Quick Note 060

Configure a TransPort router as an EZVPN Client (XAUTH and MODECFG) to a Cisco Router running IOS 15.x

17 August 2017
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.2</td>
<td>Cisco EasyVPN</td>
<td>3</td>
</tr>
<tr>
<td>1.3</td>
<td>XAUTH</td>
<td>4</td>
</tr>
<tr>
<td>1.4</td>
<td>MODECFG</td>
<td>4</td>
</tr>
<tr>
<td>1.5</td>
<td>Network Diagram</td>
<td>4</td>
</tr>
<tr>
<td>1.6</td>
<td>Outline</td>
<td>5</td>
</tr>
<tr>
<td>1.7</td>
<td>Assumptions</td>
<td>5</td>
</tr>
<tr>
<td>1.8</td>
<td>Corrections</td>
<td>5</td>
</tr>
<tr>
<td>1.9</td>
<td>Version</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>TransPort Configuration</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>Local Ethernet Interface Configuration</td>
<td>6</td>
</tr>
<tr>
<td>2.2</td>
<td>WAN interface configuration</td>
<td>7</td>
</tr>
<tr>
<td>2.3</td>
<td>Tunnel Configuration</td>
<td>8</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Phase 1 Settings</td>
<td>8</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Phase 2 settings</td>
<td>9</td>
</tr>
<tr>
<td>2.4</td>
<td>Configure users</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Cisco 1841 Configuration</td>
<td>13</td>
</tr>
<tr>
<td>3.1</td>
<td>Cisco 1841 Configuration</td>
<td>13</td>
</tr>
<tr>
<td>3.2</td>
<td>Configure basic routing</td>
<td>13</td>
</tr>
<tr>
<td>3.3</td>
<td>Configure IKE/ISAKMP</td>
<td>14</td>
</tr>
<tr>
<td>3.4</td>
<td>Configure IPsec</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>Testing</td>
<td>15</td>
</tr>
<tr>
<td>4.1</td>
<td>Tunnel Status</td>
<td>15</td>
</tr>
<tr>
<td>4.2</td>
<td>Ping test</td>
<td>17</td>
</tr>
<tr>
<td>4.2.1</td>
<td>TransPort</td>
<td>17</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Cisco</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>Configuration Files</td>
<td>18</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Introduction

The use of XAUTH and MODECFG with IPsec is not part of the standard IPsec implementation as published in the RFCs. There were some internet drafts which have now expired. However, many vendors including Cisco have chosen to implement XAUTH and MODECFG.

1.2 Cisco EasyVPN

Cisco solutions using EasyVPN (also known as EzVPN) and also the Cisco software “VPN Client” make use of XAUTH and MODECFG. XAUTH and MODECFG are supported in TransPort firmware, and have been tested with the Cisco 1841 running IOS version 15.1. It is therefore possible to configure the TransPort to connect to Cisco 1841 using XAUTH and MODECFG, in a similar manner to the Cisco VPN Client.

The configuration suggested in this Application Note should also work on Cisco Routers running IOS version 15.x without modification.

It may also be possible to connect to other Cisco models and software versions, however testing all hardware and software variants is not possible.

For various reasons, it can be difficult to configure a Cisco VPN server (such as the Cisco 1841) to perform EasyVPN with the Cisco software VPN Client (i.e. to perform XAUTH and MODECFG) and to also perform “standard” IPsec with a non-Cisco device. To create a standard IPsec tunnel (i.e. not using XAUTH and MODECFG) between a Cisco and non-Cisco device, the restrictions seem to be that fixed IP addresses or certificate-based authentication must be used for the non-Cisco device. This is not always practical. For this reason, support for XAUTH and MODECFG is included in TransPort firmware.

EasyVPN supports two modes of operation: Client mode and Network Extension mode.

In Client mode, all traffic from the client side uses a single IP address for all hosts on the private network. This single IP address is assigned by the Cisco EasyVPN server as an attribute using MODECFG. All traffic that goes through the IPsec tunnel, regardless of which host on the client’s network it originated from, is translated by the client using NAT so that the source address seen by the EasyVPN server is the single IP address that it assigned to the client and that it therefore expects to see.

Network Extension mode allows the client to present a full, routable network to the tunnelled (i.e. Cisco side) network. There are actually two sub-modes within Network Extension mode: NEM and NEM+. TransPort firmware currently supports Client mode and NEM mode, but not NEM+.

This application note will show only the steps required to set up Client mode connections.
1.3 XAUTH

XAUTH (IKE Extended Authentication) is an extra authentication process that occurs in between phase 1 and phase 2 of IPsec. It provides an additional level of authentication by allowing the IPsec gateway (i.e. VPN responder or server) to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN.

XAUTH essentially functions by firstly forming an IKE phase 1 SA using conventional IKE, then by extending the IKE exchange to include additional user authentication exchanges.

This means that a single pre-shared key can be used for many remote VPN users, but each user can have their own username and password for XAUTH. The head-end unit can be configured to authorise the username and password against a local table, or against an external device using for example RADIUS or TACACS.

1.4 MODECFG

MODECFG allows configuration information to be assigned by the IPsec server to the client. For EasyVPN Client mode as described in this application note, MODECFG is essentially used by the EasyVPN server (Cisco 1841) to assign a single IP address to the client (TransPort WR21) which must be used as the source address for all traffic traversing the IPsec tunnel from the client side.

1.5 Network Diagram
1.6 Outline

This guide details the steps involved in configuring a Digi TransPort as an Easy VPN client to a Cisco 1841 running IOS 15.x (configuration may differ on older versions). The document will assume that WAN connectivity is configured and available on both units. In this example, the TransPort will use 0.0.0.0/0.0.0.0 for the Remote LAN configuration. All traffic will be sent through the tunnel.

1.7 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and configure it with basic routing functions.

This application note applies to:

- **Model**: Digi TransPort WR11/21/31/41/44
- **Model**: Cisco 1841
- **Firmware versions**:
  - **WR44**: 5.2.17.10 and later
  - **Cisco**: 15.1 and later

**Configuration**: This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

**Please note**: This application note has been specifically rewritten for the specified firmware versions and later but will work on earlier versions of firmware. Please contact tech.support@digi.com if you require assistance in upgrading the firmware of the TransPort WR routers.

1.8 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com Requests for new application notes can be sent to the same address.

1.9 Version

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Completed 14.08.2017</td>
</tr>
</tbody>
</table>
2 TRANSPORT CONFIGURATION

2.1 Local Ethernet Interface Configuration

Navigate to Configuration – Network > Interfaces > Ethernet > Ethernet 0

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the following settings</td>
<td>Checked</td>
<td>A static IP Address will be used in this example</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.10.1</td>
<td>IP Address of the TransPort WR21 Ethernet Interface. In this example, this IP Address is in the subnet range used for the Tunnel (useful for testing)</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Subnet mask</td>
</tr>
</tbody>
</table>
2.2 **WAN interface configuration**

In this example, the mobile interface will be used as the WAN interface on which the IPsec tunnel will be established.

Navigate to:

**Configuration – Network > Interfaces > Mobile**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Plan / APN</td>
<td>Your.APN.goes.here</td>
<td>Enter the APN of your mobile provider</td>
</tr>
<tr>
<td>Enable IPsec on this interface</td>
<td>Checked</td>
<td>Enable IPsec to be built on this WAN interface</td>
</tr>
</tbody>
</table>

**Please note:** If required, enter a SIM PIN and Username/Password for this SIM card and APN.
2.3 Tunnel Configuration

Open a web browser to the IP address of the TransPort WR21 router.

2.3.1 Phase 1 Settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IKE > IKE 0

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>DES</td>
<td>Encryption algorithm used in this tunnel</td>
</tr>
<tr>
<td>Authentication</td>
<td>SHA1</td>
<td>Authentication algorithm used in this tunnel</td>
</tr>
<tr>
<td>Mode</td>
<td>Aggressive</td>
<td>IKE Mode used in this tunnel</td>
</tr>
<tr>
<td>MODP Group for Phase 1</td>
<td>2 (1024)</td>
<td>Key length used in the IKE Diffie-Hellman exchange</td>
</tr>
<tr>
<td>MODP Group for Phase 2</td>
<td>No PFS</td>
<td>Key length used in the ESP Diffie-Hellman exchange</td>
</tr>
</tbody>
</table>
2.3.2 Phase 2 settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec 0 – 9 > IPsec 0

Virtual Private Networking (VPN)
- IPsec
- IPsec Tunnels
- IPsec 0

Description: 

The IP address or hostname of the remote unit 1.2.3.4
Use: 
as a backup unit

Local LAN
- Use these settings for the local LAN
  IP Address: 192.168.10.0
  Mask: 255.255.255.0
- Use interface PPP

Remote LAN
- Use these settings for the remote LAN
  IP Address: 0.0.0.0
  Mask: 0.0.0.0
- Remote Subnet ID:

Use the following security on this tunnel
- Off
- Preshared Keys
- XAUTH Init Preshared Keys
- RSA Signatures
- XAUTH Init RSA

Our ID: Client3G
Our ID type: IKE ID
FQDN: User FQDN
IPv4 Address:
Remote ID: 1.2.3.4

Use DES encryption on this tunnel
Use SHA1 authentication on this tunnel
Use Diffie Hellman group No PFS

Use IKE v1 to negotiate this tunnel
Use IKE configuration:

Bring this tunnel up
- All the time
- Whenever a route to the destination is available
- On demand

If the tunnel is down and a packet is ready to be sent: Bring the tunnel up

Bring this tunnel down if it is idle for: 0 hrs 0 mins 0 secs
Renew the tunnel after: 0 hrs 0 mins 0 secs
0 KBytes of traffic

Tunnel Negotiation
- Advanced
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or hostname of the remote unit</td>
<td>1.2.3.4</td>
<td>WAN IP Address of the Cisco 1841</td>
</tr>
<tr>
<td>Local LAN settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use these settings for the local LAN</td>
<td>Checked</td>
<td>Local LAN subnet</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.10.0</td>
<td>Local LAN subnet IP Address</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Local LAN subnet mask</td>
</tr>
<tr>
<td>Remote LAN settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use these settings for the local LAN</td>
<td>Checked</td>
<td>Remote LAN subnet</td>
</tr>
<tr>
<td>IP Address</td>
<td>0.0.0.0</td>
<td>Remote LAN subnet IP Address</td>
</tr>
<tr>
<td>Mask</td>
<td>0.0.0.0</td>
<td>Remote LAN subnet mask</td>
</tr>
<tr>
<td>Tunnel Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XAUTH Init Preshared Keys</td>
<td>Checked</td>
<td>Use XAUTH Init preshared keys for authentication on this tunnel</td>
</tr>
<tr>
<td>Our ID</td>
<td>client3G</td>
<td>The ID of the VPN initiator router (this router)</td>
</tr>
<tr>
<td>Remote ID</td>
<td>1.2.3.4</td>
<td>The ID of the VPN responder router (remote router)</td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Use IKE ID type ID</td>
</tr>
<tr>
<td>Use () encryption on this tunnel</td>
<td>DES</td>
<td>The IPsec encryption algorithm to use is DES</td>
</tr>
<tr>
<td>Use () authentication on this tunnel</td>
<td>SHA1</td>
<td>The IPsec ESP authentication to use is SHA1</td>
</tr>
<tr>
<td>Tunnel creation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>On demand</td>
<td></td>
</tr>
<tr>
<td>If the tunnel is down and a packet is ready to be sent</td>
<td>Bring the tunnel up</td>
<td></td>
</tr>
</tbody>
</table>

Click **Apply**
Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec 0 – 9 > IPsec 0 > Tunnel Negotiation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XAuth ID</td>
<td>xauthclient</td>
<td>XAuth username</td>
</tr>
</tbody>
</table>

Click **Apply**

### 2.4 Configure users

Navigate to Configuration - Security > Users > User 0-9 > User 8

Here the pre-shared key is configured using the hostname or IP address of the Cisco. The username value should therefore match the Peer ID set in the IPsec configuration above:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>1.2.3.4</td>
<td>Enter the IP Address of the Cisco (WAN)</td>
</tr>
<tr>
<td>Password</td>
<td>digidigi</td>
<td>Enter the vpn_group password</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>As this user is only for the pre-shared key, no access will be granted to the router for this username</td>
</tr>
</tbody>
</table>
Navigate to **Configuration - Security > Users > User 0-9 > User 9**

This is where the VPN user password is stored. The username for this user has to match the XAUTH ID in the IPsec configuration above:

![User 9 - xauthclient](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>xauthclient</td>
<td>Enter the XAUTH username which must be the same as the XAUTH ID configured in the IPsec tunnel instance</td>
</tr>
<tr>
<td>Password</td>
<td>digixauth</td>
<td>Enter XAUTH password</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>As this user is only for the group, no access will be granted to the router for this username</td>
</tr>
</tbody>
</table>

Click **Apply**

**Save** configuration
3  CISCO 1841 CONFIGURATION

3.1  Cisco 1841 Configuration

The following will assume that the Cisco is a model 1841 running firmware version 15.1, that it is not currently in service and that it has been reset to factory defaults.

**Do not proceed with a reset if the 1841 is in service.** Normal precautions should be taken, for example backing up existing configuration.


Some of the commands that are shown grouped together below must be entered in the exact sequence indicated, therefore it is recommended to enter the commands in the order in which they appear below.

3.2  Configure basic routing

Configure the WAN interface

```plaintext
interface FastEthernet0/0
no shut
ip address 1.2.3.4 255.255.255.248
duplex auto
speed auto
```

Configure the LAN interface

```plaintext
interface FastEthernet0/1
ip address 10.1.1.254 255.255.255.0
duplex auto
speed auto
```

Configure the default route, which in this example points to an ADSL Router via the WAN interface

```plaintext
ip route 0.0.0.0 0.0.0.0 62.11.22.33
```

Configure authentication

```plaintext
aaa new-model
aaa authentication login userauthen local
aaa authorization network groupauth local
aaa session-id common
```

Configure the XAUTH username and PASSWORD:

```plaintext
username xauthclient password 0 digixauth
```
3.3 Configure IKE/ISAKMP

Configure an IKE policy. The following parameters should all match the respective parameters in the TransPort configuration. The policy [priority] uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

The default settings will be used besides the following:

```plaintext
crypto isakmp policy 10
authentication pre-share
group 2
crypto isakmp keepalive 60 periodic
```

Configure the isakmp client configuration group (vpn_group):

```plaintext
crypto isakmp client configuration group client3G
key digixauth
save-password
```

3.4 Configure IPsec

Create a transform-set to match the TransPort’s configuration:

```plaintext
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
```

Create the EZVPN client configuration and group:

```plaintext
crypto ipsec client ezvpn client3G
connect auto
group client-acc3G key digixauth
mode network-extension
peer a.b.c.d default
peer e.f.g.h
idletime 60
username xauthclient password digixauth
xauth userid mode local
```

Create the crypto dynamic-map that match TransPort’s configuration:

```plaintext
crypto dynamic-map Dyn-acc3G 1
set transform-set ESP-DES-SHA
```

Create the crypto map that match TransPort’s configuration and set the authentication for IPSEC to use user authentication:

```plaintext
crypto map Map-acc3G client authentication list userauthen
crypto map Map-acc3G isakmp authorization list groupauthor
crypto map Map-acc3G client configuration address respond
crypto map Map-acc3G 1 ipsec-isakmp dynamic Dyn-acc3G
```

Apply the crypto map to the WAN interface

```plaintext
interface FastEthernet0/0
crypto map Map-acc3G
crypto ipsec client ezvpn client-acc3G
```

Save Configuration

```plaintext
write mem
```
4 TESTING

4.1 Tunnel Status

Verify that the tunnel is now up on.

**Digi TransPort:**

Navigate to Management > Connections > VPN > IPsec > IPsec Tunnels

---

**Cisco:**

```
Router#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: Map-acc3G, local addr 62.00.00.000
    protected vrf: (none)
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
    current peer 92.001.000.000 port 4500
        PERMIT, flags={}
        #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
        #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 1
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts compr. failed: 0
        #pkts not decompressed: 0, #pkts decompress failed: 0
        #send errors 0, #recv errors 0

    local crypto endpt.: 62.00.00.000, remote crypto endpt.: 92.001.000.000
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
    current outbound spi: 0xD1AD18B(219861387)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
        spi: 0x17A213CB(396497867)
        transform: esp-des esp-sha-hmac
        in use settings ={Tunnel UDP-Encaps, }
```
conn id: 2011, flow_id: FPGA:11, sibling_flags 80000046, crypto map: Map-acc3G
  sa timing: remaining key lifetime (k/sec): (4580251/2296)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
    spi: 0xD1AD18B(219861387)
    transform: esp-des esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }

conn id: 2012, flow_id: FPGA:12, sibling_flags 80000046, crypto map: Map-acc3G
  sa timing: remaining key lifetime (k/sec): (4580251/2296)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

  outbound ah sas:

  outbound pcp sas:
4.2 Ping test

4.2.1 TransPort

To test that the VPN connection is successful, traffic needs to be routed via the TransPort to the remote network from ETH 0.

From a computer connected to the TransPort’s ETH 0 port and in the 192.168.10.0 subnet, issue a ping to the Cisco’s FastEthernet0/1 address:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\System32>ping 10.1.1.254
Pinging 10.1.1.254 with 32 bytes of data:
Reply from 10.1.1.254: bytes=32 time=2100ms TTL=126
Reply from 10.1.1.254: bytes=32 time=95ms TTL=126
Reply from 10.1.1.254: bytes=32 time=110ms TTL=126
Reply from 10.1.1.254: bytes=32 time=104ms TTL=126
Ping statistics for 10.1.1.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 95ms, Maximum = 2100ms, Average = 602ms
```

From the TransPort’s web interface, Navigate to Administration > Execute a command

**Ping 10.1.1.254 -e2**

Command: ping 10.1.1.254 -e2

Command result

<table>
<thead>
<tr>
<th>Pinging Addr [10.1.1.254]</th>
</tr>
</thead>
<tbody>
<tr>
<td>sent PING # 1</td>
</tr>
<tr>
<td>PING receipt # 1 : response time 0.06 seconds</td>
</tr>
<tr>
<td>Iface: ETH 0</td>
</tr>
<tr>
<td>Ping Statistics</td>
</tr>
<tr>
<td>Sent : 1</td>
</tr>
<tr>
<td>Received : 1</td>
</tr>
<tr>
<td>Success : 100 %</td>
</tr>
<tr>
<td>Average RTT : 0.06 seconds</td>
</tr>
</tbody>
</table>

OK

4.2.2 Cisco

```
Router#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/64 ms
Router#
```
5 CONFIGURATION FILES

TransPort WR21

eth 0 IPaddr "192.168.10.1"
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "1.2.3.4"
eroute 0 peerid "1.2.3.4"
eroute 0 ourid "client3G"
eroute 0 locip "192.168.10.0"
eroute 0 locmask "255.255.255.0"
eroute 0 remip "0.0.0.0"
eroute 0 remmsk "0.0.0.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "DES"
eroute 0 authmeth "XAUTHINITPRE"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 enckeybits 128
eroute 0 xauthid "xauthclient"
eroute 0 debug ON
ppp 1 ipsec ON
ike 0 keybits 128
ike 0 authalg "SHA1"
ike 0 aggressive ON
ike 0 ikegroup 2
ike 0 noresp ON
ike 0 deblevel 4
ike 0 delmode 3
user 8 name "1.2.3.4"
user 8 epassword "xxxxxxxx"
user 8 access 4
user 9 name "xauthclient"
user 9 epassword "xxxxxxxx"
user 9 access 4

Cisco 1841

aaa new-model
!aaa authentication login userauthen local
aaa authorization network groupauth local
!aaa session-id common
!username xauthclient password 0 digixauth
!crypto isakmp policy 10
authentication pre-share
group 2
crypto isakmp keepalive 60 periodic
!
crypto isakmp client configuration group client3G
key digixauth
save-password
!
!
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
!
!
crypto dynamic-map Dyn-acc3G 1
set transform-set ESP-DES-SHA
!
!
crypto map Map-acc3G client authentication list userauthen
crypto map Map-acc3G isakmp authorization list groupauthor
crypto map Map-acc3G client configuration address respond
crypto map Map-acc3G 1 ipsec-isakmp dynamic Dyn-acc3G
!

!
!
interface FastEthernet0/0
  ip address 1.2.3.4 255.255.255.248
duplex auto
  speed auto
crypto map Map-acc3G
crypto ipsec client ezvpn client3G
!
interface FastEthernet0/1
  ip address 10.1.1.254 255.255.255.0
duplex auto
  speed auto
!
!
ip route 0.0.0.0 0.0.0.0 62.00.00.000
!