VPN FOR THE REST OF US

Affordable, Enterprise-Strength Virtual Private Networks for SMBs

Executive Summary

Enterprises have long enjoyed the increased security, reliability, and performance of virtual private networks (VPNs). But their cost, complexity, and maintenance have made them prohibitively expensive for small-to-medium-sized businesses (SMBs). This disparity has become critical as SMBs are increasingly the target of cyber-attacks and cyber theft, which VPNs could dramatically reduce. In response, Linksys has developed VPN routers that SMBs can cost-effectively deploy without the complexity and maintenance of enterprise VPN solutions, and, most importantly, without sacrificing security, reliability, or performance.

Why Should SMBs Use Virtual Private Networks?

The short answer is that connecting to networks or mobile devices outside of any organization's own secure network is risky. Companies most at risk are those that depend on mobile workers, remote locations, and business partners who log into a business' host network—in other words, nearly every modern business, large or small. But SMBs do not have the budget, expertise, or security tools that larger enterprises have at their disposal on a daily basis. While hackers do target high-value big businesses most often, SMBs are an increasingly vulnerable target for organized cyber criminals.

According to research results, as of 2013, 31 percent of all cyber-attacks are now focused on SMBs—an 18 percent rise over the previous year. There is no reason to assume the attacks will not continue to escalate. In the past, many SMB owners felt they were "too small" to become targets, but hackers have automated their hacking processes and use software to scan for any and all networks that are vulnerable and take whatever assets they can from them. The same study showed that 60 percent of all SMBs that are victim to cyber-attacks go out of business in six months or less.[1]

The list of potential consequences of lax security for SMBs is alarming. Allowing insecure logins or transactions across business networks can result in data breaches that expose SMBs to:

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

Table of Contents

In addition, businesses regulated by government agencies, such as local banks, healthcare clinics, municipal offices, and others are subject to fines if their security does not meet strict, audited guidelines. Meanwhile, every business is susceptible to loss of data or a complete network failure if a cyber-attack successfully breaches the company's network. Anti-virus software alone cannot stop sophisticated, hands-on attacks by hackers. Yet many SMB owners and operators feel anti-virus protection is all the security they need. Research data—and tens of millions of lost dollars each year—prove this is not true. Companies should add strong firewall and user authentication—in the form of VPN routers—to help stem the tide of cyber-attacks.

What Is a VPN?

A basic VPN is a secure point-to-point connection established over the Internet between two devices, usually a client (PC, laptop, etc.) to its destination network (business LAN, remote server, etc.). While the connection is over the public Internet, each data packet sent to and from the VPN communication endpoints is encapsulated with encryption. This encoding, in effect, provides a private "tunnel" through the public IP network, providing a highly secure connection. As a result, any and all public IP traffic on the Internet cannot access VPN content. When the session ends, the VPN tunnel disappears. In essence, a VPN connection is like a private wire carried over the public network (see Figure 1). In fact, before the advent of VPNs, many large corporations relied on leased, physical wired connections to remote locations, and some still use this technology, although it is prohibitively expensive for most businesses.

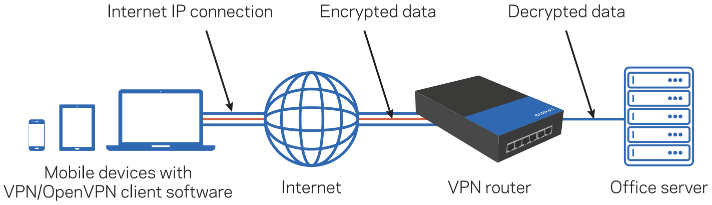


Figure 1. Encrypted data in the VPN "tunnel."

A VPN requires router-to-router or client-to-router connections. Client software on a remote server, laptop, or mobile device sends an authentication request to its VPN host router. The host router verifies the authenticity of the client request by looking it up in its Machine Access Control (MAC) table, and then sets up the secure VPN tunnel after exchanging encryption keys. MAC addresses are specific to each device, expressed in hexadecimal numbers in the router table. Authenticated client MAC IDs must be populated in the VPN routers—much the same way that user names and passwords are stored in network security login tables. So why not simply rely on user name and password logins? Passwords can easily be hacked. And open IP connections can be intercepted. Only the VPN router and its client(s), behind their firewall protection, have the encryption and authentication keys for setting up VPN connections. Outsiders are just that—locked out. With a VPN, all data is encrypted across the Internet.

How Should SMBs Use VPNs?

Small- to medium-sized businesses should consider VPN routing for a number of reasons—all of which directly improve the bottom line, drive greater efficiencies, and vastly improve security. The following are just some of the ways a VPN can improve an SMB's competitive edge:

Support for Remote and Mobile Workers

Most businesses rely at least in part on mobile access to their networks for workers and business partners. Sales personnel travel with laptops, tablets, and smartphones. Field personnel log orders from remote locations. Home-based workers must connect to the office for document and data sharing. Each and every remote connection is a potential gateway for hackers to exploit. As the number or remote locations increase, so does a business's vulnerability to cyber-attacks. VPNs, combined with smart router firewalls, are a proven solution to greatly reduce cyber risk without compromising the competitive edge remote and mobile workforces give SMBs.

Improved Quality of Service and Performance

It is amazing how quickly businesses have become reliant on the public Internet. Research shows that 87 percent of SMBs rely on Internet connectivity to run their businesses on a daily basis.[1] That means that Internet performance is essential for better business efficiency. VPNs, with their secured connections and ability in some routers to combine bandwidth, can squeeze the most out of any Internet connection, taking priority over other dynamically allocated traffic.

Additional Security

Antivirus and firewall protection can only go so far. According to 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 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 draconian 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

Typical VPN solutions have simply cost too much for many SMBs to consider. Operating on tight budgets and subject to constant cash-flow unpredictability, SMBs do not have the money to spend on traditional VPN technology. Whether it is a pay-per-use VPN software solution or investment in expensive VPN routers, SMBs have been priced out of the market.

Complexity

VPNs are effective. But setting up most VPN solutions on the market today requires careful installation. One wrong port assignment or connection can actually introduce more vulnerabilities rather than prevent them. And SMBs simply do not have the technical expertise or trained personnel to properly deploy VPNs on their networks.

Maintenance

Buying and installing a VPN is only part of the technology budget. Maintaining a typical VPN solution requires constant management, maintenance, and oversight. That means relying on a monthly service contract or hiring and training an IT professional. Maintenance, in fact, may far outstrip the already high price of the equipment and software alone.

Linksys Business VPN Routers

With the rise in SMB cyber-attacks and the lack of affordable security for SMBs, Linksys saw a distinct need in the market for affordable, easy-to-use, yet highly secure VPN routers. Its business-class Gigabit 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, Linksys 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.

LINKSYS LRT214
Gigabit VPN Router

LINKSYS LRT224
Dual WAN Gigabit VPN Router

Figure 2. Linksys Gigabit and Dual WAN VPN Routers.

Cost-Effective VPN

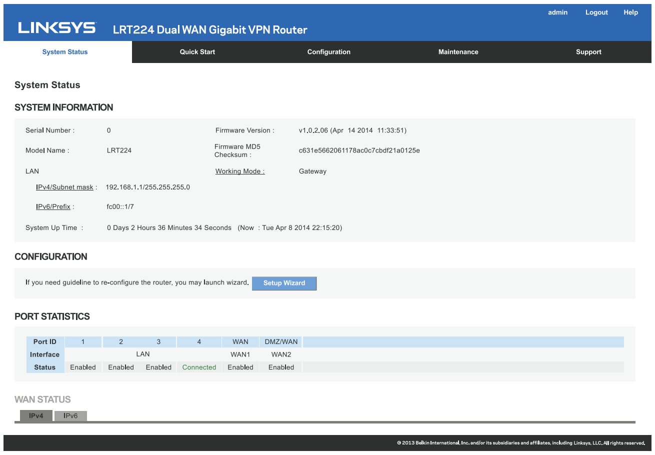
The truth is, most SMBs do not need the number of ports or redundancies that typical enterprises do. Therefore, Linksys Gigabit and Dual WAN Gigabit Routers are a perfect fit for SMBs on a budget. Purchase of a Linksys VPN router gives SMBs ownership of their VPN environment, with no monthly software fees or expensive VPN clients to buy or rent.

Easy to Use

Linksys designed its Gigabit VPN Routers for ease of use. No in-house technical expertise of VPN technology is needed. 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 intelligent firmware and Web-based secure management software with extensive online help is all it takes to easily and quickly maintain Linksys Gigabit VPN Routers (see Figure 3).



System Status

SYSTEM INFORMATION

Serial Number : 0
Firmware Version : v1.0.2.06 (Apr 14 2014 11:33:51)
Model Name : LRT224
Firmware MD5 Checksum : c631e5662061178ac0c7cbdf21a0125e
LAN
Working Mode : Gateway
IPv4/Subnet mask : 192.168.1.1/255.255.255.0
IPv6/Prefix : fc00::1/7
System Up Time : 0 Days 2 Hours 36 Minutes 34 Seconds (Now : Tue Apr 8 2014 22:15:20)

CONFIGURATION

If you need guideline to re-configure the router, you may launch wizard.

PORT STATISTICS

Port ID	1	2	3	4	WAN	DMZ/WAN
Interface	LAN				WAN1	WAN2
Status	Enabled	Enabled	Enabled	Connected	Enabled	Enabled

WAN STATUS

© 2013 Belkin International, Inc. and/or its subsidiaries and affiliates, including Linksys, LLC. All rights reserved.

FIGURE 3. Linksys Web-based VPN management software.

Premium Features

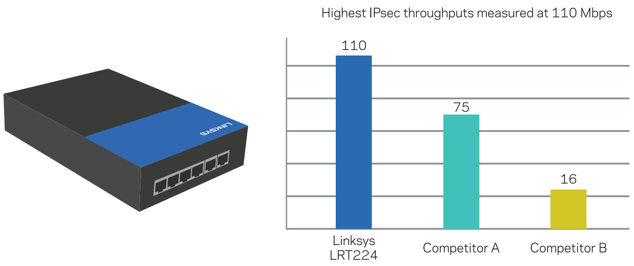
So what do SMBs sacrifice when buying Linksys Gigabit VPN Routers over enterprise-class solutions? Other than the number of VPN tunnels, absolutely nothing is lost. In fact, Linksys Gigabit VPN Routers have greater ease-of-use and lower maintenance than their high-priced counterparts.

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

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



And based on vendor-supplied specifications, Linksys Gigabit VPN Routers out-perform similar competitors by over 25 percent or more (see Figure 4) when using industry-standard IPsec secure tunneling.

Figure 4. Mobile performance of Linksys versus competitors.

Fault-Tolerant Performance and Automatic Bandwidth Management

Because so many SMBs rely on the Internet to operate their businesses, downtime or poor performance is not an option. The Dual WAN Linksys Gigabit VPN Router is a perfect choice when both increased performance and reliable connectivity is essential. With dual Gigabit I/O channels, the Linksys Dual WAN Router performs two functions: First, if a connection to the Internet (and thereby remote office or device) goes down, the second channel automatically steps in and channels packets securely with no loss of data. Secondly, by using dual channels, sites that deploy the Linksys Dual WAN Router enjoy automatic load balancing of traffic—the router determines the ebb and flow of incoming and outgoing traffic and distributes it evenly among its two channels, providing an even flow of traffic and maximizing an SMB's Internet bandwidth (See Figure 5).

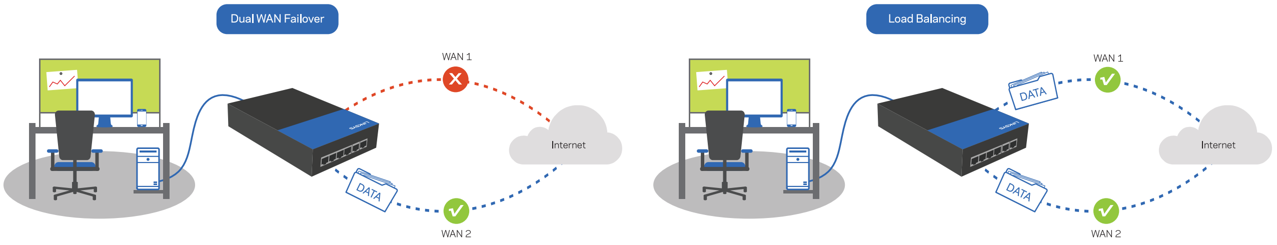


Figure 5. The Linksys Dual WAN VPN Router features resiliency and load balancing.

Firewall Protection With No Performance Loss

Linksys Gigabit VPN Routers also include integrated firewall support that SMBs can deploy with confidence, out of the box, with simple settings. The firewall provides a robust set of granular filters and rules, however, to provide SMBs even greater control over incoming traffic to its networks (see Figure 6). Rules for access, content filtering and packet inspection deliver a high level of custom protection, all within an easy-to-use, secure Web-based management console. Filtering and blocking, in particular, can stop Denial of Service (DoS) flooding attacks, which can cripple a network with an onslaught of hacking traffic requests. These extensive firewall options allow SMBs to securely host a company website internally, or make certain their security is as tight as their business requires. In SMBs that must conform to industry or government compliance mandates, documented firewall protection is often a key audit requirement.

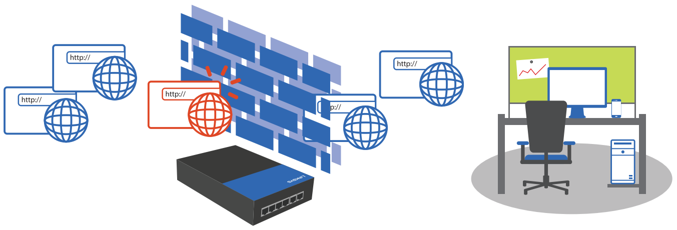
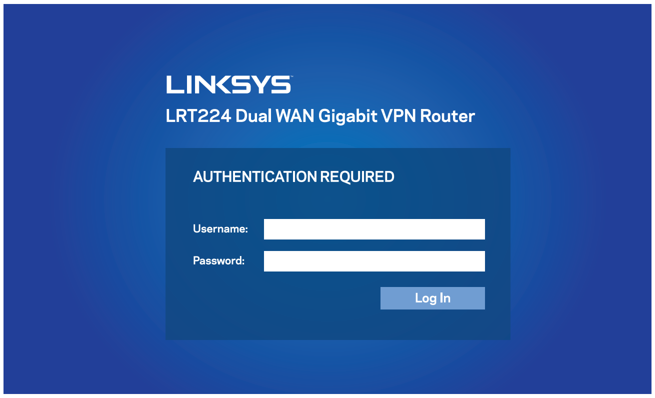


Figure 6.
Linksys firewall protection for greater security and reliability.

A Simple Three-Step Installation Process

Unlike many other VPN routers, the Linksys Gigabit VPN Routers have just a simple, automated three-step setup process. There is no manual MAC address entry or MAC address table flooding (see Figure 7).

Step 1: Login



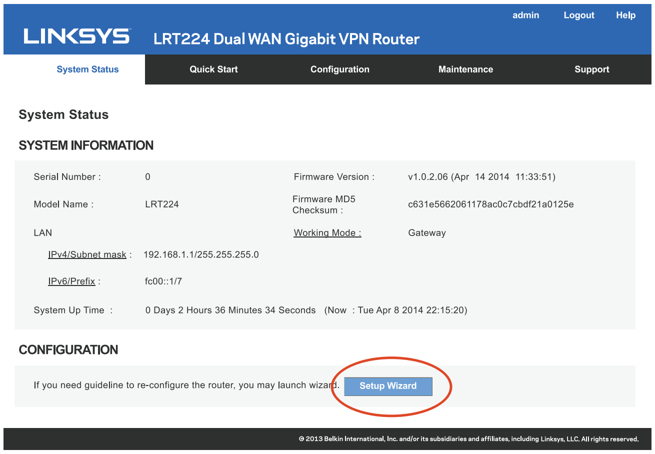
LRT224 Dual WAN Gigabit VPN Router

AUTHENTICATION REQUIRED

Username:

Password:

Step 2: Launch the wizard



LRT224 Dual WAN Gigabit VPN Router

System Status

SYSTEM INFORMATION

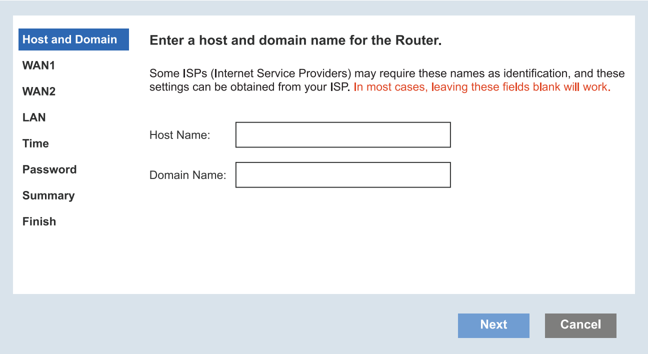
Serial Number :	0	Firmware Version :	v1.0.2.06 (Apr 14 2014 11:33:51)
Model Name :	LRT224	Firmware MD5 Checksum :	c631e5662061178ac0c7cbdf21a0125e
LAN		Working Mode :	Gateway
IPv4/Subnet mask :	192.168.1.1/255.255.255.0		
IPv6/Prefix :	fc00::1/7		
System Up Time :	0 Days 2 Hours 36 Minutes 34 Seconds (Now : Tue Apr 8 2014 22:15:20)		

CONFIGURATION

If you need guideline to re-configure the router, you may launch wizard.

© 2013 Belkin International, Inc. and/or its subsidiaries and affiliates, including Linksys, LLC. All rights reserved.

Step 3: Follow the intuitive setup



Enter a host and domain name for the Router.

Some ISPs (Internet Service Providers) may require these names as identification, and these settings can be obtained from your ISP. In most cases, leaving these fields blank will work.

Host Name:

Domain Name:

FIGURE 7. The Linksys automated three-step VPN router setup process.

Summary

The Linksys Gigabit VPN Routers are truly "VPN for the rest of us." 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 Linksys Gigabit VPN Routers 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:

Contact Information here
xxx-xxx-xxxx

[1] StaySafeOnline.org/Symantec. "Small Business Online Security." http://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

[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

Insight®

Work smarter

At Insight, we'll help you solve challenges and improve performance with intelligent technology solutions.

Learn more