

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: <u>support@proxicast.com</u>

Internet: <u>www.proxicast.com</u> © Copyright 2005-2012, Proxicast LLC. All rights reserved.

Proxicast is a registered trademark and LAN-Cell, and LAN-Cell Mobile Gateway are trademarks of Proxicast LLC. All other trademarks mentioned herein are the property of their respective owners.

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 <u>LCTN0014: LAN-Cell 2 to Cisco ASA 5500 VPN Example</u>

Document Revision History:

Date	Comments
July 2, 2012	First release



Introduction

The LAN-Cell can establish "<u>site-to-site</u>" 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 <u>EXACTLY</u> between the 2 devices.
- It is helpful to have simultaneous access to the to parameter and log screens of both devices during setup 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 <u>LAN-Cell 3 Users Guide</u> for more detailed information on VPN parameters and configuration. We also recommend the <u>LAN-Cell VPN Planner TechNote</u> for gathering the necessary VPN parameters and planning your network topology.

Also see the Proxicast Support website (<u>http://www.proxicast.com/support</u>) 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 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.



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.

Aeps .	Peer Device Identificat	on	
I. Introduction	This step lets you iden	tfy the peer VPN device by its IP address and the interface used t	to access the peer.
2. Peer Device Identification	Peer IP Address:	155.163.74.215	-
. KE Version		l	
. Traffic to protect	VPN Access Interface:	outside ·	
 Authentication Methods 			
Encryption Algorithms			
Miscellaneous			
. Summery			

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).

1. Introduction 2. Peer Device InterfaceSon 3. SQL Version 4. Constraints 4. 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. 3. SQL Version 4. Traffic to protect 5. Authentication Methods 6. Encryption Algorithms 7. Miscellaneous 8. Summery	Steps	IBE Version
	Introduction I	ASA supports both version 1 and version 2 of the INE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.

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.

Steps	Traffic to protect
I. Introduction 2. Peer Device Identification 3. IXE Version 4. Traffic to protect	This step lets you identify the local network and remote network between which the traffic is to be protected using encryption. IP Address Type: IPV4 IPV6 Local Network: 192.168.1.0/24
 Authentication Methods Encryption Algorithms Miscellaneous Summary 	Remote Network: 10.1.1.0/24
	< Back Next > Cancel H

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.

Steps	Authentication Met	hods				
I. Introduction 2. Peer Device Identification	This step lets you DE version 1	configure the method	s to authenticate with t	he peer device.		
 IXE Version 	Pre-shared Key:	******				
. Traffic to protect	Device Certificate:	None			Manage	
Autoenocation Methods Encryption Algorithms Miscellaneous Summary						

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).

	It broduction This step left you select the types of encrypton algorithms used to protect the dots. Feer Device about the select of encrypton algorithms used to protect the dots. KE version XE Pelice: used assiste, rais big are sha, pre chore are sha, crack are 100 cha, via spice 131 XE Pelice: used assiste, rais big are sha, pre chore are sha, crack are 100 cha, via spice 131 XE Pelice: used assiste, rais big are sha, pre chore are sha, crack are 100 cha, via spice 131 XE Pelice: used assiste, rais big are sha, pre chore are sha, crack are 100 cha, via spice 131 Xenerophice Applitume Kewnen K	(api	Encryption Algorithms		
2. For Foreion 3. E virtuen 3. Ford frie protect 4. Ford frie protect 5. Addestatue 5. Solen 5. Managetee 5.	2. For Foreice 3. For version 3. Everywain 3. Everywain 3. Everywain 3. Everywain 3. Everywain 3. Foreice 3.	1. Introduction	This step lets you select the types of encryption	on algorithms used to protect the data.	
J. Dia Version 3E Fellor: create and sign of the sign and sign	D. Do Version 32 Fellor: track assists rais og assists, per star, per star, ess 105 da, rais og assists N. Traffic to protect Frec Proposit ESP AES 120 SHA, ESP AES 120 MDS, ESP AES	2. Feer Device Uportification	XE version 1		
Tuelfr is protect Tuelfr is	A Traffe to prefect A Traffe to prefect Added A Traffe to prefect Added	2. Dis version	3E Policy: Unock acc shis, ros oig aco s	sha, pre share aas sha, crack aco 152 sha, roa sig aas 25	Managa
5. Adhenscher Nachols Agwithen 2. Moolessam 5. Semmory	5. Addressater Nachos Algolithem R. Mordinasza B. Sammery	4. Traffic to protect	The Proposal: ESP AES 120 SHA ESP AES	128 MDS, ESP ACS 192 SHA, ESP ACS 192 MDS, ESP AE	Select.
6. Iacryptica Alguritan 7. Moclanage 8. Samery 8. Samery 9. Catol Net X	6. Bacypicke Algorithms 7. Moodiseaam 5. Sweeniny 6. Sect. Not 5. Casol intr	5. Authentication Mathods			
2. Micolaneau E. Summary	2. Novelaneau 5. Summary Canol Not >	6. Encryption Algorithms			
I. Summery	Second Letter	7. Mocelaneam			
(sect. Not >	Catool Heb	5. Saturay			
Report of the second seco					
				Canol	- Helt
				. canol	(Held
Tig Configure 107 v1 Poincies	Ta Configue 107 v1 Poixies	a	enfgue ICI vi Pokies		145
Configure 107 v1 Proticies	Configure 162 v1 Prolicies Configure apeologic Internet New Cosharge (182) elgentifies and parameters, within the Their, Internet Security Association Kay Masagamant Protocol (SEACMP) framework, for the Ark and ISP Press protocols.	12	Configure 107 v1 Policies Configure 107 v1 Policies Configure 107 v1 Policies	Cancel Cancel Control of Social Control of Social Control of Social Control of Social Control (Social P) Francework, for the Avi and ESP	140
Configure 107 v1 Proteines Configure 207 v1 Proteines Configure apendic teternet Key Coulonge (302) elgorithms and parameters, within the 31-set Prese outwards. Autority Aut	Configure 100 v1 Prolicies Configure secolic Internet Key Exchange (XE) objections and parameters, while the Their, Internet Secontry Association Key Weegement Protocol (SACMP) Internet, for the Ari and USP Protocolicitation Add (2) Fold (2) Device Prod	3	 ← Back Net > Configure 107 V1 Proisies Configure 2007 (2017) edge Configure 3000 (2017) edge Configure 3000 (2017) edge Configure 3000 (2017) edge 	Cancel or Bins and parameters, within the Then cool (S.KXIP) frameword, for the AH and ESP	IND

79 H (-128	140	1.00	, crain	95-190	ł
\$9 acc-120	ma		2 ma-pg	06404	R
90 aes 120	916		2 pre-share	06404	P
40 aes 192	976		2 crack	36494	
50 eet-192	sist		2 menuio	55404	
63 sep-192	516		2 pre-share	00488	١.,

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.

Steps	Miscellaneous
Introduction Peer Device Identification INE Version A. Traffic to protect Authentication Methods Encryption Algorithmis Miscellaneous Summary	This step lets you configure some other important parameters.
	Constant I marked a state

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.

	Summary	
17	Here is the summary of the configuration.	
2210	Isame	Value
and a state	Sommary	
	Peer Device IP Address	155.163.74.215
the second se	VPN Access Interface	outside
Carrier I	Protected Traffic	Local Network: 192.168.1.0/24 Remote Network: 10.1.1.0/24
and the second	IKE Version Allowed	IKE version 1 only
dia	Authentication Method	
	IKE v1	Use pre-shared key
	Encryption Policy	
	Perfect Forward Secrecy (PFS)	Disabled
	E NEV1	
A-	IXE Policy	crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-shere-aes-192-sha, crack-aes-256-sha, rsa-sig-36es-sha, pre-share-aes-256-sha, crack-36es-sha, rsa-sig-36es-sha, pre-share-des-sha, crack-des-sha, rsa-sig-36es-sha, pre-share-des-sha, pre-share-des-md5
N Wizard	Piec 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-JDES-SHA, ESP-JDES-MD5, ESP-DES-SHA, ESP-DES-MD5
- I	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)

The off	t View Tools Wizards Wi	ndow Help storing 🗔 Save (🔁 Refresh	O lisck ()	Lool	k For:	1	cisco
	Frewal d P	Configuration >	Frewall >	T + J = II	- Q. Find 🖽 Despren	n 🐙 Paciat Trace.	/ Addresses [Services]	<i>d</i> 1
• [Dev	C. Service Policy Pulses AvA Roles Public Servers VRL Piber Roles VRL Pibers Servers S	Match Crit Source Inff 1 mode	eria: Origi Dest Inf Set of C Subade	nal Packet Source (*1) gif otj_any	Destination	Service	Add - Elott ■ Dearlie Reat Fibati In arce 1 Bryet Network Objects windse-network/24 通 In Side-network/24 通 In Side-network/24 通 In Side-network/24 通 In Side-network/24 windse-network/24 winds	R, Where O
•	Device Setup Proved Proved Bernate Access VPA Sec-to-site VPA	lingt						
	Device Monagement		1	ADDY	Rest			

Figure 11: ASA Adding a NAT Rule



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

	i allo			ni an	-
source interface:	- Any		Destination interface:	Any	
Source Address:	any	10	Destination Address:	any	B
			Service:	any	12
Action: Translated Packet					
Source NAT Type:	Static	•			
Source Address:	Original	E	Destination Address:	- Original	8
PAT Pool Translated Address:		10	Service:	- Original	6
Round Robin					
Round Robin	er destination instead	of per loterf	808		
Round Robin Bidend PAT unqueneos to p Tramslate TOP and UDP port	er destination instead a min flat renge 1034-	of per loterf 63535	sca Include range 1-1023		
Round Robin Extend PAT unquerieds to p Translate TCP and UDP port Teal through to interface PAT	er destination instead a wito flat range 1034	of per interf 43535	ooa Include range 1-1023		
Round Robin Detend PAT unspanneess to p Translate TCP and UDP port Fall through to interface PAT Options	er destination instead a into flat renge 1034	of per lotert 43535 [^[]]	sce Include range 1-1023		
Round Robin Detend PAT unspanneess to p Translate TCP and UDP port Fall through to interface PAT Options Detender rule	er destination instand i into flat range 1024	of per loterf 63535	sce Include range 1-1023		
Round Robin Eddend PAT unsqueeten to p Translate TCP and UOP port Fall through to interface PAT Options Enable rule Translate DNS replies that mot	er destination instead a into flat range 1034 ch this rule	of per interf	558 Jachide range 1-1023		
Round Robin Eddend PAT unsquentells to p Translate TCP and UOP port Fall through to interface PAT Options Enable rule Translate DNS replies that mot Disable Proxy ARP on ogress to	er destination instead a into flat renge 1034 th this rule terface	of per loterf 63333	BCB Include range 1-1023		
Round Robin Eddend PAT unsquentells to p Translate TCP and UOP port Fall through to interface PAT Options Translate INIS replies that mot Disable Proxy ARP on ogress to Lookup route table to locate eg	er destination instead a into flat renge 1034 th this rule terface press interface	of per interf	808 Include range 1-1023		
Round Robin Eddend PAT unsquentells to p Translate TCP and UOP port Fall through to interface PAT Dotions Translate INIS replies that mot Disable Proxy ARP on ogness at Lookup route table to locate eg prection: Both	er destination insteed a into flat renge 1034 th this rule terface press interface	of per interf	808 Include range 1-1023		

Figure 12: Add NAT Rule Screen

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

				Filter Ch
Name *1	IP Address	Netmask	Description	Object NAT Addr
DV4 Networ	k Objects			
bob_a	ny 0.0.0.0	0.0.0.0		any (P), outside
🌩 aliy		1		
🖹 Interfaces				
inside				
COCHE				
Selected Origin	al Destination Add	1458		

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	
Гуре;	Network	•
IP Address:	10.1.1.0	
Netmask:	255.255.255.0	•
Description:	Inside subnet of LAN-Cell 3	
		(8)
1225		1/2

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	ID Addresse			
	a viceress	Netmask	Description	Object NAT Addr.
IPv4 Network Of	bjects			
any obj_any or any	0.0.0.0	0.0.0.0		any (P), outside
CALCUL	10.1.1.0	255,255,255	a biside subnet of CAN-Cell 3	
Interfaces				
- El inside				

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-12l 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).

Psec			Erable	e 🧧 Estable	
User Rules					
Connection Name	Puls Encoled	Econal Interfece	Remote Deterring	Plainora Subnat IP / Subnat Mear	
Add Denis	Minkly	Mone Up 1	Three Down		

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.

Remote Su Remote Su Netmask Connection IKE Key Mo	bnet IP 19 bhet 26 h Initiation 27 ode P	5 256 256.0	Phase 1 Local ID Phase 1 Remote ID Phase 1 Lifetime Phase 21 idefime	29800	Seconds (3600 ~ 28800
Remote Su Netmask Connection IKE Key Mo	bnet 26 h Initiation V ode P	5 255 255 0	Phase 1 Remote ID Phase 1 Lifetime Phase 21 ifetime	29800	Seconds (3600 ~ 28800
Net Connection IKE Key Mo SB Modem	n Initiation 📝 ode P	255,255,0	Phase 1 Lifetime	29800	Seconds (3600 ~ 28800
Connection IKE Key Mo	nitiation 🦉 ode P		Phase 21 itelima		
Cel Moderni •		STREET.	FILSTE & CARGANIA	29800	Seconds (3600 ~ 28800
Preshared	Key 12	345679	Phase 1 Authentication	MD5 💌	
DPD Enable			Phase 1 Encryption	DES 💌	1
DPD Interva	al 10	Seconds (10 ~ 1200)	Phase 1 Group Key Management	DH1	
DPD Timeo	ut 60	Seconds (30 ~ 3600)	Phase 2 Authentication	SHA1	
			Phase 2 Encryption	DES 💌	1
			Phase 2 Group Key	-	
	255.0 DPD Interv DPD Times	255.0 DPD Interval 10 DPD Timeout 60	255.0 DPD Interval 10 Seconds (10 ~ 1200 DPD Timeout 60 Seconds (30 ~ 3600	2550 DPD Interval 10 Seconds (10 - 1200) DPD Timeout 60 Seconds (30 - 3600) Phase 2 Authentication Phase 2 Encryption Phase 2 Group Key Management (PFS)	2550 DPD Interval 10 Seconds (10 - 1200) DPD Timeout 60 Seconds (30 - 3600) Phase 1 Group Key Phase 2 Authentication Phase 2 Encryption Phase 2 Group Key Management (PFS) Phase 2 Group Key Management (PFS)

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

<u>Always On</u>

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).

	iser Rules	Rule Enabled	Esternal rderfisce VAN (USB	e Enable Remote Cadeway	Remote Subnet iP	/ Phase Pru 1 2	850
2	iser Rules Intestion Inte	Rule Enabled	Edomal Methode VAN (USB	Remole Gateway	Remote Subnet P Subnet Mask	/ Phuse Phu 1 2	10 C
651 AS	Aneston	Rule Enabled	VAN (USB	Remote Gateway	Remote Subnet IP Subnet Masia	/ Phase Plu 1 2	850
AS	A	× 1	NAN (USB				
100	and a second second		in the second se	24.23.99.02	192.168.1.0/255.2	55.255.09	
	Delet	Modify	Move Lip	Move Down			
to ASDM 6.4 for A	SA - 192 168 1	1			11000		
view Tools Wa	tants Windo	w Help			Look Far:		ahah
us 20 cadenas	and J. Manatary	and some C	Raforen O	Back of Strength and	(reb)		cisco
Vita Garates		celturing > Viti	IN VIELENCES	tics > Session			
		The second	1000	0.000			And a second
Crypto Statistic Compression 57	antitica	Type Secto-Sec VPN	Adive	Canvietov	Feat C 85	HOUTHRE I	hadve
Cobs MI/Pre	stes : Statistics	305vt Free		î	15	i.	
RAC Sector St	mminy D						
VLNI Mapping 1 Classifiers SSL VPH	Seccione						
Easy VPN Client VPN Connection Cr.	-			all an annual		il mark	
WSX Savalarsi		HOW NY I PARKS	are to see	T. I. Al Seven		- TRAC	NY.
		P Address	 Protocal Encryption 	e Durster	5	Byten Rx	- Detars
	11	CONTRACTOR OF THE	Birst and	a an 10.14	VTC-Gen Ref 3 2613	122	Logent
		10111/4/20	Constraint.	- Handaria	24	1149	.Pire

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.

Stelu-Steven d. C	forign after a She he Sile V	01.2. Onection Publics			
Group Polices	Access Interfaces Enable interfaces for Plast acc	-			
Advented Tunnel Graps Grypts Mape SE Policies SE Poli	Interface Allow BE v1 A Invitable (2) Inside (2)	Aber IXI vi Acara			
Prec Prefragmentation Pol Gardinate to Consider IV System Option ACL Manager	R institution of the second with second with second	ns to bypase interface access juns. Gra	p policy and per-user e-	chorcustion access faits	i still apply 5
	Connection Profiles				
	Connection profile identifies the to be encounted, and other part	a peer of a site-to-site connection. It is president. You can continue the mount	ectles what data traffic	is to be encrypted, have	e the details
	◆ Add III Gette III Deleta		10160101000000	1111-122072215	
	Name Interface	Local liebaurk Remote Network	SOVE Fuebled	MPv2 Frashed	Group Pa
4					
A growth Samp					
1 Binnes 1					
e et e S forier temp E transit S formere access VIII					
4 10 10 10 10 10 10 10 10 10 10 10 10 10	Finds	O OF Match Care			

Figure 21: Connection Profile Settings

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

Name:	Default1210	roup			-	
sec Enabling						
Group Policy Name:	DfttGrpPolicy					
	(Following t	wo field KE vt	s are attribute	s of the group v2	polic	y selected abov
sec Settings						
BE vt Settings						
Authentication					-	
Pre-shared Key:					•	
Device Certificate:	None				26	Manage
IKE Peer ID Validation	Do not che	dk.			•	
E Keepalive						
Disable keepalives	É.					
Monitor keepalive	ē					
Confidence Interv	al: 10		seconda			
Rebry Interval:	2		seconds			
	of the second	-	10.000			

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	n Sets)		
IKE v1 IPsec Proposal: ESI	NAES-128-SHA, ESP-AES-128-MD5, ESP-A	ES-192-S> Select	
IKE v2 IPsec Proposal:		Select	
Peer Settings - Optional S	Ine Promannie County Man Enterine		
The Connection Type is a type policies are used for connection type may speci	of opinienic organised policies only. Uni-d plicable to static tunnel policies only. Uni-d Al-to-LAN redundancy. Tunnel policies of I fy up to 10 redundant peers.	rectional connection the 'Driginate Only'	
The Connection Type is a type policies are used for connection type may spect	ded:	rectional connection the 'Originate Only'	
The Connection Type is a type policies are used for connection type may spect P Address of Peer to Be A	ded:	rectional connection the 'Originate Only'	
The Connection Type is a type policies are used for connection type may spect IP Address of Peer to Be A	dded: Add >> Remove	rectional connection the 'Driginate Only'	
The Connection Type is a type policies are used for connection type may spect IP Address of Peer to Be A	ded: Add >>> Remove	Move Up	

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		-	-	-	-	Concession in the local distance of the loca	 X
Tunnel Policy (Cryp	to Map)	- Basic Tu	innel Policy (Cr	ypto Map) - Adva	nced Traffic S	Selection	
Enable NAT-T	•	_					
Enable Revent	e Route	Injection					
Security Association	Lifetime	Settings					
Time:	8 :	0:0	hh:mm:sa	←			
Traffic Volume:		4608000	K Bytes				
	_						
			OK	Cance		Help	
			- un			1	

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 R	ule		 X
Tunnel Policy	(Crypto Map) - Basic Tunnel Policy (Cryp	to Map) - Advanced Traffic Selection	
Action: 🔍 I	Protect 🕐 Do not Protect		
Source:	192.168.1.0/24	6	
Destination	10.1.1.0/24		
Service:	¢		-
Description:			
More Opti	ons		۲
(2) Enable	Rule	and the second second	
Source Ser	nice:	(TCP or UDP service only)	
Time Rang	e:		
	15	an 17 - 1	
	OK	Cancel Help	

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.

A man P containing	window Help	Aug Ores	1.000	Part)	195.	dia.
Ste-to-Ska VPR /T 8	Configuration > Site to -Site VI	a housed a	NLP-Alls			
Connaction Healted Croug Prices Croug Price Read Analysis Croug Price Price Messagement Price Prices Price	Cardigure specific bitemet Key E Profecol (SJAMP) framowark, fo RGA Poloies Add GF fail () Deles	schange (XE) olgori ir the AH and ESP IP Red:	tena ani pororretora no pretocela.	within the Poec Internet	Security Association Kay Man	agerne
	Prenty # Exception 132 X044 120 X045 120 X045 120 X045 120 X045 120 X045	n Hash Fra Fra Fra Fra Fra Fra	D-H Grava	Auffrentission 3 res-og 2 pro-share 2 res-share 2 res-share 2 res-share	Lifetime (seconds)	KC0 *
	3052 Policies ♦ Act # 10 8 Dolwy / Priority # Encryption	Priority: Authenticyton Encrypton: D-H Group: Hash: Edistance OK	1 produce des 1 noti Unitented 21 Cancel	nce jarcods *	(Jetare (seconda)	
Berne Barepenet			- and -	Tool	,	

Figure 26: New IKE Policy



File View Tools Witanh	Window Help		Look Far:		91.	diat
S Hone & Configuration	Ventrag an Gradien (Back O Tornant	reb			cisc
Ste-to-Size VPN of 8	Configuration > Site to Site VPS	> Advanted > All Ma	MORT.		-	
Cennection Profiles	🗣 Acc = 🕼 Edt 🏦 Dates 🛨 - 4	L B B . Q Fre				
Certificate Management	# Brabled Source	Ubbr	Oedtwahon	Service	Action	Lágpin
Turnel Groups	 cvtiale_oryptamap 			1.000	2422.00	S. A.C.
Diz Połcies	2 S	militer in the second s	Se lanta		Per Perme	
DE Parenteria Desc Proceeds (Transform)	CO FRIACE					
Post Prohagmentation Pole					-	
Paker	Adlor: @ Estint @ Dary					
System Options	Source: 192.268.1.6/24					
CANADA CA	liter:		-			
	Overlaution 10.1.1.0					
	Service: 0					
	Description					
	Constraint -					- 1
	2 Enable Logging					
	Logang Level: Default *					
 Constitution of the 	More Opticas					
3, pecca setup		parties and states	10 10 COM -			
Frankl			rcal Help			
General Access Vits	1			_	_	_
CH Star to Star VIII	A Manual and a second second	(16)		and a local data		
T Dente Management	Colleges A2 Expend AL	Piter 🖬 B	ED OPHING OPHI	-		
S. Series Berdinse		(AN	Near			
1	ā	1 200				

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

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.

March Otheries: Original Packet					
Source Demlece:	- ANY++		Bestretos biteface:	- 44	•2
Source Address:	313		Destrebes Address:	10.3.3.9	G
			Server	ang	
Actan: Transitied Pecket					
Searce BAT Type:	Static.				
Source Address:	- Original -		Destination Address:	- Original	6
PAT Hal Translated Address:		13	1000	- received	1.1
	-		Service:	- Crighter	
Tread Rates		2 3		Colored a	
Frank Hotes	or Beenveton evenue n emo Part cango 1004	af per smirts 455.05	na hrlas nege i-1823		
interest Patters	er Bernartos esenar a una fait serge 1524	af per smith 65535	na na hitoir nige 1-1833		
Frankf Holes Science PHT Lenguesess III (P Translane TTP and LEP (PHT The Science PHT Options IP Lookle role	er Bestratton evenan n smi fad Længe 1334	af per much 455.05	na nikon ninge 1-1823		
Insured Patters Section 21107 assessments to p Transition 7127 and GDP parts Transition 7127 and GDP parts Transition 21107 assessments Transition 20107 registers	er Skonnanton evenam nami Parl Lange 1524 och thorealte	af par smet 65535	ne nege i 1833		
Insure Fielders Indured Field Languages of the general sector of the general se	er Resmanne versam nam Pat Lange 1324 tah tha role derface	af per med 623.03	na hitois ninga i-1823		
Insure Fielder Insure Fielder Insure Field Stategueneum m.p. Transition 7129 and State park Field Strength In Interface PAY Genome Deable rule Transition DNI registers that more Deable Pressy APP on expecta in Learning much table in Income m.	er Sammatton Patham n ann Pat Lange 1004 toh thornais tertison areas stattbor	af par smet essan	ne ne hilde nege i-1023		
Insure Finders Insure Finders Insure First Annual An	er Bestmatten vorsam n mit Parl Lange 1254 teh Herrola teh Herrola	af per smith 62533	na hallor inge 1-1023		

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:

System Log)					
Log Class	a: ALL	~	refresh	clear		
<ipsec></ipsec>	Jul 1 20:43:43	ASA	#2: STAT	E_QUIC	I2: sent QI2 IPsec SA established tunnel mode	*
{ESP=>0x	7e218a4d <0x0	ibb6a5	43 xfrm=D	ES_0-HM	AC_SHA1 NATOA=none NATD=none DPD=enabled}	1
<ipsec></ipsec>	Jul 1 20:43:43	7 ASA	#2: trans	tion from	state STATE_QUICK_I1 to state STATE_QUICK_I2	
<ipsec></ipsec>	Jul 1 20:43:43	7 ASA	#2: Dead	Peer De	tection (RFC 3706): enabled	
<ipsec></ipsec>	Jul 1 20:43:40	ASA	#2: initiat	ing Quick	Mode PSK+ENCRYPT+TUNNEL+UP+IKEv2ALLOW	
{using isak	mp#1 msgid:c1	d3ed13	proposal=	DES(2)_	064-SHA1(2)_160 ptsgroup=no-pts}	
<ipsec></ipsec>	Jul 1 20:43:40	ASA	#1: Dead	Peer De	tection (RFC 3706): enabled	
<ipsec></ipsec>	JUI 1 20:43:40	D ASA	#1: STAT	E_MAIN_	14: ISAKMP SA established	Ξ
{auti=OA	Jul 1 20.42.4	ED_NE	#1. transi	tion from	s_cbc_o4 pri=oakley_mus group=moup/o8}	
<ipsec></ipsec>	Jul 1 20.43.4	5 ASA	#1. Uditsi #1. Main	mode pe	ar ID is ID ID/4 ADDR: 24 23 00 62	
<ipsec></ipsec>	Jul 1 20:43:4	5 I nrot	tocol/port i	n Dhace	I ID Davload is 17/0 accented with port floating	
NAT-T	Jul 1 20.43.4	1 piot		II FIId3C	ID Payload is 1770. accepted with port_libating	
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: receiv	ved Vend	or ID navload [Dead Peer Detection]	
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: STAT	E MAIN	I3: sent MI3 expecting MR3	-
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: transi	tion from	state STATE MAIN 12 to state STATE MAIN 13	
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: NAT-	Traversal	Result using RFC 3947 (NAT-Traversal): no NAT	
detected					CITIE SALLES AND ALL ALL ALL ALL	
<ipsec></ipsec>	Jul 1 20:43:44	5 ASA	#1: ignori	ng Vend	or ID payload [Cisco VPN 3000 Series]	
<ipsec></ipsec>	Jul 1 20:43:44	5 ASA	#1: ignori	ng unkno	own Vendor ID payload	
[115a700a	30da1b31d777	076753	36d8e29]			
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: receiv	ved Vend	or ID payload [XAUTH]	
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: receiv	ved Vend	or ID payload [Cisco-Unity]	
<ipsec></ipsec>	Jul 1 20:43:40	5 ASA	#1: STAT	E_MAIN_	I2: sent MI2 expecting MR2	
<ipsec></ipsec>	Jul 1 20:43:44	ASA	#1: trans	tion from	state STATE_MAIN_I1 to state STATE_MAIN_I2	
<ipsec></ipsec>	Jul 1 20:43:40	ASA	#1: enabl	ing possil	ble NAT-traversal with method 4	
<ipsec></ipsec>	Jul 1 20:43:40	ASA	#1: ignor	ng vend	or ID payload [FRAGMENTATION COUDOUUU]	
<ipsec></ipsec>	Jul 1 20:43:40	ASA	#1: recen		ATNU TIL initiate	
<ipsec></ipsec>	Jul 1 20:43:4.	2 104	ACA #1:0	TATE M	AIN_II: Initiate	
<ipsec></ipsec>	Jul 1 20:43:4	0 454	#1: initiat	ing Main	Mode	
<ipsec></ipsec>	Jul 1 20.43.4	003 1	AT-Traver	cal. Tryin	n new style NAT-T	
<ipsec></ipsec>	Jul 1 20:43:4	003 1	AT-Traver	sal. Tryin	n new style NAT-T	-
CIPOLO2	501 1 20.45.4	005	in 1- mayer	Sal Hylli		



Phase 1 Parameter Mismatch (NO_PROP_CHOSEN):

System Log				
Log Class :	ALL	~	refresh clear	
<ipsec> Ju <ipsec> Ju</ipsec></ipsec>	l 1 20:53:52 l 1 20:53:52	ASA a	#1: received and ignored informational message #1: ignoring informational payload type NO_PROPOSAL_CHOSEN	
<ipsec> Ju <ipsec> Ju <ipsec> Ju</ipsec></ipsec></ipsec>	l 1 20:53:32 l 1 20:53:32	ASA a	#1: received and ignored informational message #1: ignoring informational payload type NO_PROPOSAL_CHOSEN	
<pre>msgid=00000 <ipsec> Ju <ipsec> Ju</ipsec></ipsec></pre>	000 1 20:53:22 1 20:53:22	ASA a	#1: received and ignored informational message #1: ignoring informational payload type NO_PROPOSAL_CHOSEN	
msgid=00000 <ipsec> Ju</ipsec>	000 1 20:53:21	104 A	SA #1: STATE_MAIN_I1: initiate	=
<ipsec> Ju <ipsec> Ju</ipsec></ipsec>	l 1 20:53:21 l 1 20:53:21	ASA	SA #1: STATE_MAIN_I1: initiate #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:

System Log						
Log Class	ALL	refre	sh)		
<ipsec> <ipsec> <ipsec> <ipsec> msgid=000</ipsec></ipsec></ipsec></ipsec>	Jul 1 21:05:20 Jul 1 21:05:20 Jul 1 21:05:20 Jul 1 21:05:20 Jul 1 21:05:20	packet from ASA #11: ASA #11: ASA #11:	24.23.99.62 received Dele received and ignoring inform	500: received and te SA payload: d ignored informat mational payload	nd ignored informatio leleting ISAKMP Stati ional message type INVALID_ID_I	nal message e #11 NFORMATION
<ipsec> {using isakn <ipsec> {IPSEC> {auth=OAK <ipsec> <ipsec></ipsec></ipsec></ipsec></ipsec>	Jul 1 21:05:20 np#11 msgid:99 Jul 1 21:05:20 Jul 1 21:05:20 GLEY_PRESHARE Jul 1 21:05:20 Jul 1 21:05:20	ASA #12: 0227c11 pro ASA #11: ASA #11: D_KEY ciph ASA #11: ASA #11:	Initiating Quic posal=DES(2) Dead Peer De STATE_MAIN er=oakley_des transition fror Main mode pe	Mode PSK+EN _064-SHA1(2)_1 _tection (RFC 37 _I4: ISAKMP SA s_cbc_64 prf=oa n state STATE_I eer ID is ID_IPV4	60 pfsgroup=no-pfs] 60 pfsgroup=no-pfs] 06): enabled established kley_md5 group=mo MAIN_I3 to state ST/ _ADDR: 24.23.99.63	dp768} ATE_MAIN_I4

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.2KY0U 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
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 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 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-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-sha-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-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-3des esp-sha-hmac
 no snmp-server contact
 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 peer 155.163.74.215
AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-AES-192-MD5
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 i kev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
  group 2
lifetime 86400
crypto i kev1 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
hash sha
group 2
lifetime 86400
crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
  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 consol e 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 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-121 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 rtsp inspect esmtp inspect sql net inspect ski nny inspect sunrpc inspect sum per 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.2KY0U 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
  securi ty-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 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-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto i psec i kevi transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto i psec i kevi transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto i psec i kevi transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto i psec i kevi 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 i kev1 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 i kev1 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
consol e 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 clic
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 sql net
inspect ski nny
   inspect sunrpc
inspect xdmcp
   inspect sip
inspect netbios
   inspect tftp
inspect ip-options
1
.
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum: c4af71926608ed5e9d8cd0d11b08e948
```

: end

