

Configuring IKE Pre-Shared Keys Using a RADIUS Server for the Cisco Secure VPN Client

Document ID: 5726

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Creating a Cisco Secure Profile
- Configuring the Router
- Configuring the Client

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure Internet Key Exchange (IKE) shared secret using a RADIUS server. The IKE shared secret feature that uses an authentication, authorization, and accounting (AAA) server enables key lookup from the AAA server. Pre-shared keys do not scale well when you deploy a large-scale VPN system without a certification authority (CA). When using dynamic IP addressing such as Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP) dial-ups, the changing IP address can make key lookup difficult or impossible unless a wildcard pre-shared key is used. In the IKE shared secret feature that uses an AAA server, the shared secret is accessed during the aggressive mode of IKE negotiation through the AAA server. The ID of the exchange is used as the user name to query AAA if no local key can be found on the Cisco IOS® router to which the user is trying to connect. This was introduced in Cisco IOS Software Release 12.1.T. You must have aggressive mode enabled on the VPN Client to use this feature.

Prerequisites

Requirements

You must have aggressive mode enabled on the VPN Client, and you must be running Cisco IOS Software Release 12.1.T or later on the router.

Components Used

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

- Cisco Secure ACS for Windows
- Cisco IOS Software Release 12.2.8T
- Cisco 1700 Router

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live

network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configure

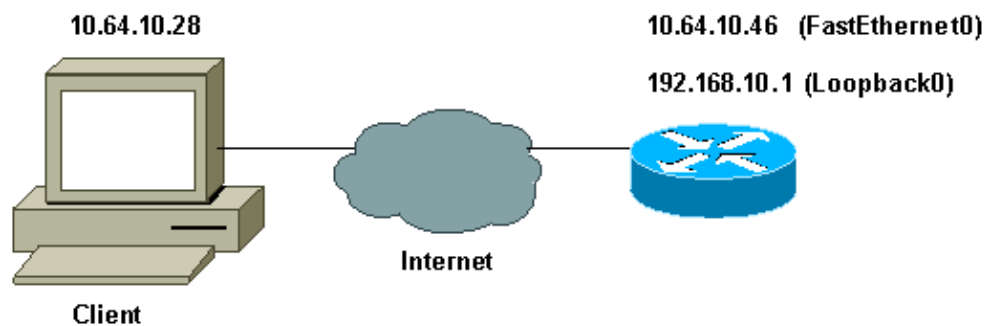
This document uses the configurations shown below.

- Creating a Cisco Secure Profile
- Configuring the Router
- Configuring the Client

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:



Creating a Cisco Secure Profile

This profile was created with UNIX, but a similar profile can be created on Cisco Secure ACS for Windows.

```
# ./ViewProfile -p 9900 -u haseeb
User Profile Information

!--- The user name is sent by the VPN Client;
!--- look at the client configuration.

user = haseeb{

radius=Cisco12.05 {
check_items= {

!--- This should always be "cisco."

2=cisco
}
reply_attributes= {
6=5
64=9
65=1

!--- Pre-shared key.
```

```

9,1="ipsec:tunnel-password=secret12345"
9,1="ipsec:key-exchange=ike"
}
}
}

```

This output shows the script that is used to add a user profile in Cisco Secure ACS for UNIX.

```

#!/bin/sh
./DeleteProfile -p 9900 -u haseeb
./AddProfile -p 9900 -u haseeb -a 'radius=Cisco12.05
{ \n check_items = { \n 2="cisco" \n } \n
reply_attributes = { \n 6=5 \n 64=9 \n 65=1 \n
9,1="ipsec:tunnel-password=cisco" \n
9,1="ipsec:key-exchange=ike" \n } \n }'

```

Follow these steps to use the GUI to configure the user profile on Cisco Secure ACS for Windows 2.6.

1. Define the user name, with "cisco" as the password.

The screenshot shows the 'Edit' window for a user named 'haseeb'. It includes a checkbox for 'Account Disabled' which is unchecked. Below this is the 'Supplementary User Info' section with fields for 'Real Name' (filled with 'hasseb') and 'Description' (filled with 'vpn user'). The 'User Setup' section is expanded, showing 'Password Authentication' set to 'CiscoSecure Database'. A note indicates 'CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)'. There are fields for 'Password' and 'Confirm Password', both containing masked characters.

2. Define the key exchange as IKE and pre-shared key under the Cisco av-pair.

The screenshot shows the 'Cisco IOS/PIX RADIUS Attributes' configuration window. A checkbox is checked next to '[009\001] cisco-av-pair'. Below this, a text area contains the following configuration script:

```

ipsec:tunnel-
password=secret12345
ipsec:key-exchange=ike

```

Configuring the Router

Cisco 1751 with IOS 12.2.8T

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1751-vpn
!
!---
Enable AAA.

aaa new-model
!
!
aaa authentication login default none

!--- Configure authorization.

aaa authorization network vpn_users group radius
aaa session-id common
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!

!--- Define IKE policy for phase 1 negotiations of the VPN Clients.

crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp client configuration address-pool local mypool
!

!--- Define IPsec policies - Phase 2 Policy for actual data encryption.

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

!--- Create dynamic crypto map.

crypto dynamic-map dynmap 10
  set transform-set myset
!

!--- Configure IKE shared secret using AAA server on this router.

crypto map intmap isakmp authorization list vpn_users

!--- IKE Mode Configuration - the router will attempt
!--- to set IP addresses for each peer.

crypto map intmap client configuration address initiate

!--- IKE Mode Configuration - the router will accept
!--- requests for IP addresses from any requesting peer.
```

```

crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
interface Loopback1
 no ip address
!
interface Ethernet0/0
 no ip address
 half-duplex
!
interface FastEthernet0/0
 ip address 10.64.10.46 255.255.255.224
 speed auto

!--- Assign crypto map to interface.

crypto map intmap
!

!--- Configure a local pool of IP addresses to be used when a
!--- remote peer connects to a point-to-point interface.

ip local pool mypool 10.1.2.1 10.1.2.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
no ip http server
ip pim bidir-enable
!

!--- Specify the security server protocol and defines security
!--- server host IP address and UDP port number.

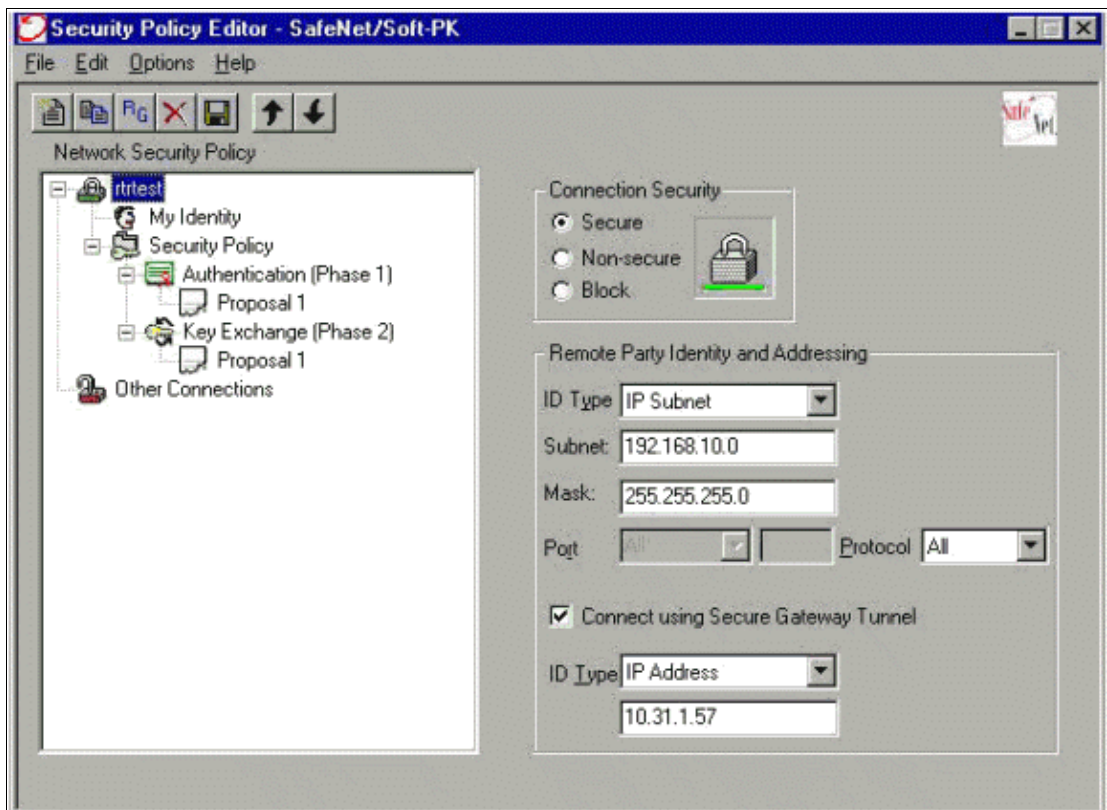
radius-server host 10.64.10.7 auth-port 1645 acct-port 1646 key cisco123
radius-server retransmit 3
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end

```

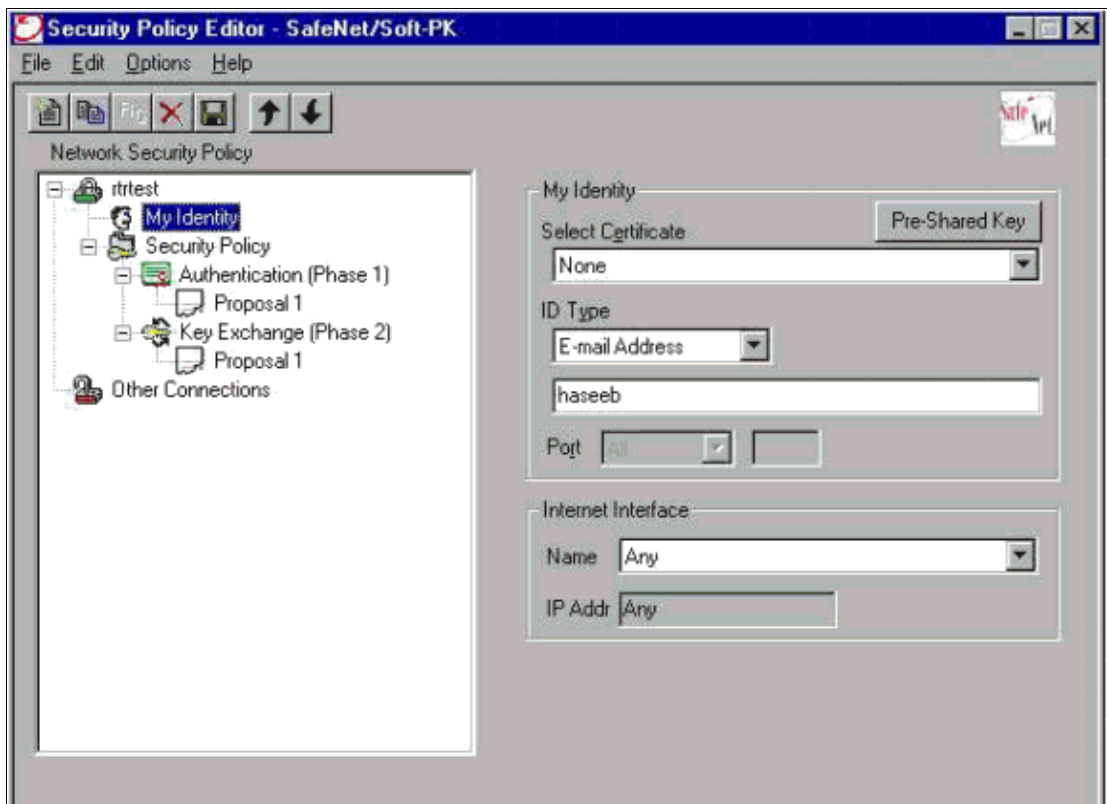
Configuring the Client

Follow these steps to configure the client.

1. In the Security Policy Editor, go to **Network Security Policy > rtrtest**. Select the **ID Type** as an e-mail address and put in a user name to be configured on the RADIUS server. If this setting is left as "IP Address," then the user name sent to the RADIUS server would be the IP address of the client PC.



2. Go to **Network Security Policy > rtrtest > My Identity** and select **Aggressive Mode**. The setup will not work if this mode is not selected.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

This output shows good debugs for this configuration:

```
23:43:41: ISAKMP (0:0): received packet from 10.64.10.28 (N) NEW SA
23:43:41: ISAKMP: local port 500, remote port 500
23:43:41: ISAKMP: Locking CONFIG struct 0x8180BEF4 from
        crypto_ikmp_config_initialize_sa, count 2
23:43:41: ISAKMP (0:3): processing SA payload. message ID = 0
23:43:41: ISAKMP (0:3): processing ID payload. message ID = 0
23:43:41: ISAKMP (0:3): processing vendor id payload
23:43:41: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
23:43:41: ISAKMP (0:3): vendor ID is XAUTH
23:43:41: ISAKMP (0:3): Checking ISAKMP transform 1 against priority 10 policy
23:43:41: ISAKMP:      encryption DES-CBC
23:43:41: ISAKMP:      hash MD5
23:43:41: ISAKMP:      default group 1
23:43:41: ISAKMP:      auth pre-share

!--- ISAKMP policy proposed by VPN Client
!--- matched the configured ISAKMP policy.

23:43:41: ISAKMP (0:3): atts are acceptable. Next payload is 0
23:43:41: ISAKMP (0:3): processing KE payload. message ID = 0
23:43:41: ISAKMP (0:3): processing NONCE payload. message ID = 0
23:43:41: ISAKMP (0:3): SKEYID state generated
23:43:41: ISAKMP (0:3): processing vendor id payload
23:43:41: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
23:43:41: ISAKMP (0:3): vendor ID is XAUTH
23:43:41: ISAKMP (0:3): SA is doing pre-shared key authentication
        using id type ID_IPV4_ADDR
23:43:41: ISAKMP (3): ID payload
        next-payload : 10
        type          : 1
        protocol      : 17
        port          : 500
        length        : 8

23:43:41: ISAKMP (3): Total payload length: 12
23:43:41: ISAKMP (0:3): sending packet to 10.64.10.28 (R) AG_INIT_EXCH
23:43:41: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_READY New State = IKE_R_AM2
23:43:42: ISAKMP (0:3): received packet from 10.64.10.28 (R) AG_INIT_EXCH
23:43:42: ISAKMP (0:3): processing HASH payload. message ID = 0
23:43:42: ISAKMP (0:3): SA has been authenticated with 10.64.10.28
23:43:42: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_R_AM2 New State = IKE_P1_COMPLETE
23:43:43: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:43: ISAKMP (0:3): Need config/address
23:43:43: ISAKMP (0:3): Need config/address
23:43:43: ISAKMP: Sending private address: 10.1.2.2
23:43:43: ISAKMP (0:3): initiating peer config to 10.64.10.28.
        ID = -1082015193
23:43:43: ISAKMP (0:3): sending packet to 10.64.10.28 (R) CONF_ADDR
23:43:43: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_SET_SENT
23:43:43: ISAKMP (0:3): received packet from 10.64.10.28 (R) CONF_ADDR
23:43:43: ISAKMP (0:3): processing transaction payload from 10.64.10.28.
        message ID = -1082015193
23:43:43: ISAKMP: Config payload ACK
23:43:43: ISAKMP (0:3): peer accepted the address!
23:43:43: ISAKMP (0:3): deleting node -1082015193 error FALSE
```

```
reason "done with transaction"
23:43:43: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK
Old State = IKE_CONFIG_MODE_SET_SENT New State = IKE_P1_COMPLETE
23:43:43: ISAKMP (0:3): Delaying response to QM request.
23:43:43: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
23:43:44: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:44: ISAKMP (0:3): processing HASH payload. message ID = -920829332
23:43:44: ISAKMP (0:3): processing SA payload. message ID = -920829332
23:43:44: ISAKMP (0:3): Checking IPsec proposal 1
23:43:44: ISAKMP: transform 1, ESP_DES
23:43:44: ISAKMP: attributes in transform:
23:43:44: ISAKMP: authenticator is HMAC-MD5
23:43:44: ISAKMP: encaps is 1

!--- Proposed Phase 2 transform set
!--- matched configured IPsec transform set.

23:43:44: ISAKMP (0:3): atts are acceptable.
23:43:44: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28,
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
23:43:44: ISAKMP (0:3): processing NONCE payload. message ID = -920829332
23:43:44: ISAKMP (0:3): processing ID payload. message ID = -920829332
23:43:44: ISAKMP (0:3): processing ID payload. message ID = -920829332
23:43:44: ISAKMP (0:3): asking for 1 spis from ipsec
23:43:44: ISAKMP (0:3): Node -920829332,
Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
23:43:44: IPSEC(key_engine): got a queue event...
23:43:44: IPSEC(spi_response): getting spi 2940839732 for SA
from 10.64.10.46 to 10.64.10.28 for prot 3
23:43:44: ISAKMP: received ke message (2/1)
23:43:45: ISAKMP (0:3): sending packet to 10.64.10.28 (R) QM_IDLE
23:43:45: ISAKMP (0:3): Node -920829332,
Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
23:43:45: ISAKMP (0:3): received packet from 10.64.10.28 (R) QM_IDLE
23:43:45: ISAKMP (0:3): Creating IPsec SAs
23:43:45: inbound SA from 10.64.10.28 to 10.64.10.46
(proxy 10.1.2.2 to 192.168.10.0)
23:43:45: has spi 0xAF49A734 and conn_id 200 and flags 4
23:43:45: outbound SA from 10.64.10.46 to 10.64.10.28
(proxy 192.168.10.0 to 10.1.2.2 )
23:43:45: has spi 1531785085 and conn_id 201 and flags C
23:43:45: ISAKMP (0:3): deleting node 1961959105 error FALSE
reason "saved qm no longer needed"
23:43:45: ISAKMP (0:3): deleting node -920829332 error FALSE
reason "quick mode done (await())"
23:43:45: ISAKMP (0:3): Node -920829332,
Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
23:43:45: IPSEC(key_engine): got a queue event...
23:43:45: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 10.64.10.46, remote= 10.64.10.28,
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xAF49A734(2940839732), conn_id= 200, keysize= 0, flags= 0x4
23:43:45: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 10.64.10.46, remote= 10.64.10.28,
```




```
local_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
remote_proxy= 10.1.2.2/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x5B4D2F7D(1531785085), conn_id= 201, keysize= 0, flags= 0xC
```

!--- IPsec SAs created.

```
23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.46,
      sa_prot= 50, sa_spi= 0xAF49A734(2940839732),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 200
23:43:45: IPSEC(create_sa): sa created, (sa) sa_dest= 10.64.10.28,
      sa_prot= 50, sa_spi= 0x5B4D2F7D(1531785085),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201
23:43:45: ISAKMP: received ke message (4/1)
23:43:45: ISAKMP: Locking CONFIG struct 0x8180BEF4
      for crypto_ikmp_config_handle_kei_mess, count 3
23:43:50: ISAKMP (0:2): purging node 618568216
23:43:50: ISAKMP (0:2): purging node -497663485
23:44:00: ISAKMP (0:2): purging SA., sa=816B5724, delme=816B5724
23:44:00: ISAKMP: Unlocking CONFIG struct 0x8180BEF4 on
      return of attributes, count 2
```

Related Information

- [RADIUS Support Page](#)
- [RADIUS in IOS Documentation](#)
- [Cisco Secure ACS for Windows Support Page](#)
- [Documentation for Cisco Secure ACS for Windows](#)
- [Cisco Secure ACS for UNIX Support Page](#)
- [Documentation for Cisco Secure ACS for UNIX](#)
- [IPsec Support Page](#)
- [Requests for Comments \(RFCs\)](#) 
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 14, 2009

Document ID: 5726
