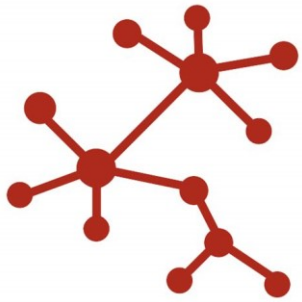
NVIS

Whitepaper



Business VPN for Everyone

Affordable, Enterprise-Strength Virtual Private Networks for SMBs
Because Hackers Can't Hack What They Can't See

Executive Summary

Enterprises have long enjoyed the increased security, dependability, and performance of Virtual Private Networks (VPNs). However, their price, complexity, and maintenance have made them prohibitively costly for large and small-to medium-sized businesses (SMBs). This inequality has become important as SMBs are progressively the target of cyber-attacks and cyber-theft. In response, NVIS has developed VPN software that allow SMBs to cost-effectively deploy without the complexity and maintenance of enterprise VPN solutions, while not sacrificing security, dependability, or performance. As businesses increasingly move assets to the cloud, the NVIS Business VPN software is the best choice to secure remote access or server-to-server internal or B2B communication. It is peer-to-peer software encrypted at Layer 2, so it avoids the Layer 3 vulnerabilities and complexity of conventional VPNs. NVIS makes your assets INVISIBLE, so they are untrackable, unblockable and unhackable.

Why Use Business VPNs?

The short answer is that connecting to networks or mobile devices outside of any organizations own secure network is risky. Corporations most in danger are people who depend upon mobile staff, remote locations, and business partners World Health Organization log into a business host networking different words, nearly each trendy business, giant or tiny. However, SMBs don't have the budget, expertise, or security tools that larger enterprises have at their disposal on a day to day. whereas hackers do target high-value huge businesses most frequently, SMBs are progressively vulnerable target for organized cyber criminals.

According to recent studies, over a third of all cyber-attacks area unit currently targeted on SMBs rise over the previous year. There's no reason to assume the attacks won't still increase. Within the past year, several SMB homeowners felt they were "too small" to become targets: however, hackers have automated their hacking processes and use software systems to scan for any and every one networks that area unit don't know what you mean here vulnerable and take no matter assets they'll from them. an equivalent study showed that sixty percent of all SMBs that area unit victim to cyber-attacks withdraw of business in six months or less. This sentence needs to be revisited

The potential consequences of weak security for businesses are disastrous. Permitting insecure logins or transactions across business networks may end up in information breaches that expose businesses to:

- **Data theft**
- **Loss of intellectual property**
- **Civil or regulatory fines**
- **Catastrophic business network failures**
- **Liability**

Table of Contents

In addition, businesses regulated by government agencies, like native banks, health care clinics, municipal offices, et al. are subject to fines if their security doesn't meet strict, audited pointers. Meanwhile, each business is liable to loss of knowledge or a whole network failure if a cyber-attack with success breaches the company's network. Antivirus software system alone cannot stop subtle, active attacks by hackers. nevertheless, several SMB homeowners and operators feel antivirus protection is all the protection they have. Analyst's data and tens of uncountable lost money every year prove this cannot be true. Corporations must add robust firewall and user authentication in the shape of VPN routers to facilitate and stem the tide of cyber-attacks.

Conventional VPNs

A conventional VPN may be a secure point-to-point association established over the net between 2 devices, sometimes a consumer (PC, laptop, etc.) to its destination network (business computer network, remote server, etc.). whereas the association is over the general public net, with every information packet sent to and from the VPN communication endpoints is encapsulated with coding. This secret writing, in effect, provides a personal "tunnel" through the general public IP network, providing an extremely secure association. As a result, any and every one public IP traffic on the net cannot access VPN content. Once the session ends, the VPN tunnel disappears. In essence, a VPN association is sort of a non-public wire carried over the general public network (see Figure 1). In fact, before the appearance of VPNs, several giant companies relied on leased, physical wired connections to remote locations, and a few still use this technology, though it's prohibitively costly for many businesses.

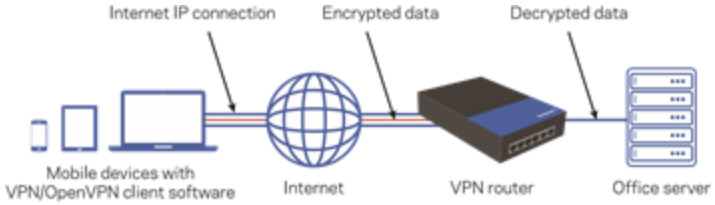


FIGURE 1. ENCRYPTED DATA IN THE VPN "TUNNEL."

A conventional VPN needs router-to-router or client-to-router connections. Software on an overseas server, laptop, or mobile device sends an authentication request to its VPN host router. The host router verifies the credibility of the consumer request by trying it in its Machine Access management (MAC) table, then sets up the secure VPN tunnel when exchanging coding keys. MAC addresses are unit specific to every device, expressed in positional representation system numbers within the router table. genuine consumer MAC IDs should be inhabited within the VPN routers much an equivalent manner that user names and passwords area unit hold on in network security login tables. Thus, why not merely deem user name and watchword logins? Passwords will simply be hacked. And open IP connections are often intercepted. solely the VPN router and its client(s), behind their firewall protection, have the coding and authentication keys for fixing VPN connections. Outsiders are simply locked out. With a VPN, all information is encrypted across the Internet.

How Do Businesses Use VPNs?

Small- to medium-sized businesses must consider VPN for variety of reasons all of that directly improve all-time low line, drive larger efficiencies, and immensely improve security. the subsequent area unit some of the ways that a VPN will improve AN SMBs competitive edge and protect business assets:

Access by Remote and Mobile Workforce

Most businesses require some level of remote access to their networks for staff and business partners. Sales personnel travel with laptops, tablets, and smartphones. Field personnel log orders from remote locations. Home-based staff should connect with the workplace for document and information sharing. every and each remote association may be a potential entry for hackers to use. As the range or remote locations increase, will a business's vulnerability to cyber-attacks will correspondingly increase. VPNs, combined with sensible router firewalls, area unit a evidenced resolution to greatly cut back cyber risk while not compromising the competitive edge remote and mobile workforces offer SMBs.

Improved Quality of Service and Performance

Today, businesses are dependent on the general public Internet. Studies show that most SMBs deem the Internet vital to run their businesses on a day-to-day basis, meaning that net performance is crucial for higher business potency. VPNs, with their secured connections can improve bandwidth and SOMETHING NEEDS TO BE ADDED HERE.

Additional Security

Antivirus and firewall protection are not enough. According to security vendor Kaspersky Labs, a recognized authority on network security, over 100,000 new threats were launched last year alone. Only secure, locked-down VPN connections with encrypted data from end-to-end can provide that crucial, additional layer of security SMB networks require for safely conducting business.[2] This is especially critical for mobile access and mobile devices.

Internet Anonymity

Intellectual property is the life-blood of many SMBs. Transferring and accessing data from remote locations anonymously is the safest way to protect data. If hackers do not know the identity or location of the data, they can't hack it. VPN provides that anonymity.

Avoid Filters in Blocking Countries

Many countries impose severe and often crippling Internet censorship by domain and IP address blocking, making it difficult to conduct business with overseas partners, or blocking mobile workers in these countries from connecting to an SMB's network. VPNs bypass these blocking mechanisms and allow the free exchange of data to and from locations throughout the world.

Why Don't All SMBs Use VPNs?

Given the advantages of VPNs combined with smart firewall features, why don't all SMBs use VPNs to safeguard their businesses and improve connectivity? Until now, a number of factors have made VPN use problematic for most SMB owners and operators, including the following:

Cost

Historically, business class VPN's have been beyond the budget for most SMB's, regardless of whether the product was hardware or a per-use solution. Whether they were looking at a CAPEX or OPEX solution, VPN's often not clear the budgetary hurdles for this size business.

Complexity

Installing most of today's VPNs requires technical expertise lacking in many SMB's IT/Security staff. An incorrectly installed VPN, whether it's a connection or a port can introduce more problems, new vulnerabilities, rather than stop existing vulnerabilities. Rather than take a chance on this happening, and without properly trained individual to do the installation, SMBs may choose the "do nothing" as the best alternative. Leaving their network vulnerable.

Maintenance

As with any hardware or software purchase the initial purchase and installation is just part of the TCO (Total Cost of Ownership). Over a multi-year period this may end up being just a fraction of the TCO, as there will be management (perhaps requiring new headcount and maintenance expenses. If a company elects not to hire additional headcount, they may find themselves having to purchase a service or support contract. This may be an unanticipated expense, and maintenance costs rarely drop over time.

NVIS Business VPN Software

With the rise in SMB cyber-attacks and the lack of affordable security for SMBs, NVIS saw a distinct need in the market for affordable, easy-to-use, yet highly secure VPN routers. Its business-class VPN Routers provide all the security and performance of high-end VPN routers scaled to fit the needs of SMBs (see Figure 2). In the process, NVIS has removed some of the other barriers-to-entry for SMBs by vastly simplifying the installation and maintenance of its VPN routers, making them "IT budget-friendly" even after purchase.

Cost-Effective VPN

VPN Software is a perfect fit for SMBs on a budget. Purchase of a NVIS VPN software gives SMBs ownership of their VPN environment, without expensive VPN hardware to buy / lease and the IT staff needed to maintain. NVIS can work on LANs or in the Cloud.

Easy to Use

NVIS designed its software for ease of use. No in-house technical expertise of VPN technology is needed. With auto-config, from installation to the addition of new VPN connections, operation is intuitive, quick to deploy, and secure.

Easy to Maintain

Maintenance is as simple as installation. Again, no VPN technology expertise is required, as a web-based Admin Dashboard makes it easy for administrators (see Figure 3).

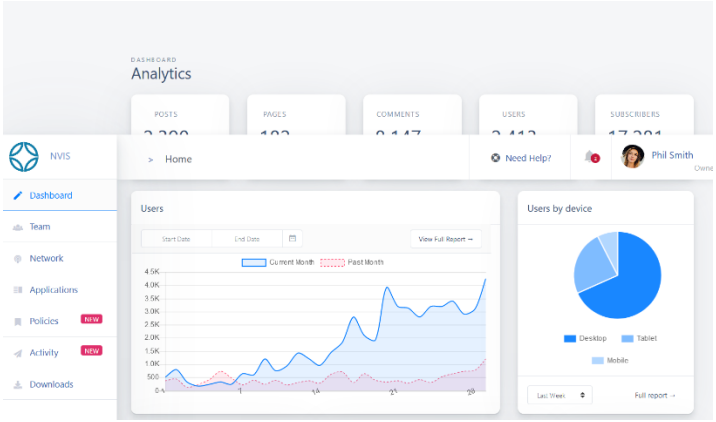


Figure 3 – NVIS Admin Dashboard

Premium Features

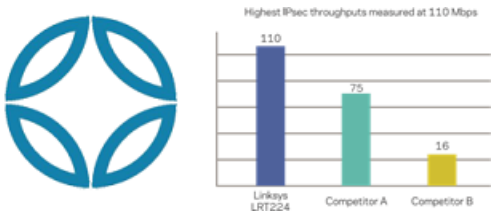
So, what do SMBs sacrifice when buying NVIS VPN Server over enterprise-class solutions? Other than the number of VPN tunnels, absolutely nothing is lost. In fact, NVIS software lowers maintenance versus their high-priced counterparts and doesn't require tunneling since everything is peer-to-peer.

Secure Multiple Location Communication

Deploy the same time-tested and trusted VPN technology as large enterprises to securely set up links and data sharing across multiple locations. Easily provide secure communication to remote users and offices. Share data with business partners and third-party providers, such as accounting firms, outsourced HR, and contact sales employees or supply vendors.

High-Performance Remote Access for Mobile Users

NVIS VPN Software gives smartphone, tablet, and laptop users the most secure, yet affordable option for connecting with SMB offices remotely. Its mobile clients are free to install on any mobile device (Android, iOS, laptop PCs and Macs).



NVIS VPN Software out-performs similar competitors by over 25 percent or more (see Figure 4) using industry-standard IPsec or SSL VPN secure tunneling.

Figure 4. Mobile performance of NVIS versus competitors. Where is figure 4. You also have this "blue" Check for color consistency across all "Figure xx's"

Fault-Tolerant Performance and Scaling

NVIS can be installed on the SMB's LAN, or in the Cloud on NVIS's own Virtual Private Server (VPS) or popular high-end VPS like Amazon Web Services (AWS) and (coming soon) Google Cloud Services (See Figure 5).

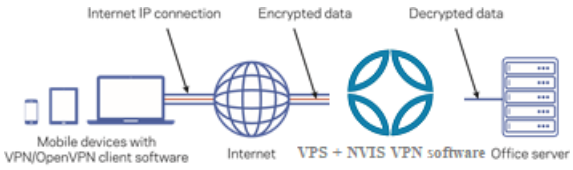


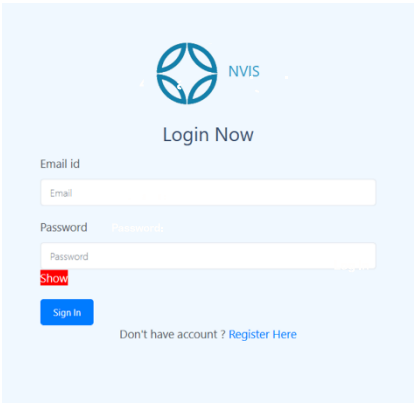
Figure 5 - NVIS VPN software

A Simple Three-Step Installation Process

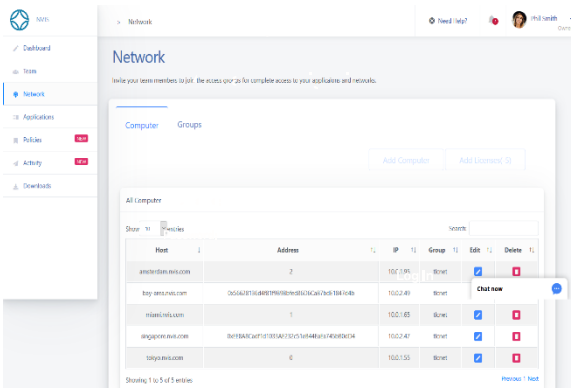
Unlike many other VPN routers, the NVIS VPN Software has a simple, three-step setup process to provision and install. There is no manual MAC address entry or IP address assignment. It is al AUTOMATIC using an Intelligent Provisioning Agent for Zero-Config (see Figure 6).

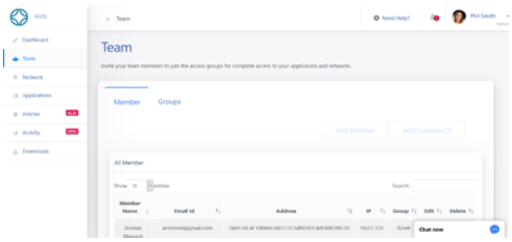
Step 1. MANAGE: Admin logs into the account's "Admin Dashboard" to provision the above assets in the plan.
Step 2: INVITE: Admin pushes the "Invite Team Member" sends an invitation email to the end-user.
Step 3: INSTALL: Team Members get the email and SIGN IN to their "User Dashboard" showing them their ID along with links to download, and other information.

Step 1: MANAGE: Log-in to the AdminDashboard



Add Groups, Computers and Team Members





Step 3: INSTALL: Team Members Login to User Dashboard to Download and install NVIS

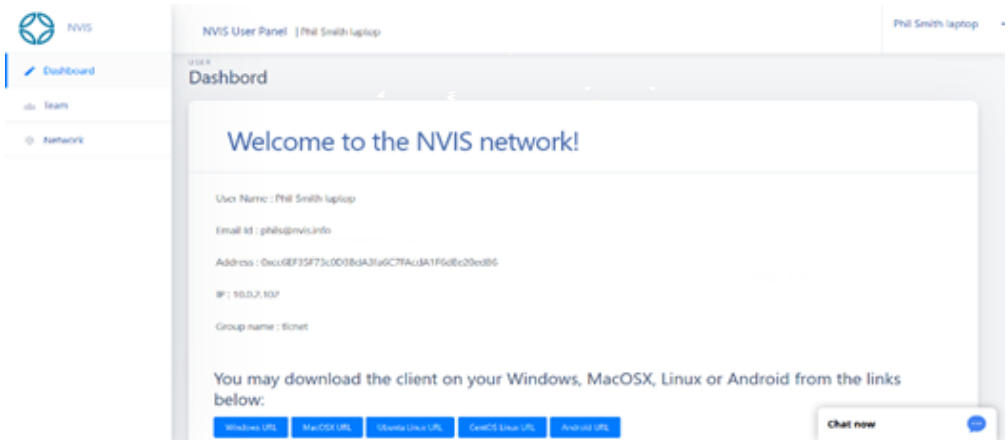
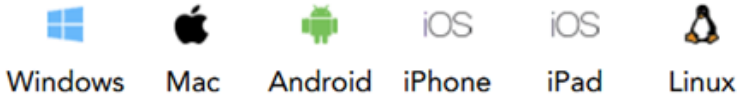


Figure 6. The NVIS automated three-step NVIS setup process.

All major platforms are available for user download and install:



Server Platforms

NVIS Server and Client Software runs on a growing list of virtual platforms;

Summary

NVIS is truly "Business VPN for Everyone". By minimizing cost, complexity, and cost of ownership, SMBs now can enjoy enterprise-class VPNs for nearly the cost of just a router alone. The NVIS VPN Software deliver the following:

- **Affordable VPN technology**
- **Enterprise-class features**
- **Easy to deploy and maintain**
- **Highest performance in its class**
- **Greater security for virtually any SMB**

For more information or for a reseller near you, contact:

1 StaySafeOnline.org/Symantec. “Small Business Online Security.” http://www.staysafeonline.org/stay-safe-online/resources/small-business-online-securityinfographic

2 Kaspersky Labs. “Kaspersky Lab Reports Mobile Malware in 2013 More Than Doubles from Previous Year.” http://usa.kaspersky.com/about-us/press-center/ press-releases/kaspersky-lab-reports-mobile-malware-2013-more-doubles-previous