7 Requirements for Pain-Free VPN Client Support

Questions to ask when planning a VPN

How many employees need to connect to the network? Are they mobile or stationary?

Do they alternate between office and home/mobile?

Where are they located? Are they local, regional, nationwide, or worldwide?

From what types of connections do they access the network?

What types of remote devices do they use?

What applications will they use over the network?

Do they need to connect to IT components such as user-defined databases, RADIUS directory service, or the like?

How tight should the security be for network access?

Secure remote access without exhausting your support resources.

The trend toward increased worker mobility and anywhere-anytime computing appears to be unstoppable. Mobile devices are now ubiquitous, and more than half of enterprise employees use them (or want to use them) for work purposes. As a result, the protection of your network and your business' confidential information has never been more critical—or more challenging.

According to the 2014 State of Endpoint Risk report, researched by Ponemon Institute LLC, 60 percent of IT respondents say the biggest threat to endpoint security "is the growing number of employees and others who use mobile devices in the workplace followed by the increase in personal devices being connected to the network."*

Virtual private networks (VPNs) are key to preventing threats to your network. But as your company grows and the number of users and devices increases, you need to make sure your VPN is never too complex to operate securely and efficiently. By deploying a VPN solution that's flexible, scalable, and straightforward to manage, you'll protect your network from hackers and other interlopers. At the same time, you can lighten the burden on your support resources, while improving their productivity and gaining the flexibility to adapt to rapidly changing technologies.

To remove the pain from supporting VPN clients, take a fresh look at your VPN environment. Does it meet these seven requirements?

1. **Runs on all operating systems.**
2. **Supports all connection types.**
3. **Adjusts for all devices.**
4. **Works with your existing infrastructure.**
5. **Has a single point of administration.**
6. **Integrates both IPsec and SSL protocols.**
7. **Offers two-factor authentication.**

7 Requirements for Pain-Free VPN Client Support

The **Uvex Safety Group**, a global supplier of workplace safety gear, needed to provide mobile connections for its large and distributed sales team. By choosing a VPN solution with a single point of administration—and one that supports all leading communication and security standards—they've been able to facilitate system migrations and uphold strict security policies.

1. Runs on all operating systems.

As the BYOD (bring your own device) trend grows, network administrators have less (or no) control over the devices, operating systems, and software that their company's employees use. Your VPN technology should facilitate remote access over the leading desktop and mobile operating systems—Windows, Mac OS X, Android, iOS, and Linux—and ideally a number of smaller platforms as well. It also should be designed to adapt quickly to changes in the popular operating systems and to the introduction of new ones down the road.

Along with universal support, VPN technologies with consistent client interfaces across devices and operating systems result in other important efficiencies. You won't have to maintain instructions for each operating system and each device, and users can have the same experience from laptop to smartphone to home desktop—reducing the load on your help desk and improving employee productivity.

When **American Hospice**, a leader in the delivery of hospice services, needed to transition to a fully mobile communication system, they were concerned about meeting stiff HIPAA security requirements. They solved the challenge with a robust VPN solution that also provided a single point of management, including network access control (NAC) functions. IT administrators are now able to easily provision users and devices, distribute updates, and control configuration settings—and rollout to 180 home healthcare professionals took only three days.

2. Supports all connection types.

Your employees may be accessing the corporate network through mobile hotspots, over public Wi-Fi networks, or over 3G or 4G/LTE connections—and they require the same security as when they're working on the secure LAN infrastructure in your office. Your VPN should shield and encrypt communications during data transmission, protecting the integrity of your company's information, through any type of connection.

At the same time, a good VPN client doesn't drop off or require a settings adjustment when the client moves from one connection type to another. Your users want to be able to roam seamlessly from their Wi-Fi network at home to a 3G/4G network on the road and on to a hotspot at the café—without needing to re-establish the connection.

7 Requirements for Pain-Free VPN Client Support

A **global technology company** that specializes in the manufacturing and distribution of office equipment has an extensive mobile workforce that uses Motorola ES400 phones. By implementing a VPN that supports reliable connections for a broad array of devices, the company's salespeople can now upload data from their ES400s—easily and instantly—to the central ERP system. The result has been reduced billing cycles, more efficient customer order fulfillment, and quicker query resolution—while lightening the load on IT.

An **architectural and engineering consultancy** that works with more than 1,000 state and local agencies has a challenging environment of overlapping networks. They found a VPN solution that would operate with their existing infrastructure and enable them to provide centralized management—including personal firewall configuration—of 650+ clients in remote field offices.

3. Adjusts for all devices.

As more of your employees connect remotely to networks through mobile phones or tablets, you may need to adjust back-end settings to keep the VPN connection open for a different standard period of time. Mobile devices often go idle more often than a laptop. Should it disconnect from the VPN tunnel each time, to prevent possible third-party infiltration? Or should it remain on, so that it's easier for employees to access the VPN? Do you need your VPN solution to handle M2M connections—with scanners, vending machines, ATMs, and the like—without requiring human interaction? Consider a VPN solution with the flexibility to address these issues, ideally one with central management capabilities for automating client-device VPN configurations and for VPN software distribution.

4. Works with your existing infrastructure.

With the proliferation of more advanced threats, communication between your network and security components is vital. Make sure your VPN technology is an integral part of your infrastructure and doesn't require you to replace network components. Your VPN solution should interoperate easily with VPN gateways—from providers such as Cisco, Juniper, Check Point, and Fortinet—protecting your investment while avoiding the pitfalls of vendor lock-in. In addition, by combining solutions from more than one vendor, you'll create multiple security layers, which will strengthen the defense-in-depth framework of your network environment.

5. Has a single point of administration.

As your company grows, you need a VPN solution that scales with your organizational needs—and keeps you in control. Look for centralized management capabilities that make it easy to support anywhere from 50 to 50,000 connections simultaneously. A single point of administration will enable you to automatically roll out VPN client configurations, personal firewall configurations, and VPN software updates; to issue, manage, and maintain certificates; and to monitor policy compliance. And if your VPN solution integrates

7 Requirements for Pain-Free VPN Client Support

Truesense Imaging, a provider of high-performance image sensors, needed a remote access VPN solution to sustain the productivity of sales teams and technicians on the road. By choosing a 100% software solution with centralized robust client management capabilities, they've been able to provide highly secure network access using two-factor authentication—including easy centralized management of mobile connect cards and one-time password (OTP) tokens and certificates.

with your existing user database, such as Active Directory or LDAP, you can easily create (and delete) user accounts.

Centralized management eliminates the need to support clients manually and individually, reducing the chance of user error and reducing help desk requests related to your VPN. Rather than providing configuration instructions (and trusting users to follow them), you may be able to embed configuration profiles into your installer, so that users can simply install the client and immediately log on to your VPN.

6. Integrates both IPsec and SSL protocols.

Your VPN environment needs to support employees to work effectively regardless of the application they're using or where they are when they connect to the network. For remote employees who need access as though they're at corporate headquarters—for example, accessing corporate share drives and applications—an IPsec (Internet Protocol Security) connection is preferable. For secure web-based applications and communications, an SSL (Secure Sockets Layer) connection may be sufficient. A VPN solution that provides both IPsec and SSL tunneling technologies in one environment can meet the needs of all the users throughout your organization—teleworkers, field services, sales, customer service, and partners—and simplify administration of a secure network.

In order to guarantee local support for its 1.5 million customers, a **large insurance provider** needed to enable its 2,500+ users to connect securely to its network from public hotspots—which required two-factor authentication of the VPN connection via smartcards and the Microsoft certificate store. The company was able to find a VPN solution that integrated with the CSP (Cryptographic Service Provider) connection, as well as with other existing infrastructure components—giving them a single remote access management system for defining all client parameters and enforcing all policy changes on end-devices within a moment's notice.

7. Offers two-factor authentication.

With many potential threats to your network, you need more than a username and password to permit remote access. A robust VPN, using state-of-the-art authentication mechanisms, is an important defense at client endpoints. What security level is necessary? Consider a VPN solution that supports two-factor authentication—based on something you have (a device or a token, for example) and something you know (username and password, for example). Adding and maintaining a second authentication factor usually requires additional resources. Make sure you have a solution that

7 Requirements for Pain-Free VPN Client Support

About NCP engineering

Since its inception in 1986, NCP engineering has delivered innovative software that allows enterprises to rethink their remote access and to overcome the complexities of creating, managing, and maintaining secure network access for their staff.

NCP's award-winning product line spans the spectrum of remote access, from IPsec and SSL VPNs to endpoint firewalls and network access control (NAC) functions. The company's products support organizations with complex remote user needs and that want to leverage the latest end-devices to increase staff productivity, reduce network administration and adapt policy changes on the fly. Each solution is interoperable with existing third-party software and hardware.

With global headquarters in Nuremberg, Germany and North American headquarters in the San Francisco Bay Area, NCP engineering serves 35,000+ customers worldwide throughout the healthcare, financial, education and government markets, as well as many Fortune 500 companies. NCP has established a network of national and regional technology, channel and OEM partners to serve its customers. For more information, visit www.ncp-e.com.

can automatically roll out certificates using your existing gear—such as smartcards or smartphones as one-time password (OTP) receivers—and that provides streamlined tools for managing these authentication mechanisms.

Stay safe. Stay vigilant. Reduce the pain.

A reliable VPN can ensure secure remote connections to your network, even as device, location, and connection type fluctuate. The best solution unites management tasks in one console and frees staff and administration from mundane tasks, training, and support—allowing them to focus on higher-value activities that require their expert attention and innovation—without compromising security.

Of course, a robust VPN isn't sufficient to ward off all cyberattacks. A VPN solution works in conjunction with firewalls, intrusion prevention systems, anti-virus software, and other network security components to shield your corporate infrastructure from intrusion. By being proactive from the outset, IT administrators can be more reactive to threats, while their security framework—including their VPN—provides most of the defense.

For questions or to schedule a demo, please contact NCP at 650.316.6273 or sales@ncp-e.com.

* The 2014 State of Endpoint Risk was independently conducted by Ponemon Institute LLC, sponsored by Lumension and published in December 2013.