

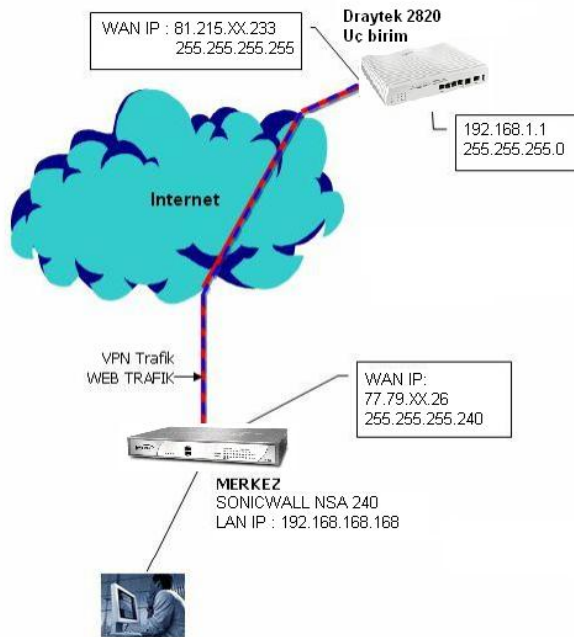
TechNote

VPN

How to Route All Traffic through a SonicWALL with Draytek

SCENARIO:

To make a VPN implementation from point to point among the two different locations, and to have the Internet traffic of the Draytek equipment by directing the Internet to Sonicwall I UTM equipment from on VPN.



Settings of Draytek 2820 (Branch)

Follow the below steps by connecting the interface of the Draytek modem...

VPN and Remote Access > LAN to LAN Choose a profile here and give a name to this profile.

The screenshot shows the web interface of a Draytek Vigor 2820 Series ADSL2/3+ Security Firewall. The left sidebar contains a navigation menu with the following items:

- Quick Start Wizard
- Online Status
- WAN
- LAN
- NAT
- Firewall
- Objects Setting
- CSM
- Bandwidth Management
- Applications
- VPN and Remote Access
 - Remote Access Control
 - PPP General Setup
 - IPSec General Setup
 - IPSec Peer Identity
 - Remote Dial-In User
 - LAN to LAN** (highlighted with a red box)
 - Connection Management
- Certificate Management
- USB Application

The main content area displays the "VPN and Remote Access >> LAN to LAN" configuration page. It includes a table of LAN-to-LAN Profiles:

Index	Name	Status
1.	sonicwall	X
2.	???	X
3.	???	X
4.	???	X
5.	???	X
6.	???	X
7.	???	X
8.	???	X
9.	???	X
10.	???	X
11.	???	X
12.	???	X

Tech Note

Enter the inside of Profile after giving the name of the Tunnel as Sonicwall. You should pay attention to all red places. The tunnel will be applied as Dial Out on IPsec and the Remote Public IP will be shown as Server IP.

- Active the profile.
- Profile Name : sonicwall
- Call Direction : Choose Dial Out and sign Always On
- Arrange the Dial Out Settings as IPsec Tunnel
- Remote Public IP : Enter the Center SonicWALL IP address.(77.79.XX.26)
- Pre-Shared Key : sonic2009dry
- IPsec Security Method : 3Des

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: <input type="text" value="sonicwall"/>	Call Direction: <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input checked="" type="checkbox"/> Always on
VPN Dial-Out Through: <input type="text" value="WAN1 Only"/>	Idle Timeout: <input type="text" value="-1"/> second(s)
Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input checked="" type="checkbox"/> Enable PING to keep alive
	PING to the IP: <input type="text" value="192.168.168.168"/>

2. Dial-Out Settings

Type of Server I am calling

PPTP
 IPsec Tunnel
 L2TP with IPsec Policy

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username:
Password:
PPP Authentication:
VJ Compression: On Off

IKE Authentication Method

Pre-Shared Key

 Digital Signature(X.509)

IPsec Security Method

Medium(A+)
 High(ESP)

Index(1-15) in [Schedule](#) Setup:
 , , ,

Make the setups for Phase 1 and Phase 2 from part of Advanced .

- IKE Phase 1: Main Mode
- IKE Phase 1 proposal: 3DES_MD5_G1
- IKE Phase 2 proposal: 3DES_MD5
- IKE Phase1 ve 2 key: 28800
- Forward Secret: Enable

IKE advanced settings

IKE phase 1 mode: <input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode
IKE phase 1 proposal: <input type="text" value="3DES_MD5_G1"/>
IKE phase 2 proposal: <input type="text" value="3DES_MD5"/>
IKE phase 1 key lifetime: <input type="text" value="28800"/> (900 ~ 86400)
IKE phase 2 key lifetime: <input type="text" value="28800"/> (600 ~ 86400)
Perfect Forward Secret: <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Local ID: <input type="text"/>

OK Close

Tech Note

Don't touch the Dial-In Settings. This is the most important place for us 4 part TCP/IP Network Settings; All of the sections can stay as 0.0.0.0. or if you want you can sign current informations too...

3. Dial-In Settings

Allowed Dial-In Type

- PPTP
- IPSec Tunnel
- L2TP with IPSec Policy Nice to Have

Specify Remote VPN Gateway

Peer VPN Server IP:

ur Peer ID:

Username:

Password:

VJ Compression: On Off

IKE Authentication Method

- Pre-Shared Key
- Digital Signature(X.509)

IKE Pre-Shared Key:

None

IPSec Security Method

- Medium(AH)
- High(ESP) DES 3DES AES

4. TCP/IP Network Settings

My WAN IP:

Remote Gateway IP:

Remote Network IP:

Remote Network Mask:

More

RIP Direction:

From first subnet to remote network, you have to do:

- Change default route to this VPN tunnel (Only single WAN supports this)

OK Clear Cancel

Draytek Users:Dont forget the sign the most important place to use the Center Sonicwall Internet.

- Change default route to this VPN Tunnel (Only single WAN support this)**
- The setups are finished for Draytek. Press OK button to active profile.

SonicWALL Settings (Center)

We active it by giving a name from VPN > Settings part..To open a new Vpn tunnel you make an entrance by pressing add button below..

VPN /

Settings

VPN Global Settings

- Enable VPN

Unique Firewall Identifier:

Give a name in **Vpn > General** part for VPN tunnel, state the Public IP and Shared Scret of opposite side..

Tech Note

Policy Type: Site to Site
Authentication Method: IKE Using Preshared Secret
Name: Draytek
IPsec Primary Gateway: 81.215.XX.233
IPsec Secondary Gateway: 0.0.0.0
Shared Secret: sonic2009dry

General	Network	Proposals	Advanced
Security Policy			
Policy Type:	Site to Site		
Authentication Method:	IKE using Preshared Secret		
Name:	Draytek		
IPsec Primary Gateway Name or Address:	81.215.XX.233		
IPsec Secondary Gateway Name or Address:	0.0.0.0		
IKE Authentication			
Shared Secret:	sonic2009dry		
Confirm Shared Secret:	sonic2009dry		<input type="checkbox"/> Mask Shared Secret
Local IKE ID:	IP Address		
Peer IKE ID:	IP Address		

Tech Note

State the title of Local Networks as Any Address in **Vpn > Network** part and create a Draytek Local Network and state it in title of Remote Networks.

Local Networks

- Choose local network from list
- Local network obtains IP addresses using DHCP through this VPN Tunnel
- Any address

Remote Networks

- Use this VPN Tunnel as default route for all Internet traffic
- Destination network obtains IP addresses using DHCP through this VPN Tunnel
- Choose destination network from list

To create a Draytek Network: enter the Network > Address Objects menu and define it as in Picture.

Name:	Draytek_VPN
Zone Assignment:	VPN
Type:	Network
Network:	192.168.1.0
Netmask:	255.255.255.0

Create the **Vpn > Proposals** part as in below. This part must be same with the opposite side's setups.

IKE (Phase 1) Proposal

Exchange:	Main Mode
DH Group:	Group 1
Encryption:	3DES
Authentication:	MD5
Life Time (seconds):	28800

Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	3DES
Authentication:	MD5
<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy	
DH Group:	Group 1
Life Time (seconds):	28800

Tech Note

Create the Vpn > Advanced part as in below...

The screenshot shows the 'Advanced' tab of a VPN Policy configuration. The 'Advanced Settings' section includes several checkboxes: 'Enable Keep Alive' (checked), 'Suppress automatic Access Rules creation for VPN Policy', 'Require authentication of VPN clients by XAUTH', 'Enable Windows Networking (NetBIOS) Broadcast', 'Enable Multicast', and 'Apply NAT Policies'. Below these are options for 'Management via this SA' (HTTP, HTTPS, SSH) and 'User login via this SA' (HTTP, HTTPS). The 'Default LAN Gateway (optional)' is set to '0.0.0.0' and the 'VPN Policy bound to' is set to 'Zone WAN'.

Approve the profile by pressing OK button after making these setups. You will see VPN tunnel will connect as in below.

The screenshot shows a table of VPN Policies. The table has columns for '#', 'Name', 'Gateway', 'Destinations', 'Crypto Suite', 'Enable', and 'Configure'. There are three rows of policies listed.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
3	Draytek	81.215. .233	192.168.1.0 - 192.168.1.255	ESP: 3DES/HMAC MD5 (IKE)	<input checked="" type="checkbox"/>	

Let's create the rule of NAT to direct the internet traffic of Users which come from Draytek to SonicWALL.

The screenshot shows the 'Advanced' tab of a NAT Policy configuration. The 'NAT Policy Settings' section includes dropdown menus for 'Original Source' (Draytek_VPN), 'Translated Source' (X1 IP), 'Original Destination' (Any), 'Translated Destination' (Original), 'Original Service' (Any), and 'Translated Service' (Original). It also includes dropdown menus for 'Inbound Interface' (Any) and 'Outbound Interface' (X1), and a text field for 'Comment'. The 'Enable NAT Policy' checkbox is checked.

Tech Note

Original Source: Draytek-VPN
Translated Source: X1 IP
Original Destination: Any
Translated Destination: Original
Original Service: Any
Translated Service: Original
Inbound Interface: Any
Outbound Interface: X1

When you make tracert to check the Internet Output,you will see it will connect from on Gateway.

```
C:\WINDOWS\system32\cmd.exe
C:\>
C:\>tracert www.google.com

En fazla 30 atlamanın üstünde
www.1.google.com [209.85.129.104]'ye izleme yolu :

 1  <1 ms    <1 ms    <1 ms    my.router [192.168.1.1]
 2  20 ms    17 ms    18 ms    reverse-77-79-1.grid.com.tr [77.79.1.1]
 3  15 ms    16 ms    16 ms    212.175.18.85
 4  24 ms    14 ms    15 ms    gayrettepe_t3_1-besiktas_t3_1.turktelekom.com.tr
[212.156.118.153]
^C
C:\>_
```

Document Last Updated: October 2009