VPN-1 SecuRemote/SecureClient

Next Generation

Frequently Asked Questions

Abstract

VPN-1 SecuRemote is the Check Point VPN client. VPN-1 SecureClient adds Personal Firewall capabilities to SecuRemote. Both products changed significantly in the Next Generation release. This document contains Frequently-Asked Questions on the Next Generation version of both products and related technologies.

Document Title: SecuRemote/SecureClient FAQ
Creation Date: 01/07/2001
Modified Date: 05/09/2001
Document Revision: #3
Product Class: VPN-1 SecuRemote/SecureClient
Product and Version: NG
Author: Cyril Sultan

DISCLAIMER

The Origin of this information may be internal or external to Check Point Software Technologies. Check Point Software Technologies makes all reasonable efforts to verify this information. However, the information provided in this document is for your information only. Check Point Software Technologies makes no explicit or implied claims to the validity of this information. Any trademarks referenced in this document are the property of their respective owners. Consult your product manuals for complete trademark information.
SecuRemote/SecureClient NG FAQ

Contents

VPN-1 SecuRemote/SecureClient................................................................. 1
Next Generation  Frequently Asked Questions ......................................... 1
Abbreviations .......................................................................................... 5
Licensing .................................................................................................. 5
SecuRemote ............................................................................................. 6

A. General Remarks .................................................................................. 6
  1. What's new in SR NG? ......................................................................... 6
  2. SR/SC backward compatibility ........................................................... 6
  3. Which Operating Systems are supported? ............................................ 6
  4. Is FWZ still supported? ........................................................................ 6
  5. What are the infrastructure changes between SR/SC 4.1 and SR/SC NG? 6

B. Topology Download .............................................................................. 7
  1. Which authentication schemes are supported for topology download? 7
  2. Can I still download the topology from the Management Server? 7
  3. How is the topology downloaded by default? .................................... 8
  4. Can I change the port for topology download? 8
  5. How can I automate topology download? 8

C. IKE Key Exchange ............................................................................... 9
  1. Does SR/SC NG support new encryption algorithms? 9
  2. What is “IKE over TCP”? ................................................................. 9
  3. What's new in UDP Encapsulation? .................................................... 9

D. Certificate Support ............................................................................... 9
  1. Does SR/SC support other certificates than Entrust? 9
  2. Does SR/SC support CA hierarchies? ................................................. 10
  3. Does SR/SC support Hardware tokens/smartcards? 10
  4. What is SR/SC support with regards to PKCS#11, PKCS#12 and CAPI?10

E. SecureClient Packaging Tool ............................................................... 10
  1. What is SecureClient Packaging Tool? ............................................. 10
  2. What are the steps to build a new SR/SC package? 10
  3. How can I define the full network topology in the custom package? 11
  4. If a new topology download port is defined, will the management be notified? 11
  5. Do I need to create a new customized package for each OS? 11
  6. Is the custom package digitally signed? .............................................. 11

F. Additional Information ........................................................................ 11
  1. Does NG support multiple VPN-1 interfaces? 11
2. The Authentication message on SC Version 4.1 when used with VPN-1 Gateway NG is corrupted. Is this normal? ................................................................. 12
3. Do I still need to create a file dnsinfo.C to encrypt DNS requests? .......................................................... 12
4. Where are the debug files fwenc.log and sr.log? ........................................................................ 12

SecureClient............................................................................................................................... 13

A. General Remarks .................................................................................................................... 13
  1. Why upgrade from SR to SC? .......................................................................................... 13
  2. What’s new in SC NG? ............................................................................................... 13

B. Policy Server ........................................................................................................................ 13
  1. What is the role of the Policy Server in NG? .............................................................. 13
  2. Is it possible to give an administrator only Desktop Policy Read/Write permissions? .... 13
  3. Where can I install a PS? ............................................................................................ 13
  4. How do I install a PS? ................................................................................................ 14
  5. Is it possible to define High Availability for policy servers? ...................................... 14
  6. When I download the Desktop policy from the PS, can I see the policy on SC? .......... 14
  7. Interface resolving for PS logon .................................................................................. 14
  8. Is PS logon encrypted? ............................................................................................... 14
  9. Is Implicit Logon to PS supported? ............................................................................. 14
 10. What happens if the PS is not installed on the same machine as the GW? ................. 15

C. Desktop Security Policy ........................................................................................................... 15
  1. How do I define a Desktop Security policy? ............................................................... 15
  3. How can I see the SC’s implied rules? ......................................................................... 16
  4. How can I enforce a more restrictive policy when encrypting with the LAN? .......... 16
  5. Are the existing connections blocked when logging on / logging off? ...................... 16
  6. What is the policy when you are not connected to the Policy Server? .................... 17
  7. What is the default policy? ....................................................................................... 17
  8. How are “dialup” IP addresses handled when SC policy includes usergroup@specific-ip’s? 17
  9. How does SC communicate with the Policy Server? ................................................ 17
 10. Is it possible to modify SC policy from SC machine? .................................................. 18

D. SecureClient Logging.............................................................................................................. 18
  1. What is the SC logging policy? .................................................................................... 18
  2. What are SC logs? ...................................................................................................... 18
  3. Sometimes, the Systray icon envelope green lock blinks. What does this mean? ....... 19
  4. Why does the SC icon not blink red for every blocked packet? ................................. 19
  5. How do the logs get to the management server? ....................................................... 19
  6. How can I view the SC logs in the management’s Log Viewer? ................................. 19
  7. What is the “default” user that appears in the logs? ................................................... 19
  8. Is it possible to switch/purge the logs in SC Log Viewer? .......................................... 19
  9. Is there any integration between the Desktop Rule Base and the Visual Policy Editor (VPE)? 20

E. Secure Configuration Verification (SCV) ........................................................................... 20
  1. What is SCV? ............................................................................................................. 20
  2. How does SCV work? ............................................................................................... 20
  3. Can SC support multiple SCV DLL’s? ....................................................................... 20
  4. How are the DLL distributed? .................................................................................. 21
  5. How can I define the SCV policy? .............................................................................. 21
6. When are the SCV checks performed on SC? ................................................................. 21
7. When is SCV information sent by SC to PS / VPN-1 GW? ........................................... 21

F. Client Software Distribution Server (SDS) ............................................................... 21
1. What is SDS? .................................................................................................................. 21
2. Where can the SDS be installed? How many SDS are supported per management server? .... 22
**Abbreviations**

SR – SecuRemote  
SC – SecureClient  
PS – Policy Server  
FW – FireWall  
GW – Gateway  
NG – Next Generation  
NAT – Network Address Translation  
IKE – Internet Key Exchange

**Licensing**

If you only have SecuRemote users, the license is free of charge, and needs to be installed on the topology server (FW Module from which SR will download the topology).

For SecureClient NG you will need two separate licenses:

- On the Management Server: SecureClient user license, specifying the number of SecureClient users allowed.
A. General Remarks

1. What’s new in SR NG?
SR Next Generation (NG) contains many new features:

- Full smart card/PKI integration through native CAPI and PKCS #12 support
- Topology download with all authentication schemes
- New encryption algorithms
- Easier installation
- UDP Encapsulation improvement
- IKE over TCP

2. SR/SC backward compatibility
SR NG is compatible with VPN-1/FireWall-1 version 4.1 or NG.
SC version 4.1 is compatible with VPN-1/FireWall-1/Policy Server version 4.1 or NG.
SC NG can encrypt with VPN-1/FireWall-1 version 4.1 or NG, but can download Desktop Policies ONLY from Policy Server NG.

3. Which Operating Systems are supported?
SR/SC is supported on: Windows NT 4.0 SP6a, Windows 2000, Windows 98 and Windows ME. SR/SC is no longer supported on Windows 95/95b.
For Windows 95/95b users, SR/SC 4.1 will still be supported on those platforms.

4. Is FWZ still supported?
FWZ and FWZ Encapsulation are still supported with SR NG.
However, SC NG supports only IKE for Logon to Policy Server.

5. What are the infrastructure changes between SR/SC 4.1 and SR/SC NG?
From a kernel perspective, SR kernel is now split in two separate drivers: Personal Firewall kernel module (fw.sys in Windows NT/2000, fwmac.vxd in Windows 98/ME) for packet filtering and inspection, and VPN kernel (vpn.sys in Windows NT/2000, fwldr.vxd in Windows 98/ME) for all encryption-based operations in kernel-space.
In the user mode in Version 4.1, all the operations were based in fwenc.exe. In NG, there are different DLLs, and three processes:
• SR_Service (runs as a service): main “daemon”, which communicates with the kernels, and contains the VPN daemon code.

• SR_WatchDog (runs as a service): guards SR_Service.exe against crashes (by reviving it) and against attempts to kill SR_Service outside of SR/SC.

• SR_Gui - it contains all of the MFC-based GUI code.

6. How does SR/SC run?
On Windows NT/2000, the first process to run is SR_service.exe, which runs as an automatic NT service. It starts SR_WatchDog, and runs SR_Gui as well. The system can be stopped via the GUI – “Stop VPN-1 SecureClient” or “Stop VPN-1 SecuRemote” (using the systray icon or the File menu in the application window). When stopping the system this way, SR_service is stopped, and SR_Gui exits as well, while SR_WatchDog stays in the background.

If SR_Gui is stopped via the Task Manager, or if it crashes, SR_WatchDog will run it again.

Two important points:

• SR/SC can be stopped from the Services menu by an administrator

• If someone decides to stop the SR_WatchDog service, and then tries to launch the GUI via Start->Program Files->SecureClient, this will not work, and SR_Service will have to be started via the Services menu to revive SR.

B. Topology Download

1. Which authentication schemes are supported for topology download?
All the authentication schemes used by IKE hybrid mode are now supported for topology download in SR/SC NG.

2. Can I still download the topology from the Management Server ?
There are now three different methods to download topology:

   1. From the Management Server in clear (FWZ keys need to be defined)

   2. From the VPN/FireWall Module: using SSL encryption with pre-shared secrets/certificates

   3. From the VPN/FireWall Module: using SSL encryption after exchanging keys via IKE with all authentication methods supported (IKE Hybrid Mode).

Methods (1) and (2) are the old methods of topology download. Method (3) is the new method introduced in NG. Method (1) is not recommended for security reasons (topology sent in clear)
3. How is the topology downloaded by default?
By default, SR/SC NG will download the topology with method (3) (SSL over IKE Hybrid authentication). If VPN-1/FireWall-1 does not support IKE/hybrid mode and certificates are not being used, then topology download/update may fail. In order to switch to methods (1) or (2) the following steps should be taken:

- On the client side, the property “topology_over_IKE” should be set to false in the userc.C options field, in order for new SR/SC installations. This can be pre-configured in the package that is distributed to users.
- On the Management station, the administrator should set the property "desktop_topology_over_IKE" to false in the :props section for users that will upgrade the client from version 4.1 to NG. Note - the client should update their topology prior to performing upgrade, or choose to “overwrite” during upgrade, and use a package that has “topology_over_IKE” set to false in the userc.C file, as described above.

4. Can I change the port for topology download?
Yes – this requires configuration both on the client and on the server.

On the Client, it can be configured in the userc.C options set manually (property "gettopo_port (264)") or by using the Packaging Tool.

On the server, the port needs to be changed in the file $FWDIR\conf\ports.conf.

If you modify the port, you should also add a new rule to the Topology Server to allow this connection.

5. How can I automate topology download?
By default, the user will have to manually update the site if he/she needs to get the latest topology.

You can make topology download automatic in the following ways. On the Management Server, edit the objects_5_0.C file (See SecureKnowledge Solution skI3301), and in the properties set:

- Configure the property “desktop_update_at_start (true)”. When this attribute is set to true, the user will be prompted to update this topology every time SR/SC starts running.
- Configure the property “desktop_update_frequency (n)”. The site’s topology will be automatically updated after key exchange if “n” seconds have passed after the last topology download.

Some other properties may be also of interest for topology download. Please refer to the VPN User Guide.
C. IKE Key Exchange

1. Does SR/SC NG support new encryption algorithms?
   - SR/SC NG supports the new encryption algorithm Rijndael (proposed AES candidate) with 128/256 key bits length. It has proven to be very fast compared to 3DES (8-12 times in some scenarios).
   - Diffie-Helman keys of different lengths are supported in IKE Phase 1 (1024, 1536).
   - IP Compression (Deflate Mode) is now supported with SC only. It is negotiated during key exchange. Moreover, Check Point’s IPCOMP implementation is “adaptive” - application data that has poor compressibility (i.e., binary oriented data) is not compressed.

2. What is “IKE over TCP”?
   IKE Phase 1 may fail due to non-standard behavior of different NAT devices. The reason is that some NAT devices do not handle UDP fragmented packets correctly. This problem appears very often in a PKI environment when a large Certificate Revocation List (CRL) is sent by the Firewall, creating a large UDP packet, which is fragmented.
   The solution in SR/SC NG and 4.1 SP4 is to force SR/SC to use IKE over TCP (in Phase 1). This can be done via the SR GUI (Tools/Encryption Schemes, Advanced button).

3. What’s new in UDP Encapsulation?
   In SR/SC version 4.1 (until SP3), UDP Encapsulation was chosen by VPN-1/FireWall-1 only if IKE source port was different from 500. Therefore, for NAT devices that did not translate the source port, UDP Encapsulation was not chosen.
   In FireWall-1 NG and FireWall-1 4.1 SP4, UDP Encapsulation detection has been improved: the firewall will automatically choose UDP encapsulation if the IKE ID is different from the source IP.
   There may be some cases in which the decision to use UDP encapsulation is not taken (when it should be), and then it may be necessary to force the use of UDP Encapsulation, you can now do it from SR/SC GUI (under Tools/Encryption Schemes, Advanced button).

D. Certificate Support

1. Does SR/SC support other certificates than Entrust?
   SR/SC version 4.1 already supports all types of certificates: Entrust, Baltimore, Verisign, etc. However, it was necessary to convert non-Entrust certificates to Entrust format (.epf).
   In NG, this limitation is removed - you can directly use PKCS#12 or CAPI certificates with SR/SC.
2. Does SR/SC support CA hierarchies?
Yes. SR/SC now supports Certificate Authority (CA) Hierarchies.

Therefore, they can now be used in networks with complex PKI deployments, such as Extranets where two or more organizations have separate CA’s with a common root CA.

3. Does SR/SC support Hardware tokens/smartcards?
Yes. In Version 4.1, we supported HW tokens, but only with Entrust certificates, and only the vendors that were Entrust certified. In SR/SC NG we support CAPI natively, and we have an OPSEC program for PKI partners, including certificate storage/generation on CAPI-compliant smartcards and other tokens.

4. What is SR/SC support with regards to PKCS#11, PKCS#12 and CAPI?
SR/SC supports CAPI and PKCS #12, but not PKCS #11.

PKCS#11 is only supported on the VPN-1 Module (i.e., gateway) for integrating public key operation accelerators and secure key generation and storage.

In addition to the OPSEC PKI Integration document, another document exists, about the “Token Integration Guidelines”. Please check the support site http://support.checkpoint.com/ for more information about both documents.

E. SecureClient Packaging Tool

1. What is SecureClient Packaging Tool?
The SC Packaging Tool is a Check Point Management client application (included in the Management Clients package) that allows administrators to configure SR and SC installation packages with site information and attributes, including answers to all installation dialogs shown to the user. The application allows administrators to configure attributes in userc.C, product.ini and entrust.ini files.

When done, the application generates a self-extracting executable from the installation package. All the user needs to do is to run the executable (no zip involved, possible fully-silent installation) and reboot, and then he/she is prompted to update the site (no need to define new site).

2. What are the steps to build a new SR/SC package?
   1. Download the latest SR/SC build, and unzip it in a directory, for instance: “C:\Temp\SC”
   2. Create a new directory “C:\Temp\SC_package1”, where you will store the new package
   3. Close all the open CP Management Client (such as the Policy Editor)
   4. Run the SecureClient Packaging Tool
   5. Create a new profile, and enter all the parameters you wish for your SR/SC users
6. At the end of the wizard, choose “Yes, Create profile and generate package”

7. In “Package Source Folder”, enter the folder: “C\Temp\SC”

8. In “Package Destination Folder”, enter the folder “C:\Temp\SC_package1”

A self-extracting executable file will be created in “C:\Temp\SC_package1”. It is the executable that you can send to your users.

3. **How can I define the full network topology in the custom package?**

If you do not want to use the Partial Topology feature, and prefer to package a userc.C file that includes the full topology of the Encryption Domain, then you should proceed this way:

- Create the userc.C file (using SecuRemote to define the site)
- Replace the userc.C file in the unzipped package (ready for customization) with the newly created userc.C file
- Use the SC Packaging Tool to configure a profile - do not choose Partial Topology. The custom package will have the full topology with the customized "options" section.

4. **If a new topology download port is defined, will the management be notified?**

No. In the SC Packaging Tool, you can configure the port to which you want your SC to download the topology (if the default port is used for another service). If you modify its default value, the Management will not be updated automatically; you’ll need to change the file in $FWDIR\conf\ports.conf and add a new rule on the Rule Base and to support this feature.

5. **Do I need to create a new customized package for each OS?**

Yes. Since the packages are different for Windows 98/ME, NT and 2000, you should repeat the package creation process for every operating system you need to support.

6. **Is the custom package digitally signed?**

The custom package is currently not signed, but this is under consideration for future versions.

**F. Additional Information**

1. **Does NG support multiple VPN-1 interfaces?**

Yes. In NG, the property “resolve_interface_ranges (true)” is set by default in objects.C. Therefore, if Anti-spoofing is configured correctly on your VPN-1/FireWall-1, SR/SC will know to which interface to encrypt.
2. The Authentication message on SC Version 4.1 when used with VPN-1 Gateway NG is corrupted. Is this normal?
It is a known issue between SR version 4.1 and VPN-1/FireWall-1 NG, which is currently under investigation.

3. Do I still need to create a file dnsinfo.C to encrypt DNS requests?
In NG, you do not need to create a file dnsinfo.C to force encrypted DNS requests. You can configure encrypted DNS the following way:
   1. In the Policy Editor, create a new server of type “SecuRemote DNS”, and define the domain name, number of labels, etc. The information generated will be stored in the file objects.C.
   2. In the Policy Editor, under “Global Properties/Desktop Security”, set the parameter “Encrypt DNS traffic”.
   3. Edit the file crypt.def and modify the appropriate property.
The information will then be stored in the objects.C file (not dnsinfo.C as in previous versions).
Nevertheless, if you want to create lmhosts entries for SDL, then you still need to use the dnsinfo.C file. The file dnsinfo.C will be merged with the DNS information created above during topology download.

4. Where are the debug files fwenc.log and sr.log?
SR/SC NG uses different log files to store its debug information.
The SecureClient Log Viewer application contains SC kernel logs, and other important information, such as SCV state changes; it is similar to the Management’s log Viewer (replaces the use of sr.log).
Each SR/SC process has its own log file:
SR_Service has sr_service_tde.log, SR_Watchdog has sr_watchdog_tde.log, and SR_Gui has sr_gui_tde.log.
All these log files are located in “C:\Program Files\CheckPoint\SecuRemote” (unless a different location was chosen during installation).
sr_service_tde.log, sr_gui_tde.log and sr_watchdog_tde correspond to the old fwenc.log, although almost all of the relevant information resides in sr_service_tde.log.
If you want to enable "full" debug logging:
   • Add sr_tde.all to c:\, and restart SR/SC – will turn on full SR/SC debugging and create sr_service_tde.log, sr_gui_tde.log, and sr_watchdog_tde.log.
   • Add fwike_debug.all in c:\, and add the environment variable FWIKE_DEBUG=1, and restart SR/SC. You will then get the IKE debug information in the program files\CheckPoint\securemote\log\ike.elg file (this information can be used by the IKEView application).
   • Add srgina.log in c:\ and restart the machine - will log gina information to c:\srgina.log.
SecureClient

A. General Remarks

1. Why upgrade from SR to SC?
VPN-1 SecureClient provides enhanced desktop security and client software management features in addition to the standard VPN-1 SecuRemote functionality.

2. What's new in SC NG?
SC NG already supports the new features of SR NG (cf. section I above).
Moreover, SC supports the following new features:

- Centrally-managed, granular Desktop Security policy (Personal Firewall)
- SCV (Secure Configuration Verification) architecture, including integration with SCV OPSEC partners
- IP Compression
- Automatic software update
- Policy Server redundancy (Backup Policy Servers)

B. Policy Server

1. What is the role of the Policy Server in NG?
The policy server has different roles:

- Delivers policies to clients
- Collects logs from client machines
- Delivers SC info to other components: SC log on/off to UAG, log and alert data to CP Management stations, maintains state on current connected SC users.

The policy server must run on a VPN-1 module, with a policy server license.

2. Is it possible to give an administrator only Desktop Policy Read/Write permissions?
No, it is currently not supported.

3. Where can I install a PS?
Policy Server NG needs to be installed on a VPN-enabled module.
However, the Policy Server cannot be a member of a Cluster object, or on a Cluster member.
4. How do I install a PS?
Unlike Version 4.1, Policy Server NG is a separate product, with its own installation package.
Once you install it on your VPN module, you need to set the Policy Server checkbox on the Network object, and specify a user group that will be allowed to logon to this Policy Server (under Authentication).

5. Is it possible to define High Availability for policy servers?
NG provides high availability by having the client use Backup Policy Servers. If you define multiple Policy Servers, and if PS-HA is enabled (it is by default), then when communication with a particular PS fails, SC will automatically try with other Policy Servers, until it finds one that responds.
Note that this type of HA may cause strange behavior if different groups of users are licensed on different Policy Servers, since SC may use a backup Policy Server on which the user is not licensed.
Another limitation to the PS-HA mechanism is that all Policy Servers should have the same Desktop Policies installed on them, otherwise users may get different policies when logging on to different Policy Servers.
In future releases we plan to enhance PS HA, and to support cluster environments.

6. When I download the Desktop policy from the PS, how can I see the policy on SC?
In the current version, it is possible to look at the file local.dt under the SecuRemote\Policy directory, and see a textual representation of the Desktop rule base.

7. Interface resolving for PS logon
SC can logon to a PS from all its interfaces (if the PS is installed on a Gateway). However, some restrictions exist; they are documented in the Release Notes.

8. Is PS logon encrypted?
Yes. PS logon is always encrypted: on the LAN (if SC is inside the Encryption Domain), SSL is used to encrypt policy download (after IKE authentication). Outside the LAN, IKE/IPSEC is used.

9. Is Implicit Logon to PS supported?
In NG, implicit logon is not supported. However, you can add the option “default_ps (x.x.x.x)” in the options section of the userc.C file. If this property exists, SC will try to automatically logon to the PS whose IP (x.x.x.x) is specified, as soon as it is launched. Note – this means that the user will see an authentication window every time SC is launched.
10. What happens if the PS is not installed on the same machine as the GW?
You need to open some ports on your GW in order to allow connections from SC to PS. These connections are:

- UDP/500, TCP/500, ESP, UDP/2746 - for IKE/IPSec/UDP Encapsulation
- TCP/18231, UDP/18233 - for PS logon and SCV status

Moreover, there is no connection between the GW and the PS. The GW will know if SC is not securely-configured, due to the SCV information which is sent from SC to the GW (when necessary).

C. Desktop Security Policy

1. How do I define a Desktop Security policy?
In the Policy Editor, define the Desktop Security policy in the “Desktop Security” tab.

Here are some basics:

In each rule, you need to define a User’s Group in the “source” or “destination” (but not both). The location of the User’s Group specifies the SC machine – rules that have user’s groups in the source relate to connections originating in the SC machine, while rules that have user’s groups in the destination relate to connection destined for the SC machine.

Rules that have “All Users” as the user’s group will apply to all SC installed users, at any time (these are called “default” rules). The rules with user’s groups other than All Users will apply to SC authenticated users who belong to this group.

If for instance, you want to define a rule: ”Any Any Drop”, you need to split it in two rules:

“All Users @ any Any Drop” (outbound rule)
“Any All Users @ any Drop” (inbound rule)

The “Install On” column is not editable; it simply indicates what type of rules you have configured: inbound (=>Dst) or outbound (=>Src).

If no default rule is configured, then there are two default rules added to the end of the policy: Block Inbound and Accept Outbound.

If you run the Policy Editor in “local mode” (log into *local), you can see some examples representing Version 4.1 policies (via File->Open->Open Individual Policies by name, choose Desktop Security).

2. Can I “verify” my Desktop Security policy?
No, you cannot verify your Desktop policy in the current version.

However, if you try and install the policy, if the policy cannot be installed you’ll get an appropriate error message during policy compilation.
3. How can I see the SC’s implied rules?
There is no possibility to see the SC implied rules, since they are included in the SC kernel module.

Here is a list of all the services allowed on SR/SC:
- UDP/259, incoming and outgoing: RDP packets
- UDP/500, incoming-outgoing: IKE
- TCP/500, outgoing: IKE Phase 1 over TCP
- UDP/53, outgoing: DNS
- TCP/264, outgoing: topology download
- TCP/256, outgoing: topology download (backwards compatibility)
- DHCP: statefully, unless disabled in userc.C (inbound DHCP packets will be accepted only if an outbound DHCP packet was recently sent).

Specifically For SC:
- UDP/18233, outgoing: SCV keep_alive packets
- TCP/18231, outgoing: PS logon
- TCP/18232, outgoing: Software Distribution Server protocol

4. How can I enforce a more restrictive policy when encrypting with the LAN?

Implementation:
Set up your Client Encrypt rules on the VPN to require Desktop Verification (SCV)
Set your "logged on" policy to be restrictive (allow only LAN connections), for example:

1. SCUsers@Any LAN Any Encrypt
2. SCUsers@Any Any Any Block
3. AllUsers@Any Any Any Accept

When logged on to a PS, Rules 1 and 2 will apply, and will effectively block out rule 3. A User that wants to access external resources will need to logoff, at which point only rule 3 will apply, and he/she won't be able to open new connections to the LAN.

5. Are the existing connections blocked when logging on / logging off?
With the above example (in question 4):
- When users log on, existing connections outside the LAN will be blocked, since they are not permitted by the Desktop Rule Base.
- When users log off, existing connections to the LAN will not be blocked, since they are still permitted by the Desktop Rule Base (they're disallowed on the Firewall).
6. What is the policy when you are not connected to the Policy Server?
After installation, SC has no policy. Even if you upgrade from SC 4.1, SC NG will have no policy until the first successful logon to PS.
After logon to PS, SC will have the logon policy: all the rules that match the current user and IP’s will be applied.
After logoff from PS, SC will have a default policy: only the rules with AllUser@ will be applied.

7. What is the default policy?
The default policy is the policy that is enforced when the user is not logged on to a Policy Server: after logoff from PS, when SC is stopped, when the machine comes up after boot and the user has not logged on to a PS yet.

8. How are “dialup” IP addresses handled when SC policy includes usergroup@specific-ip’s?
Usually the user would perform Logon to Policy Server in the Dialup case after he has an IP address.
During the Logon to PS process the IP addresses in the Desktop Rule Base will be checked against the IP addresses on the machine to see whether the rule applies (only rules that apply to the current user and IP addresses will be enforced): the Desktop Security Policy will be reloaded.

9. How does SC communicate with the Policy Server?
There are two different connections:
- TCP/18231: Periodic log on to PS. It is used for Security Policy, SCV policy, and Logging Policy download.
- UDP/18233: SCV State Keep Alive.
What is the end-user impact with SC NG?
The end-users should logon to the policy server: click on the right button on the systray icon, “Logon to Policy Server”. This can be automated by defining a Default Policy Server (via default_ps (n.n.n.n) in the options section of userc.C or in the SC Packaging Tool). If a Default Policy Server is defined, SC will attempt to logon to this PS as soon as it runs.
During SC logon to a PS, it will check policy hashes, and get new policy files if they have changed on the Policy Server. It will start execute SCV checks and if everything is correctly configured, it will be able to access the corporate network.
Note that SCV checks happen all the time, not just after logon to PS.
After the logon process is over, the user has access to all resources defined for his user’s groups (for example, the mail server).
If the user wants to revert to the Default Policy, he/she will need to logoff from the Policy Server.

10. Is it possible to modify SC policy from SC machine?
No. You can try and edit the file local.dt on SC, but once SC started, its policy will be removed, and you will be asked to download a new policy.

D. SecureClient Logging

1. What is the SC logging policy?
SecureClient logging policy is defined on the management server in $FWDIR\conf\local.lp. During PS logon, this policy will be downloaded to SC. The local.lp file defines the amount of disk space the logs will occupy on the client’s disk by defining a number of file “generations”, and size per file generation.

The local.lp that is installed on the management server by default has the following structure and values:

(LogObject
   :LocalPolicy (    :gennum (5)
      :filesize (100000)
   )
   :UploadPolicy (    :retriesnum (3)
      :gennum (5)
      :filesize (20000)
      :action_filter (        :action (1)
         :drop (1)
         :reject (1)
      )
   )
)

There are two policies:

LocalPolicy: policy for the logs in local.
UploadPolicy: policy for the logs that should be uploaded. Note that it has smaller generations size, therefore these log files will contain fewer logs.

The retriesnum attribute defines the number of times that SC will try to upload a file before those logs become obsolete.

For more information about the SC log policy, please read the VPN User’s Guide.

2. What are SC logs?
SC produces three types of logs:
1. Connection-oriented logs - the usual connection information logs
2. SC Control logs - user policy installed, machine is not configured, etc.
3. SCV Check logs - Logs that are generated by external SCV checks that want to report relevant information.

3. Sometimes, the Systray icon envelope green lock blinks. What does this mean?
   It happens only when SC is logging on to a Policy Server. Once SC finishes the logon process, the green lock is fixed.

4. Why does the SC icon not blink red for every blocked packet?
   The icon will blink red if and only if the blocked connection is logged.
   The user can also choose to "log all blocked connections" from the SC/Tools menu. This will force logging on every blocked connection.

5. How do the logs get to the management server?
   Each time SC performs logon to PS it will try to upload the logs that were defined for upload. Currently SC NG will upload only logs that have been marked as alerts.

6. How can I view the SC logs in the management’s Log Viewer?
   The SC logs will be sent from the PS to the management server
   Moreover, you can also take the files manually from SecuRemote\Log directory, zip them and copy them to the log directory on the Management Server. You will be able to see them using the VPN-1/FireWall-1 Management log viewer (File/Open…).

7. What is the “default” user that appears in the logs?
   As explained above, SC sends its logs to PS and then to the management server.
   The logs that one can see on the management server with user “default” are logs that occurred when no user was logged on to a PS, and the default security policy was running (rules with All Users). It is not recommended to define a username “default”, as logs generated by this user will not be distinguishable from SC’s default user.
   Logs generated when SC is logged on to PS will show the logged-on-user’s username.
   The reason for this behavior is that it is impossible for SC to establish the identity of the user until he/she logs on to a PS.

8. Is it possible to switch/purge the logs in SC Log Viewer?
   You cannot manually switch the logs (logswitch) on SC. This is done automatically when the log file reaches a predefined size. The size is determined by the Logging Policy, which is configurable by the administrator.
“Purge” of logs is not supported. The only way to remove logs is to stop SC, remove all the files in SecuRemote/Log directory, and then launch SC again.

The administrator can limit user access to the Log directory in order to prevent users from erasing logs; this can be done by restricting user access to administrators only for the Log directory (in Windows NT/2000).

9. Is there any integration between the Desktop Rule Base and the Visual Policy Editor (VPE)?

No. There is currently no integration with VPE.

E. Secure Configuration Verification (SCV)

1. What is SCV?

Secure Configuration Verification is a platform that allows SecureClient to determine whether the machine is securely-configured. Firewall modules may require the client to be Securely-Configured in order to accept connections from the client.

SecureClient already contains the basic SCV checks that were available in Version 4.1, and enforces them via the Policy Editor (Global Properties - Desktop Security). SecureClient NG also supports 3rd party SCV checks, and there is a new OPSEC API for partners to write their own SCV DLL’s. On the firewall side, VPN/FireWall Modules support SCV checks for Client Encrypt and Client Auth rules in NG.

2. How does SCV work?

- The administrator sets the SCV checks and installs the SCV policy on Policy Servers (by installing on Desktop Security targets).
- If the SCV check is external – the SCV DLL should be installed on the SC machine.
- SC logs onto Policy Server, installs Desktop Security and SCV policies (only if changed from last PS logon)
- SC periodically launches SCV checks and reports state to PS (UDP) for status/logging /single-sign-on (for User Authority) purposes.

Each individual SCV check simply reports pass/fail, the machine’s SCV state is considered “Securely-Configured” if all SCV DLL’s reported that the check passed.

A single SCV check can validate/test many settings: for instance, if the Antivirus is executing and has updated virus definition files, etc.

3. Can SC support multiple SCV DLL’s?

Yes. SC can support multiple SCV DLL. You may have for instance one DLL to check your anti-virus setting, and another DLL to check your Internet Explorer settings.
4. How are the DLL distributed?
SCV DLL’s can be distributed via the Client Software Distribution mechanism. The SCV policy is distributed via the PS logon.
However, the SC Packaging Tool does not support SCV DLL packaging with its custom packages.

5. How can I define the SCV policy?
On the Management Server, edit the file local.scv (located in $FWDIR\conf directory).. Once done, install on Desktop Security targets (Policy Servers).

6. When are the SCV checks performed on SC?
SC performs a check with SCV DLL's every 15 seconds.
Moreover, SCV DLL's can report that a certain SCV check failed immediately to SecureClient (without waiting for the regular SCV check described above)
As soon as SecureClient's SCV status moves to not-securely-configured, it sends SCV status packets immediately to any Policy Servers and Gateways that it is currently connected to (the Policy Server that it logged on to, and any Gateways that asked for SCV status within the past 5 minutes).

7. When is SCV information sent by SC to PS / VPN-1 GW?
There are two kinds of SCV keep-alive connections:

- SCV state UDP packets to the PS: Sent after logon to PS, these packets are sent once a minute for monitoring the client's status, as long as SC is logged on.
- SCV state UDP packets to the GW: Sent when a Gateway requests SCV information from a client machine (after a packet was matched on a rule that required SCV information). These packets are sent every 20 seconds (for 5 minutes).

These UDP packets (for Gateways and Policy Servers) are slightly different. If a PS resides on a GW that requires SCV checks, UDP packets of both types will be sent.
All of the connection frequencies and settings can be configurable on the management server (See the VPN User’s Guide for more information).

F. Client Software Distribution Server (SDS)

1. What is SDS?
SDS stands for Software Distribution Server. After the client downloads topology, it determines if components are out of date. In case it needs to update components, it gets new packages from the SDS, installs them, and restarts SR service or reboots as needed. The user is prompted for confirmation before downloading components and before installation of the new package.
2. Where can the SDS be installed? How many SDS are supported per management server?

SDS should be installed on a VPN/FireWall Module. In the current version, only one SDS server is supported per management server.