LAN-Cell to Cisco ASA VPN Example

Tech Note LCTN0014

Proxicast, LLC
312 Sunnyfield Drive
Suite 200
Glenshaw, PA 15116

1-877-77PROXI
1-877-777-7694
1-412-213-2477

Fax:
1-412-492-9386

E-Mail:
support@proxicast.com

Internet:
www.proxicast.com

This Tech Note applies to LAN-Cell models:

LAN-Cell 2:
LC2-411

CDMA:
1xMG-401
1xMG-401S

GSM:
GPRS-401

Minimum LAN-Cell Firmware Revision: 3.62(XF2).

Note for Original LAN-Cell Model (1xMG & GPRS) Users:

The VPN configuration screens in the original LAN-Cell's Web GUI differ slightly from the examples in this Technote. Please locate the corresponding parameter fields in the VPN Configuration section of the LAN-Cell's user interface under VPN Rules (IKE). See also the LAN-Cell's *User Guide* for more information on VPN configuration.

Document Revision History:

Date	Comments
March 9, 2009	First release

Introduction

The LAN-Cell can establish "site-to-site" IPSec VPN tunnels (also called "LAN-to-LAN" or "L2L") with Cisco ASA 5500 series hardware devices. Most other Cisco VPN hardware devices such as IOS-based routers and PIX firewalls are also supported.

Site-to-Site VPNs are the most common way to set up a secure connection to a remote site. The IPSec tunnel will be established between the remote LAN-Cell and the Cisco ASA on your "headquarters" network.

A site-to-site VPN tunnel results in the "private" (inside) subnets behind each VPN device being able to communicate with each other directly and securely as if they were on the same physical network.

This TechNote is presents examples of how to configure both the LAN-Cell and the Cisco Adaptive Security Appliance (ASA) hardware for a site-to-site IPSec VPN tunnel when the LAN-Cell has either a static WAN IP Address (Example 1 on page 3) or a Dynamic WAN IP address (Example 2 on page 11). The LAN-Cell and ASA devices are assumed to be at their "factory default" configurations with no other settings configured except any required LAN & WAN access parameters.

This TechNote is for illustration purposes only. Other configuration parameters may be required on your devices depending on your specific network configuration and application requirements. If you are making changes to "production" LAN-Cell and/or ASA devices, consider the impact of any changes on your existing network and VPN configurations.

Usage Notes

- In general, all VPN parameters much match EXACTLY between the 2 devices.
- It is helpful to can have simultaneous access to the to parameter and log screens of both devices during set-up and testing.
- The network on the LAN side of the LAN-Cell and on the "inside" of the ASA must be on different subnets.
- Most users find it easiest to configure VPNs if both end-points have static public IP addresses. Contact your ISP or cellular network operator to determine if static IP addresses are available. Otherwise, you will need to define a dynamic tunnel for your LAN-Cell on the ASA device. (See Example 2)
- The examples assume that the Cisco ASA has a static WAN IP address; however, the LAN-Cell also supports VPN tunnels to devices with Dynamic DNS names. Simply replace the ASA's WAN IP address with its FQDN name (e.g. *main-office.prxd.com*) in the examples.
- The LAN-Cell can be either the VPN initiator or responder for site-to-site VPNs when it has a static WAN IP address. When the LAN-Cell as a dynamic WAN IP address, it must initiate the VPN tunnel as the ASA will not know the LAN-Cell's WAN IP address in advance.
- These examples were created using a LAN-Cell 2 with firmware version 4.02(AQP.3) and an ASA 5505 with firmware version 7.2(3).

Please see the *LAN-Cell Users Guide* for more detailed information on VPN parameters and configuration. We also recommend the *LAN-Cell VPN Planner TechNote* for gathering the necessary VPN parameters and planning your network topology.

Also see the Proxicast Support website (http://www.proxicast.com/support) for additional VPN information and configuration examples.

Example 1: Static WAN IP on the LAN-Cell

Figure 1 shows the IP addressing scheme for our example site-to-site VPN configuration with the LAN-Cell having a static WAN IP (166.139.37.167) assigned to its 3G modem card by the cellular carrier.

Figure 2 is for you to record the network addresses of the key nodes in your VPN network.

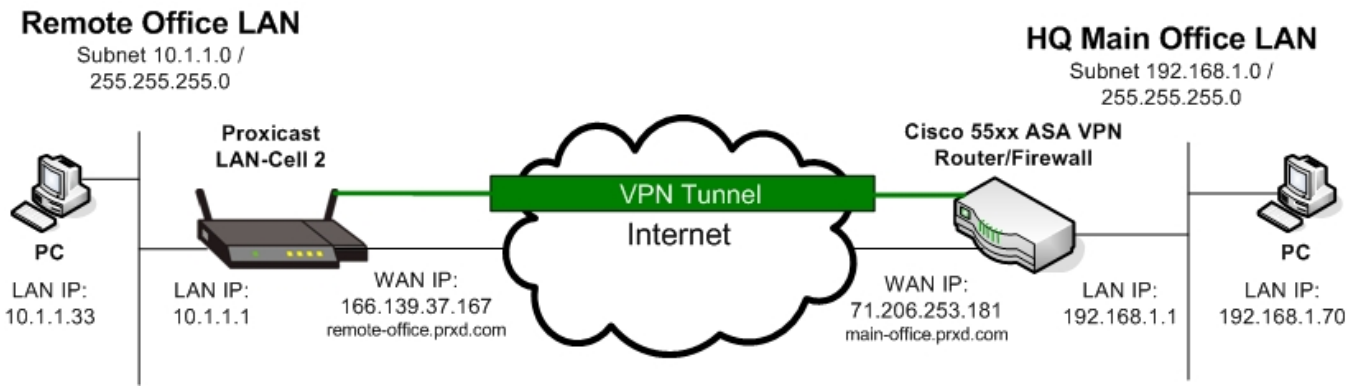


Figure 1: Example Cisco ASA Site-to-Site VPN Network Topology

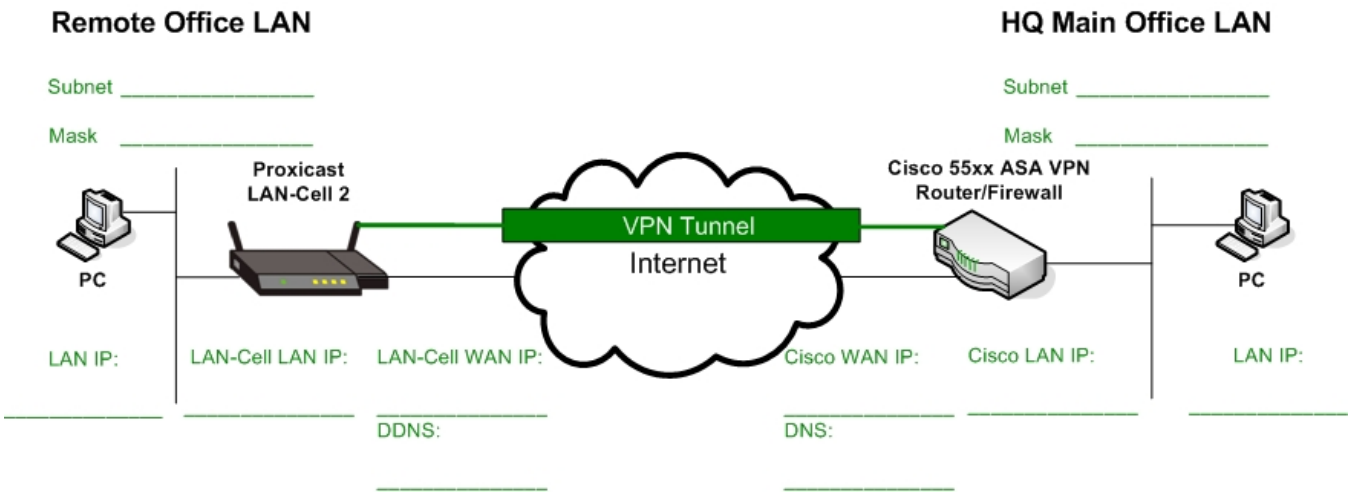


Figure 2: Your Cisco ASA Site-to-Site VPN Network Topology

Cisco ASA Parameters

For this example, we will use the Cisco ASA's VPN Wizard in the Adaptive Security Device Manager (ASDM) software v5.2(3). At the end of this section, the equivalent command-line commands are also shown (Figure 8).

Start the VPN Wizard as shown in Figure 3 and select "Site-to-Site" as the **VPN Tunnel Type**.

Figure 3: ASA VPN Wizard Step 1

Next, enter the static WAN IP address of the LAN-Cell (166.139.37.167 in the example) as the **Peer IP Address**. Also enter a **Pre-Shared Key** value of at least 8 alphanumeric characters (Figure 4). Note that the **Tunnel Group Name** will be automatically filled in with the LAN-Cell's static IP address. Do not change the Tunnel Group Name.

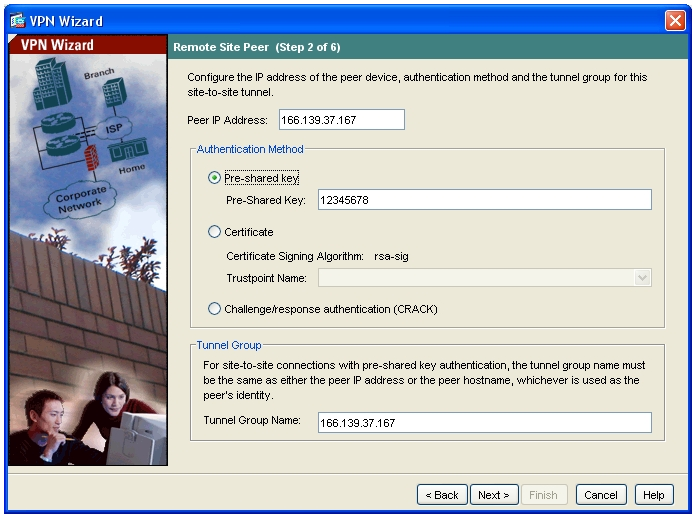


Figure 4: ASA VPN Wizard Step 2

For Steps 3 and 4 of the ASDM VPN Wizard, we will accept the default values for **Encryption** (3DES) and **Authentication** (SHA/DH2) settings on the ASA and change the LAN-Cell's VPN parameters to match these values (Figure 5).

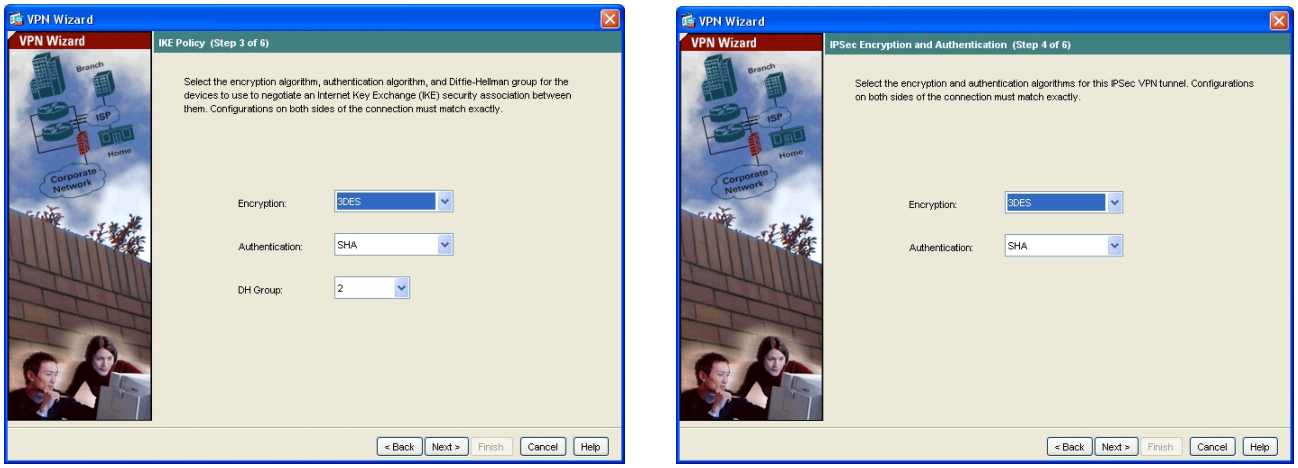


Figure 5: ASA VPN Wizard Steps 3 & 4

In Step 5 of the ASDM VPN Wizard, we define the **Source** or "inside" subnet behind the ASA (192.168.1.0) and the **Destination** (or Remote) private subnet behind the LAN-Cell (10.1.1.0) that are to be linked into the VPN tunnel (Figure 6). Note that the entire subnets are defined on both sides and that the subnets do not overlap.

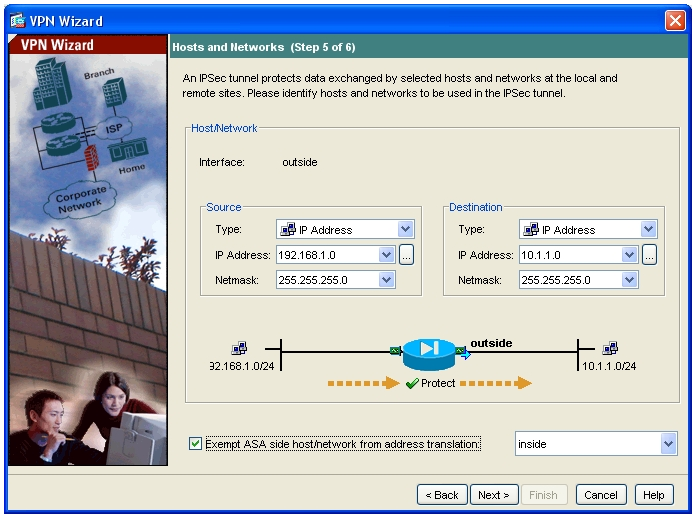


Figure 6: ASA VPN Wizard Step 5

Step 6 of the wizard simply summarizes the parameters for this VPN tunnel. Note that **Perfect Forward Secrecy** (PFS) is enabled by default by the wizard (Figure 7).

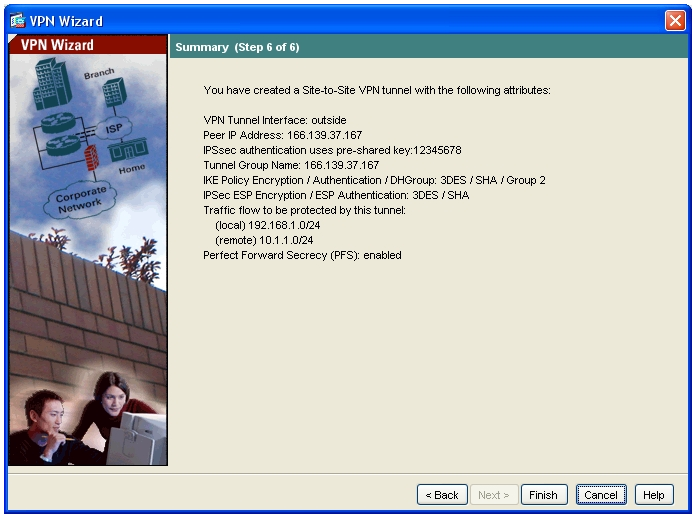


Figure 7: ASA VPN Wizard Step 6

The commands that the ASDM VPN Wizard applies to the ASA device are summarized below (Figure 8). A complete listing of the ASA's running configuration is shown in Appendix A.

```
access-list outside_1_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
nat (inside) 0 access-list inside_nat0_outbound
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 166.139.37.167
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 166.139.37.167 type ipsec-l2l
tunnel-group 166.139.37.167 ipsec-attributes
 pre-shared-key 12345678
```

Figure 8: ASA VPN Commands (Static Tunnel)

LAN-Cell VPN Setup

To configure the LAN-Cell 2, we can use the **VPN Wizard** under the **Security** menu. Figure 9 shows Step 1 of the LAN-Cell's VPN Wizard where the **Gateway Policy Name**, **LAN-Cell's static WAN IP Address** and the **ASA's public WAN IP Address** are specified.

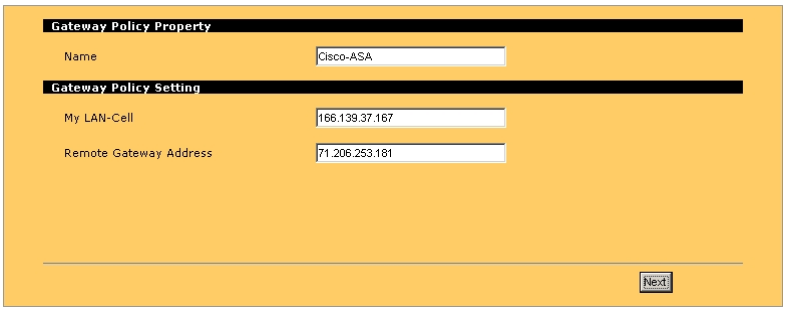


Figure 9: LAN-Cell VPN Wizard Step 1

In Step 2, the local network addresses behind each VPN appliance are defined. Note that these values are the exact opposite of how they are specified on the ASA; that is "L**ocal**" now refers to the LAN-Cell and "**Remote**" to the ASA. Again, specify a complete non-overlapping subnet address for each side (Figure 10).

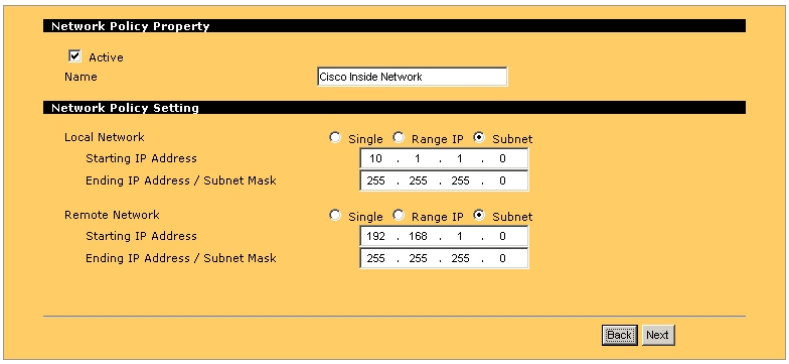


Figure 10: LAN-Cell VPN Wizard Step 2

Figure 11 shows Step 3 of the wizard where the Phase 1 (IKE) **Encryption** and **Authentication** parameters are specified to match the defaults created for the VPN tunnel by the ASA. In our example this is 3DES, SHA1, DH2, **SA Lifetime** = 86400 and the same **Pre-Shared Key** as entered on the ASA (12345678 in our example).

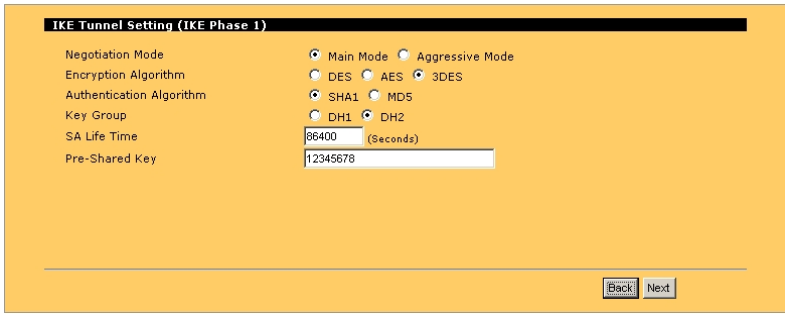


Figure 11: LAN-Cell VPN Wizard Step 3

Wizard Step 4 sets the Phase 2 (IPSec) parameters for the tunnel. To match the ASA defaults, select Tunnel, ESP, 3DES, SHA1, **SA Lifetime** = 28800 and **PFS** = DH2 as shown in Figure 12.

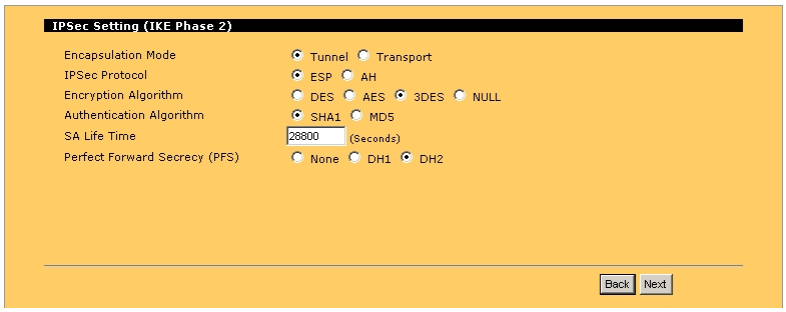


Figure 12: LAN-Cell VPN Wizard Step 4

The final LAN-Cell VPN Wizard screen summarizes the tunnel parameters which will be used to create the Gateway and Network Policy Rules on the LAN-Cell (Figure 13).

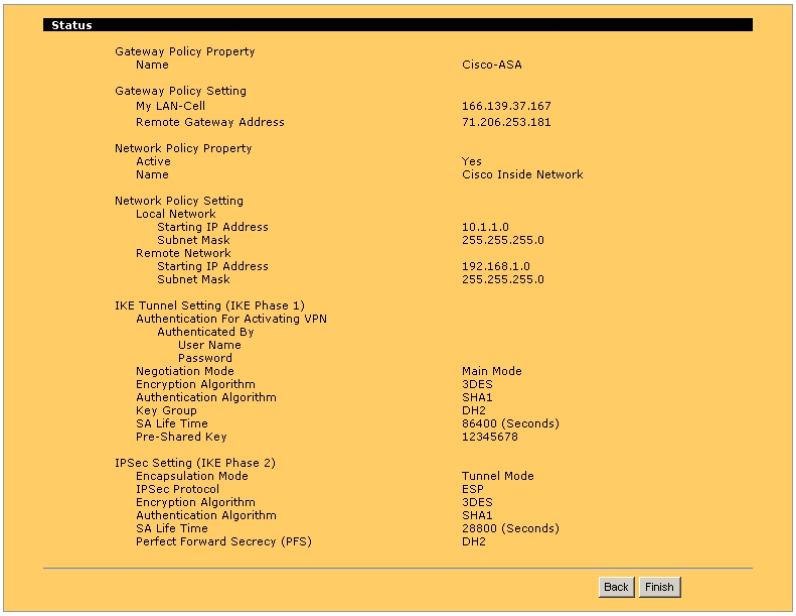


Figure 13: LAN-Cell VPN Wizard Step 5

Once you have completed the LAN-Cell VPN Wizard, you can review the Gateway and Network Rules it created by selecting **VPN Config** under the **Security Menu**. Figure 14 shows the newly created rules. Click on the **Edit** icon ( ) to open the corresponding rule.

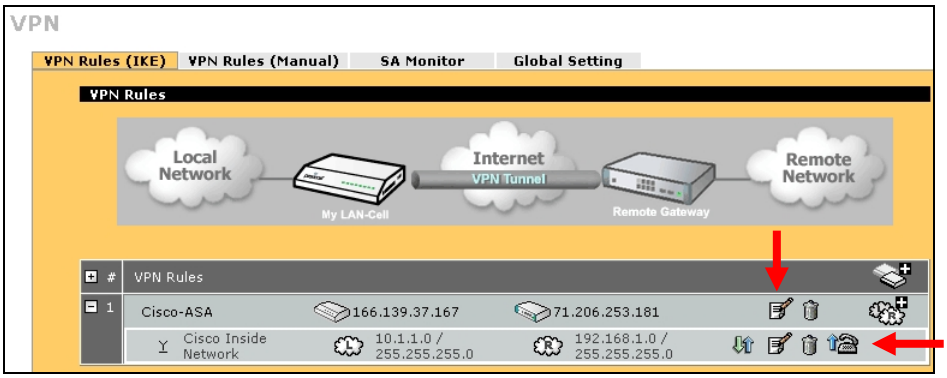


Figure 14: LAN-Cell VPN Gateway & Network Rules

proxicast®

A VPN tunnel can be successfully opened between the LAN-Cell and the Cisco ASA without any further edits to the LAN-Cell VPN Rules. However, you may wish to modify the Network Policy Rule to set the VPN tunnel to be "nailed-up", that is always connected even when there is no traffic or to generate periodic traffic through the tunnel by having the LAN-Cell "ping" a device on the other subnet. Figure 15 indicates where to adjust these settings.

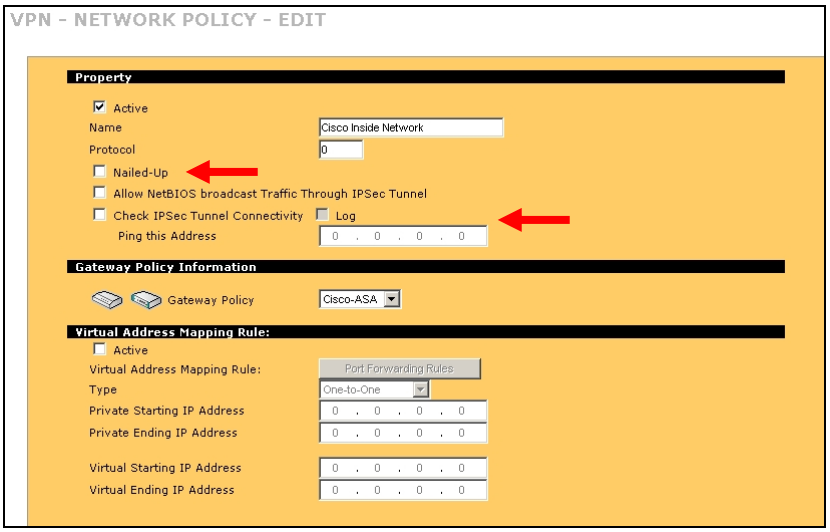


Figure 15: LAN-Cell VPN Network Policy

Opening a VPN Tunnel

There are several ways to open and test a VPN tunnel.

Always On

If you defined the Network Policy as "Nailed-Up", the VPN tunnel creation will be attempted automatically by the LAN-Cell once the Network Policy is saved. You can view the current status of the VPN tunnel connections (called Security Associations – SA) using the **SA Monitor** screen as shown in Figure 16.

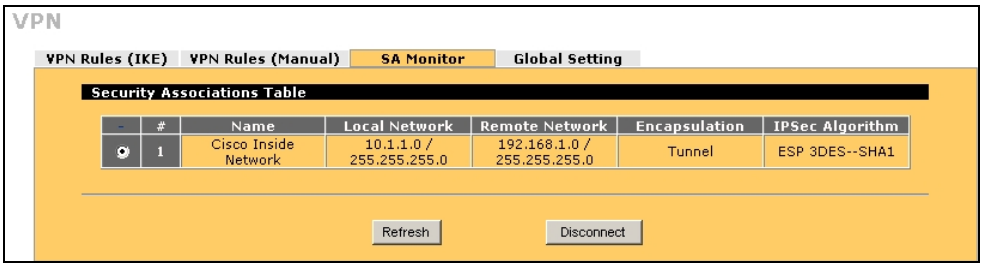
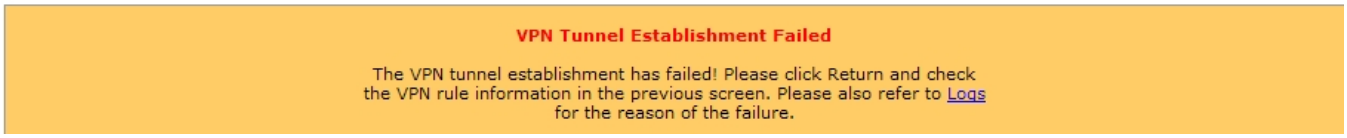


Figure 16: SA Monitor

Manual Connection

You can manually "dial up" the ASA device by clicking the **Dial** icon ( ) next to the Network Policy rule on the VPN Rule Summary screen (Figure 14). The LAN-Cell will monitor the progress of the tunnel creation and indicate success or failure (Figure 17). The **Dial** icon can also be used to disconnect an active tunnel.



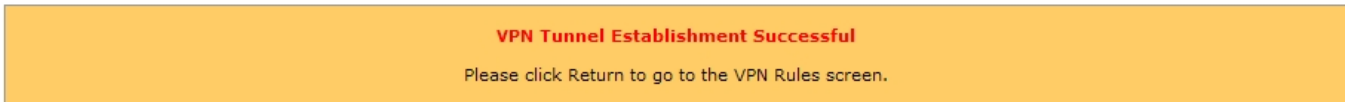


Figure 17: Failed & Successful VPN Connection

Traffic Generation

Once your VPN tunnel parameters have been entered, any traffic destined for the other private network will cause the tunnel to be automatically created. For example, a PING from a device on the LAN-Cell's LAN to the HQ LAN (ASA) will bring up the tunnel. You can also initiate the tunnel from the Main Office ASA LAN by PING'ing a device on the LAN-Cell's LAN.

Note that negotiating the tunnel may take several seconds and your first few PINGs may not be acknowledged. When using this method to test a VPN connection, we do not recommend sending continuous PINGs, as this can create excessive IKE retransmits which may slow down or even prevent tunnel creation. Also, if your initial attempts at opening a tunnel fail, please either manually clear the ISAKMP & IPSec SA's on the ASA or wait several seconds for them to time-out before reattempting the tunnel.

Example 2: Dynamic WAN IP on the LAN-Cell

The second example uses the exact same network topology as Example 1 (Figure 1), except that the public WAN IP address of the LAN-Cell is dynamically assigned by the ISP and can change every time a new WAN connection is made or under other circumstances. The Cisco ASA has no way of knowing the LAN-Cell's WAN IP address in advance; therefore a static VPN tunnel definition cannot be created. The ASA does not currently support fully-qualified domain names (FQDN) as VPN tunnel end-points.[1]

Cisco ASA Parameters

The ASDM VPN Wizard is not capable of creating a "dynamic" tunnel group on the ASA, so you must manually enter the commands necessary to create the proper policies (Figure 18). For this example, we will use the default settings from the LAN-Cell and change the ASA to match the default values created by the LAN-Cell's VPN Wizard. A complete listing of the ASA's runtime configuration in shown in Appendix B.

```
access-list outside_cryptomap_20.1 extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
nat (inside) 0 access-list outside_cryptomap_20.1
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto dynamic-map cisco 1 match address outside_cryptomap_20.1
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
crypto isakmp enable outside
crypto isakmp policy 20
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800
tunnel-group DefaultL2LGroup ipsec-attributes
 pre-shared-key 12345678
```

Figure 18: ASA VPN Commands (Dynamic Tunnel)

Note that we have modified the default L2L Tunnel Group on the ASA to have the Pre-Shared Key from the LAN-Cell (last 2 lines in Figure 18). This is necessary so that IKE Main Mode negotiation can take place. If you create a new Tunnel Group for dynamic end-points, you must change the LAN-Cell's IKE Negotiation Mode to Aggressive. Also, no two Tunnel Groups should have the same Pre-Shared Key; the ASA will use the Pre-Shared Key value along with the access-list addresses to match the incoming IKE request from the LAN-Cell and determine the correct tunnel parameters to use.

LAN-Cell VPN Setup

We can use the LAN-Cell's VPN Wizard to create the Gateway and Network Policy Rules necessary for establishing a "dynamic" tunnel to the Cisco ASA.

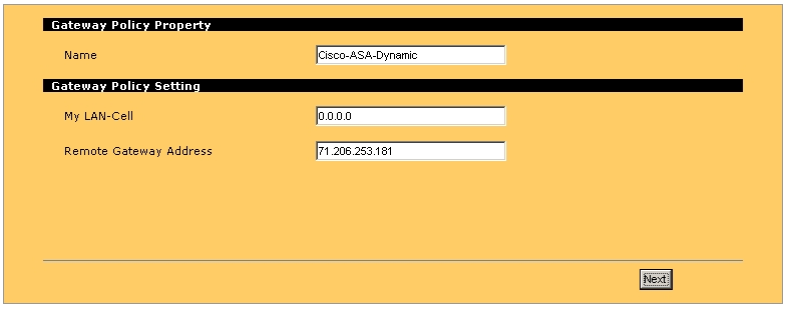


Figure 19: LAN-Cell Dynamic VPN Wizard Step 1

[1] Some Cisco IOS-based products include a feature extension called *Real-Time Resolution for IPsec Tunnel Peer* which allows VPN tunnel end-points to be specified as DNS names. The PIX and ASA product lines do not currently offer this feature. Contact Cisco for more information on the availability of this feature for your specific device.

In Figure 19, the **My LAN-Cell** address is set to 0.0.0.0 since it is dynamic. If you have defined a Dynamic DNS hostname for your LAN-Cell, you can optionally enter that FQDN here.[2] Also enter the public WAN IP address (or DNS name) of the Cisco ASA as the **Remote Gateway Address**.

During Step 2 as shown in Figure 20, define the **Local** (LAN-Cell) and **Remote** (ASA) private network addresses. Be sure to specify non-overlapping subnets.

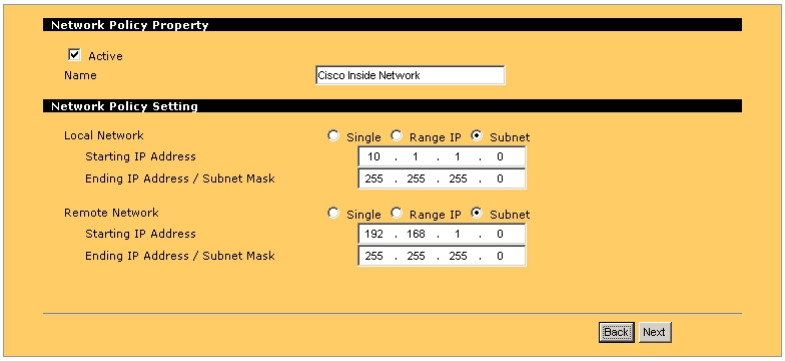


Figure 20: LAN-Cell Dynamic VPN Wizard Step 2

Accept the default **Encryption** and **Authentication** settings for Phase 1 and Phase 2 (Figures 21 & 22) and specify the same **Pre-Shared Key** value that was entered into the ASA.

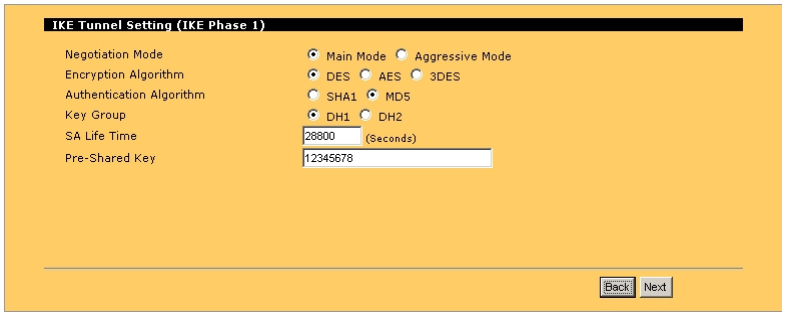


Figure 21: LAN-Cell Dynamic VPN Wizard Step 3

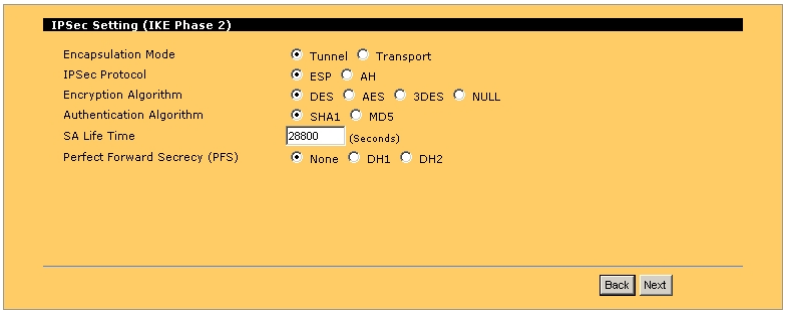


Figure 22: LAN-Cell Dynamic VPN Wizard Step 4

Once you have completed the LAN-Cell VPN Wizard, please refer to Figures 14 through 18 above for information on modifying the tunnel parameters and testing your VPN tunnel with the ASA.

Remember that the LAN-Cell must initiate the VPN tunnel connection to the ASA if the LAN-Cell has a dynamic WAN IP address.

[2] Although not strictly necessary, you may find it helpful to create a Dynamic DNS name for your LAN-Cell which has a dynamic WAN IP address, especially for remote access via the WAN. See ADVANCED > DNS > DDNS and the *LAN-Cell Users Guide* for more information.

Tips

- Backup your LAN-Cell and Cisco configuration files before beginning to enter VPN parameters and again after successfully completing the VPN configuration.
- Ensure that you have a reliable Internet connection and that your ISP/Cellular account is provisioned to allow IKE/IPSec traffic in both directions.
- Start by successfully configuring the simplest VPN tunnel possible (e.g. pre-shared keys, no XAUTH, static IP addresses, etc.) before attempting to configure more advanced settings.
- Clear the log on each VPN device after each unsuccessful connection attempt to make it easier to trace the current tunnel session.

Troubleshooting

The most common issues that arise when configuring site-to-site VPN tunnels include:

- *Stuck at Phase 1 ID Mismatch*
  It is recommended that you enter an IP address other than 0.0.0.0 in the local Content field or use the DNS (hostname) or E-mail ID Type in the following situations:
  - When there is a NAT router between the two IPSec routers.
  - When you want the HQ IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.
- *Stuck at Phase 1 No Proposal Chosen*
  Try different encryption and authentication settings. Check the Diffie-Hellman key length. Use the Enable Multiple IKE Proposals option to allow the LAN-Cell to automatically match the other VPN device's settings.
- *Phase 2 will not complete*
  Most often this is a mismatch with the local and remote network subnet definitions. Ensure that you are specifying a complete subnet (if appropriate). Remember, for a full Class-C subnet, the last octet of the address should be 0 with a subnet mask of 255.255.255.0. Also the private subnets behind each VPN device must be different.

  You can also enable Multiple IPSec Proposals to allow the LAN-Cell to match the incoming parameters from the other VPN device.
- *Tunnel goes down after a few minutes*
  This is normal behavior if you do not specify "Nailed up" or IPSec Continuity for the Network Policy. By default, the tunnel will be dropped after 2 minutes of inactivity. You can modify the input and output timers on the VPN Config Global Settings screen.
- *Sometimes the tunnel connects and sometimes it doesn't*
  Be sure that both VPN devices have completely deleted their security associations before a new tunnel request is initiated. Either manually drop the tunnel or adjust the timer values to drop the tunnel quickly if the VPN peer device does not respond. On the ASA, enter:

  ```
  clear crypto isakmp sa
  clear crypto ipsec sa
  ```

Cisco also has a detailed troubleshooting guide for site-to-site VPN tunnels for the PIX/ASA series:
http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a00807e0aca.shtml

Logging

The LAN-Cell has extensive error logging features. If initial attempts at creating the VPN tunnel are unsuccessful, use the **LOGS** menu to obtain more information about the error. You should also consult the logs and documentation for your Cisco VPN appliance for additional troubleshooting assistance. For the Cisco ASA, VPN debugging can be enabled with the commands:

```
debug crypto ipsec
debug crypto isakmp [level] (1 to 255)
```

Here are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:

#	Time ▲	Message	Source	Destination	Note
1	2009-03-08 00:47:54	Rule [Cisco Inside Network] Tunnel built successfully	166.139.37.167	71.206.253.181	IKE
2	2009-03-08 00:47:54	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
3	2009-03-08 00:47:54	Send:[HASH]	166.139.37.167	71.206.253.181	IKE
4	2009-03-08 00:47:54	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
5	2009-03-08 00:47:54	Adjust TCP MSS to 1390	166.139.37.167	71.206.253.181	IKE
6	2009-03-08 00:47:53	Recv:[HASH][SA][NONCE][KE][ID][ID]	71.206.253.181	166.139.37.167	IKE
7	2009-03-08 00:47:53	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	71.206.253.181	166.139.37.167	IKE
8	2009-03-08 00:47:53	Send:[HASH][SA][NONCE][KE][ID][ID]	166.139.37.167	71.206.253.181	IKE
9	2009-03-08 00:47:53	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
10	2009-03-08 00:47:52	Phase 1 IKE SA process done	166.139.37.167	71.206.253.181	IKE
11	2009-03-08 00:47:52	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
12	2009-03-08 00:47:52	Recv:[ID][HASH][VID]	71.206.253.181	166.139.37.167	IKE
13	2009-03-08 00:47:52	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	71.206.253.181	166.139.37.167	IKE
14	2009-03-08 00:47:52	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	71.206.253.181	IKE
15	2009-03-08 00:47:52	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
16	2009-03-08 00:47:52	Recv:[KE][NONCE][VID][VID][VID][VID	71.206.253.181	166.139.37.167	IKE
17	2009-03-08 00:47:52	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	71.206.253.181	166.139.37.167	IKE
18	2009-03-08 00:47:52	Send:[KE][NONCE]	166.139.37.167	71.206.253.181	IKE
19	2009-03-08 00:47:52	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	166.139.37.167	71.206.253.181	IKE
20	2009-03-08 00:47:51	Recv:[SA][VID]	71.206.253.181	166.139.37.167	IKE
21	2009-03-08 00:47:51	The cookie pair is : 0xAEE5C74B60FE9577 / 0x66D6DCB7E751CF30	71.206.253.181	166.139.37.167	IKE
22	2009-03-08 00:47:51	Send:[SA][VID][VID]	166.139.37.167	71.206.253.181	IKE
23	2009-03-08 00:47:51	The cookie pair is : 0xAEE5C74B60FE9577 / 0x0000000000000000	166.139.37.167	71.206.253.181	IKE
24	2009-03-08 00:47:51	Send Main Mode request to [71.206.253.181]	166.139.37.167	71.206.253.181	IKE
25	2009-03-08 00:47:51	Rule [Cisco-ASA] Sending IKE request	166.139.37.167	71.206.253.181	IKE

Phase 1 Parameter Mismatch (NO_PROP_CHOSEN):

#	Time	Message	Source	Destination	Note
1	2009-03-09 04:08:59	Recv:[NOTFY:NO_PROP_CHOSEN]	71.206.253.181	166.139.37.167	IKE
2	2009-03-09 04:08:59	The cookie pair is : 0x6467A05B098F2390 / 0x0000000000000000	71.206.253.181	166.139.37.167	IKE
3	2009-03-09 04:08:59	Send:[SA][VID][VID]	166.139.37.167	71.206.253.181	IKE
4	2009-03-09 04:08:59	The cookie pair is : 0x6467A05B098F2390 / 0x0000000000000000	166.139.37.167	71.206.253.181	IKE
5	2009-03-09 04:08:59	Send Main Mode request to [71.206.253.181]	166.139.37.167	71.206.253.181	IKE
6	2009-03-09 04:08:59	Rule [Cisco-ASA] Sending IKE request	166.139.37.167	71.206.253.181	IKE
7	2009-03-09 04:08:59	The cookie pair is : 0x6467A05B098F2390 / 0x0000000000000000	166.139.37.167	71.206.253.181	IKE

Compare the Phase 1 parameters on the Remote Office LAN-Cell VPN Gateway Policy Edit page with the corresponding Phase 1 (IKE/ISAKMP) parameters on your Cisco VPN device, in particular the Encryption, Authentication and the Key Group. Note: DH1 = DH768 and DH2 = DH1024.

Phase 1 ID Type Mismatch:

#	Time	Message	Source	Destination	Note
1	2009-03-09 04:11:03	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	71.206.253.181	IKE
2	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	166.139.37.167	71.206.253.181	IKE
3	2009-03-09 04:11:03	[ID] : ID type mismatch. Local / Peer: DNS / IP	71.206.253.181	166.139.37.167	IKE
4	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
5	2009-03-09 04:11:03	[ID] : Rule [Cisco-ASA] Phase 1 ID mismatch	71.206.253.181	166.139.37.167	IKE
6	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
7	2009-03-09 04:11:03	Send:[HASH][NOTFY:ERR_ID_INFO]	166.139.37.167	71.206.253.181	IKE
8	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	166.139.37.167	71.206.253.181	IKE
9	2009-03-09 04:11:03	[ID] : Rule [Cisco-ASA] Phase 1 ID mismatch	71.206.253.181	166.139.37.167	IKE
10	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
11	2009-03-09 04:11:03	Recv:[ID][HASH][VID]	71.206.253.181	166.139.37.167	IKE
12	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
13	2009-03-09 04:11:03	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	71.206.253.181	IKE
14	2009-03-09 04:11:03	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	166.139.37.167	71.206.253.181	IKE
15	2009-03-09 04:11:02	Recv:[KE][NONCE][VID][VID][VID][VID	71.206.253.181	166.139.37.167	IKE
16	2009-03-09 04:11:02	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
17	2009-03-09 04:11:02	Send:[KE][NONCE]	166.139.37.167	71.206.253.181	IKE
18	2009-03-09 04:11:02	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	166.139.37.167	71.206.253.181	IKE
19	2009-03-09 04:11:02	Recv:[SA][VID]	71.206.253.181	166.139.37.167	IKE
20	2009-03-09 04:11:02	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x4223EDB4B8C6E879	71.206.253.181	166.139.37.167	IKE
21	2009-03-09 04:11:02	Send:[SA][VID][VID]	166.139.37.167	71.206.253.181	IKE
22	2009-03-09 04:11:02	The cookie pair is : 0xE5DADB2F19F8B1F8 / 0x0000000000000000	166.139.37.167	71.206.253.181	IKE
23	2009-03-09 04:11:02	Send Main Mode request to [71.206.253.181]	166.139.37.167	71.206.253.181	IKE
24	2009-03-09 04:11:02	Rule [Cisco-ASA] Sending IKE request	166.139.37.167	71.206.253.181	IKE

This error is commonly caused when the Local and Remote ID types and/or Content values are not the same on each device. Check that both devices are using IP Address as the type and the same IP address values. You can also use E-Mail or DNS (hostname) ID Types/Content as long as they match the corresponding settings on the LAN-Cell. Remember that the Local and Remote values are relative to each device.

Phase 2 Parameter Mismatch:

#	Time	Message	Source	Destination	Note
1	2009-03-09 04:16:12	Send:[HASH][DEL]	166.139.37.167	71.206.253.181	IKE
2	2009-03-09 04:16:12	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
3	2009-03-09 04:16:12	Send:[HASH][DEL]	166.139.37.167	71.206.253.181	IKE
4	2009-03-09 04:16:12	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
5	2009-03-09 04:16:12	Recv:[HASH][NOTFY:NO_PROP_CHOSEN]	71.206.253.181	166.139.37.167	IKE
6	2009-03-09 04:16:12	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	71.206.253.181	166.139.37.167	IKE
7	2009-03-09 04:16:12	Send:[HASH][SA][NONCE][KE][ID][ID]	166.139.37.167	71.206.253.181	IKE
8	2009-03-09 04:16:12	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
9	2009-03-09 04:16:11	Phase 1 IKE SA process done	166.139.37.167	71.206.253.181	IKE
10	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
11	2009-03-09 04:16:11	Recv:[ID][HASH][VID]	71.206.253.181	166.139.37.167	IKE
12	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	71.206.253.181	166.139.37.167	IKE
13	2009-03-09 04:16:11	Send:[ID][HASH][NOTFY:INIT_CONTACT]	166.139.37.167	71.206.253.181	IKE
14	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
15	2009-03-09 04:16:11	Recv:[KE][NONCE][VID][VID][VID][VID	71.206.253.181	166.139.37.167	IKE
16	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	71.206.253.181	166.139.37.167	IKE
17	2009-03-09 04:16:11	Send:[KE][NONCE]	166.139.37.167	71.206.253.181	IKE
18	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	166.139.37.167	71.206.253.181	IKE
19	2009-03-09 04:16:11	Recv:[SA][VID]	71.206.253.181	166.139.37.167	IKE
20	2009-03-09 04:16:11	The cookie pair is : 0xA8E63FC526D7A192 / 0x26BDE6197D382552	71.206.253.181	166.139.37.167	IKE
21	2009-03-09 04:16:10	Send:[SA][VID][VID]	166.139.37.167	71.206.253.181	IKE
22	2009-03-09 04:16:10	The cookie pair is : 0xA8E63FC526D7A192 / 0x0000000000000000	166.139.37.167	71.206.253.181	IKE
23	2009-03-09 04:16:10	Send Main Mode request to [71.206.253.181]	166.139.37.167	71.206.253.181	IKE
24	2009-03-09 04:16:10	Rule [Cisco-ASA] Sending IKE request	166.139.37.167	71.206.253.181	IKE

Similar to a Phase 1 proposal error, this indicates that the Phase 2 parameters do not match (note that Phase 1 completed successfully). Check the LAN-Cell's VPN Network Policy Edit page settings against the Cisco's Phase 2 (IPSec) settings.

Frequently Asked Questions

Q: Can I have more than 1 VPN connection from the Remote LAN-Cell at the same time?

A: Yes. The LAN-Cell 2 supports 5 simultaneous non-overlapping VPN tunnels; the original LAN-Cell Mobile Gateway supports 2 VPN tunnels. Simply define the Gateway and Network Policies you need for each tunnel.

Q: Can I force all Internet bound traffic from the LAN-Cell to go through the VPN tunnel before going on to the Internet?

A: Yes. See TechNote *LCTN0009: Routing all Internet-bound Traffic Through a VPN Tunnel* for an example of how to configure this type of VPN tunnel.

Q: How do I stop the LAN-Cell log from filling up with messages like these after the VPN tunnel is up?

#	Time ▲	Message	Source	Destination	Note
1	2009-03-09 04:17:41	Send:[HASH][NOTFY:R_U_THERE_ACK]	166.139.37.167	71.206.253.181	IKE
2	2009-03-09 04:17:41	The cookie pair is : 0x46CCD1E78566A8A7 / 0x5047FBE95FC2CA79	166.139.37.167	71.206.253.181	IKE
3	2009-03-09 04:17:41	Recv:[HASH][NOTFY:R_U_THERE]	71.206.253.181	166.139.37.167	IKE
4	2009-03-09 04:17:41	The cookie pair is : 0x46CCD1E78566A8A7 / 0x5047FBE95FC2CA79	71.206.253.181	166.139.37.167	IKE

A: These are normal messages back and forth between the VPN devices as they confirm that each side is still present (also known as dead-peer-detection). To suppress logging of these messages, deselect the **IKE** option on the **LOG SETTINGS** screen. This will also disable logging of routine IKE connection attempts during tunnel establishment, so be certain your tunnels are correctly configured before disabling IKE logging.

Q: Does the LAN-Cell support Mode-Config?

A: No. You must use the LAN-Cell VPN Wizard or the configuration screens to enter the necessary VPN tunnel parameters.

Q: Does the LAN-Cell support AES encryption?

A: Yes. If only “AES” is available as a choice in the LAN-Cell encryption selection boxes, it represents 128-bit AES. You can also specify the AES key length for IPSec packets via the LAN-Cell’s Command Line interface. Telnet/SSH to the device and select Menu 24, then Menu 8. Enter the following commands (case-sensitive):

```
ipsec ipsecList                    ; to get a list of IPSec Network Rules
ipsec ipsecEdit n                  ; where n is the Network rule # to edit
ipsec ipsecConfig encryAlgo 3      ; 3 is AES
ipsec ipsecConfig encryKeyLen 2    ; 0 = 128 bit, 1 = 192 bit, 2 = 256 bit
ipsec ipsecSave                    ; Save your changes
```

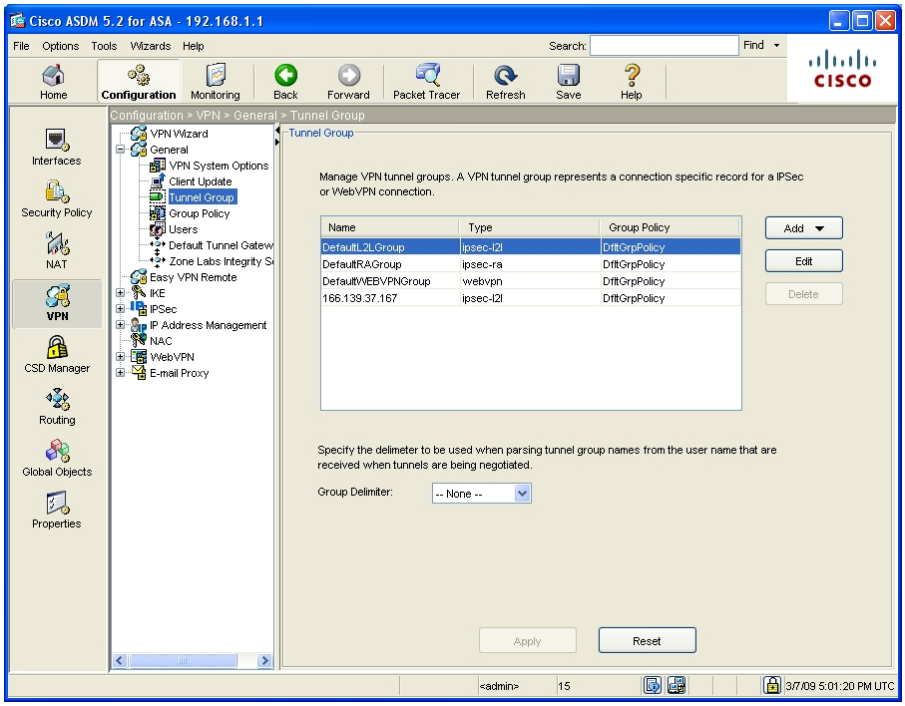
At this time, only AES-128 is supported during the IKE Phase 1 negotiation.

Appendix A: Cisco ASA 5505 Runtime Configuration – Static Tunnel

```
ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list outside_1_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-523.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 0.0.0.0 0.0.0.0
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 uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 166.139.37.167
crypto map outside_map 1 set transform-set ESP-3DES-SHA
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
```

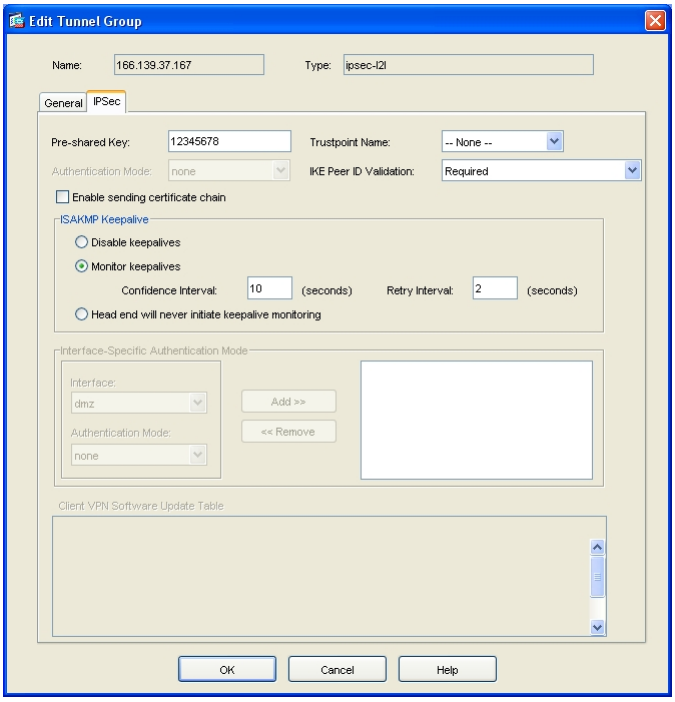
```
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
tunnel-group 166.139.37.167 type ipsec-l2l
tunnel-group 166.139.37.167 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:76025129adc08fda9a9dfc4828cf7f89
: end
```

ASDM Configuration Screens (non-Wizard mode) for Static IP Tunnel

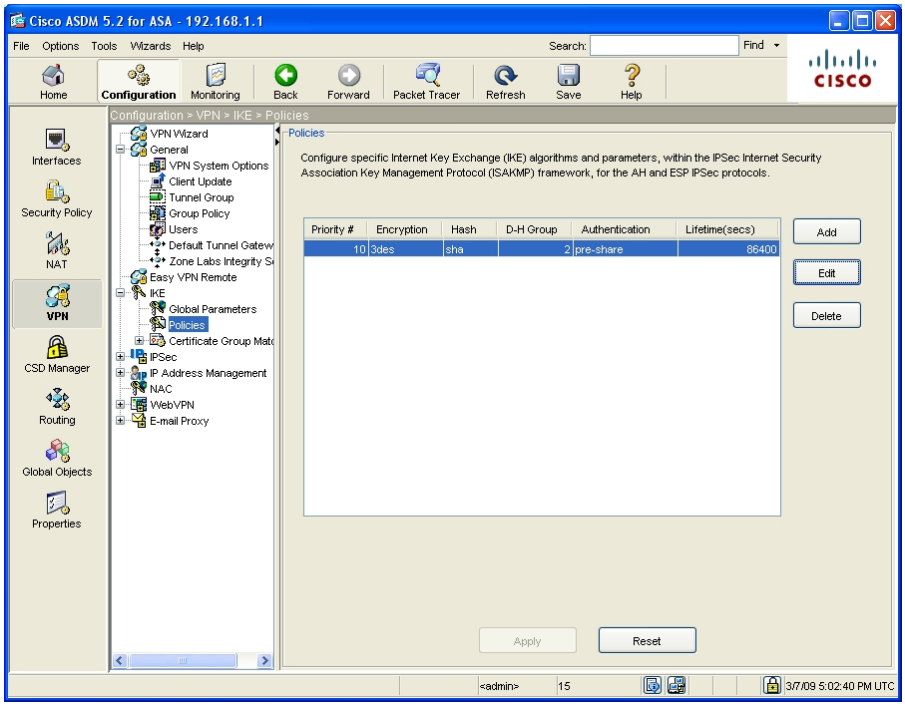


New Tunnel Group for the Remote LAN-Cell

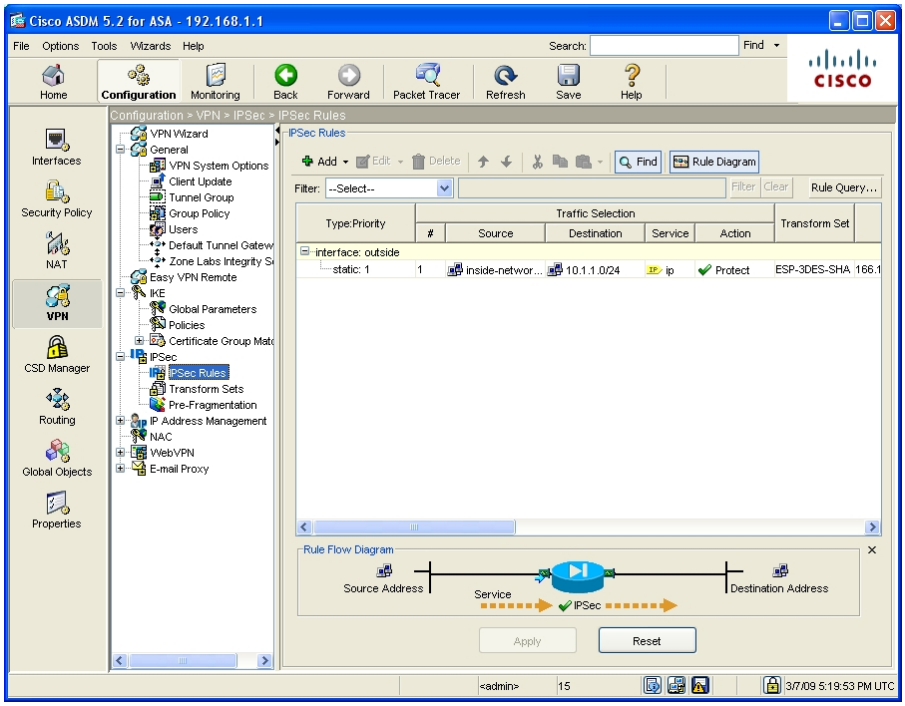
proxicast®



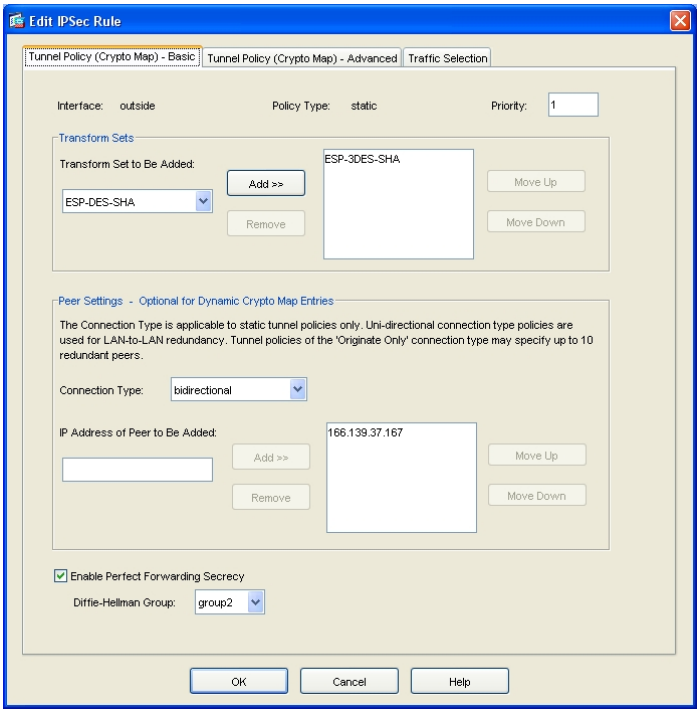
Tunnel Group Pre-Shared Key



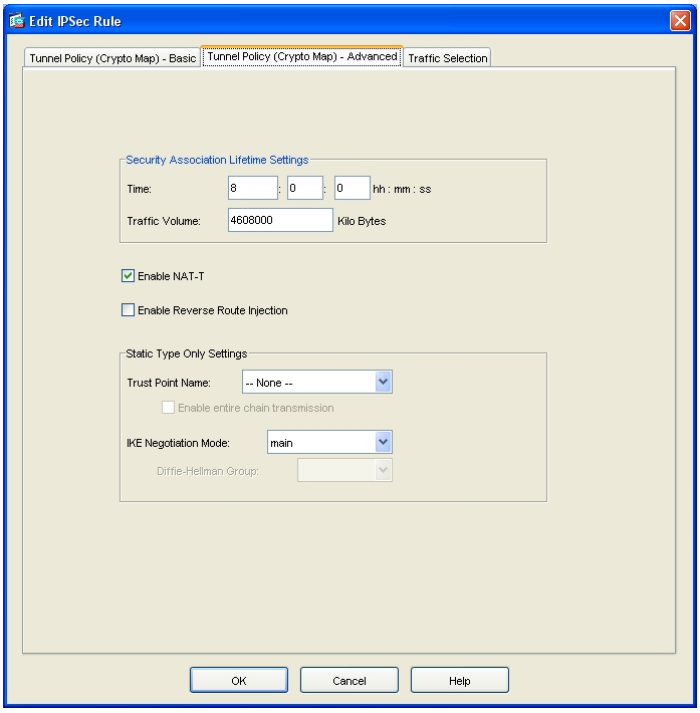
IKE Policy (Phase 1)



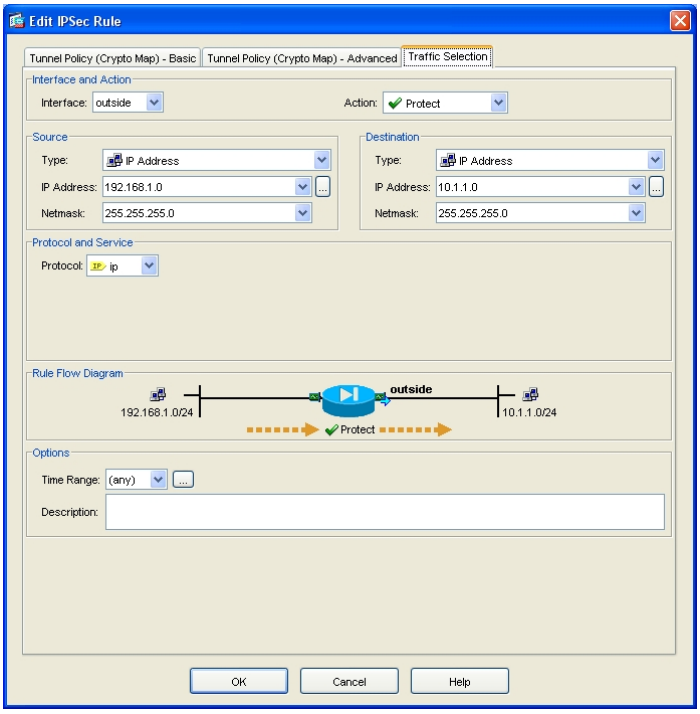
IPSec Rule Summary (Phase 2)



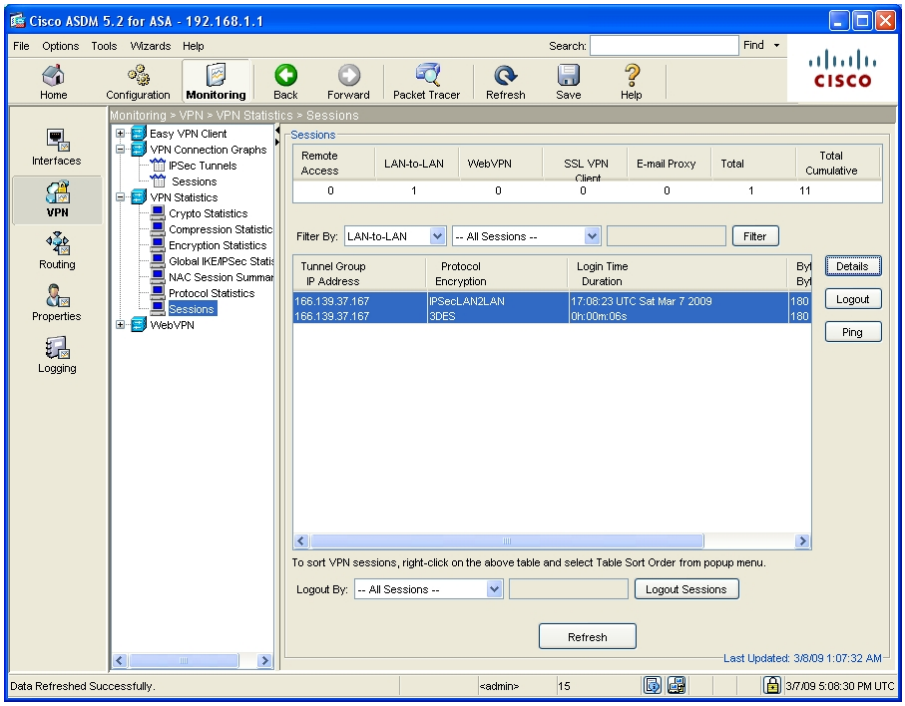
Phase 2 Crypto Map Transform Set



Phase 2 SA Lifetime



Phase 2 Local & Remote Subnets



ASDM VPN Session Monitor

Appendix B: Cisco ASA 5505 Runtime Configuration – Dynamic Tunnel

```
ASA Version 7.2(3)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list outside_cryptomap_20.1 extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-523.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list outside_cryptomap_20.1
nat (inside) 1 0.0.0.0 0.0.0.0
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 uauth 0:05:00 absolute
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto dynamic-map cisco 1 match address outside_cryptomap_20.1
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
crypto isakmp enable outside
crypto isakmp policy 20
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd auto_config outside
!
dhcpd address 192.168.1.2-192.168.1.33 inside
dhcpd enable inside
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
```

```
  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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
tunnel-group DefaultL2LGroup ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:1257f8862222f6d50d277578d65793f6
: end
```

# # #