TheGreenBow IPSec VPN Client
Configuration Guide
Cisco PIX-506E

WebSite: http://www.thegreenbow.com
Contact: support@thegreenbow.com
Table of contents

1 Introduction .................................................................................................................................................... 3
  1.1 Goal of this document ............................................................................................................................ 3
  1.2 VPN Network topology ........................................................................................................................... 3
  1.3 Cisco PIX-506E Security Appliance ....................................................................................................... 3
  1.4 Cisco PIX-506E Security Appliance product info ................................................................................... 3

2 Cisco PIX-506E VPN configuration ................................................................................................................ 4
  2.1 Main settings .......................................................................................................................................... 4
  2.2 Main Configuration of Point-to-multiple_Point mode .............................................................................. 5

3 TheGreenBow IPSec VPN Client configuration ............................................................................................. 8
  3.1 VPN Client Phase 1 (IKE) Configuration ................................................................................................ 8
  3.2 VPN Client Phase 2 (IPSec) Configuration ............................................................................................ 9
  3.3 Open IPSec VPN tunnels ....................................................................................................................... 9

4 Tools in case of trouble ................................................................................................................................ 11
  4.1 A good network analyser: wireshark .................................................................................................... 11

5 VPN IPSec Troubleshooting ..................................................................................................... ................... 12
  5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) ................................................................. 12
  5.2 « INVALID COOKIE » error .................................................................................................................. 12
  5.3 « no keystore » error ............................................................................................................................ 12
  5.4 « received remote ID other than expected » error ................................................................................ 12
  5.5 « NO PROPOSAL CHOSEN » error .................................................................................................... 13
  5.6 « INVALID ID INFORMATION » error .................................................................................................. 13
  5.7 I clicked on “Open tunnel”, but nothing happens ................................................................................. 13
  5.8 The VPN tunnel is up but I can’t ping ! ................................................................................................. 13

6 Contacts ....................................................................................................................................................... 15
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Cisco PIX-506E Firewall.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Cisco PIX-506E firewall. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.

1.3 Cisco PIX-506E Security Appliance

Our tests and VPN configuration have been conducted with Cisco PIX-506E firmware release version 6.3(5)

1.4 Cisco PIX-506E Security Appliance product info

It is critical that users find all necessary information about Cisco PIX-506E Security Appliance. All product info, User Guide and knowledge base for the Cisco PIX-506E Security Appliance can be found on the Cisco website: www.cisco.com.

|---------------------------|------------------------------------------------------------------------|
2 Cisco PIX-506E VPN configuration

This section describes how to build an IPSec VPN configuration with your Cisco PIX-506E Firewall.

2.1 Cisco PIX-506E Main settings

Show version:
Cisco PIX Firewall Version 6.3(5)
Cisco PIX Device Manager Version 3.0(4)
Compiled on Thu 04-Aug-05 21:40 by morlee
ciscopix up 43 mins 15 secs
Hardware: PIX-506E, 32 MB RAM, CPU Pentium II 300 MHz
Flash E28F640J3 @ 0x300, 8MB
BIOS Flash AM29F400B @ 0xffffd8000, 32KB

0: ethernet0: address is 000f.f79f.ab4e, irq 10
1: ethernet1: address is 000f.f79f.ab4f, irq 11
Licensed Features:
Failover: Disabled
VPN-DES: Enabled
VPN-3DES-AES: Enabled
Maximum Physical Interfaces: 2
Maximum Interfaces: 4
Cut-through Proxy: Enabled
Guards: Enabled
URL-filtering: Enabled
Inside Hosts: Unlimited
Throughput: Unlimited
IKE peers: Unlimited
2.2 Cisco PIX-506E Main Configuration of Point-to-Multiple Point mode

PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 10baset
nameif ethernet0 outside security0
nameif ethernet1 inside security100

fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

access-list 115 permit ip 192.168.0.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list 115 deny ip 192.168.0.0 255.255.255.0 any
access-list inside permit ip any any
access-list outside permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 192.168.1.1 255.255.255.0
ip address inside 192.168.0.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 192.168.1.2 2

timeout xlate 3:00:00

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00

timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00

timeout sip-disconnect 0:02:00 sip-invite 0:03:00

timeout uauth 0:05:00 absolute

aaa-server TACACS+ protocol tacacs+

aaa-server TACACS+ max-failed-attempts 3

aaa-server TACACS+ deadtime 10

aaa-server RADIUS protocol radius

aaa-server RADIUS max-failed-attempts 3

aaa-server RADIUS deadtime 10

aaa-server LOCAL protocol local

http server enable

http 192.168.0.2 255.255.255.255 inside

no snmp-server location

no snmp-server contact

snmp-server community public

no snmp-server enable traps

floodguard enable

sysopt connection permit-ipsec

crypto ipsec transform-set myset esp-3des esp-md5-hmac

crypto dynamic-map cisco 1 set transform-set myset

crypto map dyn-map 20 ipsec-isakmp dynamic cisco

crypto map dyn-map interface outside

isakmp enable outside

isakmp key 123456 address 0.0.0.0 netmask 0.0.0.0

isakmp identity address

isakmp policy 10 authentication pre-share

isakmp policy 10 encryption 3des

isakmp policy 10 hash md5

isakmp policy 10 group 1

isakmp policy 10 lifetime 28800

telnet timeout 5

ssh timeout 5

console timeout 0
terminal width 80
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

The remote Firewall IP address is either an explicit IP address, or a DNS Name.

The phase 1 configuration dialog is shown.

Phase 1 configuration
3.2 VPN Client Phase 2 (IPSec) Configuration

You may define a static virtual IP address here. If you use 0.0.0.0, you will have error “Local-ID” is missing. It does not prevent you from establishing a tunnel.

Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

3.3 Open IPSec VPN tunnels

Once both Cisco PIX-506E firewall and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "Save & Apply" to take into account all modifications we’ve made on your VPN Client configuration

2. Click on "Open Tunnel", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)

3. Select "Connections" to see opened VPN Tunnels

4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Cisco PIX-506E Firewall.
4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website http://www.wireshark.org/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).
5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification type PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification type INVALID_COOKIE
115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 « no keystate » error

115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected support@thegreenbow.fr

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.
5.5 « NO PROPOSAL CHOSEN » error

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 « INVALID ID INFORMATION » error

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

```
5.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

5.8 The VPN tunnel is up but I can’t ping!

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
• If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
• Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
• You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
• We recommend you to install wireshark (http://www.wireshark.com) on one of your target computer. You can check that your pings arrive inside the LAN.
6 Contacts

News and updates on TheGreenBow web site: http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts by email at info@thegreenbow.com