



SofaWare Safe@ 3.0.32 Release Notes

January 2002

Table Of Contents

INTRODUCTION.....
Supported Platforms
More Information
CHANGES BETWEEN SAFE@ 3.0.25 AND 3.0.32.....
New Features
Bug Fixes.....
CHANGES BETWEEN SAFE@ 3.0.23 AND 3.0.25.....
New Features
CHANGES BETWEEN SAFE@ 3.0.14 AND 3.0.23.....
New Features
Bug fixes
CHANGES BETWEEN SAFE@ 2.0.39 AND 3.0.14.....
Integration with Check Point SMART Center FP3.....
Enhanced VPN support
Enhanced Firewall Engine
Enhanced User Rules support
Enhanced Connectivity Options
Enhanced Setup Options and Wizard
Logging and Reports.....



We Secure the Internet.

Managed Services.....

Bug Fixes.....

SMP COMPATIBILITY ISSUES.....



Introduction

This document contains the summary of changes between Safe@ firmware 2.0.39 to Safe@ firmware 3.0.32.

Supported Platforms

The following hardware platforms are supported by Safe@ 3.0.32:

- Nokia IP30*
- SofaWare S-box
- Celestix Orion
- VPN Dynamics V4
- Intrusion PDS500
- NEC SecureBlade

* Nokia IP30 requires a different firmware image.

More Information

- More information will be available on SofaWare web site:
<http://www.sofaware.com/support/>

For technical support and assistance please email <mailto:support@sofaware.com>



Changes Between Safe@ 3.0.25 and 3.0.32

New Features

LAN Network

The LAN subnet mask can now be changed from the default, also in NAT mode.

H.323

H.323 is the international standard for IP telephony, and is used by many VoIP applications. Safe@ 3.0.32 fully supports the H.323 standard with NAT off and on. To allow incoming H323 connections, create an “Allow Incoming” rule for TCP port 1720.

Passive FTP

“Allow Incoming” FTP rules now support also Passive Mode FTP.

Bug Fixes

Connectivity

- In “PPTP + DHCP Client” WAN mode, the PPTP connection is now restarted if the DHCP address has been changed by the ISP
- Few bugs in the DHCP client, that were introduced in version 3.0.25, were resolved.

VPN

- Fixed a bug with SecureID support in Remote Access VPN mode, when the wrong password has been entered
- A problem was resolved, which caused VPN topology download to fail with the log message "Refused unauthenticated request".
- A problem was resolved, which caused VPN establishment to fail with the log message "delay request" .
- A bug was fixed that prevented configuring a VPN remote access connection to Check Point Smart Center using RADIUS authentication in “generic*” mode



Changes Between Safe@ 3.0.23 and 3.0.25

New Features

Connectivity

Safe@ now supports connecting to the internet using additional methods:

- BPA (Bigpond Advanced) – the protocol used by Telstra cable
- DHCP + PPTP: Obtain an IP address using DHCP, then connect to a PPTP server

The WAN IP address can now be preconfigured in PPTP mode.

Anti-Virus

Improved the ability to read more than one email at a time.

VPN

IKE negotiations with a source port other than 500 are now supported (useful when operating behind a NAT device)



Changes Between Safe@ 3.0.14 and 3.0.23

New Features

Static Routes

In Safe@Office, Up to 5 static routes can be configured in LAN or Cable mode. Static routes allow you to route all traffic to a specified network or host through a specified router. Generally you won't need to set up static routes unless you know you need to.

VPN Certificates Support

Site-to-Site VPN in Safe@Office can be configured with X.509 certificate for authentication, not only pre-shared secret.

Site-to-Site VPN with dynamic IP

A Safe@Office Gateway can be defined as a "Dynamic IP Gateway" and joined as a member of a "Star" community in Check Point VPN-1 NG. To act as a Dynamic IP Gateway, a valid X.509 certificate must be installed on the Safe@ gateway.

Safe@Home Pro and Safe@Office continue to support dynamic IP in Remote Access (RAS) VPN. In RAS VPN mode, X.509 certificates are not required, and pre-shared secret authentication is supported.

MAC Cloning in all network modes

Some ISPs requires the registration of the MAC addresses before connection can be established. MAC Cloning is now supported in all network modes – Cable, LAN, and DSL.

Improved Performance

- Firewall performance was improved in NAT-off mode.
- Mail Anti-Virus Service performance was improved

Bug fixes

Mail Anti-Virus Service

A bug was fixed which prevented Mail Anti-Virus Service from operating correctly when two or more clients are downloading E-Mails concurrently from two different E-Mail servers.

VPN

Some major issues regarding the VPN where fixe d.



Changes Between Safe@ 2.0.39 and 3.0.14

Integration with Check Point SMART Center FP3

Safe@ 3.0 gateways can be managed directly from the SmartDashboard, using SofaWare SmartCenter Connector (SSC). This is useful for customers who do not need the full functionality of the Security Management Portal (SMP).

Enhanced VPN support

Restricted and Unrestricted Modes

An unrestricted site can access the internal network without restriction and bypass Network Address Translation (NAT). The definitions for Restricted and Unrestricted modes are as followed:

- **Unrestricted Mode with NAT'd network**
The user can access all NAT'd computers behind VPN server using the non-routable IP addresses. Access is not bound to security rules.
- **Restricted Mode with NAT'd network**
The user can access the NAT'd computers behind VPN server using the hiding address. Access is bound to security rules and NAT limitations (a single rule per port).
- **Unrestricted Mode with routable IP addresses network**
The user can access the encryption domain computers using the routable IP addresses. Access is not bound to security rules.
- **Restricted Mode with routable IP addresses network**
The user can access the encryption domain computers using the routable IP addresses. Access is bound to security rules.

IKE Hybrid mode is supported

Hybrid mode support is needed for SecureID authentication and remote user databases to be used, such as RADIUS. This feature is not reflected in the local gateway user interface, as this is transparent to the user. Both 4.1 and NG platforms are supported.

AES encryption is supported, for better performance.

AES (Advanced Encryption Standard) provides a better combination of safety and speed than DES. Using 128-bit secret keys, AES offers higher security against



We Secure the Internet.

brute-force attack than the old 56-bit DES keys, and AES can use larger 192-bit and 256-bit keys, if necessary.

When establishing a VPN tunnel with VPN-1 NG FP3, and using communities, the encryption is determined by the community defaults.

Known limitations:

- Safe@ 3.0 to Safe@ 3.0 negotiate AES/SHA1
- Safe@ 3.0 to Other negotiate 3DES/SHA1 by default

UDP encapsulation is supported in the VPN client.

When the appliance remote access is behind a NAT device, UDP encapsulation is activated automatically. UDP encapsulation is needed to enable the NAT device to send the returning ESP packets to the NAT's appliance.

Site-to-Site communications use IKE Main Mode.

IPSec IKE is a 2-phase protocol. During phase 1, use of aggressive mode, with only three messages, is more efficient for most applications. However, use of main mode, with 6 messages is a more secured option to avoid possible signal tracing and targeted attacks in a complex network environment. Safe@ will use main mode by default, in Site-to-Site VPN.

Safe@ appliance IKE is interoperable with Windows 2000 IKE implementation

Main mode is used with windows 2000 IPSec, hence site-to-site VPN connections can be established to windows 2000. More information about setting windows 2000 IPSec tunnels can be obtained on Microsoft web sites:

<http://support.microsoft.com/default.aspx?scid=KB:EN-US:q252735&>

VPN keep alive

In automatic client mode, the client keeps pinging the gateway, and thus the connection is always available.

Split DNS is supported

Split DNS is used in order to resolve domain names inside the VPN network. Safe@ supports Split DNS, using the site network topology definitions.

Improved Tools for Troubleshooting VPN Connections

- **Better logging of VPN messages**
Troubleshooting VPN connections is easier than ever with Safe@ 3.0. Better



We Secure the Internet.

VPN connections logging and a variety of internal or captured from Checkpoint VPN-1 error messages are displayed on different events.

- **VPN Topology display**
VPN topology can be viewed by surfing to <http://my.firewall/vpntopo.html>
- **Advanced VPN connection parameters display**
Encryption parameters are shown in the active connections table. To view the encryption parameters, enter the **Reports>Active Connections** page and move the mouse over the lock icon for the appropriate connection.

VPN Sites can be Enabled or Disable

This is a similar feature as in Checkpoint's SecureClient application. The VPN site can be disabled (terminated) from the UI. Once disabled, data will not be encrypted nor authenticated.

VPN gateways name resolving

VPN gateway names can be resolved by the DNS defined for the gateway. Hence, the local user can use the gateway domain name instead of its IP address.

Enhanced Firewall Engine

Improved performance while under DoS attacks

DoS (Denial Of Service) attacks are designed to bring the network to its knees by flooding it with useless traffic. The Safe@ firewall engine is now designed to provide better performance and accessibility to the local UI while under DoS attacks.

H.323 Support

H.323 is the international standard for IP telephony, and is used by many VoIP applications. Safe@ 3.0 fully supports H.323 standard with NAT off.

Known limitations:

When working with NAT on, only outgoing calls are supported.

This means that the client behind Safe@ gateway has to initiate the call first.



Additional IP protocols support for DMZ

NAT also folds protocols other than TCP and UDP. As a result, DMZ can now accept IGMP packets etc.

Known limitations:

ICMP packets are not forwarded to the DMZ

Enhanced User Rules support

IP Filtering

Safe@ 3.0 enables custom user security rules with IP filtering:

- Source IP filtering for the “allow” and “Virtual servers” user rules.
- Destination IP filtering in the “block” user rules
- In NAT off mode, multiple servers for the same service can be defined. Moreover, certain ports can be allowed in for all internal computers.

Additional IP Protocols Filtering

Safe@ 3.0 enables filtering for additional designated IP protocols:

- GRE (protocol 47)
- ESP (protocol 50)

Allow and block rules supported, enabling hosting of applications such as PPTP server, IPSEC VPN server at the local network.

Enhanced Connectivity Options

Internal Network Subnet Mask

Subnet Mask can be determined when working with routable IP addresses (disabled NAT). This eliminates the limitation of using only “class C” IP addresses.

Known limitations:

- This feature is not supported when working with NAT enabled.
- This feature is only available in [Safe@Office](#) and [Safe@Office Plus](#) products.

Safe@ gateway Internal IP address

The internal IP address of the Safe@ gateway can be changed to other than the first within the internal subnet. This enables more flexibility when integrating the Safe@ gateway in a network who has the first IP already in use.



Support up to 100 nodes

The Safe@ 3.0 gateway's DHCP server now supports up to 100 nodes. This enables integration of Safe@ gateway within larger networks.

Static DNS configuration

Static DNS servers can be configured also when working with DHCP, PPTP and PPPoE. Primary and secondary DNS servers can be manually configured to fit the networking needs, especially when using the ISP DNS services as well the ones in the internal network. DNS configuration can still be obtained automatically according to the user's choice.

Improved connectivity monitoring

Connectivity with the default gateway is periodically checked, both in LAN, Cable and PPP modes.

MAC Cloning

This feature is intended mainly for cable connection users. Some ISPs require the registration of the MAC addresses of the computer behind the cable modem before connection can be established. The Safe@ gateway takes the place of the computer behind the modem, and the local user can use the MAC Cloning option to enter the original PC MAC address, without contacting the ISP for changing that information.

Enhanced Setup Options and Wizard

Easy Connection to Service Center

- Service Center can be entered by DNS name instead of its IP address, for example: usercenter.sofaware.com
- When configured in the SMP without a Registration Key, the user needs to enter only the service center name.
- The list of configured services and subscription end date is presented for user confirmation.
- The user can now choose to manually update the box firmware in software subscription mode.
- Product registration can be performed through the wizard at the user choice.



HTTPS Remote Management

- HTTPS access is now configurable in the local gateway UI.
The user can configure HTTPS independently from what is configured in the SMP.
- When using HTTPS, a Windows browser authentication (popup window) is used before the gateway configuration page appears. This prevents a potential hacker from detecting that he is communicating with a Safe@ Gateway.
- To enhance management security, HTTPS login is not allowed until the administrator password is set.

Logging and Reports

Traffic Source Identification

- Source and destination ports are added to the Reports page and to the Active Connections page. This makes it easier for the user to analyze traffic passing or blocked through the appliance.
- WHOIS resolving is supported in “active connections”. This feature makes it easier for the user to identify the source of a potential hacker.

Improved Display

- my.firewall Logins are logged
- Active computers are displayed in a graphic map.

Managed Services

Anti-Virus

Virus Scanning of outgoing SMTP is supported (in addition to the existing incoming POP3).

Enhanced Subscription Services

- Separated services to: Management, Web Filtering, Anti-Virus, Logging, Software Subscription
- When Remote Management service is enabled the following can be configured from the SMP:
 - Product Key
 - Enabled services list
 - Web Filtering mode and categories
 - Mail Anti Virus mode



- Security Policy
- User Interface



Remote Administration through the SMP

- When the gateway is installed with a remote management plan, the SMP manager can perform certain actions with the remote gateway as basic technical support steps, by sending direct commands:
 - Connect to the local gateway my.firewall page using HTTPS.
 - Update now option – to force the gateway to be updated with the latest information from the SMP.
 - Reboot the local gateway from remote.

Known limitation:

- Connecting to the local gateway from the SMP via HTTPS is enabled only when permitted by the plan installed on the gateway.
- The S-box does not accept commands or configuration updates from the server if “management service” is not enabled. Specifically: If “management service” is not enabled, and the server wishes to enable / disable a service, the user must approve this by going through the registration wizard again, and the "Managed Mode" cannot be switched on by the management server without the user's approval.

Remote Management Options

- "Remote Management Service" cannot be switched on without a registration key. Other services (Software Subscription, UFP, mail AV) can be connected to without a registration key.
- If “Software Updates” service is enabled, and “Remote Management” service is not enabled, the user can set the software updates mode to “Automatic” or “Manual”
- When Web Filtering & Mail Anti Virus services are set to “remotely managed” their local configuration pages become read only. The SMP admin may choose to use this configuration, or alternatively, let the user control it.
- Added a services status table

Bug Fixes

- Drop log on SYN packet after reject from internal host removed.
- No more connection drops when closing manual VPN window.
- VPN login pop-up window doesn't close when changing external IP, disconnecting from Internet etc.
- VPN server off closes all currently active incoming tunnels.



We Secure the Internet.

- Error conditions that cause “Ping pong” between SMSs are prevented. The Safe@ gateways always recognizes an active SMP. As a result the gateway will not accept redirect command to a non-functional SMS.

SMP Compatibility Issues

- Safe@ 3.0 is fully compatible with SMP 3.0.
- SMP 2.X servers can enable/disable UFP, CVP and remote logging of Safe@ 3.x, and download firmware, policy and GUI updates.
- SMP 2.X cannot change Safe@ 3.0 product license (Safe@Home, Safe@Office, node limit) and https settings.