

VPN-1 SECURECLIENT

Secure Virtual Network Architecture

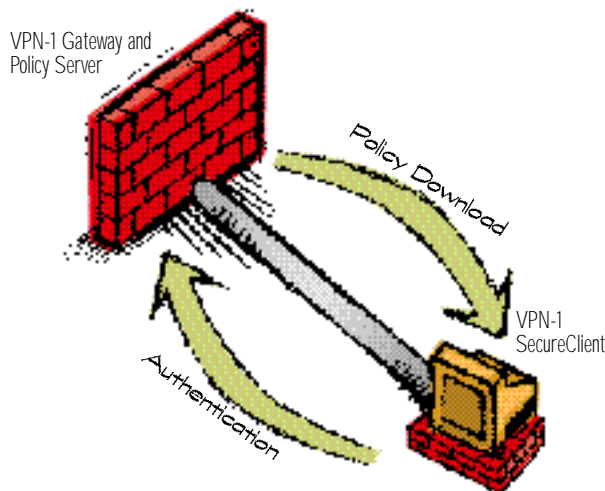
The Challenge:

The rapid adoption of VPN technology has created a new extended enterprise in which more internal corporate network resources are being made externally accessible. Increasing numbers of Remote Access VPN clients connect to corporate networks using Internet access technologies such as cable modems and Digital Subscriber Lines (DSL). The lack of security in these broadband environments, as well as "always on" Internet connectivity, leaves individual machines open to intrusion, thereby putting at risk both the client and the network to which it is connected.

While most network security managers concentrate on protecting their networks against external attacks, recent studies confirm that the majority of threats originate inside an organization. Therefore security measures such as access control, encryption, and user authentication must also be deployed internally. Data on desktop machines must be protected against unsanctioned access. Sensitive client-server communications must be protected against eavesdropping by unauthorized users. And every client system, whether local or remote, opens up a potential door into the corporate network if configured in an insecure manner.

The Solution:

VPN-1 SecureClient extends Check Point Software Technologies' market-leading network security solutions by enforcing security on client machines. While VPN-1 SecuRemote™ provides standard VPN connectivity with client-side encryption and user authentication, VPN-1 SecureClient adds powerful client security features such as access control and security configuration control. VPN-1 SecureClient strengthens the security of the entire corporate network by ensuring that intruders—such as users on shared outside networks—cannot take advantage of an insecure remote client machine to hijack an existing VPN connection into the corporate network. VPN-1 SecureClient also provides the ability to automatically verify that users' machines across the extended enterprise are configured securely.



Policy-based security for clients

Once a VPN user successfully authenticates, the enterprise desktop security policy is downloaded onto the client machine.

DATA SHEET

Product Features

- Encrypts communications from remote and local clients
- Provides personal firewall policies for PCs within enterprise networks
- Enforces secure configurations on client systems

Product Benefits

- Protects client-gateway and client-server communications against eavesdropping and data tampering
- Safeguards the entire network by enforcing access controls on all clients
- Strengthens overall enterprise security by requiring that network clients be configured securely

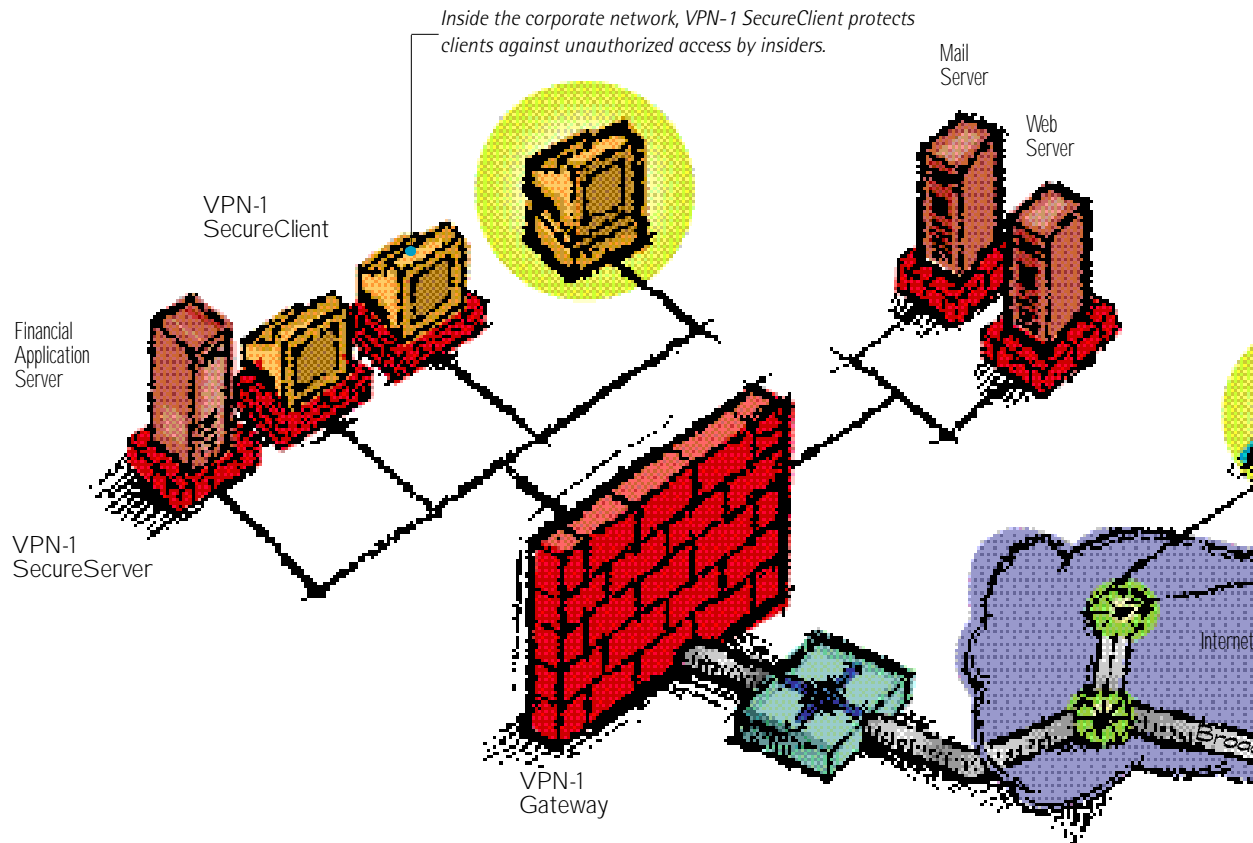


Flexible Deployment

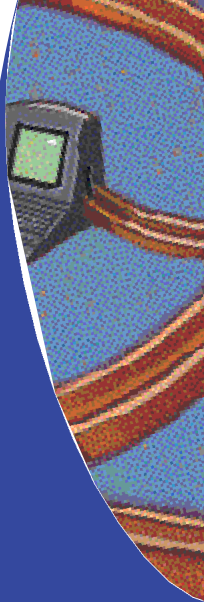
VPN-1 SecureClient provides secure connectivity for both Remote Access and Intranet VPN clients. The VPN-1 SecureClient software installs on any Windows 9x/NT PC and supports all IP-based network communications. For telecommuters and mobile workers using either dial-up or broadband Internet connections, VPN-1 SecureClient supports both dynamic and fixed IP addressing. When installed internally, VPN-1 SecureClient protects critical business communications between desktop clients and either VPN-1 SecureServer or VPN-1 Gateway.

Personal Firewall Capabilities

VPN-1 SecureClient protects local and remote client systems using the same patented Stateful Inspection technology in the market-leading FireWall-1® and VPN-1 solutions. Pre-defined policies are provided which specify allowable traffic and encryption policies for all network clients. For example, a policy can specify that all traffic to and from clients must be encrypted. Deploying policy-based security to clients not only protects the data on client machines from unauthorized access, but in the case of remote access VPN users, eliminates those machines' vulnerability to attacks from neighboring users on shared networks.

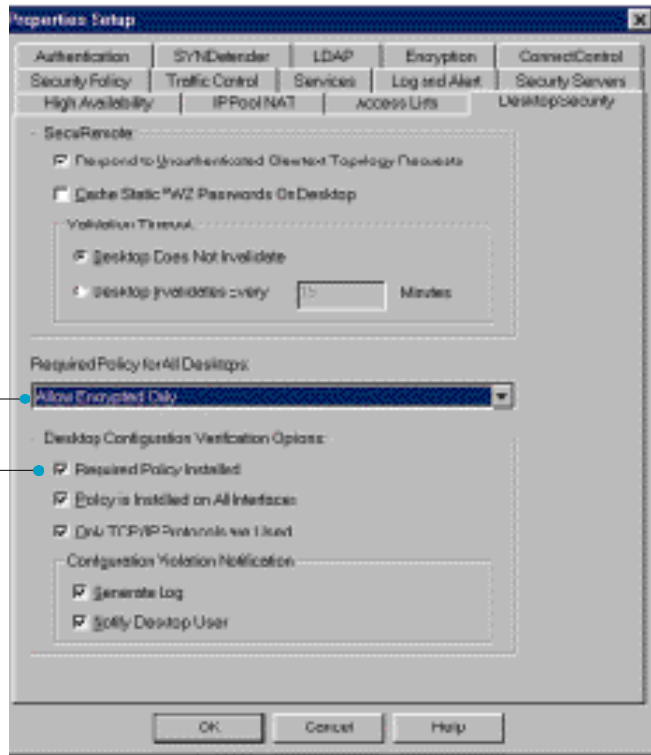


VPN-1 SecureClient can be deployed to secure either LAN clients or Remote Access VPN users.

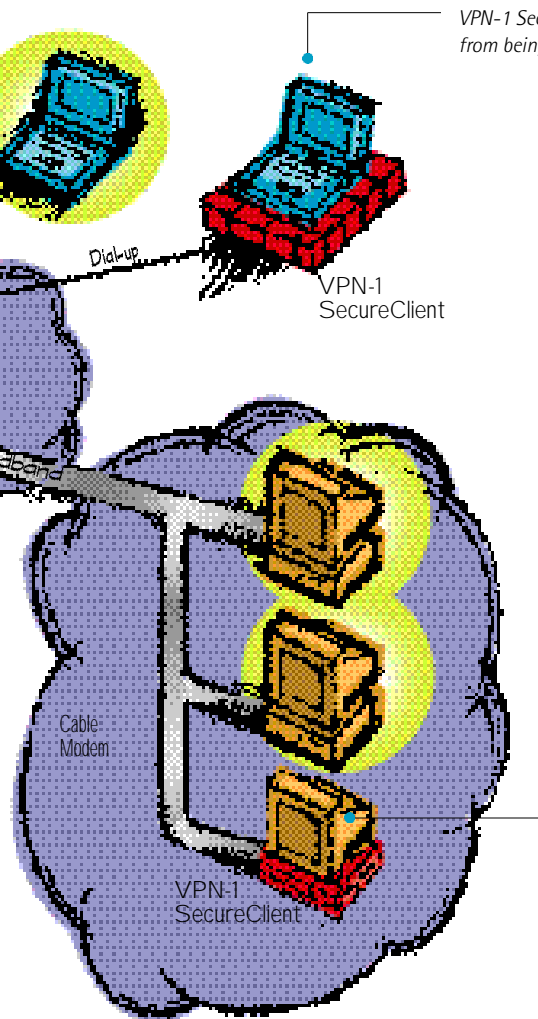


The Desktop Security Policy specifies that all traffic to and from client machines must be encrypted.

Both remote and local client machines must meet the selected security configuration requirements.



VPN-1 SecureClient settings are defined as "Desktop Security" properties of the enterprise security policy



VPN-1 SecureClient protects remote access VPN connections from being "hijacked" by neighboring Internet users.

Security Configuration Control

VPN-1 SecureClient strengthens enterprise security by ensuring client machines cannot be configured in a way that circumvents the enterprise security policy. Users can be denied network access unless their machines are currently operating with an approved configuration. For example, managers can specify that a properly configured machine has no non-IP protocols in use, has IP forwarding turned off, and is running the correct security policy. Only once the configuration of the client has been verified may that client establish a VPN connection to a corporate gateway or server.

Policy-based Architecture

VPN-1 SecureClient uses a centralized Policy Server to protect network clients. First, the VPN-1 administrator defines the level of client security to be deployed across the enterprise. This management decision consists of two components: the Security Policy to be installed on client machines, and the required Security Configuration settings to be enforced. Users must successfully authenticate themselves in order to download the enterprise-wide security policy from the Policy Server. Their machines must then meet the specified security configuration requirements in order to establish VPN connections.

Support for Industry Standard Protocols

VPN-1 SecureClient supports industry standard VPN protocols and algorithms for complete compatibility with VPN-1 security policies.

Encryption Algorithm	Key Length
Triple DES*	168-bit
DES	56-bit
FWZ-1	48-bit
DES-40*	40-bit
CAST-40*	40-bit

User Authentication
X.509 Digital Certificates*
IKE Pre-shared secret*
RADIUS
TACACS/TACACS+
Token-based (two factor)
Operating System Password
FireWall-1 Password
S/Key

Public Key Algorithms	Key Length
RSA	512-1024* bit
Diffie-Hellman	512-1024* bit

Key Management
IKE (ISAKMP/Oakley)
FWZ

* Supported for IKE



VPN-1 SecureClient can inform the end user when the client machine does not meet the enterprise security requirements.

Enterprise Security Integration

VPN-1 SecureClient works seamlessly with Check Point's market-leading VPN-1 enterprise security suite. Client security policies and security configuration controls are specified within the centralized Check Point VPN-1 Management Console. And because VPN-1 SecureClient establishes VPN tunnels directly with either VPN-1 Gateway or VPN-1 SecureServer, all elements of an enterprise security policy are strictly enforced, including access control, user authentication, and logging.

Specifications

Operating Systems	Windows 95 Windows 98 Windows NT 4.0 (SP3 or SP4)
Disk Space	6 MB
Memory	32 MB
Network Adapters	No known restriction
Media	CD-ROM and Web download

Secure Virtual Network Architecture

All Check Point Software products are built on our Secure Virtual Network (SVN) Architecture to provide secure and seamless connectivity of users, networks, systems, and applications across Internet, intranet, and extranet environments. Check Point Software's SVN solutions are available from industry-leading resellers and service providers worldwide.

For more information, please go to: www.checkpoint.com