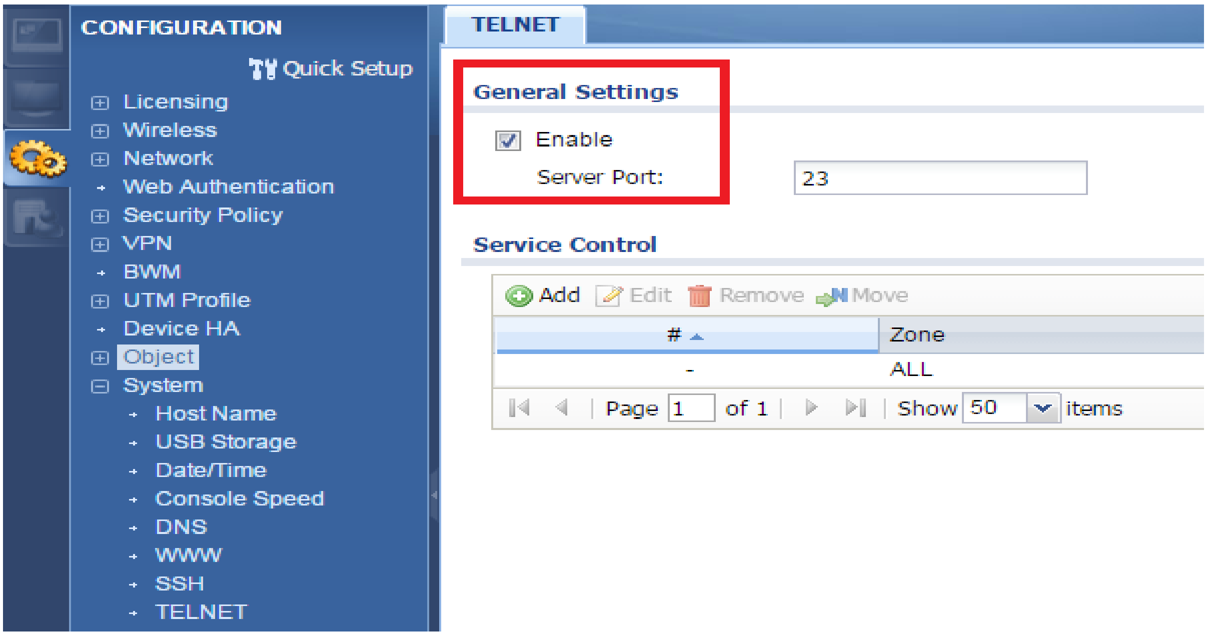
Steps

Step 1: Enable the TELNET service of your device through the graphical user interface (GUI). Before connecting to PuTTY (described in Step 2), make sure the function of TELNET is set to “Enable”. Configuration=>system=>TELNET and click "Apply”



General Settings

☑ Enable

Server Port: 23

Service Control

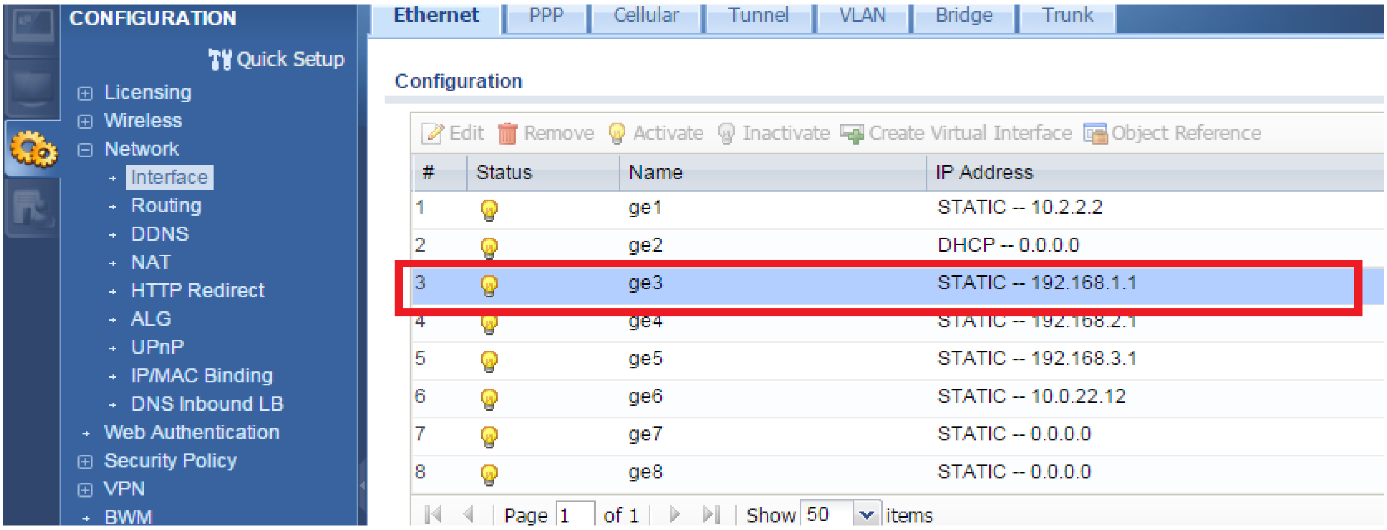
#	Zone
-	ALL

Page 1 of 1 Show 50 items

If you do not know the IP address of your router, please:

Login GUI => Configuration => Interface => Ethernet and check the port you connected

For example: When you connect to ge3, check the IP address of ge3. In this example, the ge3 ip address is 192.16.1.1

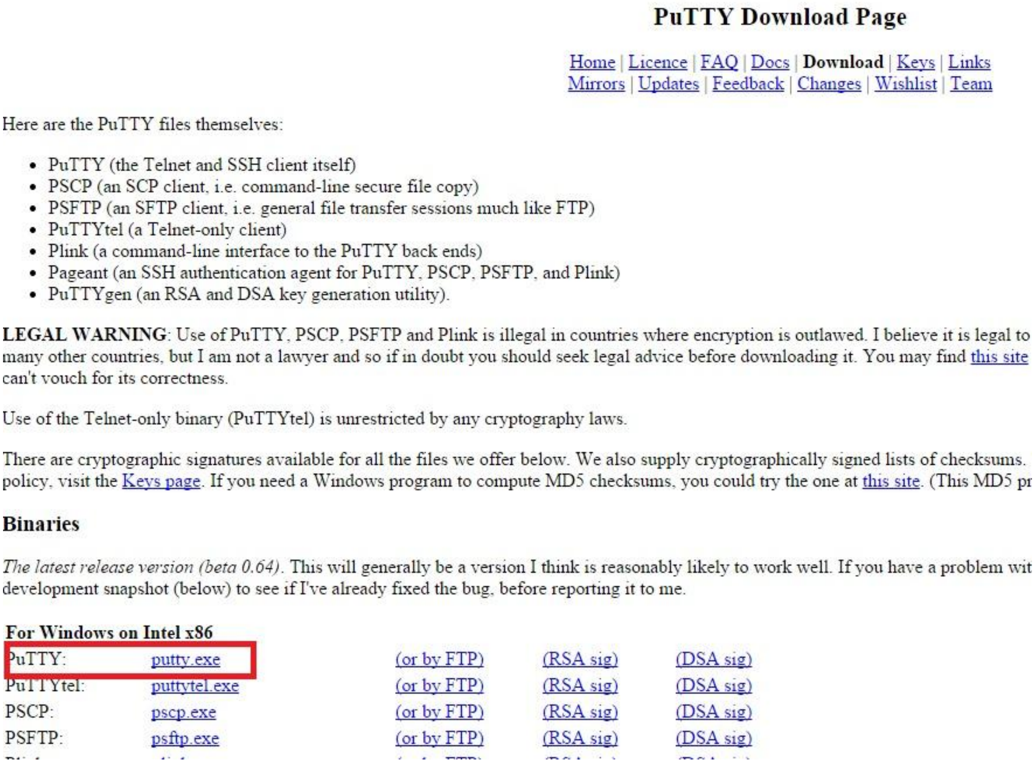


Configuration

#	Status	Name	IP Address
1	💡	ge1	STATIC -- 10.2.2.2
2	💡	ge2	DHCP -- 0.0.0.0
3	💡	ge3	STATIC -- 192.168.1.1
4	💡	ge4	STATIC -- 192.168.2.1
5	💡	ge5	STATIC -- 192.168.3.1
6	💡	ge6	STATIC -- 10.0.22.12
7	💡	ge7	STATIC -- 0.0.0.0
8	💡	ge8	STATIC -- 0.0.0.0

Page 1 of 1 Show 50 items

Step2: Download "PuTTY" from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Choose "putty.exe", as circled below.



PuTTY Download Page

Home | Licence | FAQ | Docs | **Download** | Keys | Links
Mirrors | Updates | Feedback | Changes | Wishlist | Team

Here are the PuTTY files themselves:

- PuTTY (the Telnet and SSH client itself)
- PSCP (an SCP client, i.e. command-line secure file copy)
- PSFTP (an SFTP client, i.e. general file transfer sessions much like FTP)
- PuTTYtel (a Telnet-only client)
- Plink (a command-line interface to the PuTTY back ends)
- Pageant (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)
- PuTTYgen (an RSA and DSA key generation utility).

LEGAL WARNING: Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. I believe it is legal to many other countries, but I am not a lawyer and so if in doubt you should seek legal advice before downloading it. You may find this site can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

There are cryptographic signatures available for all the files we offer below. We also supply cryptographically signed lists of checksums. policy, visit the Keys page. If you need a Windows program to compute MD5 checksums, you could try the one at this site. (This MD5 pr

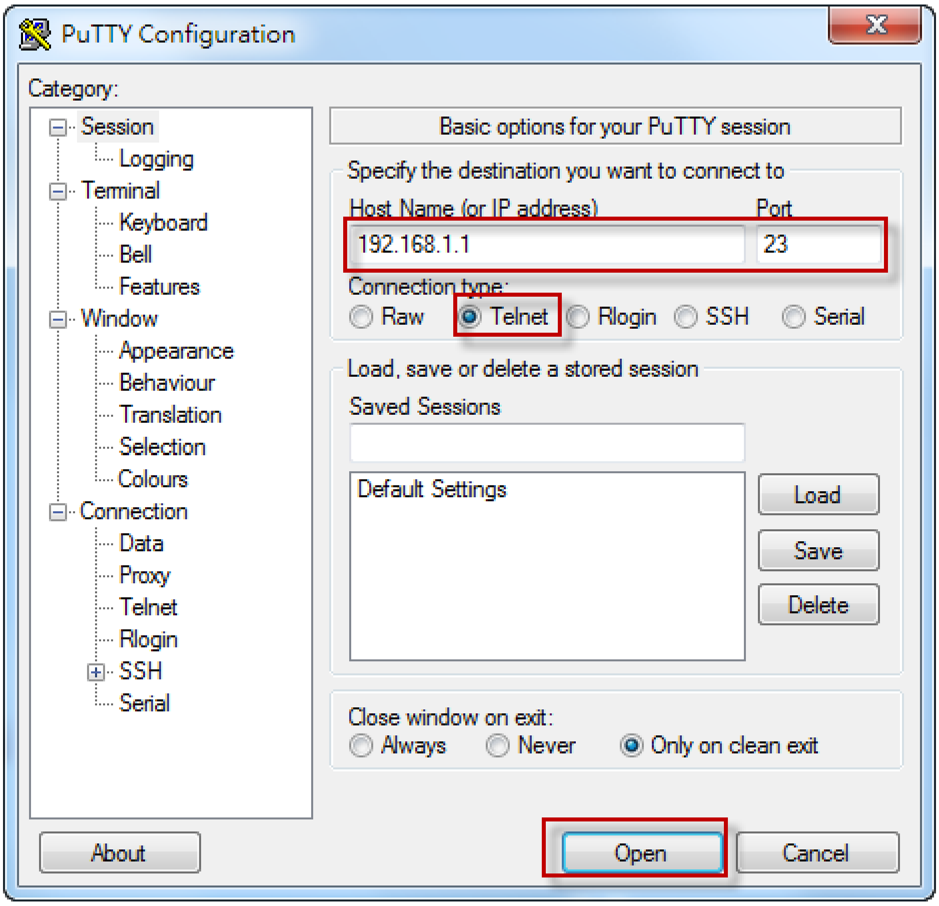
Binaries

The latest release version (beta 0.64). This will generally be a version I think is reasonably likely to work well. If you have a problem wit development snapshot (below) to see if I've already fixed the bug, before reporting it to me.

For Windows on Intel x86

PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)

Step 3: Login Telnet by PuTTY.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1

Port: 23

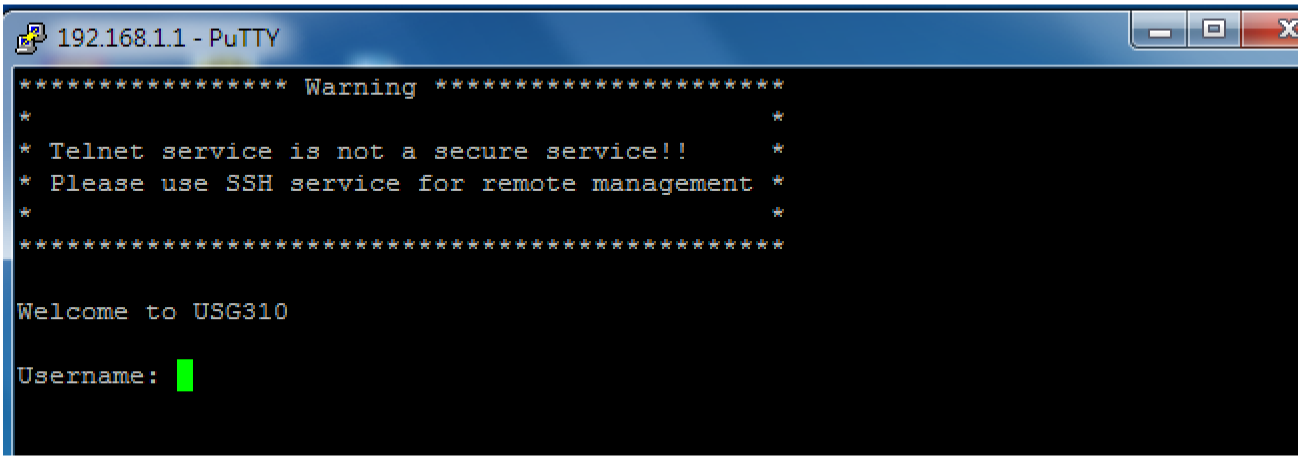
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Login to the device with username/password (The default is admin/1234).



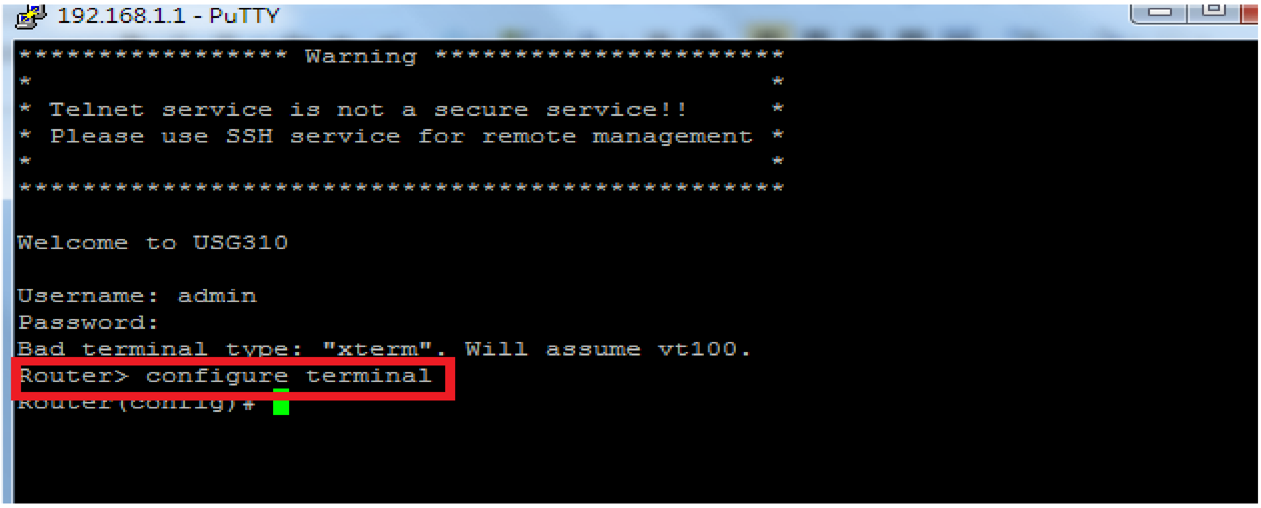
192.168.1.1 - PuTTY

```
****************** Warning ************************
*                                                 *
* Telnet service is not a secure service!!        *
* Please use SSH service for remote management *
*                                                 *
***************************************************

Welcome to USG310

Username:
```

Step 4: Enter the CLI command “**configure terminal**” to enter configuration mode.

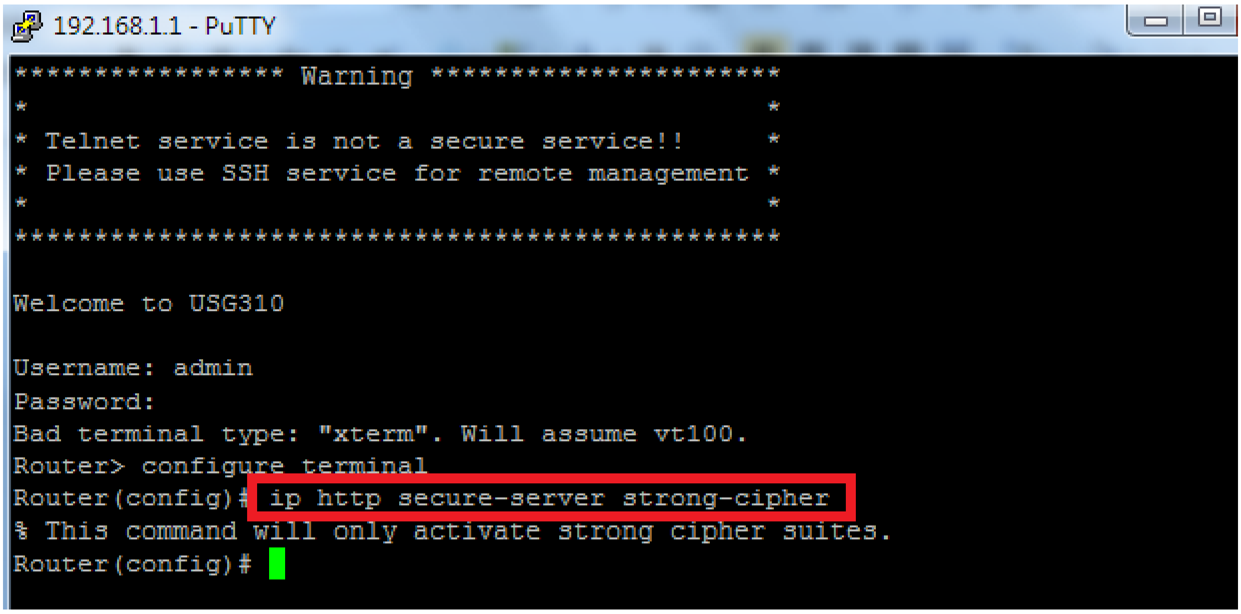


```
****************** Warning ************************
*                                                 *
* Telnet service is not a secure service!!        *
* Please use SSH service for remote management    *
*                                                 *
***************************************************

Welcome to USG310

Username: admin
Password:
Bad terminal type: "xterm". Will assume vt100.
Router> configure terminal
Router(config)#
```

Step 5: Enter the CLI command “**ip http secure-server strong-cipher**” to enable a stronger cipher.

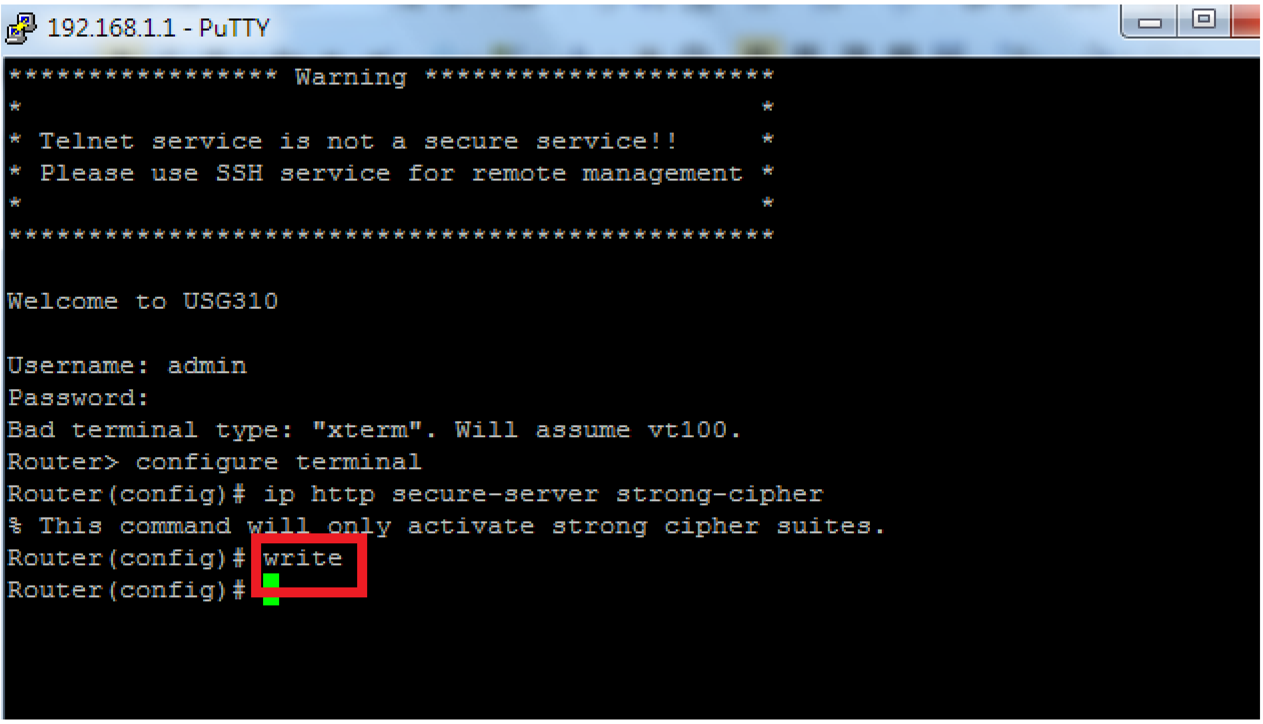


```
****************** Warning ************************
*                                                 *
* Telnet service is not a secure service!!        *
* Please use SSH service for remote management    *
*                                                 *
***************************************************

Welcome to USG310

Username: admin
Password:
Bad terminal type: "xterm". Will assume vt100.
Router> configure terminal
Router(config)# ip http secure-server strong-cipher
% This command will only activate strong cipher suites.
Router(config)#
```

Step 6: Enter the CLI command "**write**" to save the configuration changes.

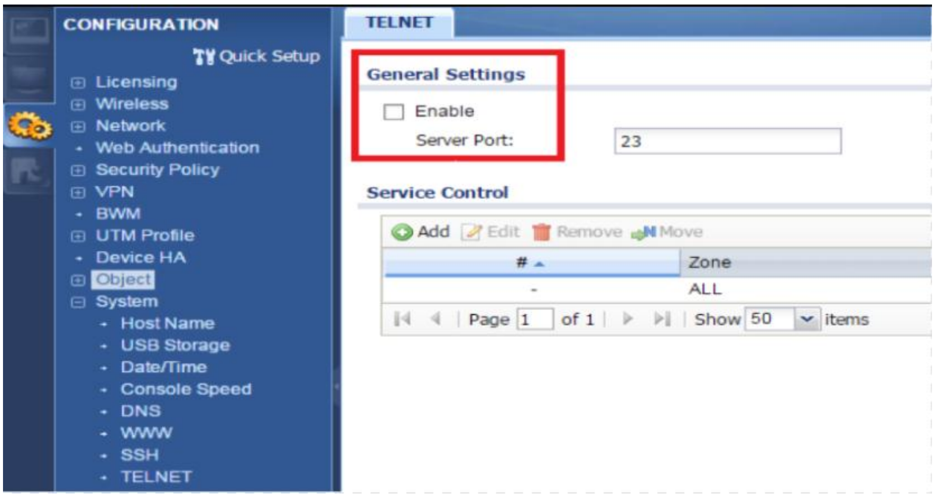


```
***************** Warning **********************
*                                              *
* Telnet service is not a secure service!!     *
* Please use SSH service for remote management *
*                                              *
************************************************

Welcome to USG310

Username: admin
Password:
Bad terminal type: "xterm". Will assume vt100.
Router> configure terminal
Router(config)# ip http secure-server strong-cipher
% This command will only activate strong cipher suites.
Router(config)# write
Router(config)#
```

Step 7: Go back to the TELNET setting on GUI. Disable the TELNET service to secure the device.



General Settings

□ Enable

Server Port: 23

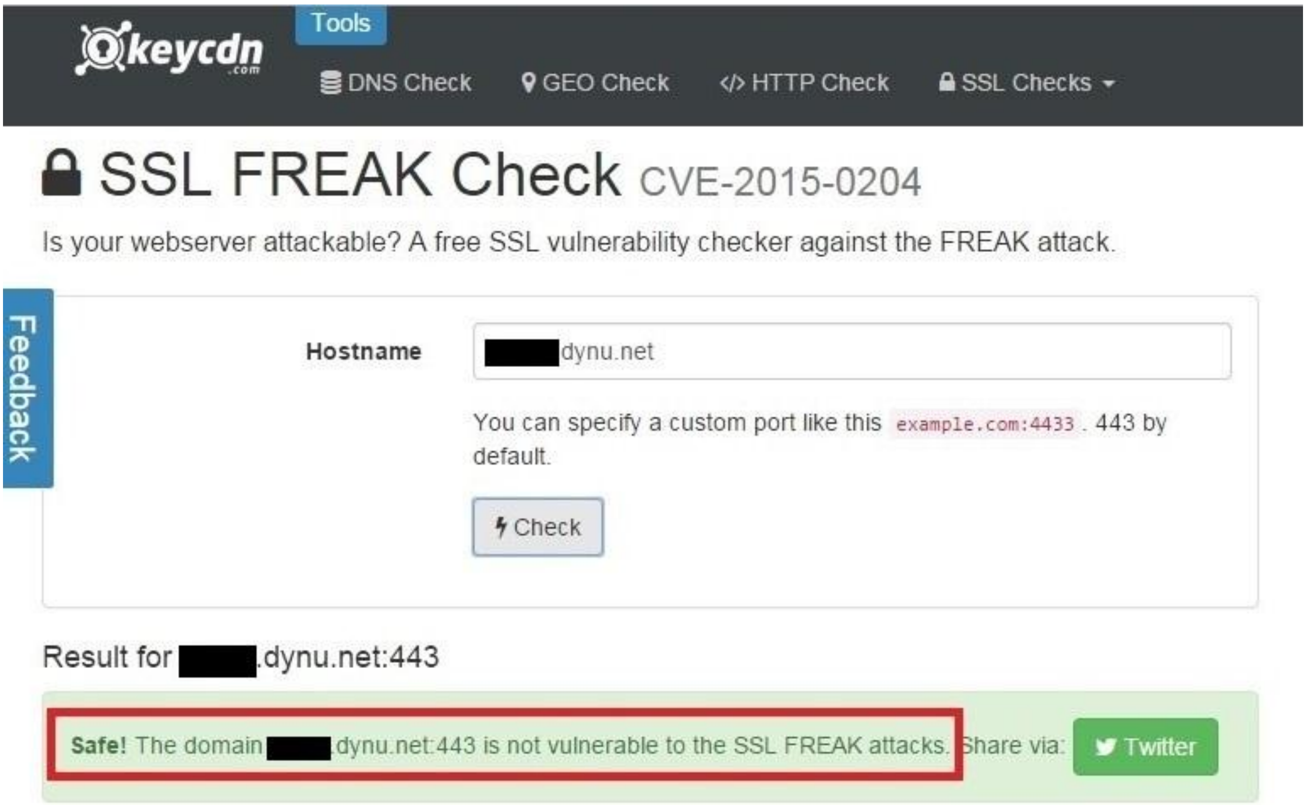
Service Control

#	Zone
-	ALL

Page 1 of 1 | Show 50 items

Upon completion of the above-mentioned steps, a stronger cipher suite will be activated.

Verification: After those CLI commands are applied, your device (USG) should be able to pass the test. Vulnerability checker: https://tools.keycdn.com/freak



SSL FREAK Check CVE-2015-0204

Is your webserver attackable? A free SSL vulnerability checker against the FREAK attack.

Hostname: [redacted]dynu.net

You can specify a custom port like this `example.com:4433`. 443 by default.

Result for [redacted].dynu.net:443

Safe! The domain [redacted].dynu.net:443 is not vulnerable to the SSL FREAK attacks. Share via: