



Level1 router IPSec VPN vs. SSH Sentinel 1.3.2

Level1 router is applicable to FBR-1407, FBR-1409TX, FBR-1417TX, WBR-2401, WBR-3403TX, WBR-3404TX and WBR-3402

Information:

SSH Sentinel IPSec VPN Client:

WBR-3403 IPSec Dynamic VPN Server:

WAN IP: 61.31.189.162

LAN IP: 192.168.123.0

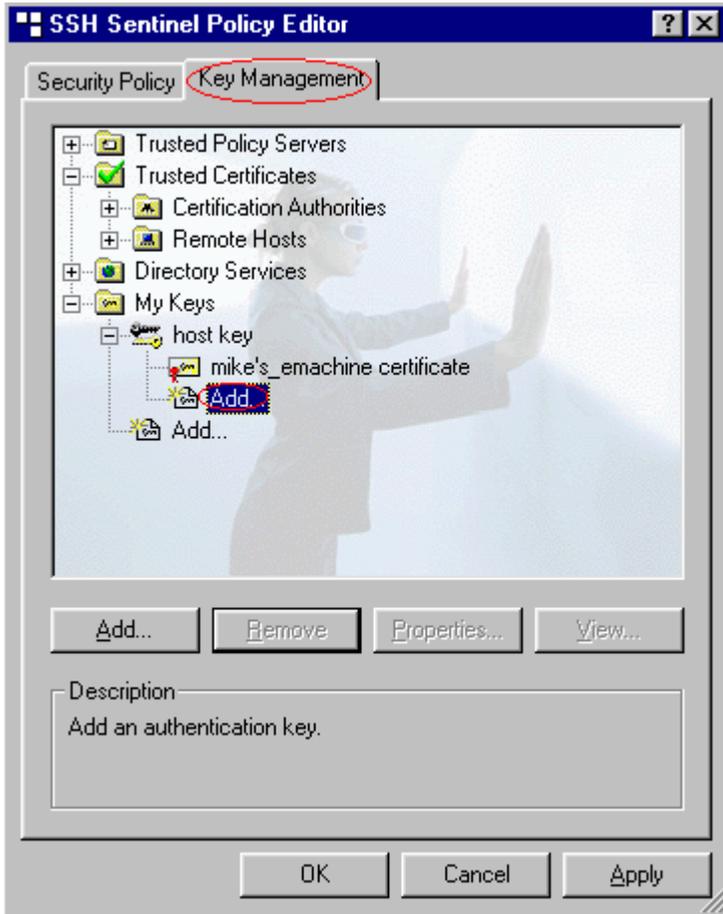
LAN IP Subnet mask: 255.255.255.0

SSH Sentinel Version 1.3 Setting Procedures

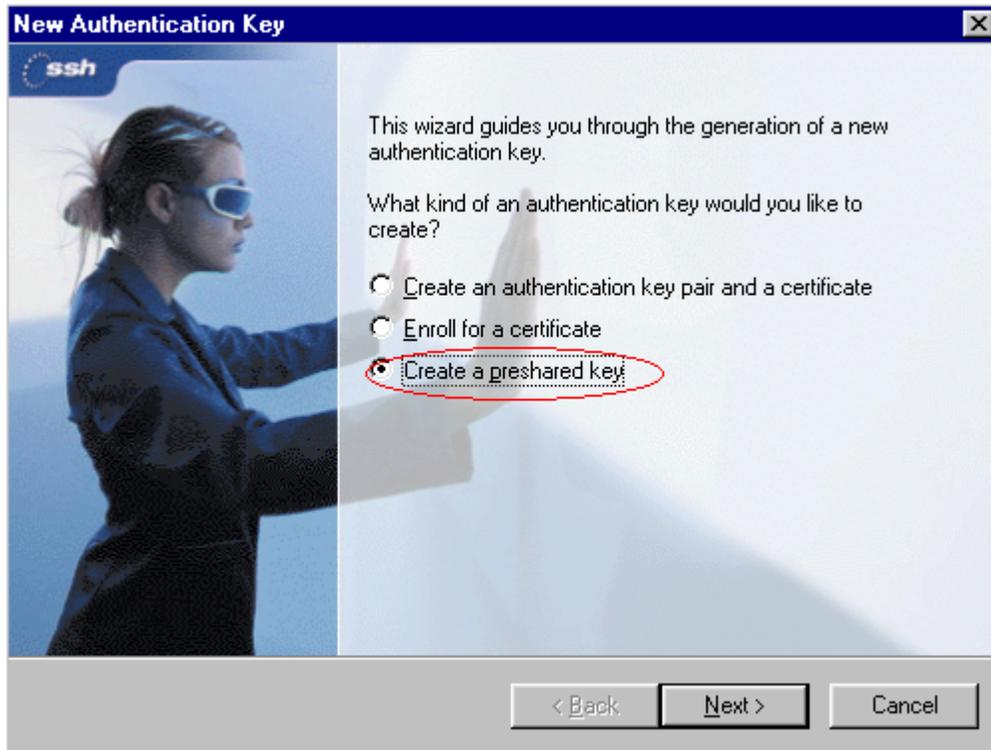
1. Right click on the SSH icon and click “Run Policy Editor”



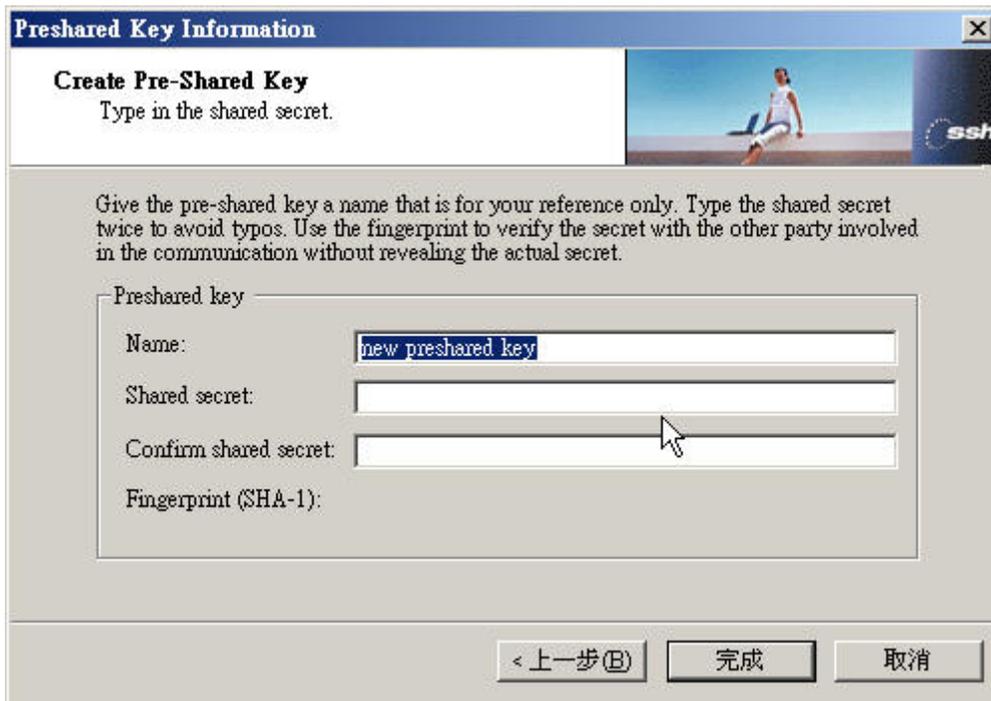
2. Select "Key Management" and click "Add".



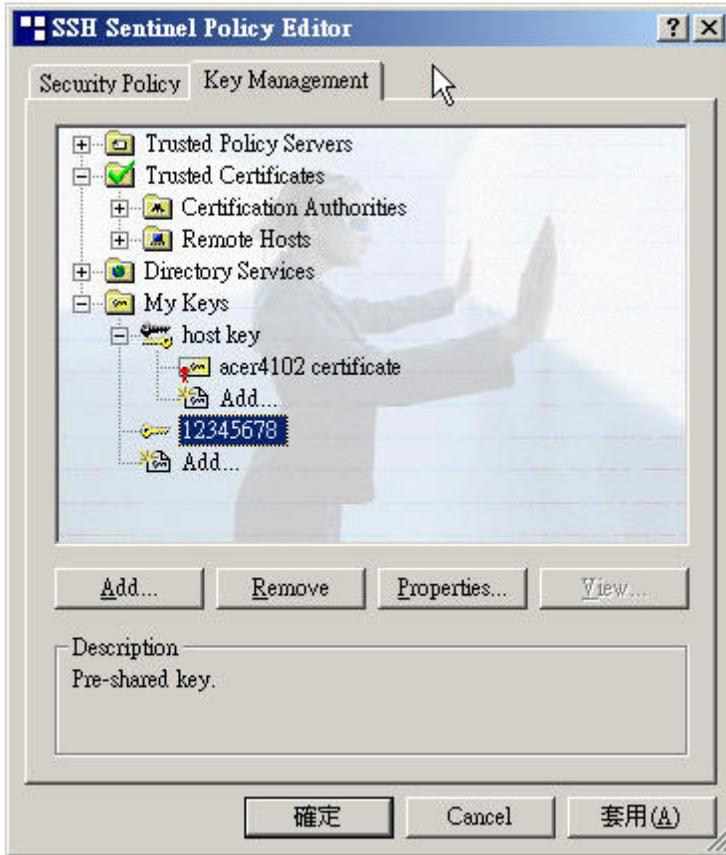
3. Select "Create a preshared key" and click "Next".



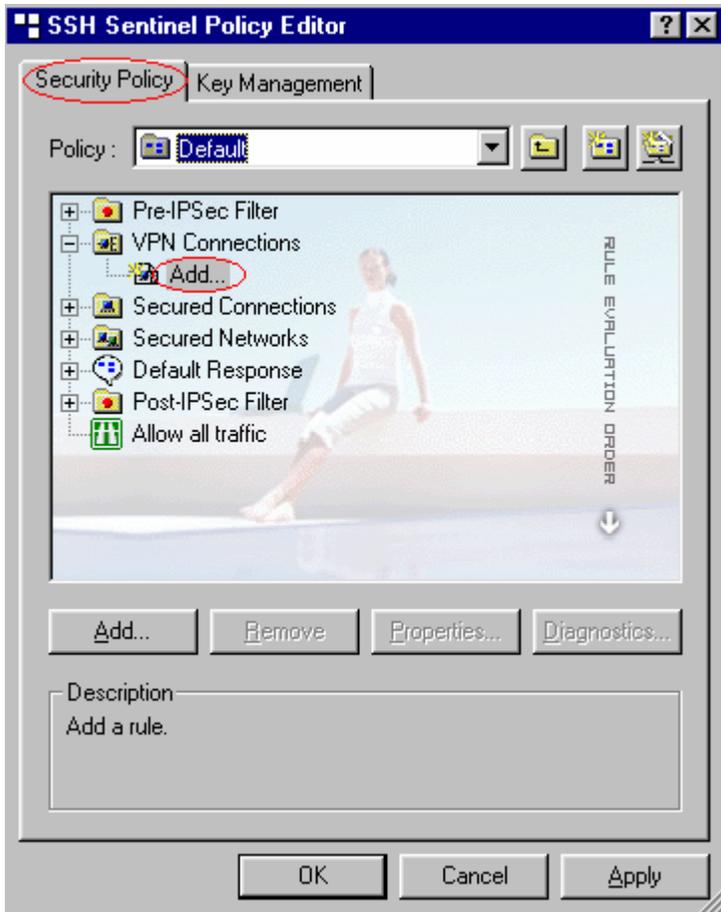
4. Type the same preshared key (Must be the same from WBR-3403 Preshare key) ex1. 12345678 (you can change it) and name it then click "Finish".



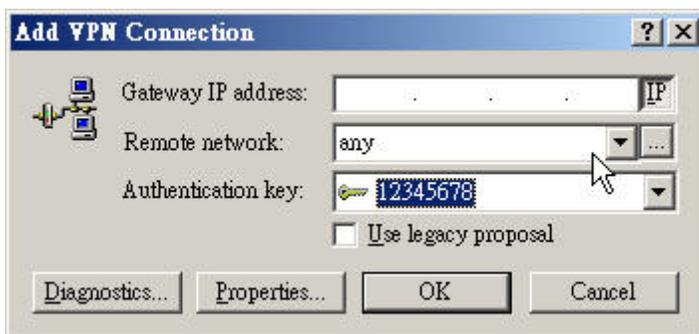
5. You will see the 12345678(for example) key under My Keys and click "Apply".



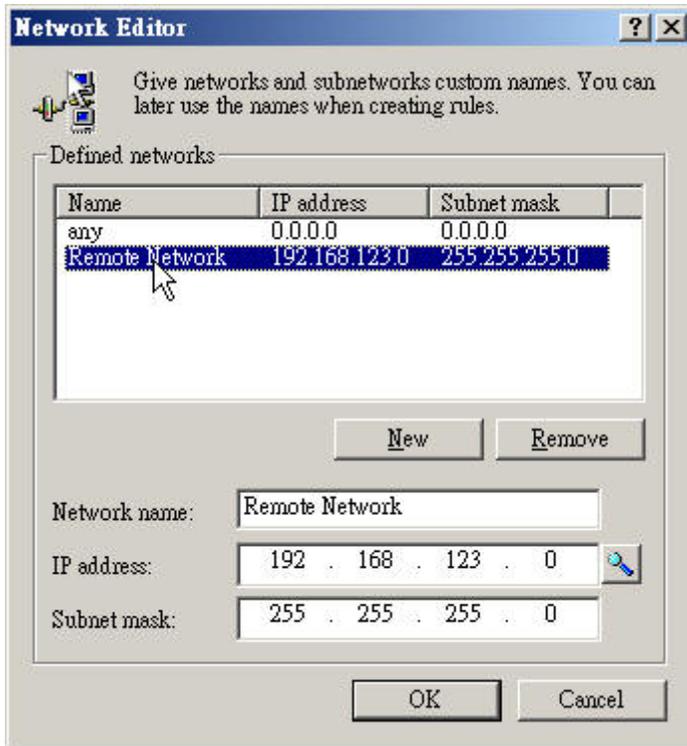
6. Select "Security Policy" and Under VPN Connections click "Add".



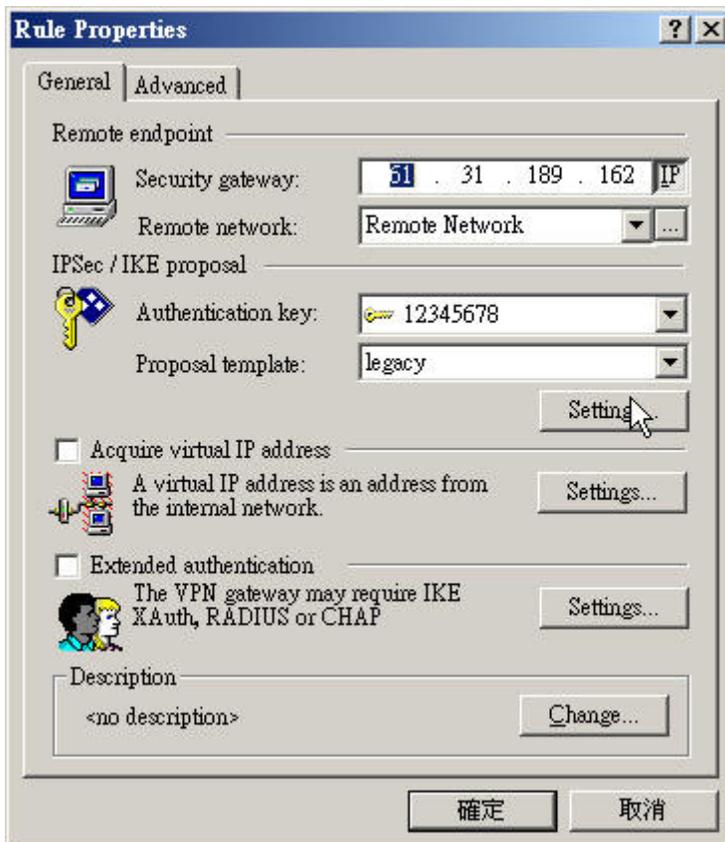
- Click "IP" button and type the Remote Gateway IP Address. Select 12345678 as Authentication key, check Use legacy proposal. Click "." button next to Remote Network will bring up Network Editor screen.



- Click New and type Network name, the remote Intranet Network IP address and subnet mask.(In our example WBR-3403 network address is 192.168.123.0/255.255.255.0)



8. Back to Rule Properties page click on IPSec/IKE proposal “Setting”.



9. Configure your IKE and IPSec proposal, be sure it's the same from WBR-3403. Click "OK" when Done.

Proposal Parameters ? X

Set the preferred value of each parameter of the IKE and IPSec proposal.

IKE proposal

Encryption: 3DES

Integrity: SHA-1

IKE mode: main mode

IKE: MODP 768 (group 1)

IPSec proposal

Encryption: 3DES

Integrity: HMAC-SHA-1

IPSec mode: tunnel

PFS group: none

Attach only the selected values to the proposal

OK Cancel

WBR-3403 Dynamic VPN Server Configuration

1. Enable VPN and set Max. number of tunnels, click on “Dynamic VPN setting”.

The screenshot shows the configuration page for a WBR-3403 router. The page title is "BroadbandRouter Configuration". The navigation menu includes: Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox and Logout. The "Security Setting" menu is expanded, showing options for Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The "VPN Settings" section is active, showing a table with columns for ID, Tunnel Name, and Method. The "VPN" item is checked as "Enable", and the "Max. number of tunnels" is set to 5. The table lists 5 tunnels, all with the "IKE" method. The current time is displayed as 2005年4月1日 上午 12:53:32. Navigation buttons include "<< Previous", "Next >>", "Save", "Undo", "Dynamic VPN Settings...", and "Help".

level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
VPN
Miscellaneous

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	5

ID	Tunnel Name	Method
1	test	IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

Current Time
2005年4月1日 上午 12:53:32

<< Previous Next >> Save Undo Dynamic VPN Settings... Help

- Configure IKE as below, you can alter the setting as long as they are the same from SSH setting.

The screenshot shows the 'VPN Settings - Dynamic VPN Tunnel - Set IKE Proposal' configuration page. The interface includes a navigation menu on the left with options like Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main area is titled 'VPN Settings - Dynamic VPN Tunnel - Set IKE Proposal' and features a table for configuring IKE proposals. A search box at the top contains the letter 'a' and a 'Remove' button. The table has columns for ID, Proposal Name, DH Group, Encrypt. algorithm, Auth. algorithm, Life Time, and Life Time Unit. The first row is populated with 'a' as the proposal name, 'Group 1' as the DH group, '3DES' as the encryption algorithm, 'SHA1' as the authentication algorithm, and '3600' as the life time in seconds. The current time is displayed as '2005年4月1日 上午 12:54:04'. At the bottom, there is a 'Proposal ID -- select one --' dropdown and an 'Add to Proposal index' button.

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	a	Group 1	3DES	SHA1	3600	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

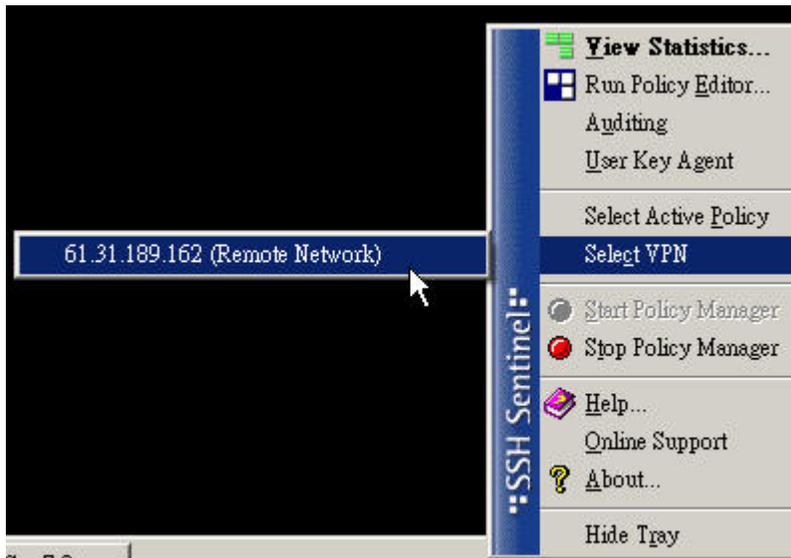
- Configure IPsec as below, you can alter the setting as long as they are the same from SSH setting.

The screenshot shows the 'VPN Settings - Dynamic VPN Tunnel - Set IPsec Proposal' configuration page. The interface is similar to the IKE proposal page, with a navigation menu on the left. The main area is titled 'VPN Settings - Dynamic VPN Tunnel - Set IPsec Proposal' and features a table for configuring IPsec proposals. A search box at the top contains the letter 'b' and a 'Remove' button. The table has columns for ID, Proposal Name, DH Group, Encap. protocol, Encrypt. algorithm, Auth. algorithm, Life Time, and Life Time Unit. The first row is populated with 'b' as the proposal name, 'None' as the DH group, 'ESP' as the encapsulation protocol, '3DES' as the encryption algorithm, 'SHA1' as the authentication algorithm, and '3600' as the life time in seconds. The current time is displayed as '2005年4月1日 上午 12:54:20'. At the bottom, there is a 'Proposal ID -- select one --' dropdown and an 'Add to Proposal index' button.

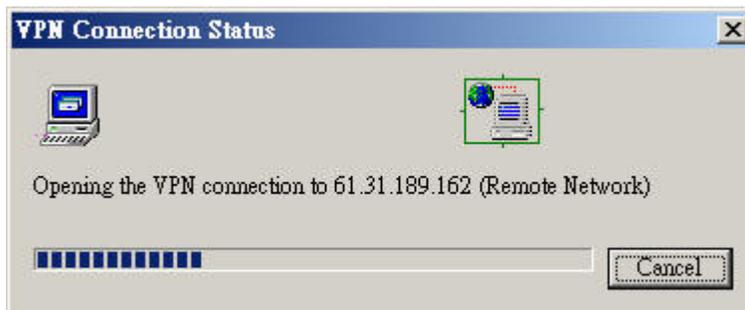
ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	b	None	ESP	3DES	SHA1	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

Establish VPN Connection

1. Right click on the SSH icon and click on "Select VPN" and choose the one just configured.



2. Establish the tunnel.



3. Ping test successful from SSH client to WBR-3403 server.

```
C:\WINDOWS\system32\cmd.exe - ping 192.168.123.254 -t
Reply from 192.168.123.254: bytes=32 time=85ms TTL=64
Reply from 192.168.123.254: bytes=32 time=89ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
Reply from 192.168.123.254: bytes=32 time=86ms TTL=64
Reply from 192.168.123.254: bytes=32 time=89ms TTL=64
Reply from 192.168.123.254: bytes=32 time=88ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
Reply from 192.168.123.254: bytes=32 time=86ms TTL=64
Reply from 192.168.123.254: bytes=32 time=86ms TTL=64
Reply from 192.168.123.254: bytes=32 time=89ms TTL=64
Reply from 192.168.123.254: bytes=32 time=88ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
Reply from 192.168.123.254: bytes=32 time=89ms TTL=64
Reply from 192.168.123.254: bytes=32 time=86ms TTL=64
Reply from 192.168.123.254: bytes=32 time=90ms TTL=64
Reply from 192.168.123.254: bytes=32 time=89ms TTL=64
Reply from 192.168.123.254: bytes=32 time=88ms TTL=64
Reply from 192.168.123.254: bytes=32 time=86ms TTL=64
Reply from 192.168.123.254: bytes=32 time=90ms TTL=64
Reply from 192.168.123.254: bytes=32 time=88ms TTL=64
Reply from 192.168.123.254: bytes=32 time=88ms TTL=64
Reply from 192.168.123.254: bytes=32 time=87ms TTL=64
```