Application Note 36

IPsec between Digi TransPort and Cisco ASA 5505 using Cisco EasyVPN (XAUTH and MODECFG)

UK Support

November 2015

CONTENTS

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. The following article explains some of the reasons why: http://isp-ceo.net/technology/remote_access_conundrum-1-1.html

1.1 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 ASA 5505 running ASA OS version 8.4(2). It is therefore possible to configure the TransPort to connect to an ASA 5505 using XAUTH and MODECFG, in a similar manner to the Cisco VPN Client.

The configuration suggested in this Application Note should also work on an ASA 5510, 5520, 5540, 5550, 5580 or 5585-X running ASA OS version 8.4(2) without modification, according to the table below, which is from the following Cisco resource:
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

ASA OS	ASDM	ASA Model:						
		ASA 5505	ASA 5510, 5520, 5540	ASA 5550	ASA 5580	ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	ASA 5585-X	ASASM
ASA 8.4(2)	ASDM 6.4(5) and later. *Recommended: 6.4(9).*	**YES**	**YES**	**YES**	**YES**	No	**YES**	No

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 ASA 5505) 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 (see section 1.3 below). 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.

1.2 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.

1.3 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 (ASA 5505) to assign a single IP address to the client (TransPort WR44) which must be used as the source address for all traffic traversing the IPsec tunnel from the client side.

In order to allow access to devices on the LAN side of the TransPort from the ASA side, it is necessary to configure TCP/UDP port forwarding, also know as static NAT mappings, on the TransPort. Information on setting up static NAT mappings is contained in section 2.7.

1.4 IPsec encryption parameters

Throughout this document, the following IPsec parameters have been used:

IKE

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Lifetime Duration: 86400 seconds (24 hours)

MODP/DH/PFS: Group 2

IPsec

ESP Encryption Algorithm: 3DES

ESP Authentication Algorithm: MD5

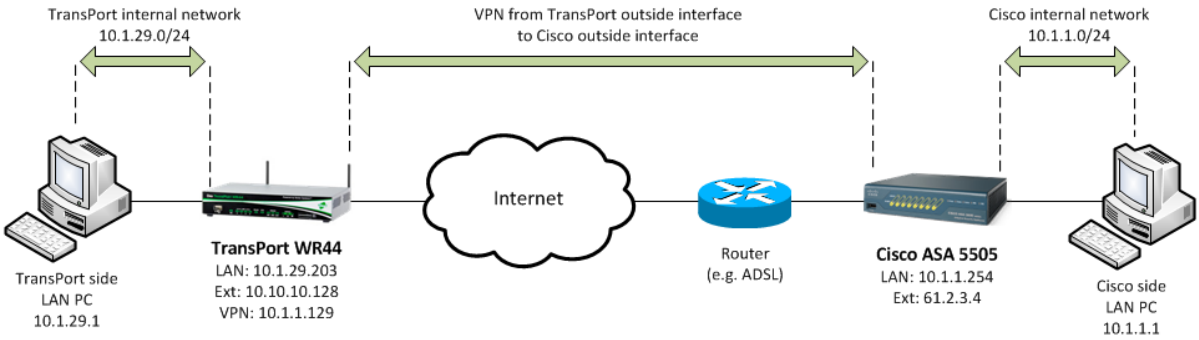
Lifetime Duration: 86400 seconds (24 hours)

Lifetime Duration: 0 bytes (Not Used)

Other parameters may be available according to software version, hardware version and licensing (for example DES, AES, etc. for encryption) depending on user requirements. Parameters must match on both the ASA and the TransPort in order for the VPN to be established correctly.

1.5 Network diagram and explanation of IP addressing

The test network used in producing this document is shown in the following diagram:



Some of the real IP addresses used for testing have been altered within this document: the Cisco's public IP address is shown as 61.2.3.4, and the TransPort's cellular IP address is shown as 10.10.10.128. The TransPort WR44 in this example uses a cellular connection as its WAN interface, so it will usually be allocated a private-range IP address by the mobile network (changed in this document to 10.10.10.128), which is translated by NAT to an internet-routable public IP address at the edge of the mobile network. It is the public IP address that is seen by the ASA, but it will not appear in any TransPort debug or logging, since the only WAN IP address that the TransPort is aware of is the private one. The TransPort's public IP address provided at the mobile network edge is shown in this document as <TransPort_public_IP>.

1.6 Assumptions and notes

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.
The version of the web interface shown in the TransPort configuration screenshots assumes that the TransPort is running firmware revision 5.123 or newer.

For hardware and firmware information relating to the TransPort WR44 and the Cisco ASA 5505 used during the testing of this Application Note, as well as full configuration listings, see section 4 towards the end of the document.

Throughout this document the TransPort WR44 router is generally referred to simply as the TransPort. The Cisco ASA 5505 is generally referred to as Cisco or ASA.

As in the wider networking community, ISAKMP and IKE are used interchangeably in this document to refer to the phase 1 stage of the IPsec VPN negotiation process. However it should be noted that, strictly speaking, they are two separate protocols. The difference can essentially be described as follows: ISAKMP provides a framework for authentication and cryptographic key exchange within an internet environment, whereas IKE provides authenticated keying material for use with ISAKMP.

1.7 Corrections

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

1.8 Version

Version Number	Status
1.0	Published
2.0	Updated for new TransPort and Cisco firmware versions

1.9 Acknowledgements

We are very grateful to David Carter from IPI for his assistance in creating this application note.

2 CONFIGURATION

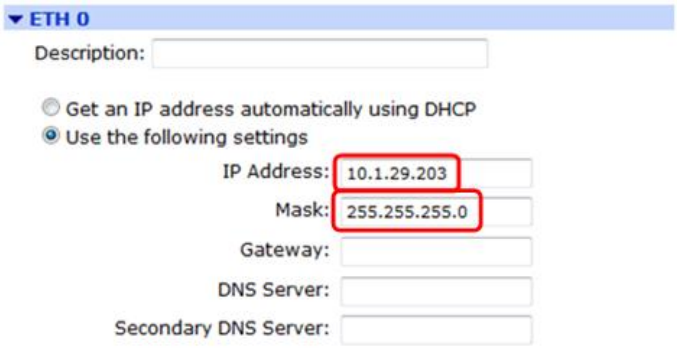
2.1 TransPort configuration

Log into the TransPort's web interface with a super level user. The configuration steps shown below assume that the TransPort is starting with a factory default configuration. Remember to save the config during and after the configuration steps below, to ensure nothing is lost during reboot.

2.2 Configure LAN interface

Navigate to **Configuration - Network > Interfaces > Ethernet > ETH 0**

Allocate an IP address to the local Ethernet interface:

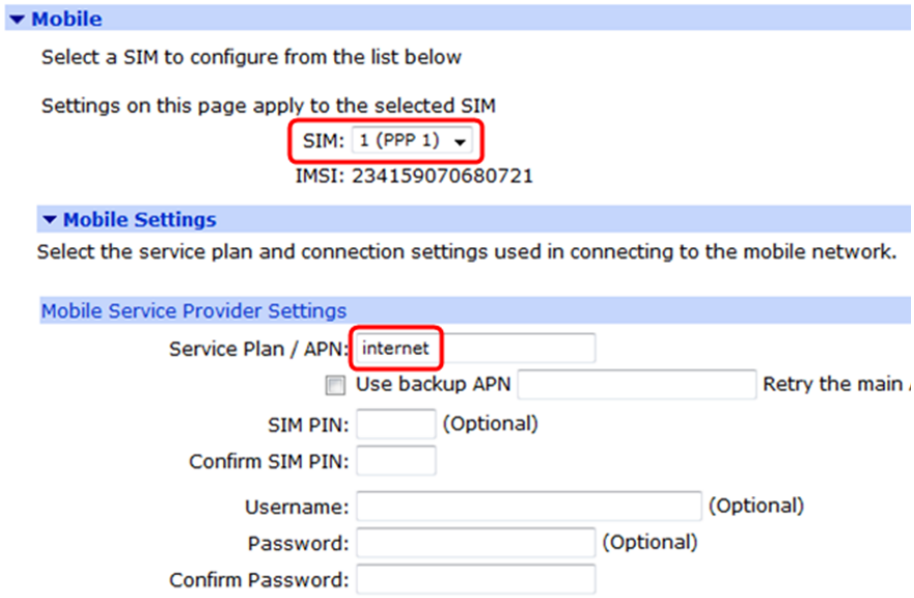


Parameter	Setting	Description
IP Address	10.1.29.203	IP address for ETH 0
Mask	255.255.255.0	Mask for ETH 0

2.3 Configure cellular WAN interface

Navigate to **Configuration - Network > Interfaces > Mobile**

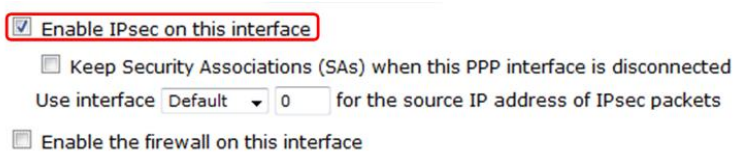
Configure the cellular connection. Ensure that from the “SIM:” drop down list, “1 (PPP 1)” is selected.This example uses a Vodafone SIM, so the Vodafone APN “internet” is used here:



Parameter	Setting	Description
APN	internet	Enter the APN for the mobile provider

Navigate to **Configuration - Network > Interfaces > Advanced > PPP 1**

Enable IPsec on the cellular interface:

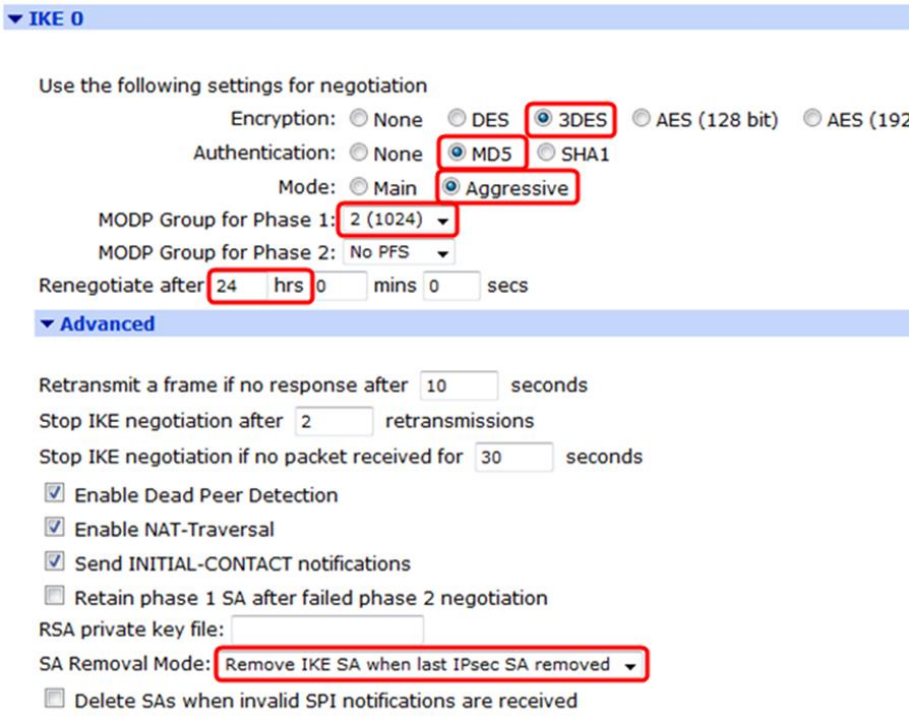


Parameter	Setting	Description
Enable IPsec on this interface	Ticked	Enables IPsec

2.4 Configure IKE

Navigate to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0**

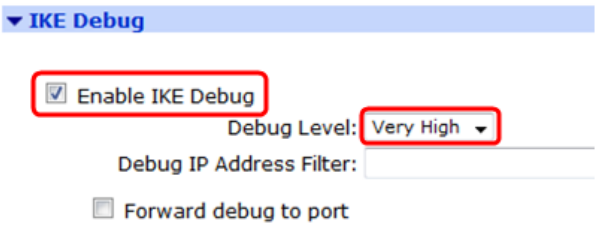
Next the phase 1 IKE key management and tunnel initialisation settings are configured here:



Parameter	Setting	Description
Encryption	3DES	Encryption algorithm
Authentication	MD5	Authentication hashing algorithm
Mode	Aggressive	Needed for EasyVPN connection to Cisco ASA
MODP Group for Phase 1	2 (1024)	Modular exponential (Diffie-Hellman) group
Renegotiate after	24 hrs	Lifetime
SA Removal Mode	Remove IKE SA when last IPsec SA removed	Ensures the IKE SA is removed when the last IPsec SA is removed

Navigate to **Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE Debug**

Enable detailed logging in case of any problems with the VPN negotiation process:

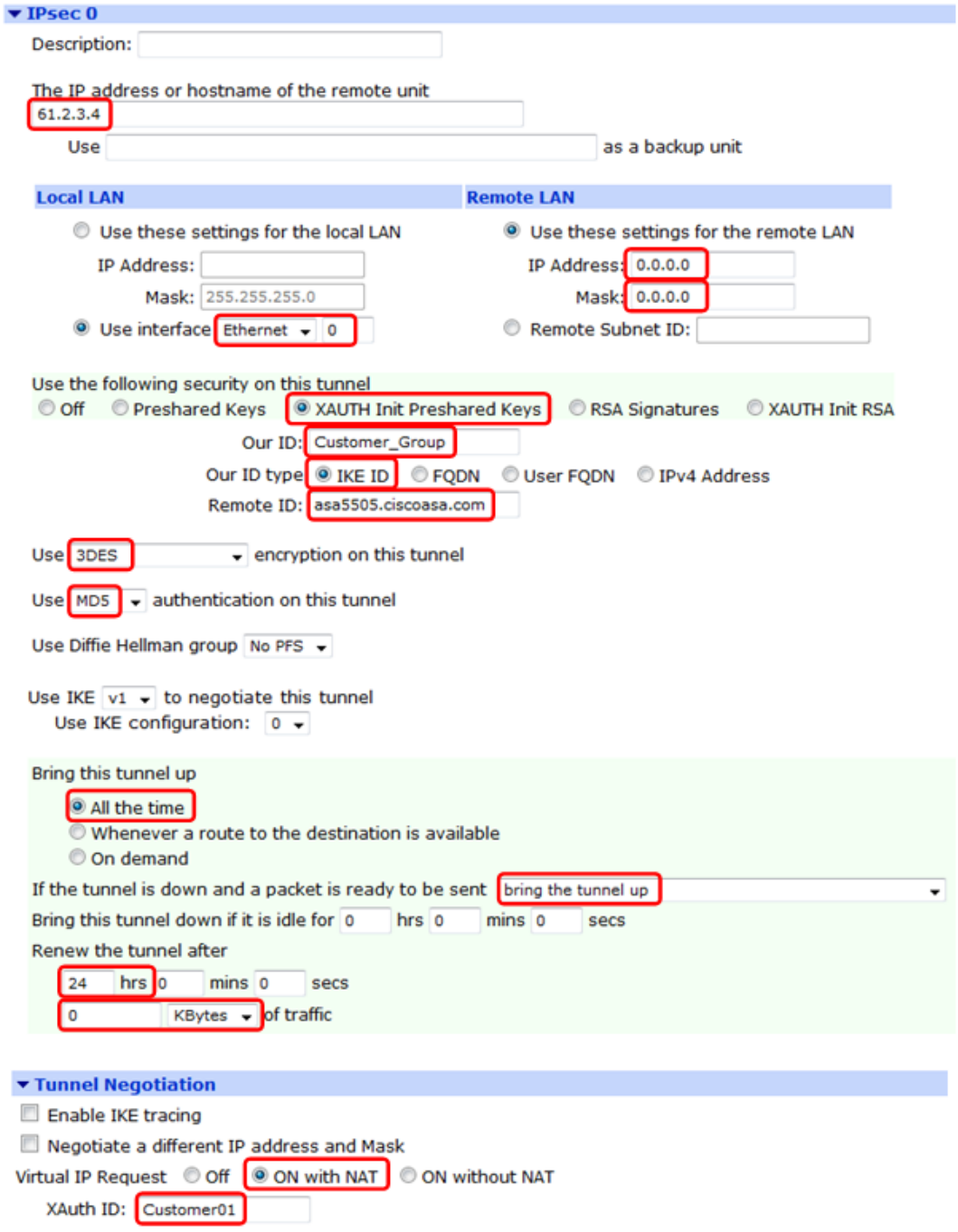


Parameter	Setting	Description
Enable IKE Debug	Ticked	Enables IKE debug
Debug Level	Very High	Enables detailed logging

2.5 Configure IPsec

Navigate to:
Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0

In this section the phase 2, MODECFG and XAUTH parameters are configured. As the TransPort router is the VPN initiator, the public IP address of the Cisco ASA (VPN responder) is used as the peer IP.

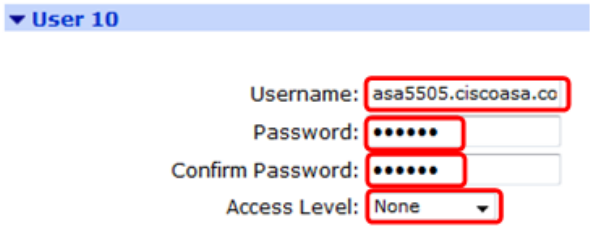

IPsec 0
Description:
The IP address or hostname of the remote unit
61.2.3.4
Use
as a backup unit
Local LAN
Remote LAN
Use these settings for the local LAN
Use these settings for the remote LAN
IP Address:
IP Address: 0.0.0.0
Mask: 255.255.255.0
Mask: 0.0.0.0
Use interface Ethernet 0
Remote Subnet ID:
Use the following security on this tunnel
Off
Preshared Keys
XAUTH Init Preshared Keys
RSA Signatures
XAUTH Init RSA
Our ID: Customer_Group
Our ID type IKE ID
FQDN
User FQDN
IPv4 Address
Remote ID: asa5505.ciscoasa.com
Use 3DES encryption on this tunnel
Use MD5 authentication on this tunnel
Use Diffie Hellman group No PFS
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0
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
24 hrs 0 mins 0 secs
0 KBytes of traffic
Tunnel Negotiation
Enable IKE tracing
Negotiate a different IP address and Mask
Virtual IP Request Off ON with NAT ON without NAT
XAuth ID: Customer01

Parameter	Setting	Description
The IP address or hostname of the remote unit	61.2.3.4	External IP of the Cisco ASA
Local LAN interface	Ethernet 0	The interface to use for the source of all encrypted traffic. Encrypt traffic that has source IP matching this network or subnet address, and destination IP matching the remote LAN
Remote LAN IP address	0.0.0.0	Network address of the remote network to be routed to via the IPsec tunnel. Encrypt traffic that has destination IP matching this network or subnet address, and source IP matching the local LAN
Remote LAN mask	0.0.0.0	Network mask for the remote network above
Use the following security on this tunnel	XAUTH Init Preshared Keys	"XAUTH Init Preshared Keys" instructs the TransPort to attempt XAUTH with the ASA using pre-shared keys
Our ID	Customer_Group	Group name matching the vpngroup on the ASA
Our ID type	IKE ID	Ensure our ID type is set to IKE ID
Remote ID	asa5505.ciscoasa.com	Full hostname of the ASA – must match hostname.domainname in ASA configuration
ESP encryption algorithm	3DES	Select a value from the list – must match the encryption algorithm used in the ASA config
ESP authentication algorithm	MD5	Select a value from the list – must match the authentication algorithm used in the ASA config
Bring this tunnel up	All the time	Select a value from the list - in this example select "All the time". This effectively creates an "always on" IPsec tunnel
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	Select a value from the list - in this example select "Bring the tunnel up". If the router receives a request to route a packet that matches an IPsec tunnel definition, it will try to initiate an IKE session to establish SAs
Renew this tunnel after	24 hrs	Configure the lifetime of the link; again this must match with the value in the ASA. The IPsec SAs will be renewed when ¾ of this time has expired
Renew this tunnel after	0 KBytes	The IPsec SAs will be renewed when this much data has been transferred (0 = disabled)
Virtual IP Request	ON with NAT	Allows the remote ASA to assign the TransPort an IP address using MODECFG
XAuth ID	Customer01	XAUTH username

2.6 Configure users

Navigate to **Configuration - Security > Users > User 10 - 14 > User 10**

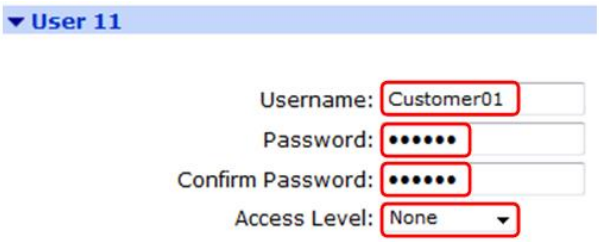
Here the pre-shared key is configured using the hostname of the ASA. The username value should therefore match the Peer ID set in the IPsec configuration above:



Parameter	Setting	Description
Name	asa5505.ciscoasa.com	Enter the fully qualified hostname of the ASA
Password	digigroup	Enter the ASA vpn_group password
Access Level	None	As this user is only for the pre-shared key, no access will be granted to the router for this username

Navigate to **Configuration - Security > Users > User 10 - 14 > User 11**

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:



Parameter	Setting	Description
Name	Customer01	Enter the XAUTH username which must be the same as the XAUTH ID configured in the IPsec tunnel instance
Password	Customer01p455	Enter XAUTH password
Access Level	None	As this user is only for the group, no access will be granted to the router for this username

2.7 Configure static Nat mappings

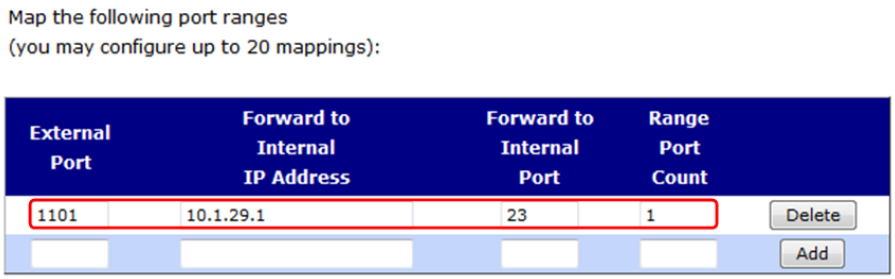
Navigate to:

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > MODECFG Static NAT mappings

If the TransPort receives a packet from its local interface that needs to be routed through the IPsec tunnel, it performs Network Address Translation (NAT) so that the source address matches the virtual IP address that has been assigned by the Cisco, before encrypting the packet using the negotiated IPsec SA. Some state information is retained, so that a reply packet coming in the opposite direction from the Cisco can have its destination address changed back to the source addresses of the original packet (in the same way as standard NAT), so that the reply packet can find its way back to the host that initiated the original packet.

If the remote (Cisco) end of the IPsec tunnel is to be able to access units connected to the TransPort's local interface, the TransPort unit needs to have one or more "static NAT mappings" configured. When a packet is received through the tunnel, the TransPort will first look up existing stateful NAT entries, followed by static NAT entries, to see if the destination address and/or port should be modified, then forwards the packet to the new address/port. If a static NAT mapping is found, the unit creates a dynamic NAT entry that will be retained for the duration of the connection. If no dynamic or stateful entry is found, the packet is directed to the local protocol handlers.

For example, the mapping below will configure the TransPort to forward packets with destination port 1101 to the PC behind it at 10.1.29.1, and to also change the destination port to 23 (Telnet):

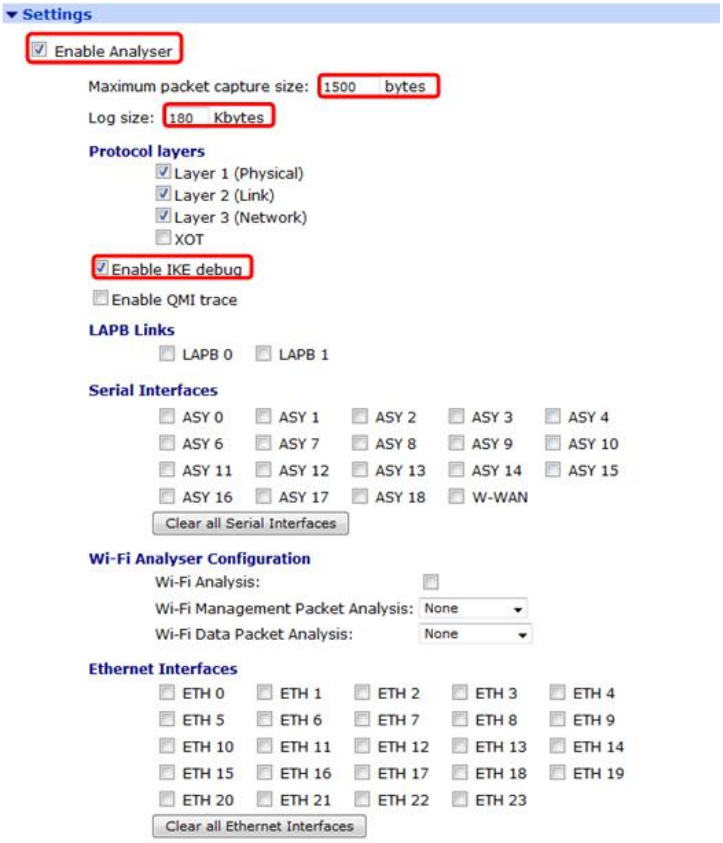


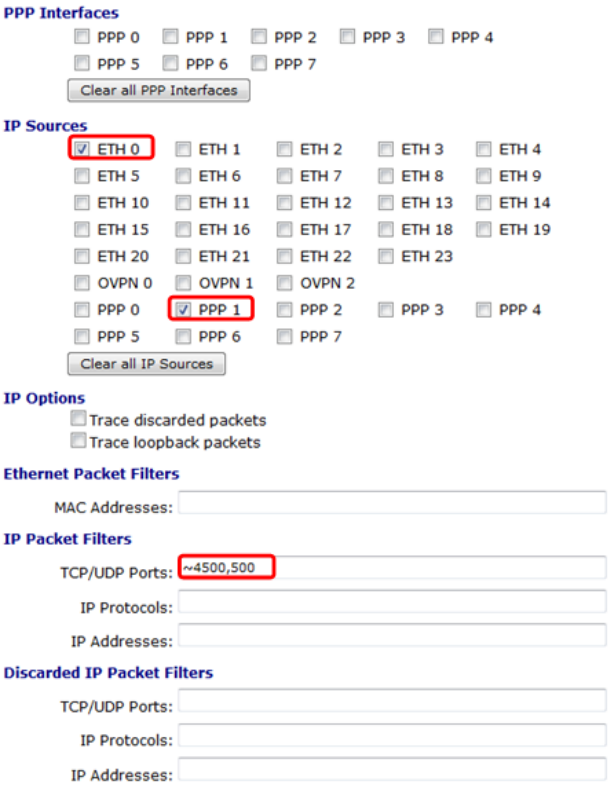
Parameter	Setting	Description
External Port	1101	Enter the lowest destination port number to be matched if a packet is to be redirected
Forward to Internal IP Address	10.1.29.1	Enter an IP address to which packets containing the specified destination port number are to be redirected
Forward to Internal Port	23	Enter a port number to which packets containing the specified destination port number are to be redirected
Range Port Count	1	Enter the number of ports to be matched

2.8 Configure analyser

Management - Analyser > Settings

The following settings will allow visibility of the IKE and IPsec packets in the analyser trace. If there are any problems with the VPN negotiation process, the analyser trace can be checked to find the cause of the problem. Clear any settings not shown here:




PPP Interfaces
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all PPP Interfaces
IP Sources
ETH 0
ETH 1
ETH 2
ETH 3
ETH 4
ETH 5
ETH 6
ETH 7
ETH 8
ETH 9
ETH 10
ETH 11
ETH 12
ETH 13
ETH 14
ETH 15
ETH 16
ETH 17
ETH 18
ETH 19
ETH 20
ETH 21
ETH 22
ETH 23
OVPN 0
OVPN 1
OVPN 2
PPP 0
PPP 1
PPP 2
PPP 3
PPP 4
PPP 5
PPP 6
PPP 7
Clear all IP Sources
IP Options
Trace discarded packets
Trace loopback packets
Ethernet Packet Filters
MAC Addresses:
IP Packet Filters
TCP/UDP Ports:
~4500,500
IP Protocols:
IP Addresses:
Discarded IP Packet Filters
TCP/UDP Ports:
IP Protocols:
IP Addresses:

Parameter	Setting	Description
Enable Analyser	Ticked	Enable logging to the analyser trace
Maximum packet capture size	1500 bytes	Set to largest possible packet capture size
Log size	180 Kbytes	Set to largest possible log size
Enable IKE debug	Ticked	Enable IKE debug in the analyser trace
IP Source	ETH 0	Enable logging for the LAN interface
IP Source	PPP 1	Enable logging for the WAN interface
IP Packet Filters > TCP/UDP Ports	~4500,500	Restrict the ports logged to show only those related to IKE and IPsec

The TransPort configuration is now complete.

Remember to save the configuration to ensure that nothing is lost on reboot.

2.9 Cisco ASA configuration

The following will assume that the Cisco ASA is a model 5505 running firmware version 8.4, that it is not currently in service and that it has been reset to factory defaults.

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

For reference the following Cisco resource explains how to configure the ASA 5500 series running firmware version 8.4 via the command line interface:
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/asa_84_cli_config.html

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.

2.10 Configure the login and enable passwords

Enter enable mode (default password is blank, i.e. simply press enter when prompted):

```
en
```

Enter configure mode:

```
conf t
```

Configure passwords:

```
passwd myloginpassword
enable password mysecret
```

2.11 Configure basic routing

Configure the outside (WAN) interface:

```
int eth0/0
no shut
switchport access vlan 11
int vlan 11
nameif outside
ip address 61.2.3.4 255.255.255.252
```

Configure the inside (LAN) interface:

```
int eth0/1
no shut
switchport access vlan 1
int vlan 1
nameif inside
ip address 10.1.1.254 255.255.255.0
```

The ASA will automatically assign a security level of “0” to an interface named “outside”, and “100” to an interface named “inside”. The security level defines how secure that network is, 0 being the lowest and 100 being a secure trusted network. This is important, as this affects the flow of data from and to the various interfaces. Data can always flow from an interface that has a higher security level than the interface that it’s going to pass through. In other words the inside network can always pass data to the outside network, due to the security level of the internal network being higher than that of the external network.

Assign a Hostname and Domain Name:

```
hostname asa5505
domain-name ciscoasa.com
```

If a registered domain name for the Cisco’s IP address does not exist, then these parameters can be anything. They are important as they will constitute the Host ID that is transmitted to the TransPort

during the IKE negotiations - the Host ID is linked to the pre-shared keys. <hostname>.<domain.name> should be the same as the username configured in the TransPort for the pre-shared key user.

Configure the default route, which in this example points to an ADSL Router via the “outside” interface:

```
route outside 0.0.0.0 0.0.0.0 192.168.25.254
```

2.12 Configure access lists

The following access list permits traffic to be sent from the 10.1.1.x network, via the IPsec tunnel, to the 10.1.2.x network:

```
access-list inside_outbound_nat0_acl permit ip any 10.1.1.128 255.255.255.240

access-list inside_outbound_nat0_acl deny ip any any
```

An additional access list is required to allow peers to connect using the vpngroup – this is set to any hosts with a permit all access list:

```
access-list Customer_Permitted_Connection permit ip any any
```

Permit connections between the dial-up VPN users and others on the private network:

```
access-list inside_access_in permit ip 10.1.1.0 255.255.255.0 10.1.1.128 255.255.255.240
```

Permit icmp for testing:

```
access-list outside_access_in permit icmp any any

icmp permit any inside
```

Assign access lists to the internal and outside interfaces:

```
access-group outside_access_in in interface outside

access-group inside_access_in in interface inside
```

2.13 Configure NAT

Enable NAT for the “VPN network”. Outbound non-VPN traffic will not have NAT applied:

```
object network obj_vpn

subnet 10.1.1.128 255.255.255.240

nat (any,outside) source static any any destination static obj_vpn obj_vpn
```

```
object network obj_any

subnet 0.0.0.0 0.0.0.0

nat (inside,outside) dynamic interface
```

2.14 Configure IKE/ISAKMP

Enable IKE on the outside interface:

```
isakmp enable outside
```

Enable NAT-traversal. NAT-traversal permits ESP packets to traverse more easily in networks where NAT is used:

```
isakmp nat-traversal 20
```

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.

Specify pre-shared keys as the authentication method:

```
isakmp policy 10 authentication pre-share
```

Specify an encryption method for the IKE negotiations:

```
isakmp policy 10 encryption 3des
```

Specify an authentication algorithm for the IKE negotiations:

```
isakmp policy 10 hash md5
```

Specify a MODP (Diffie-Hellman) group for the IKE negotiations:

```
isakmp policy 10 group 2
```

Specify a key lifetime:

```
isakmp policy 10 lifetime 86400
```

Configure the ASA to use <hostname>.<domain-name> as its IKE ID during negotiations:

```
crypto isakmp identity hostname
```

Enable debugging:

```
debug crypto ikev1 5
```

2.15 Configure IPsec

Configure a transform set for the IPsec security association:

```
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
```

Create a dynamic crypto map entry:

```
crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-MD5
```

Create a crypto map entry:

```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
```

Specify the identifying interface to be used by the ASA to identify itself to peers:

```
crypto map outside_map interface outside
```

Permit all inbound IPsec authenticated cipher sessions. This allows IPsec traffic to pass through the ASA:

```
sysopt connection permit-ipsec
```

Enable debugging:

```
debug crypto ipsec 5
```

2.16 Configure VPN group

Specify the pool of IP addresses that will be allocated to IPsec VPN users. Addresses in the pool should be in the same range as the internal interface, and there should be enough addresses to allocate to each of the sites required to connect to the ASA:

```
ip local pool Customer_Address_Pool 10.1.1.129-10.1.1.134
```

Allocate this pool to a VPN group, and configure the password for the VPN group:

```
tunnel-group Customer_Group type ipsec-ra

tunnel-group Customer_Group general-attributes

address-pool Customer_Address_Pool

tunnel-group Customer_Group ipsec-attributes

pre-shared-key digigroup
```

“Split tunnelling” on the Cisco will allow access to the network specified by the access-list via the IPsec tunnel, whilst all other traffic will be sent in the clear. For example this could be used to encrypt all intranet traffic, and leave all internet traffic in the clear, thus reducing overhead. If split tunnelling is not used, then any traffic not destined for the target network will be dropped. In this example the access list includes all IP traffic to be encrypted:

```
group-policy DfltGrpPolicy attributes

split-tunnel-policy tunnelspecified

split-tunnel-network-list value Customer_Permitted_Connection
```

2.17 Configure user authentication

Set up a username for authentication:

```
username Customer01 password Customer01p455 privilege 2
```

2.18 Save the configuration

Save the configuration to flash memory:

```
write mem
```

The ASA configuration is now complete.

3 TESTING

3.1 Ping a node on the remote (ASA) network from the TransPort's LAN

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

For the test network shown in section 1.5, the PC at 10.1.29.1 on the TransPort's LAN needs to have a route to 10.1.1.1 (the PC on the ASA's LAN) via the TransPort at 10.1.29.203, or the TransPort will need to be configured as its network gateway.

To add an appropriate route to the PC on the TransPort side (assuming it is running Windows), open a command prompt then issue the command:

```
route add 10.1.1.1 10.1.29.203
```

The local PC on the TransPort network will also need to know how to get to 10.1.29.203. In this example the PC is on the same subnet with IP address 10.1.29.1 and the subnet mask is 255.255.255.0 which matches the TransPort.

Usually it will not be possible to ping-test the internal interface of the ASA. A PC or other device on the LAN side of the ASA will need to be configured for testing purposes.

The PC on the ASA's internal network will need to be configured with the IP address 10.1.1.1 so that it can respond to test traffic sent over the VPN.

Check that the ASA can ping the 10.1.1.1 node.

To test the VPN, ping 10.1.1.1 from the TransPort side PC, for example the following shows a successful ping over the IPsec tunnel from the Windows command prompt on the TransPort side PC:

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=2100ms TTL=126
Reply from 10.1.1.1: bytes=32 time=95ms TTL=126
Reply from 10.1.1.1: bytes=32 time=110ms TTL=126
Reply from 10.1.1.1: bytes=32 time=104ms TTL=126

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 95ms, Maximum = 2100ms, Average = 602ms
```

Check the event logs to verify that the traffic actually traversed the link, but this simple test should show that traffic from the PC on the TransPort side was received by the TransPort, that the TransPort encapsulated the traffic within the IPsec tunnel to the ASA, and that the traffic also traversed the same

VPN link back to the originating PC on the TransPort side.

More detailed logging can be seen in an analyser trace on the TransPort, where the traffic can be seen to come into the Ethernet port destined for 10.1.1.1, and can then be seen to be sent to the ASA in encapsulated form “through the IPsec tunnel”. The reply from the ASA is received, decrypted and re-sent out of the Ethernet port to the original requesting PC.

To change the TransPort’s analyser settings so that instead of capturing IKE and IPsec packets, ping packets are captured, assuming the analyser has already been configured as described in section 2.8, remove the entry “~4500,500” from the field “IP Packet Filters > TCP/UDP Ports" and add the entry “~1” (without the quotes) to the field “IP Packet Filters > IP Protocols”.

3.2 Test static NAT mapping

A test can be made from a node on the Cisco network to show that the static mapping is working. In this example port 1101 is mapped to port 23 (Telnet), and a Telnet server is running on the TransPort side PC to respond to traffic from the Cisco side PC. In general when testing a service, ensure that there is a node on the TransPort local network answering on the port and IP address that is being redirected.

Open a command prompt in Windows, or a terminal in Linux, and type the command:

```
telnet <TransPort VPN IP address> <port number>
```

The expected response should be seen, for example the following test shows that the Microsoft Telnet server running on the TransPort side Windows PC responded to a Telnet request from the Cisco side PC:

```
telnet 10.1.1.129 1101
…
Welcome to Microsoft Telnet Client
…
```

3.3 Check the VPN negotiation process in the TransPort and ASA logs

Below is the output from the TransPort's event log, showing successful connection to the ASA using EasyVPN (note that the most recent entries are at the top of the log file):

```
13:14:31, 15 Aug 2012,Eroute 0 VPN up peer: asa5505.ciscoasa.com
13:14:31, 15 Aug 2012,New IPSec SA created by asa5505.ciscoasa.com
13:14:30, 15 Aug 2012,(126) IKE Notification: Responder Lifetime,RX
13:14:30, 15 Aug 2012,(126) New Phase 2 IKE Session 61.2.3.4,Initiator
13:14:30, 15 Aug 2012,(125) IKE SA Removed. Peer: asa5505.ciscoasa.com,Successful Negotiation
13:14:30, 15 Aug 2012,(124) IKE SA Removed. Peer: asa5505.ciscoasa.com,Successful Negotiation
13:14:30, 15 Aug 2012,(123) IKE SA Removed. Peer: asa5505.ciscoasa.com,Successful Negotiation
13:14:30, 15 Aug 2012,(122) IKE Keys Negotiated. Peer: asa5505.ciscoasa.com
13:14:30, 15 Aug 2012,(122) New Phase 1 IKE Session 61.2.3.4,Initiator
13:14:30, 15 Aug 2012,IKE Request Received From Eroute 0
```

Below is the debug output from the ASA during a subsequent re-initiation of the VPN by the TransPort, showing a successful connection from the TransPort router. The TransPort's public IP address that the ASA sees (translated by NAT at the edge of the mobile network) is shown as <TransPort_public_IP>:

```
Aug 15 13:42:58 [IKEv1 DEBUG]IP = <TransPort_public_IP>, IKE Peer included IKE fragmentation
capability flags:  Main Mode:        True  Aggressive Mode:  False
Aug 15 13:42:58 [IKEv1]IP = <TransPort_public_IP>, Connection landed on tunnel_group
Customer_Group
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, IP = <TransPort_public_IP>, IKE SA Proposal
# 1, Transform # 1 acceptable  Matches global IKE entry # 1
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, IP = <TransPort_public_IP>, Automatic NAT
Detection Status:     Remote end   IS   behind a NAT device     This   end   IS   behind a NAT
device
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
User (Customer01) authenticated.
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Client Type:   Client Application Version:
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Assigned private IP address 10.1.1.129 to remote user
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Gratuitous ARP sent for 10.1.1.129
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
PHASE 1 COMPLETED
Aug 15 13:42:58 [IKEv1]IP = <TransPort_public_IP>, Keep-alive type for this connection: DPD
```

```
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Starting P1 rekey timer: 82080 seconds.
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Received remote Proxy Host data in ID Payload:  Address 10.1.1.129, Protocol 0, Port 0
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Received local IP Proxy Subnet data in ID Payload:   Address 0.0.0.0, Mask 0.0.0.0, Protocol 0,
Port 0
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
QM IsRekeyed old sa not found by addr
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Selecting only UDP-Encapsulated-Tunnel and  UDP-Encapsulated-Transport
modes defined by NAT-Traversal
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
IKE Remote Peer configured for crypto map: outside_dyn_map
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, processing IPSec SA payload
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, IPSec SA Proposal # 1, Transform # 1 acceptable  Matches global IPSec SA
entry # 10
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0xcb6c5df8,
    SCB: 0xCB5FF390,
    Direction: inbound
    SPI      : 0xB2996080
    Session ID: 0x00013000
    VPIF num  : 0x00000002
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Overriding Initiator's IPSec rekeying duration from 86400 to 28800 seconds
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Transmitting Proxy Id:
  Remote host: 10.1.1.129  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Sending RESPONDER LIFETIME notification to Initiator
IPSEC: New embryonic SA created @ 0xcb13ae80,
    SCB: 0xCB555C28,
    Direction: outbound
    SPI      : 0x3DC35092
    Session ID: 0x00013000
    VPIF num  : 0x00000002
    Tunnel type: ra
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x3DC35092
IPSEC: Creating outbound VPN context, SPI 0x3DC35092
    Flags: 0x00000025
    SA   : 0xcb13ae80
    SPI  : 0x3DC35092
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x030E201F
    Channel: 0xc82ad040
IPSEC: Completed outbound VPN context, SPI 0x3DC35092
    VPN handle: 0x0012990c
IPSEC: New outbound encrypt rule, SPI 0x3DC35092
    Src addr: 0.0.0.0
    Src mask: 0.0.0.0
    Dst addr: 10.1.1.129
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
```

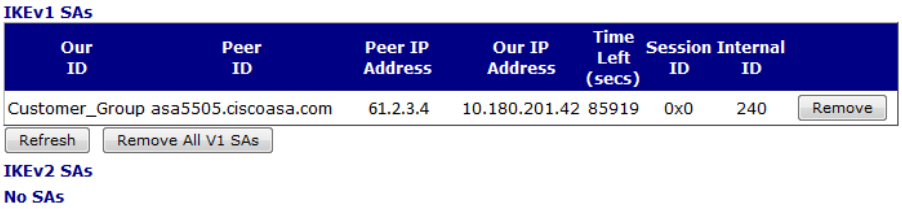
```
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 0
    Use protocol: false
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x3DC35092
    Rule ID: 0xcb6c6b18
IPSEC: New outbound permit rule, SPI 0x3DC35092
    Src addr: 61.2.3.4
    Src mask: 255.255.255.255
    Dst addr: <TransPort_public_IP>
    Dst mask: 255.255.255.255
    Src ports
      Upper: 4500
      Lower: 4500
      Op   : equal
    Dst ports
      Upper: 29677
      Lower: 29677
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed outbound permit rule, SPI 0x3DC35092
    Rule ID: 0xcb6c6eb0
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Security negotiation complete for User (Customer01)  Responder, Inbound SPI = 0xb2996080,
Outbound SPI = 0x3dc35092
IPSEC: Completed host IBSA update, SPI 0xB2996080
IPSEC: Creating inbound VPN context, SPI 0xB2996080
    Flags: 0x00000026
    SA   : 0xcb6c5df8
    SPI  : 0xB2996080
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x0012990C
    SCB  : 0x030DDC59
    Channel: 0xc82ad040
IPSEC: Completed inbound VPN context, SPI 0xB2996080
    VPN handle: 0x0013594c
IPSEC: Updating outbound VPN context 0x0012990C, SPI 0x3DC35092
    Flags: 0x00000025
    SA   : 0xcb13ae80
    SPI  : 0x3DC35092
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0013594C
    SCB  : 0x030E201F
    Channel: 0xc82ad040
IPSEC: Completed outbound VPN context, SPI 0x3DC35092
    VPN handle: 0x0012990c
IPSEC: Completed outbound inner rule, SPI 0x3DC35092
    Rule ID: 0xcb6c6b18
IPSEC: Completed outbound outer SPD rule, SPI 0x3DC35092
    Rule ID: 0xcb6c6eb0
IPSEC: New inbound tunnel flow rule, SPI 0xB2996080
    Src addr: 10.1.1.129
    Src mask: 255.255.255.255
    Dst addr: 0.0.0.0
    Dst mask: 0.0.0.0
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
```

```
      Lower: 0
      Op   : ignore
    Protocol: 0
    Use protocol: false
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0xB2996080
    Rule ID: 0xcb6be7c8
IPSEC: New inbound decrypt rule, SPI 0xB2996080
    Src addr: <TransPort_public_IP>
    Src mask: 255.255.255.255
    Dst addr: 61.2.3.4
    Dst mask: 255.255.255.255
    Src ports
      Upper: 29677
      Lower: 29677
      Op   : equal
    Dst ports
      Upper: 4500
      Lower: 4500
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound decrypt rule, SPI 0xB2996080
    Rule ID: 0xcb6bedf8
IPSEC: New inbound permit rule, SPI 0xB2996080
    Src addr: <TransPort_public_IP>
    Src mask: 255.255.255.255
    Dst addr: 61.2.3.4
    Dst mask: 255.255.255.255
    Src ports
      Upper: 29677
      Lower: 29677
      Op   : equal
    Dst ports
      Upper: 4500
      Lower: 4500
      Op   : equal
    Protocol: 17
    Use protocol: true
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound permit rule, SPI 0xB2996080
    Rule ID: 0xcb5fee48
Aug 15 13:42:58 [IKEv1 DEBUG]Group = Customer_Group, Username = Customer01, IP =
<TransPort_public_IP>, Starting P2 rekey timer: 27360 seconds.
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
Adding static route for client address: 10.1.1.129
Aug 15 13:42:58 [IKEv1]Group = Customer_Group, Username = Customer01, IP = <TransPort_public_IP>,
PHASE 2 COMPLETED (msgid=6b874a18)
```

3.4 Check the VPN status on the TransPort and the ASA

On the TransPort, the IKE SA can be seen in the following page in the web interface:

Management - Connections > Virtual Private Networking (VPN) > IPsec > IKE SAs

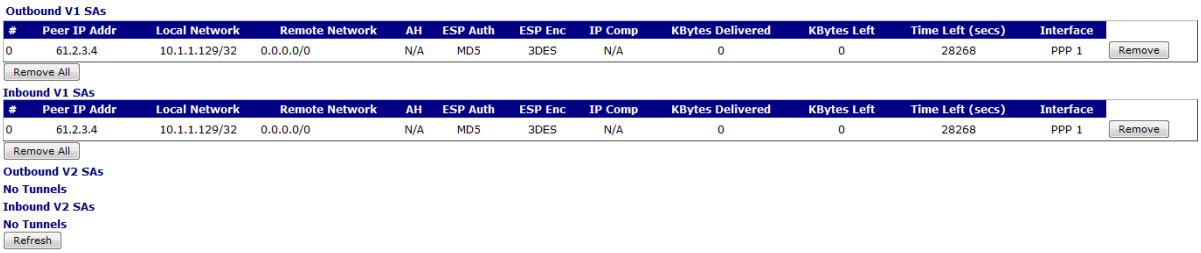


The successful IPsec connection will be shown in the IPsec Peers status page:

Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Peers

The IPsec SA can be seen in this page:

Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels



On the ASA, run the commands shown in bold below to view the IKE and IPsec SAs:

```
asa5505# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: <TransPort_public_IP>
    Type    : user            Role    : responder
```

```
    Rekey   : no              State   : AM_ACTIVE

There are no IKEv2 SAs

asa5505# show crypto ipsec sa

interface: outside
    Crypto map tag: outside_dyn_map, seq num: 10, local addr: 61.2.3.4

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.129/255.255.255.255/0/0)
      current_peer: <TransPort_public_IP>, username: Customer01
      dynamic allocated peer ip: 10.1.1.129

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 61.2.3.4/4500, remote crypto endpt.: <TransPort_public_IP>/29677
      path mtu 1500, ipsec overhead 66, media mtu 1500
      current outbound spi: 3DC35095
      current inbound spi : 90CADF16

    inbound esp sas:
      spi: 0x90CADF16 (2429214486)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel,  NAT-T-Encaps, }
         slot: 0, conn_id: 90112, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 28395
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x3DC35095 (1036210325)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel,  NAT-T-Encaps, }
         slot: 0, conn_id: 90112, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (sec): 28395
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

4 HARDWARE, FIRMWARE AND CONFIGURATION OF TEST DEVICES

4.1 TransPort WR44 configuration

This is the configuration from the TransPort WR44 used for testing:

```
eth 0 IPaddr "10.1.29.203"
eth 0 ipanon ON
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
def_route 0 ll_ent "ppp"
def_route 0 ll_add 1
eroute 0 peerip "61.2.3.4"
eroute 0 peerid "asa5505.ciscoasa.com"
eroute 0 ourid "Customer_Group"
eroute 0 locipifent "ETH"
eroute 0 remip "0.0.0.0"
eroute 0 remmsk "0.0.0.0"
eroute 0 ESPauth "MD5"
eroute 0 ESPenc "3DES"
eroute 0 ltime 86400
eroute 0 authmeth "XAUTHINITPRE"
eroute 0 nosa "TRY"
eroute 0 autosa 2
eroute 0 vip 1
eroute 0 xauthid "Customer01"
tunsnat 0 IPaddr "10.1.29.1"
tunsnat 0 minport 1101
tunsnat 0 mapport 23
tunsnat 0 maxport 1101
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 username "username"
ppp 1 IPaddr "0.0.0.0"
ppp 1 timeout 0
ppp 1 ipsec 1
ppp 1 use_modem 1
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 ipanon ON
ppp 1 r_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
ike 0 encalg "3DES"
ike 0 ltime 86400
ike 0 aggressive ON
ike 0 ikegroup 2
ike 0 deblevel 4
ike 0 delmode 1
modemcc 0 info_asy_add 6
modemcc 0 init_str "+CGQREQ=1"
modemcc 0 init_str1 "+CGQMIN=1"
modemcc 0 apn "internet"
```

```
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 l1on ON
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 ipfilt "~4500,500"
ana 0 ikeon ON
ana 0 maxdata 1500
ana 0 logsize 180
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 1
cmd 0 tremto 1200
user 0 access 0
user 1 name "username"
user 1 epassword "KD5lSVJDVVg="
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 "asa5505.ciscoasa.com"
user 10 epassword "PDZxU0JeSElC"
user 10 access 4
user 11 name "Customer01"
user 11 epassword "GyplTkpBQk4CDFFJA0k="
user 11 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
```

4.2 TransPort WR44 hardware and firmware

This is the hardware and firmware information from the TransPort WR44 used for testing:

```
Digi TransPort WR44-HXT1-WE1-XX Ser#:160601
Software Build Ver5156.  May 17 2012 19:55:43  SW
ARM Bios Ver 6.67 v39 400MHz B512-M512-F80-O0,0 MAC:00042d027359
Async Driver              Revision: 1.19  Int clk
Wi-Fi                     Revision: 2.0
IX                        Revision: 1.0
Ethernet Port Isolate Driver Revision: 1.11
Firewall                  Revision: 1.0
EventEdit                 Revision: 1.0
Timer Module              Revision: 1.1
(B)USBHOST                Revision: 1.0
L2TP                      Revision: 1.10
PPTP                      Revision: 1.00
TACPLUS                   Revision: 1.00
MODBUS                    Revision: 0.00
MySQL                     Revision: 0.01
RealPort                  Revision: 0.00
MultiTX                   Revision: 1.00
LAPB                      Revision: 1.12
X25 Layer                 Revision: 1.19
MACRO                     Revision: 1.0
PAD                       Revision: 1.4
X25 Switch                Revision: 1.7
V120                      Revision: 1.16
TPAD Interface            Revision: 1.12
GPS                       Revision: 1.0
SCRIBATSK                 Revision: 1.0
BASTSK                    Revision: 1.0
PYTHON                    Revision: 1.0
ARM Sync Driver           Revision: 1.18
TCP (HASH mode)           Revision: 1.14
TCP Utils                 Revision: 1.13
PPP                       Revision: 1.19
WEB                       Revision: 1.5
SMTP                      Revision: 1.1
FTP Client                Revision: 1.5
FTP                       Revision: 1.4
IKE                       Revision: 1.0
PollANS                   Revision: 1.2
PPPOE                     Revision: 1.0
BRIDGE                    Revision: 1.1
MODEM CC (Ericsson 3G)    Revision: 1.4
FLASH Write               Revision: 1.2
Command Interpreter       Revision: 1.38
SSLCLI                    Revision: 1.0
OSPF                      Revision: 1.0
BGP                       Revision: 1.0
QOS                       Revision: 1.0
RADIUS Client             Revision: 1.0
SSH Server                Revision: 1.0
SCP                       Revision: 1.0
CERT                      Revision: 1.0
LowPrio                   Revision: 1.0
Tunnel                    Revision: 1.2
OVPN                      Revision: 1.2
QDL                       Revision: 1.0
WiMax                     Revision: 1.0
iDigi                     Revision: 2.0
```

4.3 Cisco ASA configuration

This is the configuration from the Cisco ASA used for testing:

```
: Saved
:
ASA Version 8.4(2)
!
hostname asa5505
domain-name ciscoasa.com
enable password T6UoMiIONDNvyn8U encrypted
passwd RoNUgpFlMxkMZLh1 encrypted
names
!
interface Ethernet0/0
 switchport access vlan 11
!
interface Ethernet0/1
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.1.1.254 255.255.255.0
!
interface Vlan11
 nameif outside
 security-level 0
 ip address 61.2.3.4 255.255.255.240
!
ftp mode passive
dns server-group DefaultDNS
 domain-name ciscoasa.com
object network obj_vpn
 subnet 10.1.1.128 255.255.255.240
object network obj_any
 subnet 0.0.0.0 0.0.0.0
access-list inside_outbound_nat0_acl extended permit ip any 10.1.1.128 255.255.255.240
access-list inside_outbound_nat0_acl extended deny ip any any
access-list Customer_Permitted_Connection extended permit ip any any
access-list inside_access_in extended permit ip 10.1.1.0 255.255.255.0 10.1.1.128 255.255.255.240
access-list outside_access_in extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool Customer_Address_Pool 10.1.1.129-10.1.1.134
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
no asdm history enable
arp timeout 14400
nat (any,outside) source static any any destination static obj_vpn obj_vpn
```

```
!
object network obj_any
 nat (inside,outside) dynamic interface
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
route outside 0.0.0.0 0.0.0.0 192.168.25.254 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set ESP-3DES-MD5
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto isakmp identity hostname
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy DfltGrpPolicy attributes
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Customer_Permitted_Connection
username Customer01 password KO3Wuzt82nC6neEM encrypted
tunnel-group Customer_Group type remote-access
tunnel-group Customer_Group general-attributes
 address-pool Customer_Address_Pool
tunnel-group Customer_Group ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
```

```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:91085f87233f42beb600946ffa22a383
: end
```

4.4 Cisco ASA hardware and firmware

This is the hardware and firmware information from the Cisco ASA used for testing:

```
Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.2(1)

Compiled on Wed 15-Jun-11 18:17 by builders
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

asa5505 up 4 hours 42 mins

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1

 0: Int: Internal-Data0/0    : address is f866.f2d6.70e7, irq 11
 1: Ext: Ethernet0/0         : address is f866.f2d6.70df, irq 255
 2: Ext: Ethernet0/1         : address is f866.f2d6.70e0, irq 255
 3: Ext: Ethernet0/2         : address is f866.f2d6.70e1, irq 255
 4: Ext: Ethernet0/3         : address is f866.f2d6.70e2, irq 255
 5: Ext: Ethernet0/4         : address is f866.f2d6.70e3, irq 255
 6: Ext: Ethernet0/5         : address is f866.f2d6.70e4, irq 255
 7: Ext: Ethernet0/6         : address is f866.f2d6.70e5, irq 255
 8: Ext: Ethernet0/7         : address is f866.f2d6.70e6, irq 255
 9: Int: Internal-Data0/1    : address is 0000.0003.0002, irq 255
10: Int: Not used            : irq 255
11: Int: Not used            : irq 255

Licensed features for this platform:
Maximum Physical Interfaces       : 8              perpetual
VLANs                             : 3              DMZ Restricted
Dual ISPs                         : Disabled       perpetual
VLAN Trunk Ports                  : 0              perpetual
Inside Hosts                      : 50             perpetual
Failover                          : Disabled       perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 10             perpetual
Total VPN Peers                   : 25             perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Disabled       perpetual
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

Serial Number: *****
Running Permanent Activation Key: *****
Configuration register is 0x1
Configuration last modified by enable_15 at 01:46:43.739 UTC Wed Aug 15 2012
```