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.

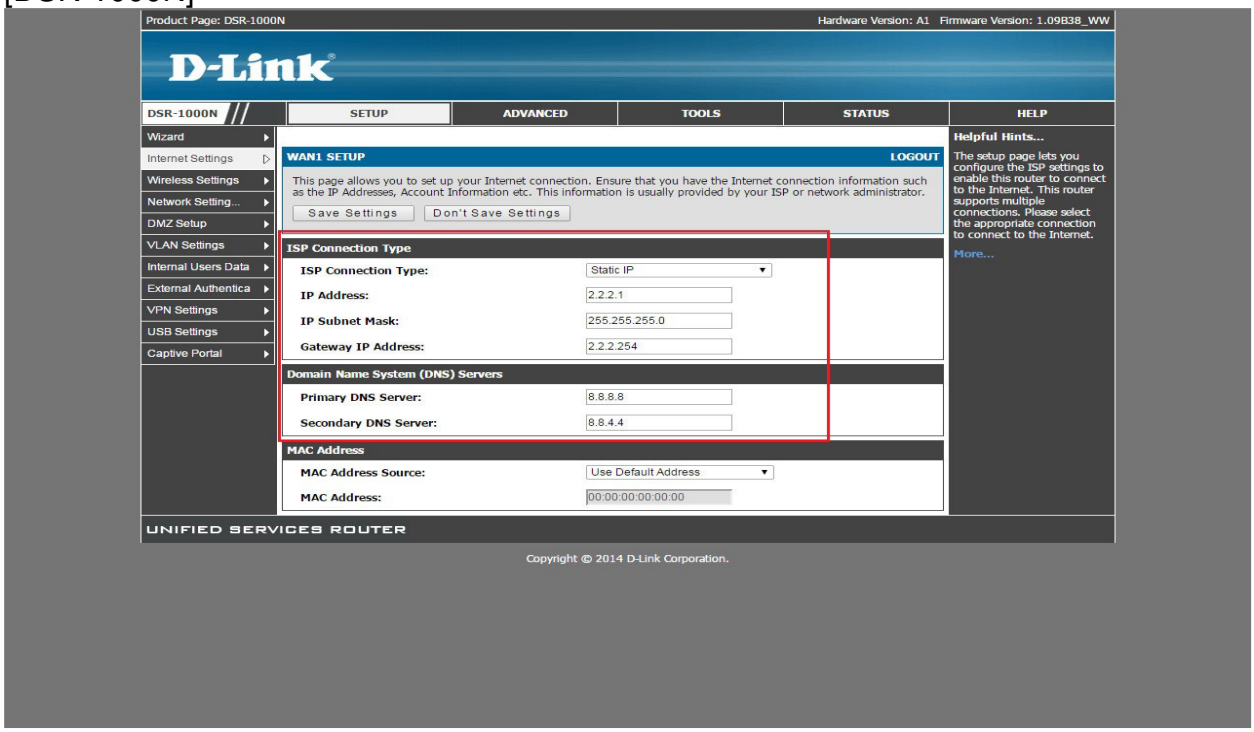
[Topology]

PC01---DSR-1000N(2.2.2.1)---(2.2.2.254) (Router)(1.1.1.254) ---(1.1.1.1) DFL-860E---Syslog Server

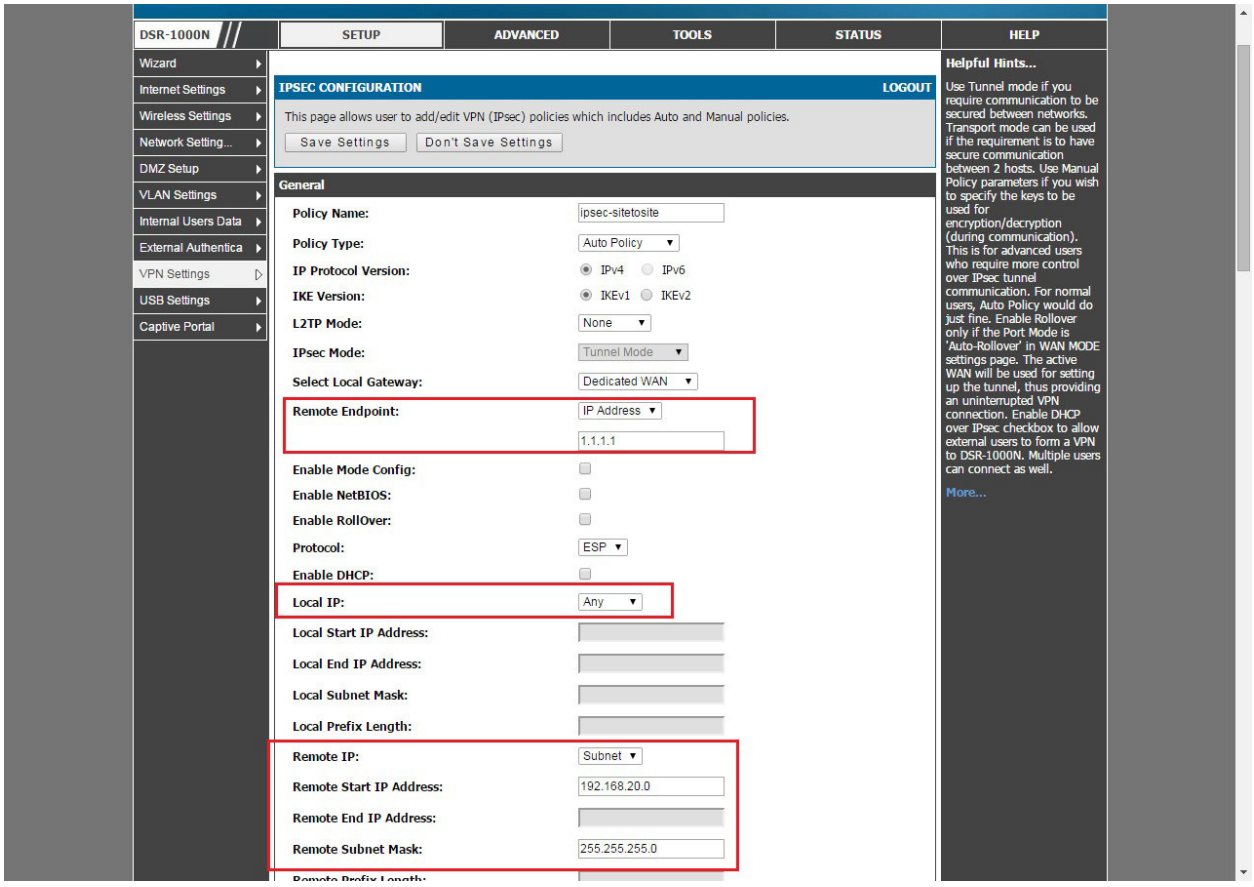
[Device]

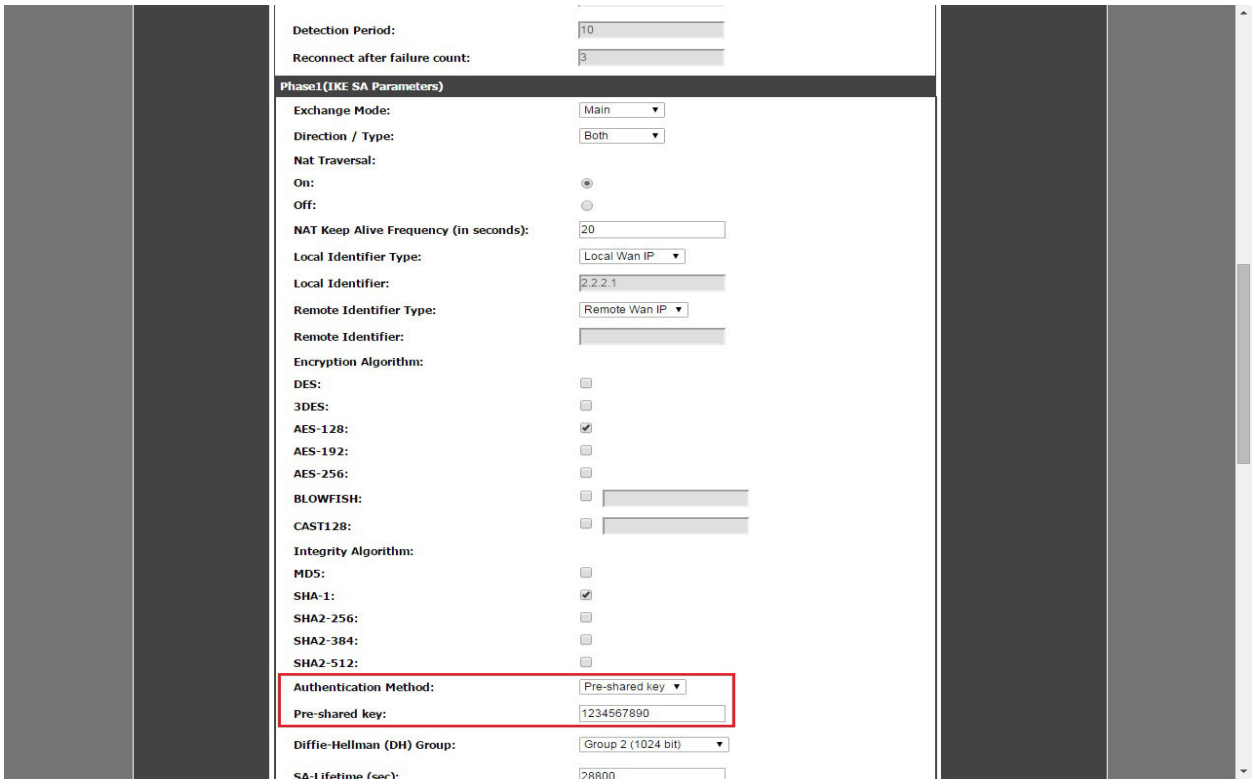
DSR-1000Nx1
Firmware Version: 1.09B38_WW
DFL-860E
Firmware Version: 2.40.00.10-16817
DGS-3620
Firmware Version: 2.00.016

[Configuration]
[DSR-1000N]

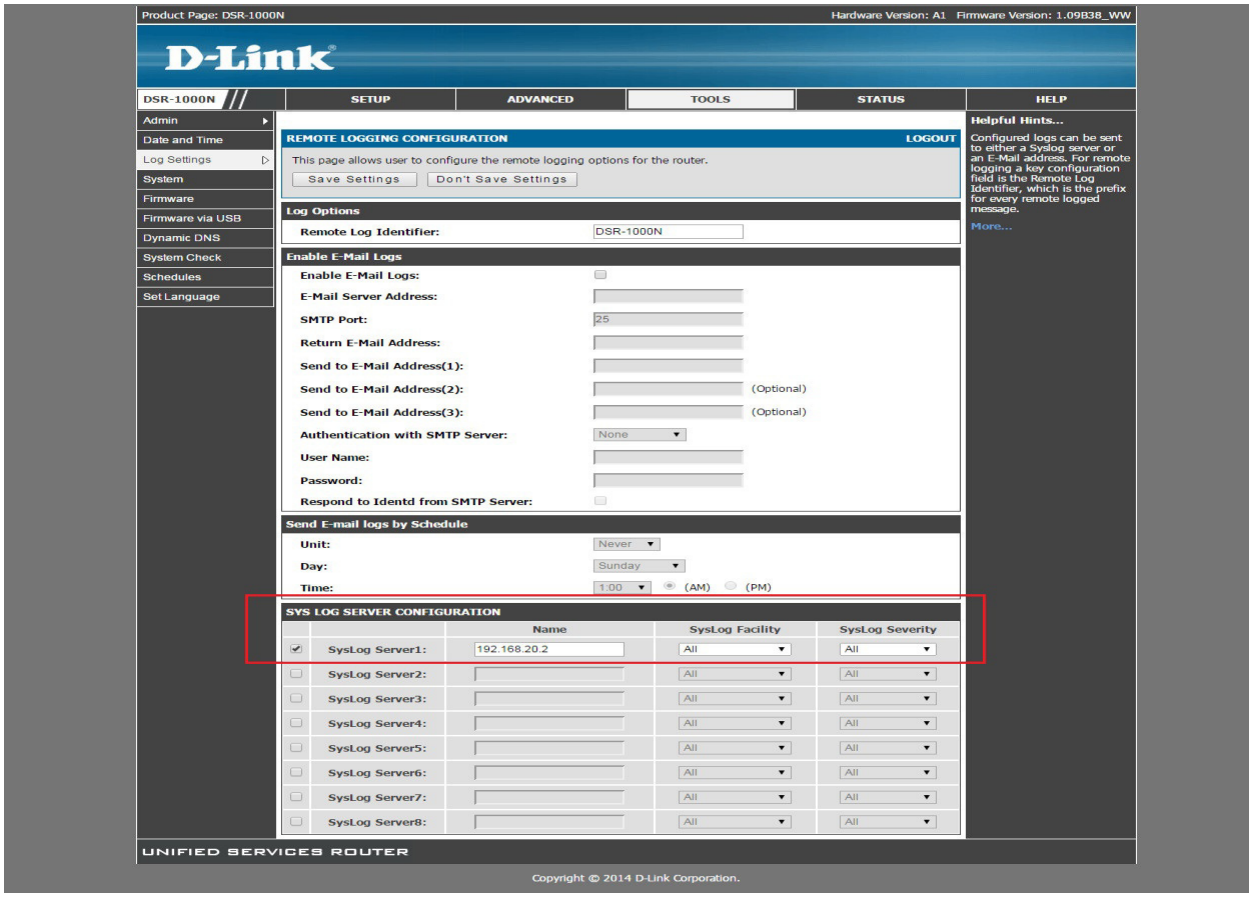


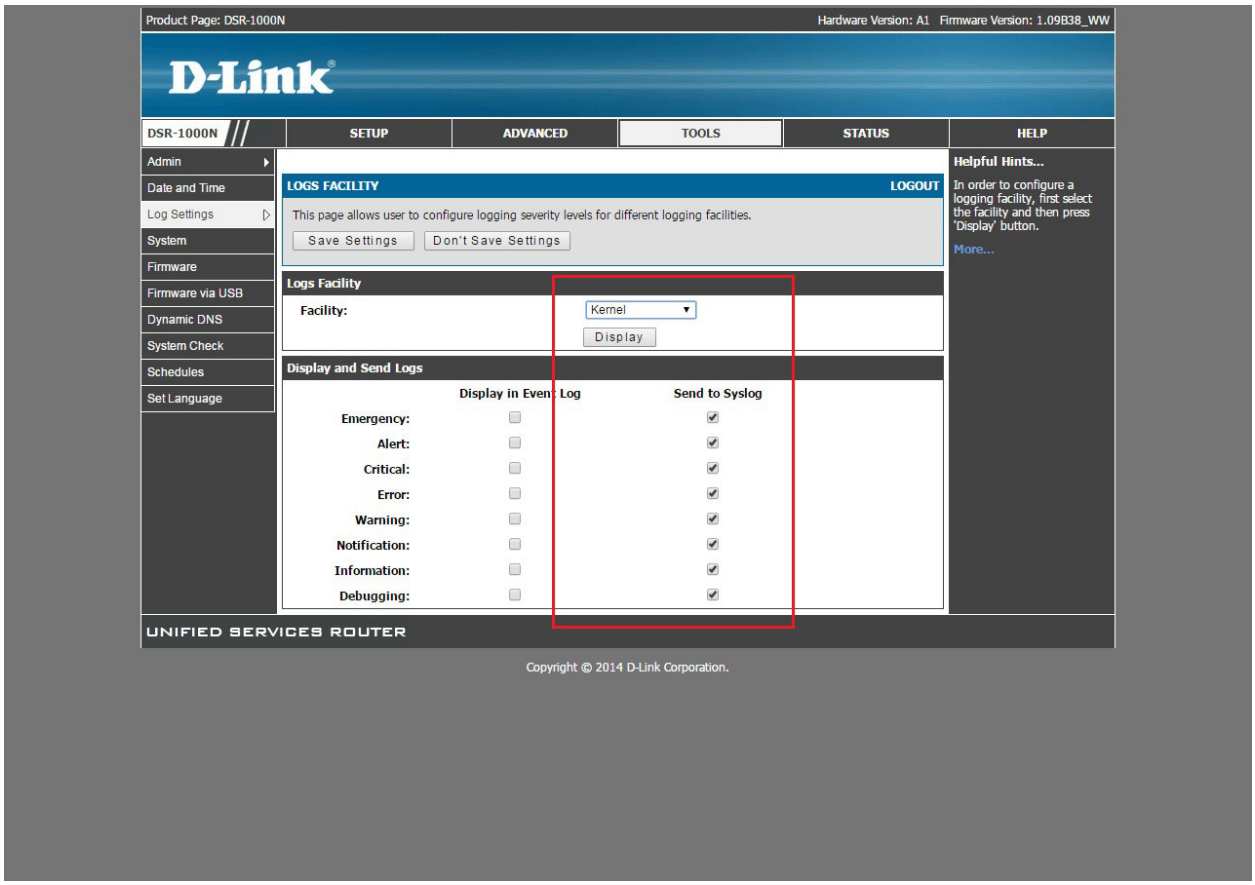
Step1. Setting up the WAN IP statically, for this demonstration the WAN IP of DSR is 2.2.2.1, gateway is 2.2.2.254

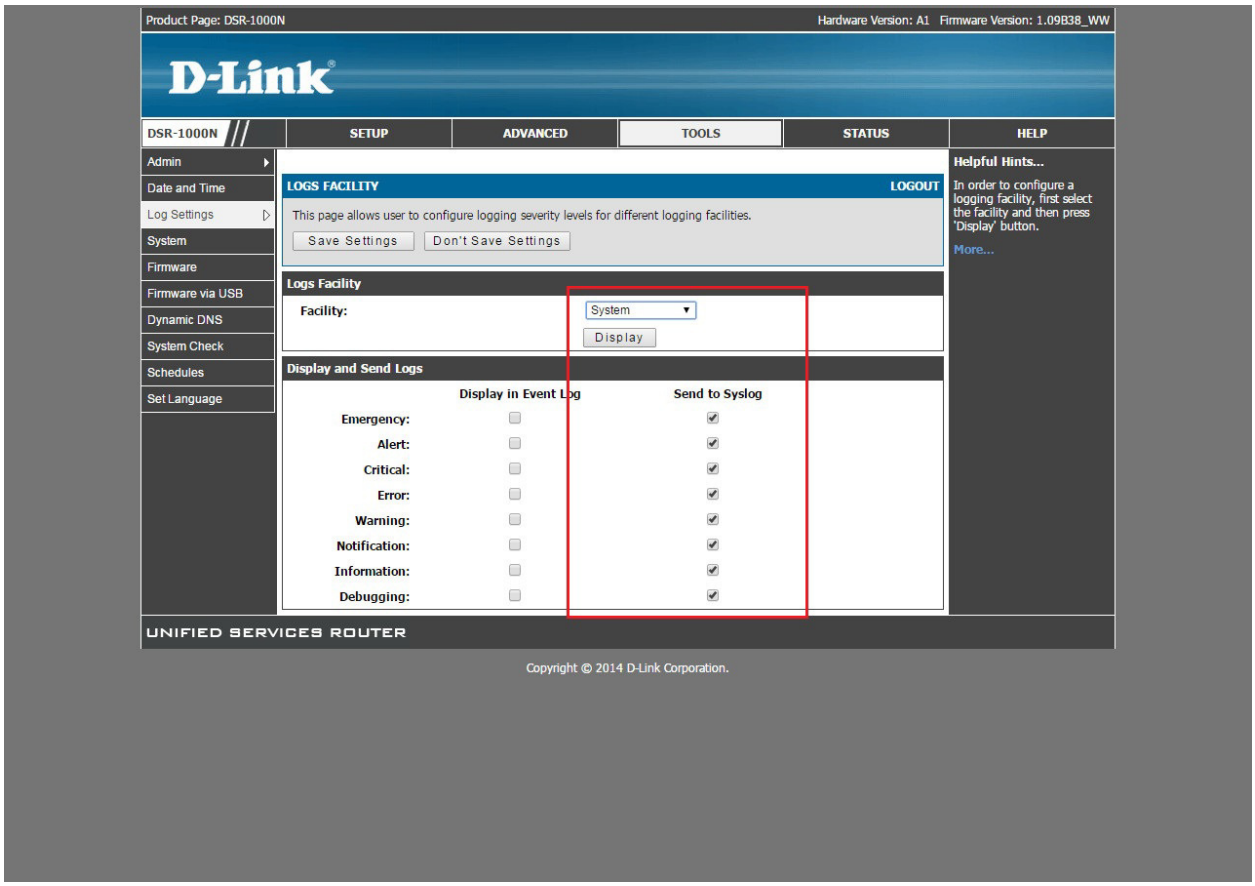




Step 2: Setting up the IPSEC policy of DSR-1000N, we used “ANY” as the local network and set 1.1.1.1 (DFL’s WANIP) as remote endpoint, also use PSK as authentication method.

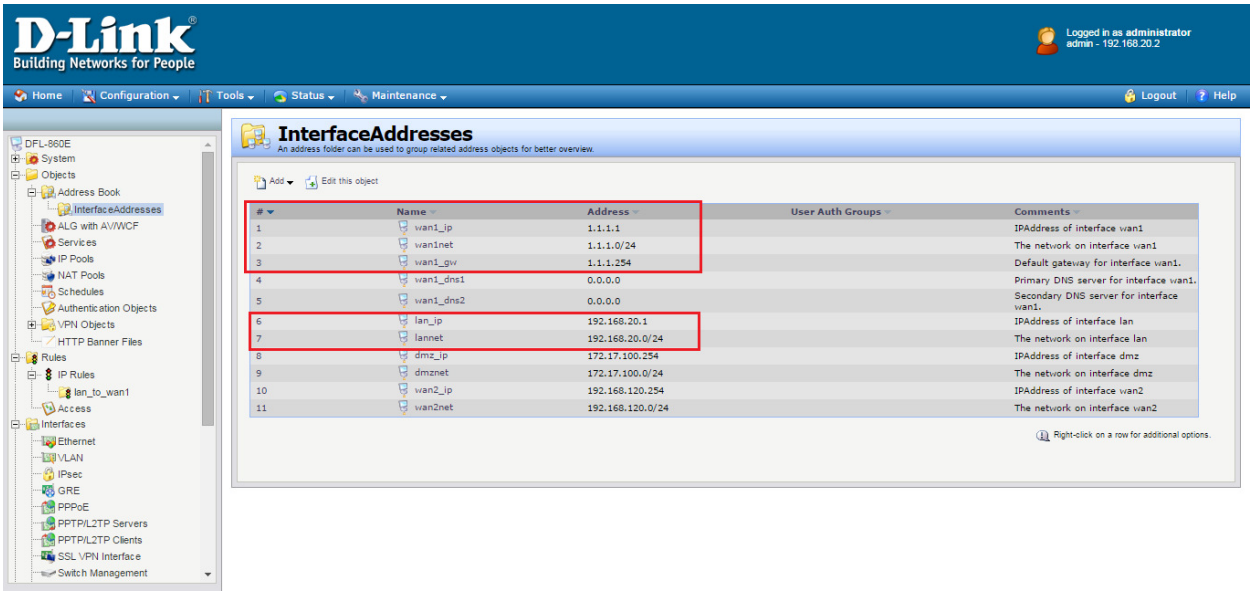



Product Page: DSR-1000N
Hardware Version: A1 Firmware Version: 1.09B38_WW
D-Link
DSR-1000N
SETUP
ADVANCED
TOOLS
STATUS
HELP
Admin
Date and Time
Log Settings
System
Firmware
Firmware via USB
Dynamic DNS
System Check
Schedules
Set Language
LOGS FACILITY
LOGOUT
This page allows user to configure logging severity levels for different logging facilities.
Save Settings
Don't Save Settings
Logs Facility
Facility:
Kernel
Display
Display and Send Logs
Display in Event Log
Send to Syslog
Emergency:
Alert:
Critical:
Error:
Warning:
Notification:
Information:
Debugging:
Helpful Hints...
In order to configure a logging facility, first select the facility and then press 'Display' button.
More...
UNIFIED SERVICES ROUTER
Copyright © 2014 D-Link Corporation.

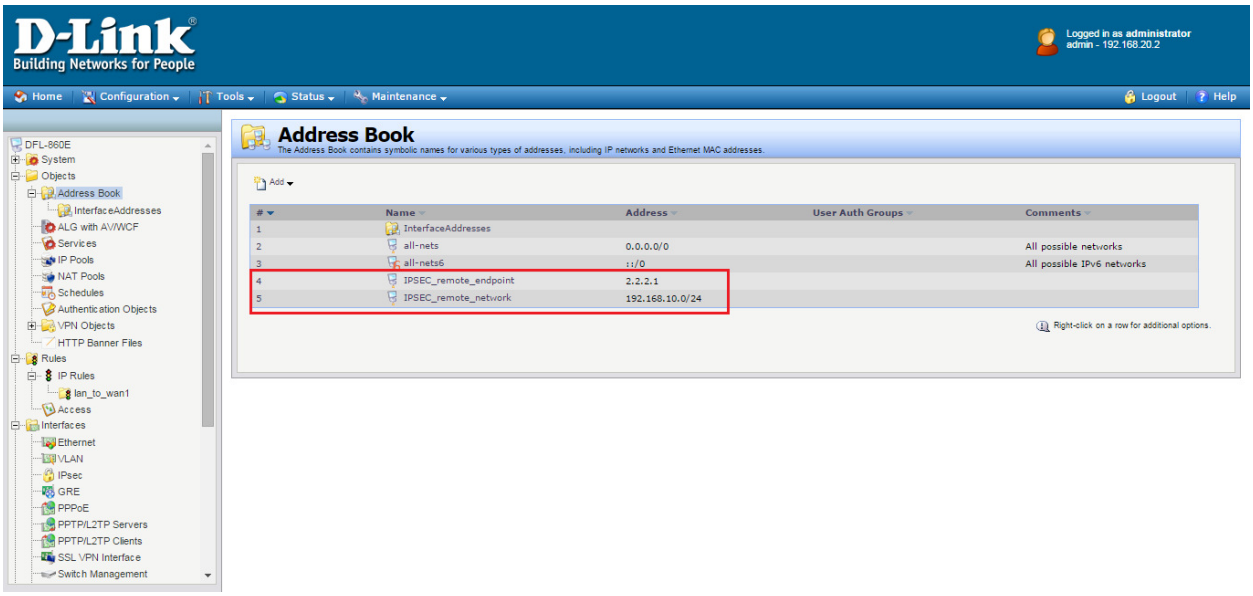

Product Page: DSR-1000N
Hardware Version: A1 Firmware Version: 1.09B38_WW
D-Link
DSR-1000N
SETUP
ADVANCED
TOOLS
STATUS
HELP
Admin
Date and Time
Log Settings
System
Firmware
Firmware via USB
Dynamic DNS
System Check
Schedules
Set Language
LOGS FACILITY
LOGOUT
This page allows user to configure logging severity levels for different logging facilities.
Save Settings
Don't Save Settings
Logs Facility
Facility:
System
Display
Display and Send Logs
Display in Event Log
Send to Syslog
Emergency:
Alert:
Critical:
Error:
Warning:
Notification:
Information:
Debugging:
Helpful Hints...
In order to configure a logging facility, first select the facility and then press 'Display' button.
More...
UNIFIED SERVICES ROUTER
Copyright © 2014 D-Link Corporation.

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.

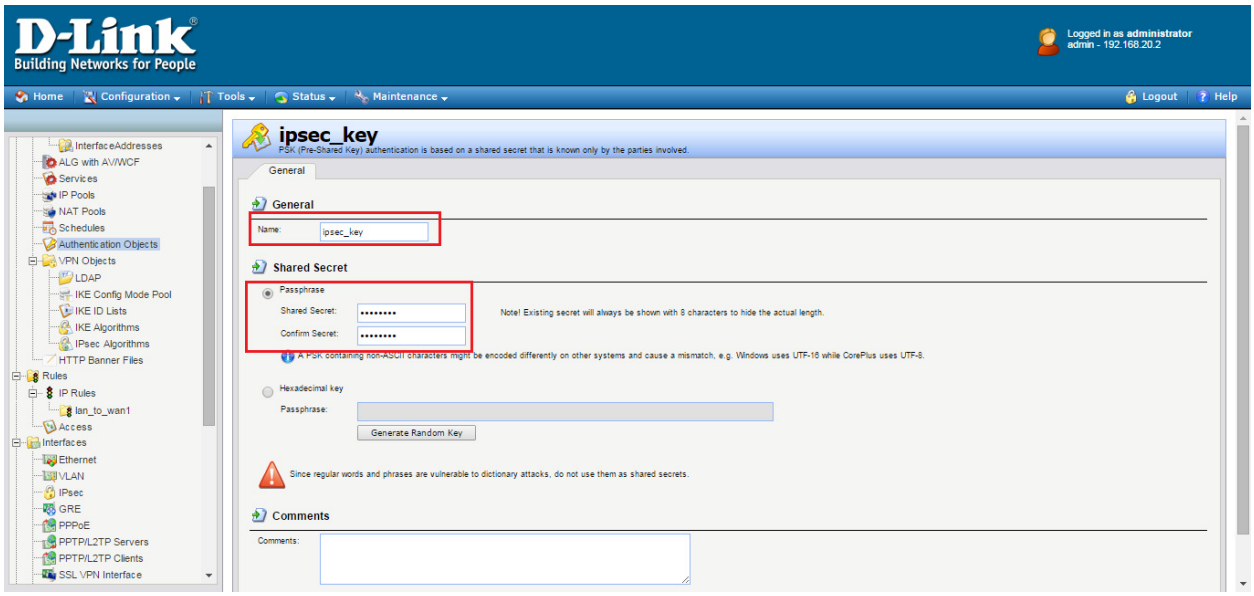
[DFL-860E]



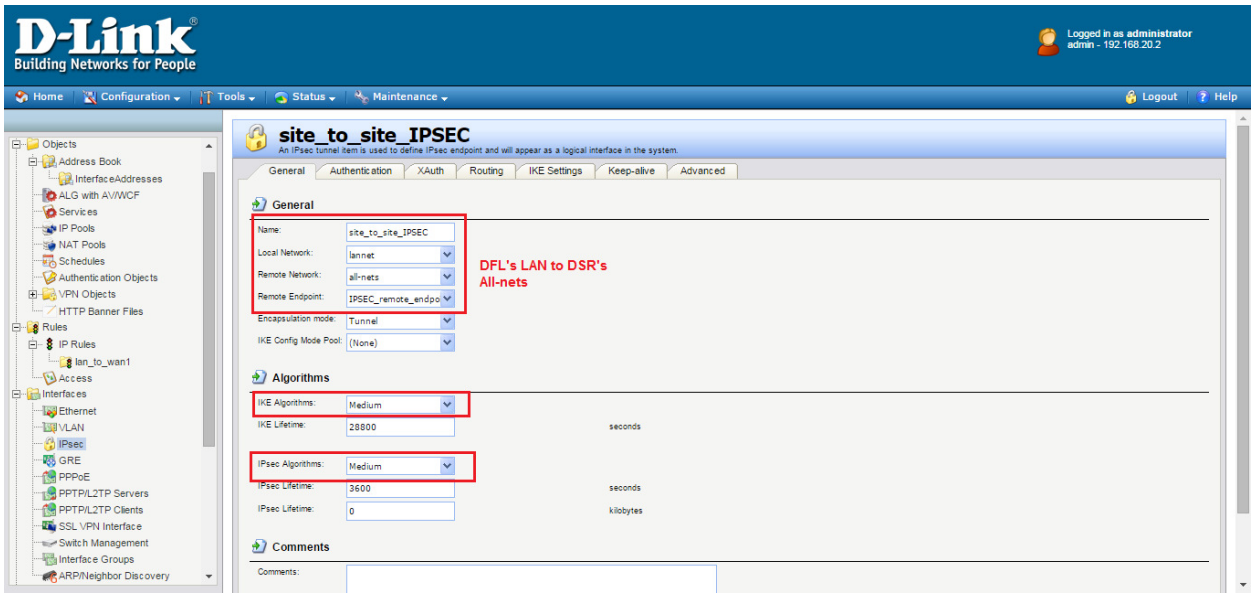
Step 1: DFL-860E's configuration is much more complicated than DSR-1000N, let's start on creating the objects for IP addresses, we change the WAN IP to 1.1.1.1 , gateway to 1.1.1.254, wan-net to 1.1.1.0/24, lap IP to 192.168.20.1/24 for this scenario.

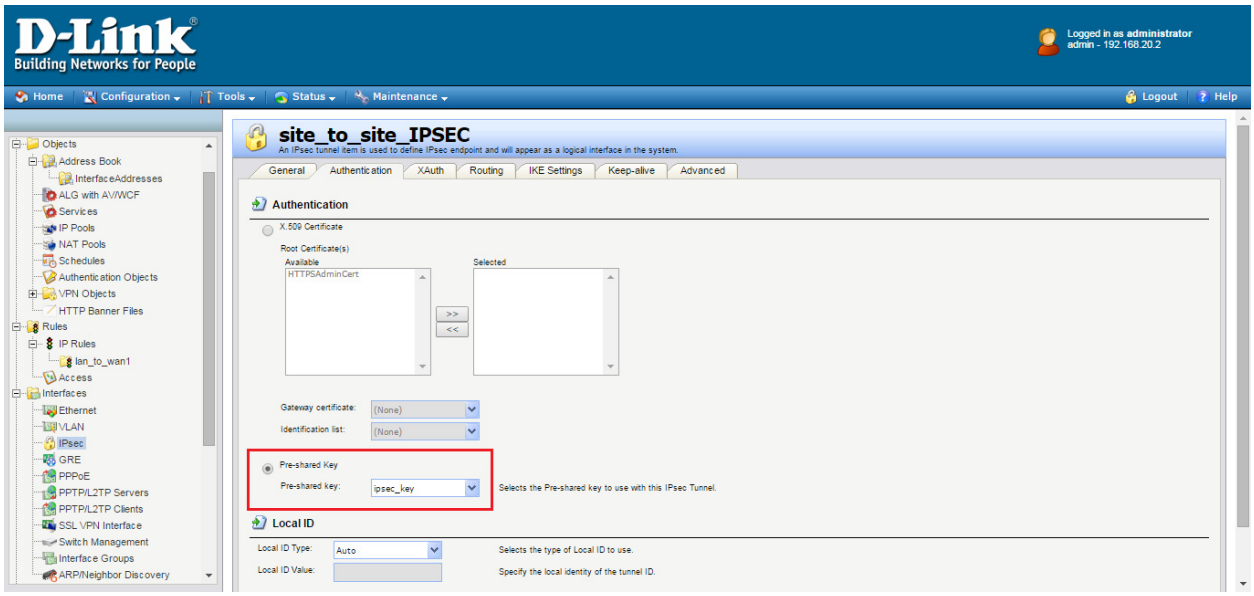


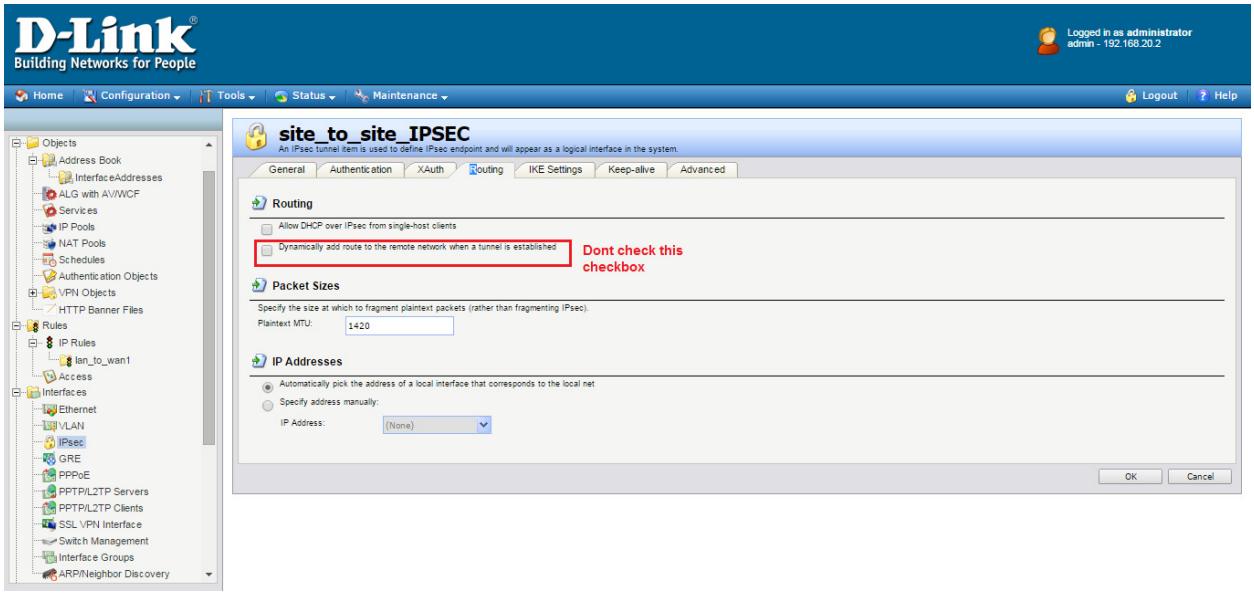
Step 2: Also create the IPSEC_remote_endpoint and remote_network, which in this case endpoint is 2.2.2.1, network is 192.168.10.0/24.

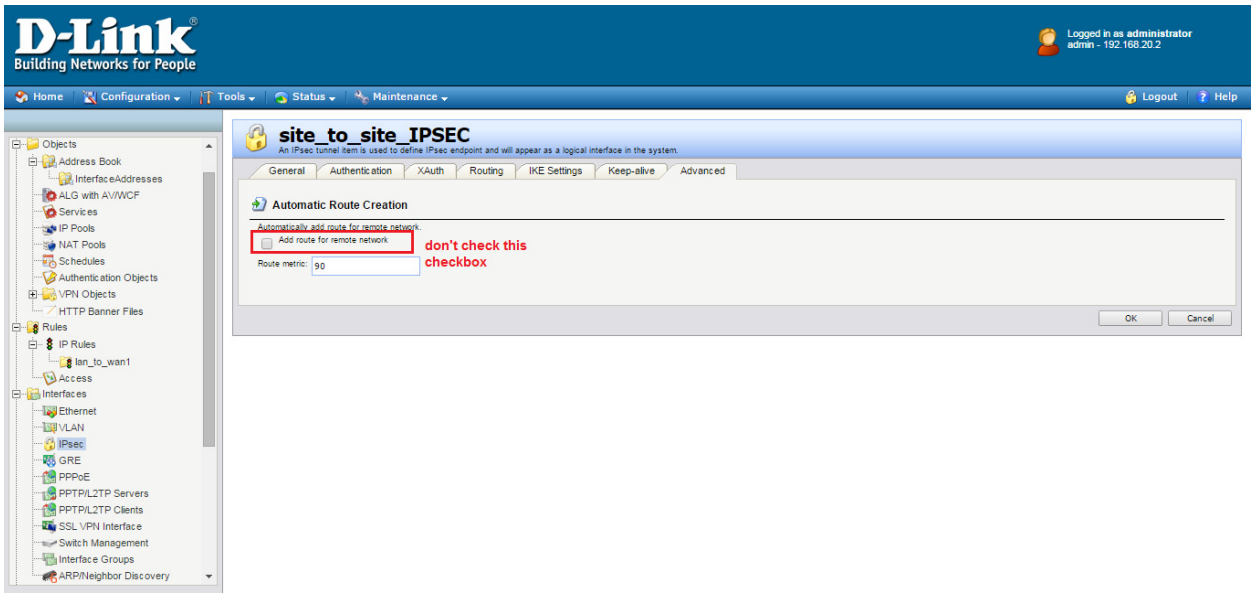


Step 3: Now we start to create the IPSEC policy, first we need to create the Pre-shared-key object, in the Authentication Objects we add a new IPSEC key, and the value must be equal to the DSR's pre-shared key.

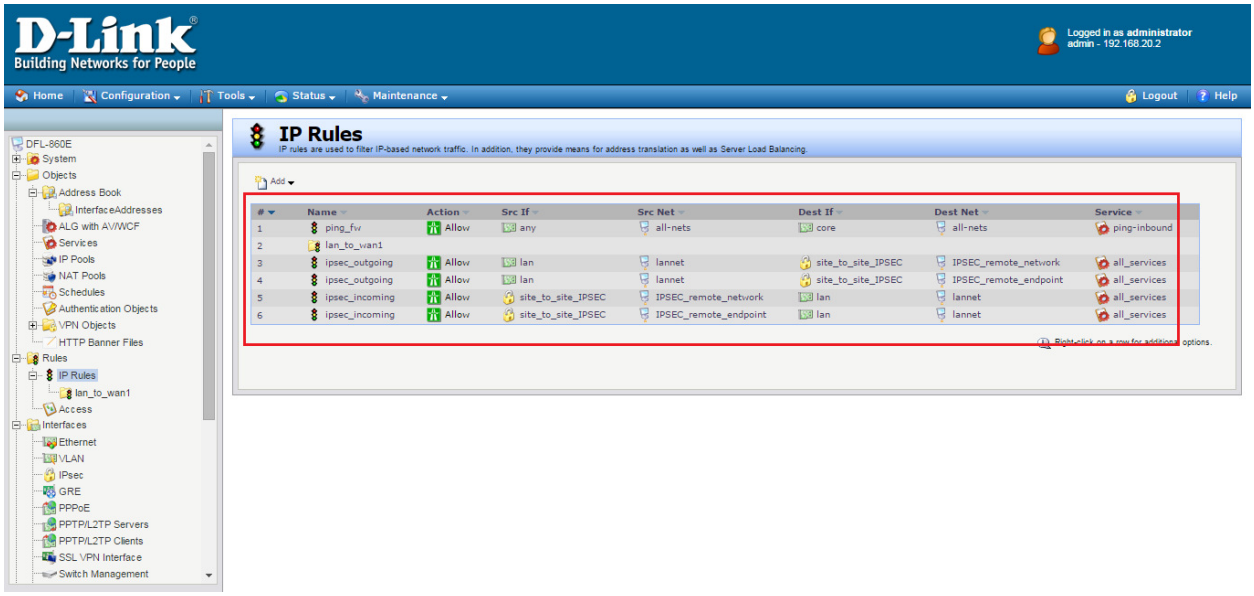



D-Link
Building Networks for People
Logged in as administrator
admin - 192.168.20.2
Home
Configuration
Tools
Status
Maintenance
Logout
Help
Objects
Address Book
InterfaceAddresses
ALG with AVWCF
Services
IP Pools
NAT Pools
Schedules
Authentication Objects
VPN Objects
HTTP Banner Files
Rules
IP Rules
lan_to_wan1
Access
Interfaces
Ethernet
VLAN
IPsec
GRE
PPPoE
PPTP/L2TP Servers
PPTP/L2TP Clients
SSL VPN Interface
Switch Management
Interface Groups
ARP/Neighbor Discovery
site_to_site_IPSEC
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.
General
Authentication
XAuth
Routing
IKE Settings
Keep-alive
Advanced
Authentication
X.509 Certificate
Root Certificate(s)
Available
HTTPSAdminCert
Selected
Gateway certificate:
(None)
Identification list:
(None)
Pre-shared Key
Pre-shared key:
ipsec_key
Selects the Pre-shared key to use with this IPsec Tunnel.
Local ID
Local ID Type:
Auto
Selects the type of Local ID to use.
Local ID Value:
Specify the local identity of the tunnel ID.

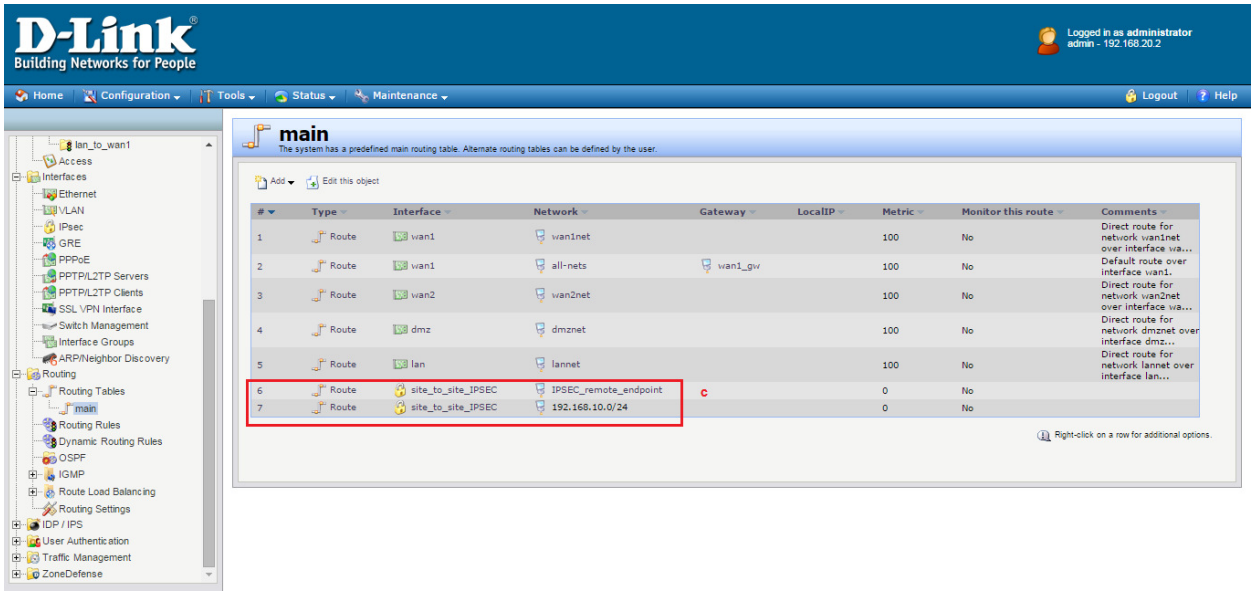

D-Link
Building Networks for People
Logged in as administrator
admin - 192.168.20.2
Home
Configuration
Tools
Status
Maintenance
Logout
Help
site_to_site_IPSEC
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.
General
Authentication
XAuth
Routing
IKE Settings
Keep-alive
Advanced
Routing
Allow DHCP over IPsec from single-host clients
Dynamically add route to the remote network when a tunnel is established
Dont check this checkbox
Packet Sizes
Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).
Plaintext MTU:
1420
IP Addresses
Automatically pick the address of a local interface that corresponds to the local net
Specify address manually:
IP Address:
(None)
OK
Cancel


D-Link
Building Networks for People
Logged in as administrator
admin - 192.168.20.2
Home
Configuration
Tools
Status
Maintenance
Logout
Help
site_to_site_IPSEC
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.
General
Authentication
XAuth
Routing
IKE Settings
Keep-alive
Advanced
Automatic Route Creation
Automatically add route for remote network.
Add route for remote network
don't check this checkbox
Route metric:
90
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.



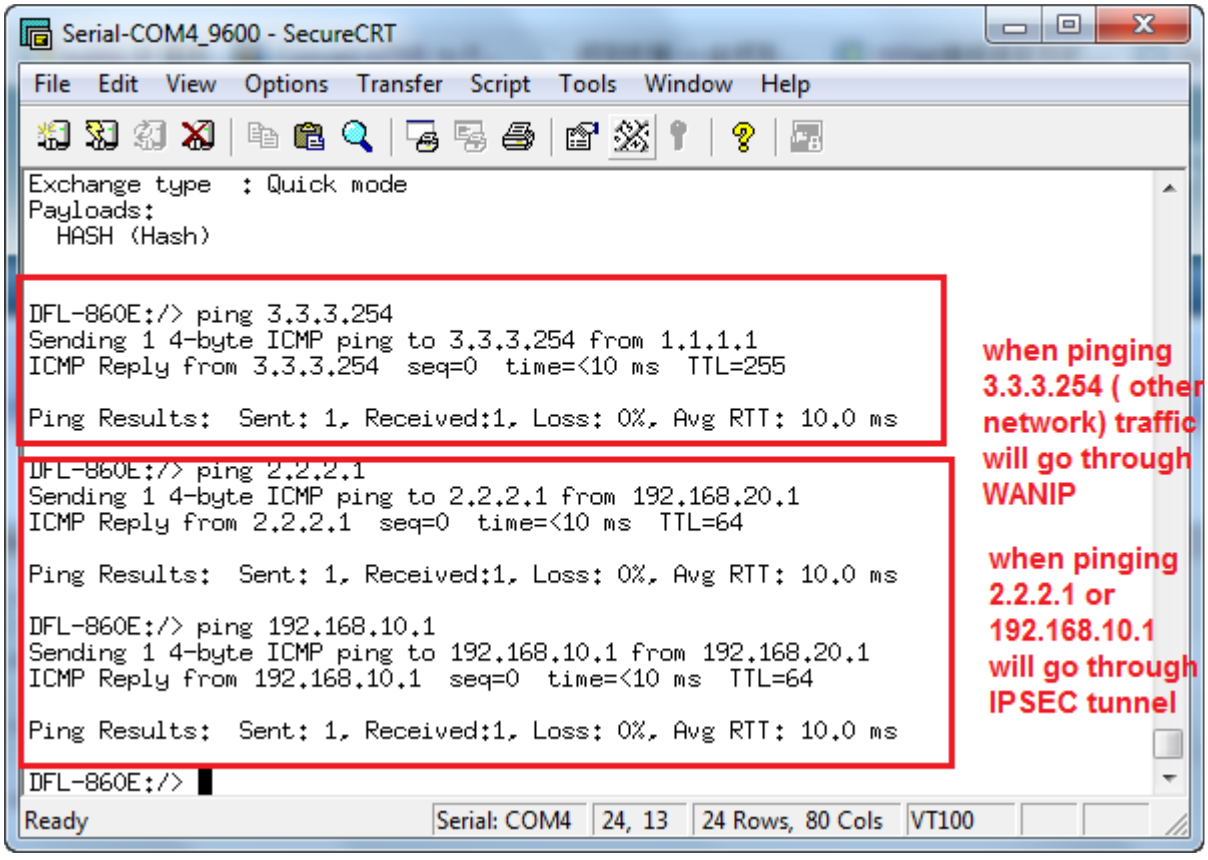
Step 5: Now we add the IP Rules which ALLOW the traffic from LAN LANNET to IPSEC interface IPSEC remote network/remote endpoint and the other side vice versa, why do we need two IP rules for this? This is because we want to allow the traffic which is from DSR's LAN network and also DSR's WAN IP.

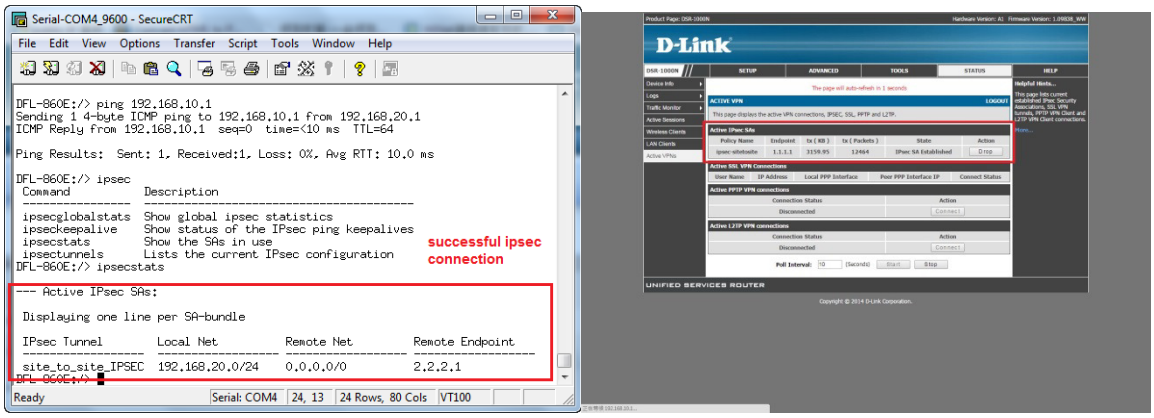


Step 6: Now we manually add the two routes which specifies that DSR's WANIP and DSR's LAN network goes through the IPSEC VPN interface.

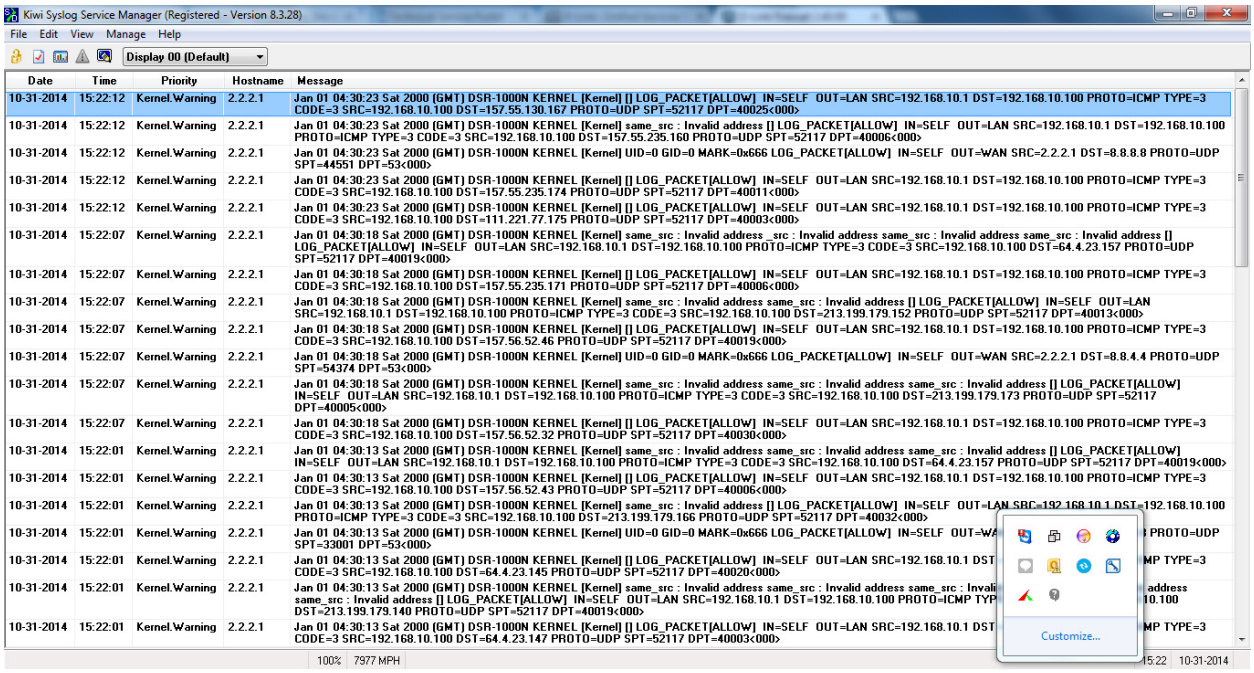
[Configuration on DGS-3620]
Set the three VLANs and their ports:
DGS-3620-52P:admin#create vlan vlanid 10
DGS-3620-52P:admin#create vlan vlanid 20
DGS-3620-52P:admin#create vlan vlanid 30
DGS-3620-52P:admin#config vlan vlanid 1 delete 1-52
DGS-3620-52P:admin#config vlan vlanid 10 add untagged 1-4
DGS-3620-52P:admin#config 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.





The IPSEC tunnel is successfully created.



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]