

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 serves 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]

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.09B38_WW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Wizard
Internet Settings > **WAN1 SETUP** LOGOUT
Wireless Settings >
Network Setting... >
DMZ Setup >
VLAN Settings >
Internal Users Data >
External Authentica >
VPN Settings >
USB Settings >
Captive Portal >

This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Address, Account Information etc. This information is usually provided by your ISP or network administrator.

Save Settings Don't Save Settings

ISP Connection Type

ISP Connection Type: Static IP

IP Address: 2.2.2.1

IP Subnet Mask: 255.255.255.0

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

MAC Address

MAC Address Source: Use Default Address

MAC Address: 00:00:00:00:00:00

UNIFIED SERVICES ROUTER

Copyright © 2014 D-Link Corporation.

Helpful Hints...
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.
More...

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
Internet Settings > **IPSEC CONFIGURATION** LOGOUT
Wireless Settings >
Network Setting... >
DMZ Setup >
VLAN Settings >
Internal Users Data >
External Authentica >
VPN Settings >
USB Settings >
Captive Portal >

This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.

Save Settings Don't Save Settings

General

Policy Name: ipsec-sitetosite

Policy Type: Auto Policy

IP Protocol Version: IPv4 IPv6

IKE Version: IKEv1 IKEv2

L2TP Mode: None

IPsec Mode: Tunnel Mode

Select Local Gateway: Dedicated WAN

Remote Endpoint: IP Address

1.1.1.1

Enable Mode Config:

Enable NetBIOS:

Enable RollOver:

Protocol: ESP

Enable DHCP:

Local IP: Any

Local Start IP Address:

Local End IP Address:

Local Subnet Mask:

Local Prefix Length:

Remote IP: Subnet

Remote Start IP Address: 192.168.20.0

Remote End IP Address:

Remote Subnet Mask: 255.255.255.0

Remote Prefix Length:

Helpful Hints...
Use Tunnel mode if you require communication to be secured between networks. Transport mode can be used if the requirement is to have secure communication between 2 hosts. Use Manual Policy parameters if you wish to specify the keys to be used for encryption/decryption (during communication). This is for advanced users who require more control over IPsec tunnel communication. For normal users, Auto Policy would do just fine. Enable Rollover only if the Port Mode is 'Auto-Rollover' in WAN MODE settings page. The active WAN will be used for setting up the tunnel, thus providing an uninterrupted VPN connection. Enable DHCP over IPsec checkbox to allow external users to form a VPN to DSR-1000N. Multiple users can connect as well.
More...

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
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)
SA Lifetime (sec): 28800

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: 1.09B3B_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

REMOTE LOGGING CONFIGURATION LOGOUT

This page allows user to configure the remote logging options for the router.
Save Settings Don't Save Settings

Log Options
Remote Log Identifier: DSR-1000N

Enable E-Mail Logs
Enable E-Mail Logs:
E-Mail Server Address:
SMTP Port: 25
Return E-Mail Address:
Send to E-Mail Address(1):
Send to E-Mail Address(2): (Optional)
Send to E-Mail Address(3): (Optional)
Authentication with SMTP Server: None
User Name:
Password:
Respond to Identd from SMTP Server:

Send E-mail logs by Schedule
Unit: Never
Day: Sunday
Time: 1:00 (AM) (PM)

SYS LOG SERVER CONFIGURATION

	Name	SysLog Facility	SysLog Severity
<input checked="" type="checkbox"/>	SysLog Server1: 192.168.20.2	All	All
<input type="checkbox"/>	SysLog Server2:	All	All
<input type="checkbox"/>	SysLog Server3:	All	All
<input type="checkbox"/>	SysLog Server4:	All	All
<input type="checkbox"/>	SysLog Server5:	All	All
<input type="checkbox"/>	SysLog Server6:	All	All
<input type="checkbox"/>	SysLog Server7:	All	All
<input type="checkbox"/>	SysLog Server8:	All	All

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: Kernel Display

Display and Send Logs

	Display in Event Log	Send to Syslog
Emergency:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Alert:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Critical:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Error:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Warning:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Notification:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Information:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Debugging:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

UNIFIED SERVICES ROUTER

Copyright © 2014 D-Link Corporation.

Helpful Hints...
In order to configure a logging facility, first select the facility and then press 'Display' button.
More...

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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Alert:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Critical:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Error:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Warning:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Notification:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Information:	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Debugging:	<input type="checkbox"/>	<input checked="" type="checkbox"/>

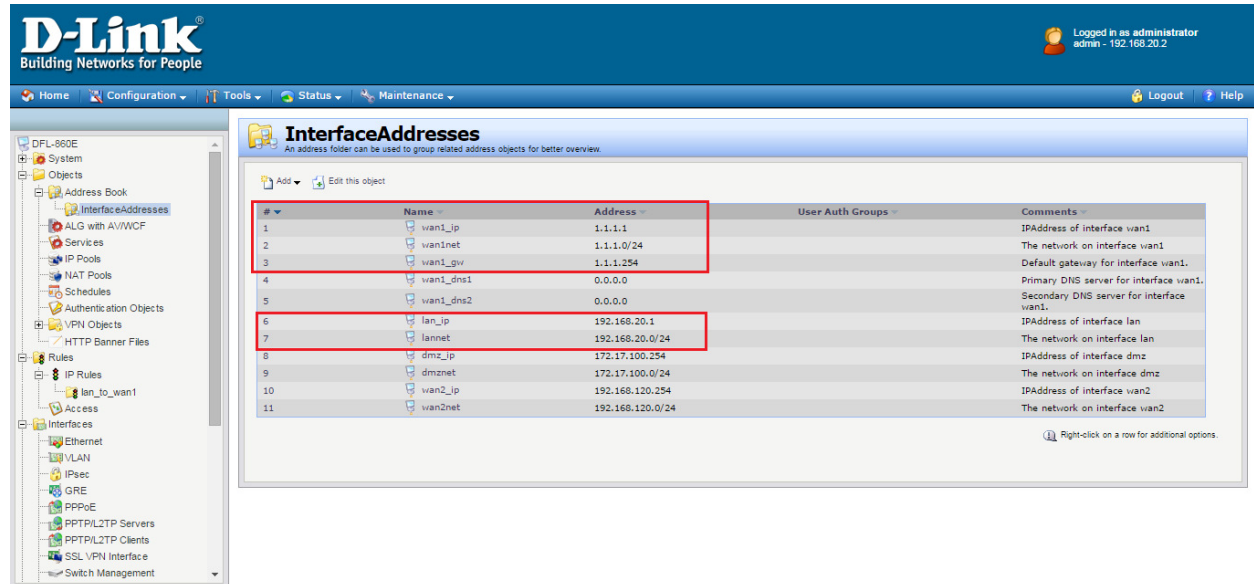
UNIFIED SERVICES ROUTER

Copyright © 2014 D-Link Corporation.

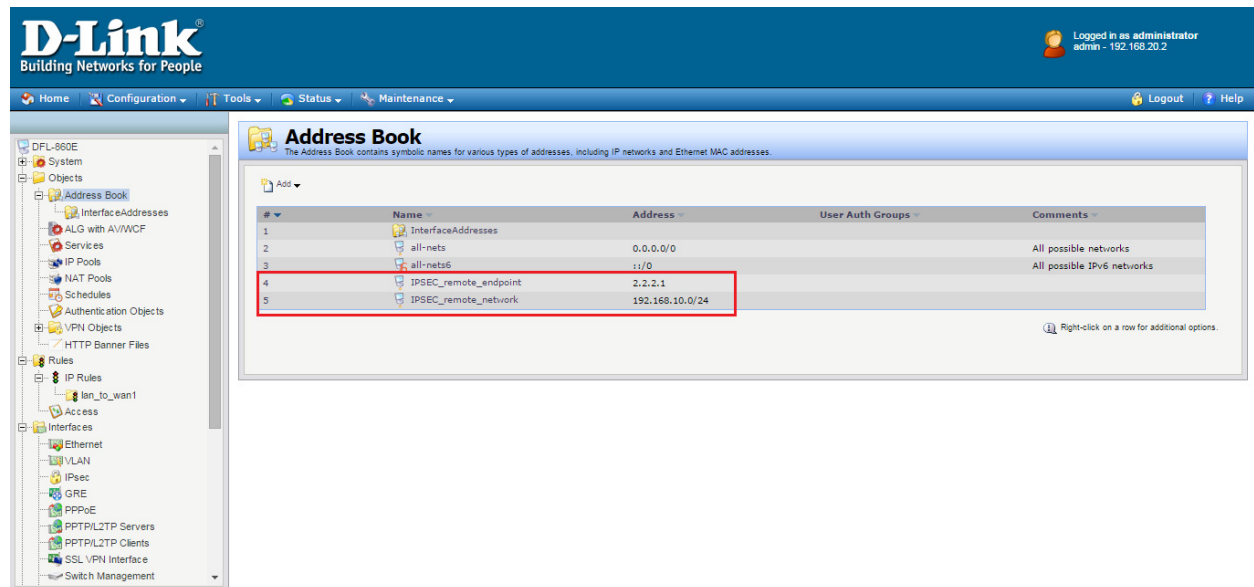
Helpful Hints...
In order to configure a logging facility, first select the facility and then press 'Display' button.
More...

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.

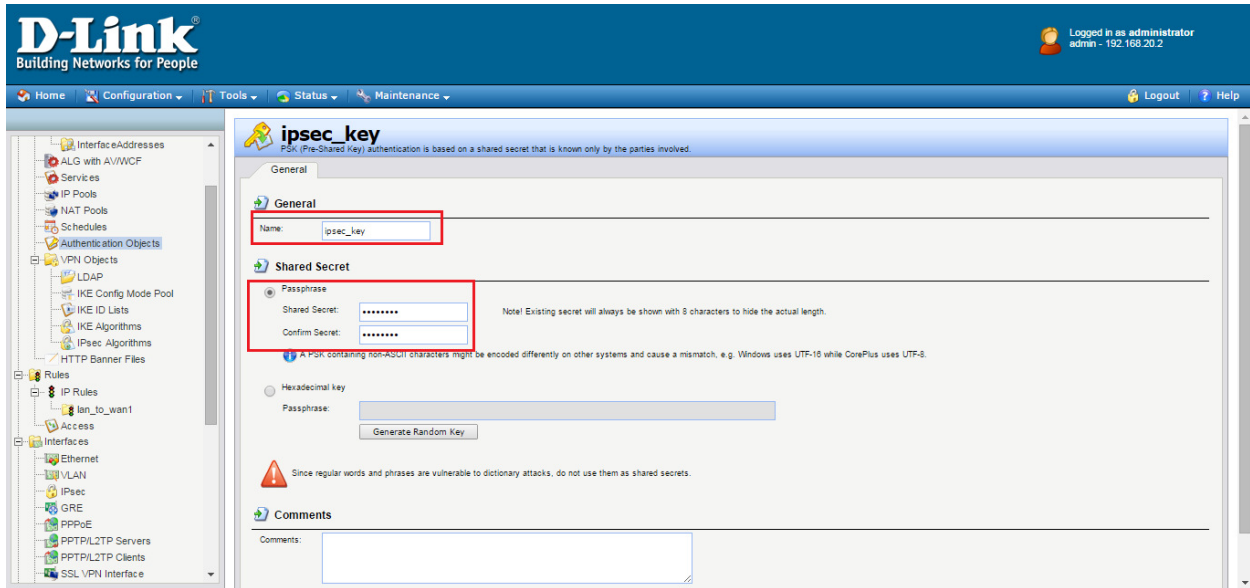
[DFL-860E]



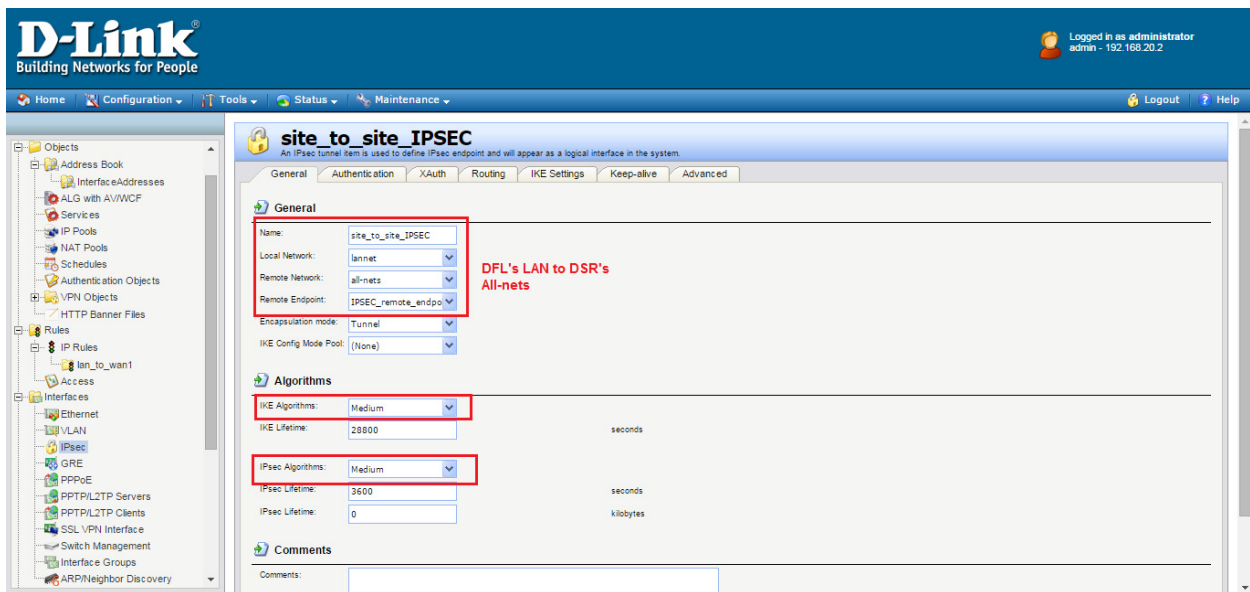
Step 1: DFL-860E's configuration is much more complicated than DSR-1000N, let's start on creating the objects for IP addresses, we change the WAN IP to 1.1.1.1, gateway to 1.1.1.254, wan-net to 1.1.1.0/24, lan IP to 192.168.20.1/24 for this scenario.



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

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

Local ID Value:

Selects the type of Local ID to use.
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

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

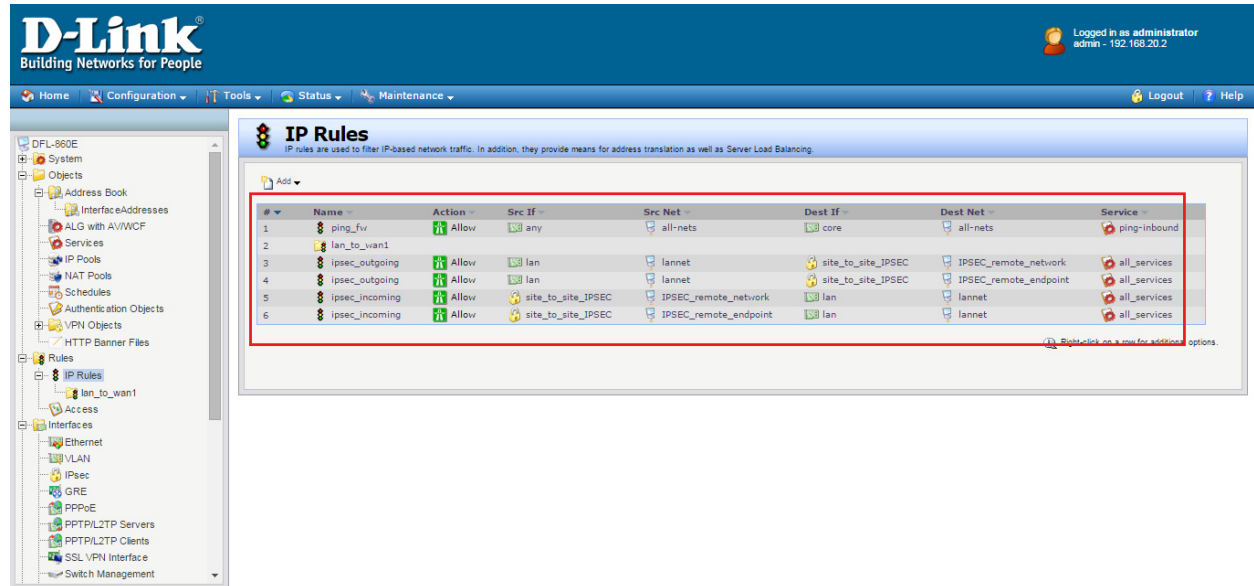
Automatically add route for remote network:

Add route for remote network

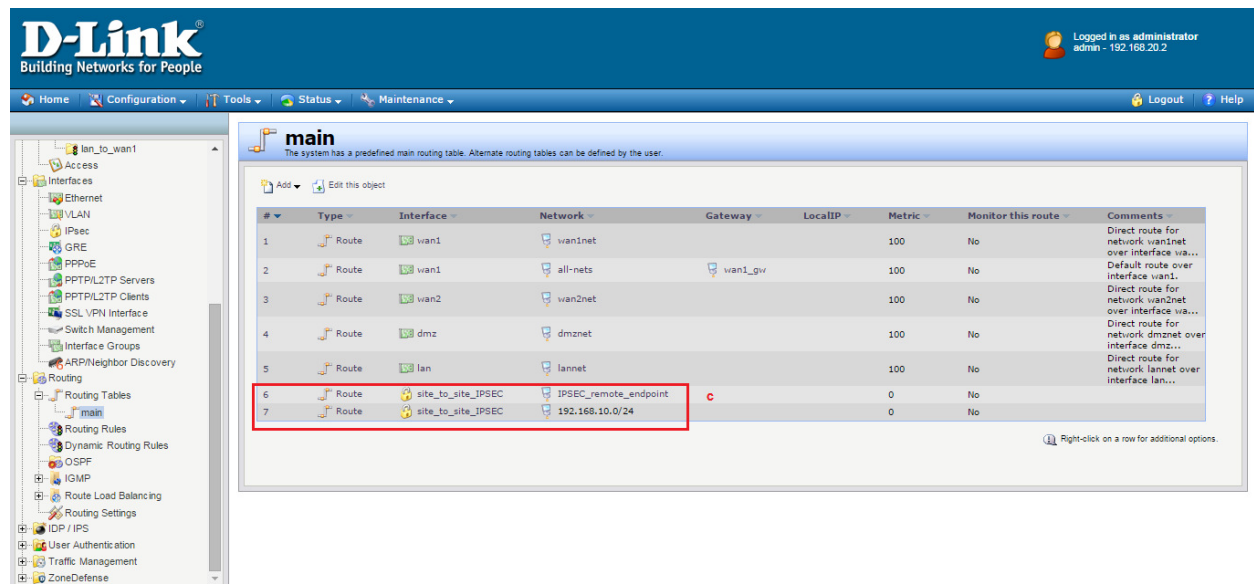
Route metric: 90

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 ping 2.2.2.1 and 192.168.10.1/24 should go through IPSEC tunnel.

```
Serial-COM4_9600 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Exchange type : Quick mode
Payloads:
HASH (Hash)

DFL-860E:/> ping 3.3.3.254
Sending 1 4-byte ICMP ping to 3.3.3.254 from 1.1.1.1
ICMP Reply from 3.3.3.254 seq=0 time=<10 ms TTL=255
Ping Results: Sent: 1, Received:1, Loss: 0%, Avg RTT: 10.0 ms

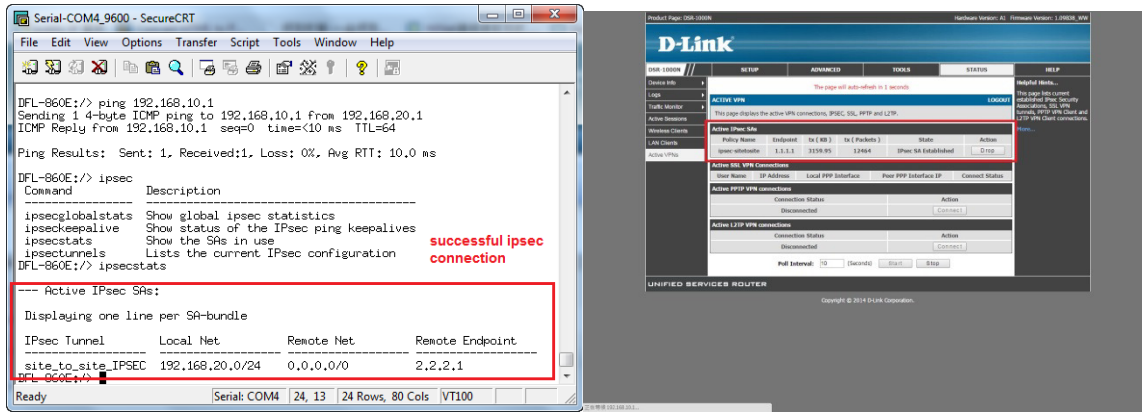
DFL-860E:/> ping 2.2.2.1
Sending 1 4-byte ICMP ping to 2.2.2.1 from 192.168.20.1
ICMP Reply from 2.2.2.1 seq=0 time=<10 ms TTL=64
Ping Results: Sent: 1, Received:1, Loss: 0%, Avg RTT: 10.0 ms

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
Ping Results: Sent: 1, Received:1, Loss: 0%, Avg RTT: 10.0 ms

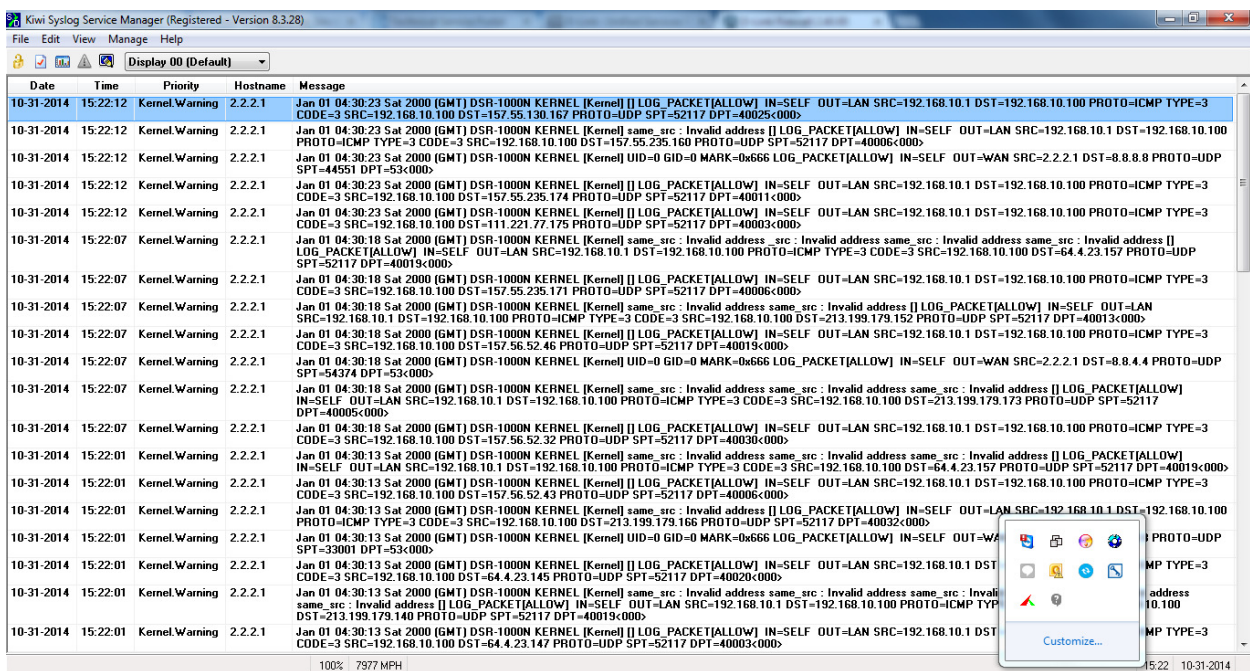
DFL-860E:/>
Ready Serial: COM4 24, 13 24 Rows, 80 Cols VT100
```

when ping 3.3.3.254 (other network) traffic will go through WANIP

when ping 2.2.2.1 or 192.168.10.1 will 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]