FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

Next Generation Network Access Technology: Overcoming Business Challenges

A Frost & Sullivan White Paper

Prepared for NCP Engineering Inc.

www.frost.com

CONTENTS

1. BACKGROUND AND PURPOSE OF WHITE PAPER

There are two key competing technologies for ensuring secure remote access: IPSec and SSL. There are ongoing discussions across the ICT industry with regards to which is superior. This white paper aims to address that:

1. There isn't a better or worse technology—each has its own merits and drawbacks;
2. As enterprises tap into a connected society, the issues of managing secure remote access can affect their ability to respond quickly to market changes;
3. An increasingly open and connected world makes managing the threat of security breaches a top priority. It is important to do so in a cost-effective way.

NCP's solution addresses these three main points. Its integrated IPSec/SSL solution combines the best of both worlds that also directly resolves the practical challenges facing enterprises that deploy both approaches. These practical challenges, including increased labour units necessary to manage more security certificates and to manually configure each new remote access requirement, incur additional costs and limit enterprises' ability to respond to market changes quickly. Finally, NCP's solution is designed so that enterprises can continue to enable remote access connectivity in a cost-effective way.

Many enterprises, either by choice or necessity, deploy both IPSec and SSL. There are examples of when enterprises migrated from IPSec to SSL, only to realise they were not getting the optimal benefits from either of the approaches. NCP's Next Generation Network Access Technology helps enterprises achieve their business objectives by enabling flexible management between the two, while also reducing the resources needed to manage the resultant complexity.

Chapter 6 of this paper provides usage scenarios to demonstrate the possible cost savings from deploying NCP's Next Generation Network Access Technology. The solution is optimal in enterprises with more than 2,000 mobile employees, where 41 percent savings can be achieved.

Besides the important cost issue, NCP's Next Generation Network Access Technology solution ensures that the basic requirement of secure access is achieved. It also allows simplified management via its Management Server dashboard, which, in turn, reduces administrative complexity.

2. THE CURRENT ENTERPRISE NEED FOR REMOTE CONNECTIVITY

A modern enterprise needs remote connectivity because the connected society is an integral part of its operating environment. The world has become smaller as a result of wider availability of connectivity for citizens by an increasing variety of technology and means. It will continue to shrink as more join this connected society. This connected society, in turn, becomes a wider marketplace with which a successful enterprise engages for sustained economic success. The enterprise's infrastructure network therefore becomes more complex to accommodate a possible exponential increase in the number of interconnections of employees, partners, suppliers and customers. It is this reality of a growing web of interconnections that a modern enterprise currently faces.

C-level executives ask how such a ubiquitous world balances the anticipated revenue benefits with the expected costs of managing a complex connectivity infrastructure. What are the holistic and practical changes needed to manage this complex web of connectivity for business purposes in a cost-efficient manner? This connectivity must be made securely available to an increasingly large pool of stakeholders who gain remote access on more devices, platforms and technological options. The resultant burden on the IT department also increases the importance of managing remote connectivity in a cost-efficient manner.

The Modern Enterprise in an Interconnected World

The modern enterprise requires remote connectivity in the following ways:

1. **A connected society links more people at a faster rate.**

The modern and successful enterprise embraces opportunities from a connected society. As more users join this connected society, the modern enterprise finds it easier to reach out to a larger audience that includes customers, suppliers, partners and employees. At the end of 1999, only 8 percent of the world's population had a mobile subscription, 5 percent of the world's inhabitants were Internet users and 0.1 percent were broadband subscribers. By the end of 2010, more than three-quarters of the world's population was a mobile customer, a third used the Internet and almost 10 percent had a broadband connection. As connectivity spreads, the modern enterprise needs a remote connectivity solution that accommodates more connections via more devices, machines and platforms by more communication protocols.

2. **Ubiquity changes user behaviour in a connected society.**

The modern enterprise adjusts to changes in user behaviour as work flexibility allows more employees to work remotely on mobility devices and Internet ubiquity widens reach to third-party stakeholders. The method of interaction between the enterprise and the marketplace is increasingly moving online. This means the modern enterprise needs to enable a cost-effective method of securing remote access for a variety of usage patterns.

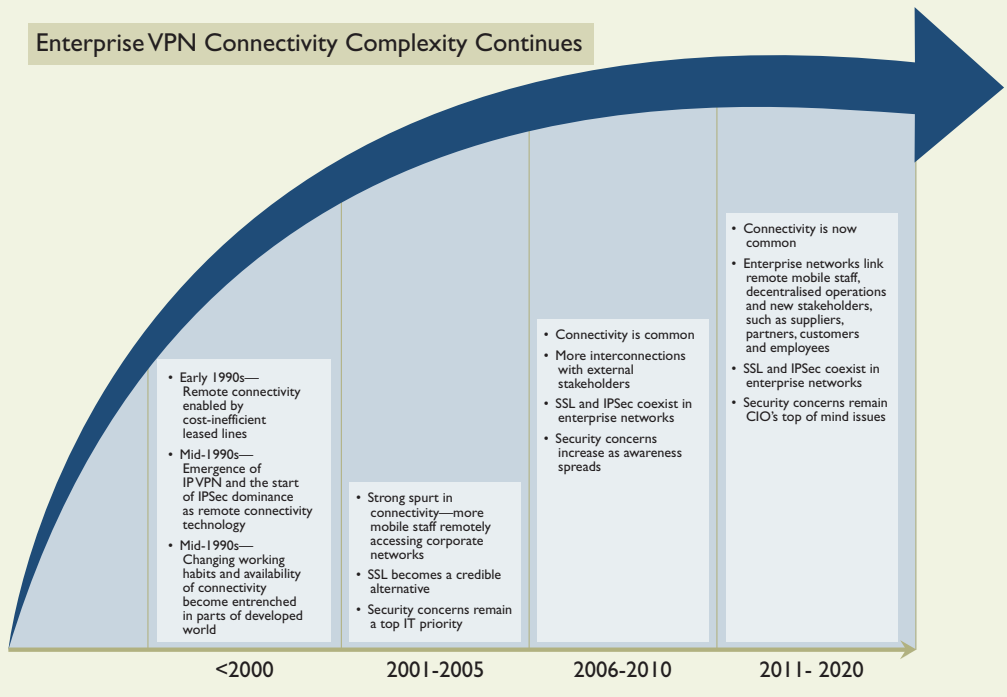
A modern enterprise taps into ubiquitous connectivity to enhance its profit-making capabilities. Remote VPN connectivity in a modern age means enterprises now manage more connections—from an increasingly large pool of stakeholders—from more devices, machines and platforms, by more communication protocols with growing and higher security demands at real or close to real-time connectivity.

3. A connected society increases security risks.

The openness of an interconnected world also increases security risks, which have to be managed cost efficiently. With more connections come increased vulnerabilities to attacks. An awareness of security risks also raises a modern enterprise's need to be seen as doing all that is possible to protect and secure its data transmitted across this interconnected web. With growing complexity in the web, a modern enterprise needs to have visibility of its remote access connections in order to secure and protect communications in a cost-efficient manner.

In short, modern enterprise need for remote connectivity evolves over time, as summarised in the illustration below. The complexity of managing remote access connectivity will also increase as the world becomes more interconnected.

Figure 1: Enterprise VPN Connectivity Complexity Continues



3. REMOTE ACCESS MARKET – APPROACHES AND SOLUTIONS

The two most common Remote Access approaches in the market—Internet Protocol Security (IPSec) and Secure Socket Layer (SSL)—have established their respective footholds in line with changes in enterprise requirements. IPSec emerged in the late 1990s as an alternative to expensive and inflexible leased lines approaches adopted for remote access connectivity. It established itself as a credible and cost-efficient alternative because enterprises mostly enabled remote access connectivity for a selected number of mobile employees and the management of decentralised site-to-site operations. During the early 2000s, SSL came to the fore as a remote access alternative to IPSec, as it coincided with enterprises' need to cope with more mobile endpoints requiring only selected access.

The debate over which approach is "best" has clouded a critical point. There is no "best" solution in absolute terms; there is only the most appropriate solution based on company characteristics and uses of remote access connectivity. Both approaches have a common goal, but differ in terms of the means to the end. Furthermore, both IPSec and SSL vendors preach their own advantages to their customers, resulting in a coexistence of both technologies in enterprises' networks. Frost & Sullivan believes that the management of both approaches negates some of the benefits that each protocol promotes, especially in terms of cost effectiveness.

"Both IPSec and SSL achieve the same results of secure transmission of data over networks. Yet, operational implementation of both solutions often creates practical challenges."

Frost & Sullivan

IPSec and SSL Achieve the Same Result

IPSec and SSL are two protocols that secure transmission of data over networks; they both achieve the same outcome by ensuring data retains integrity, confidentiality and authenticity. The illustration below summarises the two approaches.

Figure 2: IPSec and SSL Cheat Sheet

	IPSec	SSL
What is it?	Achieves secure remote access via a set of ratified protocols by IETF to use the Internet to transmit data	Achieves secure remote access using widely available protocol found on most Web browsers
How it secures remote connectivity	Works on IP layer using encryption and authentication protocols offering data authenticity, integrity and confidentiality	Working on the Application layer, SSL also uses encryption and authentication protocols
Why it is popular	Positioned as a low-cost alternative to expensive and inflexible leased lines for connecting VPNs	Positioned as clientless and application-based alternative to traditional VPN solutions
What it is best for	Universal secure remote access for company site-to-site connections, remote and mobile employees	Application-based connectivity for mobile users, especially external stakeholders such as partners and suppliers

Source: Frost & Sullivan

IPSec—A Dominant Approach

IPSec is a set of protocol that was ratified by the Internet Engineering Task Force (IETF) in the late 1990s. It secures data transmission at the IP layer, ensuring data integrity, authenticity and confidentiality. It does so by encrypting data in both transport and tunnel modes. Data is secured by requiring IPSec-compliant sending and receiving devices to encrypt and decrypt each packet of data by the same shared public key. This is established through a protocol that allows the receiver to obtain a public key and authenticate the sender using digital certificates. IPSec became popular because it followed a set of open standards that ensured secure private communications over the Internet. The fact that it was ratified by the IETF helped to overcome initial adoption issues. IPSec works well in site-to-site connectivity and in remote access situations for linking remote and mobile employees. It is also well-suited to situations where enterprises are seeking to secure remotely connected, decentralised operations.

SSL—The Alternative

SSL is the second main approach to secure remote access connectivity. It utilises a set of commonly available Web protocols to secure data transmission over the Internet; SSL is added to HTTP to secure the session without the hassle of additional software downloads or requiring additional user knowledge.

It secures data transmission at the application layer and also achieves the required data characteristics of data integrity, authenticity and confidentiality. SSL achieves this by authenticating the user and enabling access to the appropriate resources and applications, encrypting and decrypting data transmission over the Internet at both ends, and presenting the appropriate content and applications to the end user. SSL gained prominence as the second main approach for secure remote connectivity because it coincided with a significant shift in user behaviour. SSL works best in an environment where enterprises must facilitate remote access for external stakeholders such as partners and suppliers. Specifically, SSL is well-suited to usage scenarios where enterprises need to secure remote connectivity for mobile users to a specific subset of corporate applications.

IPSec and SSL—Underlining the Differences

While both IPSec and SSL achieve the same outcomes of enabling secure remote connectivity for enterprises, they secure remote connectivity in different layers of the network. IPSec secures remote networks at the IP layer, thereby optimally achieving always-on and reliable connectivity for remote users to the whole enterprise resource. SSL works on the application layer, providing flexibility to enterprises to manage access policies. This difference, therefore, allows enterprises to use IPSec and SSL accordingly; IPSec for linking a company's sites, remote and mobile employees with secure, reliable and always-on connectivity and SSL for linking individuals who are remote workers or external partners.

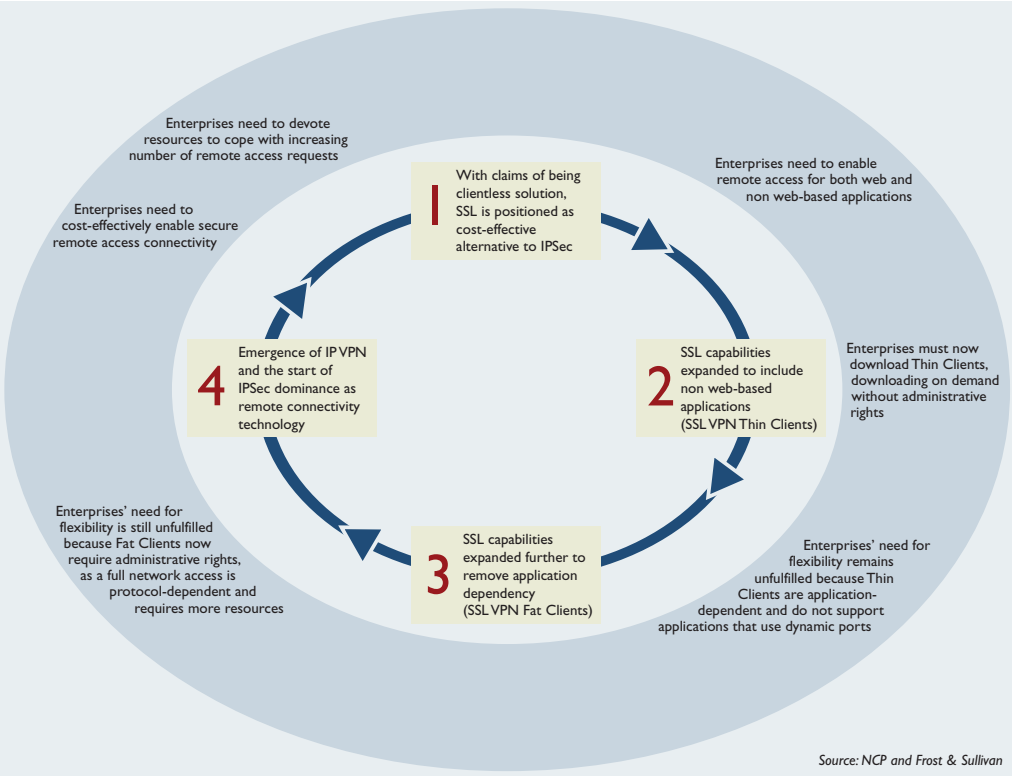
IPSec also differs from SSL in that it provides transparent network access. SSL has its origin in the application-based approach. Its claims of being clientless SSL VPN only applies in such webified application environments as Outlook Web access. In cases where enterprises demand additional requirements, SSL functionalities are expanded, which ultimately leads to client functionality. This additional complexity is described in the next section.

IPSec and SSL—Is there a Middle Ground?

One of the practical ways to gain a sweet spot of both IPSec and SSL benefits is for enterprises to deploy both according to their operational structure and business requirements. Frost & Sullivan has observed that many vendors provide as complete a remote access solution as possible. For example, many SSL vendors also allow their solutions to integrate with other technologies to be supported on other devices and be aggregated onto a single client network. On the other hand, SSL vendors have also continuously widened their solution functionalities to address enterprises' implementation challenges.

However, such SSL solution enhancements diminish its original claim to be a cost-effective alternative. The illustration below summarises how as SSL capabilities widen, it becomes similar to IPSec.

Figure 3: IPSec & SSL – A Middle Ground Still Brings Us Full Circle to Enterprises' Practical Needs



As illustrated above, a middle ground does not fully address enterprises' practical needs.

1. SSL is positioned as an easy-to-deploy and cost-effective remote access method. This is anchored in SSL's proposition that it is a clientless solution. Yet, as practical implementation issues arise, enterprises find themselves devoting more resources to enable remote access as practical functionalities are required. For example, enterprises often require secure remote access connectivity for both Web- and non-Web-based applications.

2. As such, SSL VPN Thin Client, an on-demand client download without requiring administrative rights, is introduced to enable remote access connectivity for non-Web-based applications. Once there are any client downloads, SSL's original claim and unique value proposition to be clientless are negated.

3. More practical deployment issues arise as enterprises also require remote access connectivity that is both application- and port-independent. SSL VPN Fat Client is introduced to overcome this issue. Yet, implementing Fat Clients now requires administrative rights as a full network access is protocol-dependent and thus consumes more resources.

4. This eventual iteration of SSL functionality may have addressed enterprises' evolving implementation needs but it also brings SSL to the same outcomes from traditional IPSec. Furthermore, with SSL Fat Client, enterprise flexibility and cost concerns are further constrained because enterprises are locked to a specific vendor as no solutions offer any sort of interoperability.

In short, Frost & Sullivan believes that the most important key to achieving the best of both worlds lies in the implementation of both IPSec and SSL. Operational implementation challenges are too often the first obstacle to a solution's effectiveness.

4. WHAT IS NEEDED TO MEET CURRENT ENTERPRISE REQUIREMENTS?

The modern enterprise uses remote connectivity as a tool to reach out to a wider audience of internal and external stakeholders. It expects secure remote access deployment to achieve the following three outcomes:

1. Ensuring data integrity, confidentiality, and authenticity during remote access sessions;

2. Enabling remote access on fixed and mobile connections;

3. Achieving cost effectiveness in terms of IT resource requirements and up-front Capex.

In short, the enterprise needs a solution that minimises cost, reduces IT complexity and ensures operational flexibility.

The Modern Enterprise Needs a Cost-Effective Solution

Many enterprises deploy both remote access approaches concurrently. The practical outcomes of implementing both approaches are such that related IT costs could outweigh the benefits of combining the two. When vendors attempt to fit both solutions toward enterprises' business goals, practical deployment issues arise, such that more IT tasks are created. As such, Frost & Sullivan believes that the key to maximising a solution's cost effectiveness lies in the implementation. A cost comparison is elaborated in Chapter 6.

The modern enterprise faces increasing IT costs because concurrent deployment of IPSec and SSL create additional tasks that add up over time. The cost burden comes from three main areas:

- **Remote access strategy set up:** The cost burden lands on both the CTO and the IT department. The former ensures that both IPSec and SSL fit internal processes and organisational structure. It spends time and effort with vendors to maximise the desired outcomes for different remote access usage patterns. This is especially so when it is necessary to fully understand the security risks in deciding the implementation of IPSec, SSL or both approaches. Secondly, the IT department is involved in the laborious task of testing and documenting both IPSec and SSL remote access approaches. Additional time is expended when deployment is scaled up to include more users, connectivity and/or endpoints.

- **Remote access operation:** The cost burden of deploying both approaches is significant. This stems particularly when traditional SSL solutions are enhanced to address practical deployment issues. Frost & Sullivan believes that SSL's value proposition as a clientless solution is not strictly so in practical terms. Since not all applications are Web-enabled, IT resources are needed to test and enable for enterprise-wide use. To overcome this operational challenge, SSL vendors further enhance their offer, such that remote users can gain access to enterprise-wide resources. Unfortunately, such improvements consume IT resources because administrative rights have to be assigned and maintained.

- **Remote access maintenance:** Maintenance of both IPSec and SSL is also a significant cost burden. Related to operating both approaches, the IT department spends resources updating documentation when deployment widens across applications and users. IT resources are also consumed when access rights must be defined, provisioned and managed across a large number of users, endpoints and connectivity access points.

"The modern enterprise needs remote connectivity solutions that are cost effective, remove operational complexity and provide operational agility."

Frost & Sullivan

A Remote Access Connectivity Solution Must Reduce IT Complexity

As outlined above, deploying both IPSec and SSL concurrently becomes less cost effective because of the increased activity burden on the IT department. The additional tasks and timespend also imply a certain amount of IT complexity. A modern enterprise needs a solution that reduces IT complexity in order to achieve accuracy in processes and to enable better compliance with any reporting requirements.

IT complexity is also evident in the following three areas:

- **Remote access strategy set up:** Both the CTO and the IT department face a more complicated dashboard when attempting to align business needs with market solutions. The CTO could face a lack of vendor support in fully maximising its remote access solutions. The IT department on the other hand expects that manual tasks of provisioning, managing and controlling remote access should be reduced, or at least simplified. When both IPSec and SSL are deployed at the same time, there will be more parameters (such as endpoint security risks) to be considered. Subsequently, this also adds to IT department complexity as IT resources have to take additional steps to minimise such endpoint security risks.

- **Remote access operation:** The practicalities of deploying SSL according to actual enterprise requirements are such that the benefit is minimal in reality. As the number of SSL sessions increases, enterprises have more security certificates to manage and they also have less visibility of their remote access control. SSL's other key selling point is its reliance on the Web-based protocol, HTTP. SSL works best in a Web environment because of the way it achieves remote access security. While SSL can work in non-Web-based applications, the additional IT resources needed to enable this negate the benefits that SSL brings in terms of simplicity of use.

- **Remote access maintenance:** The IT department faces a complex web of tasks when managing both IPSec and SSL concurrently. The risk of "missing the forest for the trees" can be high, especially for enterprises that face high financial or brand penalty for getting things wrong.

A Solution that Provides Operational Flexibility

Traditional IPSec as a standalone solution provides operational flexibility within the confines of managed devices and trusted networks. There remains the need to pro-actively respond to market trends.

In contrast, SSL's reliance on Web-based protocol allows enterprises to more easily manage remote access connectivity. However, this is often not the case, especially when it becomes necessary for the IT resource to also balance the management tasks of both IPSec and SSL. Most importantly, Frost & Sullivan believes that SSL's benefits of being able to provide a more granular access control could backfire and complicate security certificate management.

As enterprises deploy both IPSec and SSL concurrently, Frost & Sullivan believes there is a gap between enterprises' needs and market solutions. The shortfall lies in implementation of both solutions; Frost & Sullivan believes NCP's solution addresses this gap.

5. NCP'S NEXT GENERATION NETWORK ACCESS TECHNOLOGY

Frost & Sullivan believes NCP's solution to be well placed in the remote access connectivity space because it provides enterprises with unique benefits and addresses their implementation challenges. In particular, NCP's integrated IPSec/SSL VPN solutions meet the enterprise needs for cost effectiveness, reduced IT complexity and increased operational flexibility.

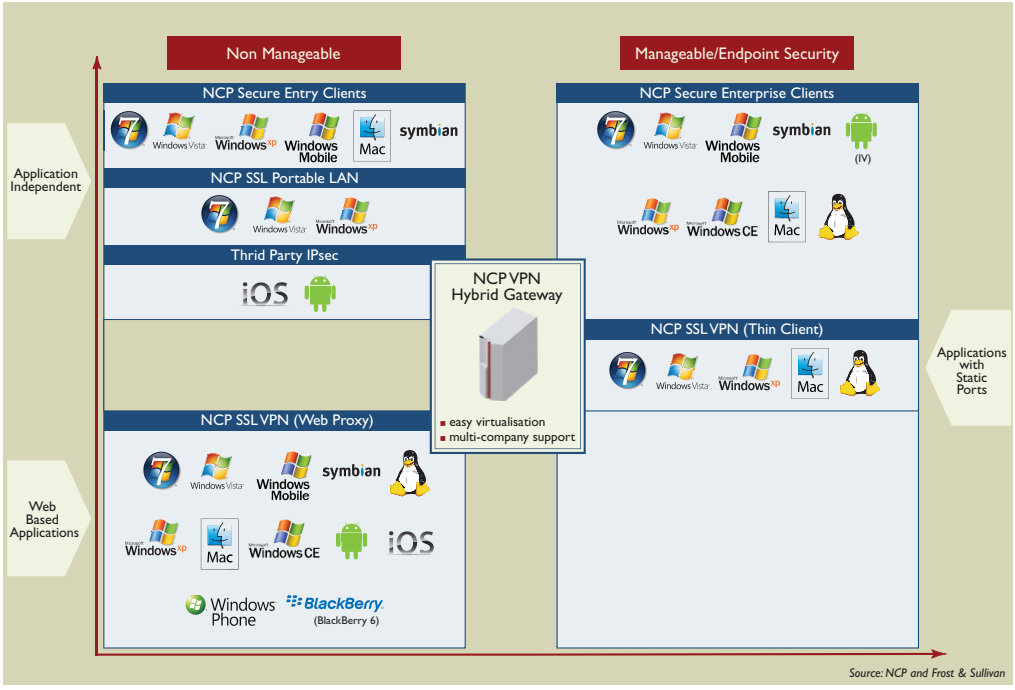
NCP's Secure Enterprise solution is made up of the following components.

- **NCP Secure Enterprise Suite:** A universal secure endpoint product that enables customers to easily and accurately manage remote access for their end users.
    - Integrated personal dynamic firewall
    - Integrated Internet Connector
    - Central Management – managing different connectivity modes and connectivity expenses
    - Path Finder Technology
    - Seamless roaming
- **NCP Secure VPN Enterprise Management:** A solution that streamlines the tasks of remote access management to a few clicks and still provides visibility of the network.
    - Fully automated remote access operation
    - Network access control
    - A single point of administration

"There is a shortfall in implementing standalone IPSec and SSL solutions; NCP's solution is positioned to overcome precisely this practical challenge while keeping to cost, complexity and agility requirements."

Frost & Sullivan

Figure 4: NCP Secure VPN Enterprise Management



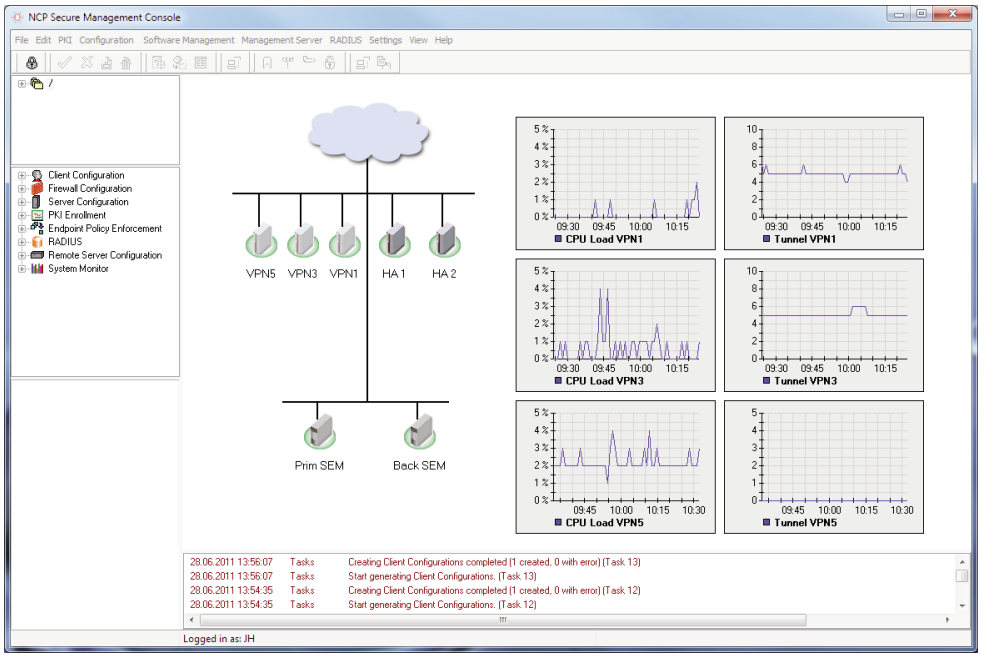
NCP is Cost Effective

NCP helps its customers deploy a cost-effective solution by reducing management, training, documentation, user help desk and maintenance costs, thereby helping enterprises with one of their biggest challenges—cost containment.

NCP's Secure Enterprise Suite is a set of solutions that directly and indirectly reduces costs to the IT department. Through NCP's single interface to the end user, the IT department no longer needs to train and document every new feature or improvement made to the enterprise's remote access approach. Indirect reduction in costs also materialises when the IT department has fewer helpdesk requests and when end users have an intuitive user interface for enabling remote access. As end users need fewer clicks, there is also less need for IT documentation and training. They also reduce the probability of making mistakes while navigating, thus eliminating unnecessary helpdesk requests. In short, this directly reduces the number—and duration of—tasks.

NCP's Secure Enterprise Management is a management console that streamlines the tasks of remote access management to a few clicks and still provides visibility of the network. For example, the IT administrator uses a Single Point of Administration to provision, configure and manage licences from a central platform. The ease of use also reduces the support costs, a significant contribution to the cost effectiveness of the solution.

Figure 5: SEM Console Screenshot



Chapter 6 makes the case with an illustrative scenario.

NCP Reduces IT Complexity

Both of NCP's products were designed to help enterprises reduce their IT complexity.

NCP's Secure Enterprise Suite includes a universal secure endpoint product that works on five different operating systems. A parameter block hinders subsequent manipulation, whether intentionally or through an accidental operation. This achieves the required security level for enterprises, as they enable remote access connectivity for unmanaged devices connecting to the whole network.

NCP's Secure Enterprise Management relies on the Single Point of Administration that frees up IT resources from low-value tasks. This console is designed for intuitive use with full visibility of network resources. Enterprises benefit from this simpler approach to management and maintenance. A related benefit for the enterprise is an easier knowledge transfer within the IT department. An easy-to-use console reduces the training time for administration. NCP's Secure Enterprise Server's integrated IPSec/SSL gateway removes the need to anticipate users' choice of protocol. This is especially important when an enterprise needs to quickly and easily scale for increase in mobile users. For example, NCP's software-based server allows enterprises to have 100,000+ connections at the same time.

NCP Gives Enterprises Operational Flexibility

As suggested above, NCP's solutions also give enterprises operational flexibility when scarce IT resources are freed from manual tasks. In particular, NCP's Secure VPN Enterprise Management allows IT resources to centrally manage all remote access connections and also provides network visibility for greater security management.

Figure 6: NCP Secure Enterprise Client

Finally, NCP's solutions directly address enterprises' implementation challenges. The ease of use via its Enterprise Suite and Enterprise Management solutions overcome the IT-related complexity of provisioning, managing and controlling remote access. Its Enterprise Client Suite further minimises the tasks related to endpoint security risks. In short, Frost & Sullivan believes that not many security vendor offerings tackle this implementation issue directly.

6. TCO CASE STUDY FOR NCP'S NEXT GENERATION NETWORK ACCESS TECHNOLOGY

Using a representative enterprise with 2,000 mobile users, NCP's cost effectiveness is compared to that of other vendors by investigating the cost components. These cost components include one-time equipment and software costs, initial deployment expenses and ongoing management and maintenance costs. The TCO example below will show that NCP's solution offers 41 percent cost savings compared to an approach by other vendors.

TCO Example

Profile of an illustrative organisation using NCP's solution (base assumptions about this organisation will be used in all ROI calculations below):

- Number of mobile employees: 2,000
- Cost of IT resource: US$150/hour

Compared to a non-NCP deployment, NCP's solutions require fewer man-hours per user to manage and maintain security certificates. NCP's solution reduces the complexity of remote access management, thus reducing the hour per user in this calculation. Based on a standard use of VPN and NCP's new solution, the latter provides a 41 percent cost savings.

The calculation of the cost of initial rollout with other vendors would be:

2,000 mobile users * (0.5 hrs/user * $150/hour) = $150,000

The calculation of the cost of initial rollout with NCP's solution would be:

2,000 mobile users * (0.1 hrs/user * $150/hour) = $30,000

The calculation of the average cost of management with other vendors (annually) would be:

2,000 mobile users * (0.75 hrs/user/year * $150/hour) = $675,000

The calculation of the average cost of management with NCP's solution (annually) would be:

2,000 mobile users * (0.1 hrs/user/year * $150/hour) = $90,000

The calculation of total maintenance expense with other vendors (annually) over two years would be:

20% * Purchase Price ($60,000) * 2 years = $24,000

The calculation of total maintenance expense with NCP's solution (annually) over two years would be:

20% * Purchase Price ($300,000) * 2 years = $120,000

"NCP's solutions offer at least 40 percent cost savings to other remote access solutions."

Frost & Sullivan

Figure 7: NCP's Solution Offers a 41% Cost Savings Over Other Remote Access Solutions

Assume the following:

- Number of mobile employees – 2,000
- IT salary/hour – US$150/hour
- Number of hours per user for:
  - Other vendors:
    - 0.5 hour/user initial rollout
    - 0.75 hour/user management
  - NCP:
    - 0.1 hour/user initial rollout
    - 0.1 hour/user management
- Annual Maintenance:
  - 20% of Purchase Price, Over 2 years
- Equipment & Software:
  - Other vendors: US$60,000
  - NCP: US$300,000

US$	Other Vendors	NCP
Equipment & Software	60,000	300,000
Initial Deployment	150,000	30,000
Annual Maintenance	24,000	120,000
Annual Management	675,000	90,000
TCO	909,000	540,000
TCO/User	454.50/user	270/user

41% cost savings!

Source: NCP

"NCP's solutions address the practical implementation challenges while keeping to cost, complexity and agility requirements by a modern enterprise."

Frost & Sullivan

7. NCP'S SOLUTION ADDRESSES THE MODERN ENTERPRISES' NEEDS

Frost & Sullivan believes that NCP's Secure Enterprise Solution is well placed to address the modern enterprises' need for remote access connectivity. This is because NCP brings the three main benefits of remote access connectivity and, more importantly, addresses the implementation challenge of achieving both IPSec and SSL unique benefits simultaneously.

NCP's cost effectiveness can be further accentuated as the number of mobile users increases. We believe that this benefit is optimally achieved when there are more than 2,000 mobile users. This, in turn, positions NCP as a strong player in the large enterprise marketplace. Finally, Frost & Sullivan believes that NCP's solution addresses the modern enterprises' needs by allowing them to securely leverage a connected society.

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

Oxford
4100 Chancellor Court
Oxford Business Park
Oxford, OX4 2GX, UK
Tel: +44 (0) 1865 398600
Fax: +44 (0) 1865 398601

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

+44 (0)20 7730 3438 • enquiries@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.