Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

What's New in Check Point® Enterprise Suite Next Generation with Application Intelligence (R54)

June 2, 2003

In This Document

Check Point Enterprise Suite Installation

1) The new upgrade provided by the Check Point installation CD allows you to upgrade your SmartCenter Server on the same production machine or to a new production machine. During the upgrade your configuration is first verified, and the installation downloads automatically upgrade software updates, to assists in completing the upgrade safely and smoothly.

2) This new upgrade allows changing the machine, platform and Operating System as part of the upgrade process.

3) In order to minimize production systems disruptions, the new upgrade process allows you to perform the following steps:
   - export and verify your production configuration to a new hardware system.
   - perform the upgrade to NG with Application Intelligence on the new system.

- The upgraded configuration may be maintained on the new system, or migrated back to the original hardware system.

FireWall-1

Stateful Inspection

Out-of-State ICMP

1) In NG with Application Intelligence the option to accept out-of-state ICMP messages is included. This option is available from **Global Properties** > **Stateful Inspection**.

Sequence Verifier

2) The TCP Sequence Verifier security feature validates the sequence numbers of each TCP packet going through Firewall-1. In NG with Application Intelligence a new mode was added to the TCP Sequence Verifier, that keeps track of the connections' sequences and performs related security decisions without dropping out-of-sequence packets. This mode, which is referred to as "database mode", is the default for FireWall-1 for NG with Application Intelligence (except for upgrades from NG FP3 machines that had sequence verification previously enabled).

Two new security features are implemented in the database mode:

1 Connections table DoS attack prevention

An attacker may send a spoofed SYN packet to a server machine, to which the server is supposed to reply with a SYN-ACK packet. Since the SYN packet was spoofed, the attacker is usually not aware of the SYN-ACK packet's sequence number.

However, the attacker can send a spoofed ACK packet, with a wrong ACK number. A firewall that does not perform sequence verification may wrongly assume that the connection is established because all three-way handshake packets were allegedly encountered.

This causes the Firewall to increase the connection's timeout to the TCP session timeout, which is an hour by default. This provides an easy way to fill the Firewall-1's connections table and cause a denial of service.

When the TCP Sequence Verifier is in database mode, it keeps track of the connection's sequence numbers and does not change the connection's state to "established" when client's ACK number is wrong.

Note -

a SYNDefender provides a comprehensive solution to all SYN flooding attacks, including the one described above. However, SYNDefender causes considerable overhead. For instance, on relay mode, each connection starts with a six-way handshake (instead of three-way) and all packets that belong to the connection must undergo sequence translation. Keeping the sequence number of the server's SYN-ACK is a much simpler solution.

b According to the RFC 793, the server's reply to the spoofed ACK packet should be a RST packet, containing the spoofed sequence. Normally, Firewall encounters the RST and decreases the connection's timeout. Therefore, even a Firewall that does not perform sequence verification and increases the connection's timeout would eventually decrease the timeout back. However, the RST packet may get lost on the way between the server and the Firewall, and Firewall should not rely on the server's response in general. To disable this feature, use the Database Tool to set the value of `fw_trust_suspicious_estab` attribute to `1`.

2 Spoofed RST attack prevention

An attacker may send spoofed RST packets over a range of ports. Such an attack can cut existing connections if there is a Firewall on the way that does not perform sequence verification, since RST packets represent connection tear down. To disable this feature, use the Database Tool to set the value of `fw_trust_suspicious_rst` attribute to `1`.

TABLE 1 Available Modes

Mode	Description	Activated when...
On	Drop and log out of sequence TCP packets (Default mode for NG FP3)	The sequence verification checkbox (located in the SmartDefense tab in SmartDashboard) is enabled.

Database	Keep track of connection's sequences and perform security related decisions. Out of sequence packet pass Firewall-1(Default mode for R54).	The sequence verification checkbox is disabled, and one or more of the following attributes is assigned a value as follows:
		`fw_trust_suspicious_estab=`
		`0fw_trust_suspicious_rst=`
		`0fw_rst_expired_conn=`1

Off	Sequences are not tracked.	The sequence verification checkbox is disabled, and all the following attributes are assigned values as follows:
		`fw_trust_suspicious_estab=`
		`1fw_trust_suspicious_rst=`
		`1fw_rst_expired_conn=0`

Use the Database Tool to change the values of the related attributes.

Connectivity Improvements

"Unexpected SYN Response" Messages

When a client tries to establish a new TCP connection using a SYN packet, FireWall-1 expects a SYN+ACK packet reply from the server as a standard procedure of TCP 3-Way handshake. In some situations the server's replies do not comply with the TCP 3-Way handshake. In such cases these reply packets are dropped using **Unexpected SYN response** message. These dropped packets can create connectivity problems.
In NG with Application Intelligence, FireWall-1 allows recovery of such connections as follows:

When the TCP Sequence numbers are enabled (default)

When FireWall-1 receives the "Unexpected SYN response" reply from the server, instead of dropping the packets, FireWall-1 sends RST packet on behalf of the client. As a result, when the client retransmits its SYN packet, the server is willing to establish the connection as expected.

When the TCP Sequence numbers are not available

FireWall-1 reverts to the pre-R54 behavior and accepts the "Unexpected SYN response" replies.

"SYN on Established Connection" Messages

FireWall-1 includes a new feature that solves the connectivity problems related to the **SYN on established connection** messages. These problems are caused by a connection reuse attempt.

Background

Connection reuse can happen when the state of connection in the FireWall-1 connection table does not match the actual connection state known to the client and server. As a result, attempts to establish a new connection using the same source IP, source port, destination IP and destination port fail. This can happen in one of the two following cases:

- the connection was not closed by the client or server.
- the connection was closed by the client by sending an RST packet that didn’t reach FireWall-1.

Solution in NG with Application Intelligence

FireWall-1’s Stateful Inspection for NG with Application Intelligence includes a mechanism that attempts to maintain connectivity in connection reuse situations by:

- trying to probe the participating hosts true state and synchronizing FireWall-1's connection table instead of

- dropping the SYN packet and disrupting connectivity.

When a client tries to reuse a TCP connection that is in an established state in FireWall-1 connections table (by sending a SYN packet), FireWall-1 allows this packet, but converts it to an ACK packet. Based on the server's response to this ACK packet, FireWall-1 detects the true connection state and adjusts itself accordingly.

HTTP

UFP Performance Improvement

1) A new UFP mode has been added in order to increase performance. In the new UFP mode, the connection is handled by TCP streaming in the kernel and do not go through the HTTP Security Server. This feature is configured in **Enhance UFP performance** mode in the **URI Resource** Properties window.

CVP Performance Improvement

2) When using CVP it is now possible to send only unsafe file types to the CVP server for inspection. Safe MIME types (such as .jpg and .gif images) are sent directly to the client. The detection is based on MIME types in the **Content-Type** HTTP header and also a verification of the magic numbers of the files themselves in order to maintain maximum security. This option is set through checking the **Send only unsafe MIME types to CVP server** in the **URI Resource Properties** window.

Cross Site Scripting (XSS)

3) FireWall-1 for NG with Application Intelligence introduces the concept of a Web Server object. Define your Web Server (as a product running on a Node object) from the Node’s **General Properties** window under **Products** by checking **Web Server**.

   Web Servers are protected by Check Point’s Application Intelligence technology against Cross Site Scripting attacks (XSS). The protection is done by filtering HTML tags from the data submitted on Web forms. It is possible to filter only dangerous tags and keywords - `<SCRIPT>` or to filter all HTML tags (by searching for the character “<”). FireWall-1 has the ability to decode UTF-8 and other encoding types, so these tags are also detected when there is an attempt to hide them using character encoding schemes. A new property page was added for Web Server enabled objects. Once you have **Web Server**, this page appears in your **Host Node Menu**.

There is a centralized view of XSS protection settings in SmartDefense under **Application Intelligence** > **Cross Site Scripting**.

Peer to Peer (P2P) detection in the kernel

4) HTTP header signatures (used for P2P and other application detection) are now performed in the kernel using TCP streaming for greater performance. These signatures can now be defined in the SmartDefense GUI. In addition, new services were added for popular P2P and messaging application ports. These services are included in the **P2P_File_Sharing_Applications** and **Messaging_Application** Service Groups.

HTTP Protocol Inspection

5) FireWall-1 now performs HTTP verification for connections being inspected using the kernel TCP streaming (such as quick UFP, P2P and worm catcher). These checks were previously available only in the HTTP Security Server.
These verifications include:
   - **HTTP format sizes** – Enforce the maximal length of URLs and HTTP headers and the maximal number of HTTP headers.
   - Prevention of binary data in HTTP requests.

It is possible to choose between optimized (TCP streaming) and strict (Security Server) protocol enforcement in SmartDefense under **Web Security** > **HTTP Protocol Inspection**.

Streaming XL

6) Connections using TCP streaming in the kernel can now be accelerated with SecureXL.

HTTP Encoding

7) FireWall-1 is able to decode non-ASCII encoded characters in URLs and HTML content. Character encoding are used for the following reasons:
   - To represent non-viewable characters to the user. The ASCII table contains only Latin characters so in order to represent foreign languages, a different system must be invoked.
   - Web servers sometimes use character encoding to hide the content (especially locations) from users.
   - To represent special control characters in a way that will not be parsed by the web servers to their special meaning.

For example

Using the less than sign "<" in HTML without delimiters is ignored since it is used as a HTML tag delimiter (<H1>). Encoding solves this by using a special entity "`&gt;`" (<`&gt;`) which is viewed by users as "<" and not parsed as an HTML tag.

It is possible to encode both the URL and the data served by the server. The encoding of the URL is usually parsed on the server side, while the client's browser usually parses the encoding of the HTML data.

Character encoding can be used in an attempt to bypass FireWall-1 URL filtering and HTML weeding.

For example the URL:

http://host/bad_page.htm

Can be represented as:

http://host/%62%61%64%5f%70%61%67%65%2e%68%74%6d.

FireWall-1 is able to decode the following encoding methods into ASCII and then run the filters over the result:

Hex encoding: The most basic encoding. Each character is represented by a percentage sign ("%") followed by its ASCII value in hex. For example, the letter 'a', which ASCII hex value is 61, is represented by "%61".

Numeric reference encoding: Another basic encoding. Each character is represented by an ampersand sign ("&") followed by a hash sign ("#"), followed by the ASCII value of the character, followed by a semicolon (";"). There are actually four variants of this encoding, where:

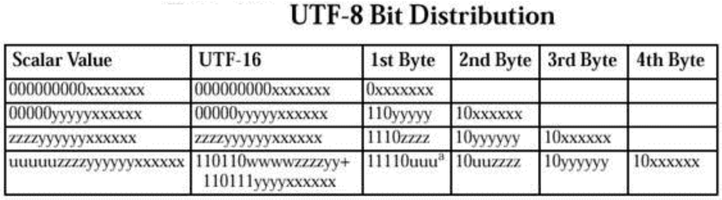
- the ASCII value is in presented decimal
- in hex (in which case a "x" sign should precede it),
- and two other variants are achieved by removing the semicolon at the end, which many browsers do not require.

For Example

To represent the letter 'a', you can use: "&#97;", "&#x97;", "&#x61;" or "&#x61".

UTF-8 and UTF-16 encodings: explains how to implement these encodings:

UTF-8 Bit Distribution



UTF-8 Bit Distribution

Scalar Value	UTF-16	1st Byte	2nd Byte	3rd Byte	4th Byte
000000000xxxxxxx	000000000xxxxxxx	0xxxxxxx			
00000yyyyyxxxxxx	00000yyyyyxxxxxx	110yyyyy	10xxxxxx		
zzzzyyyyyyxxxxxx	zzzzyyyyyyxxxxxx	1110zzzz	10yyyyyy	10xxxxxx	
uuuuuzzzzyyyyyyxxxxxx	110110wwwwzzzzyy+ 110111yyyyxxxxxx	11110uuu[a]	10uuzzzz	10yyyyyy	10xxxxxx

Services

Improved Non-server Port Check

8) The security check done for FTP (and other protocols) data connections when not using a well-known server port has been improved by adding a new mode that checks only specific services ports. It can be defined in the SmartDefense GUI.

DNS

9) There is now added support for DNS verification of EDNS queries. DNS verification speed has been improved by over 50%. DNS query information is now logged and displayed in the **Information** column of SmartView Tracker.

10) Added EDNS support.

11) Added DNSSEC support.

12) Added support for Notify and Update messages and their extensions for Windows 2000 Active Directory.

SSHv2 Verification

13) It is possible to verify that SSH connections are using version 2 or higher of the protocol in order to prevent known security problems from earlier versions of SSH. SSHv2 enforcement is enabled using the **ssh_version_2** service.

SSLv3 Clients Verification

14) It is possible to verify that SSL client connections are using version 3 or higher of the SSL protocol in order to prevent security problems known with earlier versions of SSL. SSLv3 enforcement is enabled using the **ssl_v3** service.

FTP BASIC protocol type

15) FTP_BASIC is a new protocol type. This protocol type enforces a reduced set of the FTP security checks done by the regular FTP protocol type. This protocol type eliminates known connectivity problems with FTP related to New Line enforcement (NL) and server port checking in the standard FTP protocol type.

New FTP Enforcement Algorithm

16) Included as an experimental alternative to the regular FTP enforcement in this release. The new algorithm does not require that each packet is terminated by a NL (new line) character and it offers better connectivity. Enable it by uncommenting the following line in base.def:

```
//  #define FTP_CHECK_PACKET
```

DCE-RPC

FireWall-1 now displays the UUIDs used by DCE-RPC Services in SmartView Tracker. A new Service called ALL_DCE_RPC matches any DCE-RPC UUID, this Service can be used for discovery of UUIDs used by different Services.

CIFS

A block remote registry connections option has been added to CIFS resources.

New Default Services

Added new service objects for ports used by common P2P (peer-to-peer) applications, Instant Messaging applications and Trojans. These services allow effective control and identification of these applications

VoIP

SIP

RFC 3261 support

17) FireWall-1 is now compliant with the new SIP RFC 3261 (except for SIP over TCP).

Instant Messaging

18) Support has been added for instant messaging using SIP for direct peer-to-peer connections.

Multiport Commands

19) Support has been added for SIP phones negotiating more than one data port in the same control connection.

Registration Using Domain Names

20) Support has been added for SIP phone registration messages. Messages can now contain domain names and phone numbers.

SIP Content Verification

21) FireWall-1 inspects SIP traffic and protects against recently published SIP vulnerabilities. This feature can be configured via SmartDefense.

New 'fw tab' Command Line Options

22) `fw tab -t sip_registration -f` displays formatted information on the SIP registration database.

23) `fw tab -t sip_state -f` displays formatted information on active SIP connections.

H.323

GateKeeper in DMZ Support

24) FireWall-1 now supports a VoIP deployment where the H.323 GateKeeper is located in the DMZ. In addition, FireWall-1 supports additional RAS messages that flow between IP phones and the GateKeeper. These messages are:

- **ARQ/ACF** – Admission Request and confirm messages.
- **RRQ/RCF** – Registration Request and confirm messages.

FireWall-1 keeps a registration database mapping IP phones to their addresses based on the RAS traffic between the IP phone and the GateKeeper.

H.245 tunneling

25) Support has been added for H.245 tunneled connections where the H.245 messages are sent via the H.225 channel.

NAT

SmartCenter Server behind NAT

26) Network Address Translation for the SmartCenter Server IP address can be easily configured. Static or Hide NAT can be configured on the SmartCenter Server address, while still allowing connectivity with managed modules. When using Hide NAT, an inbound connection coming from a managed module to the hiding address, is port mapped to the real IP address of the SmartCenter Server. To enable NAT for the SmartCenter Server address, check **Apply for VPN-1 & FireWall-1 control connections** in the **NAT** page of the SmartCenter Server object.

IPv6

27) In NG with Application Intelligence, FireWall-1 supports IPv6 out of the box.

Supported platforms

- Solaris 8/9
- Nokia IPSO 3.7

Supported features

- Dual stack – both IPv6 and IPv4 on the same interface.
- IPv6 access control with accept/drop/reject actions and the tracking options are: none/log/account.
- Simple TCP, UDP and ICMPv6 services.
- IPv6 FTP service (active and passive).

  - IPv6 Host and Network objects.
  - Using IPv6 & IPv4 objects in the same rule base.
  - IPv6 logging and IPv6 filters.
  - Implied rules for enabling traffic needed for IPv6 discovery
  - IPv6 fragments
  - Using IPv6 requires a special license which is not included in the trial period and EVAL licenses.

Authentication

28) VPN-1/FireWall-1 now supports all RADIUS attributes (RFC 2865). This eliminates the need to use the `:radius_ignore` property.

Platform Specific - Linux

To get large amounts of memory on Linux machines with 1GB memory or more, perform the following actions:

1. Create a file named `fwkern.conf` in `$FWDIR/boot/modules/`
(it may already exist - if so, keep the current contents).

2. Add the following two lines to the file:

```
fw_smem_use_alternate_malloc=1
fw_hmem_use_alternate_malloc=1
```

3. Reboot the machine.

SMTP Security Server

- RFC 2821 compliance improvements:
Use blank <`mail from`> header when sending error messages
- Added support for CNAME records when using MX resolving.

ConnectControl

- New Load Agent for Linux platforms
- Load Agent improvements for Windows:
  - Windows 2000 support
  - New algorithm for load calculation, the Load Agent now supports the full load average options like the Unix versions (load for the last 1,5,15 minutes)

SmartDefense

Automatic Updates

1) SmartDefense can be updated by automatically downloading updates from the SmartDefense web site. The following are examples of these updates:
   - Protections against various attacks such as HTTP and MS File and Print sharing protocol (CIFS) Worms.
   - Enhancements to the SmartDefense INSPECT code.
   - Protection against new attacks
   - Point-to-point application signatures

2) Updates and advisories are available to licensed customers. To receive these valuable and important security advisories, and to obtain SmartDefense updates, registered users are required to authenticate using their User Center credentials. Advisories can be accessed with a valid SmartDefense subscription license. For more information about creating User Center accounts go to the User Center at:

   http://www.checkpoint.com/usercenter

IP Fragments

3) New capabilities of IP Fragments reassembly were added to SmartDefense. The following are examples of these capabilities, the System Administrator can:
   - configure whether or not fragmented IP packets are allowed to pass through SmartDefense gateways.
   - configure the way SmartDefense handles packet fragments.

Network Quota

4) A new protection against Denial Of Service attacks is achieved by enforcing a limit upon the number of connections that are allowed from the same source IP address.

Fingerprint Scrambling

5) By scrambling some of the fields that are commonly used for the Operating System fingerprints, the original identity of the hosts that are behind SmartDefense gateways is masked.

MS Networking Protocols

6) Protections against various attacks that are using MS Networking Protocols are available. The following are examples of these protections:

- stop Worms that are propagated using CIFS (Common Internet File System), also known as SMB.
- block the Windows messenger service.
- protect against `NULL` Session attacks on mis-configured CIFS servers.

SmartCenter

Upgrade and Migration

The new upgrade utilities allows you to:

- verify your configuration prior to the upgrade,
- export your configuration from your production machine *and then*
- import and upgrade it on a new machine.

This transition can be done between various platforms and operating system, while all the necessary conversion is done automatically. These utilities can also be used for migration from one SmartCenter Server NG with Application Intelligence to another, and for fast and safe backup and restore.

SmartView Tracker

1) The Centralized views now enable you to see all records of a certain Source, Destination or User. These views can be opened by right-clicking a certain log-record.

2) The Remote Command enables you to run commands on a remote machine. The remote machine can be the source, destination, origin or user of a log record. In addition to the pre-defined `ping` and `whois` commands, more commands can be configured.

3) The improved **Audit** view allows for easy recognition of the audit log type with a new column that classifies the **audit log subject** and **icon**.

SmartCenter Login Security

4) SmartCenter server allows you to lock administrator after a certain amount of sequential login failures. Lock out and unlock of administrators can be monitored from SmartView Tracker.

OPSEC

5) Configuration of Remote Access for Roaming Administrator client is done by checking **Allow remote registration of OPSEC products** in the **OPSEC** tab under the **Global Properties** of the SmartDashboard instead of using the `cpra.conf` configuration file.

6) The Recognition of an AMON schema of OPSEC application with no private schema is done automatically by SmartCenter based on the definition of the OPSEC Application Object. Therefore it is no longer necessary to define private schema only to support the specific OPSEC services (CVP, UFP, LEA, ELA, CPMI, SAM) schema.

7) 42 new OPSEC certified products were added to the list of predefined OPSEC certified products. This list is available when you define a new OPSEC application object.

Managing FireWall-1 GX

1) An Application Intelligent SmartCenter can manage FireWall-1 GX 2.0 modules. In order to do this, a FireWall-1 GX management license needed to be used. Application Intelligent enforcement modules do not include FireWall-1 GX functionality. See *Managing FireWall-1 GX* in the *"Upgrade and Backward Compatibility Notes*" of the Release Notes for information on upgrading FireWall-1 GX 2.0 Management Only hosts to the NG with Application Intelligence SmartCenter.

VPN-1

Hub Mode (VPN Routing)

1) Simple scenarios of Hub Mode are now supported in SmartDashboard:
   - Hub & spokes support on star community: routing traffic between satellites through the center of the star.
   - Routing traffic from the satellites in the star community to the Internet through the center of the star.
   - Routing traffic from the satellites to VPN gateways that are not part of the star community through the center of the star.

2) By supporting Hub Mode for remote access VPN clients, VPN-1 now offers an alternative for split tunnels. VPN-1 clients and VPN-1 modules now support routing of traffic from the client through the gateway, enabling two options:
   - Split tunnels (the traditional way): traffic goes through the tunnel only if the destination is part of the VPN domain of the specific gateway or
   - Eliminate split tunnels: routing all traffic through the gateway, including traffic to the Internet and to destinations protected by other VPN-1 gateways.

3) VPN client to VPN client connectivity is now supported when using Hub Mode for Remote Access VPN clients. This is done by using the VPN-1 gateway as a relay among clients so that traffic from one client can reach another, passing through the IPsec tunnels both clients have created with the same VPN-1 gateway.

4) A route injection and a tunnel maintenance mechanism are now available:

- **Route Injection:** When a tunnel changes status, a custom-made script can be used for routing purposes. Once this script is installed, a VPN-1 gateway can send a report to its protected domain with the status of networks at the other side of the tunnel as available or unavailable. Hosts in the internal network can then route traffic accordingly.
- **VPN tunnels keep-alive:** Using a periodic test packet you can keep the IPsec tunnel alive and detect any tunnel status change.
- This mechanism is integrated with MEP functionality.

High Availability, Load Sharing (MEP/SEP) Load Balancing

5) Interface resolving mechanisms (Dynamic/Static) for third-party clusters are now supported for cases where interfaces are configured on the cluster (for example clusters that are based on VRRP).

VPN Hardware/Software Acceleration

6) VPN Accelerator III is now available. VPN performance is expected to be more than doubled using the accelerator.

IKE Denial of Service Protections

Note - When the DoS protection feature detects that the gateway is under heavy load, it request the peer to perform extra tasks. Older Check Point gateways and clients as well as third party devices cannot perform those tasks, therefore when under attack communication with they fail. Very heavy loads may be mistakenly interpreted as an attack. For a system which is constantly under attack, this may cause interoperability problems.

7) Protection against IKE Denial of Service attacks is now available in VPN-1 systems. This enables protection against IKE negotiations flooding. Optionally:
   - It prevents an attacker from pretending to be a known friendly VPN peer by using a spoofed IP address.
   - The Gateway under attack forces the peer machine (attacker) to perform a task (e.g. solving a puzzle) before it will agree to continue the negotiation. This task prevents the peer from initiating multiple IKE negotiations from the same (or from several) machines simultaneously.

PKI, PKCS

8) Replacing a CA certificate with a newer one in a VPN-1 system is now supported, assuming that the new certificate has the exact same pair of keys as the old one had.

Internal CA Management

9) A new set of web based management tools for the Internal CA is now available.

Features highlights:

User Certificates management

- Search
- Revoke
- Remove

User Certificates creation

- for ANY DN (not just for internal entities)
- Based on text files created from ldap_search operation

Bulk operations are enabled

CA properties configuration/tuning

CRL management

Internal CA High Availability

10) Internal CA High Availability is now available:

- All management servers are polled for a potential CRL (Certificate Revocation List)
- Stand-by management continues to issue CRLs to ensure a valid CRL for primary management failure.
- A CRL pre-fetch mechanism was added, the mechanism also improves the VPN tunnel setup process by eliminating the CRL retrieval period during tunnel setup process.

VPN Diagnostics (Logging, Monitoring, Planning)

11) To enable better remote access VPN auditing, logging is now available for Remote Access VPN that specifies the user's connect and disconnect actions.

Miscellaneous

12) Interface High Availability enhancements:

- Selection of a primary interface of the destination VPN-1 gateway is now available.
- Interface selection granularity has been improved to per packet. In the past granularity was per connection and when the interface in use went down, a new interface was selected only for new connections. Now VPN-1 can choose a new interface for already active connections.

Office Mode

13) Granular allocation of Office Mode addresses is now available using a configuration file located on the VPN-1 Module:

    - IP per user: a user (using a VPN IPsec client) can be defined to receive exclusive and specific IP address from a certain VPN-1 gateway.
    - IP pool per group of users: ability to allocate exclusive IP pools for certain groups of users. The VPN-1 gateway will allocate IP addresses from the specified pool only to users in the defined group.

14) When the VPN-1 gateway has multiple external interfaces, Office Mode is now functional. The following configuration exists:

    - where one (or more) interfaces are used to connect to the Internet *and*
    - one (or more) interfaces are used to connect to Remote Access VPN (for instance wireless LAN).
    - This feature involves enhanced routing and anti spoofing decisions when Office Mode is in use.

Visitor Mode (TCP Tunneling)

15) Remote Access VPN from a restricted location (disrupting outgoing/incoming VPN traffic) is now enabled. Remote VPN clients that are located at sites where the type of enabled outgoing traffic is very limited (enabling mostly web browsing over HTTP) is now possible using Visitor Mode, which is based on sending VPN traffic encapsulated in a TCP tunnel.

VPN-1 and SecuRemote/SecureClient Issues

16) Enhanced connectivity for broadband remote access users: ADSL and cable modems users often stumble into connectivity issues which can be solved by manually lowering the MTU settings on the client machine (see SecureKnowledge solution sk15830). Instead of having to solve the problem manually, a path MTU discovery mechanism which automatically detects the problem and solves it, is now available.

Nokia Clients (Crypto & Symbian) Support

17) Topology export for Nokia VPN clients is now available from Check Point's SmartCenter. Using the command line interface (CLI) the topology of Remote Access VPN-1 servers can be easily exported to the Nokia topology server (NSSM), to be distributed to the Nokia clients.

SecuRemote/SecureClient

Connectivity Enhancements

1) Remote Access VPN from restricted locations is now enabled. SecureClients that are located at sites with limited access to Internet protocols (e.g. enabling only web browsing over HTTP/HTTPS) can now use Visitor Mode (the ability to send VPN traffic inside a TCP tunnel).

2) In order to solve Path MTU (PMTU) problems, the client performs active MTU discovery (by default) and analyzes ICMP MTU size adjustments.

3) All traffic (not only traffic to the encryption domain) can now be routed through the Gateway per profile.

4) Office mode addresses can now be part of the encryption domain.

Office Mode

5) Client-to-Client encryption is now available via the gateway. Office mode addresses are used for peer identification.

6) Office mode IP assignment can be done per user and/or per group of users (using a configuration file on the module).

7) Anti spoofing is performed on allocated Office mode addresses.

8) Office Mode allocation can now be done through several Gateway interfaces.

Improved Secure Configuration Verification (SCV) infrastructure

9) There is now gateway support for verification without enforcement, which allows for smooth SCV policy transitions.

10) Notifications to the user have been improved, both upon SCV status changes, and connections being blocked due to SCV.

11) In local enforcement an option to disconnect upon unverified has been added.

New Secure Configuration Verification (SCV) products capabilities:

12) Anti-Virus checking is available for Trend Micro, Symantec and McAfee Software.

13) Registry Monitoring enables the checking of registry keys as an SCV check.

14) The ability to run .bat/.exe as SCV checks has been added.

Miscellaneous

15) The ability to run .bat/.exe after each successful connect has been added.

16) CAPI can now be used for SDL authentication.

SecurePlatform

1) The Web GUI now allows you to manage your SecurePlatform machine more easily.

2) NTP (Network Time Protocol) support to allow you to synchronize the clocks in the system.

3) Multiple administrators to allow easy auditing of changes to the SecurePlatform machine.

4) Enhanced Backup (that does not require `cpstop`) and Restore (that restores the network configuration from backups done before the upgrade).

5) SSH and SCP clients on the SecurePlatform machine.

6) Binary Integrity verification during boot (automatically turned off).

7) Dynamic Routing support is now available through a Zebra package included in the SecurePlatform. Enter **expert** mode to configure it.

New Features

8) Until the installation of Check Point products is complete, the `sysconfig` command will operate in the "wizard mode". The wizard mode allows you to configure system settings, install and configure Check Point products.

9) You can install additional Check Point products using the `sysconfig` command. Use option "8" (Products Installation) in `sysconfig` to add new Check Point products.

SmartUpdate

1) SmartUpdate now provides a single-step upgrade of your operating system and Check Point applications for both the Nokia and SecurePlatform platforms. Meaning that in a single step, you can upgrade both the operating system and the security software versions on a security appliance thus simplifying network management of remote appliances.

2) SmartUpdate now supports remotely upgrades of Safe@ devices managed from SmartCenter or SmartCenter Pro.

3) SmartUpdate supports remote installation of OPSEC applications. Administrators can maintain and upgrade content security, authentication, and other OPSEC applications that include support for SmartUpdate, using Check Point's centralized software management tool.

4) A hotfix can be remotely installed and removed using SmartUpdate for easier management and deployment of software fixes.

SmartView Monitor

1) By drilling down using complex filters an administrator can now view traffic on specific narrow scopes. For example, viewing the top IP only for traffic from a specific source network that is done using a specific application service.

2) A view has been added in order to view and manage Suspicious Activity Rules (SAM rules) that are implied on a module. You have the ability to add and remove these rules. Additionally, in Real-Time traffic views, by right clicking on an IP address or a service you can request to block this specific traffic for a limited time.

3) The session configuration tree offers predefined and custom saved views on the left side of the application. This allows for easy access to common views and customization for users.

4) Performance has improved on connection based reports.

5) Connection based real-time reports and history reports were added with lowered performance impact on the module.

6) History views can now be exported to tab and comma delimited files.

7) HTML reports that can be scheduled and distributed in various methods are available through SmartView Reporter. These "Express" reports are based on SmartView Monitor history data.

SmartView Reporter

1) A new set of predefined **Express reports** gives you the ability to generate reports very quickly. Express reports are based on the modules' counters information.

2) The database table you want the report to run on is configurable via the **Reports** tab. In the previous version this parameter was global and could not be defined per single report.

3) A new tab called **Input** has been added to the **Reports Customization** tabs. In this tab you can choose the modules you want to apply to your report. In addition, you can choose whether you want to receive a separate table or graph per module or to combine the information into a single table or graph.

4) You can delete reports from the history list manually or define the size of the history list in the **tools** > **options** menu. The list grows up until the defined history size. Reports are removed in a cyclic manner starting from the oldest report defined.

SmartLSM

1) You can enhance the VPN-1 domain of a ROBO Gateway from only the ROBO Gateway's external IP (as it was in NG FP3) to include the resolved range of any Dynamic Object. When resolving the value of a Dynamic Object per ROBO Gateway, check the check box **Add to VPN Domain**.

2) You can initiate a VPN-1 tunnel directly from a host behind the CO Gateway to a server behind the ROBO Gateway. In NG FP3 this feature was only allowed as a back connection.

3) If the option to use a **single GUI to all Gateways** is deployed in your system, you can view regular Gateways and their statuses in the SmartLSM GUI.

4) SmartUpdate is now integrated with SmartLSM allowing administrators to perform centralized remote software updates to ROBO gateways.

5) Remote Access VPN from SecureClients to a ROBO gateway is now supported.

6) SmartLSM can now manage Safe@ gateways as ROBO Gateways.

7) The SmartLSM Command Line Utility now allows you to perform batch ROBO gateway management operations through scripts.

   - The new `Convert` command line utility allows you to convert a ROBO gateway object to a regular Check Point gateway managed through SmartDashboard (in case the gateway "grows" in size from being a ROBO gateway to a regular gateway) - or to convert a regular Check Point gateway to a ROBO gateway managed through SmartLSM (in case you want to convert a few regular gateways to work in SmartLSM).

Performance Pack

Newly Accelerated Features

1) For increased performance the following SmartDefense features have been accelerated:

   a. General HTTP worm catcher

   b. HTTP protocol enforcement - accelerated when "perform protocol enforcement in kernel" is enabled.

2) For increased performance new resources have been accelerated:

a. URI resource - accelerated when "Optimized for URL logging" is enabled

b. CIFS resource

3) For increased performance, TCP session rate has been improved.

4) The Sequence Verifier is now accelerated.

5) ClusterXL Load Sharing is supported and accelerated on SecurePlatform.

New Features

6) A new feature was added for Performance Pack and ClusterXL called Delayed Synchronization that increases performance. This feature enables selective cluster synchronization based on the connections duration. Synchronization of short connections is common for HTTP traffic pattern. In cases where synchronization is not required (for example, with short HTTP transactions), a time value can be defined for a service. This value indicates that connections terminated before the specified expiration time, will not be synchronized. As a result, in a cluster environment the synchronized traffic is reduced and the overall performance increases.

Supported Features

7) Performance Pack now supports ClusterXL in New High Availability mode on the Solaris platform.

8) Performance Pack is now supported on the Solaris 2.9 Operating System.

ClusterXL

1) A new Load Sharing mode (ClusterXL Unicast Load Sharing mode) enables the usage of unicast based traffic by customers who use legacy routers that do not support the use of a multicast MAC address for a unicast IP address. In Unicast Load Sharing mode, one of the cluster members serves as a Pivot. The Pivot is responsible for forwarding and distributing the traffic throughout the cluster while implementing both load sharing and redundancy solutions. It also permits the user to configure the traffic distribution between cluster members.

2) In Load Sharing configurations (either Multicast or Unicast), there is now a higher level of security by enforcing the TCP handshake order on the Cluster.

3) Internal, External and sync interfaces of multiple clusters can now be connected on the same VLAN.

4) Instead of using a dedicated sync network, it is possible to use the internal or DMZ network for synchronization. The external interface should not be used for sync.

5) In the SmartDashboard, cluster members can now be removed from the cluster object without the cluster member objects being deleted.

6) When a third party cluster provider ensures that both the inwards and outwards packets of the same connection pass through the same cluster member, it is possible to configure the sync mechanism for optimized performance.

7) Cluster IP addresses are protected against address spoofing.

8) Two options are available for enforcing installed policy on cluster members:

- **install on all or non cluster members** - If policy cannot be installed on all members it will not be installed on any member.
- **install on some cluster members** - An icon will appear on SmartDashboard Security tab view to reflect it.

9) ClusterXL manageability has improved.

10) It is now possible to configure cluster topology when working with OPSEC partner's clusters. Please refer to the VPN-1 documentation for more details.

11) The state synchronization mechanism is protected from overflow scenarios.

12) There is better handling of stress scenarios with **Monitoring Active Connections** turned on.

13) Performance Pack is now supported also with ClusterXL New High Availability and Multicast Load Sharing modes on SecurePlatform.

14) Performance Pack is now supported also with ClusterXL New High Availability on the Solaris platform.

15) Performance Pack with ClusterXL Multicast Load Sharing mode **is not** supported on the Solaris platform.

FloodGate-1

Support of Windows Groups using Authenticated QoS

1) This new feature allows QoS where the FloodGate-1 module uses predefined Windows Groups. It does so by querying the UserAuthority Server. Consult the "*Check Point UserAuthority User Guide*" section of the SecureAgent for more technical information.

Citrix ICA Support

2) Introducing the QoS solution for Citrix ICA protocol:

- Classifying all ICA applications running over Citrix through layer 7.

- Differentiating between the Citrix traffic based on ICA published applications to ICA printing traffic.

Performance Enhancements

3) NG with Application Intelligence includes enhanced throughput capabilities. The maximum throughput supported by FloodGate-1 (depending on the type of traffic):

Long UDP packets have increased:

- more than 1.1Gbps in Express Mode *or*
- up to 890Mbps in Traditional Mode.

Real-world traffic has increased:

- up to 330Mbps in Express Mode *or*
- up to 255Mbps in Traditional Mode.

These numbers were measured on a high performance SecurePlatform server.

Load Sharing

4) We present the first QoS fault-tolerant solution for cluster load sharing that deploys a unique distributed WFQ bandwidth management technology. You can specify a unified QoS policy per virtual interface of the cluster. The resulting bandwidth allocation will be identical to that obtained by installing the same policy on a single server.

VPN-1 Net Support

5) FloodGate-1 can be installed along with the VPN-1 Net product.

UserAuthority

Citrix Metaframe and Microsoft Terminal Server

For NG with Application Intelligence, secure Single Sign-on access to business critical applications for enterprise customers of Citrix Metaframe and Microsoft Terminal Server has been added. UserAuthority seamlessly inter-operates with Citrix MetaFrame XP and Microsoft Terminal Server to benefit you by streamlining access to network applications, improving user productivity and reducing overall costs of managing an enterprise security deployment. The solution provides the following benefits:

- **Single Sign-on** - Rules for access control and logging on VPN-1/FireWall-1 (based on User Groups) inspect outbound traffic from the Citrix/Terminal Sever. The user's identity, based on the original user's login to the Citrix/Terminal Server, is securely passed to VPN-1/FireWall-1 through UserAuthority. Because VPN-1/FireWall-1 knows the user's identity there is no need for re-authentication.

  - **Logging** - Once a user's identity is known, standard logging features from Check Point and OPSEC partners can be utilized to report user access to the Internet and other resources.
  - **Access Control** - Once a user's identity is known VPN-1/FireWall-1 can restrict access to resources (HTTP and others) based on a user's group membership.
- **Integration with ActiveDirectory** - Users and groups can be used directly from Microsoft ActiveDirectory and various LDAP servers.
- **WebAccess Integration** - WebAccess, can use a user's identity for Single Sign-on, access control, and logging services on a web server.

In addition, WebAccess provides Single Sign-on to the Citrix Web front end: NFUse.

WebAccess Proxy Server

This is new component that is based on SecurePlatform and available on the Linux Operating System too. It offers an alternate deployment model and is available from NG with Application Intelligence.

- The WebAccess Proxy enables you to support any kind of HTTP application server.
- The WebAccess Proxy Server eliminates the need for multiple plug-ins.
- The WebAccess Proxy Server enhances security by hiding internal network topology and disallowing non-authenticated traffic.

Support of Windows NT Groups for Audit and Authorization

This is a new feature that allows the Gateway to use already defined Windows NT domain groups for Audit and Authorization.

User Management (LDAP Account Management)

1) LDAP certificate based authentication is a new feature that allows FireWall-1 to authenticate itself to the LDAP server using a X.509 certificate issued by a Certificate Authority (CA) that is recognized by the LDAP server. This is an alternate authentication method to the basic `user/password` authentication (LDAP Simple Bind) using SSL.

2) The S/Key authentication method is no longer supported. The Check Point schema extension no longer defines the S/Key-related attributes. Previous schema-extended directories may include entries with S/Key attributes. These attributes are no longer required for fetching user information and it is recommended to remove them. Users whose authentication method is S/Key will fail to authenticate and must be assigned a different authentication method.

General Features (Available for all Products)

CP daemons

By default, CP daemons use cyclic log files (`*.elg`) for debug output. When a log file reaches a predefined size, the file is switched. The number of log files and their sizes (in Megabytes) are specified by the variables:

```
CP_<AppName>_ELG_FILE_NUM
CP_<AppName>_ELG_FILE_SIZE
```

For example:

To set 5 files of 10 MB each (on UNIX systems), for fwd daemon using environment variable (requires restart of `fwd`):

```
setenv CP_FWD_ELG_FILE_NUM 5
```

```
setenv CP_FWD_ELG_FILE_SIZE 10
```

The predefined default values are:

Number of files: 10

Size of each file: 20 MB.

To set a new defaults for the whole systems (all the daemons) the following environment variables can be set:

```
CP_ALL_ELG_FILE_NUM
CP_ALL_ELG_FILE_SIZE
```

New Improved Online Help

The online help for NG with Application Intelligence has now been fully integrated with the Check Point documentation suite. This integration includes:

- New and improved documentation for most Check Point Products (such a FireWall-1, VPN-1 and SmartCenter).
- Enhanced accessibility to documentation from online help. From most help windows you can access conceptual information and configuration details by clicking the new buttons (concept, general configuration and advanced configuration) at the top of the Online Help window.