



We Secure the Internet.



# VPN-1 Clients

## PRODUCT FEATURES:

- Securely connects mobile users to VPN-1 Pro gateways
- Supports industry-standard VPN protocols
- Provides centrally-managed personal firewall
- Automates software distribution and maintenance

## PRODUCT BENEFITS:

- Enables local and remote users to securely access resources on the corporate network
- Allows organizations to implement authentication solutions that best meet their needs
- Protects client systems from attack
- Minimizes help desk support costs

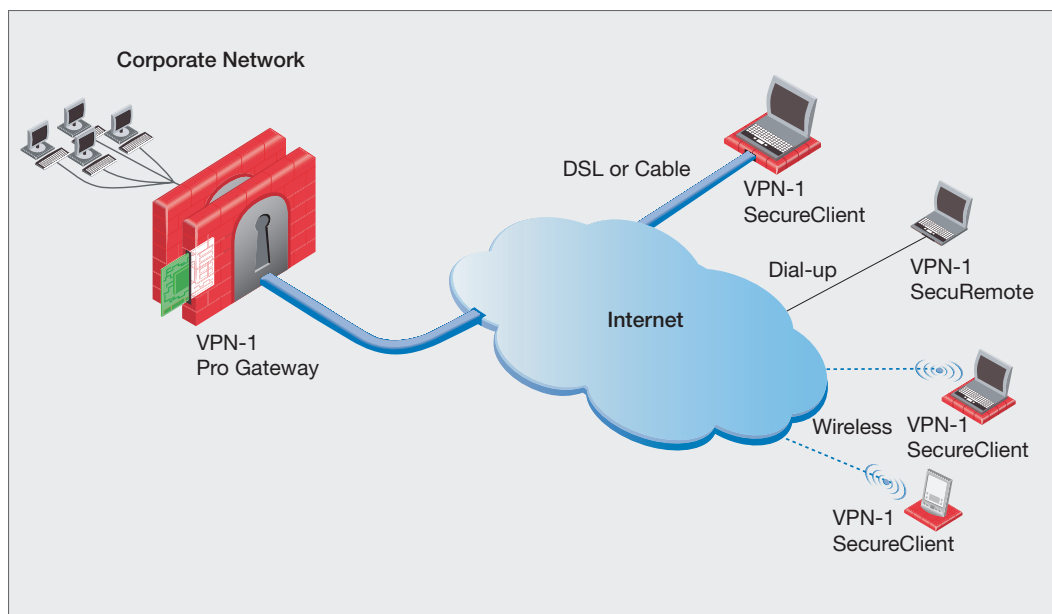
## YOUR CHALLENGE

The wide adoption and deployment of remote access VPN technologies has been in large part due to the tremendous cost advantages they promise. Yet, as organizations continue to deploy remote access VPNs, network security managers face a number of challenges in trying to connect, protect and manage increasingly large numbers of client systems. First, remote access VPN clients need to deliver connectivity from any network, including dial-up, broadband and wireless, without any additional administrative overhead. Second, the client must be able to protect remote user machines against attacks as remote users try connecting to the corporate network over the unprotected Internet. Finally, to truly deliver on the promise of cost-savings VPN client software must deliver simple, and transparent administrative processes for deployment and maintenance.

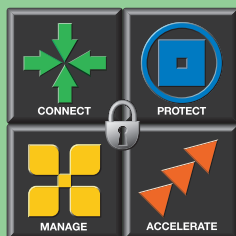
## OUR SOLUTION

VPN-1® SecuRemote™ provides flexible VPN support for both remote and local users. Using VPN-1 SecuRemote, remote users gain secure access to critical corporate resources. The VPN client transparently encrypts and authenticates critical data to protect against eavesdropping and malicious data tampering.

VPN-1 SecureClient™ adds powerful client security and management features to the basic VPN-1 SecuRemote functionality. VPN-1 SecureClient includes a centrally-managed personal firewall to prevent unauthorized access to client systems, thus strengthening the security of the entire enterprise by ensuring that intruders cannot hijack an existing VPN connection.



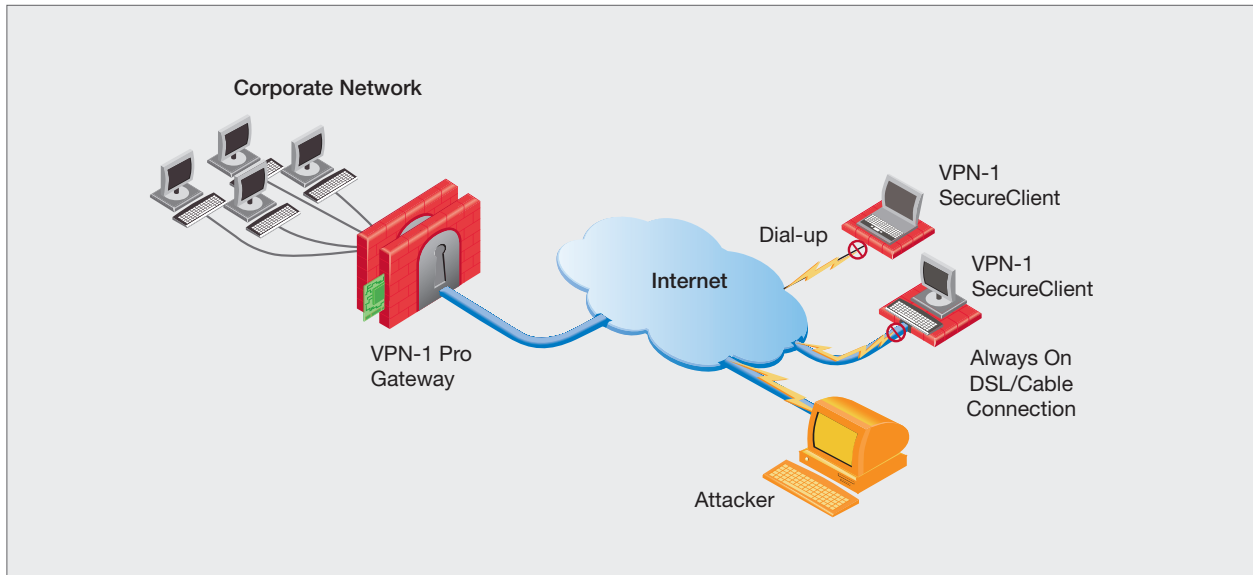
VPN-1 SecuRemote and VPN-1 SecureClient enable state-of-the-art remote access VPNs.



## VPN-1 SECURECLIENT AND VPN-1 SECUREREMOTE Enterprise Security Integration for Centralized Control

VPN-1 SecureClient and VPN-1 SecuRemote work seamlessly with Check Point's market-leading VPN-1 solutions. It is easy to incorporate secure remote access as part of an overall security policy. And because VPN-1 clients establish VPN tunnels directly with VPN-1 Pro™,

remote user to install two separate pieces of software and authenticate twice. VPN-1 SecureClient and VPN-1 SecuRemote maintain detailed information on all VPN sites for a seamless user experience. All VPN functionality, including key negotiation and data encryption, is completely transparent to the user. Both VPN-1 SecureClient and VPN-1 SecuRemote offer a choice of usage modes:



*VPN-1 SecureClient protects end-users' systems against attacks and misuse.*

all elements of an enterprise security policy are strictly enforced, including access control, user authentication and logging.

### One-Click VPNs for Easy Deployment

Check Point's One-Click technology simplifies VPN setup and management into a single step, making it easy to deploy remote access VPNs. Remote access VPNs can be created with a single operation by simply placing all participating VPN-1 SecureClient and VPN-1 SecuRemote users into a "VPN Community." A VPN Community enables organizations to define the security parameters for an entire group of remote access users. As new members are added to the Community, they automatically inherit the appropriate properties and can immediately establish secure remote access connections to the corporate VPN gateway.

### Multiple Modes of Deployment for Greater Flexibility

VPN-1 clients support dynamic and fixed IP addressing for all Internet Service Provider (ISP) services — dial-up, cable modem or Digital Subscriber Lines (DSL) — making them the ideal solution for telecommuters and mobile workers. Additionally, both clients can come bundled with an ISP's dialer, which eliminates the need for a

### • Transparent Mode

Each time a user attempts to connect to the corporate network, VPN-1 SecureClient and VPN-1 SecuRemote capture the request and automatically challenge the user for proper authentication. Once authenticated, the VPN connection is established and all corporate communications are protected.

### • Connect Mode

With Connect Mode, users manually establish and disconnect VPN sessions. This feature is designed for users familiar with the "dial-up" model for Internet connectivity. For increased flexibility, the OfficeMode feature in VPN-1 SecureClient enables users to receive an IP address, as well as DNS and WINS information, from the VPN-1 gateway, making them appear as if they were "in the office" when connecting remotely.

### Universal Connectivity

VPN-1 SecureClient and VPN-1 SecuRemote enable users to connect to the corporate network from anywhere, even if a firewall or NAT device resides between the VPN user and the corporate VPN gateway.

### Flexible Authentication to Suit Customer Needs

In addition to pre-shared secrets and X.509 digital certificates natively supported by the IPSec standard, Check Point's unique Hybrid Mode Authentication enables organizations to implement other user authentication technologies. These include SecurID tokens, RADIUS-based solutions, and more.

Organizations that want to implement strong authentication "out of the box" can use Check Point One-Click Certificates. With the Internal Certificate Authority included with VPN-1 solutions, X.509 digital certificates can be issued to both VPN-1 SecureClient users and VPN-1 gateways. One-Click Certificates provide industry-standard, two-factor authentication for users without requiring the rollout of complex and expensive PKI systems.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	COMMENT
1	All Users@Any	Any	Any	Accept	None	Src	Allow all outbound traffic
2	Any	All Users@Any	Any	Encrypt	Alert	Dst	Incoming traffic must be encrypted

VPN-1 SecureClient enforces centrally managed personal firewall policies.

### High Availability for Remote Access

Check Point's VPN Load Distribution feature is a high availability and load sharing solution for remote access VPN connections. Inbound VPN connections can be distributed across a cluster of VPN-1 gateways. If one gateway fails, new VPN connections will automatically connect to remaining cluster members.

### ADVANCED VPN-1 SECURECLIENT FEATURES

VPN-1 SecureClient is an enhanced application providing all of the capabilities of VPN-1 SecuRemote plus additional features for client security and software management.

### Personal Firewall Capabilities

VPN-1 SecureClient provides sophisticated security for remote access users. Using the same patented Stateful Inspection technology in market-leading FireWall-1®, VPN-1 SecureClient firewall policies provide access control based on the source, destination and type of network traffic received by or sent from the client system. Security rules may be defined for users or groups of users, enabling organizations with different types of remote access VPN users — such as salespeople and IT staff — to tailor client security policies to their users' varying needs. These policies not only protect the data on client machines from unauthorized access, but also eliminate these users' vulnerability to attacks from fellow users on shared networks. Unauthorized access attempts can either be logged locally or sent as alerts to the management station.

### Secure Configuration Verification

VPN-1 SecureClient strengthens enterprise security by ensuring client machines cannot be configured in a way that circumvents the enterprise security policy. Using Secure Configuration Verification (SCV), managers can

specify SCV checks — a set of conditions that define a securely configured client system, such as the proper operation of the personal firewall policy. These security checks are performed regularly to ensure that only securely configured systems are connected to the corporate VPN.

In addition to the checks that have been pre-defined, security administrators can define custom checks. For example, an SCV check can be written to ensure that VPN-1 SecureClient users are running the most current version of anti-virus software.

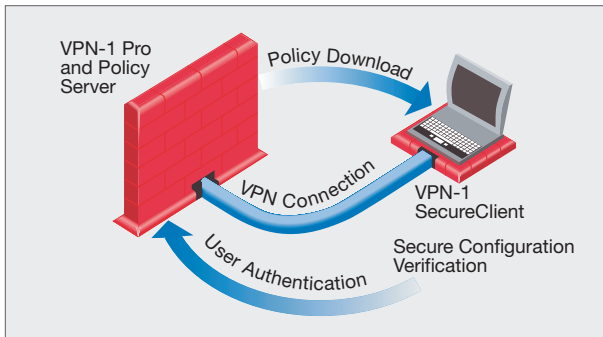
Check	Description
Process Monitor	Checks whether or not process is running
Group Monitor	Checks whether a user belongs to a specific group (domain or local machine)
OS Monitor	Verifies the operating system version, service pack and screen saver configuration
HotFix Monitor	Checks that operating system security patches are installed
Browser Monitor	Verifies Web browser version
Version Checker	Verifies VPN-1 SecureClient version

Predefined SCV checks.

### Streamlined Software Distribution and Management

VPN-1 SecureClient includes features to streamline the initial distribution and ongoing maintenance of client software. These features dramatically decrease end-user support costs associated with the VPN, and improve overall security by ensuring that client software installations are always consistent and current. With the VPN-1 SecureClient Packaging Tool, security administrators can create customized, self-extracting installation packages for their VPN-1 SecureClient users.

All VPN-1 SecureClient options may be pre-configured, eliminating the need for the end-user to configure any settings. Once the user has obtained the software package (either by Web download, email or physical media distribution), he or she simply runs the executable file and reboots. After the initial installation, VPN-1 SecureClient automatically downloads the updated security policy from the VPN-1 SecureClient Policy Server, which resides on the VPN-1 Pro gateway. Policy updates are made transparently on the client machine. All components, including the security policy, are regularly checked and automatically updated if not current.



VPN-1 SecureClient ensures that users can only connect if their systems are secure.

### Security for Mobile Devices

Organizations deploying mobile devices for convenient corporate access require security to protect corporate data residing on these devices and prevent them from becoming a backdoor into the larger corporate network. "Secured by Check Point" mobile devices are certified to interoperate with VPN-1 SecureClient and VPN-1 SecuRemote, providing integrated VPN and personal firewall functionality with centralized management.

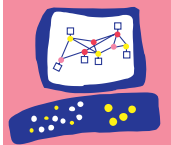
### Diagnostic Tools

To aid administrators in troubleshooting client connection and security issues, VPN-1 SecureClient includes a client log viewer, desktop policy viewer and connection status viewer. These tools provide valuable information about the current state of remote access client systems and connections, as well as any unauthorized access attempts.

## SYSTEM REQUIREMENTS

<b>OPERATING SYSTEM</b>	Windows 2000 Windows 98 Windows CE/PocketPC 2002 Windows ME Windows NT 4.0 Windows XP
<b>DISK SPACE</b>	20 MB
<b>MEMORY</b>	64 MB
<b>NETWORK ADAPTERS</b>	No known restriction
<b>MEDIA</b>	CD-ROM and Web download

**Check Point**  
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

© 2003 Check Point Software Technologies Ltd. All rights reserved.

Check Point, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 SmallOffice, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, IQ Engine, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenterPro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SVN, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Net, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 SmallOffice, and VPN-1 VSX are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

P/N 500559