Check Point
SOFTWARE TECHNOLOGIES LTD.

SecuRemote SecureClient

NGX R60 HFA03

Release Notes

28 January, 2010

More Information

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=10626

For additional technical information about Check Point visit Check Point Support Center (http://supportcenter.checkpoint.com).

Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to us (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SecuRemote SecureClient NGX R60 HFA03 Release Notes).

© 2010 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Please refer to our Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Please refer to our Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights.

Introduction

Thank you for using Check Point SecureClient NGX R60 HFA 03.

This version supports the Windows 7 operating system. Make sure that you read this document carefully before installing NGX R60_HFA_03 on your system.

SecureClient allows you to connect to your organization in a secure manner, while at the same time protecting your machine from attacks that originate on the Internet. You can access private files over the Internet knowing that unauthorized persons cannot view the same file or alter it. With SecureClient, remote users connect to the organization using any network adapter (including wireless adapters) or modem dialup. Once the both sides are sure they are communicating with the intended party, all subsequent communication is private (encrypted) and secure.

What's New

Windows 7 Support

This version of SecureClient supports the Windows 7 operating system (32-bit).

Secure Domain Logon (SDL)

SecureClient on Windows 7 introduces Secure Domain Logon in two operational modes that are only supported on the Windows 7 and Vista Platforms:

- Explicit mode
- Implicit mode

Explicit Mode

SDL can be invoked explicitly, prior to the domain logon. Using Explicit Mode, SDL is implemented as a Pre-Logon Access Provider (PLAP).

A PLAP is a component that enables Pre Logon Connection to the Internet. For example, a dialup connection appears as such a pre logon connection. Once SDL is enabled, or if Windows enables its own PLAP, a new button for Network Logon is added to the logon screen at the lower right corner.

Clicking the **Network Logon** button will redirect the user to a screen showing all available pre logon connection methods (PLAPs), in which SecureClient SDL participates. If the user clicks the Network Logon button and the SecureClient PLAP is the only PLAP registered, then the connect dialog box will appear and the user can proceed with connecting to the VPN gateway.

If more than one PLAP is registered, the user will get a screen with a list of all the registered PLAPs. When choosing SecureClient PLAP the connect dialog will appear and the user can proceed with connecting to the VPN gateway.

The user can then proceed with the log on to windows.

Implicit Mode

Implicit mode SDL is invoked automatically and immediately after the user authenticates to the domain controller. This means that while using implicit mode, authentication to the domain controller over a VPN tunnel is not provided. It does, however, provide Group Policy and logon scripts over the VPN tunnel.

Note - By default, windows performs authentication to the domain controller against the cache it holds. This means that, unless configured otherwise, actual domain connectivity will not be required for domain authentication.

In addition, implicit mode SDL will not be invoked when using Smart Card logon to windows.

Note - The user does not have to configure the client to employ implicit mode. SDL in implicit mode

will be invoked automatically if SecureClient was configured for SDL and the user did not already connect to the site using the SDL PLAP (explicit mode).

To select the best SDL mode that fits your requirements, consider:

Configuration Scenario	Recommended Method
Windows Cached Logon Enabled	Either mode
Windows Cached Logon Disabled	Explicit Mode
Smart Card Windows Logon	Explicit Mode
User Name / Password Windows	Either mode
SecureClient Auto Local Logon	Implicit Mode

Disabling Cache of User Name

By default, SecureClient caches the user name of the last user that connected. This behavior can now be disabled by:

- Adding a new attribute, `delete_user_session_info`, to the userc.C file under the `options` attribute.
- Setting the value to `true`.

SCV Anti Virus Check

A new type was added (McAfee) for the McAfee VirusScan Enterprise 8.5.0i, and has the same syntax as the type VirusScan. The signature should be according to the antivirus DATversion. The current DATversion can be seen at:

VirusScan Console/help/About VirusScan Enterprise section.

Example of how to edit the local.scv in order to use this type:

```
 : (AntiVirusMonitor
      :type (plugin)
      :parameters (
            :type (McAfee)
            :Signature (">=5005")
            :begin_admin (admin)
            :send_log (alert)
            :mismatchmessage (“Please update your AntiVirus.”)
            :end (admin)
      )
)
```

IPv6 Traffic Blocking

By default, SecureClient R65 HFA03 blocks all IPv6 traffic. The SCV version check can be used to centrally enforce this enhancement by adding to the local.scv policy the following lines:

```
: (sc_ver_scv
        :type (plugin)
        :parameters (
                     :Default_SecureClientBuildNumber (<SC build number>)
                     :Default_EnforceBuildOperand (">=")
                     :MismatchMessage ("Please upgrade your SecureClient.")
        )

 )

: (RegMonitor
      :type (plugin)
      :parameters (
          :begin_or (or1)
             :value
("System\CurrentControlSet\Services\FW1\Parameters\BlockIPv6Packets!=0")
             :valuenexist
("System\CurrentControlSet\Services\FW1\Parameters\BlockIPv6Packets")
          :end (or1)
          :begin_admin (admin)
             :send_log (alert)
             :mismatchmessage ("Your SC is not configured to block IPv6 Packets")
             :end (admin)
         )
 )

...



SCVPolicy (

...

    : (sc_ver_scv)

    : (RegMonitor)

...

)
```

Where build number is the build number of SecuRemote/SecureClient.

Supported Platforms

- Windows XP Professional SP3
- Windows Vista Enterprise SP1
- Windows 7 Enterprise and Ultimate editions (32-bit)

Build Numbers

Platform	Build Number
Windows	630044011_1

Installation

If you plan to upgrade to Windows 7, uninstall any old versions of SecuRemote/SecureClient before doing so. If you are already using Windows 7:

1. Uninstall any previous versions of SecuRemote/SecureClient
2. Download the SecuRemote/SecureClient NGX HFA3 EA msi installation file.
3. Run the msi file.

Clarifications and Known Limitations

ID	Description
00335258	Upgrading from Windows XP or Windows 2000 to Windows 7 while SecureClient is installed is currently not supported. Workaround: 1. Uninstall SecureClient. 2. Upgrade operating system. 3. Install SecureClient NGX HFA_03.
	On Windows 2000, SecureClient HFA3 is supported only with Windows 2000 SP4
	Check Point SecureClient NGX R60 HFA_03 is only available with an MSI installation.
00335087	SecureClient does not support Fast User Switching. In order to avoid any compatibility issues, the SecureClient installation disables the Fast User Switch feature.
00350508	When enrolling for a user certificate with the option of placing the certificate in CAPI and a certificate from the internal CA already exists in the Trusted Root CA store, the user will be prompted to approve the deletion of the existing certificate. (Prompting for deletion only applies when using Windows 7 and Vista.) Once deleted, the user will be prompted again to approve the insertion of the newly received Internal CA certificate to the Trusted Root CA store.
00353223	The SCV check Hotfix monitor is not supported on Windows 7 and Vista

ID	Description
00526624	Mobile Broadband (WWAN) devices introduced in Windows 7 are not currently supported.
00527466	By default all IPv6 traffic is blocked. To allow IPv6 traffic: 1. Open the Windows registry (**Start > run > regedit**) 2. Browse to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FW1\Parameters`. 3. Create a new **DWORD value** called **BlockIPv6Packets.** 4. Assign it the value: 0 See also: IPv6 Traffic Blocking (on page 5)