Application Note 58

AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

18 November 2015
# Contents

1  Introduction .............................................................................................................. 5  
   1.1 Outline ................................................................................................................ 5  
   1.2 Assumptions ........................................................................................................... 5  
   1.3 Corrections .......................................................................................................... 5  
   1.4 Version .................................................................................................................... 5  
2  Scenario ..................................................................................................................... 6  
3  Digi TransPort router configuration - Initiator .......................................................... 7  
   3.1 LAN Settings ........................................................................................................... 7  
   3.2 WAN Settings ......................................................................................................... 8  
   3.3 Default Route ......................................................................................................... 10  
   3.4 IKEv2 Configuration .............................................................................................. 11  
   3.5 IPsec Tunnel configuration .................................................................................... 12  
   3.6 Preshared Key configuration ................................................................................ 14  
4  Cisco router configuration - Responder ...................................................................... 16  
   4.1 LAN Settings ......................................................................................................... 16  
   4.2 WAN Settings ......................................................................................................... 16  
   4.3 Default Route ......................................................................................................... 16  
   4.4 IKEv2 Configuration and Preshared Key ................................................................. 17  
   4.5 IPsec Tunnel configuration .................................................................................... 18  
   4.6 Access List configuration ...................................................................................... 19  
   4.7 Crypto Map configuration ...................................................................................... 19  
5  Testing ....................................................................................................................... 21  
   5.1 Debug settings on TransPort .................................................................................. 21  
   5.2 Debug settings on Cisco ........................................................................................ 25  
   5.3 Setting the tunnel UP .............................................................................................. 25  
   5.4 IPsev SAs status ..................................................................................................... 26  
   5.5 Testing traffic on the tunnel .................................................................................. 27
AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

6  Configuration file............................................................................................................................. 31
6.1  Initiator (TransPort) Configuration File.......................................................................................... 31
6.2  Responder (Cisco) Configuration File............................................................................................ 34
### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1-1</td>
<td>Initiator LAN settings</td>
<td>7</td>
</tr>
<tr>
<td>3.2-1</td>
<td>Initiator WAN settings</td>
<td>8</td>
</tr>
<tr>
<td>3.2-2</td>
<td>Enabling IPsec on WAN</td>
<td>9</td>
</tr>
<tr>
<td>3.3-1</td>
<td>Default route</td>
<td>10</td>
</tr>
<tr>
<td>3.4-1</td>
<td>Initiator IKEv2 settings</td>
<td>11</td>
</tr>
<tr>
<td>3.5-1</td>
<td>Initiator IPsec settings</td>
<td>12</td>
</tr>
<tr>
<td>3.6-1</td>
<td>Remote peer Preshared Key</td>
<td>14</td>
</tr>
<tr>
<td>3.6-2</td>
<td>Local peer Preshared Key</td>
<td>15</td>
</tr>
<tr>
<td>4.1-1</td>
<td>Initiator LAN settings</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.2-1</td>
<td>Initiator WAN settings</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.2-2</td>
<td>Enabling IPsec on WAN</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.3-1</td>
<td>Default route</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.4-1</td>
<td>IKEv2 Responder</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.5-1</td>
<td>Responder IPsec Settings</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.6-1</td>
<td>Remote Peer Preshared key</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>4.6-2</td>
<td>Local Peer Preshared key</td>
<td>Error! Bookmark not defined.</td>
</tr>
<tr>
<td>5.1-1</td>
<td>Analyser settings - 1</td>
<td>21</td>
</tr>
<tr>
<td>5.1-2</td>
<td>Analyser settings – 2</td>
<td>22</td>
</tr>
<tr>
<td>5.1-3</td>
<td>Enabling IKE debug</td>
<td>24</td>
</tr>
<tr>
<td>5.2-1</td>
<td>IPsec and IKE SAs status</td>
<td>Error! Bookmark not defined.</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Outline

Internet Protocol Security (IPsec) is a set of protocols providing cryptographic security services and allows creation of encrypted tunnel between two private networks (VPN). In order to set up and maintain the IPsec VPN, Internet Key Exchange Protocol (IKE) is used. In the last few years, a new version has been designed for IKE protocol (IKEv2), that has the basic outcome as IKEv1 but introduces many improvements as decreased latency (only 4 messages need to be exchanged for set up the VPN) and reliability (all messages are acknowledge and sequenced).

This Application Note gives a guide on configuring an IPsec VPN with IKEv2 between a TransPort router that acts as Initiator and a Cisco router acting as the responder.

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.

**Preconditions:** This guide assumes that two Digi TransPort are reachable to each other via an Ethernet connection passing through another router. Other kind of WAN technology can be used.

**Models shown:** Digi TransPort WR44

**Other Compatible Models:** All other Digi TransPort products with IPsec enabled.

**Firmware versions:** All Versions

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

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.

1.4 Version

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
</tr>
</tbody>
</table>
This application note will consider the following scenario:

The Transport device acts as Initiator and the Cisco as responder. An IPsec tunnel will be set up between the peers using IKEv2 negotiation. The tunnel will protect the LAN to LAN traffic between them (192.168.1.10/24 <-> 172.16.1.0/24).
3 DIGI TRANSPORT ROUTER CONFIGURATION - INITIATOR

In order to configure the Digi TransPort, connect a PC to the ETH0 of the TransPort and log into the Web User Interface (WebUI) with a browser at the default address 192.168.1.1. Then follow the sections below.

3.1 LAN Settings

In this AN the LAN interface of the Transport that acts as Initiator is configured on ETH 0 and left as default (192.168.1.1). The configuration can be checked going to the WEB UI at the section Configuration – Network > Interfaces > Ethernet > ETH 0:

![Figure 3.1-1: Initiator LAN settings](image)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>Specifies the IP address of this Ethernet port</td>
<td><code>eth 0 ipaddr 192.168.1.1</code></td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port</td>
<td><code>eth 0 mask 255.255.255.0</code></td>
</tr>
</tbody>
</table>
3.2 WAN Settings

In this Application note we will configure the ETH 1 as WAN connection as follows:

![Figure 3.2-1: Initiator WAN settings](image)

Then, IPSec must be enabled under the interface, going into the advance section:
## Figure 3.2-2: Enabling IPsec on WAN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>10.10.1.1</td>
<td>Specifies the IP address of this Ethernet port</td>
<td><code>eth 1 ipaddr 10.10.1.1</code></td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0</td>
<td>Specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port</td>
<td><code>eth 0 mask 255.255.255.0</code></td>
</tr>
<tr>
<td>Gateway</td>
<td>10.10.1.3</td>
<td>Specifies the IP address of a gateway to be used by the unit</td>
<td><code>eth 1 gateway 10.10.1.3</code></td>
</tr>
<tr>
<td>Enable IPsec on this interface</td>
<td>Enabled</td>
<td>Enable IPsec security features for this interface</td>
<td><code>eth 1 ipsec 1</code></td>
</tr>
</tbody>
</table>
3.3 Default Route

In the scenario considered in this AN, the default gateway for the TransPort that acts as Initiator is 10.10.1.3, so a default route need to be configured going in Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0:

![Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route 0](image)

**Figure 3.3-1: Default route**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>10.10.1.3</td>
<td>Set the IP address of the default gateway</td>
<td><code>def_route 0 gateway 10.10.1.3</code></td>
</tr>
<tr>
<td>Interface</td>
<td>Ethernet 1</td>
<td>Set the interface used to default route the packets, is selected from the drop-down list and the interface instance number is entered into the adjacent text box</td>
<td><code>def_route 0 ll_ent &quot;eth&quot;</code> <code>def_route 0 ll_add 1</code></td>
</tr>
</tbody>
</table>
3.4 IKEv2 Configuration

In order to configure the IKEv2 part for the initiator, go to the section Configuration – Network > VPN > IPsec > IKE > IKEv2 > IKEv2 0 and set the parameters as indicated below:

![Diagram of IKEv2 settings]

**Figure 3.4-1: Initiator IKEv2 settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES (128 bit)</td>
<td>Defines the encryption algorithm used</td>
<td>ike2 0 iencalg &quot;AES&quot; ike2 0 ienckeybits 128</td>
</tr>
<tr>
<td>Authentication</td>
<td>SHA1</td>
<td>Defines the authentication algorithm used</td>
<td>ike2 0 iauthalg sha1</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>SHA1</td>
<td>Defines the PRF (Pseudo Random Function) algorithm used</td>
<td>ike2 0 iprfalg sha1</td>
</tr>
<tr>
<td>MODP Group for Phase 1</td>
<td>2 (1024)</td>
<td>Sets the key length used in the IKE Diffie-Hellman exchange</td>
<td>ike2 0 idhgroup 2</td>
</tr>
</tbody>
</table>

**Table 3.4-1: Initiator IKEv2 settings**

Click apply to temporarily save the changes.
3.5 IPsec Tunnel configuration

The following section describes how to configure the Digi TransPort’s IPsec Tunnel settings on the initiator.

Browse to Configuration – Network > VPN > IPsec > IPsec Tunnels > IPsec 0 and refer to the following picture and table for the settings of parameters:

![Figure 3.5-1: Initiator IPsec settings](image-url)
### AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or hostname of the remote unit</td>
<td>10.10.2.1</td>
<td>The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.</td>
<td><code>eroute 0 peerip &quot;10.10.2.1&quot;</code></td>
</tr>
<tr>
<td>Local LAN &gt; Use these settings for the Local LAN</td>
<td>IP address: 192.168.1.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the local peer</td>
<td><code>eroute 0 locip &quot;192.168.1.0&quot; eroute 0 locmsk &quot;255.255.255.0&quot;</code></td>
</tr>
<tr>
<td>Remote LAN &gt; Use these settings for the Remote LAN</td>
<td>IP address: 172.16.1.0 Mask: 255.255.255.0</td>
<td>The subnet LAN of the other peer</td>
<td><code>eroute 0 remip &quot;172.16.1.0&quot; eroute 0 remmsk &quot;255.255.255.0&quot;</code></td>
</tr>
<tr>
<td>Use the following security on this tunnel</td>
<td>Preshared Keys (Selected)</td>
<td>Choose the security type for the connection. In this AN, Preshared Keys are used</td>
<td><code>eroute 0 authmeth &quot;PRESHARED&quot;</code></td>
</tr>
<tr>
<td>Our ID</td>
<td>transport</td>
<td>The ID that the initiator will use. In this AN, Preshared Keys will be used</td>
<td><code>eroute 0 ourid &quot;transport&quot;</code></td>
</tr>
<tr>
<td>Our ID type</td>
<td>IKE ID</td>
<td>Choose the type of ID used, IKE ID allows the use of descriptive text strings (friendly names)</td>
<td><code>eroute 0 ouridtype 0</code></td>
</tr>
<tr>
<td>Remote ID</td>
<td>cisco1</td>
<td>Set the ID that responder will use. In this AN, we will use the ID “transport2” as the Remote ID for this tunnel.</td>
<td><code>eroute 0 peerid &quot;cisco1&quot;</code></td>
</tr>
<tr>
<td>Use &lt;&gt; encryption on this tunnel</td>
<td>3DES</td>
<td>This is the encryption type to use for the tunnel. This AN uses 3DES</td>
<td><code>eroute 0 ESPenc &quot;3DES&quot;</code></td>
</tr>
<tr>
<td>Use &lt;&gt; authentication on this tunnel</td>
<td>SHA1</td>
<td>This is the authentication type to use for the tunnel. This AN uses SHA1.</td>
<td><code>eroute 0 ESPauth &quot;SHA1&quot;</code></td>
</tr>
<tr>
<td>Use Diffie Hellman group &lt;&gt;</td>
<td>2</td>
<td>This is the Diffie Hellman (DH) group to use. This AN uses group 2.</td>
<td><code>eroute 0 dhgroup 2</code></td>
</tr>
<tr>
<td>Use IKE &lt;&gt; to negotiate this tunnel</td>
<td>v2</td>
<td>Set the IKE version to use to negotiate this IPsec tunnel, for this AN select “v2”</td>
<td><code>eroute 0 ikever 2</code></td>
</tr>
<tr>
<td>Bring this tunnel up</td>
<td>All the time</td>
<td>This controls how the IPsec tunnel is brought up, for the initiator “All the time” option is chosen</td>
<td><code>eroute 0 autosa 2</code></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>Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. For the initiator in this AN the “bring the tunnel up” option is chosen</td>
<td><code>eroute 0 nosa “try&quot;</code></td>
</tr>
</tbody>
</table>

*Table 3.5-1: Initiator IPsec settings*
3.6 Preshared Key configuration

In IKEv2 for the configuration of Preshared Key, two users need to be configured, one for the local peer and one for the remote. The key for the two users can be different (but each has to match the one configured on the other peer for the same user).

Note that any user can be used as the user for the Preshared Key, but best practice recommends using a user in the upper range of users because these users have the (router management) Access Level already set to ‘None’. If a lower User number is configured, the Access Level should be changed to be ‘None’.

Browse to Configuration – Security > Users > User 10-14 > User 10 and > User 11 and refer to the following pictures and tables for the configuration of the users:

**Remote peer:**

![Remote peer Preshared Key configuration](image)

**Figure 3.6-1: Remote peer Preshared Key**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>cisco1</td>
<td>This is the username for the remote peer and should match the Remote ID configured in the IPSec tunnel</td>
<td>user 10 name &quot;cisco1&quot;</td>
</tr>
<tr>
<td>Password/Confirm</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the VPN tunnel.</td>
<td>user 10 epassword ****</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
<td>user 10 access 4</td>
</tr>
</tbody>
</table>

**Table 3.6-1: Remote peer Preshared Key**
AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

**Local peer:**

![Local peer Preshared Key](image)

**Figure 3.6-2: Local peer Preshared Key**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
<th>CLI command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>transport</td>
<td>This is the username for the local peer and should match the Our ID configured in the IPsec tunnel</td>
<td>user 11 name &quot;transport&quot;</td>
</tr>
<tr>
<td>Password/Confirm password</td>
<td>****</td>
<td>Fill this field with the Preshared Key for the VPN tunnel.</td>
<td>user 11 epassword ****</td>
</tr>
<tr>
<td>Access Level</td>
<td>None</td>
<td>This is the access level for the user, in the case of preshared key user, it will not be granted any admin access</td>
<td>user 11 access 4</td>
</tr>
</tbody>
</table>

**Table 3.6-2: Local peer Preshared Key**

Click Apply and Save the settings after applying.
4 CISCO ROUTER CONFIGURATION - RESPONDER

The first step is to obtain a command prompt at the Cisco router and establish that the IPsec option has been installed and if IKEv2 is supported. If IPsec option is not installed has not, you will not be able to enter the keyword “crypto” without getting an error. If IKEv2 is not supported by the firmware, you will not be able to enter the keywords “crypto ikev2” without getting an error.

Remember as well that you need to be in Enable mode and have entered configuration mode (e.g. by typing “configure terminal”) to enter configuration commands.

4.1 LAN Settings

For the LAN settings on the cisco, type the following commands:

```
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
speed auto
duplex auto
```

4.2 WAN Settings

For the WAN settings on the cisco, type the following commands:

```
interface FastEthernet0/1
ip address 10.10.2.1 255.255.255.0
speed auto
duplex auto
```

4.3 Default Route

In the scenario considered in this AN, the default gateway for the Cisco that acts as Responder is 10.10.2.3, so a default route needs to be configured typing the following command:

```
ip route 0.0.0.0 0.0.0.0 10.10.2.3
```
4.4 IKEv2 Configuration and Preshared Key

In order to configure the IKEv2 part for the responder, type the following commands (details are reported on each part)

Proposal:

```bash
crypto ikev2 proposal proposal1
  encryption aes-cbc-128
  integrity sha1
  group 2
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ikev2 proposal</code></td>
<td>proposal1</td>
<td>Create the proposal and set a name for it</td>
</tr>
<tr>
<td><code>encryption</code></td>
<td>aes-cbc-128</td>
<td>Set the acceptable encryption algorithm</td>
</tr>
<tr>
<td><code>integrity</code></td>
<td>sha1</td>
<td>Set the acceptable authentication algorithm</td>
</tr>
<tr>
<td><code>group</code></td>
<td>2</td>
<td>Set the acceptable DH group</td>
</tr>
</tbody>
</table>

Policy:

```bash
crypto ikev2 policy policy1
  proposal proposal1
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ikev2 policy</code></td>
<td>policy1</td>
<td>Create the policy and set a name for it</td>
</tr>
<tr>
<td><code>proposal</code></td>
<td>proposal1</td>
<td>Apply the proposal already created to the policy</td>
</tr>
</tbody>
</table>

Keyring:

```bash
crypto ikev2 keyring kyr1
  peer transport
```
AN How to Configure an IKEv2 VPN Tunnel Between a TransPort router and a Cisco Responder

identity key-id transport
pres-shared-key digidigi

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>keyring</td>
<td>kyr1</td>
<td>Create a keyring and set a name for it</td>
</tr>
<tr>
<td>peer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transport</td>
<td>Create a peer under the keyring and set a name for it</td>
</tr>
<tr>
<td>identity key-id</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transport</td>
<td>Set the ID for the remote peer (and the type)</td>
</tr>
<tr>
<td>pre-shared-key</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>digidigi</td>
<td>Set the preshared key for the remote peer</td>
</tr>
</tbody>
</table>

**Profile:**

crypto ikev2 profile prof
match identity remote key-id transport
identity local key-id cisco1
authentication remote pre-share
authentication local pre-share
keyring local kyr1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>profile</td>
<td>prof</td>
<td>Create an IKEv2 profile and set a name for it</td>
</tr>
<tr>
<td>match identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote key-id</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transport</td>
<td>match this profile with the remote peer ID and ID type</td>
</tr>
<tr>
<td>identity local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>key-id</td>
<td>cisco1</td>
<td>define local ID and ID type</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>remote</td>
<td>pre-share</td>
<td>define authentication method for remote peer ID</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>local</td>
<td>pre-share</td>
<td>define authentication method for local peer ID</td>
</tr>
<tr>
<td>keyring local</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>kyr1</td>
<td>apply the keyring created in the step before to the profile</td>
</tr>
</tbody>
</table>

**4.5 IPsec Tunnel configuration**

In order to configure the IPsec part for the responder, type the following commands:

crypto ipsec transform-set trans esp-3des esp-sha-hmac
Mode tunnel

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ipsec transform-set</td>
<td>trans esp-3des esp-sha-hmac</td>
<td>Create an IPsec transform set with a name and encryption/authentication algorithms</td>
</tr>
</tbody>
</table>

4.6 Access List configuration

In order to define which kind of traffic has to be tunnelled, an Access List needs to be configured, typing the following commands:

```
ip access-list extended ikev2list
permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

So, as configured on the TransPort (IPsec Tunnel section), with this ACL we defined that LAN to LAN traffic need to be protected and sent through the tunnel.

4.7 Crypto Map configuration

In Cisco devices, a Crypto Map needs to be configured in order to combine together the settings for IKEv2, IPsec, and traffic that need to be tunneled.

Please note that IOS supports two different types of CMs: static and dynamic. Static CMs are used to define remote peering relationships when all of the variables needed to establish an IPsec peering relationship are known prior to any negotiation between the VPN gateway and the remote peer taking place. Dynamic CMs are used when only some of the remote peer parameters are known prior to negotiation with the VPN gateway. In the case described in this AN, as the Cisco acts as responder, so maybe it doesn't know the other peer IP address, a dynamic map is a good choice.

Also, Dynamic CMs are anchored to a static CM; they are not directly applied to a router interface. The dynamic CM is created with the command: “crypto dynamic-map {dynamic map name} {1-65535}”.

Once created, it is added to the static CM using some options on the static CM command: “crypto map {static map name} {1-65535} {ipsec-isakmp} {dynamic} {dynamic map name}”. A dynamic CM must be created before it can be anchored to the static CM.

In order to configure the Crypto Map, type the following commands:

```
crypto dynamic-map dmap 1
set transform-set trans
```
set ikev2-profile prof
match address ikev2list

! crypto map cmap 1 ipsec-isakmp dynamic dmap
! interface FastEthernet0/1
crypto map cmap

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto dynamic-map</td>
<td>dmap 1</td>
<td>Create the Dynamic Crypto Map and a name</td>
</tr>
<tr>
<td>set transform-set</td>
<td>trans</td>
<td>Apply the IPsec transfor set already created</td>
</tr>
<tr>
<td>set ikev2-profile prof</td>
<td>prof</td>
<td>Apply the IKEv2 profile already created</td>
</tr>
<tr>
<td>match address ikev2list</td>
<td>ikev2list</td>
<td>Apply the access list already created</td>
</tr>
<tr>
<td>crypto map</td>
<td>cmap 1 ipsec-isakmp dynamic dmap</td>
<td>Create a CM to which is applied the DM already created and set it to an IPsec-ISAKMP type</td>
</tr>
<tr>
<td>interface FastEthernet0/1</td>
<td>-</td>
<td>Enter in the WAN Interface Configuration mode</td>
</tr>
<tr>
<td>crypto map</td>
<td>cmap</td>
<td>Apply the Crypto Map to the WAN Interface</td>
</tr>
</tbody>
</table>
5 TESTING

5.1 Debug settings on TransPort

In many cases is very useful configure the device in order to have a debug trace for the IKE negotiation in case of issues of setting up the VPN and for check that the traffic is correctly tunnelled.

On the TransPort, go to Management - Analyser > Settings and change the settings as shown below (uncheck everything else):

![Analyser settings - 1](image)

Figure 5.1-1: Analyser settings - 1
## Parameter | Setting | Description | CLI command
--- | --- | --- | ---
Enable Analyser | Selected | This checkbox is used to enable or disable the analyser. | ana 0 anon ON
Maximum packet capture size | 1500 | The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Common practice is to set it to 1500 | ana 0 maxdata 1500
Log Size | 180 | The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Common practice is to | ana 0 logsize 180
### Parameter | Setting | Description | CLI command
---|---|---|---
Protocol layers | Layer 3 (Network) | Specify which protocol layers are captured and included in the analyser trace. For the purpose of this AN the Network Layer (Layer 3) is chosen | ana 0 l3on
Enable IKE debug | Selected | Used to enable/disable the inclusion of IKE packets in the analyser trace when using IPsec | ana 0 ikeon ON
IP Sources | ETH 0 ETH 1 | Select the IP sources over which packets will be captured and included in the analyser trace | eth 0 ipanon on eth 1 ipanon on
IP Packet Filters / TCP/UDP Ports | ~500,4500 | This parameter is used to filter out TCP or UDP packets with particular source or destination port numbers. In order to filter the IKE negotiation phases, set to 500 and 4500. In order to capture data traffic, leave the field empty | ana 0 ipfilt "~500,4500"

It is also needed to enable the IKE debug under IKE settings ([Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug]):
Figure 5.1-3: Enabling IKE debug
5.2 Debug settings on Cisco

To double check what is going on during testing, it would be good, if possible, to enable some debugs also on Cisco device. In order to do that, please type the following commands:

```
terminal monitor
deb ug crypto ikev2
deb ug crypto ikev2 packet
deb ug crypto ikev2 internal
```

Please note that the first command “Terminal Monitor” is only needed if you connect to the Cisco with Telnet or SSH as, by default, Cisco IOS does not send log messages to a terminal session over IP. Instead, console connections on a serial cable do have logging enabled by default.

5.3 Setting the tunnel UP

As soon as the initiator is configured to set up a VPN, it will try to connect to the responder. For a successful negotiation we should see the following logs

**Initiator (TransPort):**

Going in the eventlog (WEB UI: Management - Event Log) of the device:

```
22:22:30, 05 Mar 2000,(5) IKEv2 Negotiation completed peer, Initiator
22:22:30, 05 Mar 2000, Eroute 0 VPN up peer: cisco1
22:22:30, 05 Mar 2000, New IPSec SA created by cisco1
```

**Responder (Cisco):**

On the terminal monitor should appear the debug, at the end of the negotiation should show the following:

```
*Jul  1 11:05:47.211: IKEv2:[SA ID = 1]:IKEV2 SA created; inserting SA into database. SA lifetime timer (86400 sec) started
*Jul  1 11:05:47.215: IKEv2:[SA ID = 1]:Session with IKE ID PAIR (transport, cisco1) is UP
*Jul  1 11:05:47.219: IKEv2: IKEv2 MIB tunnel started, tunnel index 1
*Jul  1 11:05:47.223: IKEv2:[SA ID = 1]:Load IPSEC key material
*Jul  1 11:05:47.223: IKEv2:[SA ID = 1]:[IPsec -> IPsec] Create IPsec SA into IPsec database
*Jul  1 11:05:47.227: IKEv2:[SA ID = 1]:Asynchronous request queued
*Jul  1 11:05:47.227: IKEv2:[SA ID = 1]:
*Jul  1 11:05:47.263: IKEv2:[SA ID = 1]:[IPsec -> IKEv2] Creation of IPsec SA into IPsec database PASSED
*Jul  1 11:05:47.275: IKEv2:[SA ID = 1]:Checking for duplicate IKEv2 SA
*Jul  1 11:05:47.279: IKEv2:[SA ID = 1]:No duplicate IKEv2 SA found
*Jul  1 11:05:47.283: IKEv2:[SA ID = 1]:Starting timer (8 sec) to delete negotiation context
```
5.4 IPsec SAs status

The status of the IPsec SAs can be verified on the CLI or going to the WEB UI at Administration - Execute a command and type: “sa stat”. The result shows that the IPsec SAs (IKEv2 type) are correctly UP:

IPsec SAs (total:1). Eroute 0 -> 4
Outbound V1 SAs
   List Empty
Inbound V1 SAs
   List Empty

Outbound V2 SAs
   SPI Eroute  Peer IP  First Rem. IP  Last Rem. IP  First Loc. IP  Last Loc. IP  TTL  KBytes Left  VIP
e0889ce1 0  10.10.2.1  172.16.1.0  172.16.1.255  192.168.1.0  192.168.1.255  28664  0    N/A

Inbound V2 SAs
   SPI Eroute  Peer IP  First Rem. IP  Last Rem. IP  First Loc. IP  Last Loc. IP  TTL  KBytes Left  VIP
c9049431 0  10.10.2.1  172.16.1.0  172.16.1.255  192.168.1.0  192.168.1.255  28664  0    N/A

OK

Also in the Cisco device it is possible to check the status of the VON with the following command:

Cisco1#sh cry se de
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: FastEthernet0/1
Uptime: 00:02:41
Session status: UP-ACTIVE
Peer: 10.10.1.1 port 500 fvrf: (none) ivrf: (none)
   Phase1_id: transport
   Desc: (none)
IKEv2 SA: local 10.10.2.1/500 remote 10.10.1.1/500 Active
   Capabilities:(none) connid:1 lifetime:23:57:19
IPSEC FLOW: permit ip 172.16.1.0/255.255.255.0 192.168.1.0/255.255.255.0
Active SAs: 2, origin: dynamic crypto map
   Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4608000/3438
   Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 4608000/3438
5.5 Testing traffic on the tunnel

Once the VPN is UP, in order to test if LAN to LAN traffic is tunnelled as configured, do a ping from an address in the Initiator LAN and an address in the responder LAN.

Looking at the trace on the initiator (Management - Analyser > Trace):

1) An ICMP ECHO REQUEST arrives on ETH 0 from 192.168.1.100:

```
----- 5-3-2000 22:26:02.370 ------
45 00 00 3C 01 D3 00 00 80 01 C9 D0 C0 A8 01 64  E..&lt;..........d
AC 10 01 01 08 00 4D 51 00 01 00 0A 61 62 63 64  ......MQ....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69  uvwbcdefghi
```

<table>
<thead>
<tr>
<th>IP (In) From REM TO LOC</th>
<th>IFACE: ETH 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>IP Ver: 4</td>
</tr>
<tr>
<td>00</td>
<td>Hdr Len: 20</td>
</tr>
<tr>
<td>00</td>
<td>TOS: Routine</td>
</tr>
<tr>
<td>00</td>
<td>Delay: Normal</td>
</tr>
<tr>
<td>00</td>
<td>Throughput: Normal</td>
</tr>
<tr>
<td>3C</td>
<td>Reliability: Normal</td>
</tr>
<tr>
<td>00</td>
<td>Length: 60</td>
</tr>
<tr>
<td>01</td>
<td>ID: 467</td>
</tr>
<tr>
<td>00</td>
<td>Frag Offset: 0</td>
</tr>
<tr>
<td>80</td>
<td>Congestion: Normal</td>
</tr>
<tr>
<td>01</td>
<td>May Fragment</td>
</tr>
<tr>
<td>00</td>
<td>Last Fragment</td>
</tr>
<tr>
<td>C9 D0</td>
<td>TTL: 128</td>
</tr>
<tr>
<td>C0 A8 01 64</td>
<td>Proto: ICMP</td>
</tr>
<tr>
<td>AC 10 01 01</td>
<td>Src IP: 192.168.1.100</td>
</tr>
<tr>
<td>AC 10 01 01</td>
<td>Dst IP: 172.16.1.1</td>
</tr>
<tr>
<td>08</td>
<td>ICMP: ECHO REQ</td>
</tr>
<tr>
<td>00</td>
<td>Code: 0</td>
</tr>
<tr>
<td>4D 51</td>
<td>Checksum: 51664</td>
</tr>
</tbody>
</table>

```
2) The packet matches the IPsec tunnel 0:
```

```
----- 5-3-2000 22:26:02.370 ------
45 00 00 3C 01 D3 00 00 7F 01 CA D0 C0 A8 01 64  E..&lt;..........d
AC 10 01 01 08 00 4D 51 00 01 00 0A 61 62 63 64  ......MQ....abcd
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74  efgijklmnopqrst
75 76 77 61 62 63 64 65 66 67 68 69  uvwbcdefghi
```

<table>
<thead>
<tr>
<th>ER 0-cisco1 From LOC TO REM</th>
<th>IFACE: ETH 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>IP Ver: 4</td>
</tr>
<tr>
<td>00</td>
<td>Hdr Len: 20</td>
</tr>
<tr>
<td>00</td>
<td>TOS: Routine</td>
</tr>
<tr>
<td>00</td>
<td>Delay: Normal</td>
</tr>
<tr>
<td>00</td>
<td>Throughput: Normal</td>
</tr>
</tbody>
</table>
3) The packet is then encrypted and sent through the tunnel with source 10.10.1.1 (initiator WAN address) and destination 10.10.2.1 (responder WAN address)

4) An ESP packet arrives on interface ETH 1 from 10.10.2.1 directed to 10.10.1.1:
5) The packet is decrypted, revealing the ICMP ECHO REPLY from 172.16.1.1 to 192.168.1.100:

5-3-2000 22:26:02.440 ------
45 00 00 3C 01 D3 00 00 FF 01 4A D0 AC 10 01 01 E..&lt;......J....
65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrstuvwxyz
5-3-2000 22:26:02.440 ------
45 00 00 00 70 00 00 00 00 00 FE 32 A5 39 0A 0A 02 01 E..p......2.9....
0A 0A 01 01 C9 04 94 31 00 00 00 00 02 34 16 73 89 ..........I....T.s.
57 1E 0A 62 6F A9 42 49 46 6D F6 8D F7 8D 85 30 FC W..bo.B.Om.x..0.
3E 6A DF 17 BE 61 25 31 AD AD DE 1F BE 01 18 93 &gt;j...a%1.......}
58 75 99 ED 50 1A 33 4D FF 75 88 6B AD 5B 22 96 Xu..P.3M.u.k.".
ED 99 8C 91 D5 8A 51 8D 3D CF 02 36 94 F8 70 13 ......Q.=..6..p.
6) The ECHO REPLY is then sent out through the ETH 0 interface to the destination host:

```
    5-3-2000 22:26:02.440 -------
    45 00 00 3C 01 D3 00 00 0E 01 4B D0 AC 10 01 01 E...K...
    C0 A8 01 64 00 00 55 51 00 01 00 0A 61 62 63 64 ...abcd
    65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 efghijklmnopqrst
    75 76 77 61 62 63 64 65 66 67 68 69 uvwabcdefghi
```

```
IP (Final) From LOC TO REM IFACE: ETH 0
45 IP Ver:  4
Hdr Len:  20
00 TOS:  Routine
Delay:  Normal
Throughput:  Normal
Reliability:  Normal
00 3C Length:  60
01 D3 ID:  467
00 00 Frag Offset:  0
Congestion:  Normal
May Fragment
Last Fragment
FE TTL:  254
01 Proto:  ICMP
4B D0 Checksum:  19408
AC 10 01 01 Src IP:  172.16.1.1
C0 A8 01 64 Dst IP:  192.168.1.100
ICMP:
00 Type:  ECHO REPLY
00 Code:  0
55 51 Checksum:  21841
```
6  CONFIGURATION FILE

6.1  Initiator (TransPort) Configuration File

This is the configuration used on the Initiator (TransPort) in this Application Note:

```
'config c show'
eth 0 descr "Transport LAN"
eth 0 IPaddr "192.168.1.1"
eth 0 ipanon ON
eth 1 descr "Transport WAN"
eth 1 IPaddr "10.10.1.1"
eth 1 ipsec 1
eth 1 ipanon ON
eth 4 mask ""
eth 5 mask ""
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
ip 0 cidr ON
route 0 mask ""
route 1 mask ""
route 2 mask ""
route 10 mask ""
route 11 mask ""
def_route 0 gateway "10.10.1.3"
def_route 0 ll_ent "eth"
def_route 0 ll_add 1
eroute 0 descr "VPN to Cisco"
eroute 0 peerip "10.10.2.1"
eroute 0 peerid "cisco1"
eroute 0 ourid "transport"
eroute 0 locip "192.168.1.0"
eroute 0 locmsk "255.255.255.0"
eroute 0 remip "172.16.1.0"
eroute 0 remmsk "255.255.255.0"
eroute 0 ESPauth "SHA1"
eroute 0 ESPenc "3DES"
eroute 0 authmeth "PRESHARED"
eroute 0 nosa "try"
eroute 0 autosa 2
route 0 ikever 2
eroute 0 dhgroup 2
eroute 0 debug ON
eroute 1 autosa 2
dhcp 0 IPmin "192.168.1.100"
```
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "192.168.1.1"
ppp 0 timeout 300
ppp 1 name "W-WAN (HSPA 3G)"
ppp 1 phonenum "*98*1#"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 use_modem 1
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 deblevel 4
ike2 0 iencalgs "AES"
ike2 0 iencalgs "AES"
ike2 0 idhgroup 2
ike2 0 raulcalgs "MD5,SHA1"
ike2 0 raulcalgs "MD5,SHA1"
ike2 0 rauthalgs "MD5,SHA1"
ike2 0 rauthalgs "MD5,SHA1"
ike2 0 rencalgs "DES,3DES,AES"
ike2 0 rencalgs "DES,3DES,AES"
ike2 0 renckeybits 128
ike2 0 renckeybits 128
modemcc 0 info_asy_add 7
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "Your.APN.goes.here"
modemcc 0 link_retries 10
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 init_str_2 "+CGQREQ=1"
modemcc 0 init_str1_2 "+CGQMIN=1"
modemcc 0 apn_2 "Your.APN.goes.here"
modemcc 0 link_retries_2 10
modemcc 0 stat_retries_2 30
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipfilt "~500,4500"
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "wr44"
cmd 0 asyled_mode 1
cmd 0 anonftp ON
cmd 0 asy_listen 8002
cmd 0 tremto 1200
cmd 0 rcihttp ON
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVWg=
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
user 9 access 0
user 10 name "cisco1"
user 10 epassword "PDZxU0FFQFU=
user 10 access 4
user 11 name "transport"
user 11 epassword "PDZxU0FFQFU=
user 11 access 4
user 12 epassword "PDZxU0FFQFU=
user 12 access 4
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "privrsa.pem"
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
tun 0 mask ""
cloud 0 ssl ON
OK
6.2 Responder (Cisco) Configuration File

This is the configuration used on the Responder (Cisco) in this Application Note:

```
Cisco1# sh run
Building configuration...

Current configuration : 1669 bytes
|
! Last configuration change at 11:00:08 UTC Tue Jul 1 2014
|
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
|
hostname Cisco1
|
boot-start-marker
boot-end-marker
|
|
no aaa new-model
no ip icmp rate-limit unreachable
|
|
|
|
no ip domain lookup
ip cef
no ipv6 cef
|
|
multilink bundle-name authenticated
|
|
|
|
|
crypto ikev2 proposal proposal1
  encryption aes-cbc-128
  integrity sha1
  group 2
|
crypto ikev2 policy policy1
  proposal proposal1
|
crypto ikev2 keyring kyr1
  peer transport
```
identity key-id transport
pre-shared-key digidigi
!

crypto ikev2 profile prof
match identity remote key-id transport
identity local key-id cisco1
authentication remote pre-share
authentication local pre-share
keyring local kyr1
!

ip tcp synwait-time 5
!

crypto ipsec transform-set trans esp-3des esp-sha-hmac
mode tunnel
!

crypto dynamic-map dmap 1
set transform-set trans
set ikev2-profile prof
match address ikev2list
!

crypto map cmap 1 ipsec-isakmp dynamic dmap
!

interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
speed auto
duplex auto

interface FastEthernet0/1
ip address 10.10.2.1 255.255.255.0
speed auto
duplex auto
crypto map cmap

ip forward-protocol nd
!

no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.2.3

ip access-list extended ikev2list
permit ip 172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255

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
  login

end