

PIX/ASA 7.x to Support IPsec over TCP on any Port Configuration Example

Document ID: 68326

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

- Verify the PIX 7.x Configuration
- Verify the Cisco VPN 3002 Hardware Client Configuration

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document describes how to configure remote access VPN sessions between a PIX Firewall and VPN Hardware Clients. This sample configuration demonstrates a configuration for IPsec over TCP on any port. This feature is introduced in PIX version 7.x.

The **isakmp ipsec-over-tcp port** command enables the PIX to connect to a Cisco VPN Software and Hardware Client on any port for IPsec over TCP.

Refer to VPN 3002 Hardware Client to PIX 6.x Configuration Example in order to learn more about the same scenario where the PIX Security Appliance runs software version 6.x.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- The PIX Firewall needs to run code version 7.0 or later.

Components Used

The information in this document is based on these software and hardware versions:

- PIX 515 version 7.0.4
- Cisco VPN 3002 Hardware Client 4.7.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

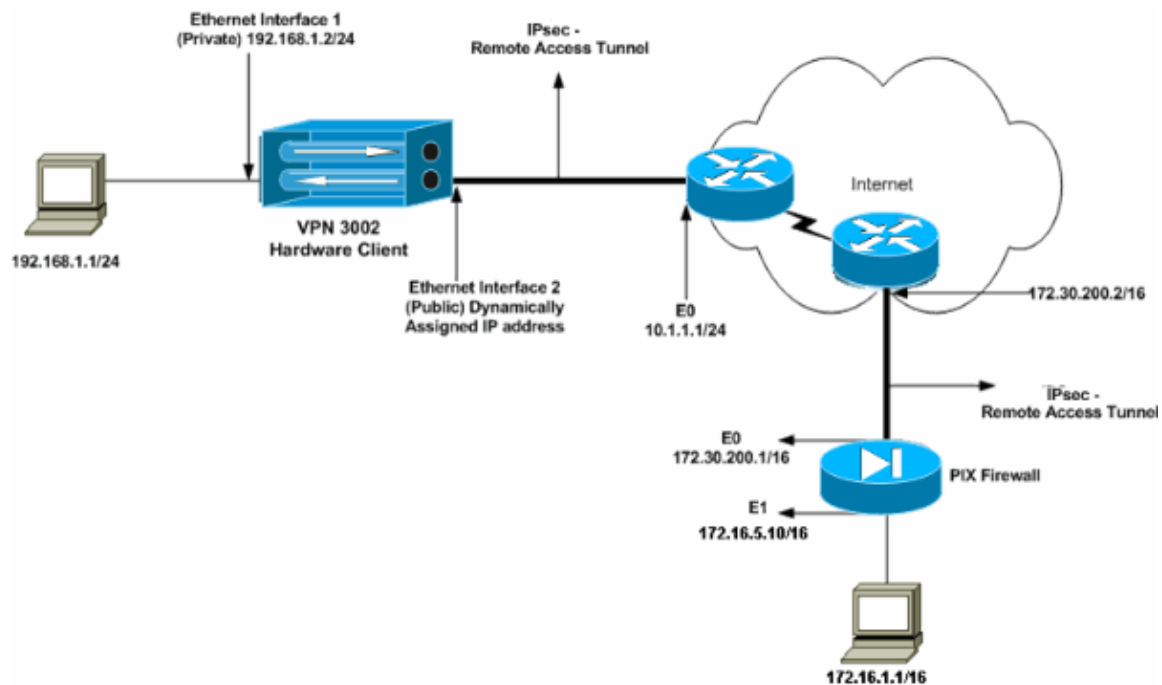
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- PIX 7.x
- Cisco VPN 3002 Hardware Client

PIX 7.x

```
PIX Version 7.0(4)
!
hostname pix
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 speed 10
 nameif outside
 security-level 0
 ip address 172.30.200.1 255.255.0.0
```

```
!  
interface Ethernet1  
  nameif inside  
  security-level 100  
  ip address 172.16.5.10 255.255.0.0  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
!  
access-list nonat extended permit ip 172.16.0.0 255.255.0.0 any  
access-list outside extended permit icmp any any  
access-list OUT extended permit ip any any  
!  
nat (inside) 0 access-list nonat  
access-group OUT in interface outside  
route outside 0.0.0.0 0.0.0.0 172.30.200.2 1  
!  
  
!--- Output is suppressed.  
  
group-policy DfltGrpPolicy attributes  
  banner none  
  wins-server none  
  dns-server none  
  dhcp-network-scope none  
  vpn-access-hours none  
  vpn-simultaneous-logins 3  
  vpn-idle-timeout 30  
  vpn-session-timeout none  
  vpn-filter none  
  vpn-tunnel-protocol IPsec  
  
!--- This specifies the VPN protocol used by this group.  
!--- The two options are IPsec and WebVPN. IPsec is configured for this example.  
  
password-storage enable  
  
!--- This allows the users to store passwords on VPN Client devices.  
!--- Password storage is disabled by default for security reasons.  
!--- Enable password storage only on systems that you know to be in secure sites.  
  
  ip-comp disable  
  re-xauth disable  
  group-lock none  
  pfs disable  
  ipsec-udp disable  
  ipsec-udp-port 10000  
  split-tunnel-policy tunnelall  
  split-tunnel-network-list none  
  default-domain none  
  split-dns none  
  secure-unit-authentication disable  
  user-authentication disable  
  user-authentication-idle-timeout 30  
  ip-phone-bypass disable  
  leap-bypass disable  
  nem enable  
  
!--- Enter the nem command with the enable keyword in  
!--- group-policy configuration mode to enable network  
!--- extension mode for hardware clients.  
!--- This is disabled by default.  
  
  backup-servers keep-client-config  
  client-firewall none  
  client-access-rule none
```

```

!--- Refer to Group Policies for more information.
!
crypto ipsec transform-set my-set esp-3des esp-md5-hmac
crypto dynamic-map dyn_outside 20 set transform-set my-set
crypto map mymap 20 ipsec-isakmp dynamic dyn_outside
crypto map mymap interface outside

!--- These are the IPsec parameters that are
!--- negotiated with the client. In this example, dynamic maps are
!--- used since the client IP address is not known.

isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400

!--- These are the Phase 1 parameters negotiated by the two peers.

isakmp ipsec-over-tcp port 10000

!--- Use the isakmp ipsec-over-tcp command
!--- in global configuration mode to enable IPsec over TCP.

tunnel-group DefaultRAGroup general-attributes

!--- A tunnel group consists of a set of records that
!--- contain tunnel connection policies. The two attributes
!--- are General and IPsec.

authentication-server-group none
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *
: end

```

Cisco VPN 3002 Hardware Client

Complete these steps:

1. Select **Configuration > Interfaces** to configure the IP address for both interfaces.


In this example the public interface has a dynamically assigned address:

Configuration | Interfaces Thursday, 19 January 2006 20:20:05
Save Refresh

This section lets you configure the VPN 3002 Hardware Client's network interfaces.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.1.2	255.255.255.0	00:05:31:A0:A6:F4	
Ethernet 2 (Public) [Renew Release]	UP/DHCP Lease expires in 23:13:18 (hh:mm:ss)	10.1.1.5	255.255.255.0	00:05:31:A0:A6:F5	10.1.1.1
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name	cisco.com				



2. Select **Configuration > System > Tunneling Protocols > IPsec** to configure the parameters relevant to the IPsec tunnel.

Make sure you select **IPsec Over TCP** and configure the same port number similar to the one configured on the PIX. This example uses port **10000**.

The Group name of the tunnel and the password is also configured in this example. This is required only in the case of pre-shared keys, this is not required if you use certificates. The Group name is **DefaultRAGroup** in this example.

The screenshot shows the configuration page for IPsec. The breadcrumb trail is "Configuration | System | Tunneling Protocols | IPsec". The main heading is "Enter the information needed to connect to the central-site VPN Concentrator server." The "Remote Easy VPN Server" field contains "172.30.200.1". The "Backup Easy VPN Servers" field is empty, with instructions: "Enter up to 10 backup server addresses/host names from high priority to low. Enter each backup server address/host name on a single line." The "Alert when disconnecting" checkbox is checked. The "IPSec over TCP" checkbox is checked, and the "IPSec over TCP Port" is "10000". The "Use Certificate" checkbox is unchecked. Under "Certificate Transmission", "Identity certificate only" is selected. The "Group" field contains "DefaultRAGroup". There are fields for "Password" and "Verify" with masked characters. "Apply" and "Cancel" buttons are at the bottom.

3. Disable PAT in order to configure the IPsec tunnel in Network Extension Mode (NEM). Select **Configuration > Policy Management > Traffic Management > PAT > Enable**.

NEM allows hardware clients to present a single, routable network to the remote private network over the VPN tunnel. IPsec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance.

The screenshot shows the configuration page for PAT. The breadcrumb trail is "Configuration | Policy Management | Traffic Management | PAT | Enable". The main heading is "Check the box to enable PAT over the tunnel. Uncheck the box to disable PAT over the tunnel (Network Extension mode)." The "PAT Enabled" checkbox is unchecked. "Apply" and "Cancel" buttons are at the bottom.

Verify

Use this section to confirm that your configuration works properly.

Verify the PIX 7.x Configuration

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa** Displays all current IKE Security Associations (SAs) at a peer. The AM_ACTIVE state denotes that Aggressive Mode was used to set up the IPsec VPN tunnel.

```

pix#show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.1.1.5
  Type      : user           Role       : responder
  Rekey     : no            State      : AM_ACTIVE

```

- **show crypto ipsec sa** Displays the settings used by current SAs. Check for the peer IP addresses, the networks accessible at both the local and remote ends, and the transform set that is used. There are two ESP SAs, one in each direction.

```

pix#show crypto ipsec sa
interface: outside
Crypto map tag: dyn_outside, seq num: 20, local addr: 172.30.200.1

local ident (addr/mask/prot/port): (172.30.200.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.1.1.5/255.255.255.255/0/0)
current_peer: 10.1.1.5, username: DefaultRAGroup
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.30.200.1/10000, remote crypto endpt.: 10.1.1.5/19
007 path mtu 1500, ipsec overhead 96, media mtu 1500
current outbound spi: 3B091B02

inbound esp sas:
spi: 0x4B73C095 (1265877141)
transform: esp-3des esp-md5-hmac
in use settings ={RA, Tunnel, TCP-Encaps, }
slot: 0, conn_id: 3, crypto-map: dyn_outside
sa timing: remaining key lifetime (sec): 28607
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0x3B091B02 (990452482)
transform: esp-3des esp-md5-hmac
in use settings ={RA, Tunnel, TCP-Encaps, }
slot: 0, conn_id: 3, crypto-map: dyn_outside
sa timing: remaining key lifetime (sec): 28605
IV size: 8 bytes
replay detection support: Y

Crypto map tag: dyn_outside, seq num: 20, local addr: 172.30.200.1

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer: 10.1.1.5, username: DefaultRAGroup
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

```

```

007      local crypto endpt.: 172.30.200.1/10000, remote crypto endpt.: 10.1.1.5/19
      path mtu 1500, ipsec overhead 96, media mtu 1500
      current outbound spi: 02E893BC

inbound esp sas:
  spi: 0x67593523 (1733899555)
    transform: esp-3des esp-md5-hmac
    in use settings = {RA, Tunnel, TCP-Encaps, }
    slot: 0, conn_id: 3, crypto-map: dyn_outside
    sa timing: remaining key lifetime (sec): 28609
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0x02E893BC (48796604)
    transform: esp-3des esp-md5-hmac
    in use settings = {RA, Tunnel, TCP-Encaps, }
    slot: 0, conn_id: 3, crypto-map: dyn_outside
    sa timing: remaining key lifetime (sec): 28609
    IV size: 8 bytes
    replay detection support: Y

```

- **show crypto isakmp ipsec-over-tcp stat** Use this command to check the IPsec over TCP parameters.

```

pix#show crypto isakmp ipsec-over-tcp stat

```

```

Global IPsec over TCP Statistics
-----
Embryonic connections: 0
Active connections: 1
Previous connections: 80
Inbound packets: 803
Inbound dropped packets: 0
Outbound packets: 540
Outbound dropped packets: 0
RST packets: 87
Received ACK heart-beat packets: 7
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0

```

Verify the Cisco VPN 3002 Hardware Client Configuration

Select **Monitoring > Statistics > IPsec** to verify if the tunnel has come up in the Cisco VPN 3002 Hardware Client. This window shows the statistics for both IKE and IPsec parameters:

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	1	Active Tunnels	2
Total Tunnels	10	Total Tunnels	20
Received Bytes	43676	Received Bytes	144176
Sent Bytes	128624	Sent Bytes	130448
Received Packets	227	Received Packets	813
Sent Packets	324	Sent Packets	1038
Received Packets Dropped	0	Received Packets Dropped	0
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notices	117	Sent Packets Dropped	0
Sent Notices	50	Inbound Authentications	813
Received Phase-2 Exchanges	0	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	20	Outbound Authentications	1038
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	813
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	1038
Phase-2 SA Delete Requests Received	12	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	6	System Capability Failures	0
Initiated Tunnels	620	No-SA Failures	0
Failed Initiated Tunnels	535	Protocol Use Failures	0
Failed Remote Tunnels	0		
Authentication Failures	0		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability Failures	0		
No-SA Failures	0		

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

The **debug** commands on PIX for VPN tunnels:

- **debug crypto isakmp sa** Debugs ISAKMP SA negotiations.
- **debug crypto ipsec sa** Debugs IPsec SA negotiations.

Related Information

- [Cisco VPN 3002 Hardware Client Support Page](#)
 - [Cisco PIX Firewall Software](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

