

WHITEPAPER



SECURE COMMUNICATIONS ■

PRESENTS

**NCP REMOTE ACCESS VPN PRODUCT
SECURITY FEATURES**

Important Notice

The information in this document is furnished for informational use only and is subject to change without notice.

NCP assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of NCP.

Trademarks

All trademarks or registered trademarks appearing in this documentation belong to their respective owners.

Summary

This document is intended to provide an overview of the security features included in NCP's secure remote access Virtual Private Networking solution.

The three applications driving Internet or any telecommunications network based VPNs are dial up access, intranets, and extranets. The need to provide LAN-to-LAN connections between branch offices has emerged to enable sharing critical resources, and the emergence of e-commerce and supply chain integration has created a demand for extranets, VPNs have emerged as an optimal solution to provide the foundation for these services.

The questions "What is VPN?" and "What is NCP's approach to VPN?" are answered in the NCP whitepaper [An Introduction to Secure Private Networking](#). For information on NCP VPN products, their architecture and how they are best applied in various environments refer to the NCP whitepaper [An Overview of the Architecture & Application of NCP VPN Products](#). The latter also provides solutions and scenarios of VPN projects that already have been installed and have been in operation for a reasonable amount of time.

Firstly this document shows some typical scenarios using remote access VPN solutions. Basically there two scenarios: (1) Remote access from a stand-alone PC, e.g. in a mobile or home office, and (2) from a PC which is integrated in a small Local Area Network, e.g. in a small office or branch.

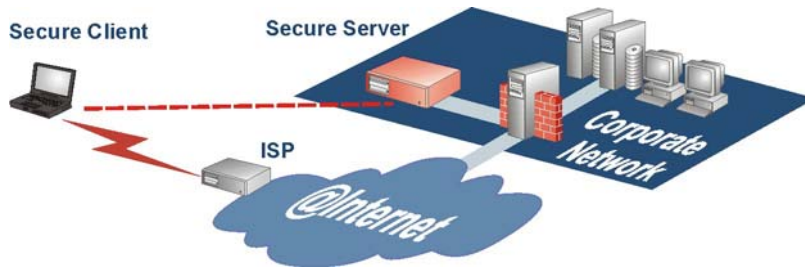
Secondly NCP's response to possible attacks against the Secure Client and the communication with the central site are shown. An unauthorized person using the PC and VPN Client of an authorized user could execute the first attack. In small offices the next attack can come from inside the LAN. It is assumed that most of today's attacks come from the intranet. The third danger is the Internet. As soon as a PC is connected through the Internet to the central site it can be accessed from the Internet as well. And even worse – the central site network could be invaded via the remote access connection. Finally the transferred data can be attacked on their way through the Internet or other WAN media. They can be read, destroyed, or manipulated. NCP has the answer to each challenge.

At the end of this document is a list of the NCP Secure Client Security Features.

VPN Scenarios

Remote Access Clients

Stand-alone remote access clients have become standard in data communication. Laptops and notebooks transform hotel rooms, airport waiting areas, cars, and other sites into mobile offices. Many industries and organizations extend the number of their employees who work at least part-time in home offices.



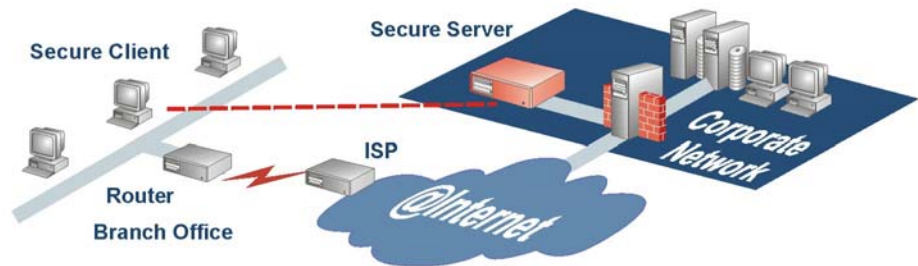
Remote access via the Internet eliminates the costs associated with both the maintenance of expensive infrastructure, and call charges. Extending your corporate network over the Internet to a remote workstation user naturally requires that strong user **authentication, encryption, and data integrity** be provided.

Intranets

Intranets provide cost-effective secure branch office connectivity. Like Remote Access, this approach offers a practical, low-cost alternative to leased line wide-area networking and offers flexibility for distant offices.

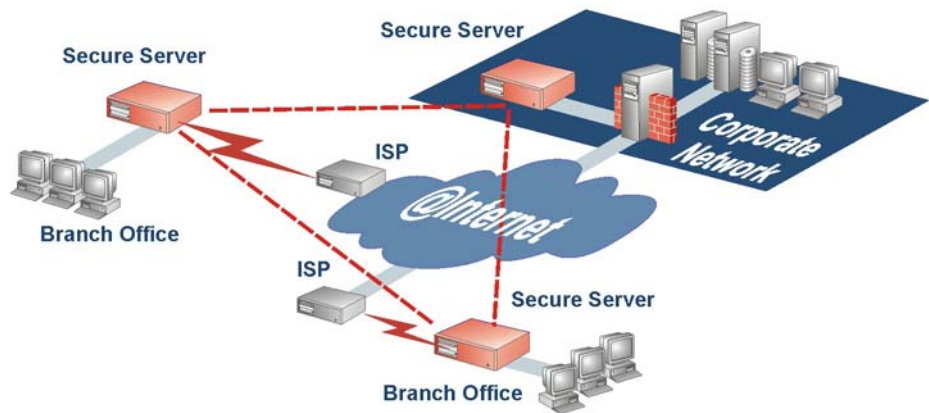
A company may have an existing branch router and certain individuals in the branch may require VPN access. In this case the VPN software can be installed on individual clients.

Alternatively, all users in a branch may be offered access to the VPN, in which case a VPN Gateway in the branch provides such a service, or it may be a business-to-business connection, referred to more commonly as an extranet.



Extranets

An extranet is a virtual private network that uses the Internet to securely share part of a business with other businesses. It can be viewed as part of a company's intranet that is extended to users outside the company. Security and privacy are key issues when implementing an extranet,



and requires firewall server management, the issuance and use of digital certificates, encryption of data, and the use of virtual private networks through the public network.

In all of these cases, an organization is suddenly confronted with a myriad of concerns about security and access control.

Attacks and NCP's Response

Authentication

The Attack: *An unauthorized person uses the PC and the Secure Client of an authorized User in order to attack not only the remote user's PC but also the central site data resources.*

NCP Security in remote access starts at the client. The user is forced to authenticate either according to CHAP / PAP by his userID and password or through NCP's Strong Authentication with his certificate. The certificate can be stored on the PC (soft certificate - a PKCS#12 file) or preferably, on a smartcard (which can be read in a smartcard reader) or USB cryptographic device. When the NCP Secure Client is configured to use a certificate for authentication purposes, the user will be prompted for the "certificate PIN" as the PC is booted, or if configured, every time a connection is made. Assuming this is the case, the unauthorized person will not be able to establish a connection without the PIN.

All the VPN technology in the world is useless if the initial action of connecting is not properly secured. Remote LAN access network security involves two fundamental activities: access control (keeping unauthorized users off the network) and authentication (ensuring that users or remote LANs actually are what they claim to be). In remote access server environments, many levels of security can be attained, ranging from light password security for small, informal networks to full-blown security protocols protecting proprietary information in corporate networks.

PPP (point-to-point protocol), used by all remote access servers, comes with password support in the form of PAP (password authentication protocol) and encrypted password support in the form of CHAP (challenge handshake authentication protocol). These protocols provide a basic level of security negotiation between third-party routers and teleworkers in multivendor networks.

Central-site access servers usually build on the baseline access control security of PPP. Typically, they add a level of authentication protection called dial-back security, in which the access server calls back the device requesting access, thereby ensuring that the user is dialing from an authorized location. In addition, there are higher-level negotiations to verify the incoming MAC addresses of remote LAN access servers. But using such features, as dial-back security in small remote access servers requires a significant configuration effort, including the establishment of a table of authorized MAC addresses. In an enterprise network with thousands of end-points, this type of access security can become extremely labour-intensive.

NCP have addressed secure remote access by providing a number of powerful features in NCP Secure clients, which when used in conjunction with NCP Secure Servers enhance the security levels of communications.

The arrival of PKI has allowed for enhancements in the areas of challenge-response, such as CHAP. CHAP although an improvement on PAP is not inherently secure. The NCP Secure Client supports the use of PKI based authentication for CHAP eliminating a known weakness in Windows environments where CHAP passwords can be stolen. By generating the CHAP password dynamically from the X.509 certificate, the password is always secure, especially when stored on smartcards. The ability to use certificate serial numbers and fingerprints adds to the level of security. This has been taken to a level where RADIUS authentication is fully integrated with LDAP/X.500 to allow RADIUS authentication to be X.509 based, rather than just via traditional Challenge – Response systems that are no longer seen as adequate security, even token based security. Secondly, the NCP Secure Client supports bi-directional authentication. This enables a client to automatically use PKI based authentication for incoming and callback connections.

Certificates however, guarantee the most secure authentication level. NCP's VPN solution also provides support for PKI and certificate related features. The X.509 based certificates used by NCP Secure Clients can be managed centrally or in conjunction with external services (e.g. OCSP, LDAP, and on-line Certificate Revocation Lists – CRLs). These certificates are used by the NCP VPN solution to provide high-level access control and encryption between NCP Secure Clients and NCP Secure Servers at the central site.

Certificates are generally acquired from a "Certification Authority" (CA), which is responsible for issuing and handling the revocation of certificates according to specific guidelines. Such certificates are normally issued on a smartcard or USB cryptographic device ("hard certificate") or as a PKCS#12 file ("soft certificate"). The NCP VPN solution supports both hard- and soft certificates, which are used for authentication purposes when building a link or VPN tunnel in conjunction with SSL or IKE.

Personal Firewall

The Attack: *It is assumed that most of today's attacks come from the intranet. In small offices an unauthorized employee could invade another person's PC via its built-in LAN adapter. Once in the PC that person is able to browse the computer as well as connect into the central site LAN.*

Secure communications also necessitates keeping unauthorized persons from accessing PCs and networks. To prevent such unwanted intrusion it is essential to use firewall techniques. The NCP Secure Client comes with a Personal Firewall feature that provides the required data and communications protection. Essentially it blocks access at the communications "IP" layer according to detection and filtering out of those not authorized to access the client PC. An intermediate driver on OSI Layer 3 manages the filtering according to the configured values.

NCP has implemented an IP filter facility that covers the need to protect data from being accessed or shown on the network. The IP filter can be configured for the filtering of IP protocol types (e.g. IP, ICMP, UDP), IP addresses (destination and source), and IP ports. Filters can be set to permit or deny access to the VPN Client. When the filters are correctly set access from the Local Area Network via the LAN adapter can be completely inhibited.

The configuration allows certain ports to be defined for certain applications without reducing any security aspects. It is, for example, possible to enable access from another PC by allowing a helpdesk application, e.g. PCAnywhere, to use a defined port. In the same manner a VPN bypass mode can be configured, which enables a non-VPN Internet connection (also referred to as "split tunneling"), however this too can be secured based on certain filter settings.

Network Address Translation

The Attack: *Common network structures allow attacks from the Internet. Without a firewall VPN and other remote access clients are completely open to the Web. Everybody with some Internet knowledge can access the remote workstation and use it as a portal to the central site LAN.*

A typical scenario will involve users accessing applications through the Internet, and one of the most commonly required features requested is Network Address Translation.

Network Address Translation (NAT) is an Internet standard that enables a user to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Typically in an Internet environment the external or provider address is dynamic.

NAT or Masquerading is usually used in routers and firewalls. NAT serves two main purposes (1) to provide a firewall type function by hiding internal IP addresses, in this case the IP address of the VPN, and, (2) to allow the use of internal IP addresses in order to assure that there will be no conflict with IP addresses used by other companies and organizations.

NAT exchanges the source IP addresses from the network against the Secure Server's own IP address, which must be an official public IP address. The port number of the data packet is modified as well so that several clients can use the same services. These modifications are stored in an allocation table, which consists of original IP address, original port number, new port number (allocated by NAT). Thus replies from the Internet upon requests from the network can be passed to the right client. The allocation table is deleted after a certain period without data traffic. In order to infiltrate a potential invader would have to know the application and port number, which is dynamically allocated by NAT. As soon as NAT receives a data packet on a port without entry in the allocation table the packet is denied.

NAT is always used for IP communications with the Internet Service Provider and cannot be reset. NAT can also be used for the VPN connection to an NCP Secure Server at the central site.

With NAT the Secure Client's IP address cannot be detected from the Internet. This protects the Client against any attack from the Web. IP NAT is described and defined in RFC 1631.

Data Encryption

The Attack: *When data is transmitted via the Internet or other public networks it is normally not protected and is therefore vulnerable to detection and attack. Data that is sent as clear text is not secure.*

Data encryption is a configurable parameter in the NCP VPN solution. Various state-of-the-art symmetric encryption modes may be selected: DES, 3DES with 168 bit encryption (not 112 bit), Blowfish with 128 bit keys and AES 128, 192 and 256 bit keys. The technical effort, the time needed, and the feasibility to crack encrypted packets exceed any reasonable limits. Therefore one can say that hackers cannot crack encrypted data transmitted via NCP's VPN, at least not today.

A distinct advantage of the NCP VPN solution is that the link and VPN tunnel are properly established prior to any user data being transmitted – and all data sent through the tunnel is encrypted.

The keys for symmetric data encryption (DES, 3DES, Blowfish, AES) are triggered dynamically according to SSL (see below).

Dynamic Key Exchange

The Attack: *Static encryption keys must be exchanged between the communicating partners. The distribution of the keys is a major logistic and security problem. Once a hacker has obtained a key he is able to read all encrypted data transferred over the VPN connection.*

In order to better understand dynamic key exchange, a quick introduction to cryptography is needed. Cryptography, i.e. encryption of information for protection and decryption of information to make it intelligible to applications and people, is the basis for all security services. There are two kinds of cryptography in common use: *symmetric* and *public-key (asymmetric)* cryptography.

Symmetric cryptography, in which a single key is used both to encrypt and decrypt information, offers the advantage of a conceptually simple architecture: Just distribute a key to both ends of the connection. However, distributing symmetric keys raises a "chicken and egg" problem: how to implement strong security for key distribution, when strong security depends on having keys.

Public-key cryptography uses pairs of keys, each pair consisting of one public key and one private key. Information encrypted with one key in the pair can only be decrypted with the other key. Thus, to have a secure connection to a VPN Gateway, the VPN Client must encrypt the data with VPN Gateway's public key. The VPN Gateway then decrypts the data with its private key, which only it has access to. Public-key cryptography solves the key distribution problem because public keys are not secret and can be distributed over non-secured networks, while private keys do not need to be distributed. Since only the owner of a private key needs to have it, the private key can be generated on the machine where it is used. NCP's mission is to enable secure and efficient VPN transactions by complementing standard PKI solutions through a combination of leading-edge technology, extensive systems integration skills and industry partnerships. NCP's early sales and partner successes confirm the company's ability to deliver a reliable, robust security solution that enables banks, and other private and public enterprises, to conduct business securely over the Internet.

For dynamic key exchange the keys for symmetric NCP VPN encryption are encrypted with 1024 Bit RSA encryption, which has not been cracked, at least not today.

VPN Tunnelling

The Attack: *A non-VPN remote access connection allows hackers to destroy or manipulate data packets without being noticed, even if the data is encrypted.*

The use of VPN guarantees the integrity of all user data transferred in the tunnel. A hash value algorithm prevents data that have been changed from entering the destination.

The NCP VPN solution fulfills all requirements for communicating securely across the Internet. It employs both Layer 2 Tunnels (L2F, L2TP and EAP-TLS) and IPSec. VPN tunnels provide end-to-end security, thus making the Internet a secure platform for corporate remote access and communication requirements. The Secure Client receives a private IP address from the Secure Server. The identity of users connecting to the Secure Server is checked. Administrators can grant the users different rights and establish user groups.

RFCs

NCP has made a major effort to implement open standards based on the RFCs of the IETF. Following are a list of some of the RFCs applicable to VPNs and secure communications.

Layer 2 Forwarding (L2F) – RFC 2341

L2F was a technology proposed by Cisco, and still used in many environments, particularly Cisco networks. L2F permits the tunnelling of the link layer (i.e., HDLC, asynchronous HDLC, or SLIP frames) of higher level protocols. Using such tunnels, it is possible to divorce the location of the initial dial-up server from the location at which the dial-up protocol connection is terminated and access to the network provided.

Layer 2 Tunnelling Protocol (L2TP) – RFC 2661

L2TP is a combination of PPTP and L2F. The objective was to integrate the best features of PPTP and L2F. The protocol encapsulates PPP frames to be sent over carrier networks. When configured to use IP as its carrier transport, L2TP can be used as a tunnelling protocol over the Internet. L2TP can also be used directly over various networks, such as Frame Relay, without an IP transport layer.

Over IP carrier networks, L2TP uses UDP and a series of L2TP messages for tunnel maintenance. L2TP also uses UDP to send L2TP-encapsulated PPP frames as the tunneled data. The data is encapsulated in PPP frames, and can be encrypted and/or compressed.

IPSec – RFC 2401-2409

Short for IP Security, IPSec defines a set of protocols to support secure exchange of packets at the IP layer. It is designed to provide security for IP traffic, for example to secure a TCP connection, and is designed with network routers, and gateways in mind. A complex security negotiation is performed between the tunnel endpoints through the Internet Key Exchange (IKE), using PKI certificates for authentication.

One of the major strengths of IPSec is that it is the first tunnelling protocol that specifically addresses the issue of encryption and authentication, based on international standards. IP packets sent by an IPSec host to a protected network are encrypted and delivered to the security gateway for that network. For IPSec to work, the sending and receiving devices must share a public key, which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

IPSec uses packet headers, called Authentication Headers, to validate users and Encapsulating Security Payloads to encrypt data, and supports multiple concurrent remote-access links, so that a user can maintain one connection to the corporate LAN and another to the public Internet.

PPP EAP TLS Authentication Protocol (RFC 2716) – L2Sec

Transport Level Security (TLS), based on the SSL 3.0 Protocol Specification as published by Netscape, provides for mutual authentication, integrity-protected cipher suite negotiation and key exchange between two endpoints. EAP-TLS has been submitted to the IETF as a draft proposal for a strong authentication method based on public-key certificates. With EAP-TLS, a client presents a user certificate to the dial-in server, and the server presents a server certificate to the client. This approach follows the standard that has become the de-facto in the application world, more commonly known as a Public-Key Infrastructure.

Point-To-Point Protocol (RFC 1661)

Today, connection to the Internet, regardless of the device used, is governed by a protocol called PPP, or Point-to-Point Protocol.

The Point-to-Point Protocol is designed for simple links, which transport packets between two peers. These links provide full-duplex simultaneous bi-directional operation, and are assumed to deliver packets in order.

The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link, for example, IP, IPX, SNA, and others.

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP also defines an extensible Link Control Protocol (LCP), which can be used to negotiate authentication methods, as well as an Encryption Control Protocol (ECP), used to negotiate data encryption over PPP links, and a Compression Control Protocol (CCP), used to negotiate compression methods.

Additionally PPP provides many other functions, such as Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP, an encrypted authentication mechanism that avoids transmission of the actual password on the connection, Callback Control, Network Address Translation (NAT), Multilink, and other features.

Encryption Control Protocol (RFC 1968)

In order to establish communications over a PPP link, each end of the link must first send LCP packets to configure and test the data link during the Link Establishment phase. After the link has been established, optional facilities may be negotiated as needed.

The Encryption Control Protocol (ECP) is responsible for configuring and enabling data encryption algorithms on both ends of the point-to-point link.

Security Feature Checklist

	NCP Secure VPN/PKI Client	NCP Secure VPN/PKI Client Enterprise	NCP Secure VPN/PKI Server
Authentication Features			
CHAP Authentication	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes
TACACS	No	No	No
X.509 v3	Yes	Yes	Yes
LDAP / Backup LDAPs	Yes/Yes	Yes/Yes	Yes/Yes
X.500	Yes	Yes	Yes
(CRLs) EPRLs & CARLs	No/Yes	No/Yes	Yes/Yes
OCSP	No	No	Yes
PKCS#11	Yes	Yes	Yes
PKCS#12	Yes	Yes	Yes
Smartcards/Tokens			
ISO 7816-1,2,3 and 4	Yes	Yes	Yes
PC/SC	Yes	Yes	Yes
CT-API	Yes	Yes	Yes
Siemens Readers	Yes	Yes	Yes
SCM	Yes	Yes	Yes
Gemplus	Yes	Yes	Yes
Cherry	Yes	Yes	Yes
Orga	Yes	Yes	Yes
Activcard	Yes	Yes	Yes
Kobil	Yes	Yes	Yes
Towitoko	Yes	Yes	Yes
Rainbow	Yes	Yes	Yes
Aladdin	Yes	Yes	Yes
Vasco	Yes	Yes	Yes
Biometric Support	Yes	Yes	Yes
PKI support and Certification Authorities			
Baltimore	Yes	Yes	Yes
RSA (Xcert)	Yes	Yes	Yes
GTE Cybertrust	Yes	Yes	Yes
Verisign	Yes	Yes	Yes
Thawte	Yes	Yes	Yes

<i>PKI support and Certification Authorities cont.,</i>			
T-Telesec	Yes	Yes	Yes
TC Trustcenter	Yes	Yes	Yes
Globalsign	Yes	Yes	Yes
SSL / OpenSSL	Yes	Yes	Yes
IKE	Yes	Yes	Yes
<i>Supported Encryption Algorithms / Hashing Mechanisms</i>			
DES	Yes	Yes	Yes
3 DES – 168 bit	Yes	Yes	Yes
IDEA (upon request)	Yes	Yes	Yes
Blowfish – 128 bit	Yes	Yes	Yes
AES 128, 192 & 256 bit	Yes	Yes	Yes
MD5/SHA	Yes/Yes	Yes/Yes	Yes/Yes
<i>Personal Firewall features</i>			
IP NAT	Yes	Yes	Yes
IP Port Filter	Yes	Yes	Yes
<i>VPN features</i>			
L2F	Yes	Yes	Yes
L2TP	Yes	Yes	Yes
PPTP	No	No	No
EAP-TLS (RFC 2716)	Yes	Yes	Yes
IPSEC AH	Yes	Yes	Yes
IPSEC ESP	Yes	Yes	Yes
L2Sec (SSL within L2TP ¹)	Yes	Yes	Yes
IP via L2F/L2TP/IPSec	Yes	Yes	Yes
IP via L2Sec	Yes	Yes	Yes
IPX via L2F/L2TP /L2Sec	Yes	Yes	Yes
SNA via L2F/L2TP/L2Sec	Yes	Yes	Yes
NetBEUI via L2F/L2TP/L2Sec	Yes	Yes	Yes
NetBIOS via L2F/L2TP/L2Sec	Yes	Yes	Yes

¹ see also RFC2716