LAN-Cell 3 to Cisco ASA 5500 VPN Example

Tech Note LCTN3014

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 3:
LC3-52U

Minimum LAN-Cell Firmware Revision: 5.1.0

Note for LAN-Cell 2 Users:

A version of this TechNote is available using the LAN-Cell 2 model. VPN configuration differs between the LAN-Cell 2 and LAN-Cell 3 models. See LCTN0014: LAN-Cell 2 to Cisco ASA 5500 VPN Example

Document Revision History:

Date	Comments
July 2, 2012	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. The LAN-Cell also supports "Remote User" VPN connections from individual PC's. That configuration is not covered in this TechNote – please refer to the Proxicast Support website for more information on Remote User VPNs.

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 a:

- Static WAN IP Address (Example 1 on page 3)
- Dynamic / Private WAN IP address (Example 2 on page 14)

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 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 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 3 with firmware version 5.1.0 and an ASA 5505 with firmware version 8.4(4). Parameters may differ slightly for other firmware versions. 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.

Please see the *LAN-Cell 3 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 (155.163.74.215) assigned to its USB modem by the cellular carrier.

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

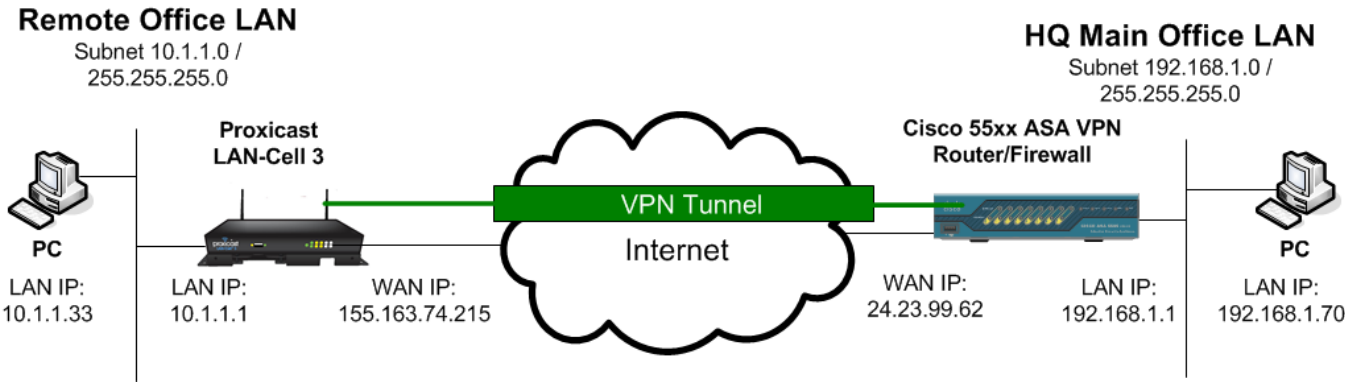


Figure 1: Example Cisco ASA Site-to-Site VPN Network Topology

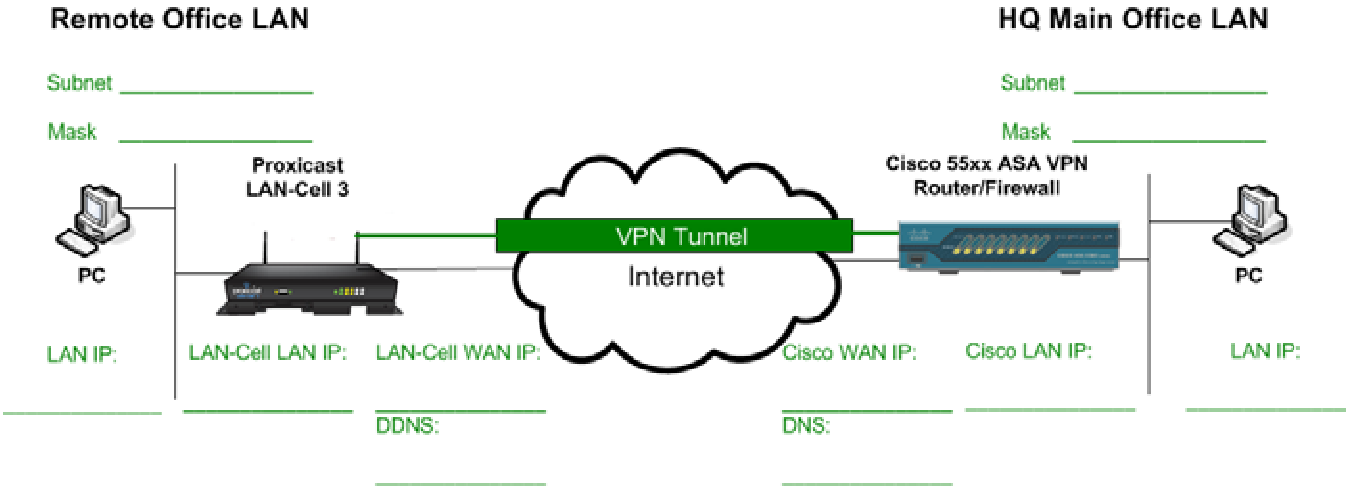
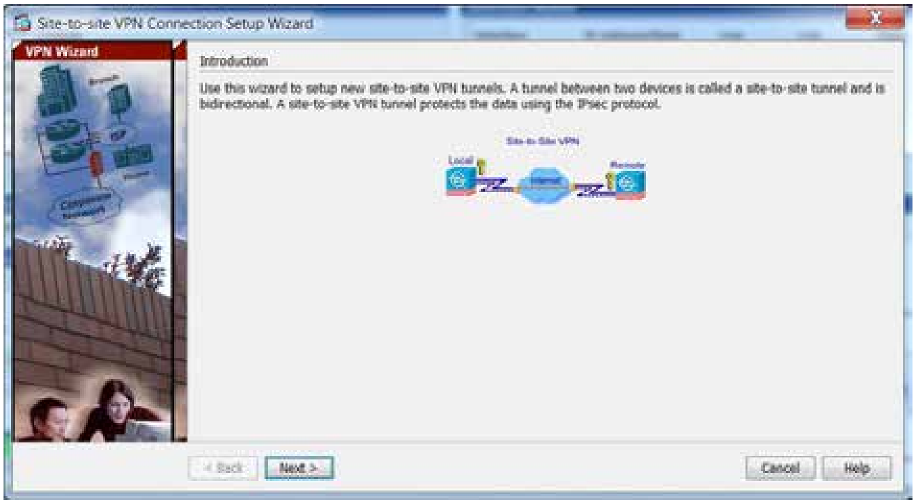


Figure 2: Your Cisco ASA Site-to-Site VPN Network Topology

Cisco ASA Parameters

For this example, we will use the Cisco ASA's VPN Wizard in the Adaptive Security Device Manager (ASDM) software v6.4. At the end of this section, the equivalent CLI commands are also shown (Figure 16).

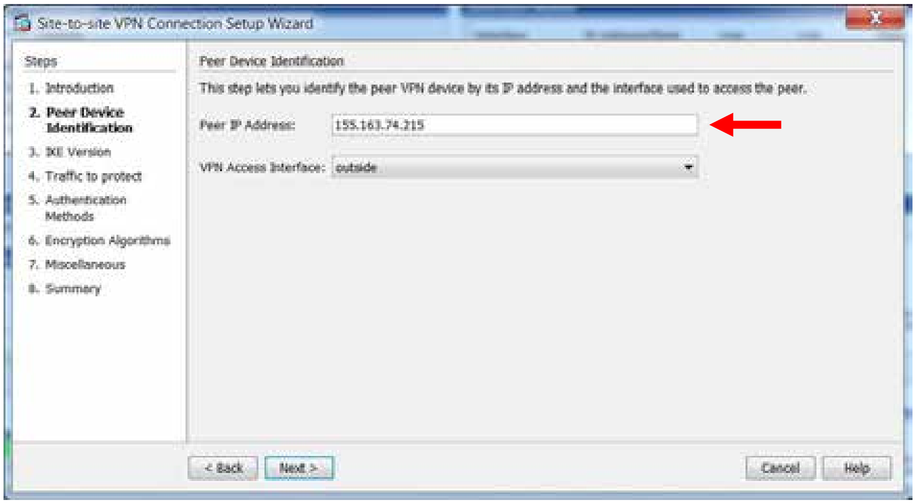
Start the Site-to-Site VPN Wizard as shown in Figure 3.



Use this wizard to setup new site-to-site VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol.

Figure 3: ASA VPN Wizard Step 1

Next, enter the static WAN IP address of the LAN-Cell (155.163.74.215 in the example) as the **Peer IP Address**.



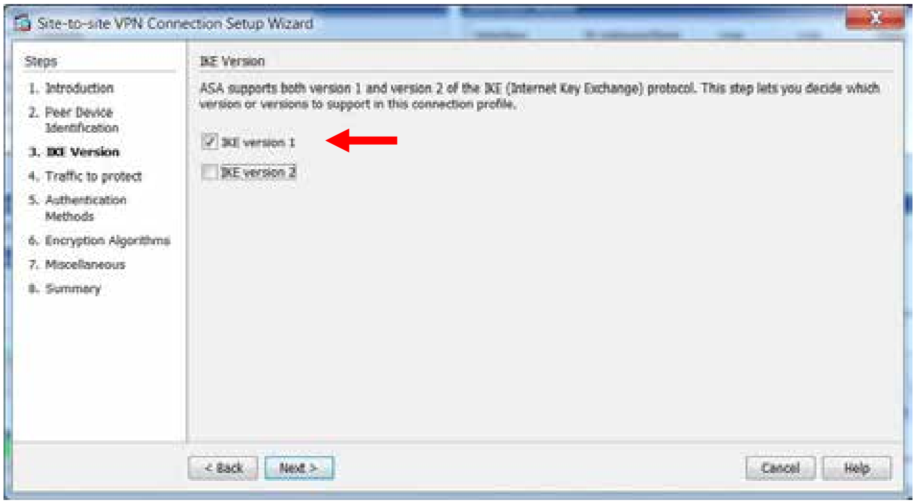
This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 155.163.74.215

VPN Access Interface: outside

Figure 4: ASA VPN Wizard Step 2

The LAN-Cell 3 supports only IKE version 1, so select that option on the next wizard screen (Figure 5).



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. **IKE Version**
4. Traffic to protect
5. Authentication Methods
6. Encryption Algorithms
7. Miscellaneous
8. Summary

IKE Version

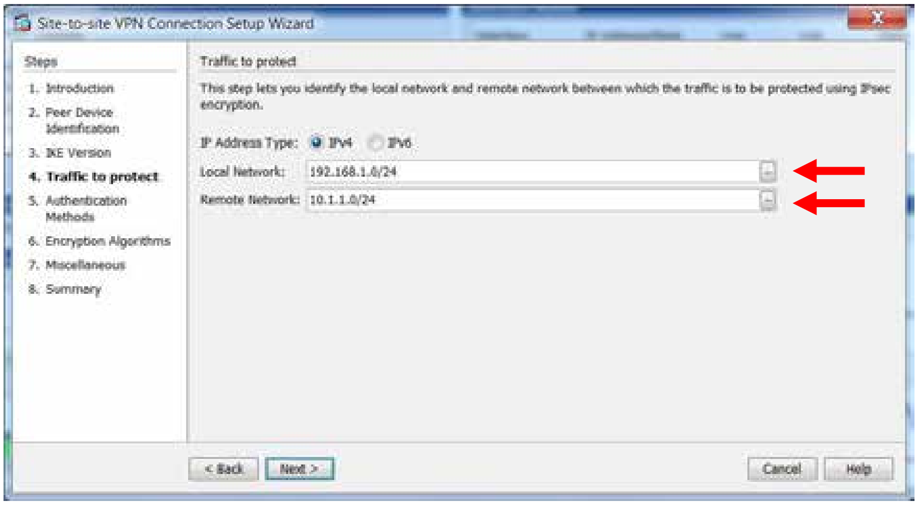
ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.

☑ IKE version 1

□ IKE version 2

Figure 5: ASA VPN Wizard Step 3

Step 4 of the ASDM VPN Wizard defines the **Local** or "inside" subnet behind the ASA (192.168.1.0) and the **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. If you prefer to use Cisco's Object nomenclature, click the button to the right of each field and define new Network Objects for these subnets.



Site-to-site VPN Connection Setup Wizard

Steps

1. Introduction
2. Peer Device Identification
3. IKE Version
4. **Traffic to protect**
5. Authentication Methods
6. Encryption Algorithms
7. Miscellaneous
8. Summary

Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

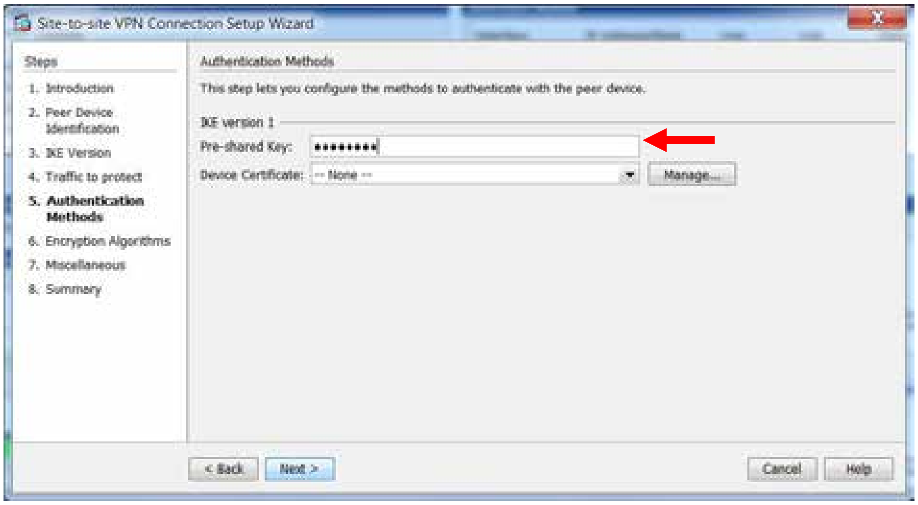
IP Address Type: ● IPv4 ○ IPv6

Local Network: 192.168.1.0/24

Remote Network: 10.1.1.0/24

Figure 6: ASA VPN Wizard Step 4

In step 5, enter a **Pre-Shared Key** value of at least 8 alphanumeric characters (Figure 7). For our example, the pre-shared key is 12345678.



This step lets you configure the methods to authenticate with the peer device.

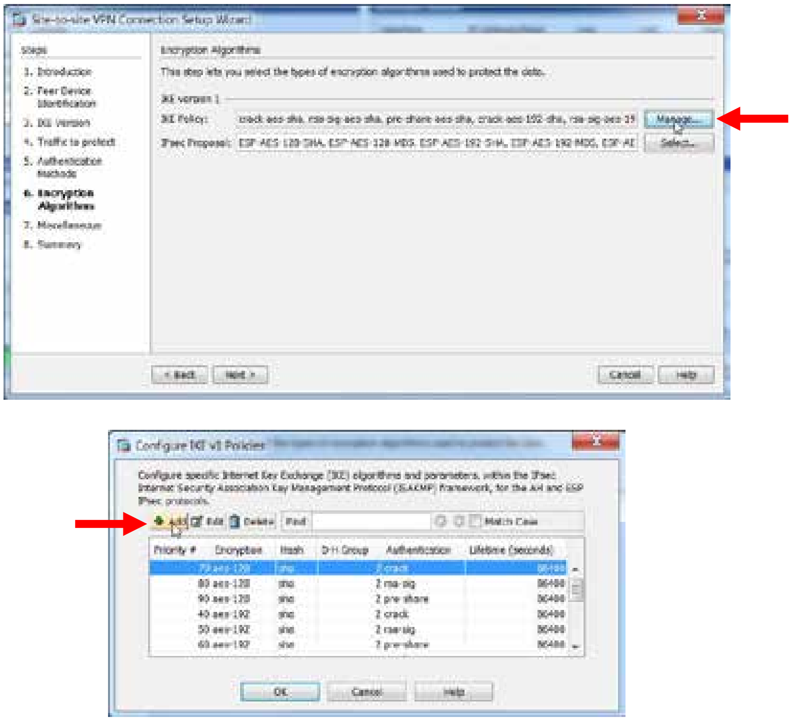
IKE version 1

Pre-shared Key: ••••••••

Device Certificate: -- None --

Figure 7: ASA VPN Wizard Step 5

VPN Wizard step 6 defines the IKE Policies and IPSec Proposals that will be valid for this tunnel. In addition to the default values, you must add a new IKE Policy to match the LAN-Cell 3's default IKE settings. Click the **Manage** and **Add** buttons to create a new IKE Policy (Figure 8).



This step lets you select the types of encryption algorithms used to protect the data.

IKE version 1

IKE Policy: crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-19

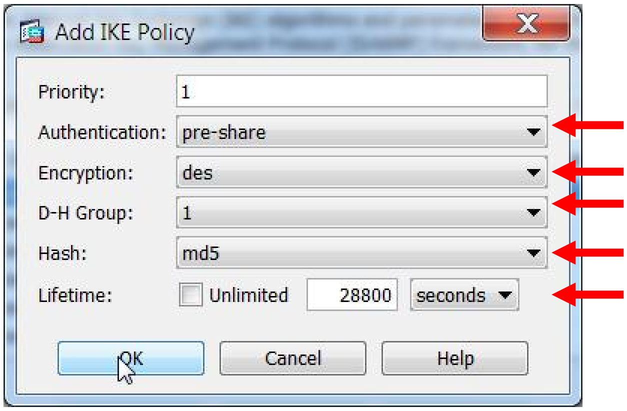
IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AE

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
70	aes-128	sha	2	crack	86400
80	aes-128	sha	2	rsa-sig	86400
90	aes-128	sha	2	pre-share	86400
40	aes-192	sha	2	crack	86400
50	aes-192	sha	2	rsa-sig	86400
60	aes-192	sha	2	pre-share	86400

Figure 8: ASA VPN Wizard Step 6

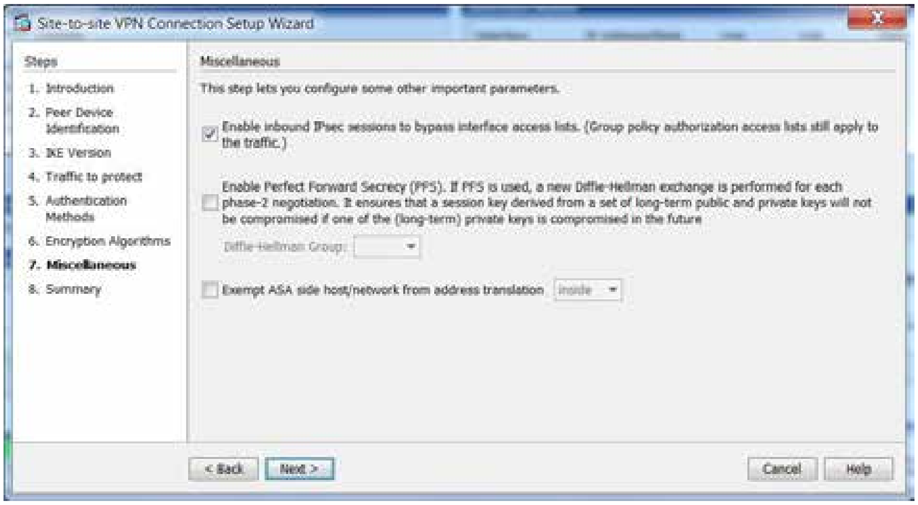
On the Add IKE Policy screen (Figure 9), select **Authentication** = pre-share, **Encryption** = DES, **D-H Group** = 1, **Hash** = md5 and **Lifetime** = 28800 seconds. Save these settings and close the Configure IKE Policies screen to return to the VPN Wizard.



Priority: 1
Authentication: pre-share
Encryption: des
D-H Group: 1
Hash: md5
Lifetime: □ Unlimited 28800 seconds

Figure 9: Adding a new IKE Policy

Step 7 (Figure 10) of the Wizard configures miscellaneous settings include **Perfect Forward Secrecy (PFS)** which is not used in our example.



Miscellaneous

This step lets you configure some other important parameters.

☑ Enable inbound IPsec sessions to bypass interface access lists. (Group policy authorization access lists still apply to the traffic.)

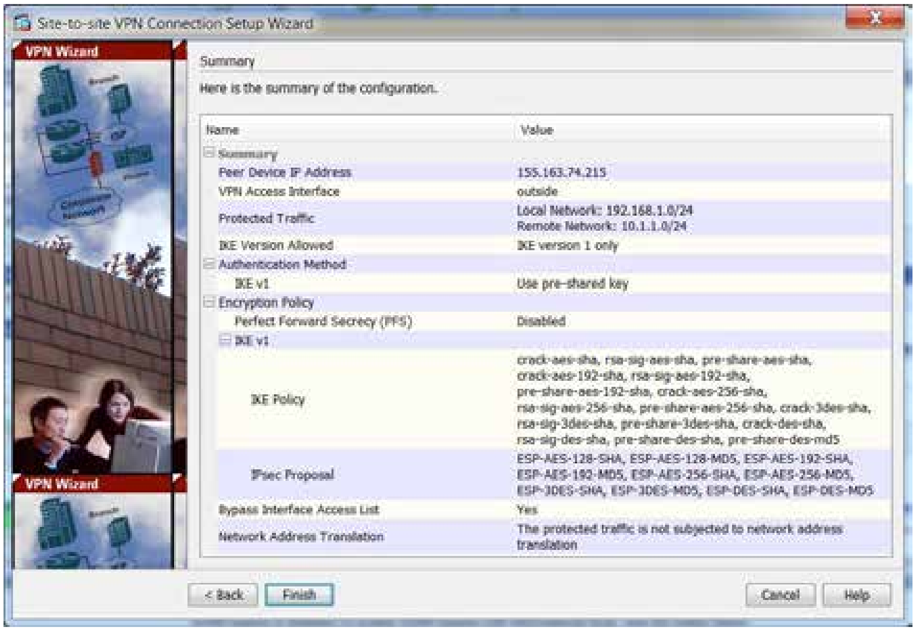
□ Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future

Diffie-Hellman Group:

□ Exempt ASA side host/network from address translation inside

Figure 10: ASA VPN Wizard Step 7

The final Wizard step (Figure 11) summarizes the VPN Tunnel settings. Review these values and make any necessary changes before finishing the Wizard.

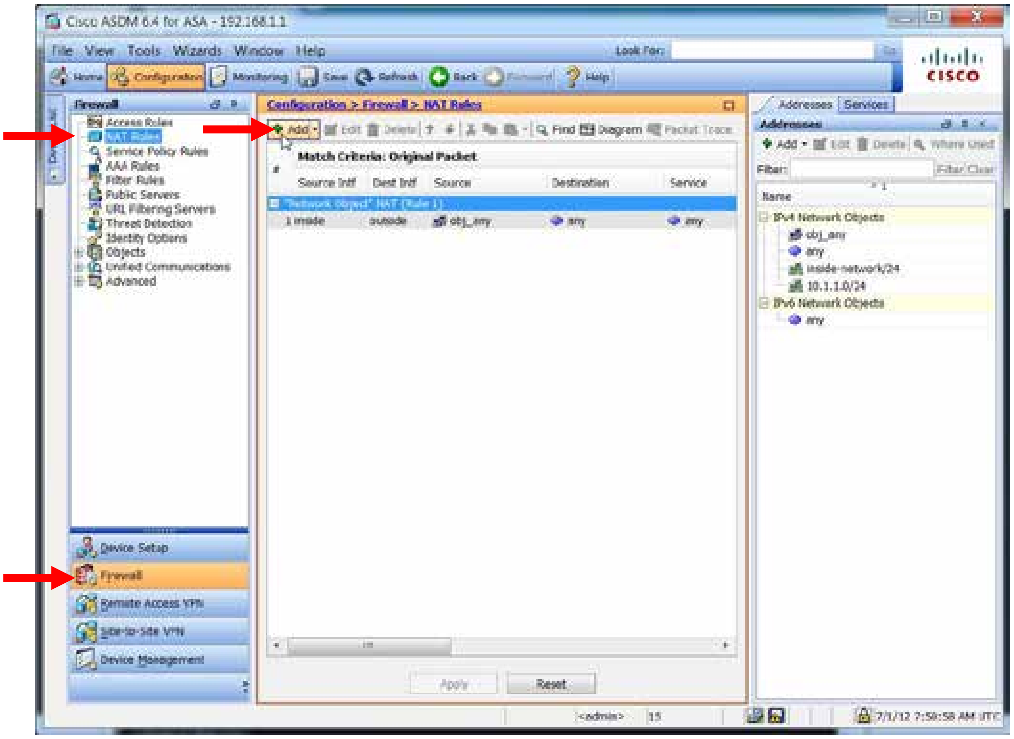


Here is the summary of the configuration.

Name	Value
Summary	
Peer Device IP Address	155.163.74.215
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.1.0/24 Remote Network: 10.1.1.0/24
IKE Version Allowed	IKE version 1 only
Authentication Method	
IKE v1	Use pre-shared key
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, crack-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-256-sha, crack-3des-sha, rsa-sig-3des-sha, pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha, pre-share-des-md5
IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
Bypass Interface Access List	Yes
Network Address Translation	The protected traffic is not subjected to network address translation

Figure 10: ASA VPN Wizard Step 8

After completing the VPN Wizard, you must add a Network Address Translation (NAT) rule for traffic between the two subnets. In ASDM, select **Configuration > Firewall, NAT Rules** and then the **Add** button (see Figure 11)



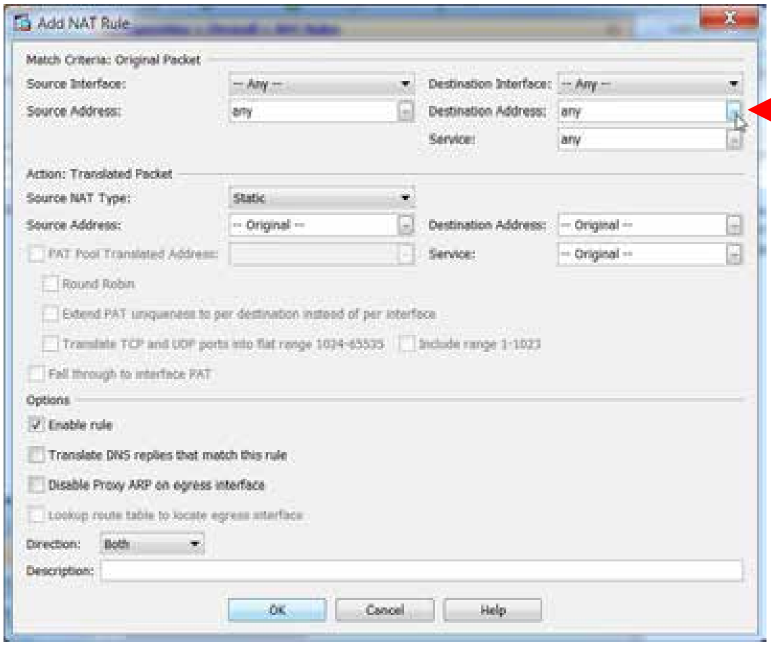
Match Criteria: Original Packet

#	Source Intf	Dest Intf	Source	Destination	Service
"Network Object" NAT (Rule 1)					
1	inside	outside	obj_any	any	any

Figure 11: ASA Adding a NAT Rule

proxicast®

On the Add NAT Rule screen, click the button to the right of the **Destination Address** field (Figure 12).



Add NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any --
Destination Interface: -- Any --
Source Address: any
Destination Address: any
Service: any

Action: Translated Packet

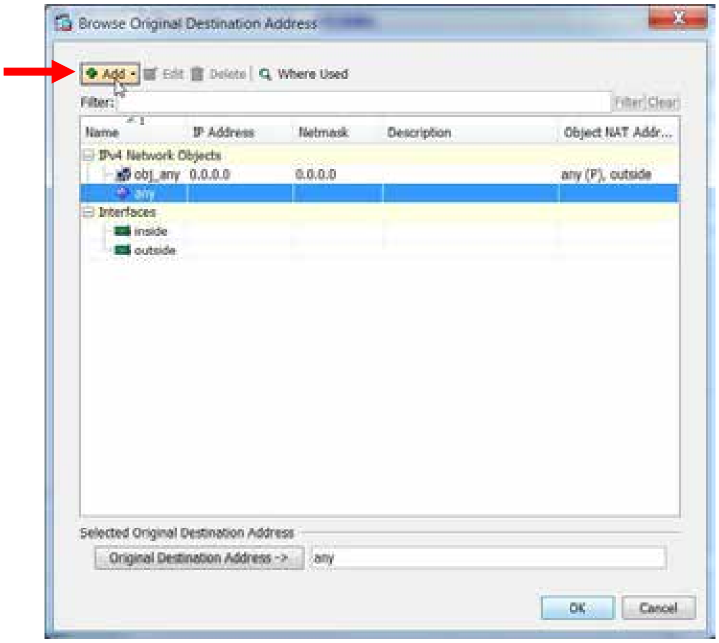
Source NAT Type: Static
Source Address: -- Original --
Destination Address: -- Original --
□ PAT Pool Translated Address:
Service: -- Original --
□ Round Robin
□ Extend PAT uniqueness to per destination instead of per interface
□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023
□ Fall through to interface PAT

Options

☑ Enable rule
□ Translate DNS replies that match this rule
□ Disable Proxy ARP on egress interface
□ Lookup route table to locate egress interface
Direction: Both
Description:

Figure 12: Add NAT Rule Screen

The click the **Add** button to add a new Destination Address object definition (Figure 13)



Browse Original Destination Address

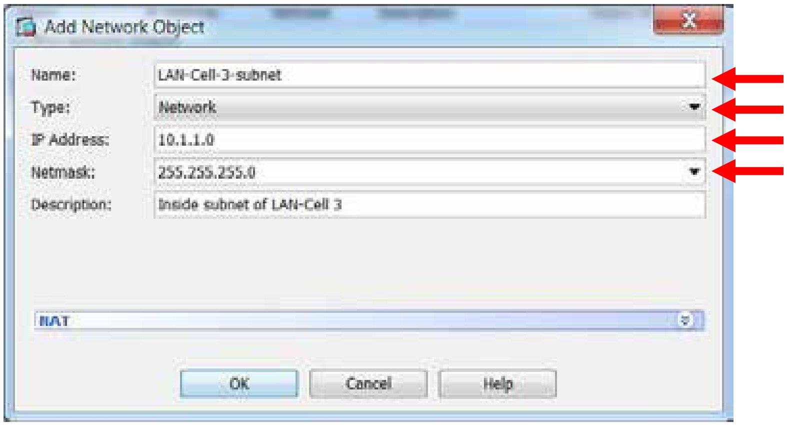
Name	IP Address	Netmask	Description	Object NAT Addr...
IPv4 Network Objects				
obj_any	0.0.0.0	0.0.0.0		any (P), outside
any				
Interfaces				
inside				
outside				

Selected Original Destination Address

Original Destination Address -> any

Figure 13: Adding a Destination Address Object

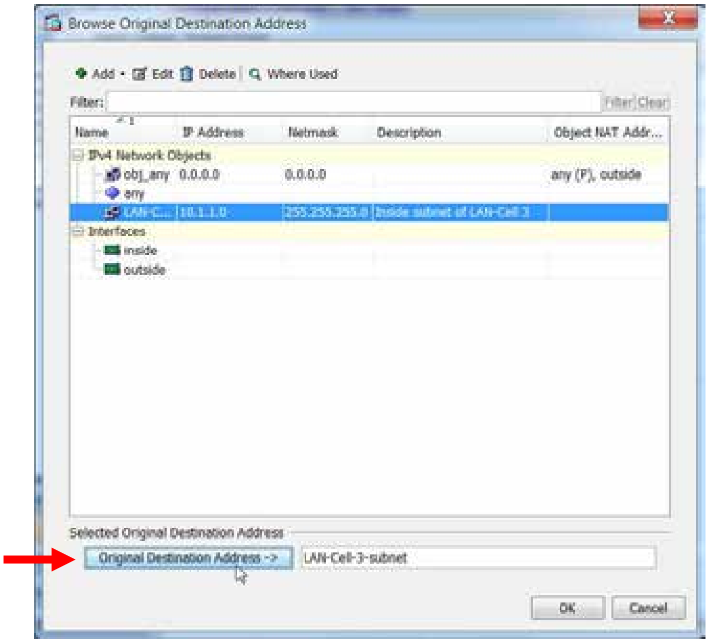
On the Add Network Object screen (Figure 14), give the destination object a **Name**, select Network as the **Type** and enter the **IP address** and **Netmask** of the LAN-Cell's private subnet (10.1.1.0 / 255.255.255.0 in our example). You can also give the object an optional description.



Name: LAN-Cell-3-subnet
Type: Network
IP Address: 10.1.1.0
Netmask: 255.255.255.0
Description: Inside subnet of LAN-Cell 3

Figure 14: Add Network Object Screen

Click OK to return to the Browse Original Destination Address screen (Figure 15). Be certain to assign the new network object value by clicking the **Original Destination Address** button at the bottom of the screen. Click OK on this screen and the next to return to the ADSM Configuration screen.



Name	IP Address	Netmask	Description	Object NAT Addr...
IPv4 Network Objects				
obj_any	0.0.0.0	0.0.0.0		any (P), outside
any				
LAN-C...	10.1.1.0	255.255.255.0	Inside subnet of LAN-Cell 3	
Interfaces				
inside				
outside				

Selected Original Destination Address
Original Destination Address -> LAN-Cell-3-subnet

Figure 15: Assigning Network Object to Destination Address

Configuration of the Cisca ASA is now complete.

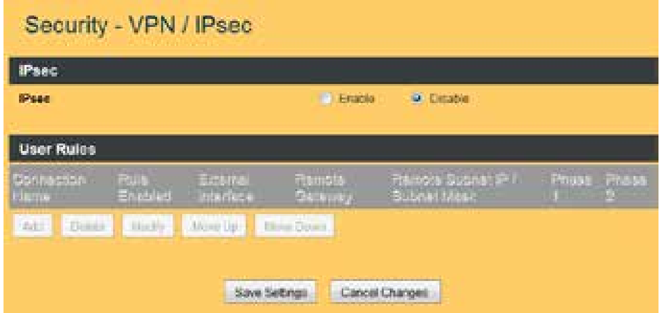
The relevant commands that ASDM applied to the ASA device are summarized below (Figure 16). A complete listing of the ASA's running configuration is shown in Appendix A.

```
object network LAN-Cell-3-subnet
  subnet 10.1.1.0 255.255.255.0
  description Inside subnet of LAN-Cell 3
  access-list outside_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0

nat (any,any) source static any any destination static LAN-Cell-3-subnet LAN-Cell-3-subnet

crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac

crypto map outside_map 1 match address outside_cryptomap

crypto map outside_map 1 set peer 155.163.74.215

crypto map outside_map 1 set ikev1 transform-set ESP-DES-MD5

crypto map outside_map interface outside

crypto ikev1 enable outside

crypto ikev1 policy 1
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800

group-policy GroupPolicy_155.163.74.215 internal

group-policy GroupPolicy_155.163.74.215 attributes
 vpn-tunnel-protocol ikev1

tunnel-group 155.163.74.215 type ipsec-l2l

tunnel-group 155.163.74.215 general-attributes
 default-group-policy GroupPolicy_155.163.74.215

tunnel-group 155.163.74.215 ipsec-attributes
 ikev1 pre-shared-key *****
```

Figure 16: ASA VPN Commands (Static IP Tunnel)

LAN-Cell VPN Setup

To configure the LAN-Cell 3, select the **Security > VPN/IPSec** screen. Select **Enable** to enable the IPSec functionality and click the **Add** button to create a new IPSec Rule (Figure 17).



Security - VPN / IPsec

IPsec

IPsec ○ Enable ● Disable

User Rules

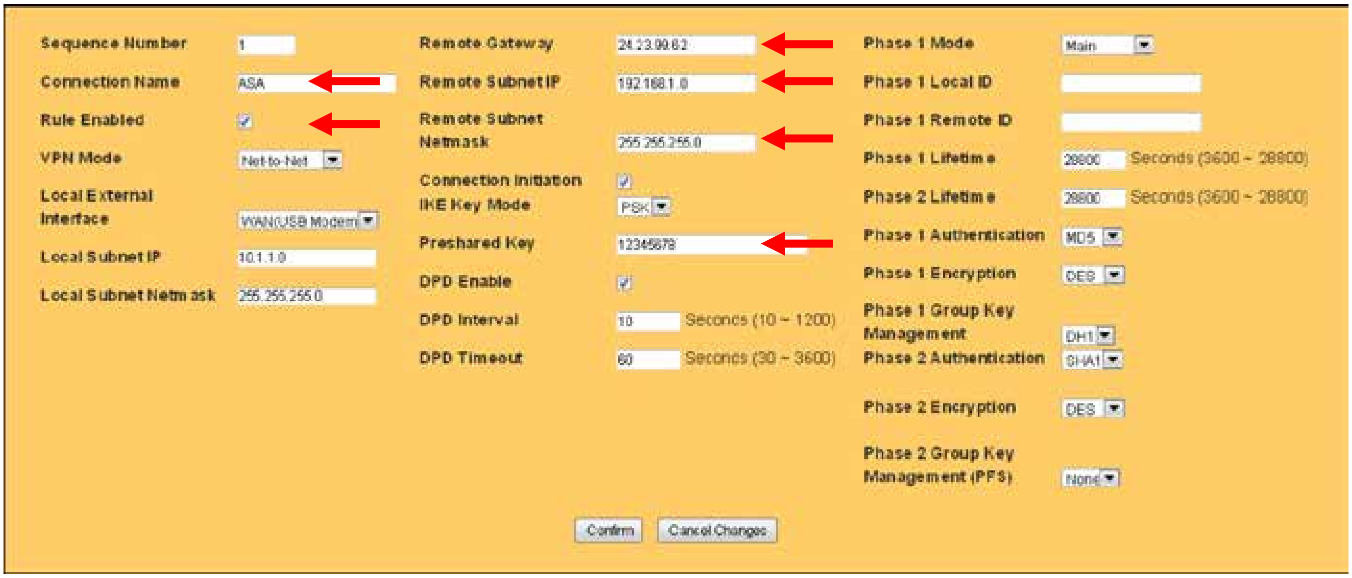
Connection Name	Rule Enabled	External Interface	Remote Gateway	Remote Subnet IP / Subnet Mask	Phase 1	Phase 2

Figure 17: LAN-Cell VPN / IPSec Screen

In the VPN Rule popup window (Figure 18), we will accept most of the default values. However, you must give the rule a **Connection Name** and mark it **Enabled**. Specify the public IP address of the ASA's outside (WAN) interface (24.23.99.62 in our example) as the **Remote Gateway** and also enter the private (inside) subnet of the ASA (192.168.1.0 / 255.255.255.0) as the **Remote Subnet IP** and **Netmask**.

Connection Initiation means that the LAN-Cell will initiate a VPN connection to the ASA and continue to bring the tunnel up whenever it goes down. If you want the tunnel to be established only when traffic from the LAN-Cell is destined for the ASA's private subnet, remove the check in this field.

Also enter the **Preshared Key** value that matches the preshared key entered on the ASA.



Sequence Number: 1
Connection Name: ASA
Rule Enabled: ☑
VPN Mode: Net-to-Net
Local External Interface: WAN(USB Modem)
Local Subnet IP: 10.1.1.0
Local Subnet Netmask: 255.255.255.0

Remote Gateway: 24.23.99.62
Remote Subnet IP: 192.168.1.0
Remote Subnet Netmask: 255.255.255.0
Connection Initiation: ☑
IKE Key Mode: PSK
Preshared Key: 12345678
DPD Enable: ☑
DPD Interval: 10 Seconds (10 ~ 1200)
DPD Timeout: 60 Seconds (30 ~ 3600)

Phase 1 Mode: Main
Phase 1 Local ID:
Phase 1 Remote ID:
Phase 1 Lifetime: 28800 Seconds (3600 ~ 28800)
Phase 2 Lifetime: 28800 Seconds (3600 ~ 28800)
Phase 1 Authentication: MD5
Phase 1 Encryption: DES
Phase 1 Group Key Management: DH1
Phase 2 Authentication: SHA1
Phase 2 Encryption: DES
Phase 2 Group Key Management (PFS): None

Figure 18: LAN-Cell 3 IPSec VPN Rule Definition

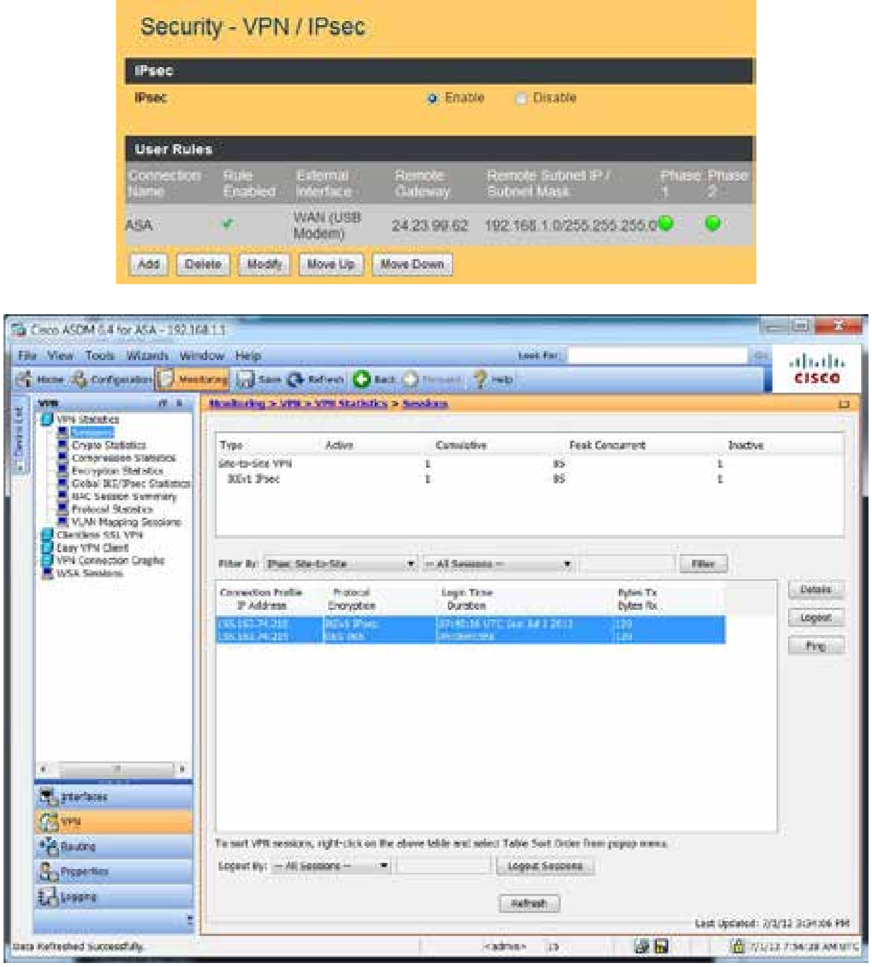
Click **Confirm** to close the popup window and click **Save Settings** to save the VPN rule.

Configuration of the LAN-Cell 3 is now complete.

Opening a VPN Tunnel

Always On

If you checked the **Connection Initiation** box on the LAN-Cell 3's VPN Rule, then the LAN-Cell will immediately attempt to establish the VPN tunnel. If the tunnel parameters are correct, the tunnel is often opened before the VPN/IPSec screen is refreshed. Colored icons next to the rule indicate the tunnel status, with green indicating an active tunnel (Figure 19).



Security - VPN / IPsec

IPsec

IPsec ● Enable ○ Disable

User Rules

Connection Name	Rule Enabled	External Interface	Remote Gateway	Remote Subnet IP / Subnet Mask	Phase 1	Phase 2
ASA	✓	WAN (USB Modem)	24.23.99.62	192.168.1.0/255.255.255.0	●	●

Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	85	1	
IKEv1 IPsec	1	85	1	

Filter By: IPsec Site-to-Site | -- All Sessions --

Connection Profile IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
[illegible] [illegible]	IKEv1 IPsec [illegible]	[illegible] [illegible]	120 120

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Last Updated: 7/3/12 3:34:06 PM

Data Refreshed Successfully.

Figure 19: Active VPN Tunnel on LAN-Cell & Cisco ASA

Traffic Generation

If **Connection Initiation** is not checked (and the ASA is not configured to keep the tunnel open), 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 or Private 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. This same configuration applies if your ISP assigns a private (non-Internet accessible) IP address to the LAN-Cell's WAN interface. 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 either use ASDM to make the necessary changes or manually enter the commands to create the proper policies (Figure 20).

A complete listing of the ASA's runtime configuration in shown in Appendix B.

```
object network 10.1.1.0
 subnet 10.1.1.0 255.255.255.0
 description LC3 inside subnet

access-list outside_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0

nat (any,any) source static any any destination static 10.1.1.0 10.1.1.0

crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map LC3-Dynamic-IP 1 match address outside_cryptomap
crypto dynamic-map LC3-Dynamic-IP 1 set ikev1 transform-set ESP-DES-SHA ESP-DES-MD5
crypto map outside_map1 1 ipsec-isakmp dynamic LC3-Dynamic-IP
crypto map outside_map1 interface outside
crypto ikev1 enable outside
crypto ikev1 enable inside
crypto ikev1 policy 1
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800

group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-clientless
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key *****
 peer-id-validate nocheck
```

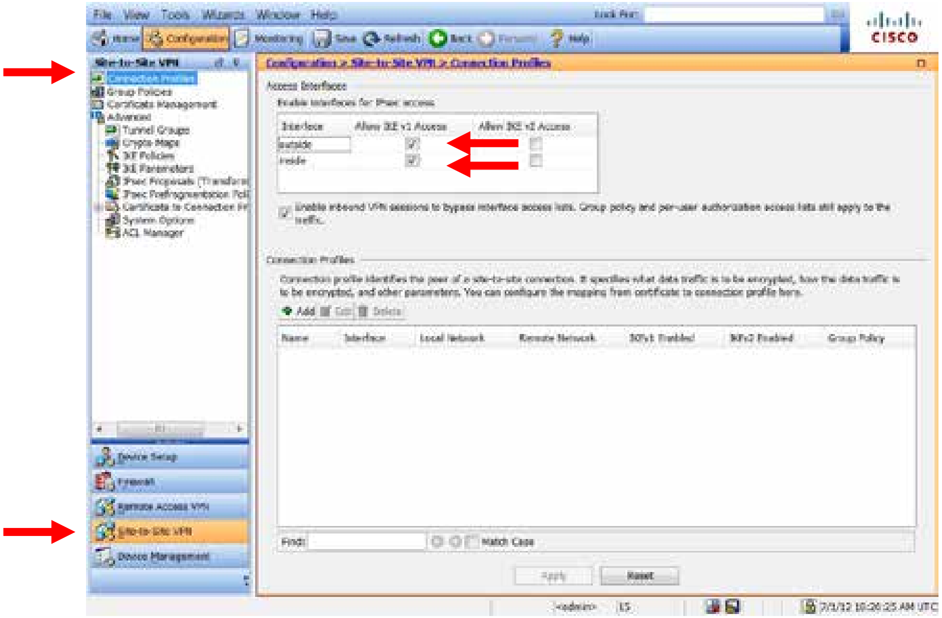
Figure 20: ASA VPN Commands (Dynamic Tunnel)

Note that we have modified the default L2L Tunnel Group on the ASA to have the Pre-Shared Key from the LAN-Cell. This is necessary so that IKE Main Mode negotiation can take place. No two Tunnel Groups should have the same Pre-Shared Key; the ASA will use the Pre-Shared Key value along with the Tunnel Group Name to match the incoming IKE request from the LAN-Cell and determine the correct tunnel parameters to use. We have also disabled peer ID validation since the address of the LAN-Cell will not match the tunnel group rule.

[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 ASA product line does not currently offer this feature. Contact Cisco for more information on the availability of this feature for your specific device.

To make these changes via ASDM, complete the following screens:

On the Connection Profiles screen (Figure 21), ensure that **IKE v1 Access** is enabled on both the inside and outside interfaces.



Configuration > Site-to-Site VPN > Connection Profiles

Access Interfaces

Enable interfaces for IPsec access

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	☑	□
inside	☑	□

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

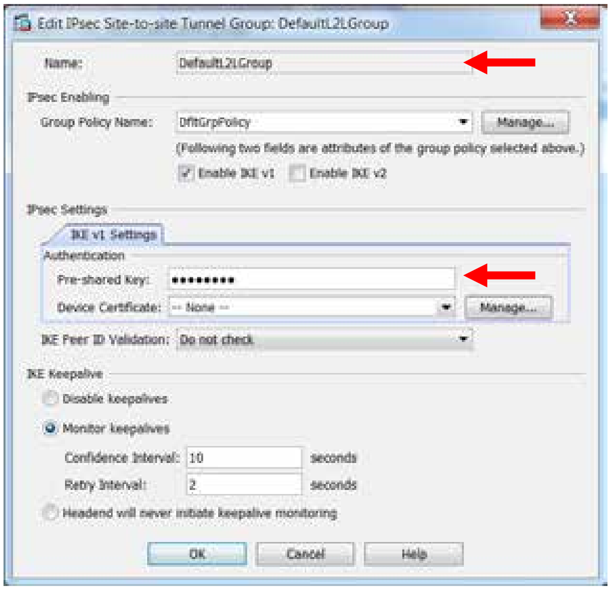
Connection Profiles

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy

Figure 21: Connection Profile Settings

On the Tunnel Groups screen (Figure 22), change the DefaultL2LGroup's IKE v1 **Pre-shared Key** to 12345678.



Edit IPsec Site-to-site Tunnel Group: DefaultL2LGroup

Name: DefaultL2LGroup

IPsec Enabling

Group Policy Name: DfltGrpPolicy

(Following two fields are attributes of the group policy selected above.)

☑ Enable IKE v1 □ Enable IKE v2

IPsec Settings

IKE v1 Settings

Authentication

Pre-shared Key: ●●●●●●●●●

Device Certificate: -- None --

IKE Peer ID Validation: Do not check

IKE Keepalive

○ Disable keepalives

● Monitor keepalives

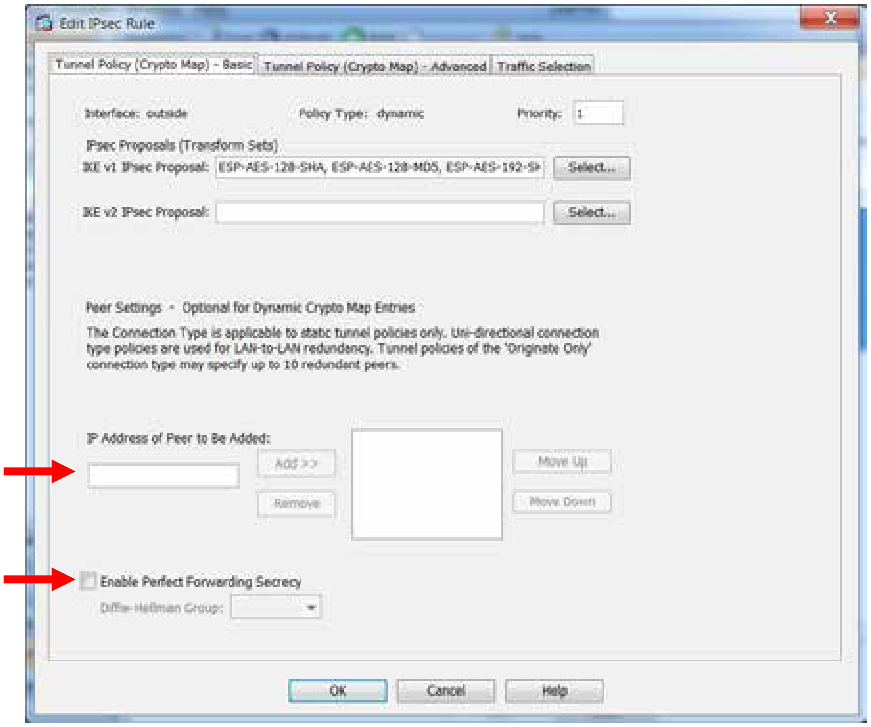
Confidence Interval: 10 seconds

Retry Interval: 2 seconds

○ Headend will never initiate keepalive monitoring

Figure 22: Tunnel Groups

On the Crypto Maps screen (Figure 23), ensure that the **Peer IP Address** is blank and the **PFS** is not selected.



Interface: outside   Policy Type: dynamic   Priority: 1

IPsec Proposals (Transform Sets)

IKE v1 IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SH

IKE v2 IPsec Proposal:

Peer Settings - Optional for Dynamic Crypto Map Entries

The Connection Type is applicable to static tunnel policies only. Uni-directional connection type policies are used for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may specify up to 10 redundant peers.

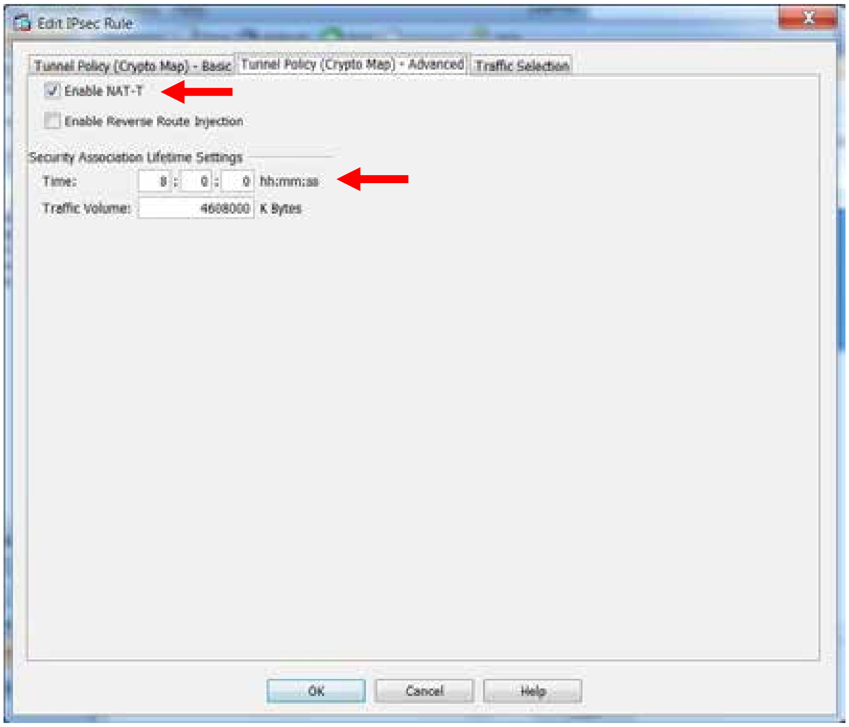
IP Address of Peer to Be Added:

□ Enable Perfect Forwarding Secrecy

Diffie-Hellman Group:

Figure 23: IPSec Rule Crypto Map Basic

On the Advanced tab (Figure 24), ensure that **NAT-T** is enabled and the **SA Lifetime** is 8 hours.


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
OK
Cancel
Help

☑ Enable NAT-T

□ Enable Reverse Route Injection

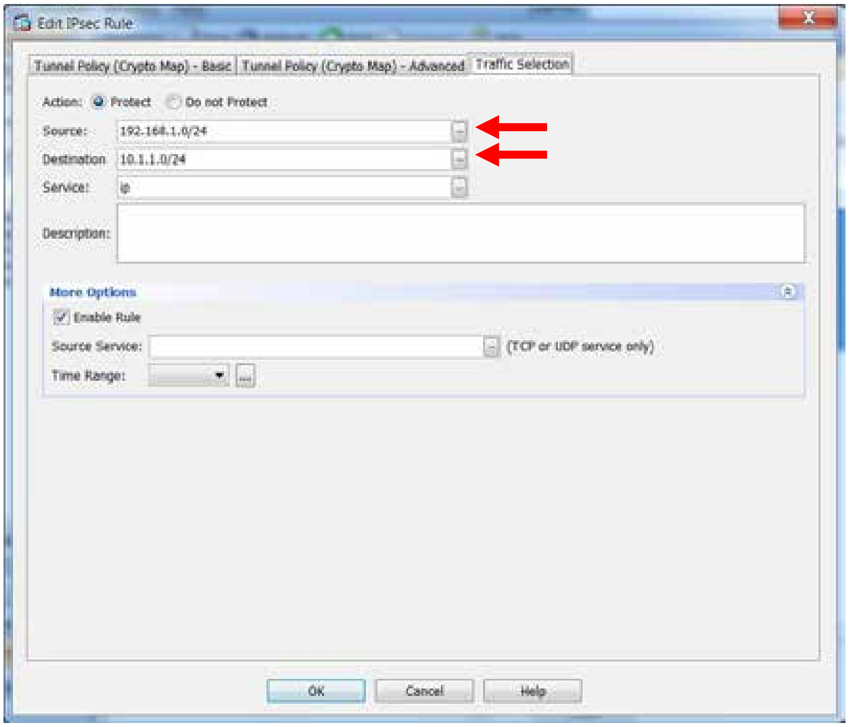
Security Association Lifetime Settings

Time: 8 : 0 : 0 hh:mm:ss

Traffic Volume: 4608000 K Bytes

Figure 24: IPSec Rule Crypto Map Advanced

On the Traffic Selection tab (Figure 25), enter the ASA's inside subnet as the **Source** and the LAN-Cell's inside subnet as the **Destination**.


Edit IPsec Rule
Tunnel Policy (Crypto Map) - Basic
Tunnel Policy (Crypto Map) - Advanced
Traffic Selection
More Options
OK
Cancel
Help

Action: ● Protect ○ Do not Protect

Source: 192.168.1.0/24

Destination: 10.1.1.0/24

Service: ip

Description:

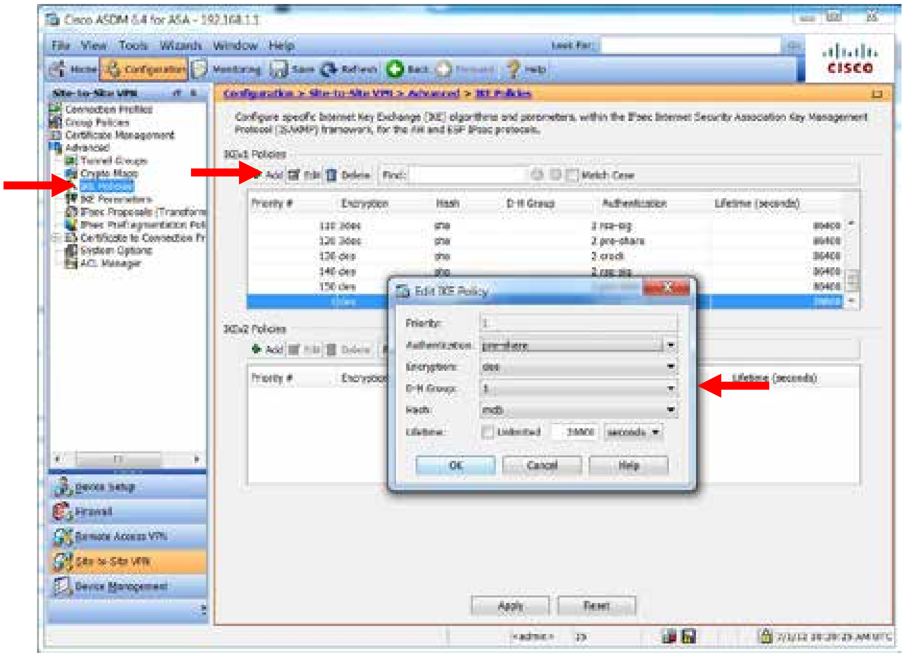
☑ Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

Figure 25: IPSec Rule Crypto Map Traffic Selection

Create a new IKE Policy (Figure 26) to match the LAN-Cell's defaults of pre-share, DES, DH1, MD5 & 28800.



Configuration > Site-to-Site VPN > Advanced > IKE Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

IKEv1 Policies

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
110	3des	sha	2	rsa-sig	86400
120	3des	sha	2	pre-share	86400
130	des	sha	2	crack	86400
140	des	sha	2	rsa-sig	86400
150	des				86400

IKEv2 Policies

Priority #	Encryption	Lifetime (seconds)

Priority: 1

Authentication: pre-share

Encryption: des

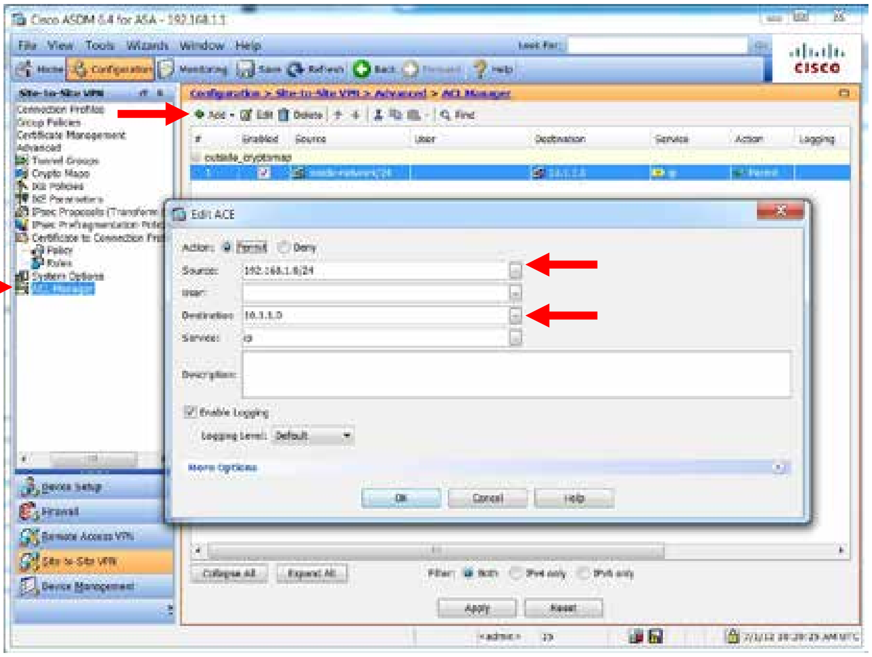
D-H Group: 1

Hash: md5

Lifetime: □ Unlimited 28800 seconds

Figure 26: New IKE Policy

Create a new Access Control Entry (Figure 27) to permit traffic between the 2 subnets.



Edit ACE

Action: ● Permit ○ Deny

Source: 192.168.1.0/24

User:

Destination: 10.1.1.0

Service: ip

Description:

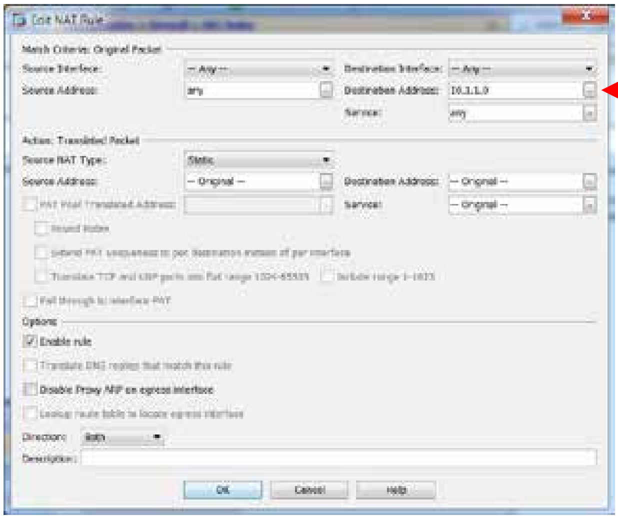
☑ Enable Logging

Logging Level: Default

Cisco ASDM 6.4 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Site-to-Site VPN
Connection Profiles
Group Policies
Certificate Management
Advanced
Tunnel Groups
Crypto Maps
IKE Policies
IKE Parameters
IPsec Proposals (Transform Sets)
IPsec Prefragmentation Policies
Certificate to Connection Profile Maps
Policy
Rules
System Options
ACL Manager
Configuration > Site-to-Site VPN > Advanced > ACL Manager
Add Edit Delete Find
# Enabled Source User Destination Service Action Logging
outside_cryptomap
inside-network/24
10.1.1.0
ip
Permit
More Options
OK Cancel Help
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Collapse All Expand All
Filter: Both IPv4 only IPv6 only
Apply Reset
<admin>

Figure 27: New Access Control Entry

Finally, create a new NAT Rule in the Firewall section (Figure 28) for the LAN-Cell's private subnet.



Edit NAT Rule

Match Criteria: Original Packet

Source Interface: -- Any --

Destination Interface: -- Any --

Source Address: any

Destination Address: 10.1.1.0

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original --

Destination Address: -- Original --

□ PAT Pool Translated Address:

Service: -- Original --

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT

Options

☑ Enable rule

□ Translate DNS replies that match this rule

□ Disable Proxy ARP on egress interface

□ Lookup route table to locate egress interface

Direction: Both

Description:

Figure 27: New NAT Rule

LAN-Cell VPN Setup

The configuration on the LAN-Cell is exactly the same regardless of whether its WAN interface has a static, dynamic or private IP address. Refer to Figure 18 for the LAN-Cell's VPN IPSec Rule configuration.

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

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 (ESP) traffic in both directions.

- 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*
  You must enter an IP address other than blank 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.

- *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 (or /24). Also the private subnets behind each VPN device must be different.

- *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

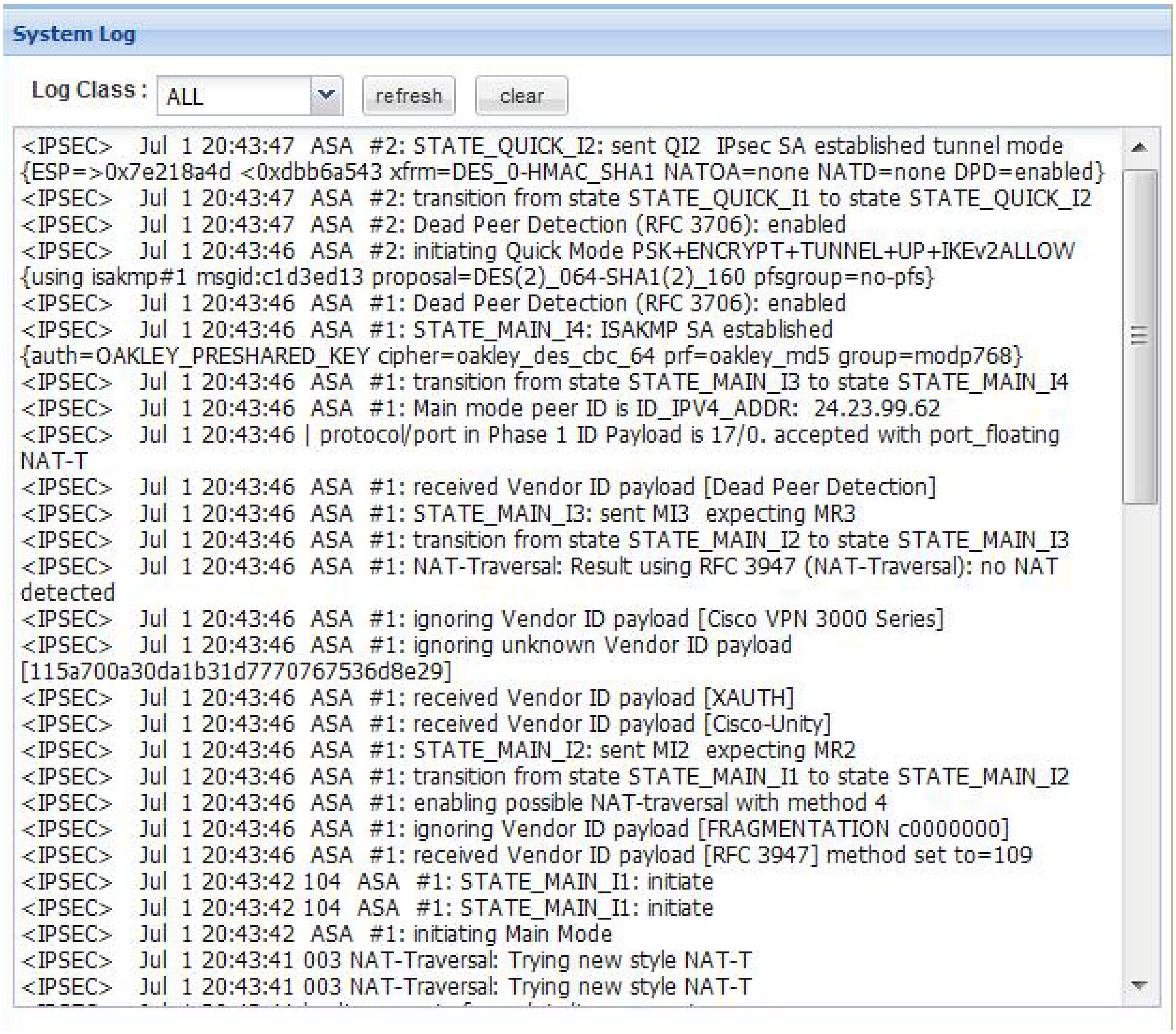
Logging

If initial attempts at creating the VPN tunnel are unsuccessful, use the **ADMIN > LOGS** screen to obtain more information about the failure. You should also consult the logs and documentation for your Cisco VPN appliance for additional troubleshooting assistance. Cisco ASA VPN debugging can be enabled with the commands:

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

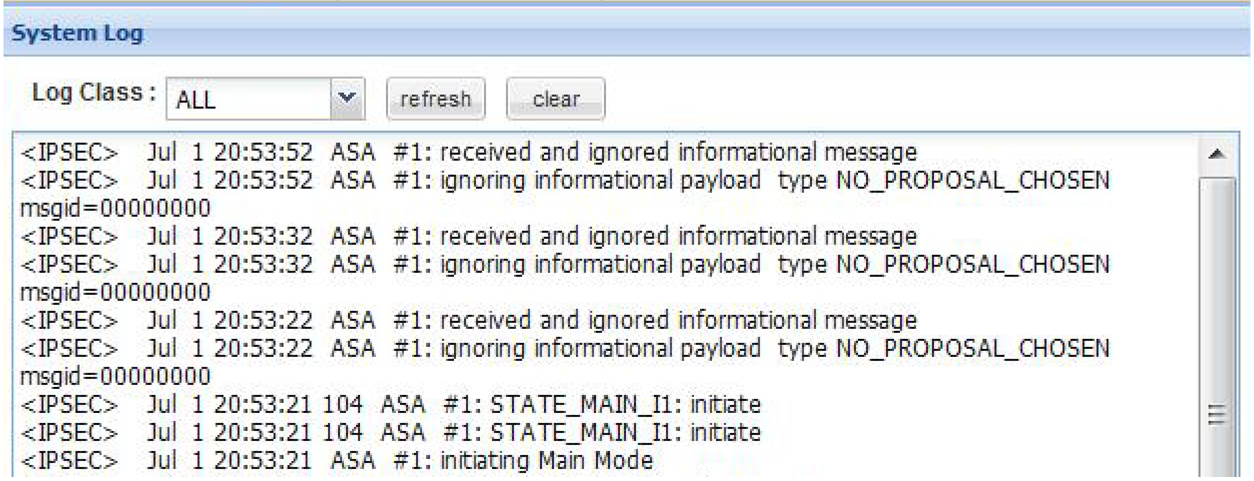
Here are some common VPN-related error messages from the LAN-Cell's log:

Successful VPN Tunnel Creation:



```
<IPSEC>   Jul  1 20:43:47  ASA  #2: STATE_QUICK_I2: sent QI2  IPsec SA established tunnel mode
{ESP=>0x7e218a4d <0xdbb6a543 xfrm=DES_0-HMAC_SHA1 NATOA=none NATD=none DPD=enabled}
<IPSEC>   Jul  1 20:43:47  ASA  #2: transition from state STATE_QUICK_I1 to state STATE_QUICK_I2
<IPSEC>   Jul  1 20:43:47  ASA  #2: Dead Peer Detection (RFC 3706): enabled
<IPSEC>   Jul  1 20:43:46  ASA  #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+IKEv2ALLOW
{using isakmp#1 msgid:c1d3ed13 proposal=DES(2)_064-SHA1(2)_160 pfsgroup=no-pfs}
<IPSEC>   Jul  1 20:43:46  ASA  #1: Dead Peer Detection (RFC 3706): enabled
<IPSEC>   Jul  1 20:43:46  ASA  #1: STATE_MAIN_I4: ISAKMP SA established
{auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp768}
<IPSEC>   Jul  1 20:43:46  ASA  #1: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
<IPSEC>   Jul  1 20:43:46  ASA  #1: Main mode peer ID is ID_IPV4_ADDR:  24.23.99.62
<IPSEC>   Jul  1 20:43:46 | protocol/port in Phase 1 ID Payload is 17/0. accepted with port_floating
NAT-T
<IPSEC>   Jul  1 20:43:46  ASA  #1: received Vendor ID payload [Dead Peer Detection]
<IPSEC>   Jul  1 20:43:46  ASA  #1: STATE_MAIN_I3: sent MI3  expecting MR3
<IPSEC>   Jul  1 20:43:46  ASA  #1: transition from state STATE_MAIN_I2 to state STATE_MAIN_I3
<IPSEC>   Jul  1 20:43:46  ASA  #1: NAT-Traversal: Result using RFC 3947 (NAT-Traversal): no NAT
detected
<IPSEC>   Jul  1 20:43:46  ASA  #1: ignoring Vendor ID payload [Cisco VPN 3000 Series]
<IPSEC>   Jul  1 20:43:46  ASA  #1: ignoring unknown Vendor ID payload
[115a700a30da1b31d7770767536d8e29]
<IPSEC>   Jul  1 20:43:46  ASA  #1: received Vendor ID payload [XAUTH]
<IPSEC>   Jul  1 20:43:46  ASA  #1: received Vendor ID payload [Cisco-Unity]
<IPSEC>   Jul  1 20:43:46  ASA  #1: STATE_MAIN_I2: sent MI2  expecting MR2
<IPSEC>   Jul  1 20:43:46  ASA  #1: transition from state STATE_MAIN_I1 to state STATE_MAIN_I2
<IPSEC>   Jul  1 20:43:46  ASA  #1: enabling possible NAT-traversal with method 4
<IPSEC>   Jul  1 20:43:46  ASA  #1: ignoring Vendor ID payload [FRAGMENTATION c0000000]
<IPSEC>   Jul  1 20:43:46  ASA  #1: received Vendor ID payload [RFC 3947] method set to=109
<IPSEC>   Jul  1 20:43:42 104  ASA  #1: STATE_MAIN_I1: initiate
<IPSEC>   Jul  1 20:43:42 104  ASA  #1: STATE_MAIN_I1: initiate
<IPSEC>   Jul  1 20:43:42  ASA  #1: initiating Main Mode
<IPSEC>   Jul  1 20:43:41 003 NAT-Traversal: Trying new style NAT-T
<IPSEC>   Jul  1 20:43:41 003 NAT-Traversal: Trying new style NAT-T
```

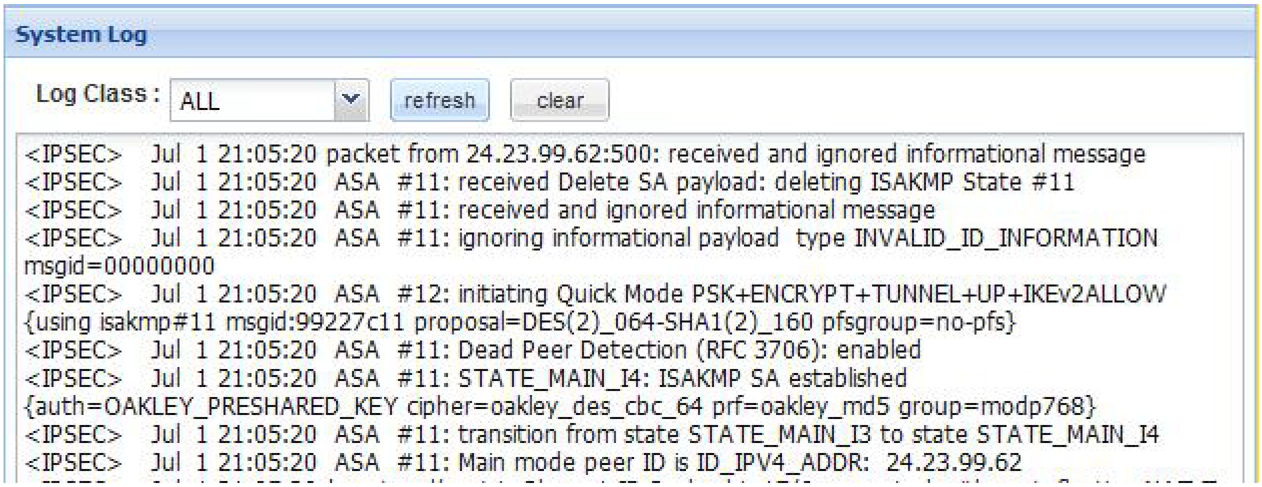
Phase 1 Parameter Mismatch (NO_PROP_CHOSEN):



```
<IPSEC>   Jul  1 20:53:52  ASA  #1: received and ignored informational message
<IPSEC>   Jul  1 20:53:52  ASA  #1: ignoring informational payload  type NO_PROPOSAL_CHOSEN
msgid=00000000
<IPSEC>   Jul  1 20:53:32  ASA  #1: received and ignored informational message
<IPSEC>   Jul  1 20:53:32  ASA  #1: ignoring informational payload  type NO_PROPOSAL_CHOSEN
msgid=00000000
<IPSEC>   Jul  1 20:53:22  ASA  #1: received and ignored informational message
<IPSEC>   Jul  1 20:53:22  ASA  #1: ignoring informational payload  type NO_PROPOSAL_CHOSEN
msgid=00000000
<IPSEC>   Jul  1 20:53:21 104  ASA  #1: STATE_MAIN_I1: initiate
<IPSEC>   Jul  1 20:53:21 104  ASA  #1: STATE_MAIN_I1: initiate
<IPSEC>   Jul  1 20:53:21  ASA  #1: initiating Main Mode
```

Compare the Phase 1 parameters on the LAN-Cell 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, DH5 = DH1536.

Phase 1 ID Type Mismatch:



```
<IPSEC>   Jul  1 21:05:20 packet from 24.23.99.62:500: received and ignored informational message
<IPSEC>   Jul  1 21:05:20  ASA  #11: received Delete SA payload: deleting ISAKMP State #11
<IPSEC>   Jul  1 21:05:20  ASA  #11: received and ignored informational message
<IPSEC>   Jul  1 21:05:20  ASA  #11: ignoring informational payload  type INVALID_ID_INFORMATION
msgid=00000000
<IPSEC>   Jul  1 21:05:20  ASA  #12: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+IKEv2ALLOW
{using isakmp#11 msgid:99227c11 proposal=DES(2)_064-SHA1(2)_160 pfsgroup=no-pfs}
<IPSEC>   Jul  1 21:05:20  ASA  #11: Dead Peer Detection (RFC 3706): enabled
<IPSEC>   Jul  1 21:05:20  ASA  #11: STATE_MAIN_I4: ISAKMP SA established
{auth=OAKLEY_PRESHARED_KEY cipher=oakley_des_cbc_64 prf=oakley_md5 group=modp768}
<IPSEC>   Jul  1 21:05:20  ASA  #11: transition from state STATE_MAIN_I3 to state STATE_MAIN_I4
<IPSEC>   Jul  1 21:05:20  ASA  #11: Main mode peer ID is ID_IPV4_ADDR:  24.23.99.62
```

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.

Frequently Asked Questions

Q: Can I have more than 1 VPN connection from the Remote LAN-Cell 3 at the same time?

A: Yes. The LAN-Cell 3 supports 25 simultaneous non-overlapping VPN tunnels. Simply define the VPN Rules that you need for each tunnel.

Q: Does this configuration work for other ASA firmware versions?

A: Prior to ASA firmware 8.2, Cisco used a different syntax for defining VPN tunnels and NAT rules. The concepts are the same, but the ASDM steps and CLI syntax is slightly different. Refer to the LAN-Cell 2 version of this TechNote for an example using ASA firmware 7.x.

Q: Do I need any special services from my ISP?

A: Some ISPs offer both restricted and unrestricted Internet service. Many cellular operators configure modems so that they cannot accept inbound connections by default or have certain ports blocked. This may interfere with establishing a VPN. Request that your ISP provide you with VPN-compatible service. In particular, your ISP must permit IKE traffic on UDP port 500 and NAT-T traffic on UDP port 4500 and permit ESP traffic to flow in both directions. Requesting a static public IP address will make it easier to configure the VPN settings on both routers.

Q: Does the LAN-Cell 3 support Mode-Config?

A: No. You must enter the necessary VPN tunnel parameters.

Q: Does the LAN-Cell 3 support XAUTH?

A: No.

Q: Does the LAN-Cell 3 support X.509 PKI Certificates?

A: Not at this time.

Q: Does the LAN-Cell 3 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.

Appendix A: Cisco ASA 5505 Configuration – Static Tunnel

```
ASA Version 8.4(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
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
!
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
!
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network LAN-Cell-3-subnet
 subnet 10.1.1.0 255.255.255.0
 description Inside subnet of LAN-Cell 3
access-list outside_cryptomap 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
no asdm history enable
arp timeout 14400
nat (any,any) source static any any destination static LAN-Cell-3-subnet LAN-Cell-3-subnet
!
object network obj_any
 nat (inside,outside) dynamic interface
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
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 warmstart
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set peer 155.163.74.215
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-
AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
```

```
crypto map outside_map interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy GroupPolicy_155.163.74.215 internal
group-policy GroupPolicy_155.163.74.215 attributes
 vpn-tunnel-protocol ikev1
tunnel-group 155.163.74.215 type ipsec-l2l
tunnel-group 155.163.74.215 general-attributes
 default-group-policy GroupPolicy_155.163.74.215
tunnel-group 155.163.74.215 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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:9cc5692f0f15a3872846b723c5248303
: end
```

Appendix B: Cisco ASA 5505 Configuration – Dynamic Tunnel

```
ASA Version 8.4(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
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
!
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
!
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network 10.1.1.0
 subnet 10.1.1.0 255.255.255.0
 description LC3 inside subnet
access-list outside_cryptomap extended permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (any,any) source static any any destination static 10.1.1.0 10.1.1.0
!
object network obj_any
 nat (inside,outside) dynamic interface
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
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 warmstart
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map LC3-Dynamic-IP 1 match address outside_cryptomap
crypto dynamic-map LC3-Dynamic-IP 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-
SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map1 1 ipsec-isakmp dynamic LC3-Dynamic-IP
crypto map outside_map1 interface outside
crypto ikev1 enable outside
crypto ikev1 enable inside
crypto ikev1 policy 1
 authentication pre-share
 encryption des
 hash md5
 group 1
 lifetime 28800
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

```
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-clientless
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key *****
 peer-id-validate nocheck
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:c4af71926608ed5e9d8cd0d11b08e948
: end
```

# # #