Global Information Assurance Certification Paper

Upgrading Check Point FireWall -1â Version 4.1 to the Latest Service Pack

Enyuan Wu
May.22 2002
Practical Assignment Version: 1.4

Introduction
In one typical enterprise information security environment, we always implement firewalls to guarantee the Inter net/Intranet/Extranet security. Checkpoint VPN -1/Firewall-1® Version 4.1 is one of the most -used firewall products in current information security market. One of the most important methods to enhance the overall state of enterprise security is to keep all those systems up-to-date with latest Service Packs/Patches.
This topic -Upgrading Checkpoint VPN -1/Firewall-1® Version 4.1 to the latest Service Pack-seems very simple as I at first decided to write, but when I reviewed the whole procedure I did, I found so me valuable points to share with the professionals in the security field. This article is based on my practical experience, and it focus itself on the whole procedure on how to upgrade the Checkpoint VPN -1/Firewall-1 ® Version 4.1 to the latest service pac k. It covers what I did, what problem I met, how I found the solution, what suggestion I can give. The conclusion is that testing all those service pack(s) or hot fix (es) before implementing them into productive environment. I hope this article can be use d as one sample document for those system security administrators on this topic.

Declaration
All the products and trademarks belong to their respective company. All the hostnames mentioned in this article are taken as imaged, if same or similar with yours, they should be treated as occasional.

Conventions
In order to simplify the problem description, here list some conventions used in this article.

- Hostnames. In one typical firewall environment, there are at least one management station, one and/or more firewall enforcement points. All those modules can be installed on one physical machine. In this article, I will use ONLY 2 physical machines to implement separate firewall functions to demonstrate the whole procedure. The method could be expanded to more complex firewall environment as business -need. Hostname: **fw_mgt** means Firewall management workstation; **fw_ep** means Firewall Enforcement Point.

The Problem
Applying Service Pack or hot fix is one of the most powerful countermeasure against the security threaten. In information security field, Service Pack and hot fix are 2 very common words we always hear. Vulnerabilities in operating systems and applications are found and reported almost everyday in the popular security websites, TV, newspapers and magazi nes. In order to fix those vulnerabilities, the companies have to react quickly and produce the hot fixes or service packs to patch those products in

order to keep the high-level security standard, however, after patching, those service packs or hot fix maybe cause other new vulnerabilities, then new service packs and hot fixes come later and again! So keeping your systems pace up with the newer service packs is not an easy thing, it needs continuous effort!
Different Firewall Versions or Service Pack levels coexistence is common. Due to the historical reasons or other factors, in firewall environments, hardware platforms are changed, and operating system are upgraded, and the firewall modules are installed at different time with different versions. One day, when you review the products version and/or service packs level, which are used in productive environment, you are astonished that they fall far from the current status! What you should do —Upgrade to the latest Version or Service Pack anyway! Obviously, if you let your systems run like this, the hacker/hostile attacker can take advantage of the published vulnerabilities to make "fun" on those systems, that is really one big threaten to the enterprise information security. But if you take careless action to do the upgrade, it could be also dangerous to the security infrastructure —maybe you will break down the Internet connection out of the plan, or you will screw up your rule bases, or you have to drop yourself in one over-time nervous work, even get negative impact on your career.
How to implement the service packs and hot fixes correctly and efficiently? This is one common question, which many system administrators face. Here I would like to give my answer to this question. I hope it will be one of the best practices.

The Solution
Checkpoint VPN-1/Firewall-1 ® can be implemented on many Unix Platforms and Windows NT/2000. So it is necessary to outline the technical environment about the solution here before proceeding on:

- Unix Platform: Solaris 2.6 and 2.7 on SUN Workstation
- Firewall: Checkpoint VPN-1/Firewall-1 ® Version 4.1 SP0 and SP2
- Service Pack: Checkpoint VPN-1/Firewall-1 ® Version 4.1 SP5
- Hot Fix: Checkpoint VPN-1/Firewall-1 ® Version 4.1 RDP Hot fix

Ways to apply Service Pack
In general, there are 2 different ways to apply the service pack or hot fix. One is direct untested implementation in productive environment. This is strongly forbidden, but it really happened in reality. We experienced such scenario several years ago, one external service company helped us to implement one service pack upgrade without test, then we had problem and had to work through the whole night to solve the problems and make the firewall work again! The other way is to test carefully before implementation. The following will describe this detail solution.

1.Set up goal
Upgrading Firewall Modules to the latest Service Pack. According to the Checkpoint product support specification, for Checkpoint VPN-1/Firewall-1 ® Version 4.1, the latest Service Pack version is SP5.

2.Define action scope

According to the assumption, we have only 2 physical machines to be covered by this upgrade. The hostnames are as following:

- fw_mgt Firewall Management Station
- fw_ep Firewall Enforcement Point

3.Service Pack Status Statistics

Before we do some improvement on the systems, we should investigate the current status. In this statistics, you had better cover the system information as much as possible, for example: the hardware platform, architecture, operating system versions and so on.

Here is the sample table (Table 3 -1):

Firewall	H/W & S/W	Check Point VPN-1(TM) & FireWall-1(R) Version	Service Packs Level
fw_ep	SUN E220r, SunOS 5.7	Version 4.1 Build 41439 [VPN + DES]	SP0
fw_mgt	SUN E250, SunOS 5.6	Version 4.1 Build 41716 [VPN + DES]	SP2

Note:

- We can run the **uname –a** and **fw –ver** command to get these information.
- Checkpoint VPN-1/Firewall-1 ® Build Number and Service Packs Mapping Table, please refer to the appendix A. This mapping table is quoted from the FW-1 FAQ website www.phoneboy.com. If you need up-to-date information, please visit the website.

4. Expected Result

All those above-mentioned Firewall Modules will be upgraded to the Service Pack 5 (**Build 41510**).

Note: The kernel version of the Solaris installation should be **Build 41512** (**fw ver -k**)

5.Installation Preparation

5.1 Define Installation List

As customer of Checkpoint, you need at least the Software Subscription support service to download the necessary servic e packs, hot fixes and other software packages from this website http://www.checkpoint.com/cgi -bin/download.cgi
After you order software subscription, you will get the username and password to access this website.

There are 2 Installation lists for you to select:

- Vpn_Des SP5 Installation List

(Detail list are omitted, they are Service Packs, related hot fixes and related Release Notes)

- Vpn_Strong SP5 Installation List

(Detail list are omitted, they are Service Packs, related hot fixes and related Release Notes)

Which list should we use? The following are the evaluation standards:

- These 2 Installation lists are for Checkpoint VPN -1/Firewall-1 ® different encryption level. Checkpoint VPN -1/Firewall-1 ® Version 4.1 support 4 levels of Encryption-None, VPN, VPN+DES and VPN+DES+Strong (Strong means 3DES). VPN+DES+Strong is only allowed in United States and Canada and other customers with special permits.
- Normally these 2 Vpn_Des and Vpn_Strong installation list should be applied on the same encryption level as that of the original firewall module. The encryption level of the firewall module can be queried with command fw ver.

According to the current encryption level of the firewall modules (refer to Table 3-1), we need to download the Vpn_Des installation list.

5.2 Refine Installation List

The installation list contains the SP5 and other 2 hot fixes (LDAP/VPN Patch and RDP Patch), those hot fixes are always service pack dependent, and not all the hot fixes need to be installed on firewall modules.

Which package in the list should we adopt?

- The SP5 should be applied basically. It is the core package.
- Dependant on the hot fix's target and your requirement.
- Reading through all those related Release Notes carefully helps to decide which one should be installed.

Here is the list we adopt:

- Checkpoint VPN-1/Firewall-1 ® Version 4.1 Service Pack 5
- Checkpoint VPN-1/Firewall-1 ® Version 4.1 SP5 RDP Hot fix (RDP Vulnerability Binary Replacement)

5.3 Download Service Pack and hot fix

According to the refined installation list, download all those packages and burn them on the CD.

5.4 Define Installation procedure

This step is one of the most important steps to reach our goal. The Service Pack and hot fix release notes already contain one general installation instruction on all supported platforms. This is true, but not enough!

I strongly recommend you to follow the process to define the installation procedure first before you take action in productive environment!

- Read through service pack and hot fix release notes carefully, especially the installation guide, draw one draft version of installation procedure meeting your own environment requirement.
- Test the draft installation procedure in integration (te st) environment and correct and refine it.

The following procedures are based on the practical experiment and modified and tested through the test environment, and later they are verified and successfully implemented in the productive environment.

5.4.1 VPN-1/FireWall-1 SP5 Installation Procedure

1. Download the zipped files and burn on CD.
2. Copy zipped files into the destination machines to temporary directory. (For example: $FWDIR/tmp or /tmp directories) (mount, cp –p).
3. Gunzip and untar the file under the temporary directory. (gzip –d and tar xvf)
4. Make the tar backup for the 2 directories: $FWDIR/bin/* and $FWDIR/conf/*. Because these 2 directory are very important for restore or back out. (tar cvf)
5. Change to the parent directory of CPFWSP410005 -01 and run the patchadd command, giving as an argument the name of the CPFWSP410005 -01 directory: **patchadd CPFWSP410005 -01**. The installation script will check the fw process whether it is running or not, if it is running, it will stop the process first. During the installation, the script will backup $FWDIR/conf/* again. (patchadd <DIR>)
   Note:
   1) Use command patchadd, not pkgadd. There are some problems raised from misusing the command.
   2) In case of backout, remember not to use -d parameter with patchadd command. Patchadd command with –d does not back up the files to be patched. So the installed patch cannot be removed.
6. Reboot the machine directly. After installation, it will warn you to reboot the machine without activating any firewall -related commands (sync; in it 6).
7. Soft restart the firewall (fwstop; fwstart). And you will notice the firewall module can load the rule base locally.
8. Check the firewall version (fw ver [–k]).

What does Service Pack 5 Installation do on the system?
During the SP 5 installation proc edure, 3 shell scripts (prepatch, installpatch, postpatch) are called accordingly. They fulfil different functionalities as following:

1) The script: prepatch is called firstly and it will mainly
   1. Stop the FireWall-1, if it is running.
   2. Save objects & configurations - backup objects.C and conf directory
   3. Backup other necessary configuration files

2) The script: installpatch is called secondly and it will mainly
   1.Copy the patch files on disk
   2.Check all relevant conditions and a pply the package files accordingly.

3.Write the installation log

3) The script: postpatch is called at last and it will mainly
1. Merge objects.C
2. Merge ifdev file, if necessary
3. Restore and modify some configuration files

5.4.2 VPN-1/Firewall-1 Version 4.1 SP5 RDP Hot fix Installation (Binary Replacement)

As the release note mentioned, this hot fix is Service Pack specific; it is available for FireWall-1/VPN-1 4.1 SP5. Users with running a version of 4.1 prior to SP5 should first upgrade, then apply this hot fix. This means we should do the SP5 installation first and successfully, then run this procedure. This dependence we should give more attention!

1. Download the zipped files and burn on CD.
2. Copy zipped files into the destination ma chines to temporary directory. (For example: $FWDIR/tmp or /tmp directories) (mount, cp –p).
3. Gunzip and untar the file under the temporary directory and you will find ONLY one executable file (fw) in this package. (gzip –d and tar xvf).
4. Change the ownershi p and attributes of the new executable file (fw) as same as the old one $FWDIR/bin/fw. (chown, chmod)
5. Stop the current firewall module (fwstop), if it is running.
6. Backup the executable file ($FWDIR/bin/fw) with original ownership and attributes to $FWDIR/t mp or /tmp directory (cp –p).
7. Replace the file (fw) located at $FWDIR/bin with the one provided in the Hot fix (cp –p).
8. Start firewall (fwstart). I strongly recommend you to reboot the machine to be sure (sync; init 6). And you will notice the firewall mod ule can load the rule base locally.
9. Check the firewall version, you will notice the output of (fw ver) is Build 41518, higher than 41510 and output of (fw ver –k) keeps the same!

Notes and Recommendations:
- The above-mentioned procedures are based on Sola ris 2.6 and 2.7.
- The assumption is that the end -users (readers) are familiar with the related commands of the operating system and Checkpoint VPN -1/Firewall-1 ® products, so in the procedures only the necessary commands are mentioned.
- According to the abov e-mentioned 2 installation procedures, we just finish service pack and hot fix upgrade on one standalone system! Please keep in mind!
- Implementation Order. It is strongly recommended to upgrade the Firewall management station (fw_mgt) first, then the Firew all enforcement point(s) (fw_ep) later.

5.4.3 Rule base load and push procedure

1. On Firewall management station (fw_mgt) manually push the conf -fw_ep.W rule base to Firewall Enforcement point machine (fw load, putkey if necessary)
2. On Firewall Enforcement point (fw_ep), soft restart the firewall module, it will download the its rule base from management station (fw_mgt) remotely and successfully (fwstop; fwstart; putkey if necessary)

Notes and Recommendations:

- This procedure is absolutely required! Because in one enterprise firewall management environment, all the rule bases are centrally managed by one management station. After the service pack and hot fix are upgraded, we must guarantee that the communication between firewall management station and firewall enforcement point(s) is okay, our goal is to keep not only one standalone system, but also the whole security infrastructure running smoothly!

6. Installation Test

"Do not blindly follow any recommendations made by security gurus, consultants, authors, or SANs presenters without first testing and evaluating them for yourselves" (Quoted from SANS Security Essential Window 2000 Security Page 3_46)

This guideline leads me to do the test and evaluation completely. I did really find some problem in the test environment. As I mentioned in defining the installation procedures, the test help me a lot and gave me confidence! I would like to say that test before implementation is one gold rule in applying service packs and hot fix.

6.1 Test Environment

In our lab I set up one test environment with the backup hard disks from the productive machines. So all the Operating Systems and Checkpoint Firewall -1 Versions and Service Pack levels are same as productive ones.

This test covers the Firewall Management Station (fw_mgt) and Firewall Enforcement Point (fw_ep).

6.2 Test Evaluation Standards

- Complete installation without errors;
- Bounce the firewall, and then reboot the firewalled machine;
- Push/Load rule bases locally and/or remotely correctly
  - fw_mgt and fw_ep can load its rule base locally;
  - fw_ep can load its rule base from fw_mgt remotely and correctly;
  - From fw_mgt to fw_ep manually push rule base remotely and correctly;

6.3 Test Result

In order to record the installation procedure, I created 2 tables. T he test results are positive and we found one problem (refer to 6.4). (Please refer to the Appendix B for the detail Test Results).

6.4 Found Problem

After upgrading fw_mgt to SP5, I tried to push the rule base conf -fw_ep.W to fw_ep, Problem happened. Error Message follows:

> *Warning: Network Object OSPF_Multicast_5 doesn't contain any IP address.*
> ...
> *Failed to push the rule base to fw_ep....*

We check that there is also another Network Object *OSPF_Multicast_6* prevent this push rule base from succeeding!

6.5 Solution

Through extensive research on the Internet and documentations, we believe that SP5 checks the Networks Object much more strictly and correctly than SP2. These 2 objects are defined and used by another team for the Open Shortest Path First Protocol. According to the Reference (15), We recommend change those Network Objects to Host Objects, then the problem are solved.

7. Productive Installation

Based on operation-like installation test and carefully refined installation procedure, according to the company change management procedure, we apply the Service Pack 5 and RDP hot fix successfully.

I still have several points to mentions:

- According to the company security change policy, make one reasonable plan;
- Make the latest backup hard disks of those systems in case of failure.

Conclusion:
The procedure is much more important than the specific issues in daily system administration. While going through the whole article, you will find that I put much more writing power on the whole procedure desc ription than that of the specific issue. In order to secure the enterprise information, one of the most important skills for system administrators is to implement the service packs and hot fixes correctly and efficiently. For the daily administration tasks , it is better to define and document appropriate procedures to guide the whole process. During the Checkpoint VPN -1/Firewall-1 ® Version 4.1 Service Pack 5 implementation, the specific firewall problems will differ from case to case. But the most importan t thing is to find the problem before it is applied in productive environment.
Test before implementation. One important performance for the system administrators is to keep the system running, and reduces the planed or unplanned downtime. And at

the same time the system administrators have to apply the service packs and hot fixes to secure the systems. In fact, no company can guarantee that the service packs are bug-free. I strongly recommend you to do the test before implementation in productive environment. The test procedure will help you familiarize the procedure, find the problems, and solve them. That will greatly reduce the productive downtime, and also increase your reputation!
I wish you enjoyed the system administration; it is really interesting and challenging!

Reference:

1. SANS, SANS Security Essential Courseware (Online) Mar 22. 2002
2. Check Point Software Technologies Ltd. VPN -1/FireWall-1 Administration Guide Feb 2.2000
3. Check Point Software Technologies Ltd. VPN -1/FireWall-1 Reference Guide Feb 2.2000
4. Check Point Software Technologies Ltd. VPN -1/FireWall-1 Management (I, II) Security Courseware Checkpoint 2000 Edition
5. Check Point Software Technologies Ltd. VPN -1/FireWall-1™ Version 4.1 SP5 Release Notes Aug. 2001
6. Check Point Software Technologi es Ltd. VPN-1/FireWall-1™ Version 4.1 SP5 LDAP/VPN Patch Release Notes Jan. 2002
7. SUN Microsystems, Inc. Solaris System Administration (I, II) November 2000,Revision A.3
8. Anonymous Maximum Security (Second Edition) Sams Publishing, Nov.1998
9. Arbaugh, Bill. "Security: Technical, Social, and Legal Challenges" COMPUTER Magazine February 2002: 109-111
10. Gaer Galvin, Peter. "The Golden Rules of Sun Systems Administration" SysAdm Magazine February 2002: 55-56
11. Knox, Thomas. "Solaris Patch Levels" SysAdm Magazine February 2002: 51-52
12. Check Point Software Technologies Ltd. "Download Site for Software Subscription" URL: http://www.checkpoint.com/cgi-bin/download.cgi (09.Apr.2002)
13. Check Point Software Technolo gies Ltd. "VPN-1/Firewall-1 RDP Stability Fix" URL: http://www.checkpoint.com/techsupport/d..senotes/rdp_comms_hf_release_notes.html (09.Apr.2002)
14. Dameon D. Welch-Abernathy. FireWall-1 FAQ: "Which Build Number of FireWall-1 to Which Service Pack?" 19 Jan 2002. URL: http://www.phoneboy.com/faq/0385.html (12 Mar 2002)
15. Dameon D. Welch-Abernathy. FireWall-1 FAQ: "OSPF and Anti-Spoofing" 12-Jan-2002 URL:http://www.phoneboy.com/faq/0228.html (11 Apr. 2002)

Appendix A

Checkpoint VPN-1/Firewall-1®
Build Number and Service Pack Mapping Table

Build Number	Service Pack
3078	3.0bSP8 (Nokia)
3083	3.0bSP8
3096	3.0bSP9
4031	4.0 SP1
4034	4.0 SP2
4056	4.0 SP3
4064	4.0 SP3 + hot fix
4066	4.0 SP4
4094	4.0 SP5
41??	4.0 SP6
4201	4.0 SP7
4304	4.0 SP8
41439	**4.1 SP0**
41489	4.1 SP1
41492	4.1 SP1 on IPSO
41716	**4.1 SP2**
41814	4.1 SP3
41821	4.1 SP3 on IPSO
41862	4.1 SP4
41864	4.1 SP4 on IPSO
41510	**4.1 SP5**
41515	4.1 SP5 hot fix on IPSO
50xxx	NG Feature Pack 0
51131	NG Feature Pack 1 (except IPSO)
51012	NG Feature Pack 1 on IPSO

(Quoted from http://www.phoneboy.com/faq/0385.html Updated on 08.04.2002)

Appendix B

Test Result Table -I

Single Machine Installation Test

Items	Management Station (fw_mgt)		Enforcement Point (fw_ep)	
	SP5 Installation	**SP5_RDP Binary Replacement**	**SP5 Installation**	**SP5_RDP Binary Replacement**
Test Preparation and Test • Configuration adjustment • Rule bases push/load locally /remotely	O.K. (1)	O.K. (4)	O.K. (7)	O.K. (10)
Hard Reboot sync; sync; sync; init 6	O.K. (2)	O.K. (5)	O.K. (8)	O.K. (11)
Soft Reboot fwstop; sleep 3;fwstart	O.K. (3)	O.K. (6)	O.K. (9)	O.K.(12)

Note:

- **Single machine installation order; please refer to the number from (1) to (12).**

Appendix B

Test Result Table-II

(Rule base Load/Push Test)

Items	Management Station (fw_mgt)		Firewall Enforcement (fw_ep)	
	SP5 Installation	**SP5_RDP Binary Replacement**	**SP5 Installation**	**SP5_RDP Binary Replacement**
Rule base Load Locally	O.K.	O.K.	Disconnect Network to force load locally, O.K.	Disconnect Network to force load locally, O.K.
Rule base Load Remotely	N/A	N/A	O.K.	O.K.
Rule base Push Remotely (From fw_mgt to fw_ep)	Problem happens! Please Refer to **6.4 Found Problem**	After correction O.K.	N/A	N/A
Rule base Load Remotely (fw_ep load from fw_mgt)	O.K (SP0 downloads fromSP5)	O.K.	O.K.	O.K.