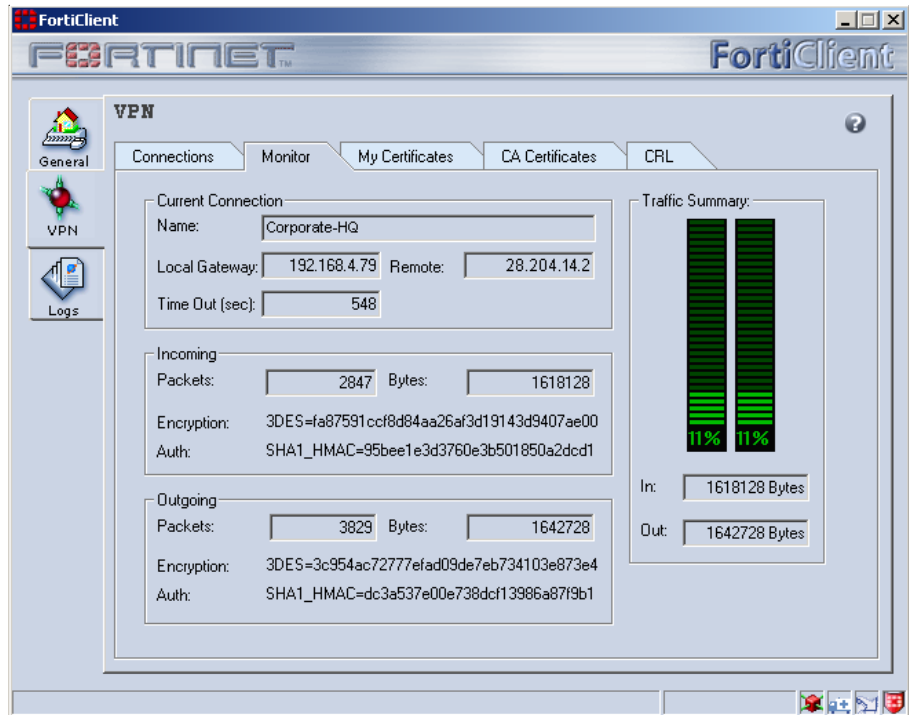


FortiClient™

Securing Remote Access for the Mobile Workforce

Fortinet's FortiClient Host Security enables your mobile employees, teleworkers, and business partners to easily and securely access networks protected by FortiGate Antivirus Firewall systems. FortiClient Host Security provides support for a wide range of applications, including remote access to corporate networks, remote system administration, file transfer, access to corporate email and to web-based intranet and extranets, all with a single, easy to use interface.



Designed to secure the network communications of a single user Windows workstation, the FortiClient Host Security protects IP-based communications using powerful, industry standard IP Security (IPSec) encryption and authentication and automatic Internet Key Exchange (IKE) key management technologies.

FortiClient Host Security is compatible with any kind of network connection, including dial-up, xDSL, and cable modem, in addition to wired and wireless LANs, and is available for Microsoft® Windows™ NT4 (Service Pack 6), 2000 and XP operating systems. The FortiClient Host Security provides industry standard encryption algorithms, such as DES, 3DES, and AES, to ensure data privacy as it traverses the public Internet. The multiple remote networks feature allows the FortiClient Host Security to connect to multiple independent networks behind a FortiGate Antivirus Firewall. Network Address Translation-Traversal (NAT-T) technology provides easy integration with existing firewall and network address translation systems.

Product Highlights

- User-friendly graphical user interface for configuration and management
- Complete interoperable implementation of IPSec and IKE protocols
- Ability to retrieve a virtual IP address from the internal network through DHCP over IPSec
- Viewable logs and built-in test tools assist in troubleshooting IPSec connections
- Xauth provides additional level of authentication for enhanced security when users request an IPSec connection
- Supports X.509 digital certificates for authentication



Key Features & Benefits

Feature	Description	Benefit
Remote Access	FortiClient allows remote users to connect securely to a network protected by FortiGate Antivirus Firewalls	Enhance productivity through anytime, anywhere access for mobile and remote workers and telecommuters
NAT Traversal	Enables IPSec connections to traverse through networks implementing Network Address Translation (NAT)	Allows remote users to create VPN tunnels through networks using private addresses
Ease of Use	Easy to configure implementation of IPSec and Internet Key Exchange (IKE) protocols	Easy installation and configuration assists in deployment
Diagnostic Tools	Comprehensive tools provide viewable logs and IPSec tunnel diagnostic test	Diagnostic test ensures remote policy settings are correct and provides viewable logs for auditing

Specifications

FortiClient Host Security

Functionality

Remote VPN Client •

VPN

- AutoKey IKE (Preshared) •
- AuthKey IKE certificate •
- ESP and AH •
- L2TP protocol support •
- NAT traversal •
- Main and aggressive mode IKE •
- Redundant gateway support •
- DHCP over IPSec •
- Manual virtual IP •
- Multiple remote networks •
- Dead peer detection •
- Simplified configuration process •

Encryption

- 3DES and DES •
- SHA-1 and MD5 •
- AES (128, 192, 256-bit) •

PKI

- PKCS #7 certificate chains •
- PKCS #10 certificate requests •
- PKCS #12 certificate import •
- X.509 certificate authority •
- Online Enrollment •

User Authentication

- Extended authentication (XAUTH) •
- RADIUS Future Enhancement
- LDAP Future Enhancement

FortiClient Host Security

Security Features

- Split tunneling •
- Personal firewall Future Enhancement
- Desktop antivirus client Future Enhancement
- Application control Future Enhancement
- Net Bios protection Future Enhancement
- Driver-level protection Future Enhancement
- AutoBlock Future Enhancement

Management, Logging, and Monitoring

- Searchable VPN logs •
- Central VPN policy management Future Enhancement
- VPN tunnel diagnostics test •
- VPN connection monitor •
- Packet logs •
- Email alerts and logs •

System Requirements

- PC-compatible computer with Pentium processor or equivalent
- Operating Systems and minimum RAM:
 - Microsoft Windows NT 4.0 (SP6) - 32MB
 - Microsoft Windows 2000 - 64MB
 - Microsoft Windows XP - 128MB
 - Microsoft Windows Server 2003 - 128MB
- 20MB of free hard disk space
- Native Microsoft TCP/IP communications protocol
- Native Microsoft PPP dialer for dial-up connections
- Ethernet for network connections
- Microsoft Internet Explorer 5.0 or later