Alteon Firewall 5100 Series 2.2.7.0

Upgrading

part number: 318723-A, September 2004

4655 Great America Parkway
Santa Clara, CA 95054
Phone 1-800-4Nortel
http://www.nortelnetworks.com

Upgrading to ASF 2.2.7.0

These configuration notes provide information on how to upgrade the Alteon Firewall 5100 Series (models ASF 5105, ASF 5106 ASF 5109, ASF 5112, ASF 5114, and ASF 5124) for release 2.2.7.0.

The following topics are addressed in this supplement:

Documentation

For more information on the *Alteon Firewall 5100 Series 2.2.7, r*efer to the following documents:

- *Alteon Firewall 5100 Series 2.2.7 Release Notes* (p/n. 213456-N)
- *Alteon Firewall 5100 Series 2.2.5 User's Guide and Command Reference* (p/n. 213455-J)
- *Alteon Firewall 5100 Series User's Hardware Installation Guide* (p/n. 216382-B)
- *Alteon Firewall 5100 Series BBI Quick Guide* (p/n 216383-B)

The manuals are PDF files that can be read and printed using the free Acrobat Reader software available from Adobe Systems Incorporated (http://www.adobe.com).

To access a manual, open the "`welcome.pdf`" file on the *Alteon Firewall 5100 Series Documentation* CD-ROM and select a title. When the manual opens, you can navigate through it by selecting the bookmarks on the left side of the window or by scrolling through the pages.

You can also download the manuals from the Nortel Networks Technical Support Web site. To access the site, follow the procedure in the Release Notes, but select **Documentation** instead of **Software**. The Documentation page will open sorted by date. Click on a title to open it in your browser.

To reduce clutter on the Documentation page, click on the **Rls** header. This will sort the page by Release and omit any document that doesn't have a Release version.

Upgrading in a Standalone Environment

1. **Perform a remote backup of the ASF 5100. You can use the backup to restore the configuration (clone) in case you have problems during upgrade.**

   `/cfg/sys/backup/bckremote`

2. **Obtain the ASF5100_2.2.7.0_FP4.pkg file and copy it to an FTP server.**

3. **Verify that you have rules to allow ping and FTP from the firewalls to the FTP server.**

4. **Verify that the firewalls can ping the FTP server.**

   `ping` *<IP address of ftp server>*

5. **Login into the firewall using the** `admin` **account and check the current version of the software as shown below.**

```
>> Boot# software
------------------------------------------------------------
[Software Management Menu]
      cur         - Display current software status
      activate    - Select software version to run
      download    - Download a new software package via TFTP/FTP
      del         - Remove downloaded (unpacked) releases
>> Software Management# cur
Version              Name            Status
-------              ----            ------
2.2.5.0              tdo             permanent
```

6. **Download the ASF5100_2.2.7.0_FP4.pkg file from the FTP server (only anonymous ftp is supported) using the following CLI commands:**

```
/boot/software/download
>> Software Management# download
Select TFTP or FTP (tftp/ftp) [tftp]: ftp
Enter hostname or IP address of server: 172.17.124.46
Enter filename on server: ASF5100_2.2.7.0_FP4.pkg
Received 53212760 bytes in 4.0 seconds

Unpacking...
ok
```

7. **When the download is complete, check the current versions of the software. The version that you downloaded has a status unpacked.**

```
>> Software Management# cur
Version              Name            Status
-------              ----            ------
2.2.7.0              tdo             unpacked
2.2.5.0             tdo             permanent
```

8. **Activate the new (unpacked) version software with the following command in the CLI:**

```
/boot/software/activate 2.2.7.0
```

9. **Do not disturb the system until it reboots.**

```
>> Software Management# act
Enter software version to activate: 2.2.7.0
Confirm action 'activate'? [y/n]: y
Activate ok, rebooting
[root@a172-17-161-10 root]# cbd[15621]: ALERT: signal handler(15)
detected. CLI may not work properly. Exiting...
Restarting system.
```

10. **The firewall will reboot after a couple of minutes. The status of the new software version changes from unpacked to permanent and the older version changes from permanent to old as shown below:**

```
>> Software Management# cur
Version              Name            Status
-------              ----            ------
2.2.7.0              tdo             permanent
2.2.5.0             tdo             old
```

11. **From the Management Server, change the version of the Check Point™ Gateway Object if needed.**

12. **If you are using centralized Check Point license, re-attach the licenses using Smart-Update.**

13. **Push the Policy to the firewall.**

Time for a Standalone Upgrade

Table 1 shows the time it takes to upgrade a standalone configuration. Use Table 1 to plan the downtime for your firewall.

Table 1 Time to Upgrade a Standalone Configuration

Platform	Download Time in minutes	Active and Reboot Time in minutes	Estimated Total time in minutes
5106	5	10	15
5109	2	4	6
5114	2	4	6
5124	2	4	6

Upgrading in an High Availability Environment

1. **Perform a remote backup of both ASF 5100s. You can use the backups to restore the configuration (clone) in case you have problems during upgrade.**

   `/cfg/sys/backup/bckremote`

2. **Obtain the ASF5100_2.2.7.0_FP4.pkg file and copy it to an FTP server.**

3. **Verify that you have rules to allow ping and FTP from the firewalls to the FTP server.**

4. **Verify that the firewalls can ping the FTP server.**

   `ping` *<IP address of ftp server>*

5. **Login into the firewall with the MIP (you can find the firewall holding the MIP by running the CLI command** `/info/summary` **and note the firewall with the *), using the**

`admin` **account and check the current version of the software. The output displayed is shown below.**

```
>> Boot# software
------------------------------------------------------------
[Software Management Menu]
      cur         - Display current software status
      activate    - Select software version to run
      download    - Download a new software package via TFTP/FTP
      del         - Remove downloaded (unpacked) releases

>> Software Management# cur
Version               Name            Status
-------               ----            ------
2.2.5.0              tdo             permanent
```

6. **Download the ASF5100_2.2.7.0_FP4.pkg file from the FTP server (only anonymous ftp is supported) using the following CLI command,** `/boot/software/download`**. The output is shown below:**

```
>> Software Management# download
Select TFTP or FTP (tftp/ftp) [tftp]: ftp
Enter hostname or IP address of server: 172.17.124.46
Enter filename on server: ASF5100_2.2.7.0_FP4.pkg
Received 53212760 bytes in 4.0 seconds

Unpacking...
ok
```

7. **After the download is complete, check the current versions of the software and you see that the version you downloaded has a status unpacked.**

```
>> Software Management# cur
Version               Name            Status
-------               ----            ------
2.2.7.0               tdo             unpacked
2.2.5.0              tdo             permanent
```

8. **Disable the firewall, Check Point Sync and HA/AA/ClusterXL by running the following CLI command.**

```
/cfg/fw/dis
/cfg/fw/sync/dis
/cfg/net/vrrp/ha n
/cfg/net/vrrp/aa n
/cfg/net/vrrp/clusterxl n
apply
```

NOTE – The commands `/cfg/net/vrrp/aa` and `/cfg/net/vrrp/clusterxl` may not be available in some older versions of the Alteon Firewall 5100 series.

9. **Wait for 2-3 minutes, because SSI (the clustering application) takes time to re-initialize.**

NOTE – If you are upgrading from version 2.1.1.0 or 2.2.1.0 FP3 images, run the `fw unload local` command at the root prompt on both the firewalls.

10. **Enter the CLI command (`/info/summary`) to make sure both firewalls are `up`.**

11. **Activate the new (unpacked) software version software by running the following command in the CLI:**

```
/boot/software/activate 2.2.7.0
```

12. **Do not disturb the system until it reboots.**

```
>> Software Management# act
Enter software version to activate: 2.2.7.0
Confirm action 'activate'? [y/n]: y
Activate ok, rebooting
[root@a172-17-161-10 root]# cbd[15621]: ALERT: signal handler(15)
detected. CLI may not work properly. Exiting...
Restarting system.
```

13. **Both the firewalls reboot after a minute or two. The status of the new software version changes from unpacked to permanent and the older version changes from permanent to old as shown below:**

```
>> Software Management# cur
Version               Name            Status
-------               ----            ------
2.2.7.0               tdo             permanent
2.2.5.0              tdo             old
```

14. **Enable the firewall by entering the following CLI command and wait for couple of minutes to start the Check Point daemons.**

```
/cfg/fw/ena/apply
```

15. **From the Management Server, change the version of the Check Point Cluster Object if needed.**

16. **If you are using centralized Check Point license, re-attach the licenses using SmartUpdate.**

17. **Push the Policy to both the firewalls and make sure both firewalls are UP in the** `/info/summary` **menu.**

18. **Enable the Check Point Sync and HA/AA/ClusterXL by entering the following commands.**

```
>> Firewall Configuration# /cfg/fw/sync/ena
Current value: n [y]
Enabling sync may reboot all SFDs when you apply. Are you sure (y|n)?
y

>> Sync Configuration#/cfg/net/vrrp/ha y/apply
[Note: Enable HA, AA or ClusterXL depends on your configuration]
```

19. **The system automatically reboots to enable the Check Point Sync.**

20. **After the system comes back, wait for 3-6 minutes for firewall and Check Point sync to start properly.**

21. **Check the status of the cluster by running the `/info/cluster` command as shown below:**

```
>> Main# /info/clu
IP Address :172.17.161.9 [MIP] [Up]
Health Report as of Tue Aug 24 05:36:58 2004
        Runtime Information...
                Hard disk usage[Read/Write partition]: 35 %
                Memory usage 16%
                CPU Load:  0%

        Application status.
                Webserver
                Running for 0Hrs 0Mins 59Secs

                SNMP
                Not running..

                Check Point Firewall-1
                Running for 0Hrs 0Mins 30Secs

                Inet server
                Running for 0Hrs 1Mins 46Secs
IP Address :172.17.161.10 [Up]
Health Report as of Tue Aug 24  05:37:08 2004

        Runtime Information...
                Hard disk usage[Read/Write partition]: 35 %
                Memory usage 41%
                CPU Load:  64%

        Application status.
                Webserver
                Running for 267Hrs 7Mins 4Secs

                SNMP
                Not running..

                Check Point Firewall-1
                Running for 175Hrs 22Mins 53Secs

                Inet server
                Running for 267Hrs 7Mins 51Secs
```

22. **Verify that Check Point sync is working properly.**

    - Login as root

- Run `cphaprob stat`
- You should see both firewalls active
- If sync is not up, do a soft reboot of the firewalls sequentially

23. **Open the Check Point logs to verify that data traffic is forwarding properly.**
24. **Verify that VRRP active-active is working properly by entering the following CLI command** `/info/net/vrrp/status`.

Time for a High Availability Upgrade

Table 2 shows the time it takes to upgrade a high availability configuration. Use Table 2 to plan the downtime for your firewalls.

Table 2 Time to Upgrade a High Availability Configuration

Platform	Download Time in minutes	Pre-upgrade Configuration	Active and Reboot Time in minutes	Post-upgrade Configuration	Estimated Total time in minutes
5106	5	3	10	9	27
5109	2	2	4	3	11
5114	2	2	4	3	11
5124	2	2	4	3	11