

Secure Configuration Verification (SCV)

Cyril Sultan
cyril@us.checkpoint.com
02/27/03

V1.5

INTRODUCTION

Check Point VPN-1 SecureClient offers two important security features :

- Centrally Managed personal Firewall
- Secure Configuration Verification (SCV)

The goal of SCV is to strengthen enterprise security by ensuring SecureClient machines cannot be configured in a way that circumvents the enterprise security policy. Using SCV, managers can specify SCV checks - a set of conditions that define a securely configured client system, such as the current version of anti-virus software or the proper operation of the personal firewall policy. These security checks are performed regularly to ensure that only securely configured systems are connected to the corporate VPN. Depending on the Client SCV status, the GW will then decide to allow/block connections from the Client machine.

The purpose of this document is to help customers/partners to easily deploy SCV in their environment.

SCV CHECKS AVAILABLE

1. Check Point SCV checks

SecureClient NG FP3 already includes the following Check Point SCV checks:

- a. Process Monitor - checks if a process is running or not.
- b. Version checker – verifies SecureClient version.
- c. Group Monitor – checks whether the logged on user is member of Domain User Groups.
- d. OS Monitor – verifies the Operating System version, service pack, and screen saver configuration.
- e. HotFix Monitor – checks that operating system security patches are installed.
- f. Browser Monitor - verifies Internet explorer version and specific configuration IE settings.

The SCV Check Point product is included by default in SecureClient NG FP3, but it can be installed as a separate package on any SecureClient NG FP2 machine.

2. OPSEC SCV checks

Okena and PestPatrol have already developed some SCV checks. Please check www.ospec.com to get an updated list of OPSEC partners.

3. Other existing checks

The company OPSWAT (www.opswat.com) has developed some SCV checks for HfNetCheck and Norton Anti-virus; please check their Web site for more information.

4. Customized checks

- Every partner/customer can use the SCV SDK (www.opsec.com) in order to write his own SCV check.
- If the partner/customer wants to outsource this, they may contact OPSWAT (www.opswat.com).

SCV IMPLEMENTATION

1. General Overview

In order to implement SCV, the following steps need to be done:

- (a) Installation of SCV products on the Client machine. You can install the Check Point SCV Products (included by default in every NG FP3 Client) or/and other SCV products.
- (b) Definition of the SCV policy on the Management station. It can be done manually by editing the file FWDIR\conf\local.scv, or using SCVEditor.
- (c) Enforce the SCV policy. In Traditional Mode, you need to edit the rule “Client Encrypt”. In Simplified Mode, it’s a global property in Remote Access/Secure Configuration Verification.
- (d) Push the Desktop Security on the Policy Server (PS): it will download the personal firewall and SCV policy onto the PS.
- (e) SecureClient connects to the PS to fetch the firewall and SCV policy
- (f) SecureClient connects to the GW; if it’s not securely configured, the GW will drop the packets.

In the next paragraphs, we’ll talk about step (b) and (f).

2. Policy (local.scv) syntax

The local.scv file includes three sections:

- SCVNames (products): name of the different SCV products.

- SCVPolicy: name of the SCV checks enforced
 - SCVGlobalParams: global parameters for SCV.
-
- The SCV checks need to be defined in the SCVNames field.
 - Customer chooses his policy, and then decided to enforce it (and mention it in “SCVPolicy”) or not.

One can also use SCVEditor instead of manually modifying the file.

For more information about the syntax of the Check Point SCV checks, please go to the Appendix.

The parameters in SCVGlobalParams are:

- `block_connections_on_unverified` (false): if “true”, SC will drop all open connections when the Desktop is not SCVed.
- `scv_policy_timeout_hours` (24): period (in hours) during which the SCV policy is considered valid since the last logon to the PS.
- `enforce_ip_forwarding` (true): decision to enforce SCV is IP Forwarding is “on”

3. Options to enforce the SCV policy

In NG FP3, the following features are supported:

a. Block 4.1 SecureClient from passing on SCV rules

To enable it, set `scv_allow_4_1_clients` in `object_5_0.c` to false (the default is true).

A de-authorized log will be generated for such clients.

b. IP forwarding enforcement

The implicit configuration enforcement decision, when IP forwarding is enabled, is controllable through the SCV policy.

To enable, set `enforce_ip_forwarding` in `local.scv` (check point 2 above)

c. Timeout for SCV checks

All the timeout for SCV checks on the machine, or the periodicity of SCV checks sent to the GW are controllable via registry key or options on the Management station. Please check the Desktop User Guide for more information.

Appendix – Check Point SCV checks

a. Process Monitor

You can check if one (or multiple) processes is running or not; the condition can be “or” or “and”.
Examples of checks :

- Antivirus x or y is running on your machine
- Trojan xxx is not running on your machine and [Anti-Virus x or y] is running
- etc.

Syntax:

“

```
ProcessMonitor
  :type (plugin)
  :parameters (
    :begin_or (or1)
    :AntiVirus1.exe (true)
    :AntiVirus2.exe (true)
    :end (or1)
    :IntrusionMonitor.exe (true)
    :ShareMyFiles.exe (false)
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please check that the following processes are
running: ( AntiVirus1.exe or AntiVirus2.exe), IntrusionMonitor.exe. Please
check that the following process are not running: ShareMyFiles.exe")
    :end (admin)
  )
“
```

Syntax explanation:

- process (true/false) : check if the process is running or not.
- begin_or (or1), end (or1) : condition “or” for all the processes between those conditions.

The condition can also be “begin_and”

- mismatchmessage: error message displayed for the user.

In this example, we check that:

- Antivirus1 or 2 is running
- IntrusionMonitor is running
- ShareMyFiles is not running.

If by chance the condition is not fulfilled, then the message “mismatchmessage” will be displayed for the user.

b. SecureClient Version

You can check SecureClient version, and make sure that they are using the correct version.

Syntax:

```

“
sc_ver_scv
  :type (plugin)
  :parameters (
    :Default_SecureClientBuildNumber (52057)
    :Default_EnforceBuildOperand ("==")
    :MismatchMessage ("You are not running the latest version of
SecureClient. Upgrade your SecureClient.")
    :EnforceBuild_9X_Operand (">=")
    :SecureClient_9X_BuildNumber (52057)
    :EnforceBuild_NT_Operand ("==")
    :SecureClient_NT_BuildNumber (52057)
    :EnforceBuild_2K_Operand (">=")
    :SecureClient_2K_BuildNumber (52057)
    :EnforceBuild_XP_Operand (">=")
    :SecureClient_XP_BuildNumber (53000)
  )
“

```

Syntax explanation:

- Default_SecureClientBuildNumber (aa) : check the default SC version on all OS
- Default_EnforceBuildOperand : operand about the build number; can be “<”, “<=”, “==”, “>=”, “>”.
- if you want more granularity per OS, then you can configure the “EnforceBuild_AA_BuildNumber” .

In this example, we check if SC has version 52057.

c. Group Monitor

You can check whether SecureClient belongs to a specific group (in domain or local machine).

Syntax:

```
groupmonitor
  :type (plugin)
  :parameters (
    : "BUILTIN\administrator" (false)
    : begin_admin (admin)
    : send_log (alert)
    : mismatchmessage ("Organization policy does not allow you to
connect as Workstation Local administrator")
    : securely_configured_no_active_user (false)
    : end (admin)
```

Syntax explanation:

- builtin\administrator : [NT Authority] \ [Groups/User] (false/true).
 - . [NT Authority] stands for the Domain the user group belongs to
 - . [Group/user] : user group or user name, Administrators, ...
- securely_configured_no_active_user : enable/disable this check even if SC does not have any active user; useful for SDL.

d. OS Monitor

You can check the OS version, Service Pack, and Screen Saver Configuration. The operand can be “and” or “or”.

Syntax:

```
OsMonitor
    :type (plugin)
    :parameters (
        :os_version_mismatchmessage ("A newer operating system version is
required. Upgrade your operating system.")
        :enforce_screen_saver_minutes_to_activate (3)
        :screen_saver_mismatchmessage ("Your screen saver configuration
does not match the organization policy. Proceed as follows:\n1. In the Display
Properties window, select the Screen Saver tab.\n2. Under Wait choose 3
minutes and check Password Protection.")
        :send_log (log)
        :major_os_version_number_9x (4)
        :minor_os_version_number_9x (10)
        :os_version_operand_9x (">=")
        :service_pack_major_version_number_9x (0)
        :service_pack_minor_version_number_9x (0)
        :service_pack_version_operand_9x (">=")
        :major_os_version_number_nt (4)
        :minor_os_version_number_nt (0)
        :os_version_operand_nt ("==")
        :service_pack_major_version_number_nt (5)
        :service_pack_minor_version_number_nt (0)
        :service_pack_version_operand_nt (">=")
        :major_os_version_number_2k (5)
        :minor_os_version_number_2k (0)
        :os_version_operand_2k ("==")
        :service_pack_major_version_number_2k (0)
        :service_pack_minor_version_number_2k (0)
        :service_pack_version_operand_2k (">=")
        :major_os_version_number_xp (5)
        :minor_os_version_number_xp (1)
        :os_version_operand_xp ("==")
        :service_pack_major_version_number_xp (0)
        :service_pack_minor_version_number_xp (0)
        :service_pack_version_operand_xp (">=")
        :screen_saver_securely_configured_on_no_active_user (false)
    )

```

Syntax explanation:

- os_version_mismatchmessage : error message for OS mismatch
- enforce_screen_saver_minutes_to_activate (3) : enforce screen-saver with password and a timeout less than 3 minutes
- screen_saver_mismatchmessage : error message is screen saver is not configured correctly
- major_os_version_number_aa (4) : major OS Version
- minor_os_version_number_aa (10) : minor OS version
- os_version_operand_aa (">=") : operand for OS version.
- service_pack_major_version_number_aa (0) : maximum SP for aa version
- service_pack_minor_version_number_9x (0) : minimum SP for aa version

In this example, we check if the screen saver is configured and if the OS is updated.

e. Hotfix Monitor

Checks MS Windows OS Hotfixes installed on your machine.

Syntax:

```
HotFixMonitor
  :type (plugin)
  :parameters (
    :begin_and ()
    :275286 (true)
    :end ()
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("The organization policy requires that you have a
SecureClient with Q275286 security patch installed.")
    :end (admin)
```

Syntax explanation:

- 275286 (true) : check if Q275286 has been installed.

Example explanation: it checks if Q275286 has been installed; in the negative case, the mismatchmessage is displayed to the end-user.

Important point : the Q[Numbers] are checked for all the platforms.

f. Browser Monitor

This check is related to Internet Explorer settings. You can check the version, and all the security settings related to activex, java permissions, etc.

Syntax:

```
BrowserMonitor
  :type (plugin)
  :parameters (
    :browser_major_version (5)
    :browser_minor_version (0)
    :browser_version_operand (">=")
    :browser_version_mismatchmessage ("A newer Internet Explorer
version is required. Upgrade your Internet Explorer.")
    :intranet_download_signed_activex (disable)
    :intranet_run_activex (disable)
    :intranet_download_files (disable)
    :intranet_jave_permissions (disable)
    :trusted_download_signed_activex (disable)
    :trusted_run_activex (disable)
    :trusted_download_files (disable)
    :trusted_jave_permissions (disable)
    :internet_download_signed_activex (disable)
    :internet_run_activex (disable)
    :internet_download_files (disable)
    :intranet_jave_permissions (disable)
    :restricted_download_signed_activex (disable)
    :restricted_run_activex (disable)
    :restricted_download_files (disable)
    :restricted_jave_permissions (disable)
    :securely_configured_no_active_user (true)
    :send_log (alert)
    :internet_options_mismatch_message ("Your Internet browser
configuration does not match the organization policy. Proceed as follows:\n1.
In the browser, go to Tools > Internet Options > Security.\n2. For each Web
content zone select custom level security and disable the following items:
DownLoad signed ActiveX, Run Activex Controls, Download Files and Java
Permissions.")
```

Syntax explanation:

All the options are self-explanatory.