applies ip accounting to an interface. This will collect all of the outbound traffic for an interface. Below, is a sample of ip accounting collected data from a cisco router.

Source	Destination	Packets	Bytes
173.185.42.166	192.168.8.224	60	5520
216.86.145.12	192.168.8.215	480	28320
11.7.248.103	192.168.8.232	61	1708

[34] Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

[35] K. Egevang and P. Francis. "The IP Network Address Translator (NAT)" May 1994
http://www.ietf.org/rfc/rfc1631.txt?number=1631

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Final Configuration:

CorpHQ# **show interface fastehternet0/0**

```
interface FastEthernet0/0
 description ***CorpHQ internet ***
 ip address 143.183.175.4 255.255.255.0
 ip access-group 101 in                          #line 1
 ip access-group 102 out                         #line 2
 ip accounting output-packets                    #line 3
 ip nat outside                                  #line 4
 duplex full
 speed 100
 crypto map CorpHQ-vpn                           #line 5
```

Line 1 – Applies access list 101 to all traffic that passes through interface FastEthernet0/0 inbound
Line 2 – Applies access list 102 to all traffic that passes through interface FastEthernet0/0 outbound
Line 3 – Records all traffic that passes through interface FastEthernet0/0
Line 4 – Applies NAT table for all outside public IP address.
Line 5 – Applies the Crypto map to the interface.

Conclusion:

The use of VPN technology continues to increase because of the tremendous cost saving advantages to companies. There are many different types of VPN technologies available, one being site-to-site VPN which is established between IPSec compliant security gateways. These security gateways can be configured with various security associations to protect private data across the internet. Configuration of security gateways has been presented and explained to assist an individual in establishing their own IPSec connection. The use of NAT, IP extended access lists and IP accounting can be implemented to provide additional security for an IPSec tunnel termination points.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

James A. Martin. "Securing Business Networks". iQ Magazine, September/October 2003
http://business.cisco.com/prod/tree.taf%3Fasset_id=103850&ID=92781&ListID=44753&public_view=true&kbns=1.html

John Mairs. "VPNs A Beginner's Guide" McGraw-Hill\Osborne, 2002

Tyrone Harding. "Configuring IPSEC and ISAKMP" White Paper # WP20010117-01, February 11th, 2003.

Road Runner. "Site-to-Site VPN Using Cisco IOS VPN" NetworkFest.com January/February 2003
http://www.networkfest.com/articles/010103/a010103_08/a010103_08.html

Eric Cole. "SANS Security Essentials T1 Conference" October 2003, Raliegh, NC.

K. Egevang and P. Francis. "The IP Network Address Translator (NAT)" May 1994
http://www.ietf.org/rfc/rfc1631.txt?number=1631

Stephen Jones. "Lease Line to VPN" Intel Global Engineering. GER – Senior Network Engineer, October 29th, 2003.

"Intel Networking Technologies" Intel Corporation, 2003.
http://www.intel.com/network/technologies/vpn.htm

Kent R. Atkinson and Madison, R. Glenn. "IPSec Network Security" Cisco Systems Inc, February 3, 2002
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm

Nancy Novato. "Easy Steps to Cisco Extended Access List" July 5, 2001
http://www.sans.org/rr/papers/index.php?id=231

John Edward Silva. "An Overview of Cryptographic Hash Functions and Their Uses" January 15, 2003.
http://www.sans.org/rr/papers/index.php?id=879

Chris Gutridge. "IPSec Tunnel Creation" March, 2003
http://www.sans.org/rr/papers/index.php?id=1107

"Internet Key Exchange Protocol" Cisco Systems, Inc. February 2, 2002

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113newft/113t/1133t/isakmp.htm

S. Kent and R. Atkinson. “IP Encapsulating Security Payload” IETF. November 1998
http://www.ietf.org/rfc/rfc2406.txt?number=2406

R. Atkinson. “Security Architecture for the Internet Protocol” IETF. August 1995
http://www.ietf.org/rfc/rfc1825.txt?number=1825

“Internet Key Exchange Security Protocol Commands” Cisco Systems, Inc. 2002, 669-73
http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_command_summary_chapter09186a00800eeaf5.html

Need CCO access
“Defining VPN Tunnel Policies**”** Cisco Systems, Inc. 1992-2003, 9.1-23
http://www.cisco.com/en/US/customer/products/sw/cscowork/ps3994/products_user_guide_chapter09186a008014f5ec.html

© SANS Institute 2004, Author retains full rights.