

How to setup SNMP/SYSLOG server traffic pass through IPSEC VPN tunnel using DSR with DFL

This demonstration based on a case no. xx, customer requires sending SNMP/SYSLOG traffic through IPSEC tunnel from DSR to DFL, and also needs the users under DFL to be able to access internet. For this solution, I used DSR-1000N with DFL-860E to construct the IPSEC tunnel, using a Router (DGS-3620) with three VLANs created (1.1.1.0/24, 2.2.2.0/24, 3.3.3.0/24); the interface IPs are 1.1.1.254, 2.2.2.254, 3.3.3.254 which is the gateways for DSR and DFL. And normally the IPSEC tunnel's traffic does not include the device it selves traffic (meaning traffic from WANIP), so we changed the local networks from DSR's subnet to "ANY", but for this to be workable, we need to alter the routes on DFL, which I will explain in the document later.

[Topology]

[Device]

DSR-1000Nx1 Firmware Version: 1.09B38_WW DFL-860E Firmware Version: 2.40.00.10-16817 DGS-3620 Firmware Version: 2.00.016



[Configuration] [DSR-1000N]

DSR-1000N	SETUP	ADVANCED	TOOLS		STATUS	HELP
Wizard 🕨						Helpful Hints
Internet Settings Vireless Settings Network Setting DMZ Setup	WANI SETUP This page allows you to set up as the IP Addresses, Account Ir Save Settings Dor	your Internet connection. En: nformation etc. This information n't Save Settings	ure that you have the In n is usually provided by	ternet connectic your ISP or net	LOGOUT on information such work administrator.	The setup page lets you configure the ISP settings to enable this router to connect to the Internet. This router supports multiple connections. Please select the appropriate connection to connect to the Internet
VLAN Settings	ISP Connection Type					More
Internal Users Data 🕨	ISP Connection Type:	Stat	c IP	•		
External Authentica	IP Address:	2.2.2	.1			
USB Settings	IP Subnet Mask:	255.	255.255.0			
Captive Portal	Gateway IP Address:	2.2.2	.254			
	Domain Name System (DNS)	Servers				
	Primary DNS Server:	8.8.8	.8			
	Secondary DNS Server:	8.8.4	.4			
1	MAC Address					
	MAC Address Source:	Use	Default Address	•		
	MAC Address:	00:0	0:00:00:00:00			
UNIFIED SERV	ICES ROUTER					
		Copyright © 20	4 D-Link Corporation.			

Step1. Setting up the WAN IP statically, for this demonstration the WAN IP of DSR is 2.2.2.1, gateway is 2.2.2.254

DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard 🕨					Helpful Hints
nternet Settings 🕨 🕨	IPSEC CONFIGURATION			LOGOUT	Use Tunnel mode if you require communication to be
ireless Settings	This page allows user to add/ed	dit VPN (IPsec) policies which	includes Auto and Manual poli	icies.	secured between networks. Transport mode can be used
etwork Setting >	Save Settings Dor	n't Save Settings			if the requirement is to have secure communication
MZ Setup	General				between 2 hosts. Use Manual Policy parameters if you wish
LAN Settings	Policy Name:	ipsec	-sitetosite		to specify the keys to be used for
nternal Users Data 🕨	Policy Type:	Auto	Policy V		encryption/decryption (during communication).
kternal Authentica 🕨	ID Drotocol Version:	() (UI	0v4 Dv6		This is for advanced users who require more control
	IKE Version:	• P	KEV1 O IKEV2		over IPsec tunnel communication. For normal
antive Portal	L2TP Mode:	None	e v		users, Auto Policy would do just fine. Enable Rollover
	IPsec Mode:	Tun	el Mode		only if the Port Mode is 'Auto-Rollover' in WAN MODE
	Select Local Gateway	Dedi	cated WAN		settings page. The active WAN will be used for setting
	Remote Endpoint:	IP Ar	idress 🔻		an uninterrupted VPN
	Remote Endpoint.	4.4.4	4		over IPsec checkbox to allow
	Enable Mede Configu				to DSR-1000N. Multiple users
	Enable NetBIOS				More
	Enable RollOver:	0			
	Protocol:	ESP	T		
	Enable DHCP:				
	Local IP:	Any	T		
	Local Start IP Address:				
	Local End IP Address:				
	Local Subnet Mask:	,			
	Local Profix Longth				
	Local Prenx Lengul:	0.15	nat e		
	Kemote IP:	Subr			
	Remote Start IP Address:	192.1	68.20.0		
	Remote End IP Address:				
	Remote Subnet Mask:	255.2	255.255.0		
	Pomoto Brofix Longth:				



Detection Period:	10
Reconnect after failure count:	3
Phase1(IKE SA Parameters)	
Exchange Mode:	Main 🔻
Direction / Type:	Both
Nat Traversal:	
On:	
Off:	•
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP 🔻
Local Identifier:	2.2.2.1
Remote Identifier Type:	Remote Wan IP V
Remote Identifier:	
Encryption Algorithm:	
DES:	
3DES:	
AES-128:	∠
AES-192:	
AES-256:	
BLOWFISH:	
CAST128:	
Integrity Algorithm:	
MD5:	
SHA-1:	✓
SHA2-256:	
SHA2-384:	
SHA2-512:	
Authentication Method:	Pre-shared key 🔻
Pre-shared key:	1234567890
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)

Step 2: Setting up the IPSEC policy of DSR-1000N, we used "ANY" as the local network and set 1.1.1.1 (DFL's WANIP) as remote endpoint, also use PSK as authentication method.

SR-1000N	SETUP	ADVANCED		TOOLS		STAT	us	HELP
dmin ►								Helpful Hints
ate and Time	REMOTE LOGGING CONFIG	GURATION			,		LOGOUT	Configured logs can be se
og Settings 🛛 ▷	This page allows user to cont	figure the remote loggin	g options for t	ne router.				an E-Mail address. For rem logging a key configuratio
ystem	Save Settings De	on't Save Settings						field is the Remote Log Identifier, which is the pre
irmware	Log Options							message.
lynamic DNS	Remote Log Identifier:		DSR-1000	4				More
ystem Check	Enable E-Mail Logs							
chedules	Enable E-Mail Logs:				_			
etLanguage	E-Mail Server Address:				_			
	SMTP Port:		25					
	Return E-Mail Address:		1		_			
	Send to E-Mail Address(1):	1					
	Send to E-Mail Address(2):	1		(Optional)			
	Send to E-Mail Address(3):	None	-	(Optional)			
	liser Name	r server:	NOTE		-			
	Deseword:				-			
	Respond to Identd from	SMTP Server:						
	Send E-mail logs by Sched	ule		_				
	Unit:		Never •]				
	Day:		Sunday	•				
	Time:		1:00 🔻	(AM)) (PM)			
	SYS LOG SERVER CONFIGU	JRATION		Course of the	Facility	Curel o = 1		
	SysLog Server1:	192.168.20.2		All	▼ Pacility	All	verity	
	SysLog Server2:			All	•	All	•	
	Syston Server3			All	•	All		
	Syston Server4:	,		All	•	All	•	
	Svel og ServerF:						•	
	Curling Servers:						-	
	SysLog Server6:			All	•	All	•	
	SysLog Server7:			All	•	All	•	
	Svel og Server9.			All	•	All	•	





yright © 2014 D-Link Corporatior

SR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP	
dmin 🕨					Helpful Hints	
te and Time	LOGS FACILITY			LOGOUT	In order to configure a	
og Settings 🛛 👂	This page allows user to con	figure logging severity levels for	different logging facilities.		the facility and then press	
rstem	Save Settings D	on't Save Settings			More	
rmware					THORE	
rmware via USB	Logs Facility			1		
ynamic DNS	Facility:	Syste	em 🔻			
vstem Check		Dis	play			
hedules	Display and Send Logs					
et Language		Display in Event Log	Send to Syslog			
	Emergency:					
	Alert:		s.			
	Critical:					
	Error:					
	Warning:					
	Notification:					
	Information:					
		-				

ight © 2014 D-Link Corporatior



Step 3: we setup the syslog server on DSR-1000N, which directs the syslog to 192.168.20.2 (syslog server IP), and setup which log severity you want to send to server.

[DFL-860E]

D-Link Building Networks for People					Logged in as administrator admin - 192 168 20 2
- 🍫 Home 🛛 📉 Configuration 🚽 🕇	🕆 Tools 🗸 📔 🧿 Status	👻 🛛 🔩 Maintenance 🗸			👸 Logout 🛛 🍞 Help
DFL-960E B- 🖗 System	An address for	faceAddresses	or better overview.		
Objects	Add 👻 🛃 E	dit this object			
InterfaceAddresses	# -	Name 💌	Address	User Auth Groups 🗸	Comments ~
ALG with AV/WCF	1	🗟 wan1_ip	1.1.1.1		IPAddress of interface wan1
	2	🖁 wan1net	1.1.1.0/24		The network on interface wan1
	3	wani gw	1,1,1,254		Default gateway for interface wan1.
	4	wan1 dns1	0.0.0.0		Primary DNS server for interface wan1.
	5	wan1_dns2	0.0.0.0		Secondary DNS server for interface van1.
EL- VPN Objects	6	😼 lan_ip	192.168.20.1		IPAddress of interface lan
HTTP Banner Files	7	🗟 lannet	192.168.20.0/24		The network on interface lan
FI- 8 Rules	8	dmz_ip	172.17.100.254		IPAddress of interface dmz
- S IP Rules	9	😌 dmznet	172.17.100.0/24		The network on interface dmz
slan to wan1	10	🦁 wan2_ip	192.168.120.254		IPAddress of interface wan2
Access	11	😌 wan2net	192.168.120.0/24		The network on interface wan2
- Contractions - Contraction					Right-click on a row for additional options.
PiPec GRE PPPoE PPTP/L2TP Servers PPTP/L2TP Clents SVRth Management Switch Management					

Step 1: DFL-860E's configuration is much more complicated than DSR-1000N, let's start on creating the objects for IP addresses, we change the WAN IP to 1.1.1.1, gateway to 1.1.1.254, wan-net to 1.1.1.0/24, lap IP to 192.168.20.1/24 for this scenario.

D-Link Building Networks for People					Logged in as administrator admin - 192.168.20.2
😵 Home 🛛 🔣 Configuration 🗸 🕴 👔 1	Tools 🚽 📔 👩 Status 🚽	Naintenance 🗸			👶 Logout 📔 🕐 Help
DFL-860E	Addree	SS BOOK nok contains symbolic names for various types of addresses.	including IP networks and Ethemet MAC addresse	es.	
Address Book	Add 🗸				
	# 🗸	Name 🔻	Address	User Auth Groups	Comments 👻
ALG with AV/WCF	1	InterfaceAddresses			
🗑 Services	2	😽 all-nets	0.0.0.0/0		All possible networks
······································	3	G all-nets6	::/0		All possible IPv6 networks
	4	IPSEC_remote_endpoint	2.2.2.1		
Schedules	5	G IPSEC_remote_network	192.168.10.0/24		
Authentication Objects					
🗉 📴 VPN Objects					Right-click on a row for additional options.
HTTP Banner Files					
🖻 🥞 Rules					
🖹 - 💲 IP Rules					
Cite Ian_to_wan1					
Access					
🛱 🔂 Interfaces 📃					
Ethernet					
😚 IPsec					
GRE					
PPTP/L2TP Servers					
PPTP/L2TP Clients					
SSL VPN Interface					
Switch Management 👻					

Step 2: Also create the IPSEC_remote_endpoint and remote_network, which in this case endpoint is 2.2.2.1, network is 192.168.10.0/24.



D-Link Building Networks for People		Logged in as administrator admin - 192.168.20.2	
😚 Home 🛛 🖹 Configuration 🗸 🗌 🎢 Too	ils 🗸 🧑 Status 🗸 🔧 Maintenance 🗸	🗳 Logout	Help
ALG with A/WCF ALG with A/WCF ALG with A/WCF A/Ke with A/WCF A/K	Solution Solution		-
an_to_wan1	Passphrase:		
Access	Generate Random Key		
E- Contractes			
Ethernet			
2 Date	Since regular words and pritases are vulneratore to dictionary attacks, do not use them as SfMaYed SeCrets.		
CRE			
PPPoE	2 Comments		
PPTP/L2TP Servers	Comments:		_
PPTP/L2TP Clients			
- 📬 SSL VPN Interface 🗸 🗸			

Step 3: Now we start to create the IPSEC policy, first we need to create the Preshared-key object, in the Authentication Objects we add a new IPSEC key, and the value must be equal to the DSR's pre-shared key.

D-Link Duilding Networks for People	es administrator 12.168.20.2
🏷 Home 💥 Configuration + 🎢 Tools + 🧟 Status + 🔩 Maintenance +	😚 Logout 🛛 👔 Help
Objects Site_to_site_IPSEC Als with AUWOF Site_to_site_IPSEC Als with AUWOF Site_to_site_IPSEC Solves General Authentication Objects Site_to_site_IPSEC Authentication Objects Innet Authentication Objects Biness Authentication Objects Biness Files Innet Interformed Tunnet Names Interformed Authentication Objects Bin_so_wanti Bin_Sowner Interformed Bin_Sowner	
Behavenet Medium	
Lig/U-LAN Inc. Ligenine 28800 seconds	
PFEPLZTP Servers PSeconds Seconds	
PPTPIL2TP Clients IPsec Lifetime: 0 kilotytes	
SSU-FN Interface Switch Management Interface Groups	
Comments:	-



D-Link Building Networks for People	Logged in as administrator admin - 192 168 20 2
🗞 Home 💥 Configuration 🗸 🎢 Tools 🗸 📀 Status 🗸 🔩 Maintenance 🗸	👶 Logout 🕐 Help
Stee to site IPSee to site IPSee Address Book Address Addres Address Address	
Bit Ethernet Gateway certificate (None) Bit Ethernet Identification fat: (None) Bit	
Switch Management Local ID Type: Auto Seets the type of Local ID to use. Local ID Value: Specify the local identity of the tunnel ID.	

D-Link Building Networks for People		dmn - 192.168.20 2
😙 Home 🛛 📉 Configuration 🗸 🛛 🕂 Tor	ols 🗸 📔 🧟 Status 🗸 🛛 🗞 Maintenance 🗸	😚 Logout 📔 🍞 Help
Coljects Collects Co	Site to site IPSEC An itsec turned item is a used to define iffsec endpoint and will appear as a logical interface in the system. General Authentication Authentication Kauth © Noting IKE Settings Alow DMCP over if Place from single-loss of lens © Dradnicatly add rouch to the memore network when a turnel is established Dont check this checkbox P acket Sizes Specify the size at which to fragment plaiment packets (rather than fragmenting iPsec). Plantent MfU: 1420 Plantent MfU: 1420 Plantent MfU: 1420 Plantentsally plak the address of a local interface that corresponds to the local net Specify address manualy: IP Addresse: IP Addresse: IP Address: Image:	OK Cancel





Step 4: the above four screenshots are the set up for our IPSEC policy on DFL, for the first screenshot, we can see that the IPSEC is DFL's LAN network to ALL-nets, and we use MEDIUM for IKE algorithm and IPSEC algorithm. The second screenshot shows we use the pre-shared key we created earlier. The third and fourth screenshots we uncheck both boxes because we don't want the DFL to automatically create the routes, we will manually create the IPSEC routes later.

D-Link Building Networks for People								gged in as administrator min - 192.168.20.2
😙 Home 🛛 📉 Configuration 🗸 🛛 🎢 Too	ls 🚽 📔 🦲	Status 🗸 📔 🗞 Mainter	nance 🚽					👶 Logout 🔰 👔 Help
DFL-860E	8 I	P Rules rules are used to filter IP-based	network traffic. In a	addition, they provide means for add	ress translation as well as Server Load Ba	lancing.		
InterfaceAddresses	# 🕶	Name 👻	Action 🔻	Src If -	Src Net 🔻	Dest If 👻	Dest Net 👻	Service 👻
ALG with AV/WCF	1	<pre>\$ ping_fw</pre>	👬 Allow	🔝 any	💡 all-nets	Core	💡 all-nets	🧑 ping-inbound
Services	2	📑 lan_to_wan1						
IP Pools	3	<pre>\$ ipsec_outgoing</pre>	Allow	🔝 lan	💡 lannet	😚 site_to_site_IPSEC	IPSEC_remote_network	all_services
Cabadulas	4	ipsec_outgoing	Allow	🔝 lan	🗟 lannet	😚 site_to_site_IPSEC	IPSEC_remote_endpoint	all_services
Authentia stice Objects	5	\$ ipsec_incoming	Allow	ite_to_site_IPSEC	IPSEC_remote_network	🔝 lan	🗟 lannet	all_services
Authentic ation Objects	6	\$ ipsec_incoming	👬 Allow	😚 site_to_site_IPSEC	IPSEC_remote_endpoint	🔝 lan	🗟 lannet	all_services
/ HTTP Banner Files							(D) Right-	lick on a row for additional ontions
E-is Rules :- S IP Rules :- Access								
I Ethornot								
- A IPsec								
- R GRE								
PPPoE								
PPTP/L2TP Servers								
PPTP/L2TP Clients								
SSL VPN Interface								
Switch Management								

Step 5: Now we add the IP Rules which ALLOW the traffic from LAN LANNET to IPSEC interface IPSEC remote network/remote endpoint and the other side vice versa, why do we need two IP rules for this? This is because we want to allow the traffic which is from DSR's LAN network and also DSR's WAN IP.

D-Link Building Networks for People								
ols 🚽 📔 🦲 S	Status 🗸 🛛 🗞	Maintenance 🗸						👶 Logout 📔 👔 Help
The The	system has a predef	ned main routing table. Alternate rou	ting tables can be defined by the user.					
# 🗸	Туре 🔻	Interface 💌	Network	Gateway 💌	LocalIP	Metric 💌	Monitor this route 🔻	Comments -
1	्री [®] Route	🔝 wani	🤤 waninet			100	No	Direct route for network wan1net over interface wa
2	्ही Route	wan1	🤤 all-nets	😽 wan1_gw		100	No	Default route over
з	्री [®] Route	wan2	💡 wan2net			100	No	Direct route for network wan2net over interface wa
4	्री Route	🔝 dmz	🦁 dmznet			100	No	Direct route for network dmznet over interface dmz
5	्री Route	🔝 lan	🦞 lannet			100	No	Direct route for network lannet over interface lan
6	ुी Route	👶 site_to_site_IPSEC	PSEC_remote_endpoint	с		0	No	
7	J Route	😚 site_to_site_IPSEC	9 192.168.10.0/24			0	No	
							(j) Roh	click on a row for additional options.
	ols • • • • • • • • • • • • • • • • • • •	ols Status S	ols V Status V Maintenance V main The system has a predefined main routing table. Atemate rou Add V Status object V Add V Add V Status object V Add V Add V Status object V Add V	Status No. Maintenance The system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its system has a predefined main routing table. Attenute routing tables can be defined by the user. Its Route Its van1 Its routing Its van1 Its Route Its van1 Its routing Its routing Its routing	Status No Maintenance Image: Status Note Maintenance Image: Status Maintenance Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status	Status Age Maintenance Imain The system has a prederied main routing table. Atemate routing tables can be defined by the user. Image: Adv	Status Note Network Gateway LocalIP Metric ~ Image: Status Interface Network ~ Gateway ~ LocalIP Metric ~ Image: Status Interface Network ~ Gateway ~ LocalIP Metric ~ Image: Status Interface Network ~ Gateway ~ LocalIP Metric ~ Image: Status Interface Network ~ Gateway ~ LocalIP Metric ~ Image: Status Image: Status	Status Net Maintenance Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status Image: Status



Step 6: Now we manually add the two routes which specifies that DSR's WANIP and DSR's LAN network goes through the IPSEC VPN interface.

[Configuration on DGS-3620] Set the three VLANs and their ports: DGS-3620-52P:admin#create vlan vlanid 10 DGS-3620-52P:admin#create vlan vlanid 20 DGS-3620-52P:admin#create vlan vlanid 30 DGS-3620-52P:admin#config vlan vlanid 1 delete 1-52 DGS-3620-52P:admin#config vlan vlanid 10 add untagged 1-4 DGS-3620-52P:admin#config vlan vlanid 20 add untagged 5-8 DGS-3620-52P:admin#config vlan vlanid 30 add untagged 9-12 DGS-3620-52P:admin#create ipif vlan10-if 1.1.1.254/24 VLAN10 DGS-3620-52P:admin#create ipif vlan20-if 2.2.2.254/24 VLAN20 DGS-3620-52P:admin#create ipif vlan30-if 3.3.3.254/24 VLAN30 The above CLI is setting up the router which has three interfaces, VLAN10 20 and 30, for VLAN10 it is directly connected to 1.1.1.1 and has interface IP 1.1.1.254, for VLAN20 it is directly connected to 2.2.2.1 which has interface IP 2.2.2.254, and finally the VLAN30 which in this case simulates the internet.

[Test Results]

We should be able to send SNMP/SYSLOG traffic to DFL's LAN network from DSR's WAN IP; also DFL's users should be able to access 3.3.3.254 through 1.1.1.1, and when pinging 2.2.2.1 and 192.168.10.1/24 should go through IPSEC tunnel.





Serial-COM4_9600 - SecureCRT			×	Product Page: 058-100	9N	Hardware Version: A1	Firmware Wesion: 1.05838_WW
File Edit View Options Transfer S	ript Tools Window Help			D-Li	nk		
13 73 43 X h & C (G S &) 1 ? 7				DSR-1000N ///	SETUP ADVANCED	TOOLS STATUS	HELP Helpful Herts
<pre>DFL-860E:/> ping 192.168.10.1 Sending 1 4-byte ICMP ping to 192.168.10.1 From 192.168.20.1 ICMP Reply From 192.168.10.1 seq=0 time=<10 ms TTL=64</pre>				Logs Frank Monitor Clients	The page will active free the ACTIVE VPN This page display the active VPK connections, IPSEC, SSL, IPTP and Active IPsec KM Policy Name Endpoint In (KB) ID (Packets)	f Locour f L219. State Action	This page lats current established Prec Security Associations, SSL VPN funnals, PTPI VPN Claint and L2TP VPN Claint connections. More
Ping Results: Sent: 1, Received DFL-860E:/> ipsec Command Description	1, Loss: 0%, Avg RTT: 10	.0 ms		Active VPNs	igsec-statistice 1.1.1.1 3159.45 12464 Active SSLVPM Connections User Name IP Address Local PPP Interface Altive PPIP VIN connections Connections Connections	Peer PPP Interface IP Connect Status Action	
ipsecglobalstats Show global ip ipseckeepalive Show status of ipsecstats Show the SAs : ipsectunnels Lists the cum DEL=860F:/>ipsecstats	sec statistics the IPsec ping keepaliv nuse ent IPsec configuration	es successful ipsec connection			Disconnected Adhes 1219 Viet connections Connection Status Disconnected Poll Interval: 10 [Second]	Action Connect Start Step	
Active IPsec SAs:				UNIFIED SER	VICES ROUTER		
Displaying one line per SA-bund					Copyright & 2014 D-Link	Colorador.	
IPsec Tunnel Local Net	Remote Net	Remote Endpoint					
site_to_site_IPSEC 192,168,20,0	/24 0.0.0.0/0	2.2.2.1	-				
Ready Seria	COM4 24, 13 24 Rows, 80	Cols VT100					

The IPSEC tunnel is successfully created.

ilo Edit I	Joervice in	anager (Registered	- version 0.5.	20)						~
		age Help Display 00 (Dofaul								
	A 1997 (Display ou (Deraul	u •	u						-
0-31-2014	15:22:12	Kernel.Warning	2.2.2.1	message Jan 01 04:30:23 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN_SRC=192.168.10.1 DST=	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	ΞĊ
	45 00 40		0004	CODE=3 SRC=192.168.10.100 DST=157.55.130.167 PROT0=UDP SPT=52117 DPT=40025<000>		400				4
0-31-2014	15:22:12	Kernel. Warning	2.2.2.1	Jan UI U4:30:23 Sat 2000 [GMT] DSH-1000N KEHNEL [Kernel] same_src : Invalid address [] LUG_PALKET[ALLUW] IN=SELF UUT=LA PROTO=ICMP TYPE=3 CODE=3 SRC=192.168.10.100 DST=157.55.235.160 PROTO=UDP SPT=52117 DPT=40006<000>	N SHL	=192.	168.1	0.1 DS	1=192.168.10.10	,
0-31-2014	15:22:12	Kernel.Warning	2.2.2.1	Jan 01 04:30:23 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] UID=0 GID=0 MARK=0x666 L0G_PACKET[ALLOW] IN=SELF 0UT=WA SPT=44551 DPT=53<000>	I SRC	=2.2.2	2.1 DS	T=8.8.	8.8 PROTO=UDP	
0-31-2014	15:22:12	Kernel.Warning	2.2.2.1	Jan 01 04:30:23 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODF=3 SRC=192.168.10.100 DST=157.55 235.124 PR010=LIDP SPT=52117 DPT=40011(000)	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	1
0-31-2014	15:22:12	Kernel.Warning	2.2.2.1	Jan 01 04:30:23 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODE=3 SRC=192.168.10.100 DST=111.221.77.175 PR010-LIDP SPT=52117 DPT=40003:0005	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src: Invalid address_src: Invalid address	ess sa .100 D	me_sr IST=6	c:ln 4.4.2	valid ac 3.157 P	idress [] 'ROTO=UDP	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODE=3 SRC=192.168.10.100 DST=157.55.235.171 PROT0=UDP SPT=52117 DPT=40006<000>	192.16	8.10.	100 P	ROTO-	ICMP TYPE=3	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src : Invalid address same_src : Invalid address [] LOG_PACKET[# SRC=192 168 10.1 DST=192 168 10.100 PR0T0=ICMP TYPE=3 CDDE=3 SRC=192 168 10.100 DST=213 199 179 152 PR0T0=UDP SF	LLO₩ T=521] IN=: 17 DP	SELF T=40	OUT= 013<00	LAN IO>	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODE=3 SRC=192.168.10.100 DST=157.56.52.46 PRDT0=UDP SPT=52117 DPT=40019<000>	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] UID=0 GID=0 MARK=0x666 L0G_PACKET[ALLOW] IN=SELF OUT=WA SPT=54374 DPT=53:000>	I SRC	=2.2.2	.1 DS	T=8.8.	4.4 PROTO-UDP	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src : Invalid address same_src : Invalid address same_src : Invalid address same_src : Invalid address same_src : Invalid IN-SELF_0UT=LAN SRC=192.168.10.1 DST=213.193.179. DPT=40005:0005	addre 173 PF	\$\$ [] L Roto=	.06_F =UDP	ACKET SPT=5	[ALLOW] 2117	
0-31-2014	15:22:07	Kernel.Warning	2.2.2.1	Jan 01 04:30:18 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODE=3 SRC=192.168.10.100 DST=157.56.52.32 PROT0=UDP SPT=52117 DPT=40030<000>	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src : Invalid address same_src : Invalid address same_src : Invalid IN-SELF OUT=LAN SRC=192.168.10.1 DST=192.168.10.100 PROTO=ICMP TYPE=3 CODE=3 SRC=192.168.10.100 DST=64.4.23.157 I	addre ROTO	ss [] L =UDP	OG_F	ACKE1	[ALLOW] DPT=40019<000	,
0-31-2014	15:22:01	Kernel.₩arning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF_OUT=LAN SRC=192.168.10.1 DST= CODE=3 SRC=192.168.10.100 DST=157.56.52.43 PRDT0=UDP SPT=52117 DPT=40006<000>	192.16	8.10.	100 P	ROTO=	ICMP TYPE=3	
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src : Invalid address [] LOG_PACKET[ALLOW] IN=SELF_OUT=LA PROTO=ICMP TYPE=3 CODE=3 SRC=192.168.10.100 DST=213.199.179.166 PROT0=UDP SPT=52117 DPT=40032(000)	N SBC	=192	168 1	0 1 DS	L=192.168.10.100	J
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] UID=0 GID=0 MARK=0x666 L0G_PACKET[ALLOW] IN=SELF OUT=WA SPT=33001 DPT=53:000>	5	昏	1	٩	PROTO=UDP	
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN-SELF_OUT=LAN_SRC=192.168.10.1 DST CODE=3 SRC=132 168 10.100 DST=64.4.23.145 PROT0=UDP_SPT=52117 DPT=40020<00D		9	0	3	MP TYPE=3	
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] same_src : Invalid address same_src : Invalid address [LGG_PACKET[ALLOW] IN-SELF_OUT=LAN SRC=192.168.10.1 DST=192.168.10.100 PROTO=ICMP TYP DST=213.197.197.140 PROTO_IDF PST=52171 DPT=4000192.0000.	*	0			address 10.100	
0-31-2014	15:22:01	Kernel.Warning	2.2.2.1	Jan 01 04:30:13 Sat 2000 (GMT) DSR-1000N KERNEL [Kernel] [] LOG_PACKET[ALLOW] IN=SELF OUT=LAN SRC=192.168.10.1 DST CODE=3 SRC=192.168.10.100 DST=64.4.23.147 PROT0=UDP SPT=52117 DPT=40003<000>	T Customize		MP TYPE=3			

The SYSLOG is successfully transferred to DFL's LAN network [Conclusion]: Using the above settings we are able to send traffic through IPSEC tunnel from DSR to DFL.

[End Of Document]