Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Support guides for the Cyberguard Firewall Appliance

The reason for this document is that there is very little out there on the internet, on training courses, product cd's, release notes or "readme" help files for Cyberguard firewall administrators to "pick up and use". Additionally, there are many occasions where there is just little information if none at all to assist (excluding paying for support) in tuning, troubleshooting and special unique guidelines. This aims to bridge the gap by providing a comprehensive guide that has been accumulated over the years of adminis...

Copyright SANS Institute

Author Retains Full Rights

AD

Support guides for the Cyberguard Firewall Appliance:-

29 August 2003

Chris Bodill
Version 1.4b
Option 2
GSEC

Abstract

The reason for this document is that there is very little out there on the internet, on training courses, product cd's, release notes or "readme" help files for Cyberguard firewall administrators to " pick up and use ". Additionally, there are many occasions where there is just little information if none at all to assist (excluding paying for support) in tuning, troubleshooting and special unique guidelines. This aims to bridge the gap by providing a comprehensive guide that has been accumulated over the years of administration and to alleviate some of the frustration for Cyberguard firewall administrators. This list of various tips and notes gathered together forms an invaluable guide due to the fact that its based on years of experience; undocumented by official lines, but proven, tried and tested in our lab plus on many Cyberguard pairs under maintenance contracts. These vary from 8 HA (high availability) pairs for MOD, another dozen pairs for commercial and e-com. enterprises and others for government departments, housed in a large outsourcing datacentre. It combines various troubleshooting guides, how–to, tips and warnings, to date. It's impossible to list every scenario, but these that I have listed below I have rated as some of the most likely, most useful and aim to be both functional and practical.

There are 5 sections:-

1) A BRIEF HISTORY PAGE 1
2) UPGRADING GUIDES PAGES 2 - 9
3) TROUBLESHOOTING / TUNING PAGES 9 - 13
4) HA ISSUES PAGE 14
5) REFERENCES PAGE 15

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A BRIEF HISTORY

"The Cyberguard firewall appliance started in 1994 when it was incorporated in conjunction with a spin-off from Harris Corporation. CyberGuard's roots extend as far back as 1967 with the founding of Datacraft, a manufacturer of hardware and software for real-time computers. In 1974, Harris Corporation purchased Datacraft and renamed it Harris Computer Systems Division. In 1994, Harris Corporation spun off Harris Computer Systems Corporation as an independent public company, which produced computers for the real-time computing market as well as the CyberGuard firewall for the secure computing market. In June 1996, following the sale of the real-time computer business, the company changed its name to CyberGuard Corporation reflecting a business focus on trusted computer systems. The company has two subsidiaries, CyberGuard Europe, Ltd., and CYBG Consultant, Inc."[1.]
(**http://www.cyberguard.com/aboutus/history.cfm**)

The Cyberguard firewall itself is one of the best on the market. Without going into a complete sales pitch, there is little to fault it. It has a list of features hard to beat plus a high accreditation standard. However, there is no such thing as a perfect firewall. [1, 2.]

UPGRADING GUIDES

CD Release Codes

Over the years, like anything else IT related, upgrades are the norm. Listed below is a table showing the various release codes over the years. The PSU (Product Software Update) relates to incremental changes as time has gone past. The code is found printed on the cd itself. I have listed the codes for reference purposes to give an idea of the level for support, and starting from Version 4.3 PSU3. Version 5 PSU 1 is the very latest and should be adopted asap. These are the most common: -

Release x PSU	Code	Date
P3 Knightstar Lancewood	1921	07/25/01
P3 Knightstar Tupelo	1922	07/25/01
P3 Knightstar Tupelo18Gb	1926	12/13/01
P4 Knightstar Tupelo 8Gb	1927	12/19/01
P4 Knightstar Tupelo 9Gb	1928	12/19/01
P4 Knightstar Lancewood	1929	12/19/01
P5 Knightstar Lancewood	1936	04/11/02
P5 Knightstar Tupelo 9Gb	1937	04/30/02
5.1 Knightstar	2602	Build code KQ01031N
5.1 Knightstar Tupelo 9Gb	2603	Build code TQ01031M
5.1 Knightstar Tupelo 18G	2604	Build code UQ01030O

This is not a complete list, but to demonstrate the UNIX builds over the years.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To see which version level the firewall is at; do the following;

1) Open a shell window
2) Type "/sbin/tfadmin newlvl SYS_PRIVATE", and press enter
3) Type " su" and enter, with an appropriate password for root
4) Type " pkginfo –l cgbase "
5) To display the patch release type " pkginfo | grep P[45]x "
6) The gui option is to double click the Cyberguard banner or the drop down menu for ABOUT under the HELP section.

To Upgrade a Cyberguard to Version 5.1

Bullet List for Upgrading Cyberguards from 4.3/5 to 5.1

- Make a KSINIT file for 5.1 using the info /hardware number/ serial number / mouse type / license key and HA information. Use cgadmin for FSO account and password. Take careful note of the heartbeat names and hostnames given.
- Have a floppy with backup~1.enc for version 5.1 (151 kb) copied onto it, ready.
- Backup the existing config onto floppy
  1) tfadmin newlvl SYS_PRIVATE
  2) su and then *password*
  3) cgbackup backup disk (with disk in drive)

NOTE REGARDING BACKUP TO FLOPPY DISK
The file /var/backup/tcpioarc.Z contains all the files that are backed up, which are in a compressed format , ready to be backed up. It does transferral by means of a " trusted CPIO", ie. A RAW trusted format, and there is no FAT on the destination floppy and unreadable in a conventional floppy disk drive using FAT and relying on DOS or Windows.
It is also recommended to do a backup onto the hard drive if one is not going to ghost the firewall; just substitute "disk" with "hard-disk". This uses a different file located in /var/backupdir/backup.cpio
If more than 1 disk is required, something is wrong. Check the directories to see if something large has been copied into there manually prior to upgrading. Often, it is the home directories which are to blame, with miscellaneous files kept there.

- Check settings for NIC's (getmib –l) and FTP log scheduling. Make a note of them. ← critical, as they are lost on the upgrade ! NB !
- Change level to network (newlvl network)
- dosdir a: (check the filename, should be backup~1.enc)
- doscp a:backup~1.enc backupconfig_orders.tar.encr
- Remove the floppy and insert a blank formatted disk.
- From the <system> drop down menu; run <Software Update>
- localhost; /home/FSO account/network
- backupconfig_orders
- FSO account and password
- /var/cgadmin
- encryption ticked and ****** p/w
- Save and Use . The conversion will run and copy files across onto disk.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Click on OK (even though it says update is invoked etc.)
- Remove all disks and ghost firewall to version 5.1
- Insert KSINIT disk after a reboot, using the 5.1 KSINIT html
- Login using the KSINIT FSO account and password,
- Insert disk that has the converted files for 5.1
- Logon as root "su" (password will be 8 last digits of MAC address)
- cginstall , menu, select 4 ; f (floppy) ; once completed; q = quit.
- Select NIC settings to specify interface speed settings from drop down windows
- Check the logging schedules. If these are missing, (more than often, they are) they can be added later after the reboot, from the notes you made earlier.
- Reboot the firewall completely to enable all the settings.
- Check all the configs, especially the heartbeat host names. Eg. 10.10.10.1 and 2.

By the way; state synchronization IS STILL NOT a feature at this level. Only from Version 5 PSU 1 have Cyberguard fixed this with a patch. If a Cyberguard is ghosted to version 5.1 with an evaluation license key, State Synchronization is seen as available on the editor for the packet rule base. HOWEVER, as soon as the firewall is licensed and a key is entered, State Synchronization is then DISABLED. The firewall has to be upgraded to version 5 PSU 1 for State Synchronization to work !!
The temporary work around for this is to manually edit the netguard.conf file.

Here's how to do it

At network level;
Change to /etc/security/firewall/ng_inet
Make a backup copy of netguard.conf
Edit netguard.conf using vi
At whatever rule state synchronization is needed, go to the end of the line and add the word " FAILOVER " to the end of it; eg:

```
Permit    ftp/tcp    FIREWALL    ALL_EXTERNAL     FAILOVER
```

Save the file and exit vi
Execute netguard -p to check for any syntax errors
Go back to the gui for packet filtering rules and make a slight change (add a comment to an existing string of comments – normally a long line), click on use and save. This will force a refresh and replication on both firewalls of a HA pair.
Finally, check /etc/security/firewall/ng_inet/netguard.conf to ensure that the State Synchronization rules have not been removed.
NOTE: If you edit anything again in the gui, the state synchronization rules that have been modified manually using vi in the netguard.conf file WILL BE LOST !

© SANS Institute 2003, Author retains full rights.

- Patch to Version 5 PSU 1 level is highly recommended here, either by Software Update or by package add (unix style)

To upgrade from the base level of Version 5 to Version 5 PSU 1 follow these steps:-

1. Copy the 28Mb PSU1 " conversion script" file on the firewall (either via cd or ftp)
2. Backup of the existing v4.3 configuration is made onto floppy disk(s)
3. "backupconfig_orders.tar.encr" file is transferred to hard disk. This must be done on both the primary and secondary firewalls.
4. Software update initiated which converts & writes the v5.x config onto floppy disk(s)
5. GHOST CD overwrites hard disk with v5.x image & v5.x KSINIT used for basic configuration
6. v5.x config created in step 3) is restored from floppy disk(s)
7. Configuration checks (interface speed)/ tests carried out (must make a note of these in 4.3)

Note: Prior to the upgrade ensure that a supply of fully formatted floppy disks is available for steps 1 & 3. The "cgbackup" command uses cpio "raw" mode to write to disk & media needs to be 100% readable.

Login to the Firewall using a valid FSO account
From the <Tools> menu drop-down run the <Shell Window> option
at the $ prompt enter :
/sbin/tfadmin newlvl SYS_PRIVATE

at the SYS_PRIVATE> prompt enter :
su <enter the current su password when prompted>

at the # prompt enter :
/usr/sbin/cgbackup backup disk

Replace floppy disks as required by the backup program (this will vary depending upon overall size of Firewall rulebase/ configuration etc).

at the # prompt enter :
newlvl network ← critical

at NETWORK> prompt enter :
dosdir a: (or dosls a:) to check the filename on floppy disk
doscp a:backup~1.enc backupconfig_orders.tar.encr

NB: For some strange reason, it has been found that on some Cyberguards, a new FSO user account has to be created for these steps to work. Therefore, if the next few steps don't work, then create a fictitious FSO user just for this upgrade, and then delete it afterwards. It should not take more than 10 mins to do the whole upgrade anyway. I am not sure why, but it did ! It happened on 2 pairs out of over a dozen.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

From the <System> drop-down menu run the <Software Update> option & enter the following –

Remote Host : **localhost**
Remote Directory: **/home/**<FSO directory>**/network**
Remote Filename: **backupconfig_orders**
Remote Username: <FSO user>
Remote Password: <FSO user>
Local Directory: **/var/cgadmin** (default)
Use Encryption box:**ticked**
Encryption password: ********

Click Save and the Use buttons

The conversion orders file will be copied into the /var/cgadmin directory & the automated process will begin (cg_getorders), the Firewall will prompt as necessary for floppy disks to be replaced (depends upon complexity of firewall configuration).

A prompt will indicate "software update has been invoked" & the system will be restarted – this is not correct, just click OK to remove this message.

Note: Remove any backup floppy disks, insert the release v5.x GHOST CD pre-configured v5.x KSINIT floppy disk
Re-boot the Firewall.

When the GHOSTing process has completed remove the v5.x CD and reboot the firewall, allow the firewall to auto-configure from the v5.x KSINIT file.
Insert floppy disk(s) as created in Step 3

Login to the Firewall using a valid FSO account
From the <Tools> menu drop-down run the <Shell Window> option
at the $ prompt enter :
/sbin/tfadmin newlvl SYS_PRIVATE

at the SYS_PRIVATE> prompt enter :
su <enter the current su password when prompted>

at the # prompt enter :
newlvl network

at NETWORK> prompt enter :
cginstall

The *** Cyberguard Firewall Installation and Upgrade *** menu will apear,

Select Menu Option **4** (Restore Configuration Files)

Enter **f** (for restore from floppy media)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

When the configuration files have been restored, you are returned to the menu, exit from menu (q) & close shell window with Ctrl-D's.

This process must be done individually for cg1 and 2. The files are specific to each firewall and not generic.

Open up the Network Interface dialog box off SYSTEM. Select the interface speeds as noted from 4.3. USE and then SAVE. Close Window.

Select SYSTEM again
Select High Availability
Place a tick in the box for "Enable" under "State Synchronization Parameters"
Save and Exit
Reboot the entire firewall for settings to take affect

When installing a Cyberguard firewall into a switched network you may have problems with the Interfaces. By default a Cyberguard will auto detect the speed of the LAN (10 or 100mbps) but it will only run at half-duplex.

In a switched environment where the switch ports are fixed at full-duplex, it may appear that things are working fine, traffic will pass the interface but you'll be clocking up collisions on the firewall and CRC errors on the switch. When lots of traffic is sent through (as in a FTP) you'll suffer from terrible performance.

<u>To hardcode a cyberguard to run dec interfaces at full duplex do the following..</u>

open a shell window
/sbin/tfadmin newlvl SYS_PRIVATE
su
enter root password
cd /etc/dec

(It has been noticed that some of these files are read only, although they say that they are not supposed to be . Try and insert a space and then save the file. If it says its read-only, issue the command " chmod 644 'filename' and then edit the file as per instructions mentioned below. After it has saved, issue the command " chmod 444 'filename' to return the file attributes to what it was originally)

cp dec.conf.tmpl dec.conf
vi dec.conf
At the bottom of the file add the following line(s)
    0   CONNTYPE   TXF

This will configure dec0, for each dec interface you need add a line changing 0 to the dec interface number 1,2,3 etc.

These steps have to be repeated if there is a adptsf interface also.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

THEN YOU NEED TO RE-BOOT THE FIREWALL !!

use the command getmib -l (that's a little L) to interrogate the interfaces,
netstat -in will show the collision count (both commands need to be run from root)

Configuration of eeE0 is a bit trickier.

Restore Steps (config on floppy)

1) If you are not at the console (i.e. you are at GUI login screen), press
<ALt><SYSreq> and then <P>
to get to the console (answer y to close the "virtual terminals" prompt)
2) At the console Login prompt, log in as an FSO
3) # /sbin/tfadmin newlvl SYS_PRIVATE ; su to root & enter password
4) # init 1 to go to single-user mode
5) At the console Login prompt, log in as an FSO again
6) # /sbin/tfadmin newlvl SYS_PRIVATE ; su to root & enter password
7) # doscp a:backup.cpi /var/backupdir/backup.cpio
8) # /usr/sbin/cgbackup restore hard-disk
9) # init 2

To obtain files for an office based security audit [3.]
There are 4 files that are useful for the purpose of doing a manual inspection security audit. Therefore, copy these off the firewall using the doscp command into txt formats.
/etc/inet/hosts (these are the hostname mappings)
/etc/security/firewall/ng_inet/netguard.conf (the rulebase)
/etc/security/firewall/ng_inet/netguard.exempt.conf (these are the exempt interface rules)
/etc/security/firewall/netguard.group (these are rulebase groups)

Additional files which are useful to check are networks; services; startup.conf; ha.conf; if.conf; routes.conf; nat*.conf; proxy and dns directories.

To set the speed of the onboard interface
This interface is in theory, auto sensing. However, as usual, not always. This is the manual way of forcing it:-
#/etc/conf/pack.d/eeE/space.c

Check the speed settings listed here. Something like eeE_speed_duplex=[0,0,0,0]

If the first 0 is changed to 4, then it will use full duplex. Then reboot in mUnix
/etc/conf/bin/ibuild –M eeE
init 6

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To Uninstall a service pack on a Cyberguard Firewall
Type the following commands:-

Boot mUnix
Kernel =mUnix
INITSTATE=1
Go
Log on as root in single mode
#pkgrm " package id" , eg. P43p5 (this is version 4.3 PSU 5)
Init 6

TROUBLESHOOTING and TUNING

To quickly check for errors for failed traffic
#cd /etc/security/firewall/ng_inet
#netguard –f netguard.conf (this command will parse the rulebase, groups, proxies, hosts, HA config etc. and outputs a list of critical messages)

If any errors are seen (NOT warnings), note the number listed as the line number. This is the reason why netguard is not running and is failing to load and will DENY all packets on the firewall !!!
Use vi to edit the netguard.conf file and go to the line corresponding to the error message ; type " :xxx ", where xxx = line number.
This will give you an accurate indication as to the problem. Don't edit this file directly.
After the problem has been fixed, restart netguard; type
#netguard –r; (this reloads netguard to start the daemon again) and then
#netguard.

Netguard is one of the most useful commands to use on a Cyberguard firewall and a thorough knowledge of its effectiveness will save hours of heartache and time (along with tcpdump and grep | etc.).
Know the switches which can be used; here are a few:-
(typing #netguard -- help ; will list the switches for you)
(-n avoids the name-to-address lookups via any name server around and displays addresses in numeric format)

#netguard –An ; displays all the current sessions which are traversing the firewall
#netguard –n –S all ; this displays the curses of current packet-filtering traffic
#netguard –p ; checks for errors in the configuration file (netguard.conf)

The other function most useful for any administrator is under Tools -> Packet Trap. Here one can specify the packet source, destination, the port (the default is ALL), the interface, max packet count, and plenty more for trapping data traffic going through the Cyberguard.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Useful Troubleshooting commands for Cyberguard network or Interface Problems

Make sure you are at the NETWORK level when issuing commands that have to do with interaction with NIC's, sockets or protocol modules etc. You do this by issuing the command

#newlvl network

/usr/sbin/ifstat shows that each of the interfaces on the firewall have the correct security status

resmgr –m dec –p "BUSNUM DEVNUM" will indicate the NIC's are in the proper sequence in the Resource Manager database. The key-pairs should be in the ascending order.

#getmib –l also tells immediately which interfaces are up and just as importantly, the duplex speeds that they are running. Version 5 now has the gui drop down menu to easily change this, but requires a system re-initialization.

To make sure that multiple NICs are in the proper sequence in the Resource Manager database: **run resmgr -m dec -p 'BUSNUM DEVNUM'**, and verify that the **<BUSNUM,DEVNUM>** key-pairs are in ascending order. If they are not, the interface unit number assignment (i.e., the interface name to physical port association) is incorrect with respect to the CyberGuard installa-tion documentation, and ultimately, NICs may be connected to the wrong net-works. In this unlikely event, the following should be performed (UnixWare only):

a. Run **resmgr -r -m de**c, once for each dec NIC (until all entries have been deleted).

b. Run **/etc/conf/bin/idconfupdat**e, to save these changes.

c. Reboot the system to re-add the NICs to the Resource Manager in the proper sequence.

.Carefully check the output of **ifconfig -a** and **netstat -i**n, to make sure the interfaces are up and configured correctly. Of course, netstat output also indi-cates whether any frames are even coming into or going out from the inter-faces, and whether errors are occurring on the interfaces.

Run **netstat -s -p** *protocol* (where *protocol* is **icm**p, **i**p, **tc**p, or **ud**p) to display statistics collected on the specified protocol.

.Run **netstat -rn** to display the available routes. For each configured NIC, there must be what is known as an *interface route*, where the following con-ditions are true:

- Destination = *NIC IP address* AND *NIC netmask*
- Netmask = *NIC sub-network mask*
- Gateway = *NIC IP address*
- Flags = U
- Interface = *NIC interface name*

Run **rtpm** to display operating system performance metrics and usage infor-mation. Select the **ETHER:** sub-screens to display specific NIC error statis-tics. Select the **TCP/IP:** sub-screens to display numerous statistics collected on ICMP, TCP, IP, and UDP. (UnixWare only)

.To display more specific NIC error statistics, for example, for dec1, run **/usr/sbin/getmib -d/dev/dec**_1. This utility is installed on the CyberGuard

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Run **netguard -An** to display all current sessions traversing the firewall. Run **netguard -n -S all** for a curses-based display of current packet-filtering traffic.

Run **tcpdump -n -p -i dec0** to display network traffic addressed to dec0.
The **-p** option turns off promiscuous mode.
Run **tcpdump -n -i dec1** to dis-play all network traffic on the collision domain to which dec1 is attached.

Example of some Cyberguard "tcpdump" commands [4.]

Description : Capture all packets to or from host 192.168.0.11 on i/f dec3
Syntax : **tcpdump -nvvi dec3 host 192.168.0.11**

Description : Capture all arp packets on i/f dec2
Syntax : **tcpdump -nvvi dec2 arp**

Description : Capture all udp type packets on i/f adeptec adptsf0
Syntax : **tcpdump -nvvi adptsf0 udp**

Description : Capture all tcp type packets on i/f adeptec adptsf1
Syntax : **tcpdump -nvvi adptsf1 tcp**

Description : Capture all packets from any host to any destination using dest port 80 (on i/f adptsf1)
Syntax : **tcpdump -nvvi adptsf1 dst port 80**

Description : Capture all packets from any host to dest host 192.168.3.40 dest port 80 (on i/f dec3)
Syntax : **tcpdump -nvvi dec3 dst host 192.168.3.40 and dst port 80**
Description : Capture all packets to or from host 192.168.0.110 to any dest using dest port 80 (on i/f adptsf1)
Syntax : **tcpdump -nvvi adptsf1 host 192.168.0.110 and dst port 80**

Description : Capture all packets to or from host 192.168.2.10 to any dest using dest port 443 (on i/f adptsf3)
Syntax : **tcpdump -nvvi adptsf3 host 192.168.2.10 and dst port 443**

Description : Capture all packets from any host to any destination using source port 7000 (on i/f adptsf3)
Syntax : **tcpdump -nvvi adptsf3 src port 7000**

Description : Capture all packets to and from Ethernet address xx:xx:xx:xx:xx:xx on i/f adptsf1
Syntax : **tcpdump -nvvi adptsf1 ether host 00:00:0c:07:ac:74**

Description : Capture all packets to or from host 192.168.0.77 on i/f dec1 that is to or from port 53
Syntax : **tcpdump -nvvi dec1 host 192.168.0.77 and port 53**

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Description : Capture all packets from host 192.168.0.77 on i/f dec2 to or from tcp port 53
Syntax : **tcpdump -nvvi dec2 src host 192.168.0.77 and tcp port 53**

Description : Capture all ICMP packets that are echo requests or replies (ping packets) on i/f adptsf2
Syntax : **tcpdump -nvvi adptsf2 \(icmp[0] =8 and icmp[0] =0\)**

Description : Capture all packets to or from host 192.168.0.77 on i/f dec5 that are using src or dest port 1433
Syntax : **tcpdump -nvvi dec5 host 192.168.0.77 and tcp port 1433**

Description : Capture all packets to or from host 192.168.0.77 on i/f dec1 to or from udp port 137
Syntax : **tcpdump -nvvi dec1 host 192.168.0.77 and udp port 137**

Description : Capture all packets from host 192.168.0.77 on i/f dec1 that is not to or from port 6000
Syntax : **tcpdump -nvvi dec1 src host 192.168.0.77 and !port 6000**

Description : Capture all ICMP packets that are not echo requests or replies (not ping type packets) on i/f dec2 (this will also capture other icmp types)
Syntax : **tcpdump -nvvi dec2 \(icmp[0] !=8 and icmp[0] !=0\)**

Description : Capture full length packets to or from host 192.168.0.37 on i/f dec2
Syntax : **tcpdump -nvvi dec2 –axs 1500 host 192.168.0.37**

The screen output of the tcpdump can be written to a file in parallel using the following syntax (note there are 2 x <u>single</u> quotation marks at the beginning and end of the command line) –

``tcpdump –l <original parameters> | tee > /tmp/filename''

e.g.1 ``tcpdump –l -nvvi adptsf1 host 192.168.0.110 and dst port 80 | tee > /tmp/http1.txt''
e.g.2 ``tcpdump –l -nvvi adptsf2 host 192.168.20.47 and port 53 | tee > /tmp/dns1.txt''

The –l (el) parameter allows buffered line output & produces a delay of 2-3 seconds before data is displayed on the screen & written to disk, the above traces are single line data captures i.e. data content is not captured – only headers etc.

To review the data captured use #**more /tmp/http1.txt**
To move this data onto floppy disk use **#doscp /tmp/http1.txt a:**
If the data file is too large to copy to floppy i.e. > 1.44MB then use **#compress /tmp/http1.txt** which will produce a file in the **/tmp** directory of **http1.Z** (the original .txt file will no longer exist). The new file produced can be uncompressed using normal WinZip when required.

The compress utility generally reduces the dump out by 8-10 times so it's possible to capture approx 11MB of data to 1 floppy, it can also be spanned if needed by using the **tar** command.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Try to run as few tcpdump processes as possible for the data you require, 2 simultaneous captures should be considered the maximum on a live platform (6 have been tested producing 30-40% CPU loading – max no. depends upon CPU usage at time of capture & how heavily utilized the firewall is).

Data can also be captured and written to disk using the following alternative syntax (this is for full length
packet capture) –

tcpdump -nvvi dec1 -axs 1500 -w /tmp/dec1out.bin

The above syntax forces a full packet capture (including payload) of all packets on interface dec1 and writes the data to a binary output format file that can then be re-interpreted by tcpdump (there is no screen output), this is used for full packet capture/ high performance use – run this for brief periods only (10-15 seconds) due to the processing overhead required & disk space used.

Additional Notes :

-n don't convert addresses/port numbers to names **-vv** use even more verbose header output
-i use i/f xxxx, otherwise lowest will be used by default **-p** don't put i/f into promiscuous mode
-t don't print a timestamp on each line **-l** buffered output

**** character = # key
| character = Shift + the # key

tcpdumps should be carried out under "newlvl NETWORK" access rights level.

Terminate tcpdump sessions using Ctrl-C sequence, data being written to file will be buffered and saved to disk
correctly.

Log files
Nobody needs to underestimate the value of these. Log file management on a Cyberguard is just as important, for both Binary (located in /var/audit) and ASCII (located in /var/audit_logs). Depending on the logging activities of the firewall and the amount of traffic passing through, the size of the log files can compromise the amount of free space on the /var partition where they reside. If it reaches 100% (70% is the highest maximum suggested utilization threshold), then the firewall will stop passing traffic and shutdown.

Read Only Mode in GUI of standby firewall (for experienced users only)
This is a wicked tip, but saves eons of time. By default, the standby firewall is in a read only state. To manually over-ride this status:-

1. $ tfadmin newlvl SYS_PRIVATE and su to root
2. # rm /etc/security/firewall/.inactive
3. Log out of the gui and log back on. Now you will have write access.
4. Touch the file again to restore the attributes.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HA – HIGH AVAILABILITY ISSUES

These packages work by monitoring the heartbeat interfaces. These can be difficult to troubleshoot, especially if the firewalls are far apart from each other, maybe located in redundant comms rooms (which will be affected by the cable distance limitations of Ethernet CAT5) . If it does not function as expected, then perform some tests like the following:-

1) On version 5 and up, a quick test is to choose System -> High Availability and in the boxed section of " Replication Status", click on the box labelled "Refresh". The box next to it, in amber, should turn to green and display a "successful" indication.
2) Check the date and time, which need to be the same on both.
3) See if you can ping the other firewall heartbeat interfaces (use the in-built ping box located under Tools -> Network Ping Test) . You should be able to do so. Ie. The active could be 10.10.10.1 and the other standby side could be 10.10.10.2, plus it could have 2 heart beats, with another pair on 10.10.11.1 / 2. Typing ifconfig –a from a shell window will give you the network settings.
4) Change to /var/cgha/ and enter "ls –a". Look for a file called " . version " It should look something like 62964 1. This number needs to be exactly the same on both the active primary and standby secondary firewalls. The long hard way is to select Reports -> System Information -> drop down to Installed Packages List and then compare these. They have to be identical.
5) Type pkginfo | wc and this will list the lines of code, which also need to be the same on both. Check that both build versions are identical.
6) The date and time on both firewalls must also be the same
7) Check the log files, /var/adm/syslog contains information regarding configuration replication
8) Lastly, check the HA logging file under /var/adm/log/qhap.log. It should give you some clues as to the failure.

<u>To force a synchronization to a HA pair</u>

If one firewall in a HA pair has had to be replaced, it is possible to rebuild it very quickly.

1) 1)After a re-ghost and KSINIT file, take it in off-line mode with no cables plugged into it. Go to HA Monitor screen and select "f" .
2) Plug ONLY the heartbeat cables into the respective interfaces
3) On the running primary active firewall, open a shell prompt and log on as root
4) Type # changed –sync and enter
5) Wait for the configuration to be replicated across to the standby firewall (this takes a few mins)
6) Now plug all the other cables into the interfaces of the standby unit
7) Bring the standby unit into " on-line mode " in the HA Monitor window. Make sure they are in a HA mode. The border colour should change to an amber colour on the standby secondary firewall as a quick eye check. Click on System -> HA -> under the box Replication Status, select Refresh, which will change the status box to green and give a successful indication.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

There are many other areas and issues to consider; such as VPN, CSmart logging, arp issues (gratuitous) – there has been a problem whereby the cached ip address is not released from a firewall failover on a redundant switch located upstream and causes chaos (solved by issuing the tcpdump –envvi xxxinterface and see the MAC address is correct etc.) , proxy issues, etc. all due for consideration in maintaining and administering Cyberguard firewall appliances.

REFERENCES

1. Cyberguard references
   http://www.cyberguard.com/home/index.cfm
   http://www.cyberguardcorp.com/home/index.cfm
   http://www.bluesky.com.au/Products/CyberGuard/index.html
   26 reasons to buy a Cyberguard:-
   http://www.bluesky.com.au/Products/CyberGuard/Comparisons/CyberGuard26reasons.pdf
   http://www.icsalabs.com/html/communities/firewalls/newsite/certification/vendors_4/CyberGuard/cyberguard.pdf

2. Accreditation
   http://niap.nist.gov/cc-scheme/ST_UK-0001-AMAv5.1.html

3. Auditing firewalls
   http://www.itsecurity.com/papers/p5.htm

4. Tcpdump commands
   http://publib16.boulder.ibm.com/pseries/en_US/cmds/aixcmds5/tcpdump.htm
   http://www.tcpdump.org/
   http://www.tcpdump.org/tcpdump_man.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced