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

IMPLEMENTING SITE-TO-SITE IPSEC VPNS USING CISCO ROUTERS

Millie Ives
May 4, 2001

1. Introduction

Businesses and organizations need a way to exchange important information with their business partners securely via the Internet. A Site-to-site Virtual Private Network (VPN) is one way to provide confidentiality/privacy for the data being passed over the Internet. If both organizations already have high-speed Internet access and Cisco routers available, this option may be a cost effective solution.

This paper will provide step-by-step instructions on how to implement a site-to-site VPN using IPSEC and Cisco Routers. The steps documented in this paper are geared for small to medium size businesses with a small number of locations that require private communications. The paper will also point out other security issues that should be considered when implementing site-to-site VPNs.

2. Hardware and Software Requirements

Cisco recommends a 2600 or 3600 series router for use in small to medium business site-to-site VPNs. First check the Internetworking Operating System (IOS). The routers ship with only the IP feature set. You have to buy another version of the IOS to use IPSEC 56 bit encryption or IPSEC 3DES encryption. If you do not know if your router has a version that supports IPSEC, the easiest way to check is to use the following commands

```
RouterA#config t
RouterA (config)# cry?
```

This command will give you a list of commands that start with "cry". If you don't see "crypto" listed, the version of the IOS on your router does not support IPSEC.

If you do see the "crypto" command listed, check for 3DES support using the following command:

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption ?
```

This will list the encryption algorithms supported by your IOS. Check for "3DES". If this algorithm is not listed, then your IOS only supports 56-bit encryption. Contact your Cisco vendor to obtain the IOS with IPSEC 3DES feature set.

You also need to make sure that you have sufficient volatile memory (RAM) and flash memory for the new IOS. Use the following command to display the amount of memory and flash on your router.

```
Router#show version
```

Check with your Cisco vendor for the minimum amount of RAM and flash required for the IPSEC 3DES IOS. I recommend 32 MB of RAM and 16 MB of flash for the 2600 series router.

3. Configuring IKE Security Protocol

The two VPN router peers will use Internet Key Exchange (IKE) in conjunction with IPSEC to negotiate three items:

- encryption algorithm,
- hash algorithm, and
- authentication method

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For the Cisco IOS, configuring IKE involves the following steps**:**

a. Ensure the IKE feature is enabled. This feature is enabled by default. Just to make sure type the following command:

Router (config)# crypto isakmp enable

b. Check the access-lists (filter rule sets) of your router. Make sure they allow "UDP port 500". This is the port used by IKE. You may have to add a rule to allow "UDP port 500".

c. Create the IKE policy to be used for your VPN. The table below lists the parameters you can configure for IPSEC.

Parameter	**Accepted Values**	**Keyword**	**Default Value**
Encryption algorithm	56-bit DES-CBC 168-bit DES	Des 3des	56-bit DES-CBC 168-bit DES
Hash algorithm	SHA-1 (HMAC variant	Sha	SHA-1
Authentication method	RSA signatures RSA encrypted nonces Pre-shared keys	Rsa-sig Rsa-encr Pre-share	RSA signatures
Diffie-Hellman group	768-bit Diffie-Hellman or 1024-bit Diffie-Hellman	1 2	768 bit Diffie-Hellman
Security association's lifetime	Any number of seconds	--	86400 seconds (one-day)

Table 1: IKE Policy Parameters[1]

The Cisco documentation provides some guidance on which values to select for these parameters. Essentially, increased security may come at the expense of performance. You will have to assess how much risk your company can tolerate versus the performance level they want to sustain. For example 168-bit DES provides more security but may use more CPU cycles. (NOTE: You can purchase an add-on card to accelerate encryption.)

The Cisco documentation also provides the following guidance:

- Authentication methods:
  - You will need a certification authority (CA) if you want to use RSA signatures. This method provides non-repudiation for the IKE negotiation.
  - Uses of RSA encrypted nonces require both organizations to possess each other's public key.
  - Pre-shared keys although easy to configure are not as secure RSA signatures.
- Diffie-Hellman group identifier
  - The Diffie-Hellman (DH) public-key cryptography protocol is used in IKE to establish session keys. The 1024-bit DH is harder to crack but takes more CPU cycles to complete.
- Hash Algorithm
  - "MD5 has a smaller digest and is considered to be slightly faster than SHA-1. There has been a demonstrated successful (but extremely difficult) attack against MD5; however, the HMAC variant used by IKE prevents this attack."[2]

[1] Configuring Internet Key Exchange Security Protocol, pp 7-8.
[2] Configuring Internet Key Exchange Security Protocol, p 21.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For the example we will use:

- Encryption algorithm: 3DES encryption 168-bit DES
- Hash algorithm: SHA-1(HMAC variant)
- Authentication method: RSA encrypted nonces
- Diffie-Hellman group identifier: 768-bit Diffie-Hellman (default setting)
- Security Association Lifetime – 86400 seconds (default setting)

Use the following commands for both routers

```
Router#configure terminal
Router (config)# crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash sha
Router(config-isakmp)#authentication rsa-encr
Router(config-isakmp)#end
```

To display the IKE policies for your router use the following command:

```
Router#show crypto isakmp policy
```

It is important that both routers agree on the IKE policy. IF the remote and local routers do not have the same policy, IPSec will not be established.

d. If you are using RSA encrypted nonces and are not using a certification authority (CA), you must manually configure RSA. Use the following commands for both the remote and the local router.

- Create and view your RSA key

```
Router (config)# crypto key generate rsa
Router (config)# show crypto key mypubkey rsa
```

Cut and paste the result for the "show crypto" command into a notepad and save it to a text document. Both organizations need to send their public key to each other. They can send the key (text document) to the each other via e-mail (using PGP encryption) or give it to each other on a floppy disk.

- Set ISAKMP Identity for each peer

Router(config)#crypto isakmp identity **IP_Address_of_peer_router**

- Specify Peer's RSA Public Key

```
Router(config)#crypto key pubkey-chain rsa
Router (config-pubkey-c)#addressed-key IP_address_of_peer_router
Router (config-pubkey-c)#key-string key-string-value-of-public-key
```

Paste in the key string value you received from your peer (see the "show crypto" step).

```
Router (config-pubkey-c)#quit
Router (config-pubkey)#end
```

© SANS Institute 2000 - 2002 - Author retains full rights.

4. Configuring Site-to-Site IPSEC Network Security

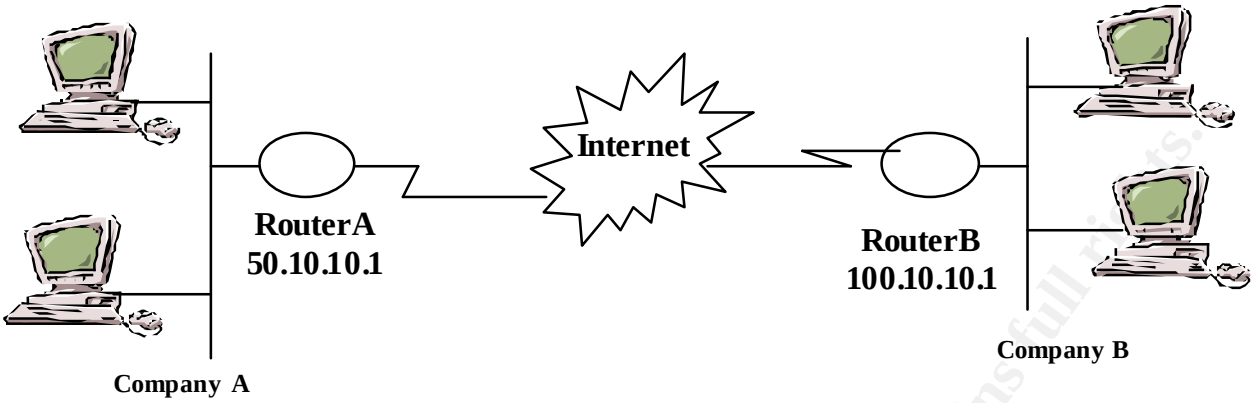


Figure 1. Site-to-Site VPN Diagram

After completing the IKE configuration, we can now configure IPSec. The steps for configuring IPSec are outlined below. Refer to Figure 1 for the IP addresses and router names used in the example.

- Check access-lists for IPSec compatibility

Make sure that both RouterA and RouterB allow IPSec traffic (protocol numbers 50 and 51).

- Create Crypto Access Lists

The crypto access list defines which IP packets will be encrypted and sent out via the VPN tunnel, and which inbound traffic will be decrypted.

Sample access-lists for RouterA and RouterB are as follows:

```
RouterA (config)# access-list 101 permit 50.10.10.0 0.0.0.255 100.10.10.0 0.0.0255
RouterB (config)#access-list 101 permit 100.10.10.0 0.0.0.255 50.10.10.0 0.0.0.255
```

- Define Transform Sets

The transform set defines the security protocols and algorithms that both peers will use for encryption and authentication. Table 2 (below) lists the allowed transformation combinations.

Transform Type	Transform	Description
AH Transform (Pick up to one)	Ah-md5-hmac Ah-sha-hmac	AH with the MD5(HMAC variant) authentication algorithm AH with the SHA (HMAC variant) authentication algorithm
ESP Encryption Transform (Pick up to one)	Esp-des Esp-3des Esp-null	ESP with the 56-bit DES encryption algorithm ESP with the 168-bit DES encryption algorithm (3DES or Triple DES) Null encryption algorithm
ESP Authentication Transform (Pick up to one)	Esp-md5-hmac Esp-sha-hmac	ESP with the MD5 (HMAC variant) authentication algorithm ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform (Pick up to one)	Comp-lzs	IP compression with the LZS algorithm

Table 2: Allowed Transform Combinations[3]

[3] Configuring IPSec Network Security, p. 17.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Authentication Header (AH) and the Encapsulation Security Payload (ESP) security protocols provide integrity, authenticity and confidentiality (only in the case of ESP) of the data. AH uses a keyed-hash function to provide authenticity and integrity. In the case of the AH, a hashing algorithm is used against the payload. The result of this algorithm is a message digest (a set of numbers). On the other end the remote router can run the same algorithm against the payload. If the result is the same as the message digest contained in the Authentication Header, the remote router has very high confidence that the message it received was not changed en-route. Encapsulation Security Payload protocol uses encryption to provide integrity, authentication and confidentiality of the information. "AH and ESP can be used independently or together, although for most applications just one of them is sufficient. In our example, we will use ESP with 3DES encryption.

For more information on the AH and ESP protocol please refer to the Request for Comments (RFCs) listed in the bibliography.

Both routers must have the same transform set configured. The following is a sample transform set:

Router (config)#Crypto ipsec transform-set set1 esp-3des

- Configure Tunnel Interface

IPSec uses tunnels to move packets through the Internet. The packet is encapsulated within another packet and assigned a new source and destination address. The source is the address of the local VPN router. The destination is the remote VPN router. Once the packet reaches the remote router, the outer source and destination addresses are removed to reveal the real source and destination address. The remote router then sends the packet to the actual destination.

An analogy would be sending a letter to your friend using a special courier service. The envelope would show your address as the source address and your friend as the destination. You would give your letter to a third party (a representative of the courier service). This third party could place your envelope inside another envelope and place its address as the source and a fourth party (a courier representative near your friend), as the destination address. Once the fourth party receives the envelope, it would remove the outer envelope revealing the original envelope. The fourth party would then give the envelope to the actual destination – your friend.

The following are some sample tunnel configurations

```
RouterA (config)#interface Tunnel0
RouterA (config-if)#ip unnumbered Serial0
RouterA (config-if)#no ip directed-broadcast
RouterA (config-if)#tunnel source Serial0
RouterA (config-if)#tunnel destination 100.10.10.1

RouterB (config)#interface Tunnel0
RouterB (config-if)#ip unnumbered Serial0
RouterB (config-if)#no ip directed-broadcast
RouterB (config-if)#tunnel source Serial0
RouterB (config-if)#tunnel destination 50.10.10.1
```

- Configure Crypto Map

The crypto map specifies the values to be used for the key management protocol. The peer address is the address of the remote router. The transform set is the name of the transform set you configured above. The access-list number used in the "match address 101" command corresponds to the crypto access-list you configured above. Sample configurations for the local and remoter router are listed below:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
RouterA(config)#crypto map map1 10 ipsec-isakmp
RouterA(config-crypto…)#set peer 100.10.10.1
RouterA(config-crypto…)#set transform-set set1
RouterA(config-crypto…)#match address 101

RouterB(config)#crypto map map1 10 ipsec-isakmp
RouterB(config-crypto…)#set peer 50.10.10.1
RouterB(config-crypto…)#set transform-set set1
RouterB(config-crypto…)#match address 101
```

- Apply Crypto Map to Tunnel Interface and to Serial Interface

Apply these commands to both routers. Apply the crypto map to both the tunnel and the router's external interface.

```
Router(config)#interface Serial0
Router(config-if)#crypto map map1
Router(config-if)#interface Tunnel0
Router(config-if)#crypto map map1
```

5. Additional Security Aspects to Consider

This paper provided step-by-step instructions on how to implement a site-to-site VPN. This paper did not cover all of the security aspects that you should consider when giving another organization access to your network. You should review your organization's security policy to see if this VPN will violate any of your organization's existing policies. Here are just some of the security aspects you should consider:

- You are giving outsiders full access to your network. Perhaps you should consider placing the VPN router in front of the firewall. This way the packets will be decrypted before they reach the firewall and will be inspected at the firewall just like all the other packets from the Internet. You could also consider using a firewall capable of providing VPN services such as the PIX firewall.
- Consider placing access-lists on the firewall that will restrict the other company's access to only the necessary servers.
- Consider using an Intrusion Detection System (IDS). An IDS is able to inspect the contents of the packets and "shun" unwanted traffic – potential intrusion attempts, etc.
- If the other organization's users will be accessing applications that implement some type of authentication, you should use the authentication. For example, if you can implement passwords on the application, make sure you turn on the password authentication.
- For a more robust and scalable security solution you may want to implement a client server based VPN instead.

6. Bibliography

(1) **CISCO – A Primer for Implementing a Cisco Virtual Private Network**, Cisco Reference Guide, http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

(2) **CISCO – IPSec, Cisco White Paper**, http://www.cisco.com/warp/public/cc/techno/protocol/ipsecure/ipsec/tech/ipsec_wp.html

(3) **CISCO- IP VPN Frequently Asked Questions**, http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/ipvpn_qp.htm

(4) **Configuring Internet Key Exchange Security Protocol**, Cisco Documentation,http://www.cisco.com/univercd/cc/td/doc/products/software/ios121/121cgcr/secur_c/scprt4/scdi….?????? (look for the rest of the url

(5) **Configuring IPSec Network Security**, Cisco Documentation, http://www.ciscocom/univercd/cc/td/doc/products/software/ios121/121cgcr/secur_c/scprt4/scdi…????look for the rest of the url

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(6) Karn, P. et al, **The ESP DES-CBC Transform,** IETF Networking Group Request for Comments 1829, August 1995, http://www.ietf.org/rfc/rfc1829.txt.
(7) Kent, S. et al. **IP Authentication Header**, IETF Networking Group Request for Comments 2402, November 1998, http://www.ietf.org/rfc/rfc2402.txt.
(8) Kent, S. et al. **IP Encapsulating Security Payload**, IETF Networking Group Request for Comments 2406, November 1998, http://www.ietf.org/rfc/rfc2406.txt
(9) Krawczyk, H. et al, **HMAC: Keyed-Hashing for Message Authentication,** IETF Networking Group Request for Comments 2104, February 1997, http://www.ietf.org/rfc/rfc2104.txt.
(10) Stallings, William. **Cryptography and Network Security Principles and Practice**, Prentice Hall, Upper Saddle River, New Jersey, 1999.

© SANS Institute 2000 - 2002, Author retains full rights.