## How to build LAN to LAN VPN connection between Vigor router and CiscoASA

This application will guide you to build LAN to LAN VPN connection between Vigor router (e.g., Vigor2910) and CiscoASA. Suppose,

- The WAN IP address of CISCO ASA is 203.70.63.90, while LAN IP address is 192.168.1.1/255.255.255.0
- The WAN1 IP address of Vigor2910 is 59.125.9.159; while LAN IP is 192.169.20.1/255.255.255.0
- 1. Choose Wizards>>IPsec VPN Wizard.

<b>1</b>	Cisco ASDM 6.1 for ASA - 192.168.1.1						
File	e <u>V</u> iew <u>T</u> oo <mark>s</mark>	Wizards Wir	ndow <u>H</u> elp	Look For: Go	ahaha		
	Home 🖧 Configur	<u>S</u> tartup W	fizard	orward 🤪 Help	CISCO		
5	Device Setup	IPsec <u>V</u> PN	Wizard	izard.			
tice Li	Startup Wiza	22F ANN A	wizard				
Dev	↓ •••••• Routing	<u>H</u> igh Avai	lability and Scalability Wizard	start the wizard.			
	→ o <sup>o</sup> Device Name → oo System Time	Packet Ca	pture Wizard				
			Startup Wizard				
		**	Adaptive Security Appliance configured ward to create a basic configuration th policies in your network. The Startup Wizard can be run at any th with values from the current running co	l and running. Use this at enforces security			
	🛃 Device Setup						
	🗊 Firewall						
	Remote Access	VPN					
	🔗 Site-to-Site VPN						
	Device <u>M</u> anager	nent					
		*		Launch Startup Wizard			

2. The VPN Wizard will be popped-up as follows. Choose **Site-to-Site** as **VPN Tunnel Type**; **Outside** as **VPN Tunnel Interface**; and click **Next**.



3. Click **Yes** to continue.

🔂 VPN Wizard	
VPN Wizard	VPN Tunnel Type (Step 1 of)
Branch	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
VPIN WIZ	
Corpo	Inbound IPsec sessions will be filtered by interface access lists. Please make sure you have an access list to the ingress interface that permits IPsec packets from all IPsec peers. Do you want to continue?           Yes         No
S.A.	VPN Tunnel Interface: outside Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	<pre></pre>

4. Type the WAN IP address of the peer in the field of **Peer IP Address** for IPsec VPN connection. Then type the Pre-shared key. Next, a profile name will be generated automatically in the field of **Tunnel Group Name**. Click **Next**.

🔂 VPN Wizard	
VPN Wizard	Remote Site Peer (Step 2 of 6)
Brandh Home Corporate Network	Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel. Peer IP Address: 59.125.9.159 Authentication Method Pre-shared key Pre-Shared Key: 12345678 Certificate Certificate Certificate Signing Algorithm: rsa-sig Certificate Name:
	Tunnel Group         For site-to-site connections with pre-shared key authentication, the tunnel group name must be the same as either the peer IP address or the peer hostname, whichever is used as the peer's identity.         Tunnel Group Name:       59.125.9.159
	≤ Back   Next > Emish Cancel Help

5. Keep the default settings of **Encryption** type and **Authentication**, and specify the **DH Group** for your request. Then, click **Next**.

📴 VPN Wizard	
VPN Wizard	IKE Policy (Step 3 of 6)
Branch Branch ISP Home Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.
Network	Encryption:
FILL IN	
	Authentication:
STATINI.	Diffie-Hellman Group
TTT	
	<u>≤ Back</u> <u>Mext</u> > Finish <u>Cancel</u> <u>H</u> elp

6. For the second phase of IKE encryption, keep the default settings and click **Next**.

📴 VPN Wizard	
VPN Wizard	IPsec Rule (Step 4 of 6)
Branch Franch Fisp Homo	Select the encryption and authentication algorithms and configure Perfect Forwarding Secrecy (PFS) for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.
Corporate	Encryption: Authentication:
- Translill	Enable Perfect Forwarding Secrecy (PFS)
TH	Diffie-Hellman Group: 1
	<u>≤ Back</u> <u>Mext</u> > <u></u> Emish <u>Cancel</u> <u>H</u> elp

7. In the following screen, type the local / remote IP address with the subnet mask for local /remote network. Then, click **Next**.

📴 VPN Wizard	×	
VPN Wizard	Hosts and Networks (Step 5 of 6)	
Branch	An IPsec tunnel protects data exchanged by selected hosts and networks at the local and remote sites. Please identify hosts and networks to be used in the IPsec tunnel.	
Home	Action: Do not Protect	
Network	Remote Networks: any	
	Exempt ASA side host/network from address translation:     inside	•
	<u>≤ Back</u> <u>Finish</u> <u>Cancel</u> <u>H</u> elp	]

8. Click Finish.



9. Click the tab of **Configuration**. Choose **Site-to-Site VPN** and click **Connection Profiles**. Now, the relational VPN settings will be displayed on the field of **Connection Profiles**. If required, you can click **Edit** on this field to modify other settings of VPN in details.

<b>1</b>	Cisco ASDM 6.1 for ASA - 192.1	68.1.1					
<u>F</u> il	e View <u>Tools Wizards Wi</u> Hom <mark>@ Configuration</mark> Monito	ndow <u>H</u> elp ring   <mark>    </mark> Save <b>( </b> Refre:	sh 🔇 Back	🕥 Forward 🛛 🦓 Help	Look For:		Go uluulu CISCO
Device List	Site-to-Site VPN T + ×	Configuration > Site-to Access Interfaces Enable interfaces for IP:	D-Site VPN > C	Connection Profiles			
	⊳- <b>I</b> ∰ ∆dvanced	Interface outside inside Connection Profiles Connection profile iden other parameters & Add Z Edit	tifies the peer of Delete	Allow Access	ecifies what data traffic	is to be encrypted, how the d	lata traffic is to be encrypted, and
(	Cevice Setup  Cevice Setup  Cevice Setup  Cevice Setup  Cevice Management  Cevice Manage	Nome 59.125.9.159 or	Interface utside	Local Network inside-network/24 Appl:	Remote Network	Enabled	Groun Policy DfilGryPolicy

 Click Edit to open the following screen. Expand the Advanced folder and choose Crypto Map Entry. Click Disable for Perfect Forward Secrecy, then choose answer-only as Connection Type. Next, click OK.

🔂 Edit IPsec Site-to-Si	te Connection Profile:	59.125.9.159
Basic ▲-Advanced Crypto Map Entry Turnel group	Priority: Perfect Forward Secrecy	1 © Disable © Enable Diffie-Hellman Group:
	NAT-T:	▼ Enable
	Reverse Route Injection:	Enable
	Security Association Lifetim	uē —————
	Time:	8 : 0 : 0 hhmm:ss
	Traffic Volum:	4608000 KBytes
	Static Crypto Map Entry Pa	rameters
1	Connection Type:	answer-only
	Send ID Cert. Chain:	Enable
	IKE Negotiation Mode:	💿 Main 💿 Aggresive
		Diffie-Hellman Group:
Find:		🔘 Next 🔘 Previous
	OK	Cancel Help

11. Click the tab of **Configuration**. Choose **Firewall** and click **Access Rules**.

12. Click Add. The Add Access Rule dialog will pop-up. Choose Inside as the Interface; and choose Permit as the Action. Choose local network as the Source; and remote network as the Destination. Next, click OK.

6	Cisco ASDM 6.1 for ASA - 1	192.168.1.1		
Eib	e <u>View Tools Wiz</u> ards	Window Help Look For:		Go
	Home 🔧 Configuration 🛐 M	Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help		CISCO
5	Firewall 🗗 🖓	× Configuration > Firewall > Access Rules	□ Addres	ses ⊡ ₽ ×
vice Li	Access Rules	💠 Add 🝷 🗹 Edit 💼 Delete 🛧 🗲 🐰 🐚 🆏 - Q. Find 🖼 Diagram 🎧 Export - 🀆 Clea	r Hits 💠 Ad	id - 🗹 Edit 👕 Delete 🔍
Å	🔍 Service Policy Rules	# Enabled Source Destination Service Action	Filter:	Filter Clear
	AAA Rules	Add Access Rule	×	-1 -1
	URL Filtering Servers			:k Objects
	Threat Detection	Interface.		any inside-network/24
	Advanced	Action: O Permit O Deny		vigor/24
		Source: inside-network/24		192.168.53.0/24
		Destination vigor/24		
		Service: ip		
	Device Setup	Description:		
	Firewall	V Enable Logging		
	Remote Access VPN	Logging Level: Default		
	Site-to-Site VPN			
	Device Management	More Options	۲	
	Novice Manuferment	OK Cancel Help		es Services Time Ra

13. Click **Add** to add another access rule. Choose **Outside** as the **Interface**; and choose **Permit** as the **Action**. Choose remote network as the **Source**; and local network as the **Destination**. Next, click **OK**.

🚺 Cisco ASDM 6.1 for ASA - 1	92.168.1.1						
File View Tools Wizards	File View Tools Wizards Window Help Look For:						
Hom Configuration 🛃 M	🚯 Hom 🦓 Configuration 🖉 Monitoring 🔚 Save 🐼 Refresh 🔇 Back 🚫 Forward 🦻 Help						
Firewall 🗗 🖓	× Configuration > Firewall > Access Rules				Addresses	ъъ×	
Access Rules	🗣 Add 🗸 🗹 Edit 📋 Delete 🛧 🗲 🐰	, 🐚 📖 - 🔍 Find 🔛 I	Diagram 🔚 Ex	port 👻 🏠 Clear Hits	💠 Add 👻 📷	Edit 💼 Delete 🔍	
C Service Policy Rules	# Enabled Source	Destination	Service	Action	Filter:	Filter Clear	
Filter Rules	🖆 Add Access Rule					±	
URL Filtering Servers					ark Ot	rjects	
Threat Detection					any A insid	le-network/24	
Advanced	Action: 💿 Permit 🔘 Deny				4 vigo	n/24	
	Source: vigor/24				§ 192	.168.53.0/24	
	Destination inside-network/24						
	Service: ip						
Q Durin Chur	Description:						
Device Setup							
Firewall							
Remote Access VPN	M Enable Logging						
	Logging Level: Default 👻						
Sile-IO-Sile VIN	More Options						
Device <u>M</u> anagement	Prote Opacito	_					
	OK	Cancel	Help	]	ses	Services Time Ra	
		<admin></admin>	15		2010/1	2/7 下午 05:43:13 CST	

14. Access into the WUI of Vigor router (e.g., Vigor2910).

LAN-to-LAN F	Profiles:			Set to Fact	ory Default
Index	Name	Status	Index	Name	Status
<u>1.</u>	2.29	×	<u>17.</u>	???	Х
<u>2.</u>	2.229	×	<u>18.</u>	???	Х
<u>3.</u>	24	×	<u>19.</u>	???	X
<u>4.</u>	25	×	<u>20.</u>	???	×
<u>5.</u>	26	×	<u>21.</u>	???	Х
<u>6.</u>	27	×	<u>22.</u>	???	Х
<u>7.</u>	28	×	<u>23.</u>	???	Х
<u>8.</u>	29	×	<u>24.</u>	???	×
<u>9.</u>	30	×	<u>25.</u>	???	Х
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	X	<u>27.</u>	???	X
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	Х	<u>29.</u>	???	Х
<u>14.</u>	???	×	<u>30.</u>	???	Х
<u>15.</u>	???	×	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	×

## 15. Open VPN and Remote Access>>LAN to LAN. Click index #1.

VPN and Remote Access >> LAN to LAN

[XXXXXX: This Dial-Out Profile has already joined for VPN BACKUP Mechanism] [XXXXXX: This Dial-Out Profile does not join for VPN TRUNK]

16. Type a name for such profile (e.g, cisco, in this case) and check the box of Enable this profile. Click Dial-Out as Call Direction and check Always on. Next, choose IPSec Tunnel as the Type of Server I am calling. Type the WAN IP address of the Peer (e.g., 203.70.63.90, in this case). Specify a Pre-Shared Key which must be the same as the settings configured in ASA.

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name Cisco Profile Name VPN Connection Through: WAN1 First Netbios Naming Packet Multicast via VPN (for some IGMP,IP-Camera,DHCP Relayetc.)	Call Direction O Both O Dial-Out O Dial-In Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP
2. Dial-Out Settings	
Type of Server I am calling          ISDN         PPTP         IPSec Tunnel         L2TP with IPSec Policy	Link Type     64k bps       Username     ???       Password
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) 203.70.63.90	IKE Authentication Method  Pre-Shared Key  IKE Pre-Shared Key  Digital Signature(X.509)  None

17. As for **IPSec Security Method**, choose **High**. Click **Advanced** to open **IKE advanced settings** dialog box. In the dialog, please choose the **IKE phase 1 proposal** and **IKE phase 2 proposal** settings based on the network environment. Next, click **OK** to save the settings and exit the dialog.

http://192.168.1.1 - IKE adva	nced settings - Microsoft Internet Explorer	
IKE advanced settings		
IKE phase 1 mode	Main mode     Aggressive mode	
IKE phase 1 proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2/AES128_MD5_G2/AES256_SHA1_G2/AES256_SHA1_G14	
IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5	_
IKE phase 1 key lifetime	28800 (900 ~ 86400)	
IKE phase 2 key lifetime	3600 (600 ~ 86400)	
Perfect Forward Secret	Disable     O Enable	
Local ID		
	OK Close	

18. Type the remote network IP address and subnet mask (e.g., the inside interface of CiscoASA). Then, click **OK**.

4. GRE over IPSec Settings						
Enable IPSec Dial-Out function GRE over IPSec						
📃 Logical Traffic	My GRE IP		Peer GRE IP			
5. TCP/IP Network Settings						
My WAN IP	0.0.0.0		RIP Direction Disable 👻			
Remote Gateway IP	0.0.0.0	]	From first subnet to remote network, you have to do			
Remote Network IP	192.168.1.0       255.255.255.0	]	Route 💌			
Remote Network Mask		J				
Local Network IP	192.168.20.1	]	Change default route to this VPN tunnel ( Only single WAN supports this )			
Local Network Mask	255.255.255.1					
	More					
OK Clear Cancel						

19. Now, a LAN to LAN VPN connection between Vigor router and CiscoASA has been established.