Quick Note 054

Digi TransPort to Cisco VPN Tunnel using OpenSSL certificates.

Digi Support
December 2014
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>1.1</td>
<td>Outline</td>
</tr>
<tr>
<td>1.2</td>
<td>Assumptions</td>
</tr>
<tr>
<td>1.3</td>
<td>Corrections</td>
</tr>
<tr>
<td>2</td>
<td>Version</td>
</tr>
<tr>
<td>3</td>
<td>certificates creation</td>
</tr>
<tr>
<td>3.1</td>
<td>Generate Test certificates using OpenSSL and XCA</td>
</tr>
<tr>
<td>3.1.1</td>
<td>Create a Root CA Certificate</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Create a CA-Signed Host Certificate (Cisco Router, Responder)</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Create a CA-Signed Client Certificate (Digi TransPort WR, initiator)</td>
</tr>
<tr>
<td>3.1.4</td>
<td>Export the certificates and keys in .PEM format</td>
</tr>
<tr>
<td>4</td>
<td>Digi transport configuration</td>
</tr>
<tr>
<td>4.1</td>
<td>Upload SSL certificates to the Digi TransPort WR (initiator)</td>
</tr>
<tr>
<td>4.1.1</td>
<td>Upload the certificates via FTP</td>
</tr>
<tr>
<td>4.1.2</td>
<td>Upload the certificates via the Web GUI</td>
</tr>
<tr>
<td>4.2</td>
<td>Configure the VPN Tunnel settings on the Digi TransPort WR (Initiator)</td>
</tr>
<tr>
<td>5</td>
<td>Cisco configuration</td>
</tr>
<tr>
<td>5.1</td>
<td>Import the certificates and private key</td>
</tr>
<tr>
<td>5.1.1</td>
<td>Create a trustpoint for the CA root certificate</td>
</tr>
<tr>
<td>5.1.2</td>
<td>Import the CA root certificate in the previously created trustpoint with copy and paste</td>
</tr>
<tr>
<td>5.1.3</td>
<td>Create a trustpoint for the public certificate and the private key</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Import the public certificate in the previously created trustpoint with copy and paste</td>
</tr>
<tr>
<td>5.2</td>
<td>Configure the tunnel</td>
</tr>
<tr>
<td>6</td>
<td>Testing</td>
</tr>
<tr>
<td>6.1</td>
<td>Confirm Traffic Traverses the IPSec Tunnels</td>
</tr>
<tr>
<td>7</td>
<td>Configuration files</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Outline

This document describes how to create, upload SSL certificates and configure Digi TransPort WR and Cisco routers to build an IPsec VPN tunnel.

1.2 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.

This application note applies only to:

**Model:** DIGI TransPort WR41/44/21

Digi TransPort WR41 routers must have the “Encryption” option
Digi TransPort WR21 routers must run Enterprise firmware

**Model:** Cisco 3725 running Advanced Enterprise Image.

**Firmware versions:** 5169 and later

*Please note:* This application note has been specifically rewritten for firmware release 5169 and later and will not work on earlier versions of firmware. Please contact tech.support@digi.com if your require assistance in upgrading the firmware of the TransPort router.

1.3 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.

2 VERSION

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Published</td>
</tr>
</tbody>
</table>
3 CERTIFICATES CREATION

If you already have certificates available, you can skip to section 3.2

3.1 Generate Test certificates using OpenSSL and XCA

Download and install the latest release of XCA which can be found at: http://sourceforge.net/projects/xca/

3.1.1 Create a Root CA Certificate

Open the XCA application

1. Click the File menu and select New Database, chose a name and click Save.
2. Chose a password and click OK
3. Click the Certificates tab
4. Click the New Certificate button
5. Under “Template for the new certificate”, select default CA and click Apply all
6. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>This is for display purposes in the tool, only</td>
</tr>
</tbody>
</table>
| State or Province Name     | The state or province where your organization is legally located. Do not abbreviate.  
In this example: Some-State |
| Locality Name              | The city where your organization is legally located. Do not abbreviate.  
In this example: Paris     |
| Organization Name          | The exact legal name of your organization. Do not abbreviate your organization name.  
In this example: Digi     |
| Organizational Unit Name   | Section of the organization.  
Examples of sections are Marketing, Research and Development, Human Resources or Sales. |
| Common Name                | In this example DigiCA will be used.                                    |
| Email Address              | Enter your organization general email address.                          
In this example certteam@digi.com |
7. The certificate should now appear in the window with the **CA : YES** confirmation. If it does not say **CA: YES**, verify that you selected CA in the template and clicked Apply All.
3.1.2 Create a CA-Signed Host Certificate (Cisco Router, Responder)

1. Click the Certificates tab
2. Click the New Certificate button
3. Under Signing, make sure to select “Use this Certificate for signing” and chose the previously created CA.
4. Under “Template for the new certificate”, select default HTTPS_server and click Apply all

5. Go to the Subject tab, fill in all the information then click the Generate a new key button and click OK
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>This is for display purposes in the tool, only</td>
</tr>
<tr>
<td>Country Name</td>
<td>The two-letter ISO 3166 abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>The state or province where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td></td>
<td>In this example: Some-State</td>
</tr>
<tr>
<td>Locality Name</td>
<td>The city where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td></td>
<td>In this example: Munich</td>
</tr>
<tr>
<td>Organization Name</td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
</tr>
<tr>
<td></td>
<td>In this example: DigiDE</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.</td>
</tr>
<tr>
<td>Common Name</td>
<td>In this example <strong>wrdigide</strong> will be used. This will be used as the router Identity for the IPSec tunnel settings.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter your organization general email address.</td>
</tr>
<tr>
<td></td>
<td>In this example <strong><a href="mailto:digide@digi.com">digide@digi.com</a></strong></td>
</tr>
</tbody>
</table>
7. The certificate should now appear in the window under the CA certificate.

3.1.3 Create a CA-Signed Client Certificate (Digi TransPort WR, initiator)

1. Click the Certificates tab
2. Click the New Certificate button
3. Under Signing, make sure to select “Use this Certificate for signing” and chose the previously created CA.
4. Under “Template for the new certificate”, select default HTTPS_client and click Apply all
5. Go to the **Subject** tab, fill in all the information then click the **Generate a new key** button and click **OK**

![Certificate and key management](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal name</td>
<td>This is for display purposes in the tool, only</td>
</tr>
<tr>
<td>Country Name</td>
<td>The two-letter <strong>ISO 3166</strong> abbreviation for your country.</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>The state or province where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Locality Name</td>
<td>The city where your organization is legally located. Do not abbreviate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>The exact legal name of your organization. Do not abbreviate your organization name.</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>Section of the organization. Examples of sections are Marketing, Research and Development, Human Resources or Sales.</td>
</tr>
<tr>
<td>Common Name</td>
<td>In this example <a href="#">wrdigide</a> will be used. This will be used as the router Identity for the IPSec tunnel settings</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter your organization general email address.</td>
</tr>
</tbody>
</table>

In this example: Some-State

In this example: Munich

In this example: DigiDE

In this example: digide@digi.com
1. The certificate should now appear in the window under the CA certificate.

3.1.4 Export the certificates and keys in .PEM format

1. Select the Certificates Tab.
2. Highlight the DigiCA certificate and click the Export button

3. In the Certificate export window, select PEM as the export format and change the filename to cacert.pem and click OK
4. Repeat the previous step for the Client and Host certificate. Rename them `cert.pem` and `certcl.pem`.

5. Select the **Private Keys** tab.

6. Highlight the host certificate and click the **Export** button.
7. In the Key export window, select **PEM** as the export format, check the box “**Export the private part of the key too**” and change the filename to **privh.pem** and click OK.

![Key export window](image)

**Please note:** Cisco routers require the private key to be encrypted. Make sure to check the box “**Encrypt the key with a password**” when export the key for the Cisco device (**privh.pem** below) and specify a passphrase.

8. Repeat the previous step for the Client key and name it **privcl.pem**.

The following files should now be available:

- `cacert.pem`: CA root certificate
- `certh.pem`: Cisco (responder) certificate
- `certcl.pem`: TransPort WR (initiator) certificate
- `privh.pem`: Cisco (responder) private key (password encrypted)
- `privcl.pem`: TransPort WR (initiator) private key

**Please note:** It is important that the file name do not exceed the 8.3 file format and to keep the file type and naming as the TransPort router will be searching for these and load them in the certificate management automatically.
Open an FTP connection to the TransPort router that you wish to update. In this example, using FileZilla.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>192.168.1.105</td>
<td>IP Address of the TransPort router</td>
</tr>
<tr>
<td>Username</td>
<td>username</td>
<td>Username with Access Level : Super to log in to the TransPort router (default : username)</td>
</tr>
<tr>
<td>Password</td>
<td>password</td>
<td>Password for the user with Access Level : Super to log in to the TransPort router (default : password)</td>
</tr>
<tr>
<td>Port</td>
<td>21</td>
<td>Default FTP port.</td>
</tr>
<tr>
<td>cacert.pem</td>
<td>-</td>
<td>CA Root certificate</td>
</tr>
<tr>
<td>certcl.pem</td>
<td>-</td>
<td>Client Certificate</td>
</tr>
<tr>
<td>privcl.pem</td>
<td>-</td>
<td>Client Private Key</td>
</tr>
</tbody>
</table>

Transfer the certificates file to the root directory of the TransPort.
4.1.2 Upload the certificates via the Web GUI

Open a web browser to the IP address of the Digi TransPort router (initiator)

Administration > X.509 Certificate Management > Certificate Authorities (CAs)

Click the browse button and select the file location where cacert.pem is located and click Upload

The CA Certificate should now appear under the Installed Certificate Authority Certificates

Administration > X.509 Certificate Management > IPSec/SSH/HTTPS Certificates

Click the browse button and select the file location where certcl.pem is located and click Upload

The Certificate should now appear under the Installed Certificates

Administration > X.509 Certificate Management > Key Files

Click the browse button and select the file location where privcl.pem is located. Under filename, type privcl.pem and click Upload.
4.2 **Configure the VPN Tunnel settings on the Digi TransPort WR (Initiator).**

Enable IPSec on PPP 1 (mobile interface):

**Configuration – Network > Interfaces > Mobile**

![Configuration – Network > Interfaces > Mobile]

**Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0-9 > IPsec 0**

![Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0-9 > IPsec 0]
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Cert Tunnel</td>
<td>Description of the IPsec tunnel</td>
</tr>
<tr>
<td>IP Address / Hostname of Remote</td>
<td>1.2.3.4</td>
<td>IP Address of the remote endpoint router B (responder)</td>
</tr>
<tr>
<td>Endpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Lan IP Address</td>
<td>192.168.10.0</td>
<td>Local Lan IP address</td>
</tr>
<tr>
<td>Local Lan Mask</td>
<td>255.255.255.0</td>
<td>Local Lan subnet mask</td>
</tr>
<tr>
<td>Remote Lan IP Address</td>
<td>192.168.1.0</td>
<td>Remote Lan IP address</td>
</tr>
<tr>
<td>Remote Lan Mask</td>
<td>255.255.255.0</td>
<td>Remote Lan subnet mask</td>
</tr>
<tr>
<td>Use the Following security on this</td>
<td>RSA Signatures</td>
<td>Select RSA signature security for this tunnel to use the uploaded certificates</td>
</tr>
<tr>
<td>tunnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA Key File</td>
<td>Privcl.pem</td>
<td>Private key file used for router A (initiator)</td>
</tr>
<tr>
<td>Our ID</td>
<td>wrdigide</td>
<td>ID that is matching the CN of the certificate in the first router (initiator)</td>
</tr>
<tr>
<td>Our ID type</td>
<td>User FQDN</td>
<td>User FQDN for the ID type (to match the CN information used in the certificate)</td>
</tr>
<tr>
<td>Remote ID</td>
<td>wrdigiuk</td>
<td>Remote ID that is matching the CN in the second router certificate (responder)</td>
</tr>
<tr>
<td>Encryption on this tunnel</td>
<td>AES 256</td>
<td>Encryption type used on this tunnel</td>
</tr>
<tr>
<td>Authentication on this tunnel</td>
<td>MD5</td>
<td>Authentication type used on this tunnel</td>
</tr>
<tr>
<td>Use Diffie Hellman Group</td>
<td>2</td>
<td>Use DH Group 2</td>
</tr>
<tr>
<td>Use IKE configuration</td>
<td>0</td>
<td>IKE settings used to setup the tunnel</td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>Whenever a route to the destination is available</td>
<td>Settings to bring the IPsec tunnel up</td>
</tr>
<tr>
<td>If the tunnel is down and a packet is</td>
<td>Bring the tunnel up</td>
<td>Drop packets to the remote side if the tunnel is down</td>
</tr>
<tr>
<td>ready to be sent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Click **Apply** and **Save** to save the settings.

**Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1**

![IKE 1 Configuration](image-url)
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES (256 bit)</td>
<td>Encryption settings used on the tunnel</td>
</tr>
<tr>
<td>Authentication</td>
<td>MD5</td>
<td>Authentication settings used on the tunnel</td>
</tr>
<tr>
<td>Mode</td>
<td>Main</td>
<td>Phase 1 negotiation type</td>
</tr>
<tr>
<td>MODP Group for Phase 1</td>
<td>1 (758)</td>
<td>DH Phase 1</td>
</tr>
<tr>
<td>MODP Group for Phase 2</td>
<td>2 (1024)</td>
<td>DH Phase 2</td>
</tr>
</tbody>
</table>

Click **Apply** and **Save** to save the settings.

**Configuration – Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 1 > Advanced**

Enter the private key file name

Click **Apply** and **Save** to save the settings.
5 CISCO CONFIGURATION

5.1 Import the certificates and private key

5.1.1 Create a trustpoint for the CA root certificate

cisco3725(config)#crypto ca trustpoint digiroot
cisco3725(ca-trustpoint)#enrollment terminal pem
cisco3725(ca-trustpoint)#crl optional
cisco3725(ca-trustpoint)#exit

5.1.2 Import the CA root certificate in the previously created trustpoint with copy and paste

cisco3725(config)#crypto ca authenticate digiroot

Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----
quit

Certificate has the following attributes:  
Fingerprint: xxxxxxxx  
% Do you accept this certificate? [yes/no]: yes  
Trustpoint CA certificate accepted.  
% Certificate successfully imported

Make sure that the certificate starts and ends like shown.
5.1.3 Create a trustpoint for the public certificate and the private key

```
cisco3725(config)#crypto ca trustpoint digitest
cisco3725(ca-trustpoint)#enrollment terminal pem
cisco3725(ca-trustpoint)#crl optional
cisco3725(ca-trustpoint)#exit
```

5.1.4 Import the public certificate in the previously created trustpoint with copy and paste

```
cisco3725(config)#crypto pki import digitest pem terminal password digitest
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
xxxxxx
-----END CERTIFICATE-----
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
xxxxxx
-----END CERTIFICATE-----
quit
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
xxxxxx
-----END CERTIFICATE-----
quit
% PEM files import succeeded.
```

The last part of the command is the password used for the private key during certificates creation.

First, re-enter the CA certificate. Second, enter the public certificate. Third, enter the private key.
5.2 Configure the tunnel

Set "our ID" type and configure use for IKE.

```
cisco3725(config)#crypto pki trustpoint digiroot
cisco3725(config)#ca-trustpoint# enrollment terminal pem
cisco3725(config)#ca-trustpoint# usage ike
cisco3725(config)#ca-trustpoint# subject-name cn=cisco
cisco3725(config)#ca-trustpoint# revocation-check none
```

Set Phase 1 and Phase 2 policy to match the configuration of the TransPort

```
cisco3725(config)#crypto isakmp policy 1
  cisco3725(config-isakmp)# encr aes 256
  cisco3725(config-isakmp)# group 2
  cisco3725(config-isakmp)#crypto isakmp identity dn
  cisco3725(config)#crypto isakmp keepalive 10
```

Tunnel Mode and phase 2 set

```
cisco3725(config)#crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
  cisco3725(config)#mode tunnel
```

Configure SA timers and create dynamic map

```
cisco3725(config)#crypto call admission limit ike sa 6000
  cisco3725(config)#crypto call admission limit ike in-negotiation-sa 3000
  cisco3725(config)#crypto dynamic-map mydynmap 1
  cisco3725(config)#set security-association lifetime seconds 86400
  cisco3725(config)#set security-association idle-time 28200
  cisco3725(config)#set transform-set myset
  cisco3725(config)#crypto map mymap1 20 ipsec-isakmp dynamic mydynmap
```

Configure the WAN interface and enable IPsec

```
cisco3725(config)#interface FastEthernet0/1
  cisco3725(config-if)# ip address 192.168.10.254 255.255.255.248
  cisco3725(config-if)# speed auto
  cisco3725(config-if)# duplex auto
  cisco3725(config-if)# crypto map mymap1
```

Configure the default route

```
ip route 0.0.0.0 0.0.0.0 82.82.182.182
```

The cisco is now configured and the tunnel should come up.
This section will show that the IPSec tunnel has been established.

The Event log will show the IPSec tunnel is up.

Management – Event Log

14:49:18, 25 Feb 2014, Eroute 0 VPN up peer: wrdigiuk
14:49:18, 25 Feb 2014, New IPSec SA created by wrdigiuk

Navigate to the above link where the status of the newly established IPSec tunnel/s can be seen. The first column shows which tunnel number the tunnel is connected to.
6.1 Confirm Traffic Traverses the IPSec Tunnels

This section will show traffic passing across the tunnel. To test this easily, an ICMP Echo Request/Reply (or PING) will pass from the Router A lan (initiator) to Router B Ethernet interface side (responder)

Administration > Execute a command

Ping 192.168.10.254 -e0

Using –e0 specifies that the source address is taken from Ethernet 0 which is the negotiated LAN settings in the IPSec tunnel.

Command: ping 192.168.10.254 -e0
Command result

Pinging Addr [192.168.10.254]

sent PING # 1
PING receipt # 1 : response time 0.26 seconds
Iface: PPP 1
Ping Statistics
Sent : 1
Received : 1
Success : 100 %
Average RTT : 0.26 seconds

OK
Digi TransPort WR 21

eroute 1 descr "Cert Tunnel"
eroute 1 peerip "1.2.3.4"
eroute 1 peerid "wrdigiuk"
eroute 1 ourid "wrdigide"
eroute 1 locip "192.168.1.0"
eroute 1 locmask "255.255.255.0"
eroute 1 remip "192.168.10.0"
eroute 1 remmask "255.255.255.0"
eroute 1 ESPauth "MD5"
eroute 1 ESPenc "AES"
eroute 1 authmeth "RSA"
eroute 1 nosa "TRY"
eroute 1 autosa 2
route 1 ikecfg 1
route 1 dhgroup 2
route 1 enckeybits 256
route 1 privkey "privcl.pem"
rout 1 debug ON
ike 1 encalg "AES"
ike 1 keybits 256
ike 1 ikegroup 2
ike 1 privrsakey "privcl.pem"
ike 1 delmode 3

Cisco 3725

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname cisco3725
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
multilink bundle-name authenticated
!
crypto pki trustpoint digiroot

enrollment terminal pem
usage ike
subject-name cn=cisco
revocation-check none
!
crypto pki trustpoint digitest
revocation-check none
rsakeypair digitest
crypto pki certificate map digitest 10
subject-name co ou = digi
subject-name co o = digi

crypto pki certificate chain digiroot
certificate ca 01
xxxx
quit
crypto pki certificate chain digitest
certificate 02
xxxx
quit
certificate ca 01
xxx
quit

ip tcp synwait-time 5

crypto isakmp policy 1
  encr aes 256
group 2
crypto isakmp identity dn
crypto isakmp keepalive 10

crypto ipsec security-association lifetime seconds 900
crypto ipsec security-association idle-time 910

crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
  mode tunnel


crypto call admission limit ike sa 6000

crypto call admission limit ike in-negotiation-sa 3000

crypto dynamic-map mydynmap 1
  set security-association lifetime seconds 86400
  set security-association idle-time 28200
  set transform-set myset


crypto map mymap1 20 ipsec-isakmp dynamic mydynmap

interface Loopback0
ip address 10.100.0.1 255.255.255.255
interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.0
  speed auto
  duplex auto

interface FastEthernet0/1
  ip address 192.168.10.0 255.255.255.248
  speed auto
  duplex auto
  crypto map mymap1

  ip forward-protocol nd

no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 82.82.82.182

control-plane

line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  password cisco
  login
line vty 5 10
  password cisco
  login

end