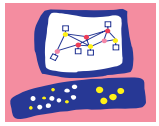
CHECK POINT
Software Technologies Ltd.



We Secure the Internet.

Check Point Integrated Suite
Check Point 2000 (Version 4.1 SP1)
Release Notes

January 2000
http://www.checkpoint.com

Contents

Important — The latest version of these Release Notes is at: **http://www.checkpoint.com/techsupport**.

製品の日本語情報をご覧になりたい方は下記URLをご覧ください。

http://www.checkpoint.co.jp/releasesj/

P/N 700006

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com

U.S. Headquarters:
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

http://www.checkpoint.com

February 2, 2000

Please direct all comments regarding this publication to **techwriters@checkpoint.com.**

Release Notes

Thank you for using Check Point Integrated Suite Version Check Point 2000 (also known as Version 4.1 SP1).

This document contains important information not included in the product User Guides. Please review this information before installing Check Point Integrated Suite products.

Up-to-date information about Check Point Integrated Suite, including the Check Point Knowledge Base, can be found at **http://www.checkpoint.com/techsupport**.

IMPORTANT — This version of Check Point Integrated Suite implements a licensing mechanism different from the one used prior to Version 4.1. Version 4.1 licenses are valid, but ***licenses from versions prior to Version 4.1 are no longer valid***. If you are upgrading from a version prior to Version 4.1, you must obtain a new license (from http://license.checkpoint.com) before using any of the products in Check Point Integrated Suite.

In This Document

Latest Version

The latest version of these Release Notes is at: **http://www.checkpoint.com/techsupport**.

VPN-1/FireWall-1 Mailing List

To subscribe to the VPN-1/FireWall-1 mailing list, send a message to **majordomo@lists.us.checkpoint.com** with "subscribe fw-1-mailinglist *email-address*" in the message text, where *email-address* is your email address.

Documentation

The CD-ROM includes copies of the Check Point Integrated Suite User Guides in Adobe Acrobat Portable Document Format (PDF), as well as Acrobat readers for most supported platforms. These readers can also be downloaded from Adobe (www.adobe.com). The CD-ROM does not contain an Acrobat reader for Solaris2-x86 or HP-UX 11. To view the PDF files in NT, exit the installation program and browse the CD (for example, with NT Explorer).

Reading the CD

AIX 4.2.1 — The Check Point CD cannot be read under AIX 4.2.1. You can download a fix for this problem from:

```
http://service.software.ibm.com/cgi-bin/support/rs6000.support/
fixsearch?fix db=aix4&srchtype=apar&query=IX82623
```

Note that this is one very long URL split across two printed lines.

VPN-1/FireWall-1

Supported Platforms

The supported platforms for VPN-1/FireWall-1 are listed in TABLE 1:

TABLE 1 Platform Summary

Component	Platforms
GUI Client	■ Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ X/Motif (Solaris, HP-UX 10.20, IBM AIX)
Management Module, VPN/FireWall Module, SecureServer	■ Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only ■ Solaris 2.6, Solaris Operating Environment 7 (formerly known as Solaris 2.7) in 32 bit installation mode only — SPARC and x86 ■ HP-UX 10.20, 11.0 ■ IBM AIX 4.2.1, 4.3.2 ■ Red Hat Linux 6.1 with kernel version 2.2.x
SecureClient, SecuRemote	Windows 9x, Windows NT 4.0 (SP4, SP5, SP6) — Intel and compatibles only

Installation

HP-UX, x86 and AIX — The installation wrapper installs only VPN-1/FireWall-1 and the integrated GUI. Other products must be installed individually, according to the procedures specified in the User Guides of those products.

Upgrading and Backward Compatibility

Note – The software in this version is an upgrade to Check Point Management Suite 4.1. If you have an earlier versions of the software components installed, they will be upgraded. If you do not have earlier versions installed, a full version will be installed.

1. For important information about upgrading VPN-1/FireWall-1 and backward compatibility, see the "Installing VPN-1/FireWall-1" chapter in the *VPN-1/FireWall-1 Administration Guide*.

Note – The Linux version does not provide a backward compatibility option for Versions 3.0 and 4.0. A Linux Management Station can manage any Version 4.1 VPN/FireWall Module.

2 Using the Enterprise Suite installation procedure, you can automatically upgrade to this version from any of the versions specified in TABLE 2.

TABLE 2 Upgrade Paths

Product	Upgrade from any of the Following Versions
VPN-1/FireWall-1	3.0b, 4.0, 4.1
GUI	3.0b, 4.0, 4.1
FloodGate-1	1.5, 4.1

3 If you upgrade to Check Point 2000 from FireWall-1 Version 3.0, you will be asked whether to:

- upgrade or overwrite your configuration files — reply "upgrade"
- save or delete Version 4.0 — reply "delete"

4 The backward compatibility feature is not available on Linux Management Stations.

5 In order to be able to manage Version 3.0 or Version 4.0 VPN/FireWall Modules from a Version Check Point 2000 Management Module, you must do one of the following:

- **upgrades (from Version 3.0b SP9)** — Upgrade the Management Module to Check Point 2000. For each remote VPN/FireWall Module, set **Version** (in the **General** tab of its **Workstation Properties** window) to 3.0. Modify `$FWDIR/lib/control.map` and `$FW_4.0_DIR/lib/control.map` (following the procedure given in item 6 below), and then perform `fw putkey` for all remote VPN/FireWall Modules. Because the ELA Proxy is installed by default, you will see "Connection broken while communicating ..." messages on the console. These can be stopped by stopping the ELA Proxy (see "Uninstalling VPN-1/FireWall-1" on page 6 for instructions on how to do this). Upgrade the VPN/FireWall Modules (following the procedure given in item 6 below).
- **upgrades (from Version 4.0)** — Upgrade the Management Module to Check Point 2000 from Version 4.0 SP3 or later. If the Management Module is pre-Version 4.0 SP3, then you must first upgrade it to Version 4.0 SP3 and then upgrade to Version Check Point 2000. You must also select the "Save Version 4.0" option during the Check Point 2000 (Version 4.1) installation.

  For your convenience, the Version 4.0 SP5 installation package is provided on the Check Point 2000 CD in the `windows\patches\ CPfw1-40-sp5` directory.
- **new installation** — Install the backward compatibility feature (on the Management Module). On Windows NT you will be asked whether to install the backward compatibility feature during the installation procedure. On Unix platforms, the backward compatibility feature is a separate package. **Important:** Do not install the backward compatibility feature if you are upgrading from Version 4.0.

6 In Check Point 2000, the control channel is encrypted even if there is no encryption license. For this reason, when upgrading a VPN/FireWall Module which has no encryption license from Version 3.0 or Version 4.0 to Check Point 2000, the control channel between the Management Module and the VPN/FireWall Module (created by the `fw putkey` command) will be lost. To re-establish the control channel, proceed as follows:

- After upgrading the Management Module to Check Point 2000, edit the `$FWDIR/lib/control.map` file on the Management Module and add a line at the end as follows:

  `NON-ENCRYPTED: <list>`

  where `list` is a comma-separated list of the IP addresses of all the VPN/FireWall Modules still running the earlier VPN-1/FireWall-1 version without encryption licenses. For example:

  `NON-ENCRYPTED: 10.2.3.4,10.5.6.7`

- Whenever you upgrade a VPN/FireWall Module to Check Point 2000, remove its IP address from `list` and run `fw putkey` for that VPN/FireWall Module.
- When `list` is empty (that is, after you have upgraded the last VPN/FireWall Module), remove the "`NON-ENCRYPTED`" line.

7 When upgrading from Version 4.0 to Check Point 2000, the **Management Station** checkbox in the **Workstation Properties** window will be checked only for the Management Station being upgraded. All other gateways defined on the Management Station will have the **Management Station** checkbox unchecked by default.

8 When upgrading VPN-1/FireWall-1 directly, that is, not using the installation wrapper, you must stop the following (if they are running):

- FloodGate-1
- In the Reporting Module: Log Consolidator and Report Server

9 When you upgrade, the `$FWDIR/lib/control.map` file is replaced. If you have made any changes to `control.map`, they will not be preserved in the new `control.map`, so you must make the same changes in the new version.

10 **Session Authentication Agent** — Installing the Version Check Point 2000 Session Authentication Agent does not overwrite the Version 4.0 Session Authentication Agent. You must uninstall the Version 4.0 Session Authentication Agent (using the Control Panel's Add/Remove Programs applet) and then install the Version Check Point 2000 Session Authentication Agent. Note that the Session Authentication Agent is shut down as part of the uninstallation process, so you must manually restart it (or reboot).

Installing VPN-1/FireWall-1

1 **HP-UX** — The Check Point installation procedure checks whether the `/usr/lib/libCsup.1` file is at level 07. If not, you must apply the appropriate HP patch, as follows:

- HP-UX 11: PHSS_14577 or later
- HP-UX 10: PHSS_16585 or later

2 **HP-UX** — The Check Point CD is created in the Rock Ridge format. It is recommended by HP that `pfs_mountd` and `pfsd` be started by `rc` and invoked in the background.

```
hostname# pfs_mountd &
hostname# pfsd 4 &
```

These commands will start four `pfs` daemons with the default cache sizes.
Now you can use the following special mount command.

```
hostname# pfs_mount -t rrip /dev/device /cdrom
```

You can leave Rock Ridge running on your machine. If you wish to stop it, make sure that all mount commands have been terminated.
See the man page for the `pfs_mount` command for details on setting up an `/etc/pfs_fstab` file.

Uninstalling VPN-1/FireWall-1

1 Before uninstalling VPN-1/FireWall-1, stop the ELA proxy (if it is running).

Unix

```
# cd $FWDIR/bin
# ./elaproxyService -stop
# ./elaproxyService -remove
```

NT

Stop the ELA proxy service (from Control Panel/Services) and change its startup state to manual.

2. If both the VPN-1/FireWall-1 and Motif GUI packages are installed, and the VPN-1/FireWall-1 package is removed, then the `$FWDIR/bin/fwpolicy` executable file is deleted and the Motif GUI cannot be run. To prevent this from happening, make a copy of `fwpolicy` before uninstalling the VPN-1/FireWall-1 package and then copy `fwpolicy` back to its original location in `$FWDIR/bin`. You should also create symbolic links to `fwpolicy` named `fwlog` and `fwstatus`.
3. The backward compatibility feature is not uninstalled when VPN-1/FireWall-1 is uninstalled, but must be separately uninstalled.
4. Before uninstalling VPN-1/FireWall-1 Version Check Point 2000 on HP-UX, ensure that you have at least 15 MB free in the `/stand` directory.

Downgrading

1. If you upgrade a VPN/FireWall Module to Version Check Point 2000 and afterwards downgrade it to Version 4.0 by uninstalling Version Check Point 2000, then the Management Station still has a Version Check Point 2000 Security Policy for this VPN/FireWall Module. After rebooting, the Version 4.0 VPN/FireWall Module will now try to fetch the Version Check Point 2000 Security Policy, with which it is incompatible.

   You can prevent this from happening as follows:

   a. Before rebooting the downgraded VPN/FireWall Module machine, remove (on the Management Station) all files named `$FWDIR/state/<module host name>.*`.
   b. In the **Workstation Properties** window for the VPN/FireWall Module, set the version number to 4.0.
   c. Reboot the VPN/FireWall Module machine.
   d. Install the Security Policy.

VPN-1 Accelerator Card

1. Installation and operating instructions for the VPN-1 Accelerator Card can be found in the *Check Point VPN-1 Accelerator Card Installation Guide* PDF file on the CD.
2. A Check Point 2000 VPN-1/FireWall-1 Management Station cannot manage a Version 4.0 VPN/FireWall Module with a VPN-1 Accelerator Card.
3. If you are upgrading from VPN-1/FireWall-1 Version 4.0 with the VPN-1 Accelerator Card, then you must uninstall the VPN-1 Accelerator Card software, upgrade to VPN-1/FireWall-1 Version Check Point 2000, and then install the VPN-1 Accelerator Card software. You must do this on the Management Module and on each of the FireWall Modules. Note that VPN-1/FireWall-1 Check Point 2000 cannot manage a Version 4.0 VPN-1 Accelerator card.

Certificates (PKI)

1. There is no Entrust (PKI) functionality for the IBM AIX 4.3.2 platform. Solaris x86 supports Entrust 3.0 and VPN-1 Certificate Manager for registration and Entrust 4.0 for validation. Thus, if Entrust 4.0 is used, a Solaris x86 machine cannot function as a VPN-1/FireWall-1 Management Module but only as a VPN/FireWall Module.

2. By default, VPN-1/FireWall-1 validates Entrust certificates using the Entrust CMS toolkit. To configure VPN-1/FireWall-1 to validate Entrust certificates using the same Check Point validation code it uses to validate OPSEC CA certificates, proceed as follows:

   a. Stop the VPN/FireWall Management Station (`fwstop`).
   b. In `objects.C`, locate the CA object to be modified and add the following new property:

      ```
      :use_cms_validation (false)
      ```

   c. Start the VPN/FireWall Management Station (`fwstart`).
   d. In the Policy Editor, define a new Account Unit object on which CRLs are published and check **CRL Retrieval**.

      Verify that the Account Unit is correctly defined (its workstation object, Bind DN and password, branches *etc*.).
   e. Install the Security Policy.

3. When generating a certificate for a Check Point Module that uses Entrust 3.0 and VPN-1 Certificate Manager, if the object's IP address has a zero component (for example, if its IP address is 10.0.23.45 or 192.34.0.44) then the CA returns an error and the certificate is not generated. The workaround is to change the offending IP address, generate the certificate and then restore the IP address.
4. A CA certificate generated by an Entrust 3.0/VPN-1 Certificate Manager CA is usually automatically updated in the VPN-1/FireWall-1 database. It sometimes happens that the CA certificate is not updated in the database even though no error message is generated. Instead, a message saying "Securely received the CA certificate of ..." is displayed. This message is misleading because there is no CA certificate and in its absence VPN-1/FireWall-1 will not accept certificates issued by that CA. The workaround is to verify the existence of the CA certificate in the VPN-1/FireWall-1 database whenever the above message is displayed. If there is indeed no CA certificate, then either generate the certificate again (which usually solves the problem), or obtain the CA certificate from another source and install it manually on the CA object.
5. If you select a certificate from a floppy drive, you will be able to launch online help only if the disk is still in the drive.
6. A SecuRemote user who authenticates using Entrust certificates will be unable to download the topology from a Management Station on which no VPN/FireWall Module is running. The workaround is to copy the CA's `ini` file — whose name (`entrust_<CAName>.ini`) depends on the CA's name, for example, `entrust_HQCA.ini` — from the `$FWDIR/conf` directory to the `$FWDIR/database` directory (on the Management Station).
7. **This note does not apply to the NT and Solaris platforms.** Because of a bug in the Entrust CMS toolkit, VPN-1/FireWall-1 sometimes sends a SecuRemote Client an invalid CRL, resulting in authentication failures (because the SecuRemote Client validates CRLs independently from the VPN/FireWall Module). The problem can be resolved by configuring VPN-1/FireWall-1 to validate certificates using the OPSEC library (see item 2 above).
8. **CRL validity** — A SecuRemote Client and a site must have their date, time of day and (on NT) daylight savings time policy synchronized to avoid a situation where a Certificate Revocation List has expired on one but not on the other. A default grace period of 15 minutes is defined, during which a CRL can be used both before and after its period of validity. Two properties in `objects.C` are relevant:
   - `crl_start_grace` — the number of seconds before the CRL's validity period during which the CRL will be regarded as valid
   - `crl_end_grace` — the number of seconds after the CRL's validity period during which the CRL will be regarded as valid

These properties should be added to `objects.C` near the `crlcache_timeout` property. The VPN/FireWall Module must be stopped (`fwstop`) and restarted (`fwstart`) for the settings to take effect. The settings take effect on the SecuRemote Client after the next topology download.

Note – See "SecuRemote/SecureClient" on page 9 for additional Release Notes relating to certificates and SecuRemote/SecureClient.

Backward Compatibility

This section applies when a VPN-1/FireWall-1 Management Station that has been upgraded to Check Point 2000 manages a Version 4.0 VPN/FireWall Module.

If the Version 4.0 VPN/FireWall Module supports certificates, the Check Point 2000 Management Station takes the `cms.ini` file (which contains CA data) from the `conf` directory of its VPN-1/FireWall-1 Version 4.0 tree.

There are two possible scenarios:

The Management Station was using Entrust CAs before the upgrade: After the upgrade, there are two instances of the `cms.ini` file on the Management Station, one in the VPN-1/FireWall-1 Version 4.0 directory (named `cms.ini`) and one in the Check Point 2000 directory (named `entrust_My_CA.ini`). If you wish to change the file, you must change both instances.

The Management Station was not using Entrust CAs before the upgrade: To use an Entrust CA after the upgrade, proceed as follows:

1. Create the CA object on the Check Point 2000 Management Station in the usual way.
2. Copy the `entrust_<CA name>.ini` file from the Check Point 2000 `conf` directory to `cms.ini` in the Version 4.0 `conf` directory.
3. In `conf/fwrl.conf` (in the Version 4.0 tree), insert a path to `cms.ini` by adding a line (in the `FILTERLOAD` segment) similar to the following (the exact syntax depends on the OS):

   ```
   NAME = conf\cms.ini; DST = database\cms.ini;
   ```

SecuRemote/SecureClient

Note – This section applies to both SecuRemote and SecureClient (SecuRemote configured with the Desktop Security feature).

1. When SecuRemote is installed, the user is asked whether to install the Desktop Security feature (SecureClient). The default is "Yes."

   It is possible to customize the installation procedure to change the default and/or not give the user the opportunity to make the choice. This is done by modifying `product.ini` on disk1 of the package. The relevant parameters are:

   - `DesktopSecurityDefault`

     `1` indicates SecureClient (enabled Desktop Security) is the default.

     `0` indicates SecuRemote (disabled Desktop Security) is the default.

   - `DesktopSecurityAskUser`

     `1` indicates that the user will be asked whether to install the Desktop Security feature.

     `0` indicates that the user will not be asked whether to install the Desktop Security feature, and the default specified by `DesktopSecurityDefault` will be chosen automatically.

2. The **Site** and **Authentication** windows are slightly different from those pictured in the User Guide.
3. If a previous version of SecuRemote is running when you upgrade (or overwrite) SecuRemote to a new version, then when the installation procedure attempts to shut down the previous version, an application error is sometimes generated.
4. Thin Client — The description in the User Guide of the Thin Client as being without certificate functionality is inaccurate. A Thin Client cannot import PKCS #12 certificates or use the Offline Certificate Utility, but it can use the Entrust PKI and other PKI's if the end user is provided by the administrator with a certificate in `EPF` format.

5. Starting with VPN-1/FireWall-1 Version 4.1, SecuRemote Clients download site information through SecuRemote Server port 264 (using the FW1_topo service). In previous versions, this information was downloaded through SecuRemote Server port 256 (using the FW1 service). For information on how to enable backward compatibility with pre-Version 4.1 SecuRemote Clients, see "Pre-Version 4.1 SecuRemote Clients" on page 141 of *Check Point Virtual Private Networks*.
6. The description of the SecuRemote automatic version update feature incorrectly specifies `desktop_sw_version` as the name of the property in `objects.C` that controls this feature. The property's name is `desktop_build_number`.
7. For Entrust Entelligence users — If you logon to certificates through the Entelligence logon windows, and you are using Entelligence 4.0, then you must manually check the "work offline" checkbox for SecuRemote authentication. In a later version of Entelligence it will be checked automatically.
8. **Error logging** — In previous versions, logging (if active) was to the C: drive only. In this version it is possible to specify an alternate drive in the registry. To do this, add a string value named "LogDrive" under `HKEY_LOCAL_MACHINE\Software\CheckPoint\SecuRemote`, and set it to the drive letter of a local drive. Though it is possible to log to a remote drive, it is not recommended to do so.

   To enable logging, you must pre-create the log file. For regular SecuRemote logging, you should create `fwenc.log` at the root (on C:\ by default). For SecureClient logging you may want to create `sr.log` for logging of blocked connections.

   You may additionally want to create `b_fwenc.log` and `b_sr.log`, for logging before the user logs on to the OS.
9. The `entrust.ini` file installed with SecuRemote contains the following lines needed to enable Netscape certificates:
   - Under `[OIDAlias]` — `uid=userid`
   - Under `[OIDTable]` — `userid=0.9.2342.19200300.100.1.1`
   - Under `[X500AttrSyntax]` — `userid=caseIgnoreStringSyntax`

   If a copy of `entrust.ini` already exists in the Windows directory, it will not be overwritten. In this case, it may be necessary to add the above lines in the corresponding sections manually (if you will be using Netscape certificates).

   Also, it may be necessary to add similar lines to support special attributes in other vendors' certificates.
10. **icmpcryptver —** All gateways and SecuRemote Clients participating in an FWZ VPN must agree on the value for `icmpcryptver` in order to enable ICMP. `icmpcryptver` is defined in `objects.C` on the gateway and in `state/userc.set` on the SecuRemote Client. Its default value is 1. Note that the existing value is not overwritten during an upgrade. A value of 0 enables compatibility with VPN-1/FireWall-1 Version 3.0.

    In SecuRemote Version 4.1 and later, FWZ encrypted pings will not work if `icmpcryptver` is 0.
11. In the **Properties Setup** window (under **Desktop Security**) you can configure how often the desktop invalidates the user's authentication, forcing re-authentication. If multiple sites are defined, the timeout for all sites will be the minimum of all the sites' timeouts.
12. **NT** — If you choose the **Reboot** option at the end of the installation process, you may only be logged off. In this case, you should select **Shut Down** and restart the computer. This will generally not happen if you adhere to the installation warning recommending that you close all applications before proceeding with the installation.
13. When using FWZ encryption with MD5, connections (especially long ones, for example FTP downloads) may hang. To resolve this problem, edit `objects.C` as follows:
    - Stop the VPN/FireWall Module (`fwstop`).
    - Change the `:icmpcryptver (n)` property as follows:

      If `n` is 0, change it to 2.

      If `n` is 1, change it to 3.
    - Start the VPN/FireWall Module (`fwstart`).

- Make the same change to the `:icmpcryptver (n)` property on the SecuRemote Client, in the `state\userc.set` file.

After making these changes, the VPN/FireWall Module will be incompatible with VPN/FireWall Modules that have not been changed, and with SecuRemote Clients up to and including build 4005.

14 If you suspend your computer (or "hibernate" or put it in "standby") for *n* minutes, when your passwords will be erased depends on the platform:

- Windows 95, NT 4.0 — The timer mechanism is suspended while the machine is. Passwords will be erased after *n* "active" minutes.
- Windows 98 and 98 SE— The timer mechanism is not suspended. Passwords will be erased after *n* minutes of elapsed time. If this occurs while the machine is suspended, they will be erased upon Resume.

SecureClient specific

Note – This section applies only to SecureClient (SecuRemote configured with the Desktop Security feature).

1 The network configuration diagram illustrating the SecureClient chapter in the User Guide might be incorrectly understood to suggest that a Policy Server must be installed on a separate machine inside the local network. This is not so. A Policy Server can be installed on the same machine as a VPN/FireWall Module (for example, a gateway).

2 If you delete the site from which a SecureClient's Desktop Policy was downloaded, the SecureClient continues to enforce the last downloaded Desktop Policy.

3 If you upgrade from SecureClient Version 4.1, you will lose your Desktop Policy until the next time you login to a Policy Server.

4 If you install SecureClient on all adapters and then connect on a dial-up line (after physically removing the network adapter), the SecureClient may still attempt to route connections through the network adapter. The solution is to rebind the adapters (**Rebind adapters** in the **Tools** menu). Note that this may conflict with the **Desktop Configuration Verification Options** specified in the **Desktop Security** tab of the **Properties Setup** window.

5 If your Desktop Policy is **Allow Outgoing Only** or **Allow Outgoing and Encrypted**, cleartext back connections will function properly only for: FTP, VDOLive and RealAudio.

6 **IKE only** — If the Desktop Policy is **Allow Outgoing Only**, then for the first connection to an encryption domain, back connections (for example, the FTP data connection) are not recognized as belonging to the control connection and will not be allowed. Subsequent connections function correctly, so the solution is to simply try again.

7 If a Policy Server is also a VPN-1/FireWall-1 gateway, and a SecureClient user in the LAN logs on to the Policy Server using FWZ, then connections from the SecureClient through the gateway to machines in the encryption domain will fail. The reason is that the SecureClient will not encrypt (because the SecureClient and the destination are in the same encryption domain) but the gateway will encrypt (because of the earlier FWZ key exchange). After less than 15 minutes, the Policy Server will "forget" the key exchange and new connections will succeed.

There are two workarounds:

- Use IKE as the encryption scheme for the SecureClient user.
- Put the Policy Server on another (non-gateway) machine (for example, a VPN-1 SecureServer). This workaround is not ideal when there are SecureClients on both sides of the gateway (both on a LAN and on a WAN). If you want your remote users to obtain policies implicitly (when they exchange encryption keys) you will still need a (second) Policy Server on the gateway.

8 SecureClient — You must define a rule on the Policy Server that allows the (pre-defined) FW1_pslogon service between the SecureClient and the Policy Server.

9 If there is a VPN/FireWall Module between the Policy Server and the SecureClient, you must allow the fw1_encapsulation and RDP services for FWZ and the IPSec service for IKE.

10. The first time you install a Security Policy that includes a Session Authentication rule with **Verify secure configuration with Policy Server** checked, you must stop and restart the VPN/FireWall Module before the setting takes effect.
11. When downloading topology from a VPN-1/FireWall-1 Version 4.0 Server that is managed by a Check Point 2000 Management Server, Policy Servers do not appear as part of the topology. The solution is to upgrade the Version 4.0 Server to Check Point 2000.
12. The result of a configuration verification is cached for the time period (in seconds) specified by the `timeout` parameter in the `$FWDIR/database/fwdtmquery.C` file.

```
(
    :cache_params (
           :timeout (15)
    )
)
```

If this file does not exist, the timeout period defaults to 15 seconds. If `timeout` is set to zero, there is no caching and the configuration is verified for each connection.

Account Management

1. This version of the Account Management Client is Y2K ready.
2. If you are upgrading to a new version of the Account Management Client, you will be asked whether to upgrade the objects on your Account Units. See the Account Management Client Build 140 Release Notes at http://www.checkpoint.com/support for details.
3. The Account Management Module requires a third-party Directory Server, which must be obtained elsewhere. Supported servers are:
   - Netscape Directory Server 4.0 and 4.1 for Windows NT and Solaris
   - NetWare Directory Service v8.0 for NetWare
   - Innosoft Distributed Directory Server 4.4.1 for Solaris
   - IBM SecureWay Directory 3.1 for Windows NT

   An updated list of OPSEC-certified LDAP Servers is available at http://www.opsec.com.

Miscellaneous

1. An administrator who does not have permission to edit the user database (User Edit) cannot add user groups to rules, even if the administrator has permission to edit the Rule Base (Rules Edit).
2. If **Accept VPN-1 & FireWall-1 Control Connections** in the **Security Policy** tab of the **Properties Setup** window is checked, the fw1_service service will be allowed between all workstations on which **VPN-1/FireWall Installed** is checked (**General** tab of the **Workstation Properties** window). In previous versions of VPN-1/FireWall-1, checking **Accept VPN-1 & FireWall-1 Control Connections** would allow the fw1_service between all network objects defined in the VPN-1/FireWall-1 database. This new meaning of **Accept VPN-1 & FireWall-1 Control Connections** excludes, for example, an OPSEC server running on a machine on which VPN-1/FireWall-1 is not installed, and the `opsec_putkey` command would fail. To enable the fw1_service for machines excluded by the new meaning, you must explicitly define a rule allowing the service.
3. The `fwui.log` file is now called `cpmgmt.aud`.
4. **Solaris** — `fwd` can sometimes crash when running UAM. The solution is to replace `fwuam.so` with the new version on the CD, as follows:
   a. Stop VPN-1/FireWall-1 (`fwstop`).
   b. Replace `/usr/lib/fwuam.so` with `/solaris2/Add-Ons/fwuam/fwuam.so` (on the CD).
   c. Restart VPN-1/FireWall-1 (`fwstart`).

5 VPN-1/FireWall-1 HP Open View Extension supports Solaris and HP-UX with HP OV version 4.x. HP-UX with HP OV versions 5.x and 6.x is not supported.

6 **Synchronized VPN/FireWall Modules —**

- Synchronized VPN/FireWall Modules must be managed by the same Management Module.
- SecuRemote connections can be synchronized.

7 If **Enable Exportable SKIP** (in the **Encryption** tab of the **Properties Setup** window) is checked, then if an internal VPN/FireWall Module has **Local** selected in the **Key Manager** tab of its **SKIP Properties** window, you must generate an exportable DH key for it (in its **SKIP Properties** window). Selective SKIP configuration (that is, some SKIP communications use exportable DH keys and some use non-exportable DH keys) can only be managed in the Rule Base.

8 If you change a Management Server's control channel encryption key (for example, by using the `fw putkey` command), then you must restart any ELA proxy that is running on that Management Server. See "Uninstalling VPN-1/FireWall-1" on page 6 for information on how to stop the ELA proxy.

9 In a High Availability configuration, each VPN/FireWall Module's license should be issued to its `hostid` or other unique ("heartbeat" or "configuration IP" interface), since any of the other interfaces can fail.

10 Do not rename a network object group that is used in the definition of a Logical Server.

11 **Unix platforms —** when remote modules are configured using the `cpconfig` program, if you try to add a new remote module you will not be able to see the list of previously configured modules. However, these modules are still defined and there is no need to reconfigure them. If you do reconfigure them, you must run `fw putkey` command again for each module.

12 The default values of some of the properties in the **Security Policy** tab of the **Properties Setup** window have changed as follows:

TABLE 3 New Default Values for Security Policy tab properties

Property	New Default Value
Apply Gateway Rules to Interface Direction	eitherbound
Accept VPN-1 & FireWall-1 Control Connections	enabled, **First**
Accept RIP	disabled
Accept Domain Name Over UDP (Queries)	disabled
Accept Domain Name Over TCP (Zone Transfer)	disabled
Accept ICMP	disabled
Accept Outgoing Packets Originating from Gateway	enabled, **Before Last**
Log Implied Rules	disabled

The new default values apply only to new installations. When you upgrade from a previous version, the existing values will *not* be changed.

Note – You should verify that the values in the **Security Policy** tab are what you expect them to be.

13 If you are using the VPN-1/FireWall-1 Check Point 2000 backward compatibility feature to manage VPN-1/FireWall-1 Version 4.0 SP1 or SP2 FireWall Modules and you use Client Authentication rules, the following workaround must be applied:

a. Edit the file `$FWDIR/lib/base.def` (where `FWDIR` specifies the directory in which the VPN-1/FireWall-1 Version 4.0 software or VPN-1/FireWall-1 Check Point 2000 backward compatibility module is installed), replacing the lines:

```
#define pm_prog   [(UDPDATA+40+rpc_cred_len+rpc_ver_len),b]
#define pm_prot   [(UDPDATA+48+rpc_cred_len+rpc_ver_len),b]
```

by the lines:

```
#define pm_prog   [68, b]
#define pm_prot   [68+8, b]
```

b. Reinstall the Security Policy on the VPN/FireWall Module.

14 **fw expdate command —** This command changes the expiration date of the users in the VPN-1/FireWall-1 users database. Any open GUI Client should be closed before running the command, otherwise the GUI will override the changes made by the command. On NT only, if `fw expdate` is executed while the Management Server was running, the Management Server should be restarted in order for the command to take effect.

15 In the Policy Editor, the menu item **File➤Installed Policies** is enabled only when FloodGate-1 is installed. If Floodgate-1 is not installed, you can view the installed policies from the **File➤Open** menu option.

16 **HP-UX 11** — VPN-1/FireWall-1 is supported only on DLPI interfaces.

CVP Manager

To install the CVP Manager, proceed as follows:

- **NT** — Run `setup.exe` in the `windows\CPcvpm-41` directory on the CD.
- **Solaris** — Run `pkgadd` to install the `CPcvpm-41` package.

After the installation is complete, edit the `cvpm.conf` file (see "CVP Manager Configuration File" in Chapter 10, "Server Objects" of *VPN-1/FireWall-1 Administration Guide*.).

To start the CVP Manager, proceed as follows:

- **NT** — Start the CVP Manager Service using the Services Manager in the Control Panel.
- **Solaris** — Run the script `S99cvpm_d` in the `/etc/rc3.d` directory.

Alternatively, reboot the machine.

To remove CVP Manager, proceed as follows:

- **NT** — Use Add/Remove programs in the Control Panel.
- **Solaris** — Run `pkgrm CPcvpm-41`.
  The target directory is not removed by this command.

MAD (Malicious Activity Detection)

If you run `fwstart` while the VPN/FireWall Module is already running, then another instance of `cpmad` will be run and any MAD messages will be issued once for each instance of `cpmad`. This can be prevented by always running `fwstop` or `fw kill cpmad` before running `fwstart`.

Open Security Extension (OSE)

Supported Routers and Security Devices

Open Security Extension (OSE) for VPN-1/FireWall-1 Version Check Point 2000 supports the following routers and security devices:

- Bay Networks Routers: Version 7.x – 12.x
- Cisco Routers: IOS Version 9, 10, 11, 12.x
- Cisco PIX Firewall: Version 3.0, 4.0, 4.1x
- 3Com NetBuilder: Version 9.x
- Microsoft Routing and Remote Access Service (RRAS) for Windows NT Server 4.0

Restrictions

Open Security Extension supports two PIX interfaces only: the internal and external interfaces.

Upgrading from OSM

A text file (OSM2OSE.txt) on the CD describes the procedure for upgrading from OSM to OSE.

FloodGate-1

Installing FloodGate-1

FloodGate-1 must be installed using the integrated installation procedure only. If you attempt to install FloodGate-1 in any other way, the installation will fail.

Uninstalling FloodGate-1

1. If FloodGate-1 was installed in stand-alone mode (without VPN-1/FireWall-1), then before uninstalling FloodGate-1, stop the ELA proxy (if it is running). See "Uninstalling VPN-1/FireWall-1" on page 6 for instructions on how to do this.

New Features

1. The Y-axis in the Real Time Monitor is now user-adjustable.
2. The Real Time Monitor now allows groups of services to be monitored.
3. If you click on an RTM graph, a tool tip is displayed which shows the value at the cursor position.
4. The **Bandwidth Actions** window has been improved and now enables the assignment of **Per Connection Guarantee** and **Number of Guaranteed Connections**, instead of the previously available **Per Connection Guarantee Allotment**.
5. Additional applications are now supported, including Netshow, NetMeeting and Echo request and reply.
6. **High Availability** — Check Point High Availability is now supported, and Traffic Management Policies can be added to cluster objects. Note that the only High Availability configuration compatible with FloodGate-1 is one in which there is only one active gateway at any given time, and the other gateways are in "hot standby" mode. In contrast, in a load sharing configuration (which is not compatible with FloodGate-1), each FloodGate Module has no knowledge of the traffic load on the other active gateways and is therefore unable to effectively manage traffic.

Clarifications Regarding Guarantees and Limits

Same Rule

7. A rule's **Guarantee Budget** is included in **Total Rule Guarantee**. The difference between the two is divided equally between all matching connections.

   Example:

   If (in the **Bandwidth Action Properties** window):
   - **Per Connection Guarantee** — 10KBps
   - **Guarantee Budget** — 80KBps
   - **Total Rule Guarantee** — 120KBps
   - **Accept Additional non-guaranteed connections** is checked

   Then the first 8 connections matching the rule will be guaranteed 10KBps each. All connections matching the rule will be guaranteed 40KBps (120 - 80) together, meaning that the first eight connections will get an extra guarantee equal to 40 / total number of connections matching the rule.

   If **Accept Additional non-guaranteed connections** is not checked, then the difference between **Guarantee Budget** and **Total Rule Guarantee** will be divided equally as an extra guarantee only for the connections open within the **Total Rule Guarantee**.
8. **Per Connection Guarantee** and **Total Rule Limit** cannot both be set in the same rule.

Sub-Rules

9. The total of guarantees specified in sub-rules may exceed the bandwidth share to which the parent rule is entitled according to its weight.

Example:

Suppose a rule should be allocated 30KBps (based on its weight and the traffic mix). If this rule has a sub rule with **Total Rule Guarantee** set to 40KBps, then FloodGate-1 will allocate 40KBps to the rule.

10 If either **Total Rule Guarantee** or **Per Connection Guarantee** is set for a rule, none of its sub-rules may set **Total Rule Guarantee** or **Per Connection Guarantee**.

Connections Matching More Than One Rule

11 If a connection matches more than one rule, then the lowest **Limit** and **Per Connection Limit** apply.

Example:

Suppose there are two rules, as follows:

- **Source**—Any; **Destination**—Any; **Service**—ftp; **Action**: **Total Rule Limit** — 50KBps
- **Source**—Any; **Destination**—FileServer; **Service**—ftp; **Action**: **Total Rule Limit**—30KBps

This will result in FTP connections to FileServer being limited to 30KBps.

12 If a connection matches more than one rule, then the bandwidth guaranteed to the connection will be the sum of the guarantees in the matching rules.

Example:

Suppose there are two rules, as follows:

- **Source**—Any; **Destination**—Any; **Service**—ftp; **Action**: **Total Rule Guarantee** — 20KBps
- **Source**—Any; **Destination**—FileServer; **Service**—ftp; **Action**: **Total Rule Guarantee**—30KBps

This will result in FTP connections to FileServer being guaranteed 30KBps + (20KBps / total number of FTP connections going through the FloodGate Module).

Example:

Suppose there are two rules, as follows:

- **Source**—Any; **Destination**—Any; **Service**—ftp; **Action**: **Total Rule Guarantee** — 20KBps
- **Source**—Any; **Destination**—FileServer; **Service**—ftp; **Action**: **Per Connection Guarantee**—3KBps

This will result in FTP connections to FileServer being guaranteed 3KBps + (20KBps / total number of FTP connections going through the FloodGate Module).

Example:

Suppose there are two rules, as follows:

- **Source**—MyHost; **Destination**—Any; **Service**—ftp; **Action**: **Total Rule Guarantee** — 20KBps
- **Source**—Any; **Destination**—FileServer; **Service**—ftp; **Action**: **Total Rule Guarantee**—50KBps

This will result in FTP connections from MyHost to FileServer being guaranteed 20KBps + (50Kbps / total number of FTP connections going to FileServer).

13 It is not recommended that it be possible for a connection to match more than one rule, where some of the rules specify limits while the others specify guarantees. In such cases, each connection matching all the rules will be allocated the limit plus its share of the guarantee.

Example:

Suppose there are two rules, as follows:

- **Source**—Any; **Destination**—Any; **Service**—ftp; **Action**: **Total Rule Guarantee** — 40KBps
- **Source**—Any; **Destination**—FileServer; **Service**—ftp; **Action**: **Per Connection Limit**—2KBps

This will result in FTP connections to FileServer being limited to 2KBps and getting an additional 40KBps / total number of FTP connections going through the FloodGate Module.

Miscellaneous

1 The minimum memory requirement for a FloodGate Module is 192 MB.

2 There is no Real Time Monitor on Solaris.

3 On Solaris, if you want to manually run VPN-1/FireWall-1 and FloodGate-1, first run `fwstart` and then run `etmstart`. To manually stop VPN-1/FireWall-1 and FloodGate-1, first run `fwstop` and then run `etmstop`.

4 If you change a Management Server's control channel encryption key (for example, by using the `fw putkey` command), then you must restart any ELA proxy that is running on that Management Server. See "Uninstalling VPN-1/FireWall-1" on page 6 for information on how to stop the ELA proxy.

Reporting Module

Platforms

The Reporting Client can be installed on Windows 9x and Windows NT platforms. The Reporting Server can be installed only on Windows NT.

Note – A Solaris version of the Reporting Server will be released at a later date. Please visit the Check Point support website or the OPSEC web site to download a copy of the Solaris version when it becomes available.

VPN-1/FireWall-1 Compatibility

1 This version of the Reporting Module is compatible with the following Management Servers and VPN/FireWall Modules:

NT

- Check Point 2000 (VPN-1/FireWall-1 Version 4.1 SP1)
- VPN-1/FireWall-1 Version 4.1
- VPN-1/FireWall-1 Version 4.0 SP2 and later

Unix

- Check Point 2000 (VPN-1/FireWall-1 Version 4.1 SP1)
- VPN-1/FireWall-1 Version 4.0 SP6 and later

Note – For Solaris, there is less than full compatibility with earlier Management Servers and VPN/FireWall Module versions. For details, please contact Check Point support.

Compatibility with Data from Pre-Version 4.0 VPN/FireWall Modules

It is NOT recommended to use the Reporting Module with log data from VPN/FireWall Modules Version 3.0 or before. In Version 3.0, the log and accounting messages do not include a marker that enables the Log Consolidator Engine to identify entries that appear in both log and accounting files.

If an event generated an entry in both the log and accounting files, the Log Consolidator Engine consolidates both entries, creating duplicate records in the Database. This will result in inaccurate reports in some instances.

Y2K

All dates now display with four-digit years (for example, "1999" instead of "99").

Licenses

Please read carefully the email you receive as part of the licensing process, as it contains much detailed and up-to-date information regarding your license.

See also the "Installation" chapter of *Getting Started with Check Point Reporting Module* for more details on licensing the Reporting Module.

When the Reporting Server starts, it displays a message: "Warning: ca not in cp.macro." This message does not indicate a probelm, and can be safely ignored.

Documentation

The following books are available in PDF format on the CD:

- *Getting Started with the Check Point Reporting Module*
  This document describes the overall product architecture, product components, installation procedure, and a step by step tutorial.

- *Check Point Reporting Module Administrator's Guide*
  This document includes chapters on defining and distributing reports, using the Log Consolidation features and additional reference information.

Online help is available for both the Log Consolidator and the Reporting Tool.

Working with Sample Connection Data

The Reporting Module includes a sample data (CON_DEMO connection table) of consolidated log entries from January 1, 1999 to February 19, 1999. Before you start creating reports from log files of VPN-1/FireWall-1, you can generate trial reports with the sample data to familiarize yourself with the product.

There are two ways to generate reports using the demo connection table:

Per Report — You can modify advanced report generation parameters per report. In this case, the sample connection data is retrieved from the demo connection table only for the generated report. To use the sample data per report, proceed as follows:

1. Open the report definition.
2. Choose **Show Current Report** from the **Run** menu.
3. In the **Runtime Parameters** window, click on **Advanced Options**. The **Advanced Options** window is displayed.
4. In **Connection Table**, choose **CON_DEMO** from the drop-down box.

Note — The Log Consolidator continues to load records to the `CON_CONNECTION` (default connection table), even if you modify the `RTGen.conf` file. If you want to generate reports using your own consolidated data, you must modify the `RTGen.conf` file once again to use the `CON_CONNECTION` table.

All Reports — You can modify general report generation parameters to use the demo connection table for all reports.

To use the sample data for all reports, modify the `CONNECTION_TABLE` attribute in the file `RTGen.conf` as follows:

```
CONNECTION_TABLE = "CON_DEMO"
```

This file specifies the general report generation parameters. Data for all reports is automatically retrieved from the connection table specified in the `CONNECTION_TABLE` attribute.

Upgrading

When upgrading VPN-1/FireWall-1 Version 4.0 installation on which a Reporting Server was installed, to VPN-1/FireWall-1 Check Point 2000, the Consolidation Engine GUI no longer functions. To solve this problem, proceed as follows:

Using a standard text editor, append the text in the file `..\Reporting Server\Log Consolidator Engine\conf\fwmaddon` (for example: `c:\Program Files\CheckPoint\Reporting Server\Log Consolidator Engine\conf\fwmaddon`) to the file `$FWDIR\conf\fwmaddon`.

New Features

Graph Labels — For all graph types, an identifying label indicating the value for each segment (bar, slice, *etc*.) now appears on all printed reports. For pie charts only, the identifying label also appears on the Client.

Restrictions

General

1. If you have modified VPN-1/FireWall-1 administration information (for example, Reporting GUI clients or administrators), you must stop and restart the Reporting Server in order for the changes to take effect.

To access the added or changed FireWall-1 objects from Reporting Module, you must wait for the Reporting Server to refresh the FireWall-1 objects. The default refresh cycle is set to 15 minutes. Then, you must exit and restart the Reporting Tool (GUI) in order to access the updated VPN-1/FireWall-1 objects. For immediate update, stop and restart the Reporting Server service as well as the Reporting Tool.

2. If the Reporting Server crashes (for example, in the event of a power failure), the database log file may become corrupted. If this occurs, delete the last database log file from the `$RTDIR/RTdatabase/log/` directory. The Reporting Module's functionality is not affected. The database can be subsequently populated by activating the log consolidation policy using the **Marker** option in the **Start Log File** field.

Administrator Permissions

For VPN-1/FireWall-1 Version 4.0, the administrator permissions defined apply to the Reporting Module as well. For VPN-1/FireWall-1 Version 4.1 or later, you must explicitly define permissions for the Reporting Tool and Log Consolidator using the Check Point Configuration Tool.

GUI Clients

1. Reporting Clients must also be defined as permitted GUI clients on the VPN-1/FireWall-1 Management Server. Clients are defined in the **GUI Clients** tab of the Check Point configuration application. After defining a new GUI client, you must stop and restart the Reporting Server.
2. If a VPN-1/FireWall-1 network object used in the Reporting Module is deleted in VPN-1/FireWall-1, it will be shown in reports as follows:
   - If the deleted object is of type workstation, the saved IP address will be used.
   - If the deleted object is of type network or address range, the first IP address of the range will be used.
   - For all other objects, the network object name will be used in the report.

Source and Destination Criteria

Domain and Gateway Cluster objects cannot be used as selection criteria.

NAT Connections

Only the translated source IP address, and *not* the original source IP address, is shown for NAT connections.

Target Tab

1. If a printer is missing in the printers list, see "Access to Printers" in *Getting Started with the Check Point Reporting Module* for information on adding a printer to the list.
2. HTML graph printing via Internet Explorer does not function properly; an empty report is printed.
3. A listing report with summary lines does not display well in Netscape, but displays correctly in MS Internet Explorer.

High Availability

NT and Solaris

1. When uninstalling this version, if changes were made to the MAC addresses (that is, the `.ha` file was imported to this machine or changes made by the product interface), you should restore your old settings as follows:

   NT

   a. Run `regedit` and browse to:

   HKEY_LOCAL_MACHINE/SYSTEM/currentControlSet/Services/*interfaceName*/parameters/

   Replace *interfaceName* with the card name, for example, E100B1. This should be done for each interface.

b. Edit the key named "NetworkAddress" (under the above key) and replace its value with an empty value.

Solaris

a. Remove the rc script `/etc/rcS.d/S31cphaboot` and the files `/etc/ether.`*XXX*, where *XXX* corresponds to each of the NICs (for example, `ether.hme0`).

2 Sometimes there is no log notification when a module goes into standby mode after it was standby after it was down.

NT only

Ethernet cards

1 The following relates to the MAC address configuration. The first six hex characters of the MAC address represent the card manufacturer. We have discovered that some cards may not accept other vendors's MAC addresses (that is, other vendors' prefixes in the MAC address). The symptom of this problem (found on NT) causes the card not to be loaded after re-boot. As a result, `cpconfig` will not display the interface afterwards (even if it was displayed the first time). To work around this (if it happens), remove the address from the windows registry as follows:

a. Using `regedit`, browse to:

HKEY_LOCAL_MACHINE/SYSTEM/currentControlSet/Services/*interfaceName*/parameters/

b. Replace *interfaceName* with the card name (for example, E100B1).

c. Edit the key named "NetworkAddress" (under the key above) and replace its value with an empty value.

d. Reboot the machine.

Now the card should be loaded with its original MAC address.

This procedure should be also used to restore the original MAC addresses when uninstalling the High Availability Module on NT).

e. Run `cpconfig` and try to export from this machine to the others.

If this does not help, try to replace the manufacturer 24 bytes with 00:00:00 (the 3 on the left) on all machines.

2 In the `cpconfig` **High Availability** tab, pressing F1 does not display the help window. Use the **Help** button instead.

Solaris only

1 When continuing a High Availability machine that was stopped using Stop+A (on the keyboard), control may be returned to the machine unnecessarily (for example, even when the active machine has *not* failed).

Visual Policy Editor

1 Windows 9x is not supported.

2 Definitions and Security Policies can be saved in local mode only and *cannot* be saved on a Management Server.

Meta IP

IMPORTANT — This version of MetaIP (Version 4.1 SP3) implements a new licensing mechanism. MetaIP Version 4.1 SP2 licenses are still valid, but new installations require a license from Check Point (from http://license.checkpoint.com). If you are integrating MetaIP with other Check Point products, you must also obtain a new license.

VPN-1/FireWall-1 UAM Integration

A document (`FW-1-UAM-41-SP3-Integration.pdf`) describing VPN-1/FireWall-1 UAM Integration is on the CD in the `Docs` directory.

This document provides late breaking or other information that supplements the Meta IP 4.1 SP3 `README.TXT` document, the Meta IP 4.1 White Paper, the FireWall-1 Meta IP 4.1 UAM Integration White Paper, the Novell Meta IP 4.1 UAM Integration White Paper, and the Meta IP 4.1 User's Guide. Refer to the `README.TXT` file for information on installation and supported platforms.

The Meta IP 4.1 User's Guide is available from http://www.metaip.checkpoint.com/supportcenter/library/.

The White Papers are available from http://www.metaip.checkpoint.com/reference/.

Note –

- For a list of all the changes in Meta IP 4.1 SP3, see the `Metaip41sp3-Changes.txt` file located in the metaip installation directory or in the Docs folder of your Check Point CD.
- The latest version of these Release Notes is available at http://www.metaip.checkpoint.com/supportcenter/library/41sp3releasenotes.txt.

Meta IP/UAT 4.1 SP2 to SP3 Configuration Changes

The three previously required configurations are no longer required on your PDC or BDC. If you are upgrading to SP3 from SP2 you can make the following configuration changes to reverse the options you instituted for SP2 as desired on your network.

- You may turn off the Windows NT option to monitor logon and logoff events.
  1. Choose **Start➤Programs➤Administrative Tools (Common)➤User Manager**.
  2. Select **Audit** from the **Policies** menu.
  3. Remove **Success** and **Failure** of the **Logon and Logoff** option in the **Audit Policy** window.
- You may turn on the Windows NT options to monitor the File and Object Access.
  1. Choose **Start➤Programs➤Administrative Tools (Common)➤User Manager**.
  2. Select **Audit** from the **Policies** menu.
  3. Remove **Success** and **Failure** of the **FIle and Object Access** option in the **Audit Policy** window.
- You may restore autodisconnect to 15 minutes.
  1. The autodisconnect feature determines the time period during which a shared connection may remain idle. The setting `-1` turns off autodisconnect.

```
net config server /autodisconnect:15
net stop Server
net start Server
```

Meta IP/UAM Novell integration installation issues

Verify installation of NLM elements prior to initializing the MIUAT.NLM

The majority of these files are automatically loaded on your server; however, verify that these elements are installed:

- calnlm32
- clib
- clxnlm32
- dsevent
- locnlm32
- netdb
- nlmlib
- tcpip
- unicode

MIUAT.NLM should not be used with Windows NT PDC Background Authentication

Novell clients running on Windows 95, 98, and NT can be directed such that they authenticate against a Windows NT PDC in the background and a Novell server in the foreground. Review your installation carefully. If you have Windows NT PDC authentication in the background, do not use the MIUAT.NLM. Instead, install the Meta IP UAT on the Windows NT PDC according to the instructions in the Meta IP 4.1 White Paper (see http://www.metaip.checkpoint.com/reference/).

Reload MIUAT.NLM to Complete Configuration Changes

When configuring MIUAT.NLM with MIUATCFG.NLM correctly the tool will return the comment that the configuration completed successfully. MIUATQRY.NLM will also show the new updates. Note that MIUAT.NLM must be reloaded prior to the changes taking effect.

Path for MIUAT.NLM Log File Must Exist

When assigning the location of the log file for MIUAT.NLM, the path to the log file must exist. New directories will not be created for this file.

Meta IP/UAM Novell Integration — Known Problems

Problem — Novell server unloads DSEVENT.NLM.

When unloading MIUAT.NLM, the Novell server will sometimes unload DSEVENT.NLM. MIUAT.NLM cannot be reloaded prior to DSEVENT.NLM being reloaded.

Resolution: If an error is encountered when reloading MIUAT.NLM the user must enter the command load DSEVENT.NLM. This will resolve the situation and MIUAT.NLM can be reloaded without further error.

Cause: Novell servers contain a linking error that can cause modules loaded by primary modules to be unloaded with the primary module.

Problem — Error when logging a log off event.

When logging a log off event on Novell 5.0 SP1 and Novell 5.0 SP2 servers two events are generated by the Novell Server.

Resolution: When manually reviewing the audit table of the UAM, there will be two log off records. Each will show the same time, user, and domain. Ignore one of the records.

Cause: This is a known bug with Novell servers. Novell is working on resolving the problem in a future release of Novell server.

Index