The F-Secure logo, featuring the text "F-SECURE" in a bold, sans-serif font above a stylized shield icon. The shield is composed of three overlapping shapes: a dark blue triangle on the left, a white triangle on the right, and a dark blue triangle at the bottom, all pointing towards the center. The logo is set against a background of a globe with a grid of latitude and longitude lines, and a blue and orange color scheme.

Protecting Wireless LANs

F-Secure Corporation

Securing the Mobile Distributed Enterprise

WHITE PAPER
APRIL 2000

Protecting Wireless LANs

White Paper April 2000

All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure™ Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

The purpose of this document is to help you identify the strengths of the integrated security solutions the F-Secure product line provides. It is not a comparative review of competitor's products but it may provide valuable information that will assist you see what makes our offering different from all the others.

<p>USA</p> <p>F-Secure Inc. 675 N. First Street, 5th floor San Jose, CA 95112, USA Tel (408) 938 6700 Fax (408) 938 6701 http://www.F-Secure.com/</p>	<p>Europe</p> <p>F-Secure Corporation PL 24 FIN-02231 Espoo, Finland Tel +358 9 859 900 Fax +358 9 8599 0599 http://www.F-Secure.com/</p>
---	--

Copyright © 1995-2000 F-Secure Corporation. All rights reserved.

Contents

1. Wireless LANs.....	1
1.1 Transparency	1
1.2 Performance.....	1
2. Remote Installation.....	1
3. Configuration.....	2
4. Capacity.....	3
5. Specifications.....	3

1. Wireless LANs

Wireless LANs are becoming more popular in corporate networks where the mobility of laptops and ad-hoc network connections are needed. Without adequate protection, wireless LAN traffic can sneak out of the room, out of the office, and out of the building, and reach the ears of eavesdroppers. Weak encryption using 40-bit keys is an added option for wireless LAN protocols. Even if the option is implemented, your wireless LAN traffic is still not safe, because this weak encryption is easily cracked. Only strong encryption can securely protect your data traveling over a wireless LAN. With today's technology, it would take several hundred years to decrypt any data protected with strong encryption. So you don't even have to worry about the most sophisticated eavesdroppers. F-Secure VPN+ is the fourth-generation Virtual Private Network software from F-Secure, the technology leader for secure networking. F-Secure VPN+ secures mission-critical networking between remote offices, business partners, telecommuters and traveling employees. This centrally managed security solution offers the following configurations to fulfill all of your networking needs. F-Secure VPN+ is an IPSec-compliant solution that protects every link in the corporate network chain — clients, servers, and gateways. Because of this, F-Secure VPN+ is ideal for corporate LANs that implement wireless LAN technology.

1.1 Transparency

F-Secure VPN+ is totally transparent to end users and applications. This transparency is achieved with a specific interceptor layer between a workstation's TCP/IP stack and the network interface. The interceptor intercepts all traffic from the client applications, encrypts the data, and passes it on to the network. Incoming packets from the network are filtered and decrypted by the interceptor, and passed on to client applications. All this is done automatically and transparently. The network administrator can change connection parameters on the fly, which will not be detected by the client application.

1.2 Performance

F-Secure VPN+ is a fast software-based IPSec implementation. F-Secure VPN+ Gateway, installed on a single 333 MHz Pentium II machine, can encrypt data at a speed as high as 24 Mbits/s with strong encryption (128-bit Blowfish). The speed of encryption is almost linear with the machine's CPU speed.

2. Remote Installation

F-Secure VPN+ can be installed remotely on workstations without any action from the users. With F-Secure Intelligent Installation, the network administrator can import hosts from an NT domain into the VPN management tool, F-Secure Administrator, and

remotely install F-Secure VPN+ Client software remotely on the hosts. Users do not need to worry about any software settings or installation.

3. Configuration

There are two approaches for configuring F-Secure VPN+ on a wireless LAN. Both approaches aim to encrypt all traffic passing over the airwaves. The first approach would be to install F-Secure VPN+ Client software on laptops using the wireless LAN, and to install F-Secure VPN+ Enterprise Gateway on a workstation in the wired LAN. The Enterprise Gateway is used to encrypt and decrypt packets to and from the F-Secure VPN+ clients and to route packets to the wired and wireless LAN. Figure 1 illustrates this configuration.

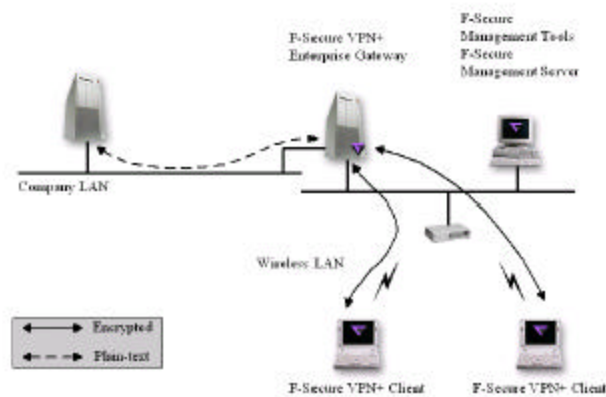


Figure 1. Encrypting Traffic over Wireless LANs

The second approach would be to install F-Secure VPN+ Server software on a wired LAN application or on file servers. This method encrypts all data, whether the data travels over a wireless or a wired LAN. Figure 2 illustrates this configuration.

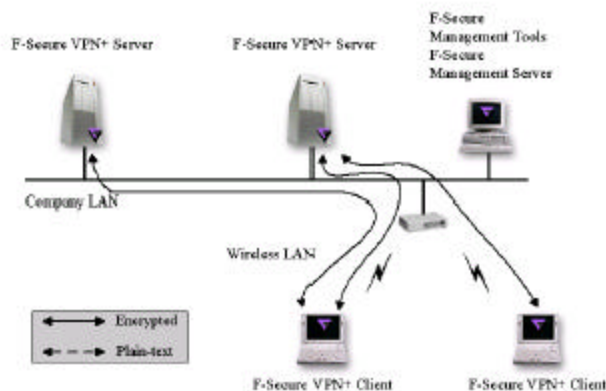


Figure 2. Encrypting Traffic over Wireless and Wired LANs

4. Capacity

Question: I have x wireless LAN access points with 2 Mbit/s of shared wireless bandwidth. How many F-Secure VPN+ Enterprise Gateways do I need to decrypt the traffic between the wireless LAN and the wired LAN?

Answer: As a general rule, one F-Secure VPN+ Enterprise Gateway can handle 10 wireless access points if the Enterprise Gateway software is installed on a 333MHz Pentium II machine. If installed on 500MHz Pentium III machine, the software can handle 14 wireless access points. These numbers assume a maximum load on the wireless LAN.

Question: My company will need more than one Enterprise Gateway. How should I configure my network to have an encrypted wireless LAN?

Answer: The best way is to divide your wireless LAN into different IP subnets. One IP subnet would be routed through one F-Secure VPN+ Enterprise Gateway. The wireless clients would also belong to different IP subnets. This way you will have a very scalable and secure wireless network.

5. Specifications

Authentication algorithms

- HMAC-MD5-96
- HMAC-SHA1-96

Encryption algorithms

- 3DES (168-bit)
- DES (56-bit)
- Blowfish (128-bit)
- CAST128 (128-bit)

Key exchange choices

- Internet Key Exchange (IKE) protocol with:
 - X.509 certificates with RSA signatures
 - RSA signatures
 - DSA/DSS signatures
 - PKCS #7, PKCS #10
- Pre-shared keys

Performance

- Average throughput: 15-20 Mbit/s

F-Secure VPN+ products

- F-Secure VPN+ Client
- F-Secure VPN+ Server
- F-Secure VPN+ Gateway
- F-Secure VPN+ Enterprise Gateway

Supported platforms

- Windows NT 4.0
- Windows 95, 98