Interested in learning more about security?

# SANS Institute InfoSec Reading Room



## VPN-1 SecureClient - Check Point's Solution for Secure Intranet Extension

Remote users are at risk when using broadband connections to access organizational resources. The VPN-1 SecureClient v4.1 and VPN-1 SecureClient NG products from Check Point Software Technologies Ltd. provide secure VPN access to these resources while protecting the remote machine with a personal firewall. These products can only be used when integrated with existing Firewall-1 v4.1 and Firewall-1 NG Check Point software, and are managed and maintained through the Firewall-1 management console. SecureClient is widely c...

Ryan Gibbons
GSEC Practical Assignment v1.3

# VPN-1 SecureClient – Check Point's Solution for Secure Intranet Extension

## ABSTRACT

Remote users are at risk when using broadband connections to access organizational resources. The VPN-1 SecureClient v4.1 and VPN-1 SecureClient NG products from Check Point Software Technologies Ltd. provide secure VPN access to these resources while protecting the remote machine with a personal firewall. These products can only be used when integrated with existing Firewall-1 v4.1 and Firewall-1 NG Check Point software, and are managed and maintained through the Firewall-1 management console. SecureClient is widely compatible and has a small footprint, making it appealing to organizations that use Check Point products and are considering such functionality.

The personal firewall included with SecureClient can adequately block external access to the remote machine and create a secure working environment. The VPN-1 products use IPSec with IKE and FWZ and are capable of strong encryption for the VPN. Setup and management are straightforward and include some very useful management features that allow the security policy to be easily maintained for a large user base. SecureClient performs all of its intended functions well and is an attractive product for those searching for such a solution.

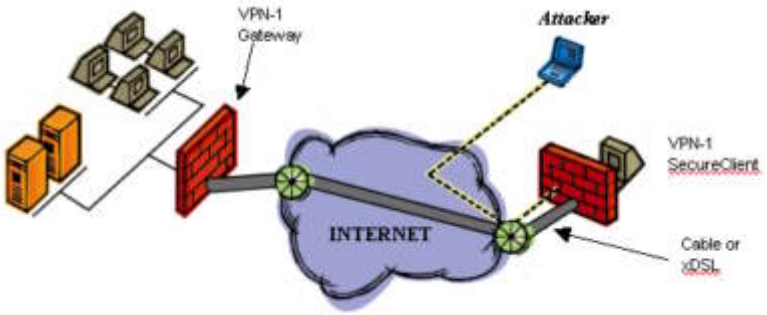


**Figure 1 - VPN-1 SecureClient Secures Remote Access** [CHK00]

## INTRODUCTION

In our current work environment, security has a tall order. Users now need to be able to connect to all of their internal applications from the office, home, hotels, airports, and anywhere else that has Internet access. Unfortunately, the security at most of these places is dismal – especially when the public Internet is involved – leaving the remote user wide open to a variety of attacks. The increased demand for constant access to the internal network from insecure locations has made virtual private network (VPN) and personal firewall technologies an essential part of security strategy. The VPN allows users to establish a virtual private tunnel with their internal network and access the

necessary applications as if they were at their office desk (albeit most likely at a slower rate). The personal firewall component is necessary to protect these new extensions to the office. It helps ensure that the person coming in through the VPN is safe from attacks and not playing host to an unknown third party – illustrated by Figure 1 above. Check Point's VPN-1 SecureClient combines these two technologies into an attractive product for the remote desktop that seamlessly integrates with existing FireWall-1 4.1 or NG installations.

## DEPLOYMENT CONSIDERATIONS

VPN-1 SecureClient is not a standalone product. In order to make use of this solution, an existing Check Point FireWall-1 infrastructure along with a SecureClient policy server should be in place. It is based on SecuRemote (the predecessor to SecureClient which lacks personal firewall capabilities) and is a straightforward upgrade as the infrastructure, policies, and trained personnel are all available to keep the project complexity to a minimum. This advantage apparently applies to a large number of users, as Check Point claims 100 million SecuRemote, SecureClient, and SecureClient NG licenses. For those who use anything else, this is obviously a major hurdle and should only be considered if the entire solution is desired. Per-seat licenses must be purchased for the management server based on the number of SecureClient users supported, and bulk-pricing discounts are applied for larger numbers of users [COM].

SecureClient compares well to other personal firewall products in circulation, while including some enterprise management features that assist in its use by large organizations. A very brief comparison will be done with last year's PCMagazine Editor's Choice – the ZoneAlarm Pro product from ZoneLabs – to highlight this point. ZoneAlarm is simple to install (hit the 'enter' key or click 'next' a few times), has a secure default configuration, and can be further customized by the user as they launch and grant approval for various applications to access the network. It is a standalone product, lacks VPN capability, and is application aware [ZON].

| | SecureClient | ZoneAlarm Pro |
|---|---|---|
| **VPN Capability** | Yes | No |
| **Security Policy** | Centrally managed | Managed by user |
| **Client-side Install** | Can be made transparent to user | Simple |
| **Preconfiguration** | Yes | No |
| **Connection Logging** | Yes – saved to text or sent to management station | Yes – saved to text file |
| **Secure Out-of-Box** | Will not work properly until it is fully configured. | Yes |
| **OSI Model Operation** | Levels 4 and 5 (TCP/IP stack) | Level 7 (Application aware) |

| | | |
|---|---|---|
| **Stateful** | Yes | Yes |
| **Cost** | $60-90 per seat | Free for home use. $36-50 for businesses (PRO) |

**Figure 2 – Comparison of Features**

SecureClient gives up some user control and simplicity in order to maintain a uniform security policy and VPN configuration for all users of the organization. User error is always a risk, and it would not be practical to allow the users to establish the VPN back to the firewall and maintain a workable security policy with any degree of confidence. Even the most highly trained and well-intentioned users would be prone to error. By keeping things centrally managed, the burden of security stays with those responsible for network security – those who have the tools and ability to make it work.

## COMPATABILITY

The footprint for SecureClient is small, requiring only 20MB of hard drive space and 64MB of RAM (< 5MB actually used) on the end user's machine. The client can be easily obtained by downloading the latest version from the Check Point website, and is available without registration or immediate purchase. There are no known restrictions regarding the specific brand of NIC (Network Interface Card) used, as SecureClient does not operate at the driver level.

Any version of SecureClient is compatible with any version of FireWall-1 v2.1c or later except for the Macintosh and NG versions. The Mac version requires FireWall-1 v4.1 SP3 or FireWall-1 NG, and SecureClient NG requires FireWall-1 NG to function properly. SecureClient (SC) has an impressive list of compatible client operating systems, including [WEL02]:

- Windows NT 4.0
- Windows 95 OSR2 (SecureClient v3.0)
- Windows 98 (SecureClient 4.0 build 4003)
- Windows ME (SecureClient v4.1 SP2 build 4165)
- Windows 2000 (SecureClient v4.1 SP2 build 4166)
- Windows XP (SecureClient 4.1 SP5 build 4199, SecureClient NG FP1)
- Mac OS 8.x and OS 9.x (VPN-1 Client for Macintosh and either FireWall-1 v4.1 SP3 or FireWall-1 NG) [CHK].
- Windows CE (SecureClient NG, March 14, 2002 build or later)

The only thing notably missing from the list of compatible client operating systems is Linux, but there aren't too many Linux laptops or home users as of yet. That may change in the future, so it will be interesting to see if the client will be ported to the different flavors of Unix. If Linux use is a must, a Windows emulator such as VMware can be used to function as Windows 9x or NT, allowing SecureClient to be run normally by mimicking the TCP/IP stack [WEL02][VMW].

A recent release of SecureClient NG allows it to work with Windows CE and PocketPC handhelds [SIN02]. This is a welcome development as it helps mitigate the rapidly growing wireless security hole. Any access into the network from public network locations should be secured with a personal firewall and use VPN technology to prevent unwanted listening. Since wireless communications are broadcasted and can travel through walls, floors, ceilings, and windows – it should be treated as if the general public were listening. Existing wireless 'security' methods such as WEP have well-known flaws, so this particular addition to SecureClient is a welcome one.

Adaptive data compression is used to shrink the data being sent down the VPN tunnel to reduce the amount of bandwidth required for the connection. Since compressed files, images, etc are already compressed; it does not attempt to further compress those in order to conserve processing requirements. Even with the data compression, Check Point recommends having large amounts of memory and a VPN-1 Accelerator card for large organizations that estimate having a high number of concurrent VPN connections. The specialized network card is able to offload much of the VPN-related burden from the CPU. Lots of memory will be required with or without the accelerator card as the device doesn't diminish the memory footprint in any way – just the CPU load. This is an important consideration if an already loaded FireWall-1 box will be used to handle a large number of new VPN connections.

## SECURITY FEATURES

SecureClient inserts itself into the TCP/IP stack (Network/Transport layers of the 7 layer OSI model) of whatever operating system it is installed on. This is a good approach as it allows SecureClient to analyze all of the authorized user traffic, compare it to the security policy (source, destination, service), and encrypt/deny/send it on its way as needed. Special consideration needs to be taken for users working remotely in a shared environment where the MAC address is particularly vulnerable. SecureClient does not protect the user against driver specific hacks targeted against a particular NIC, so cautious use and an in-depth defense may still need to be considered.

The personal firewall feature of SecureClient is configurable and stateful. It is not aware of application level requirements (OSI layer 7), but does benefit from Check Point's long experience with TCP/IP. SecureClient v4.1 has the following options available for directing the behavior of the personal firewall:

- Allow All
- Allow Outgoing and Encrypted
- Allow Outgoing Only
- Allow Encrypted Only

Of these, the second (outgoing + encrypted) makes the most sense as it allows VPN and standard user-initiated traffic to pass, but blocks any externally initiated connections. SecureClient NG (The newest version of SecureClient) is capable of having a completely granular setup where specific services can be allowed or blocked in any direction - depending on the user's requirements [SUL01].

SecureClient provides end-to-end encryption from the user's machine to the organization's firewall. This is an important distinction, as many VPN devices exist as separate devices – allowing the traffic to travel in the clear between the dedicated VPN device and the user's machine. Check Point's solution wraps the data from the TCP/IP stack all the way to the destination Firewall to prevent any clear text transmission of the data.

Configuring the appropriate Firewall-1 gateways can control access by SecureClient users back into the intranet. When a user (or group of users) successfully establishes a VPN connection with the FireWall-1 device, they do not have to be given free rein to all of the available resources. Instead, access can be restricted based on the nature of the user and the associated approved destinations by setting up corresponding firewall rules in the security policy. Any unauthorized attempts can be logged locally or sent to the management station as alerts [CHK01].

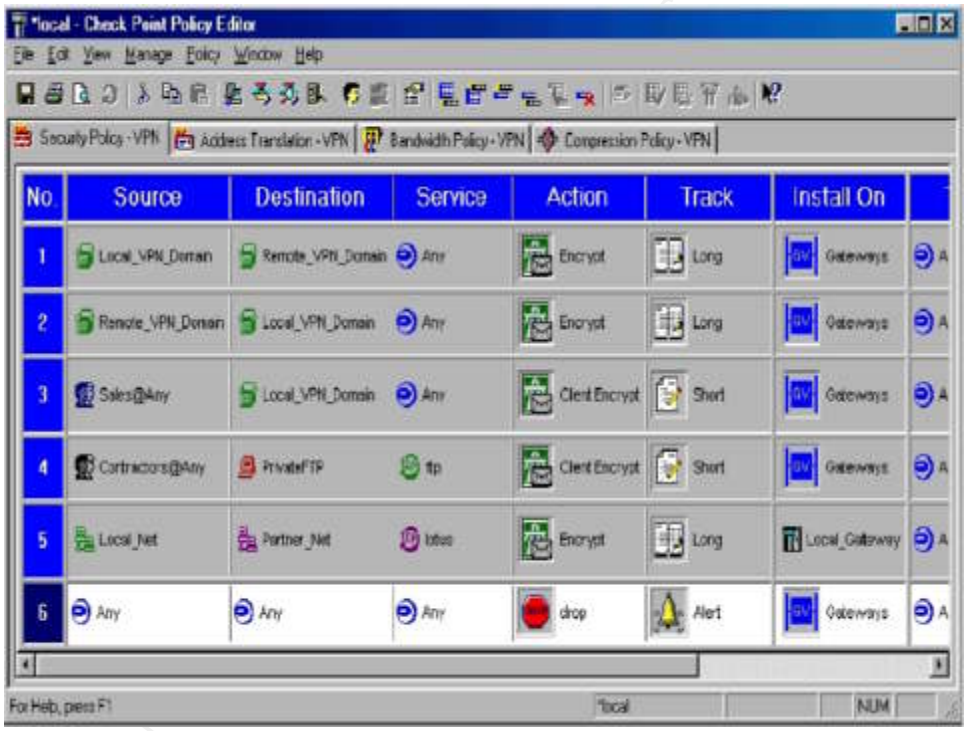


**Figure 3 – Sample Remote Policy** [CHK00]

Figure 3 above illustrates how access to internal network resources can be given only to the appropriate users if desired. Rule three specifies the source as 'Sales@Any', the Destination as 'Local_VPN_Domain', and the Service as 'Any'. This essentially allows anybody from the sales group to access any servers in the entire encryption domain (generally the entire local network) via any ports or protocols. Rule four is much more restrictive. It allows members of the 'Contractors@Any' group to access the resource(s) configured in the 'PrivateFTP' object via the FTP protocol only. Rule five allows Lotus Notes access from the local network to a partner network, and Rule six drops all packets not otherwise allowed.

## ENCRYPTION CAPABILITIES

Check Point's VPN solution is compliant with the ICSA 1.0a IPSec conformance criteria [CHK00]. This refers to the open standards developed and maintained by the IETF (Internet Engineering Task Force) that are intended to provide guidelines for secure connections over the public Internet. These guidelines have been reviewed favorably by the industry and are now in widespread use by connections (such as a VPN) that require authentication, confidentiality, and data integrity while traversing an insecure network. IPSec uses IP Type 50 (ESP) and IP Type 51 (AH) for the encapsulation and transmission of information. Of these protocols, ESP is by far the most frequently utilized since it provides the same message integrity functions as AH while simultaneously providing confidentiality through encryption.

SecureClient uses IKE (Internet Key Exchange – supported since Firewall-1 v4.0 build 4003), or FWZ to handle the IPSec requirement for authentication. IKE was created with RFC 2409 and is a hybrid of both ISAKMP and OAKLEY authentication and key exchange methods [H-C98]. IKE includes the two-phase process adopted from ISAKMP to accomplish this and uses UDP 500 for transmission. The process is designed to make sure that the computers involved in the security association (SA) successfully negotiate the encryption algorithm, hash algorithm, authentication method, and information about a group over which to do Diffie-Hellman key exchange [H-C98].

Both aggressive mode and main mode are supported for ISAKMP Phase one. Phase one consists of either a 3-way handshake (aggressive) or 6-way handshake (main mode) where the security association is negotiated. Aggressive mode is more limited in features and should not be used if greater attribute negotiation is required. IKE phase two negotiates the permanent settings and sets up the IPSec tunnel in a three-way handshake that occurs over the temporary encrypted tunnel set up in phase one [ALT02]. Once this occurs the VPN has been completely established and traffic in the defined SA will be sent using the agreed upon encryption algorithm.

FWZ, Check Point's proprietary authentication method, is available in both unencapsulated and encapsulated modes and uses UDP 259 for transmission. Unencapsulated FWZ encrypts only the data portion of the packet, leaving the IP headers alone. Encapsulated FWZ also encrypts only the data portion, but then wraps the packet in IP Type 94 before sending it out. Neither implementation of FWZ encrypts the entire packet or is capable of strong encryption, making this solution a poor solution when compared to IKE.

A variety of encryption algorithms are included in IPSec for encrypting traffic as it traverses the Internet (confidentiality). SecureClient supports the following for the VPN tunnel [CHK01]:

- Reijndael (Advanced Encryption Standard – AES) 128 to 256-bit (NG only)
- Triple DES 168-bit (FireWall-1 4.0 and later)
- DES 56-bit

- FWZ-1 48-bit (used primarily with FWZ authentication)
- DES-40 40-bit
- CAST-40 40-bit

From the list above, only Reijndael and Triple Des (3DES) can be recommended for implementation, as they are the only algorithms capable of providing a reasonable level of comfort in the current Internet environment. DES is still in widespread use, but must be cautioned against because of its relatively small key length.

The hash algorithms SHA-1 and MD5 handle data authentication for SecureClient and make sure that the data isn't tampered with in transit. These hash algorithms are essentially one-way functions that create a fixed-length unique fingerprint of the encapsulated payload and are attached to the end of the packet (the ESP trailer). This can then be used to make sure the payload is intact by comparing the fingerprint of the original data packet when it is received with the fingerprint attached at the end of the ESP packet. Since the result of a hash is unique, any variation found in the comparison would indicate that the payload was tampered with and should be discarded [SHA]. Of the two data authentication methods supported, SHA-1 is recommended because of a recently discovered theoretical vulnerability with MD5.

For encrypted user authentication, SecureClient and FireWall-1 support pre-shared secrets, digital certificates, and a hybrid authentication mode to give organizations a greater amount of flexibility in determining the method that works best for them. If FWZ is being used for VPN negotiation, only pre-shared secrets and digital certificates are supported – IKE is required for hybrid mode authentication.

Here are brief descriptions of the encryption capabilities:

> Pre-shared secrets - This is an IPSec standard method of authentication where the passwords are distributed to users by some means other than the VPN (over the phone, etc…). SecureClient is then configured to use the secret key during the VPN setup phase when the connection is initiated. This is a fast and simple way to set up a limited number of remote users, but becomes difficult to manage when the number of users grows too large. [CHK00]
>
> Digital certificates - Digital certificates are another IPSec standard method of authentication where the identity of a user is verified by a specific digital key (a unique string of characters of a given length). The key can be stored on the machine in a secure manner or as a token carried by the user that is connected to the computer when authentication is required. This method is stronger (two factor authentication instead of one factor authentication) and easier to scale than shared secrets, but can be more difficult to deploy. A Public Key Infrastructure (PKI) can automate management of the certificates in order to ease the burden of distributing the keys and keeping them valid and current. Check Point supports most standard PKI vendor solutions. [CHK00]

Hybrid Mode Authentication – Check Point also employs a hybrid mode of authentication that allows organizations to leverage their current system of authentication. This is quite appealing to many, as it would be quite costly to roll out a separate PKI authentication system for a large organization when they already have something in place. Hybrid mode authentication supports SecurID Cards, TACACS+, S/Key, RADIUS, LDAP, or the Firewall-1 Internal Password. [DIP00]

Use of pre-shared secrets, digital certificates, or hybrid-mode authentication may lead to UDP fragmentation in the IKE negotiation phase of IPSec. This can cause problems when authenticating depending on the NAT gateways used and size of the final UDP packets. To overcome this limitation the first phase of the SecureClient IKE negotiation can be configured to use IKE over TCP (TCP 500) instead of UDP 500 to ensure that the traffic arrives at the gateway intact. SecureClient Build 4185 and above and FireWall-1 4.1 SP4 and above support this configuration [WEL02].

## MANAGEMENT FEATURES

One of the most useful new features of SecureClient is the capability to have the security policy automatically updated (Through port TCP 264 by default). Once SecureClient is installed and the client machine rebooted, SecureClient will update the configuration (stored in the /checkpoint/database/userc.C file) on the machine to bring it in line with the current firewall policy on the internal policy server [CHK01]. This makes it very simple to roll out changes to the security policy and make adjustments to the encryption domain should that occur.

After the current policy is pushed down to the user's desktop, a feature called Secure Configuration Verification (SCV) can be used with SecureClient NG to make sure that the local copy of the userc.C file has not been changed in a way that would violate organizational security standards. If a change is detected, the local policy will be flagged as corrupted and the user will be prompted to download a new policy [FRA01]. SecureClient will not be allowed to run until the new policy has been downloaded and verified, ensuring that VPN connections are only initiated with approved hosts. This is an important consideration since the local policy file is stored as a standard text file, is unencrypted, and has read/write access available to the user. Without the verification step, it would easily be possible for the user or some third party to modify the settings to allow additional types of traffic. SCV can be set to run at regular intervals can also make sure that the anti-virus software is enabled before giving its approval for the client to connect [CHK01].

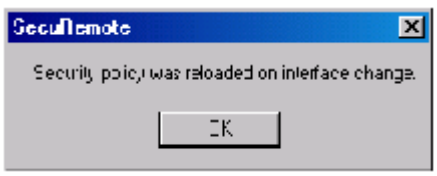


**Figure 4 – Binding Update Notification**

It is possible in Windows 9x/2000 to specify which interfaces (RAS/Dial-up, NIC, etc…) are to be protected by SecureClient by manipulating the bindings in the network settings. Windows NT does not provide a way to change interfaces in this manner, so all interfaces must be included. [W-A02] This allows SecureClient some flexibility when operating in multi-homed network configurations on non-Windows NT clients. If the organization wishes to specify that all interfaces must be protected in order for the VPN connection to take place, SCV can be configured to accommodate that. This is highly recommended unless one of the interfaces is connected to a secure local network segment only – otherwise you sacrifice the protection of the personal firewall. In the event of a network interface change while the machine is running, SecureClient will display the message shown in Figure 4 after automatically binding itself to the new connection. This is particularly useful to laptop users that may have to switch frequently between their home network and the client's network and use different PCMCIA NIC cards to do so.

SecureClient can also be configured for corporate host name resolution to help remote users access the internal resources in a more familiar manner. If the user tried to access an internal site by using DNS while working remotely and that site had the same name on the internal network as a different site on the public network – the public DNS would direct them to the external site with the registered version of the name. In order to get around this and facilitate access to the intended internal server, SecureClient can first perform a DNS lookup on the organization's private DNS servers to see if there is a match for the requested name [CHK00]. If the match is found, a connection to the server is initiated across the VPN and access continues as intended.

VPN-1 SecureClient differentiates between traffic bound for a resource found in the encryption domain and public Internet traffic. Only traffic bound for the organization's network is sent across the VPN, while other traffic is sent out normally (if allowed by the security policy). This process is known as split tunneling and is much more efficient than other solutions that send all traffic back to the gateway before differentiating the traffic by destination [CHK00].

## OTHER FUNCTIONALITY

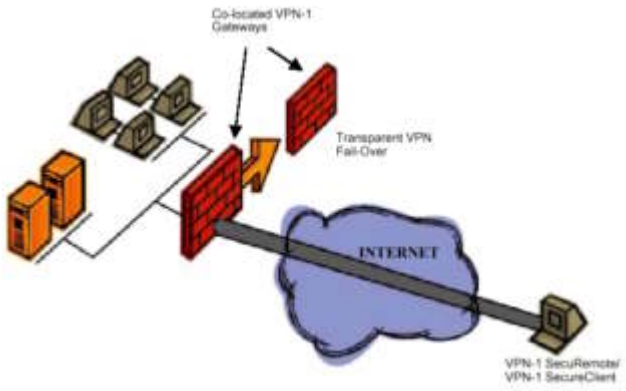


**Figure 5 – High-Availability through Gateway Clustering** [CHK00]

SecureClient and FireWall-1 4.1 SP1 or later provides support for high-availability (Figure 5). By defining a Gateway Cluster and configuring all of the encryption schemes and keys within that object (instead of on the individual FireWall-1 objects), SecureClient is able to access the network through any member of the cluster and be treated identically [W-A02]. This feature also allows seamless failover for remote connections should any member of the cluster go down. It is not a transparent transition, as any current connections are dropped, but the next object in the cluster will be able to pick up where the failed Firewall left off.

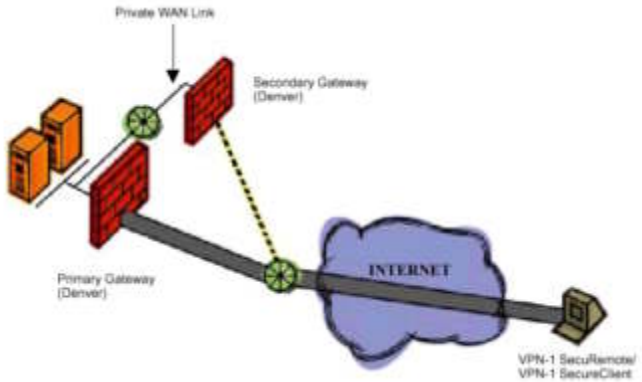


**Figure 6 – Resilient Remote Access** [CHK00]

Resilient remote access is another high-availability feature supported by SecureClient (Figure 6). "With resilient remote access, if a primary gateway in one location becomes unreachable, VPN-1 SecuRemote or VPN-1 SecureClient automatically redirects connections to a secondary gateway located elsewhere." [CHK00] This adds redundancy to the network without having to duplicate gateways and links at each location. The transition is not seamless, as the existing VPN connections are dropped and the users are required to authenticate on the new firewall, but this should not pose much of an issue when the advantages to the approach are considered.

SecureClient works in most external networking environments. The type of media and the interfaces to connect to that media are largely irrelevant – cable modem, DSL, dial-up, and many other connection types are supported. As long as UDP 500, and IP type 50 (ESP) are allowed, the VPN connection should be able to be established and the traffic will then be sent to the intranet through the tunneled connection. An issue does arise when both the user's remote network and the organization's FireWall-1 device use hide-NAT. Since ESP has no source or destination port information contained in the packets (IP type 6 and IP type 17 – TCP and UDP – do use port designations), Check Point is unable to use port mapping to remember the relationship between the internal host and encrypting (source) gateway [HAR01].

To overcome this limitation, IKE with UDP encapsulation must be used - requiring FW-1 4.1 SP2 build 4165 or later. The ESP packets used in the IPSec connection are wrapped again in UDP 2746 and sent to the decrypting firewall, which allows the port mapping process to work properly. The one catch to this process comes when both networks use the same internal addressing scheme. If both sides used 10.x

addresses for the private network, the firewall would be confused when attempting to send the return packets, as its routing tables would instruct to send the still unencrypted return packets back out the internal interface instead of encapsulating them and sending them back over the VPN. Check Point has developed a solution to this additional limitation with Office Mode in NG FP1 or above [WEL02].

The SC Packaging Tool is a Check Point Management client application that is included in the Management Clients package. This tool allows administrators the ability to preconfigure all of the site information and attributes into a package that can be installed (silently if desired) on the remote user's machine as a self-extracting executable. All of the necessary user files can be modified in this manner (userc.C, product.ini, and entrust.ini), and answers to any installation dialogs can be configured to be shown to the user. After the package is installed, the user will only have to reboot and update the site to download the current security policy (supplying any authentication credentials if applicable) in order to make SecureClient fully operational. [SUL01]

## SETUP AND INSTALLATION

Below is a high-level example of how SecureClient can be added to an existing FireWall-1 v4.1 or FireWall-1 NG infrastructure – intended to demonstrate how straightforward the procedure is. Those who are not running FireWall-1 but wish to use SecureClient will first have to purchase a firewall license from Check Point and see that it is set up properly before continuing.

Steps to configure SecureClient on FireWall-1 [W-A02]:

1. Choose an appropriate encryption scheme - Either FWZ or IKE can be used, but IKE with 3Des or AES is recommended.
2. Configure firewall workstation object for SecureClient - The firewall object must be configured with the appropriate encryption types and encryption domain. If you are using IKE, you need to edit the encryption scheme and define the appropriate type of authentication. If you are using FWZ you need to generate the Certificate Authority and Diffie-Hellman keys.
3. Create SecureClient users – The same user objects enabled for outbound access can be used to authenticate users for inbound access. On the user properties tab, define which encryption method to use, the encryption settings (3Des, SHA-1, etc…) and appropriate authentication settings.
4. Install the user database
5. Create Client Encryption rules – Three firewall rules are necessary to allow the VPN traffic to communicate properly through the firewall. The first should allow TCP 256 and TCP 264 (FW1 and FW1_topo services) to the management console. The second should allow IKE or RDP (for FWZ) packets and TCP 18207 (FW1_pslogon) to the firewall. This will allow the necessary access to the firewall and policy server. Finally, a third rule needs to be created to allow the SecureClient users to access the servers in the defined encryption domain with Client Encrypt defined as the action.

6. Configure Desktop Security options – Open the 'Rulebase Properties Desktop Security' tab and configure the appropriate settings. Note that checking the 'Apply Rule Only if Desktop Configuration Options are Verified' box will prevent previous SecuRemote users from connecting to the firewall.
7. Install security policy – Create a policy server on the firewall and specify which users will be associated. Go to the Desktop Security tab in the Properties Setup and set the options to match the requirements of the implementation

Steps to install SecureClient (for setups where the SC Packaging Tool is not used):

1. Download software - Obtain a copy of the appropriate software from the Check Point web page. (http://www.checkpoint.com/techsupport/downloads_sr.html)
2. Install SecureClient – Install SecureClient to the appropriate directory. Specify that you would like to 'Install Desktop Security support' on the Desktop Security Screen. Install on the appropriate adapters and restart the computer.
3. Configure SecureClient – Open the icon in the system tray and create a new site. Enter either the fully qualified domain name or IP address of the policy server.

If everything has been installed correctly, the user should see the SecureClient lock and key icon active in the system tray – as shown in Figure 7.


**Figure 7 – Taskbar Icon**

If the lock is green and flashing, then congratulations are in order as traffic is being successfully negotiated with the destination FireWall-1 device. All of the VPN functionality, including key negotiation and data encryption, is completely transparent to the user. When the user attempts to connect to a resource located on the internal network segment, VPN-1 SecureClient intercepts the connection and determines the gateway that should be properly associated with that resource. Once that happens, SecureClient is automatically initiated and the desired user authentication process is invoked. [CHK01]

## CONCLUSION

For network administrators who currently use Check Point's FireWall-1 solution for their firewall and want to extend VPN access to a large number of users – SecureClient is a clear choice. It protects those computers outside the corporate firewall while allowing them complete access to all necessary applications through industry standard VPN tunneling techniques. It also integrates seamlessly with the existing infrastructure, updates automatically, and has other features designed to add flexibility and usability to the product.

## APPENDIX

Here is a list of all the services allowed on SecureClient:

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

[SUL01]

**REFERENCES**


[ALA]
Aladdin products. URL:
http://www.eliashim.com/etoken/enterprise/datasheets/ds_checkpoint_securemote.asp

[ALT02]
Alterson, Gary. "Comparing BGP/MPLS and IPSec VPNs." January 9, 2002. URL:
http://rr.sans.org/encryption/MPLS2.php

[CHK]
Check Point products. URL: http://www.checkpoint.com/products/

[CHK00]
"Remote Access VPN Solutions." June 2000. Check Point Software Technologies Ltd.
URL: http://www.checkpoint.com/products/security/whitepapers/vpn-1_remote_access.pdf

[CHK01]
"VPN-1 Clients: Secure Virtual Network Architecture." 2001. Check Point Software Technologies Ltd. URL: http://www.checkpoint.com/products/downloads/vpn-1_clients_datasheet.pdf

[CLA02]
Clark, Daniel. "Vulnerability's of IPSEC: A Discussion of Possible Weaknesses in IPSEC Implementation and Protocols." March 14, 2002. URL:
http://rr.sans.org/encryption/weak_IPSEC.php

[COM]
Computers4SURE website. URL: http://www.computers4sure.com

[DEV99]
Devera, Richard. "How to Install and Configure SecureClient and SecureServer." October 19, 1999 Check Point Software Technologies Ltd. URL:
http://support.fishnetsecurity.com/public/cppublic/secureclient-secureserver.pdf

[DIP00]
DiPietro, Joe. “Hybrid Mode IKE for SecuRemote Authentication.” September 6, 2000. Check Point Software Technologies Ltd. URL: http://support.checkpoint.com/kb/docs/public/securemote/4_1/pdf/hybrid-2-10.pdf

[FRA01]
Fratto, Mike. “Check Point Next Generation: FireWall-1 Gets a Forklift.” Network Computing. July 23, 2001. URL: http://www.networkcomputing.com/1215/1215sp1.html

[HAR01]
Harcup, Andy. “Understanding Check Point FireWall-1 UDP Encapsulation & HIDE NAT.” March 26, 2001. URL: http://www.phoneboy.com/docs/UDP-Encapsulation.htm

[H-C98]
Harkins, D., Carrel, D. “The Internet Key Exchange (IKE).“ Network Working Group, RFC 2409. November 1998. URL: http://www.ietf.org/rfc/rfc2409.txt

[HIG01]
Higgins, Sean. “SecureClient.” August 19, 2001. URL: http://www.systura.com/Firewall1/configurations/secureclient.htm

[JON00]
Jones, Will. “SecuRemote/SecurID Implementation on Nokia VPN-1 Appliance.” July 19, 2000. URL: http://www.phoneboy.com/docs/securemote-securid.pdf

[SHA]
The Secure Hash Algorithm Directory - MD5, SHA-1 and HMAC Resources. Website URL: http://www.secure-hash-algorithm-md5-sha-1.co.uk/

[SIN02]
Singer, Michael. “VPN-1 SecureClient Now For Handhelds.” Internet.com. March 14, 2002. URL: http://siliconvalley.internet.com/news/article/0,2198,3531_991751,00.html

[SUL01]
Sultan, Cyril. “VPN-1 SecuRemote/SecureClient Next Generation.” May 9, 2001. Check Point Software Technologies Ltd. URL: http://www.swanholm.com/software/download/SecuRemote_Client_NG_FAQ.pdf

[VMW]
Vmware website. URL: http://www.vmware.com/

[W-A02]
Welch-Abernathy, Dameon D. Essential Check Point FireWall-1: An Installation, Configuration, and Troubleshooting Guide. Addison-Wesley. 2002.

[WEL02]
Welch, Dameon D. "Phoneboy's Firewall-1 FAQ's." 2002. URL: http://www.phoneboy.com/

[ZON]
ZoneLabs Website. URL: http://www.zonelabs.com/products/za/index.html

Last Updated: May 27th, 2017

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Madrid 2017 | Madrid, ES | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Atlanta 2017 | Atlanta, GAUS | May 30, 2017 - Jun 04, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CAUS | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DCUS | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TXUS | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Milan 2017 | Milan, IT | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SEC555: SIEM-Tactical Analytics | San Diego, CAUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NCUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Secure Europe 2017 | Amsterdam, NL | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, COUS | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MNUS | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| DFIR Summit & Training 2017 | Austin, TXUS | Jun 22, 2017 - Jun 29, 2017 | Live Event |
| SANS Paris 2017 | Paris, FR | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, AU | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MDUS | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SEC564:Red Team Ops | San Diego, CAUS | Jun 29, 2017 - Jun 30, 2017 | Live Event |
| SANS London July 2017 | London, GB | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, JP | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, SG | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CAUS | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS ICS & Energy-Houston 2017 | Houston, TXUS | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, DE | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANSFIRE 2017 | Washington, DCUS | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Security Awareness Summit  & Training 2017 | Nashville, TNUS | Jul 31, 2017 - Aug 09, 2017 | Live Event |
| SANS San Antonio 2017 | San Antonio, TXUS | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, CZ | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Boston 2017 | Boston, MAUS | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Hyderabad 2017 | Hyderabad, IN | Aug 07, 2017 - Aug 12, 2017 | Live Event |
| SANS Salt Lake City 2017 | Salt Lake City, UTUS | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS New York City 2017 | New York City, NYUS | Aug 14, 2017 - Aug 19, 2017 | Live Event |
| SANS Chicago 2017 | Chicago, ILUS | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Adelaide 2017 | Adelaide, AU | Aug 21, 2017 - Aug 26, 2017 | Live Event |
| SANS Stockholm 2017 | OnlineSE | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |