Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT COMPLIANCE CHECKING WITH SECURE CONFIGURATION VERIFICATION (SCV)

"

ELEGANT SOLUTION TO ENHANCE CORPORATE SECURITY COMPLIANCE FOR CHECK POINT VPN USERS

"

BACKGROUND

Secure Configuration Verification (SCV) provides an elegant compliance checking solution for enterprises using Check Point Endpoint Security VPN Client and Check Point Mobile for Windows Client. SCV strengthens enterprise security by ensuring client machines are configured in accordance with the enterprise Security Policy. SCV augments and complements Desktop Security Policy. SCV is the platform for creating and using SCV checks. SCV checks are sets of conditions that define a securely configured client system, such as the user's browser configuration, the current version of the Anti-Virus software installed on the computer, the proper operation of the personal firewall policy, etc. The SCV security compliance checks are performed at pre-defined intervals via the Check Point Endpoint Security VPN Client and the Check Point Mobile for Windows Client. Depending on result of the SCV security compliance checks, the Check Point VPN Gateway decides whether to allow or block connections from the Endpoint to the corporate network.

SCV provides capability for the following compliance checks:

- OS Monitor - verifies Operating System version, Service Pack, and Screen Saver configuration
- HotFix Monitor- verifies status operating system security patches are installed
- Group Monitor - verifies that the user logged into the operating system and is a member of specified Domain User Groups.
- Process Monitor - verifies that a process is running, or not running
- Browser Monitor - verifies Internet Explorer version and configuration settings, such as Java and ActiveX options.
- Registry Monitor - verifies System Registry keys, values, and their contents.
- Anti-virus Monitor - verifies that an Anti-virus is running and checks its version.
- SCVMonitor - verifies the version of the SCV product, specifically the versions of the SCV DLLs installed on the client's machine.
- HWMonitor - verifies CPU type, family, and model.
- ScriptRun - runs a specified executable on the client machine and checks the return code of the executable. For example, a script can check if a certain file is present on the client machine. It can perform additional configuration checks that based on customer need.
- Windows Security Monitor - verifies that components monitored by Window Security Center are installed and enforced (for example, check if there is Anti-virus installed and running). Define specific Windows components to check.
- Third Party SCV Checks - SCV checks can be written by third party vendors using Check Point's OPSEC SCV SDK. After these applications are installed, the administrator can use these SCV checks in the SCV Policy.

SOLUTION COMPONENTS

Check Point Endpoint Security VPN Client and Check Point Mobile for Windows Client

First a bit of background about these specific SmartDashboard-managed clients:

1. **Endpoint Security VPN - incorporates Remote Access VPN with Desktop Security in a single client. It is recommended for managed endpoints that require a simple and transparent remote access experience together with desktop firewall rules.**

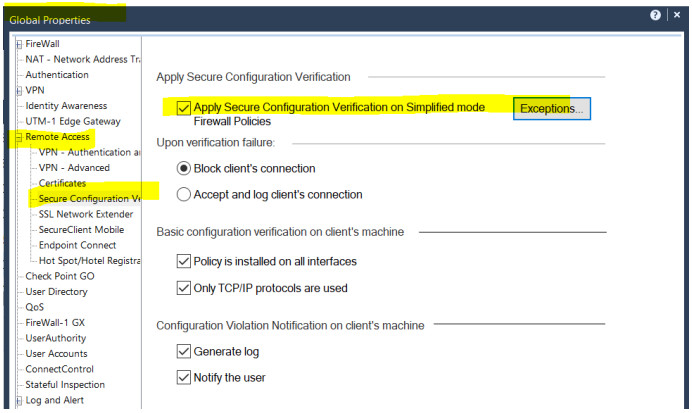
2. **Check Point Mobile for Windows - easy to use IPsec VPN client to connect securely to corporate resources. Together with the Check Point Mobile clients for iPhone and Android, and the Check Point SSL VPN portal, this client offers a simple experience that is primarily targeted for non-managed machines.**

   - SCV checks are performed through special DLLs which check elements of the Check Point Endpoint Security VPN Client and the Check Point Mobile for Windows Client configuration and return the results of these checks. An SCV application registers its SCV DLLs in the system registry. The first step in configuring SCV is for the administrator to install the applications that provide the SCV checks on the client. During installation, these applications register themselves as SCV plug-ins and write a hash value of their SCV DLLs to prevent tampering.

   - Check Point Endpoint Security VPN Client, and the Check Point Mobile for Windows Client are able to determine whether the client is securely configured. Once all the organization's clients have been configured according to the previous steps, the administrator specifies the actions to be taken on the Check Point VPN Gateway based on the client's SCV status. Example: the administrator can specify that non-securely configured clients cannot access some or all of the resources on the corporate network, protecting the organization from the dangers associated with the client's poor security configuration. The administrator can choose whether to enforce SCV for remote clients. If SCV is enforced, only securely configured clients are allowed access under the rule. If SCV is not enforced, all clients are allowed access under the rule. In simplified mode, this is configured globally. In traditional mode, this is configured individually for each rule. See "Server Side Configuration" for more information.

Check Point MultiDomain Security Management (MDS) or Security Management Server (SMS)

- Global Properties enables Secure Configuration Verification enforcement and basic configuration verification settings, block or allow when client configuration is not compliant, client notification of violations, and logging. Global Properties is where SCV is applied:



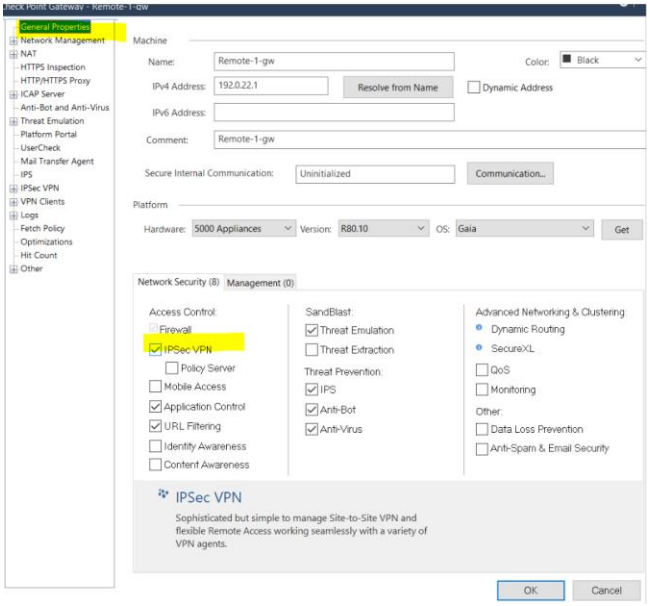
- $FWDIR/conf/local.scv – edit the current text file on the MDS/SMS to define the set of compliance checks to be performed when remote access client attempts to connect to the Check Point VPN Gateway.

- [Expert@HostName]# mdsenv <Domain_Name>
- Create backup file before editing original [Expert@HostName]# cp $FWDIR/conf/local.scv $FWDIR/conf/local.scv_ORIGINAL

- SmartDashboard GUI Desktop Policy Configuration – when Desktop Policy is installed, the $FWDIR/conf/local.scv file is pushed from MDS/SMS to the Check Point VPN Gateway.
  - On the MDS/SMS = $FWDIR/state/<Name_of_GW_Object>/PS directory
  - From MDS/MDM to VPN Gateway $FWDIR/state/local/FW1/ directory
  - Check Point Endpoint Security VPN Client and the Check Point Mobile for Windows Client gets a copy of this file after downloading the Topology.

Check Point VPN Gateway

IPSec VPN enabled and VPN Clients configured:



HOW IT WORKS

The Check Point Endpoint Security VPN Client and the Check Point Mobile for Windows Client downloads the SCV policy at connection time. The policy is enforced each time the client connects, at disconnect time, and at regular 20 second intervals. If client has SCV compliance violations, the actions defined in SmartDashboard are enforced.

When the Check Point Endpoint Security VPN Client and the Check Point Mobile for Windows Client connects to the Check Point VPN Gateway, an IKE negotiation takes place between the Check Point Endpoint Security VPN Client or the Check Point Mobile for Windows Client and the Check Point VPN Gateway. If the Check Point VPN Gateway Security Policy requires an SCV check to be made, the Check Point VPN Gateway holds the connection while it checks if the client is securely configured (SCV). If the Check Point VPN Gateway already knows the client's SCV status (example: the SCV status was checked in the last 5 minutes), then:

- If the client is securely configured, the Check Point VPN Gateway allows the connection.
- If the client is not securely configured, the Check Point VPN Gateway either drops the connection, or accepts and logs it (this behavior is configurable).

If the Check Point VPN Gateway does not know the client's SCV status, it initiates an SCV check by sending an ICMP unreachable error message containing an SCV query to the client.

When a client gets this SCV query, it tries to determine its SCV status.

In Connect mode, the client also connects to a Policy Server to download an updated SCV Policy. In parallel, when the client gets the SCV query, it starts sending SCV status replies to the gateway via UDP port 18233 every 20 seconds for 5 minutes.

These replies are used as a keep-alive mechanism, in order to keep the user's connection alive in the Check Point VPN Gateway's state tables while the client is trying to determine its SCV status. The keep alive packets also allow the user to open subsequent connections in the 5 minute period in which they are sent without a need for further SCV queries.

When the client determines its SCV status, it sends an SCV reply containing the status back to the Check Point VPN Gateway via UDP port 18233.

When the Check Point VPN Gateway receives the SCV status of the user, it decides how to handle the user's connection.

SCV POLICY SETS AND SYNTAX

Location at the MDS/SMS $FWDIR/conf/local.scv

The policy file contains: sets, subsets and expressions. Please see Micki Boland's Check Point White Paper Titled "SCV File Deep Dive" for in-depth build of the SCV file itself.

```
(SetName
   :SubSetName1 (
      :ExpressionName1_1 (5)
      :ExpressionName1_2 (false)
   )
   :SubSetName2 (
      :ExpressionName2_1 (true)
      :SubSetName2_1 (
         :ExpressionName2_1_1 (10)
      )
   )
)
```

For syntax details review Remote Access VPN R80.20 Administration Guide Secure Configuration Verification (SCV) Section and Check Point White Paper titled SCV File Deep Dive.

The file contains one single root set (SCVObject) containing five (5) pre-defined subsets:

1. SCVNames Defines legacy checks and actions (parameters for the checks)
2. SCVPolicy Activates checks defined at SCVNames (which checks are to be enforced)
3. SCVEpsPolicy Activates checks defined at SCVEpsNames
4. SCVEpsNames Defines checks supported from R75HFA1
5. SCVGlobalParams Defines global parameters

SCV PARAMETERS EXAMPLES

WindowsSecurityMonitor - This check uses Windows Security Center to monitor the status of computer security settings. Configure it in the SCVEpsNames section and activate it in the SCVEpsPolicy section. It includes the following checks:

- Network Firewall check
- Virus Protection check
- Spyware and Unwanted Software Protection check
- Windows Update check

CLIENT LOGS

Initiate debugging on the client - a cab file is created with the entire debug files inside. The file is located under C:\Documents and Settings\root\Local Settings\Temp\EndpointConnect\

Use the latest file called trlog_xx-xx-2012_time.cab

1) Initiate debugs on the Endpoint client:
   - Right click on the Endpoint Icon
   - Click "VPN Options"
   - Click on the "Advanced" Tab >> check the box "Enable Logging"
   - Click close
2) Replicate the issue
3) Collect debugs from the Endpoint client:
   - Right Click again on the Endpoint Icon
   - Click "VPN Options"
   - Click on the "Advanced" Tab >> click on the button "Collect Logs"

HELPFUL TIPS

Secure Configuration Verification (SCV) Traversal

Check Point Endpoint Security VPN Client or the Check Point Mobile for Windows Client users can connect to a gateway that requires SCV validation. In cases where a VPN Gateway is configured to only allow access to clients that have passed the SCV checks, an exception can be made not to apply the SCV check to SSL clients. This includes Endpoint Check Point Mobile and SSL Network Extender (SNX).

- To enable this feature, navigate to Global Properties >> Remote Access >> Secure
- Configuration Verification (SCV) >> Exceptions. Select the Do not apply Secure Configuration
- Verification on SSL clients connections checkbox.

SCV Granularity for VPN Communities

Access can be granted to specific hosts without being verified in order to allow the remote host to become fully compliant with the networks Security Policy. For example, if the Anti-Virus software is not up-to-date on a remote host, the gateway would normally block the connection entirely. However, access can be granted to the antivirus server in order to get the appropriate updates. After the updates are retrieved and installed on the remote host, it will pass the SCV check and get full access. SCV granularity is supported for Simplified Mode configuration only.

Blocking Unverified SCV Connections

When a client becomes unverified, there is an option in the local.scv file to block connections that require verification: block_scv_client_connections. When this feature is active, and the client enters an unverified state, all SCV connections are blocked, even those which were opened during the time the client was verified. However, only SCV connections are blocked; that is, only those connections that require the client to be in a verified state. Other connections are not blocked.

CONTACT US
Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2117 | Fax: 650-654-4233 | www.checkpoint.com

Connect Mode

The remote access clients connect with gateways using Connect mode. During Connect Mode, the remote user deliberately initiates a VPN link to a specific VPN Gateway. Subsequent connections to any host behind other gateways will transparently initiate additional VPN links as required. Connect Mode offers:

- Office mode, to resolve routing issues between the client and the gateway.
- Visitor mode, for when the client needs to tunnel all client to gateway traffic through a regular TCP connection on port 443.
- Routing all traffic through Gateway (Hub mode), to achieve higher levels of security and connectivity.
- Auto connect, when an application tries to open a connection to a host behind a gateway, the user is prompted to initiate a VPN link to that gateway. For example, when the e-mail client tries to access the IMAP server behind gateway X, SecureClient prompts the user to initiate a tunnel to that gateway.
- User profiles (Location Profiles)

Additional Script Elements

- SCVpolicy - selects SCV checks out of the ones defined in SCVNames that will run on the user's desktop.

- SCVGlobalParams - used to define general SCV parameters.

A network administrator can easily enable a set of specific SCV checks (e.g. only check that the user's SecureClient is enforcing a security policy) or as many SCV checks as required (e.g. all of the above SCV checks). The SCV checks are performed independently by the SCV Dynamic Link Libraries, and SecureClient checks their status through the SCV plugins every 20 seconds, and determines whether the user is securely configured or not. If one or more of the tests fails, the SecureClient is considered to be non-securely configured. Note - To enforce a specific SCV check, set the parameters of the check in the SCVNames section, and include the name of the check in SCVPolicy.

TROUBLESHOOTING SCV

Error: "file is corrupt"

Symptom: Client shows an error message … "Compliance Policy file is corrupt. Please contact your system administrator."

Scenario: An SCV check defined in the SCVPolicy section is not defined in the local.scv policy, SCVNames section.

Solution: Make sure that the SCVNames section includes all the checks that are to be run on clients.

Error: "unsupported format"

Symptom: Client shows an error message: Compliance Policy is in an supported format

Scenario: Can be one of these issues:

• There is no SCVObject section in the local.scv policy file.

• An SCV plug-in configured in the local.scv policy file does not exist on the client computer, or it has a functionality issue.

• The SCV Check type as defined in the local.scv policy is not a plug-in.

• The local.scv policy context has an incorrect format.

• The local.scv file was edited on an operating system that is different than the gateway operating system and the file was saved in an encoding that the gateway cannot read.

Solution: See the SCV section in this Administration Guide and follow the instructions to edit and maintain the local.scv file.

Error: "policy is not updated"

Symptom: Client shows an error message: Compliance policy is corrupt. Please connect again to update the policy.

Scenario: The policy enforced on the client computer is not updated with the latest security policy defined on the gateway.

Solution: Connect the client computer again to the gateway. The client pulls the latest security policy when it connects to the gateway.

LEARN TO CUSTOM BUILD THE SCV FILE

Please see Micki Boland's Check Point White Paper Titled "SCV File Deep Dive" for in-depth build of the SCV file itself.

DOCUMENT INFORMATION

Filenames: CheckPoint_WhitePaper_SCV_v1_MLB_17MAY2019.pdf

White paper friendly name: Check Point Secure Configuration Verification (SCV) White Paper

Version: v5

Author: Michele (Micki) Boland

Contact: mboland@checkpoint.com

Mobile: +1 615-593-0311