Table of Contents

PIX 7.x/ASA and VPN Client for Public Internet VPN on a Stick Configuration Example

Document ID: 67986

Introduction

This document describes how to set up a PIX 7.0.1 and later firewall to perform IPsec on a stick. This setup applies to a specific case where the PIX does not allow split tunneling, and users connect directly to the PIX before they are permitted to go to the Internet.

Prerequisites

Requirements

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

- The hub PIX Security Appliance needs to run version 7.0.1 or later
- Cisco VPN Client version 4.x

Components Used

The information in this document is based on the PIX or ASA security appliance version 7.0.1.

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.

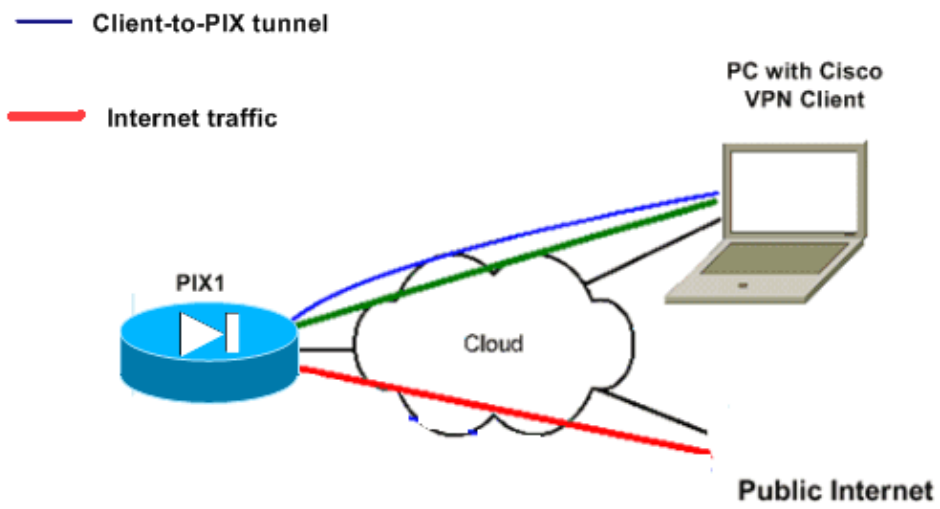
Configure

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/ASA
- VPN Client

PIX/ASA

```
PIX Version 7.0(1)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet2
shutdown
```

```
no nameif
no security−level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security−level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security−level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security−level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname W2N−5.6−PIX515−A
ftp mode passive

!−−− Command that permits IPsec traffic to enter and exit the same interface.

same−security−traffic permit intra−interface
access−list 100 extended permit icmp any any echo−reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500

!−−− The address pool for the VPN Clients.

ip local pool vpnpool 192.168.10.1−192.168.10.254

no failover
monitor−interface outside
monitor−interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat−control


!−−− The global address for Internet access used by VPN Clients.
!−−− Note: Uses an RFC 1918 range for lab setup.
!−−− Apply an address from your public range provided by your ISP.


global (outside) 1 172.18.124.166


!−−− The NAT statement to define what to encrypt (the addresses from the vpn−pool).


nat (outside) 1 192.168.10.0 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0
```

```
static (inside,outside) 10.10.10.2 10.10.10.2 netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute


!--- The configuration of group-policy for VPN Clients.


group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20


!--- Forces VPN Clients over the tunnel for Internet access.


split-tunnel-policy tunnelall


no snmp-server location
no snmp-server contact
snmp-server enable traps snmp


!--- Configuration of IPsec Phase 2.


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


!--- Crypto map configuration for VPN Clients that connect to this PIX.


crypto dynamic-map rtpdynmap 20 set transform-set myset


!--- Binds the dynamic map to the crypto map process.


crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap


!--- Crypto map applied to the outside interface.


crypto map mymap interface outside


!--- Enable ISAKMP on the outside interface.


isakmp identity address
isakmp enable outside


!--- Configuration of ISAKMP policy.


isakmp policy 10 authentication pre-share
```

```
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0


!--- Configuration of tunnel-group with group information for VPN Clients.


tunnel-group rtptacvpn type ipsec-ra


!--- Configuration of group parameters for the VPN Clients.


tunnel-group rtptacvpn general-attributes
address-pool vpnpool


!--- Disable user authentication.


authentication-server-group none
authorization-server-group LOCAL


!--- Bind group-policy parameters to the tunnel-group for VPN Clients.


default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp

 inspect sip
 inspect xdmcp
!
service-policy global_policy global
```

```
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

Note 1: The **sysopt connection permit−ipsec** command needs to be configured. The **show running−config sysopt** command verifies if it is configured.

Note 2: Add this output for the optional UDP transport:

```
group−policy clientgroup attributes
vpn−idle−timeout 20
ipsec−udp enable
ipsec−udp−port 10000
split−tunnel−policy tunnelspecified
split−tunnel−network−list value splittunnel
```

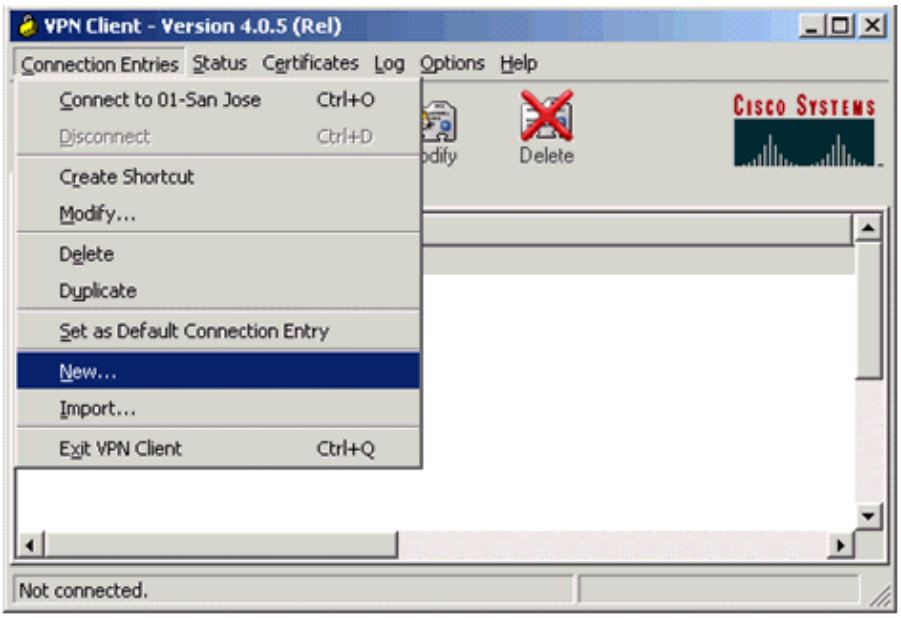
Note 3: Configure this command in the global configuration of the PIX appliance in order for VPN Clients to connect via IPsec over TCP:

```
isakmp ipsec−over−tcp port 10000
```

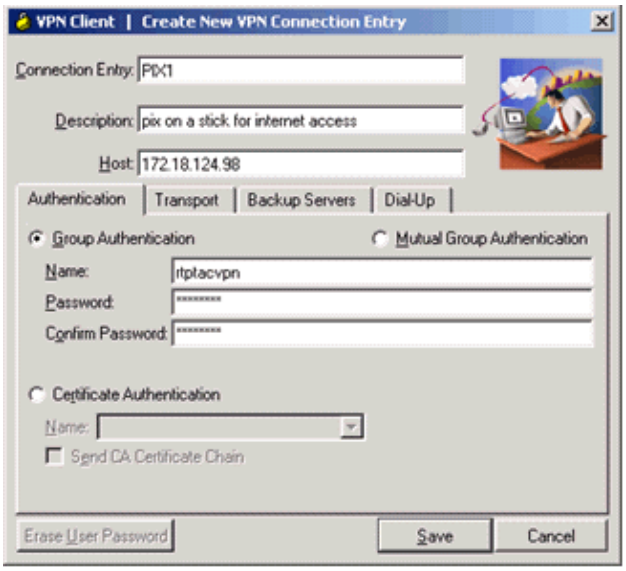
VPN Client

Complete these steps to configure the VPN Client:

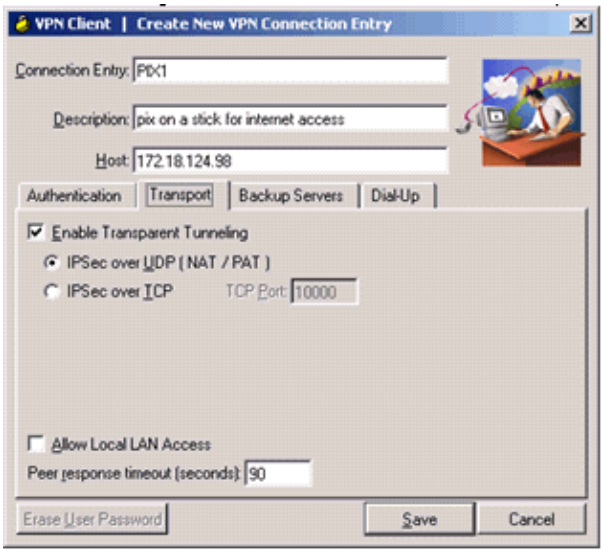
1. Select **Connection Entries** > **New**.



2. Enter the PIX and group information.



3. (*Optional*) Click **Enable Transparent Tunneling** under the Transport tab. (This is optional and requires the additional PIX/ASA configuration mentioned in note 2.)



4. Save the profile.

Verify

Use this section to confirm that your configuration works properly.

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.
- **show crypto ipsec sa** Displays all current SAs. Look for encrypt and decrypt packets on the SA that define the VPN Client traffic.

Attempt to ping or browse to a public IP address from the client such as www.cisco.com.

VPN Client Verification

Complete these steps to verify the VPN Client.

1. Right−click on the VPN Client lock icon present at the system tray after a successful connection and choose the option for **statistics** to view encrypts and decrypts.
2. Click on the Route Details tab in order to verify the no split−tunnel list passed down from the appliance.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- **Enhanced Spoke−to−Client VPN Configuration Example for PIX Security Appliance Version 7.0**
- **Cisco VPN Client**
- **IPsec Negotiation/IKE Protocols**
- **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**

Updated: Nov 28, 2005 Document ID: 67986