



Quick Note

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router.

Digi Technical Support

8 June 2017

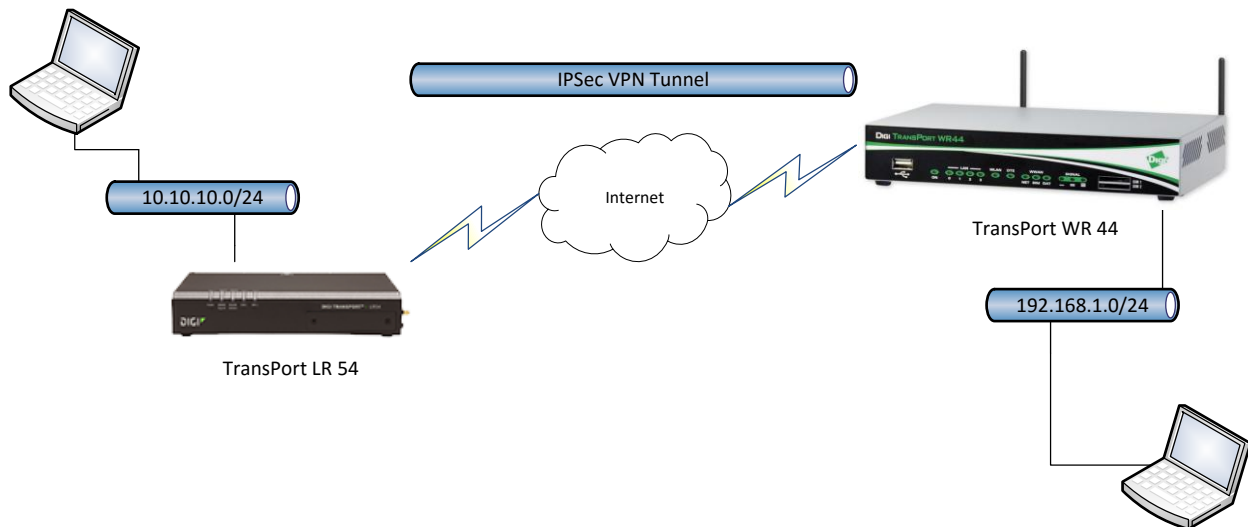
Contents

1	Introduction.....	3
1.1	Outline	3
1.2	Assumptions	3
1.3	Corrections	4
2	Version	4
3	TransPort WR44 Configuration (Responder)	5
3.1	Local Ethernet Interface configuration	5
3.2	WAN interface configuration	6
3.3	Tunnel Configuration	7
3.3.1	Phase 1 Settings.....	7
3.3.2	Phase 2 settings	8
3.3.3	Preshared key settings	10
3.4	Save configuration.....	11
4	TransPort LR54 Configuration	12
4.1	Configure a local interface	12
4.2	Configure Phase 1 settings	12
4.3	Configure Phase 2 settings	13
4.3.1	Authentication and encryption settings	13
4.3.2	Local and Remote traffic selector settings.....	14
4.4	Configure Peer address	15
4.5	Turn IPSec on.....	15
4.6	Configure the Firewall	16
4.6.1	Firewall rules needed for MAIN mode VPN.....	16
4.6.2	Firewall rules needed for RESPONDER configuration	16
4.7	Save Configuration	16
5	Check Tunnel Status	17
5.1	TransPort WR44	17
5.2	TransPort LR54	18
6	Testing.....	19
6.1	TransPort WR44	19
6.2	TransPort LR54	19

1 INTRODUCTION

1.1 Outline

This document will describe how to configure an IPSec VPN tunnel between a TransPort LR54 as the INITIATOR and a TransPort WR router as the RESPONDER. The document will assume that WAN connectivity is configured and available on both units.



1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router and configure it with basic routing functions

This application note applies to:

Model: Digi TransPort LR54 and Digi TransPort WR44

Firmware versions:

LR54: 1.1.0.6 and later

WR44: 2.17.10 and later

Configuration: This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

Please note: This application note has been specifically rewritten for the specified firmware versions and later but will work on earlier versions of firmware. Please contact tech.support@digi.com if you require assistance in upgrading the firmware of the TransPort LR or TransPort WR routers.

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: tech.support@digi.com Requests for new application notes can be sent to the same address.

2 VERSION

Version Number	Status
1.0	published
1.1	Added notes and firewall rules for MAIN mode and RESPONDER

3 TRANSPORT WR44 CONFIGURATION (RESPONDER)

3.1 Local Ethernet Interface configuration

Navigate to:

Configuration – Network > Interfaces > Ethernet > ETH 0

[Configuration – Network > Interfaces > Ethernet > ETH 0](#)

▼ **Interfaces**

▼ **Ethernet**

▼ **ETH 0**

Description:

Get an IP address automatically using DHCP
 Use the following settings

IP Address:

Mask:

Gateway:

DNS Server:

Secondary DNS Server:

Changes to these parameters may affect your browser connection

[▶ Advanced](#)
[▶ QoS](#)
[▶ VRRP](#)

Parameter	Setting	Description
Use the following settings	Checked	A static IP Address will be used in this example
IP Address	192.168.1.44	IP Address of the TransPort WR44 Ethernet Interface. In this example, this IP Address is in the subnet range used for the Tunnel (useful for testing)
Mask	255.255.255.0	Subnet mask

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

3.2 WAN interface configuration

In this example, the mobile interface will be used as the WAN interface on which the IPsec tunnel will be established.

Navigate to:

Configuration – Network > Interfaces > Mobile

[Configuration - Network > Interfaces > Mobile](#)

Mobile

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP 1) ▼

IMSI: Unknown

Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

Service Plan / APN: your.apn.goes.here

Use backup APN [] Retry the main APN after 0 minutes

SIM PIN: [] (Optional)

Confirm SIM PIN: []

Username: [] (Optional)

Password: [] (Optional)

Confirm Password: []

Mobile Connection Settings

Re-establish connection when no data is received for a period of time

Mobile Network Settings

Enable NAT on this interface

IP address IP address and Port

Enable IPsec on this interface

Keep Security Associations (SAs) when this Mobile interface is disconnected

Use interface Default [] for the source IP address of IPsec packets

Enable the firewall on this interface

Parameter	Setting	Description
Service Plan / APN	Your.APN.goes.here	Enter the APN of your mobile provider
Enable IPsec on this interface	Checked	Enable IPsec to be built on this WAN interface

Please note: If required, enter a SIM PIN and Username/Password for this SIM card and APN.

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

3.3 Tunnel Configuration

Open a web browser to the IP address of the TransPort WR44 router.

3.3.1 Phase 1 Settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IKE > IKE 0

[Configuration - Network > Virtual Private Networking \(VPN\) > IPsec > IKE > IKE 0](#)

Use the following settings for negotiation

Encryption: None DES 3DES AES (128 bit) AES (192 bit) AES (256 bit)

Authentication: None MD5 SHA1 SHA256

Mode: Main Aggressive

MODP Group for Phase 1: 14 (2048) ▼

MODP Group for Phase 2: No PFS ▼

Renegotiate after 8 hrs 0 mins 0 secs

[Advanced](#)

Parameter	Setting	Description
Encryption	AES (256 bit)	Encryption algorithm used in this tunnel
Authentication	SHA1	Authentication algorithm used in this tunnel
Mode	Aggressive	IKE Mode used in this tunnel
MODP Group for Phase 1	14 (2048)	Key length used in the IKE Diffie-Hellman exchange
MODP Group for Phase 2	No PFS	Key length used in the ESP Diffie-Hellman exchange

Configure an IPsec VPN tunnel between a TransPort LR router and a TransPort WR router

3.3.2 Phase 2 settings

Navigate to:

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec 0 – 9 > IPsec 0

[Configuration - Network > Virtual Private Networking \(VPN\) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0](#)

▼ IPsec

▼ IPsec Tunnels

▼ IPsec 0 - 9

▼ IPsec 0

Description:

The IP address or hostname of the remote unit

Use as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text" value="192.168.1.0"/>	IP Address: <input type="text" value="10.10.10.0"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

Off Preshared Keys XAUTH Init Preshared Keys RSA Signatures XAUTH Init RSA

Our ID:

Our ID type IKE ID FQDN User FQDN IPv4 Address

Remote ID:

Use encryption on this tunnel

Use authentication on this tunnel

Use Diffie Hellman group

Use IKE to negotiate this tunnel

Use IKE configuration:

Bring this tunnel up

All the time

Whenever a route to the destination is available

On demand

If the tunnel is down and a packet is ready to be sent

Bring this tunnel down if it is idle for hrs mins secs

Renew the tunnel after

hrs mins secs

KBytes of traffic

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

Parameter	Setting	Description
Local LAN settings		
Use these settings for the local LAN	Checked	Local LAN subnet
IP Address	192.168.1.0	Local LAN subnet IP Address
Mask	255.255.255.0	Local LAN subnet mask
Remote LAN settings		
Use these settings for the local LAN	Checked	Remote LAN subnet
IP Address	10.10.10.0	Remote LAN subnet IP Address
Mask	255.255.255.0	Remote LAN subnet mask
Tunnel Security		
Preshared Keys	Checked	Use preshared keys for authentication on this tunnel
Our ID	wr44	The ID of the VPN responder router (this router)
Remote ID	lr54	The ID of the VPN initiator router (remote router)
Our ID type	FQDN	Use Fully Qualified Domain Name type ID
Use () encryption on this tunnel	AES (256 bit keys)	The IPsec encryption algorithm to use is AES
Use () authentication on this tunnel	SHA1	The IPsec ESP authentication to use is SHA1
Tunnel creation		
Bring this tunnel up	On demand	
If the tunnel is down and a packet is ready to be sent	Bring the tunnel up	

Click **Apply**

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

3.3.3 Preshared key settings

The pre-shared key is enabled by creating a username with the name of the remote peer (Remote ID from the Phase 2 settings) and the password is the preshared key.

Navigate to:

Configuration – Security > Users > Users 0 - 9 > User 9

Configuration - Security > Users > User 0 - 9 > User 9

System

Users

User 0 - 9

User 0

User 1 - username

User 2

User 3

User 4

User 5

User 6

User 7

User 8

User 9 - lr54

Username: lr54

Password: ●●●●●●

Confirm Password:

Access Level: None

Advanced

Apply

Parameter	Setting	Description
Username	lr54	Name should match the Remote ID value from Phase 2 settings
Password	digitestvpn123	Enter the password which will be used as the preshared key. This has to match the value on the Remote router.
Confirm password	digitestvpn123	Re-enter the password
Access Level	None	This user will not be granted any admin access as it is only used as a preshared key.

Click **Apply**

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

3.4 Save configuration

Navigate to:

Administration – Save Configuration

Administration – Save configuration

Save current configuration to Config

Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all registers on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

Click **Save**. The configuration will now be saved to the unit.

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

4 TRANSPORT LR54 CONFIGURATION

Please Note: At the time of this document, the configuration of the TransPort LR54 is exclusively done via CLI (Command Line Interface)

4.1 Configure a local interface

In this example, we will use the 10.10.10.0/24 subnet on LAN 1. To configure this:

```
lan 1 ip-address 10.10.10.1  
lan 1 mask 255.255.255.0
```

All **IKE** and **IPSec** configuration is done within the **ipsec** command.

The following command will show all available options:

```
ipsec 1 ?
```

4.2 Configure Phase 1 settings

Configure the IKE Phase 1 settings to match the settings of the Connect WAN Router.

- IKE version 1
- SHA 1
- Group 14
- AES 256
- 4800 lifetime
- AGGRESSIVE mode

Enter the parameters as follow:

```
digi.router> ipsec 1 ike 1  
digi.router> ipsec 1 ike-authentication sha1  
digi.router> ipsec 1 ike-diffie-hellman group14  
digi.router> ipsec 1 ike-encryption aes256  
digi.router> ipsec 1 ike-lifetime 4800  
digi.router> ipsec 1 ike-mode aggressive
```

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

Type the following to verify the IKE Phase 1 settings:

```
ipsec 1 ik?  
digi.router> ipsec 1 ik?  
  
Configures an IPsec tunnel  
  
Syntax:  
ipsec 1 <parameter> <value>  
  
Available Parameters:  
Parameter          Current Value      Description  
-----  
ike                 1                 IKE version to use for this IPsec tunnel  
ike-authentication sha1              IKE authentication type for IPsec tunnel  
ike-diffie-hellman group14          IKE Diffie-Hellman group for IPsec  
ike-encryption     aes256            IKE encryption type  
ike-lifetime       4800              Key lifetime in seconds  
ike-mode           aggressive        IKEv1 mode to use for this IPsec tunnel  
ike-tries          3                 Number of attempts to negotiate
```

4.3 Configure Phase 2 settings

4.3.1 Authentication and encryption settings

Configure the Phase 2 authentication and encryption settings to match the settings of the Connect WAN Router.

- Pre-shared key
- SHA 1
- Group 14
- AES 256
- 3600 lifetime
- psk

Enter the parameters as follow:

```
digi.router> ipsec 1 auth-by psk  
digi.router> ipsec 1 esp-authentication sha1  
digi.router> ipsec 1 esp-diffie-hellman group14  
digi.router> ipsec 1 esp-encryption aes256  
digi.router> ipsec 1 lifetime 3600  
digi.router> ipsec 1 psk digitestvpn123
```

Configure an IPsec VPN tunnel between a TransPort LR router and a TransPort WR router

Type the following to verify the Phase 2 authentication and encryption settings:

```
digi.router> ipsec 1 es?
```

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:

Parameter	Current Value	Description
esp-authentication	sha1	ESP authentication type for IPsec tunnel
esp-diffie-hellman	group5	ESP Diffie-Hellman group for IPsec
esp-encryption	aes128	ESP encryption type for IPsec tunnel

4.3.2 Local and Remote traffic selector settings

Configure the Phase 2 local and remote traffic selector settings to match the settings of the Connect WAN Router.

- Local ID
- Remote ID
- Local network : 10.10.10.0
- Local mask : 255.255.255.0
- Remote network: 192.168.1.0
- Remote mask : 255.255.255.0

Enter the parameters as follow:

```
digi.router> ipsec 1 local-id lr54
digi.router> ipsec 1 remote-id wr44
digi.router> ipsec 1 local-mask 255.255.255.0
digi.router> ipsec 1 local-network 10.10.10.0
digi.router> ipsec 1 remote-mask 255.255.255.0
digi.router> ipsec 1 remote-network 192.168.1.0
```

Configure an IPsec VPN tunnel between a TransPort LR router and a TransPort WR router

Type the following to verify the Phase 2 local and remote traffic selector settings:

```
digi.router> ipsec 1 loc?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
Parameter          Current Value      Description
-----
local-id           lr54               Local ID used for this IPsec tunnel
local-mask         255.255.255.0     Local network mask for this IPsec tunnel
local-network      10.10.10.0        Local network for this IPsec tunnel

digi.router> ipsec 1 rem?

Configures an IPsec tunnel

Syntax:
ipsec 1 <parameter> <value>

Available Parameters:
Parameter          Current Value      Description
-----
remote-id          wr44               Remote ID used for this IPsec tunnel
remote-mask        255.255.255.0     Remote network mask for this tunnel
remote-network     192.168.1.0       Remote network for this IPsec tunnel
```

4.4 Configure Peer address

To configure the Peer address, in this example, the IP address of the Mobile interface of the Connect WAN router do the following:

```
digi.router> ipsec 1 peer x.x.x.x
```

x.x.x.x being an IP address reachable via the WAN interface of the LR54.

4.5 Turn IPsec on

To enable the configured IPsec VPN tunnel, do the following:

```
digi.router> ipsec 1 state on
```

The configuration is complete and the tunnel should now be built.

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

4.6 Configure the Firewall

Please note: By default, no traffic will be allowed inside the tunnel. It is necessary to add the following firewall rule to bypass the MASQUERADE (NAT) rules in place:

```
firewall -t nat -I POSTROUTING 1 -s 10.10.0.0/16 -d 192.168.1.0/24 -j ACCEPT
```

4.6.1 Firewall rules needed for MAIN mode VPN.

The example used in this document uses an Aggressive mode VPN. If a MAIN mode VPN is used, the following rule will be required to allow ESP packets inbound:

```
firewall -A INPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

4.6.2 Firewall rules needed for RESPONDER configuration

The example used in this document uses the LR 54 as the INITIATOR.

If the LR 54 is used as the RESPONDER, the following rules will be required to allow inbound VPN connections:

```
firewall -A INPUT -p udp -m multiport --dports 500,4500 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
firewall -A OUTPUT -p udp -m multiport --dports 500,4500 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
firewall -A INPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

```
firewall -A OUTPUT -p 50 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

4.7 Save Configuration

To save configuration, do the following:

```
digi.router> save config
```


Configure an IPsec VPN tunnel between a TransPort LR router and a TransPort WR router

5 CHECK TUNNEL STATUS

5.1 TransPort WR44

Navigate to

Management – Event Log

The following line should show that the tunnel was built successfully:

```
11:05:56, 22 Feb 2017, (287) IKE SA Removed. Peer: lr54, Successful Negotiation
11:05:53, 22 Feb 2017, Eroute 0 VPN up peer: lr54
11:05:53, 22 Feb 2017, New IPsec SA created by lr54
11:05:53, 22 Feb 2017, (287) New Phase 2 IKE Session 80.12.43.69, Responder
11:05:52, 22 Feb 2017, (286) IKE Keys Negotiated. Peer: lr54
11:05:52, 22 Feb 2017, (286) New Phase 1 IKE Session 80.12.43.69, Responder
```

Navigate to

Management – Virtual Private Networking (VPN) > IPsec > IPsec Tunnels 0 – 9 > IPsec Tunnels 0 – 9

[Management – Connections > Virtual Private Networking \(VPN\) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9](#)

The screenshot displays the configuration page for IPsec Tunnels. The navigation path is: Management – Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9. The page shows a tree view with 'IPsec Tunnels 0 - 9' expanded. Below this, there are sections for 'Outbound V1 SAs' and 'Inbound V1 SAs'. Each section contains a table with one entry for tunnel 0. The 'Outbound V1 SAs' table has columns: #, Peer IP Addr, Local Network, Remote Network, AH, ESP Auth, ESP Enc, IP Comp, KBytes Delivered, KBytes Left, Time Left (secs), Interface, and VIP. The entry for tunnel 0 shows Peer IP Addr 80.12.43.69, Local Network 192.168.1.0/24, Remote Network 10.10.10.0/24, AH N/A, ESP Auth SHA1, ESP Enc AES(256), IP Comp N/A, KBytes Delivered 0, KBytes Left 0, Time Left (secs) 3548, Interface ETH 0, and VIP N/A. There is a 'Remove' button next to the entry. The 'Inbound V1 SAs' table has the same structure and shows a matching entry for tunnel 0. There are also sections for 'Outbound V2 SAs', 'Inbound V2 SAs', and 'No Tunnels' with a 'Refresh' button at the bottom.

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP
0	80.12.43.69	192.168.1.0/24	10.10.10.0/24	N/A	SHA1	AES(256)	N/A	0	0	3548	ETH 0	N/A

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface	VIP
0	80.12.43.69	192.168.1.0/24	10.10.10.0/24	N/A	SHA1	AES(256)	N/A	0	0	3548	ETH 0	N/A

Configure an IPsec VPN tunnel between a TransPort LR router and a TransPort WR router

5.2 TransPort LR54

To verify if the tunnel is up, do the following:

```
digi.router> show ipsec 1

IPsec 1 Status and Statistics
-----
Description      :
Admin Status     : Up
Oper Status      : Up
Uptime           : 7 seconds

Peer              : 86.200.150.100
Local Network    : 10.10.10.0/24
Remote Network   : 192.168.1.0/24

IKE Information
-----
Key Negotiation  : IKEv1, aes256, sha1, modp2048
SPIs             : 2b5b3cf0b24e2d30_i* ae4f7a47b6e7b81d_r

Tunnel Information
-----
Rekeying In      : 69 minutes
AH Cipher Suite  : Not Used
ESP Cipher Suite : aes256, sha1, modp2048
Renegotiating In : 43 minutes
Outbound ESP SAs : 0dbd35cf
Inbound ESP SAs  : cf29fbb7

Dead Peer Detection is on

Bytes In         : 0
Bytes Out        : 0
```

Configure an IPSec VPN tunnel between a TransPort LR router and a TransPort WR router

6 TESTING

Verify that data is going through the tunnel by issuing a ping from each side of the tunnel.

6.1 TransPort WR44

From the web interface (similar to CLI), this can be done from **Administration – Execute a command**

Make sure to specify the interface used to generate this ping (in this example, we use ETH 0)

```
Ping 10.10.10.1 -e0
```

```
Pinging Addr [10.10.10.1]

sent PING # 1
PING receipt # 1 : response time 1.18 seconds
Iface: ETH 0
Ping Statistics
Sent          : 1
Received     : 1
Success      : 100 %
Average RTT  : 1.18 seconds

OK
```

6.2 TransPort LR54

From the web interface (similar to CLI), this can be done from **System > Device Console**

```
digi.router> ping 192.168.1.44
```

```
PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
64 bytes from 192.168.1.44: icmp_seq=1 ttl=251 time=57.5 ms
64 bytes from 192.168.1.44: icmp_seq=2 ttl=251 time=55.2 ms
64 bytes from 192.168.1.44: icmp_seq=3 ttl=251 time=60.3 ms

--- 192.168.1.44 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3011ms
rtt min/avg/max/mdev = 55.270/57.708/60.306/2.077 ms
```

If no traffic is going through, make sure that the firewall rule has been added properly, see [section 4.6](#)

You can view firewall rules by using the following:

```
firewall -t nat -L -v
```