Check Point® Enterprise Suite
Next Generation with Application Intelligence (R55)
Resolved Limitations from (R54) to (R55)
November 19, 2003

Introduction
This document contains former release notes that were released with NG with Application Intelligence (R54) and were resolved by the release of Next Generation with Application Intelligence (R55).

These are not the Release Notes.
The latest available version of the Release Notes can be found at:
http://www.checkpoint.com/techsupport/ng_application_intelligence/releasenotes.html

Resolved Limitations since Next Generation with Application Intelligence (R54)

In This Document

<table>
<thead>
<tr>
<th>FireWall-1 Resolved Issues page 1</th>
<th>SmartView Reporter Resolved Issues page 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartCenter Resolved Issues page 2</td>
<td>Performance Pack Resolved Issues page 5</td>
</tr>
<tr>
<td>VPN-1 Resolved Issues page 3</td>
<td>ClusterXL Resolved Issues page 6</td>
</tr>
<tr>
<td>SecuRemote/SecurePlatform Resolved Issues page 3</td>
<td>FloodGate-1 Resolved Issues page 6</td>
</tr>
<tr>
<td>SecurePlatform Resolved Issues page 4</td>
<td>SmartDirectory (LDAP) Resolved Issues page 7</td>
</tr>
<tr>
<td>SmartView Monitor Resolved Issues page 5</td>
<td></td>
</tr>
</tbody>
</table>

FireWall-1 Resolved Issues

Installation and Upgrade

1) On Windows XP SP1 machines, after the installation from the wrapper completes an application error message on IKernel.exe may be displayed. This problem is a result of a conflict between Window XP Hotfix Q328310 and InstallShield engine. To correct this problem, please follow the step described in:
http://support.installshield.com/kb/view.asp?articleid=q108020 or

Last Update — November 19, 2003
Resolved Check Point NG with Application Intelligence (R54) to (R55). Last Update — November 19, 2003

Platform Specific - Windows

2) To Enable FireWall-1 SNMP extension for Windows perform the following steps:
   Install Microsoft’s SNMP service on the FireWall-1 Module machine. Run the
   following from the FireWall-1 module command line command: cpsnmp_config add.

Platform Specific - Linux

3) Connection are being dropped when working with a T3 WAN serial card with the
   error message fw_filterout: invalid header length. The problem is with a wrong
   calculation of the WAN packets header length. Please contact support for a specific fix
   for this problem.

NAT

4) When you have a network that is contained inside another network and you wish to
   define a different hide translation, the effected translation is the one that is defined for
   the network which contains the new hide translation network.

Security Servers

5) SOAP connections will not fail when using a SOAP URI resource and the Exception
   Track property of the resource is set to None.

6) If both of the following options are activated in the CVP tab of the URI resource:
   a. send only unsafe MIME types
   b. return data before content is approved
   Then when installing a policy with a URI resource that has CVP installed, some of the
   HTML pages arrive incorrectly. Disable either of the two options above, preferably
   option “b”.

7) When using the HTTP Security Server, RealPlayer connections that use HTTP ports
   are dropped.

SmartCenter Resolved Issues

Management High Availability

1) After establishing SIC with a Secondary Management, perform cpstop and cpstart on
   the Secondary Management before synchronizing it.

SmartConsole Applications

2) Opening one SmartConsole Client from another SmartConsole Client is now enabled
   using all authentication methods, including SecurID, operating system password etc.
   Any passwords longer than 10 characters used to be abbreviated, now they are
   supported.
VPN-1 Resolved Issues

PKI, PKCS

1) After upgrading from NG FCS or NG FP1 to either version of NG with AI (direct upgrade or gradual, through NG FP2 and NG FP3), CRL recreation using the Internal CA management tools is supported only after transitioning to the new CRL mode (available since NG with AI). In order to perform this transition please consult Secure Knowledge solution sk22050.

NAT with VPN

2) The use of the option that disables NAT (in the community) is applicable to hide NAT and not to static NAT.

Office Mode

3) The use of Office Mode anti spoofing (configurable in the Remote Access tab of a VPN-1 Gateway) may cause connectivity problems on clusters. The reason is that when using the Office Mode IP pool for each member, cluster members may not be familiar with IP addresses allocated from pools of other members and may drop the packets. The work around is to define a new group that will contain all Office Mode IP pools for the cluster and select it in the om_additional_ip_for AntiSpoofing selection box.

4) If your Remote Access VPN is configured where Office Mode is in use and the feature to route through a different interface is in use and you run your VPN-1 gateway on either the Linux platform or on SecurePlatform you may experience connectivity issues when trying to setup a VPN connection with the gateway. Please contact support for a relevant fix.

VPN-1 and SecuRemote/SecureClient Issues

5) Back Connections (e.g. use of X.11) from a VPN-1 gateway to SecuRemote/SecureClient are not supported when using IP pool NAT for those clients. Please contact support for a relevant fix if needed.

6) Scenario - Visitor Mode server and ClusterXL HA in Legacy mode Problem - It is not possible to define a specific listening IP for the Visitor Mode server bind IP address, only the "All IPs" option is available (this is also the default). WA - none.

SecuRemote/SecurePlatform Resolved Issues

Installation, Backward Compatibility, Upgrade

1) If after upgrading management to NG with Application Intelligence (R55), you encounter CPMI General Error while trying to save SecureClient package to SDS server, please run following command lines on the upgraded management:
sdsutil p user_name password localhost -command createCL CL_SC_NT
sdsutil p user_name password localhost -command createCL CL_SC_9X
sdsutil p user_name password localhost -command createCL CL_SC_2K

Office Mode

2) The use of Office Mode anti-spoofing (configurable in the Remote Access tab of a VPN-1 Gateway) may cause connectivity problems on clusters. The reason is that when using the Office Mode IP pool for each member, cluster members may not be familiar with IP addresses allocated from pools of other members and may drop the packets. The work around is to define a new group that will contain all Office Mode IP pools for the cluster and select it in the om_additional_ip_forAntiSpoofing selection box.

3) If your Remote Access VPN is configured where Office Mode is in use and the feature to route through a different interface is in use and you run your VPN-1 gateway on either the Linux platform or on SecurePlatform you may experience connectivity issues when trying to setup a VPN connection with the gateway. Please contact support for a relevant fix.

Desktop Security

4) If a desktop has several active network interfaces and the desktop element is location restricted then when defining desktop security rules, the following occurs: Location restricted rules will be matched according to the IP addresses of all active network interfaces. When one of the of the active network interfaces is down, the location restriction which was defined by that network interface IP address, will still be applicable for the other (still active) network interfaces.

Secure Configuration Verification (SCV)

5) AntiVirusMonitor supports McAfee's VirusScan 7.1.0.

6) Secure Configuration Verification HotFix monitor checks only Microsoft hotfixes of type Qxxxxxxx. It does not support other types (e.g. KBxxxxxxx).

SecureRemote/SecureClient Issues

7) The following scenario does not work: When SecureClient is using a profile that implies Route All Traffic Through the Gateway and Office Mode and Tunnel All protocols over TCP and TCPT is configure to use a proxy server which relays on the same network like the client, or the same network like Gateway.

SecurePlatform Resolved Issues

General

1) The error message: cpboot: [FAILED] appears on the console during the first boot. This message can be safely ignored. The message disappears when you complete installing your Check Point Products.

2) Network installation from a Windows based FTP Server is not supported. Use Linux based FTP Server.
SmartView Monitor Resolved Issues

Installation, Backward Compatibility, Upgrade

General

1) SmartView Monitor history tables will not be updated if you change the Modules system time substantially backward. To work around this problem you need to stop the module and run a utility that will clean the tables of records that still have later time than the current time. To do this Perform the following:
   a) run cpstop -fwflag -proc
   b) run "upgrade_persistency -clean"
   c) run cpstart

SmartView Reporter Resolved Issues

Installation, Backward Compatibility, Upgrade

1) The export mechanism of the advanced upgrade does not copy the logo files. Before performing an advanced upgrade, save logo files (.jpg, .png) found in the directory $RTDIR/bin and restore them following the advanced upgrade.

2) In NG with Application Intelligence we have added new attributes to filter reports by: URL and interface. After upgrade from NG FP3 to NG with Application Intelligence, some of the reports will not be able to use these new attributes. If you wish to use these attributes to filter your reports, you can do one of the following: Use the Tools > Restore Default Settings menu option. This option restores the default settings of the report and adds URL and Interface to the attributes list in the Filter tab. All custom definitions you made will be restored to default (and therefore lost). Refer to item SK20136 in SecureKnowledge database. Download the utility UpgradeFilters. This utility adds the missing filter attributes to the reports without losing their content. Place this utility in directory $RTDIR/bin on your SmartCenter machine run the cpstop command, run the UpgradeFilters command, run the cpstart command.

3) The SmartCenter package can be removed from a server without testing for dependence upon the SmartView Reporter add-on. If the SmartView Reporter add-on is installed on the server when the SmartCenter is removed, the SmartView Reporter will not be functional and information will be lost when it is subsequently connected to a new SmartCenter server.

General

Performance Pack Resolved Issues

Accelerated Features

1) SecureXL acceleration for GRE traffic was added.

2) ClusterXL Load Sharing Multicast and Unicast modes are now supported by Performance Pack on the Solaris Platform and on SecurePlatform.
ClusterXL Resolved Issues

General
1) Active FTP now works with static NAT and Load sharing configuration with Performance Pack enabled.

2) Fixed a problem which caused the following error message to appear on the console: fwha_receive_fwhap_msg: received incomplete HAP packet (read 48 bytes). It should no longer appear.

Configuration
3) Fixed a problem which caused failover during policy installation on clusters on which disconnected interfaces are defined.

FloodGate-1 Resolved Issues

General
1) The messages: FG-1: cannot create opaque for chain c910045c (fg_chain) and FG-1: Unable to create Logging Stat that may appear on the console from time to time can be safely ignored. On Windows platforms the message appears in the Event Viewer.

Platform Specific - Linux
2) On some Linux machines the etmstart command fails with the following error message: Unable to open /dev/etm0: No such file or directory

3) If you get this message, do the following:
4) Edit the $FGDIR/bin/etmstart script and replace the following line:
5) cd $FG_BOOT_DIR/modules;/bin/tcsh etm.mkdev with
6) cd $FG_BOOT_DIR/modules;/bin/tcsh -f etm.mkdev
7) Reboot the machine.

QoS Verifier
8) If a new object (of any type such as: service, network object etc.) was added to the database and the QoS verifier was activated without saving the object first to the QoS Policy operation, the QoS verifier may malfunction. To overcome this problem, save the QoS policy and then verify the QoS policy.

Citrix ICA
1) It is possible to define an Express mode QoS policy with services of type Citrix TCP. However, Citrix ICA applications are not supported in an Express mode policy. Citrix TCP rules are regarded as regular TCP services and all traffic on port 1494 (Citrix ICA port) is matched to the Citrix TCP rules.
**SmartDirectory (LDAP) Resolved Issues**

**LDAP**
Microsoft Active Directory disabled accounts no longer pass VPN-1 & Firewall-1 Password Authentication. The SmartDirectory (LDAP) server does not enforce this user limitation directly. This is now enforced by Firewall-1 by evaluating the userAccountControl user attribute as referenced by Firewall-1’s Microsoft_AD profile's AccountDisabled attribute. Other External Authentication methods, such as SecureID, do not enforce this user limitation and this should be enforced on authentication server being used.

**GUI**
When using Active Directory .NET (2003) with NG_AI errors are encountered while changing the account expiration user attribute. When adding a value instead of a template value or when removing an existing value to use the template one. Using AD 2000 does not cause these errors.