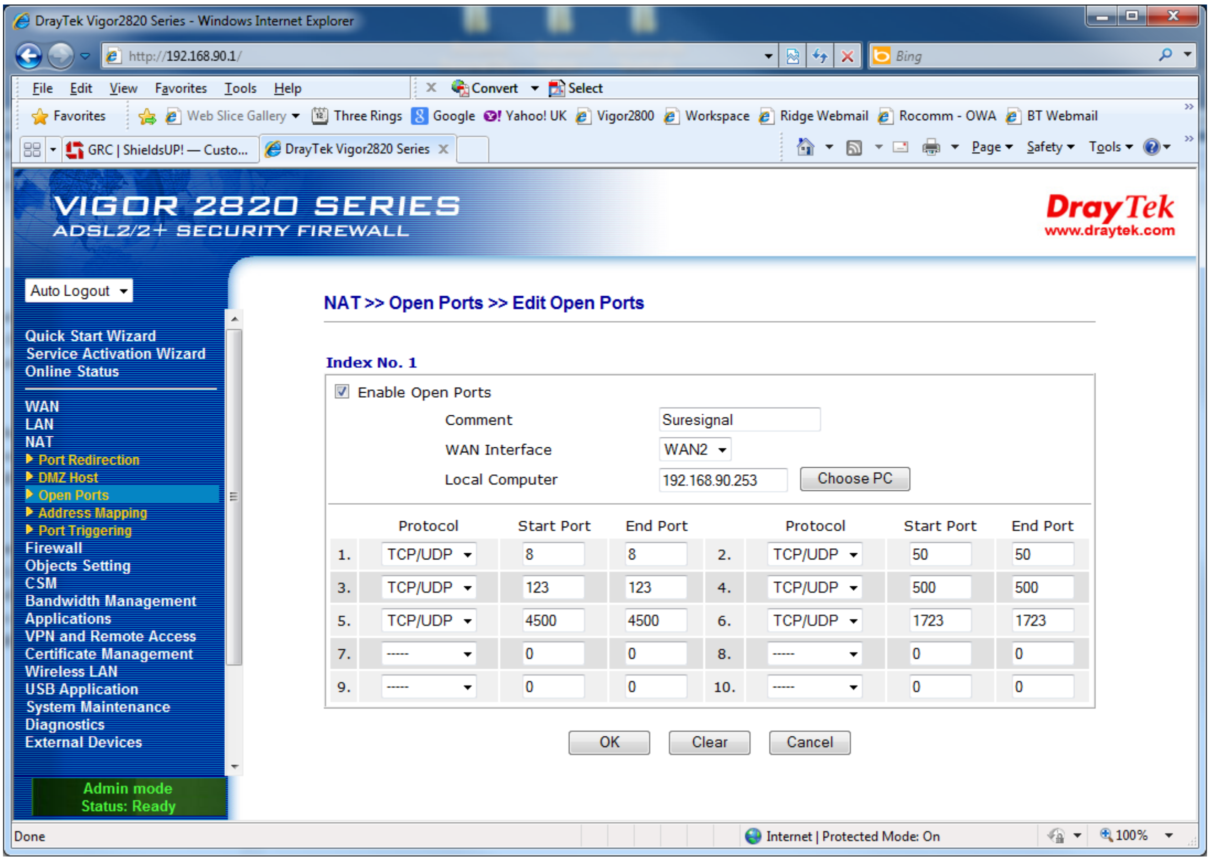
Configuration of Draytek 2820n router



NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

Comment: Suresignal

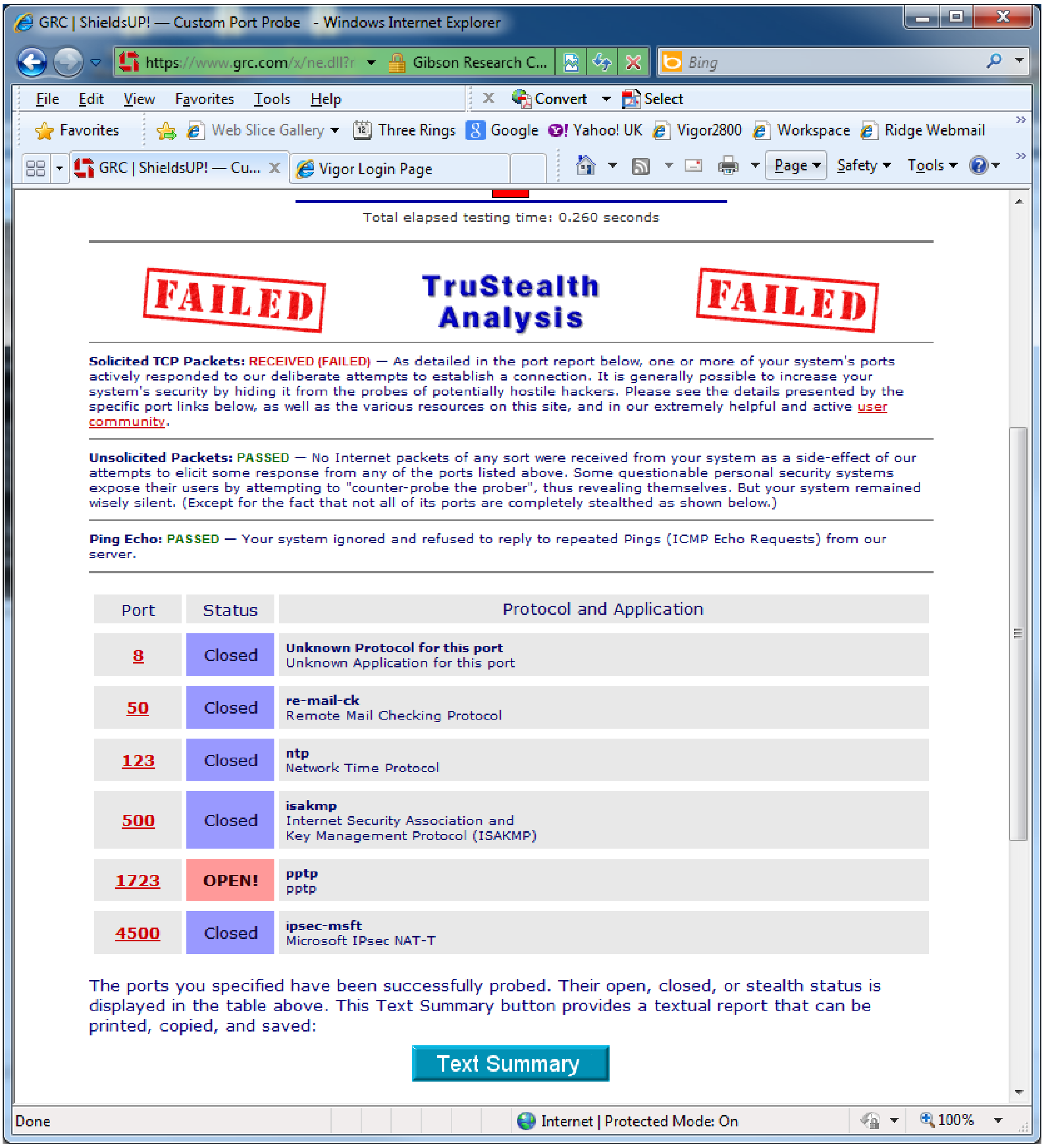
WAN Interface: WAN2

Local Computer: 192.168.90.253 [Choose PC]

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP/UDP	8	8	2.	TCP/UDP	50	50
3.	TCP/UDP	123	123	4.	TCP/UDP	500	500
5.	TCP/UDP	4500	4500	6.	TCP/UDP	1723	1723
7.	-----	0	0	8.	-----	0	0
9.	-----	0	0	10.	-----	0	0

[OK] [Clear] [Cancel]

Laptop with Windows XP firewall disabled


GRC | ShieldsUP! — Custom Port Probe - Windows Internet Explorer
https://www.grc.com/x/ne.dll?r
Gibson Research C...
Bing
File Edit View Favorites Tools Help
Convert Select
Favorites Web Slice Gallery Three Rings Google Yahoo! UK Vigor2800 Workspace Ridge Webmail
GRC | ShieldsUP! — Cu... Vigor Login Page
Page Safety Tools
Done
Internet | Protected Mode: On
100%

Total elapsed testing time: 0.260 seconds

FAILED **TruStealth Analysis** FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

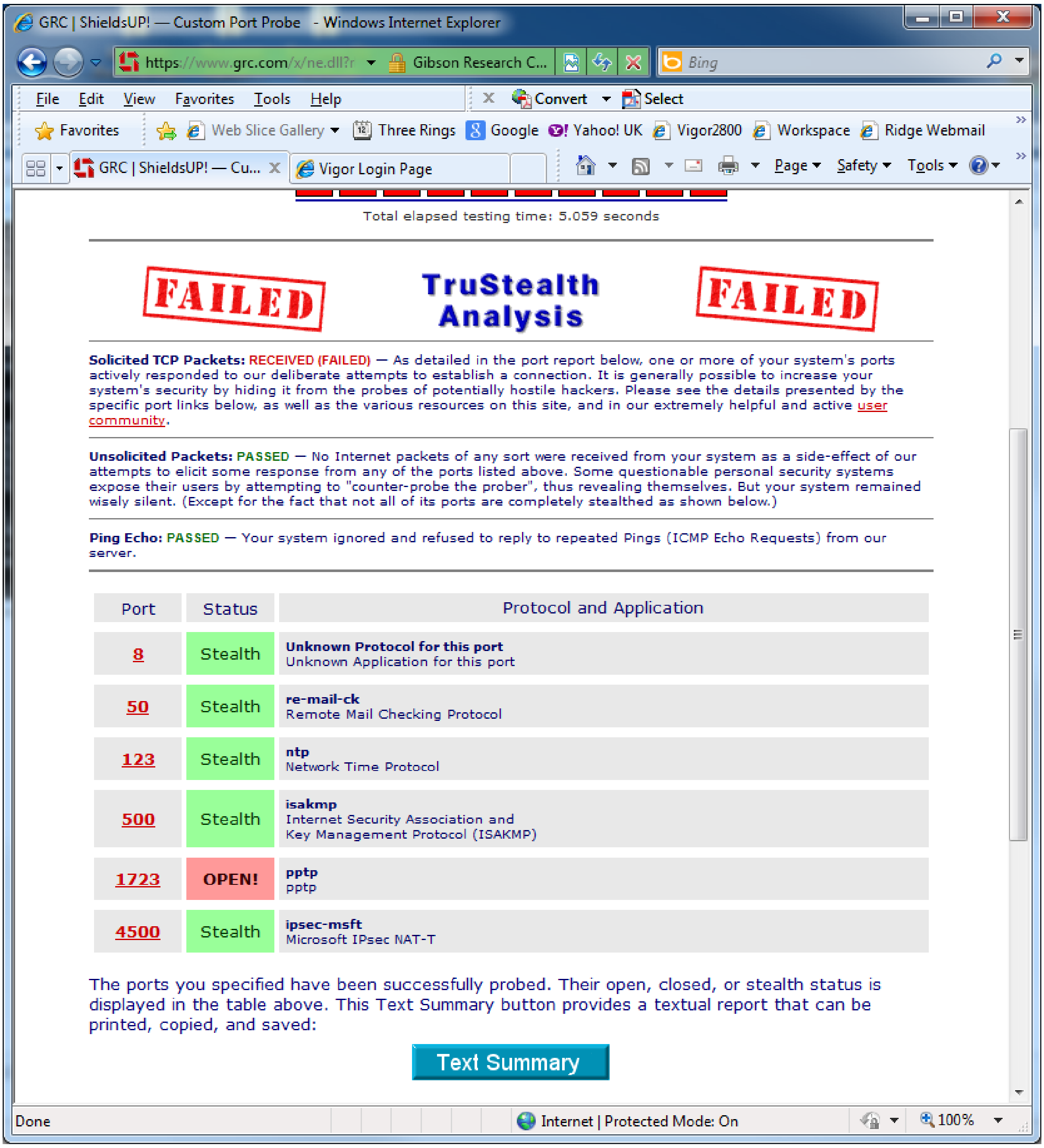
Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Status	Protocol and Application
8	Closed	**Unknown Protocol for this port** Unknown Application for this port
50	Closed	**re-mail-ck** Remote Mail Checking Protocol
123	Closed	**ntp** Network Time Protocol
500	Closed	**isakmp** Internet Security Association and Key Management Protocol (ISAKMP)
1723	OPEN!	**pptp** pptp
4500	Closed	**ipsec-msft** Microsoft IPsec NAT-T

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

Text Summary

Laptop with Windows XP firewall enabled



Total elapsed testing time: 5.059 seconds

FAILED

TruStealth Analysis

FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

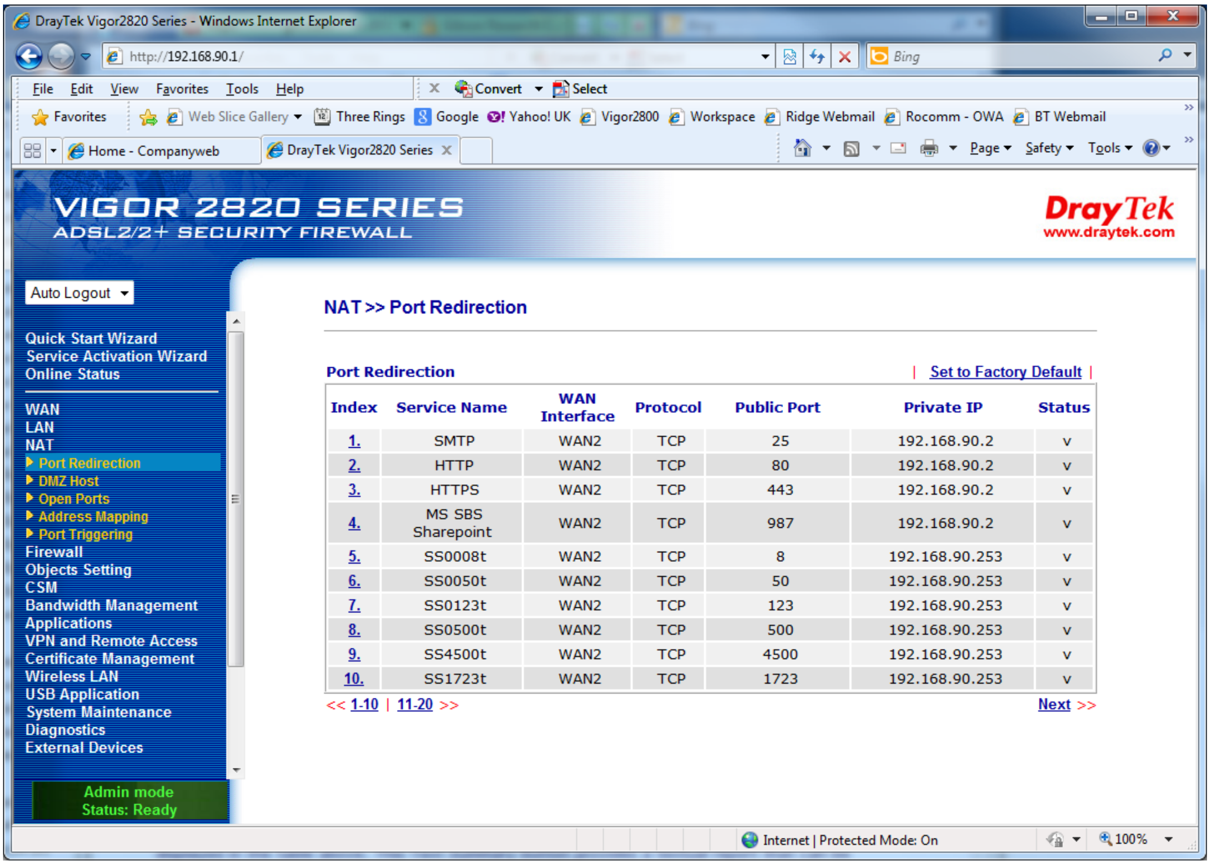
Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Status	Protocol and Application
8	Stealth	**Unknown Protocol for this port** Unknown Application for this port
50	Stealth	**re-mail-ck** Remote Mail Checking Protocol
123	Stealth	**ntp** Network Time Protocol
500	Stealth	**isakmp** Internet Security Association and Key Management Protocol (ISAKMP)
1723	OPEN!	**pptp** pptp
4500	Stealth	**ipsec-msft** Microsoft IPsec NAT-T

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

Text Summary

Configuration of Draytek 2820n router – TCP ports



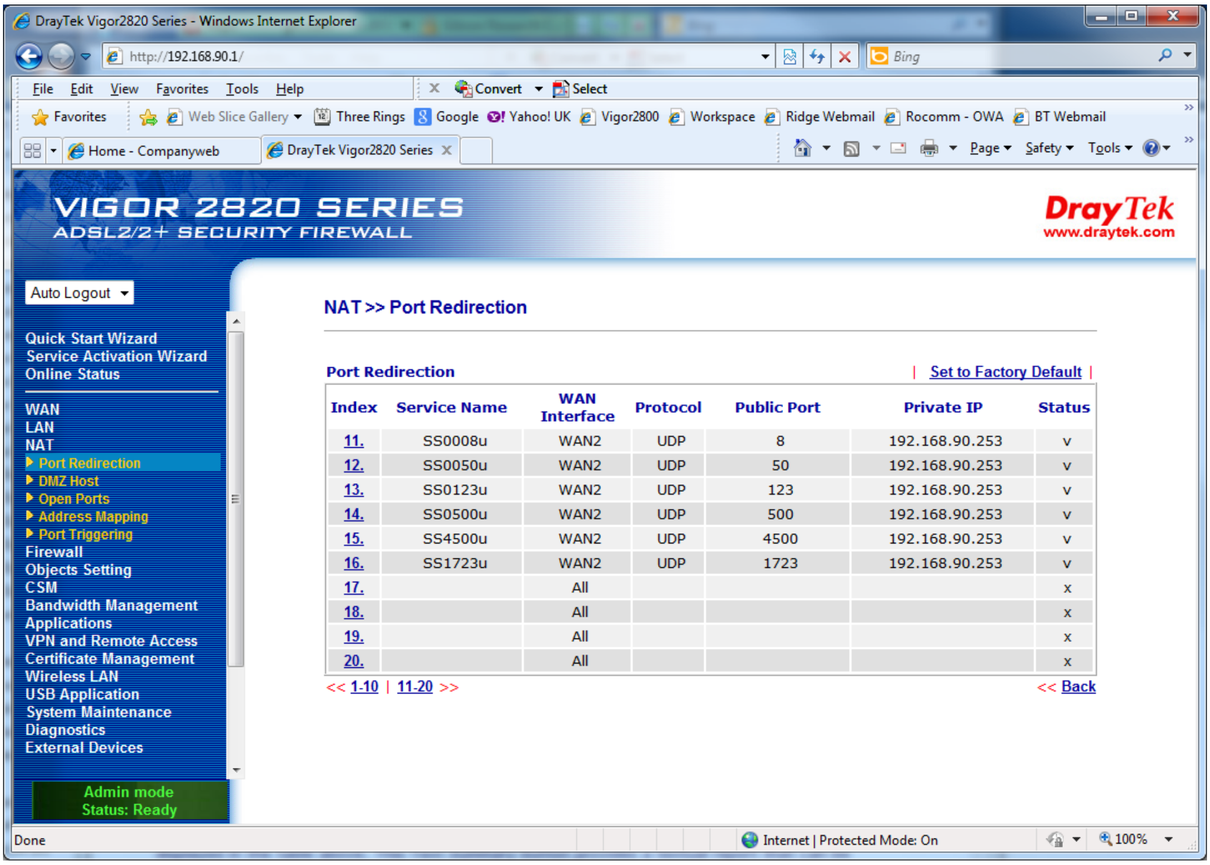
NAT >> Port Redirection

Port Redirection | Set to Factory Default |

Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
1.	SMTP	WAN2	TCP	25	192.168.90.2	v
2.	HTTP	WAN2	TCP	80	192.168.90.2	v
3.	HTTPS	WAN2	TCP	443	192.168.90.2	v
4.	MS SBS Sharepoint	WAN2	TCP	987	192.168.90.2	v
5.	SS0008t	WAN2	TCP	8	192.168.90.253	v
6.	SS0050t	WAN2	TCP	50	192.168.90.253	v
7.	SS0123t	WAN2	TCP	123	192.168.90.253	v
8.	SS0500t	WAN2	TCP	500	192.168.90.253	v
9.	SS4500t	WAN2	TCP	4500	192.168.90.253	v
10.	SS1723t	WAN2	TCP	1723	192.168.90.253	v

<< 1-10 | 11-20 >> Next >>

Configuration of Draytek 2820n router – UDP ports



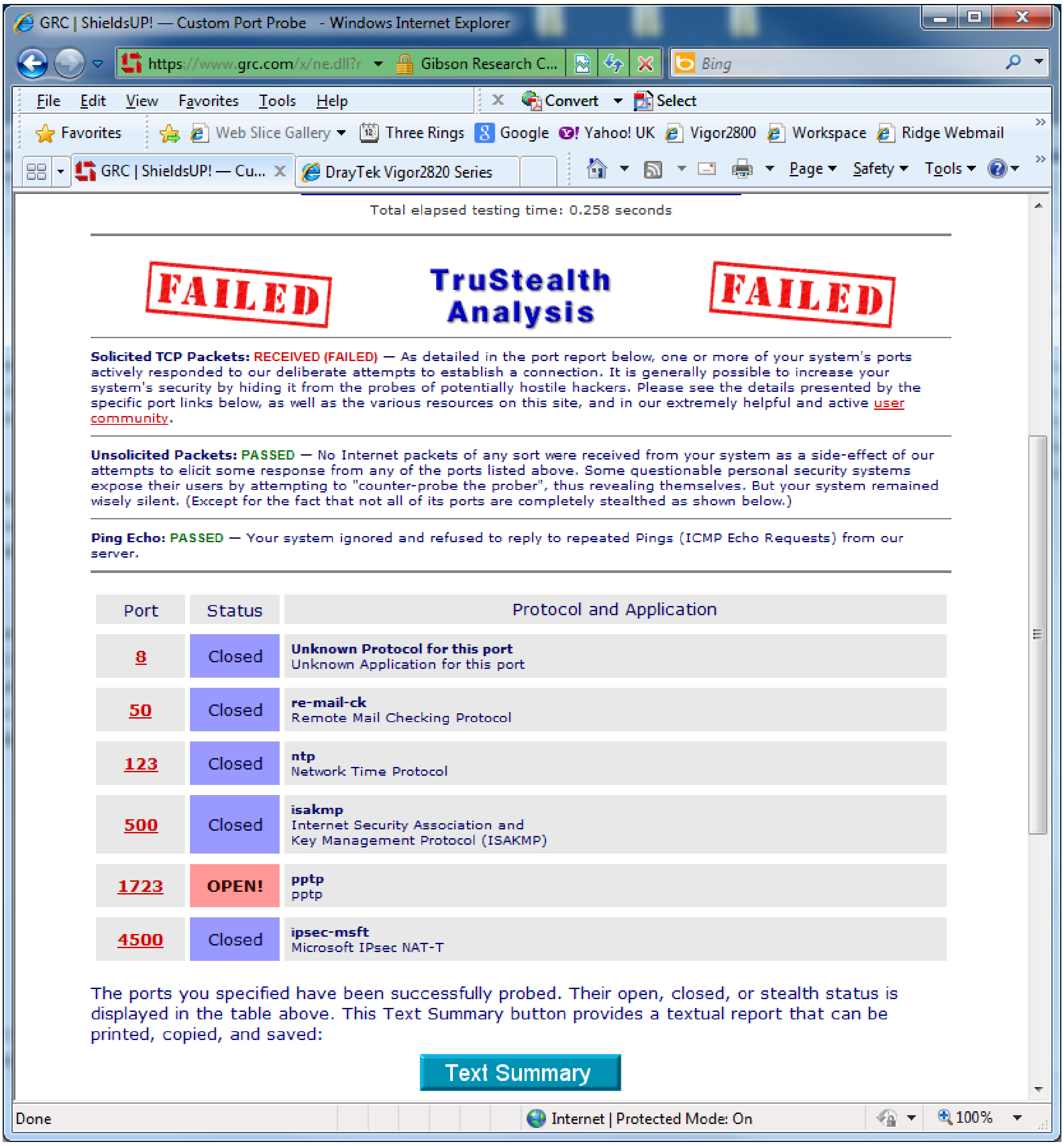
NAT >> Port Redirection

Port Redirection | Set to Factory Default |

Index	Service Name	WAN Interface	Protocol	Public Port	Private IP	Status
11.	SS0008u	WAN2	UDP	8	192.168.90.253	v
12.	SS0050u	WAN2	UDP	50	192.168.90.253	v
13.	SS0123u	WAN2	UDP	123	192.168.90.253	v
14.	SS0500u	WAN2	UDP	500	192.168.90.253	v
15.	SS4500u	WAN2	UDP	4500	192.168.90.253	v
16.	SS1723u	WAN2	UDP	1723	192.168.90.253	v
17.		All				x
18.		All				x
19.		All				x
20.		All				x

<< 1-10 | 11-20 >> << Back

Laptop with Windows XP firewall disabled



Total elapsed testing time: 0.258 seconds

FAILED **TruStealth Analysis** FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

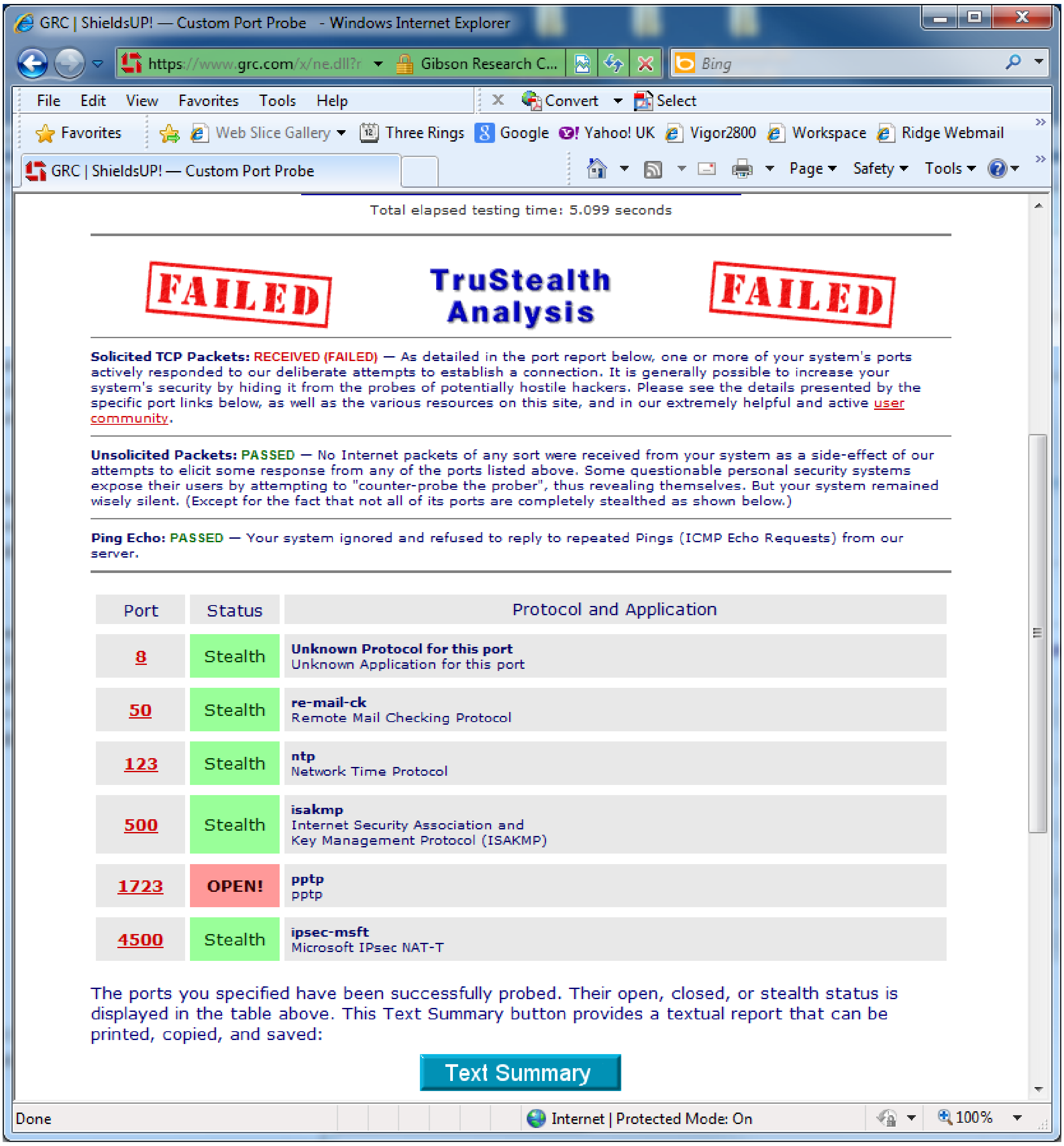
Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Status	Protocol and Application
8	Closed	**Unknown Protocol for this port** Unknown Application for this port
50	Closed	**re-mail-ck** Remote Mail Checking Protocol
123	Closed	**ntp** Network Time Protocol
500	Closed	**isakmp** Internet Security Association and Key Management Protocol (ISAKMP)
1723	OPEN!	**pptp** pptp
4500	Closed	**ipsec-msft** Microsoft IPsec NAT-T

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

Text Summary

Laptop with Windows XP firewall enabled


GRC | ShieldsUP! — Custom Port Probe - Windows Internet Explorer
https://www.grc.com/x/ne.dll?r
Gibson Research C...
Bing
File Edit View Favorites Tools Help
Convert
Select
Favorites
Web Slice Gallery
Three Rings
Google
Yahoo! UK
Vigor2800
Workspace
Ridge Webmail
GRC | ShieldsUP! — Custom Port Probe
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

Total elapsed testing time: 5.099 seconds

FAILED TruStealth Analysis FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

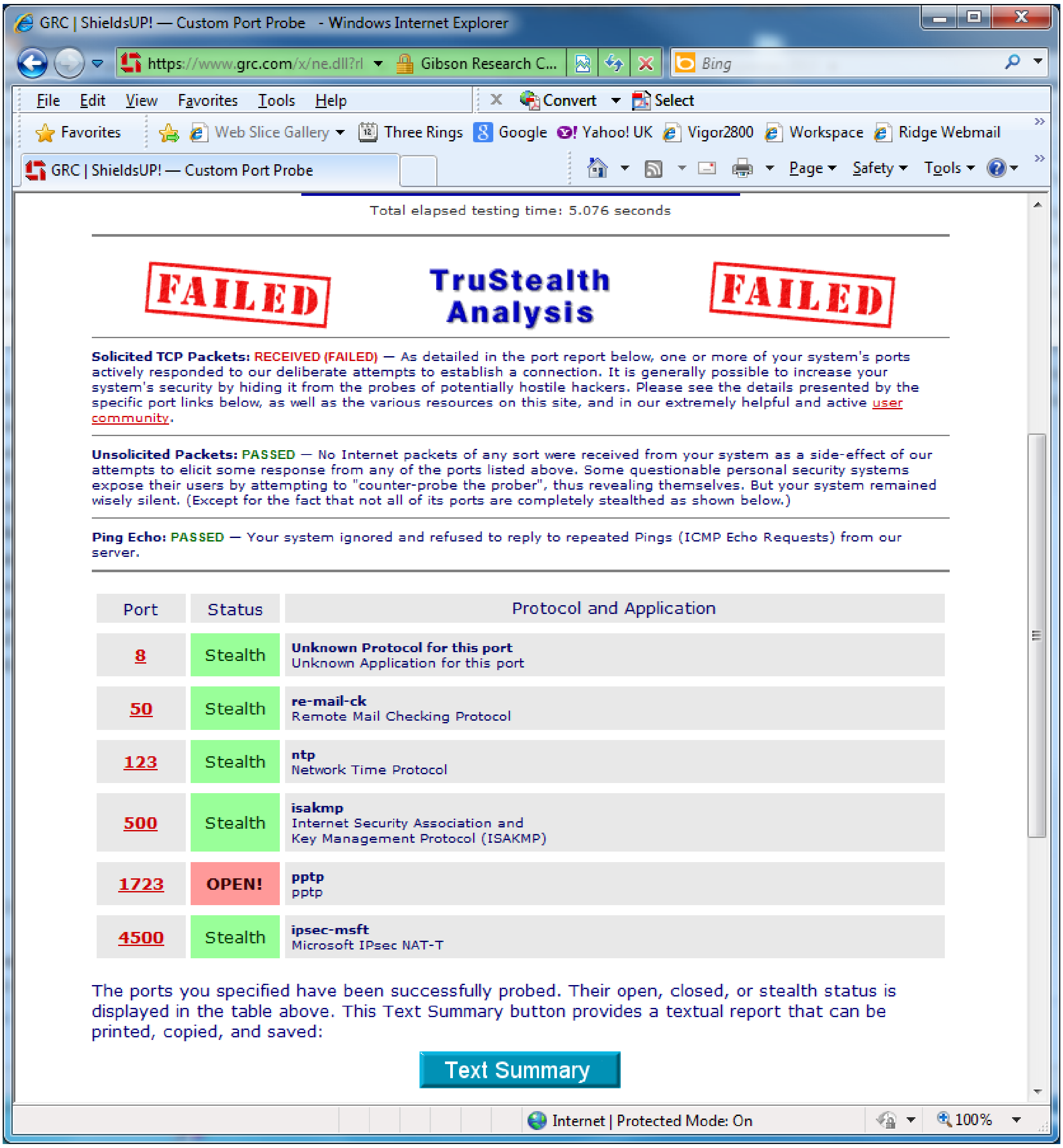
Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Status	Protocol and Application
8	Stealth	**Unknown Protocol for this port** Unknown Application for this port
50	Stealth	**re-mail-ck** Remote Mail Checking Protocol
123	Stealth	**ntp** Network Time Protocol
500	Stealth	**isakmp** Internet Security Association and Key Management Protocol (ISAKMP)
1723	OPEN!	**pptp** pptp
4500	Stealth	**ipsec-msft** Microsoft IPsec NAT-T

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved:

Text Summary

This is the result with the Suresignal connected



Total elapsed testing time: 5.076 seconds

FAILED **TruStealth Analysis** FAILED

Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Status	Protocol and Application
8	Stealth	**Unknown Protocol for this port** Unknown Application for this port
50	Stealth	**re-mail-ck** Remote Mail Checking Protocol
123	Stealth	**ntp** Network Time Protocol
500	Stealth	**isakmp** Internet Security Association and Key Management Protocol (ISAKMP)
1723	OPEN!	**pptp** pptp
4500	Stealth	**ipsec-msft** Microsoft IPsec NAT-T

The ports you specified have been successfully probed. Their open, closed, or stealth status is displayed in the table above. This Text Summary button provides a textual report that can be printed, copied, and saved: