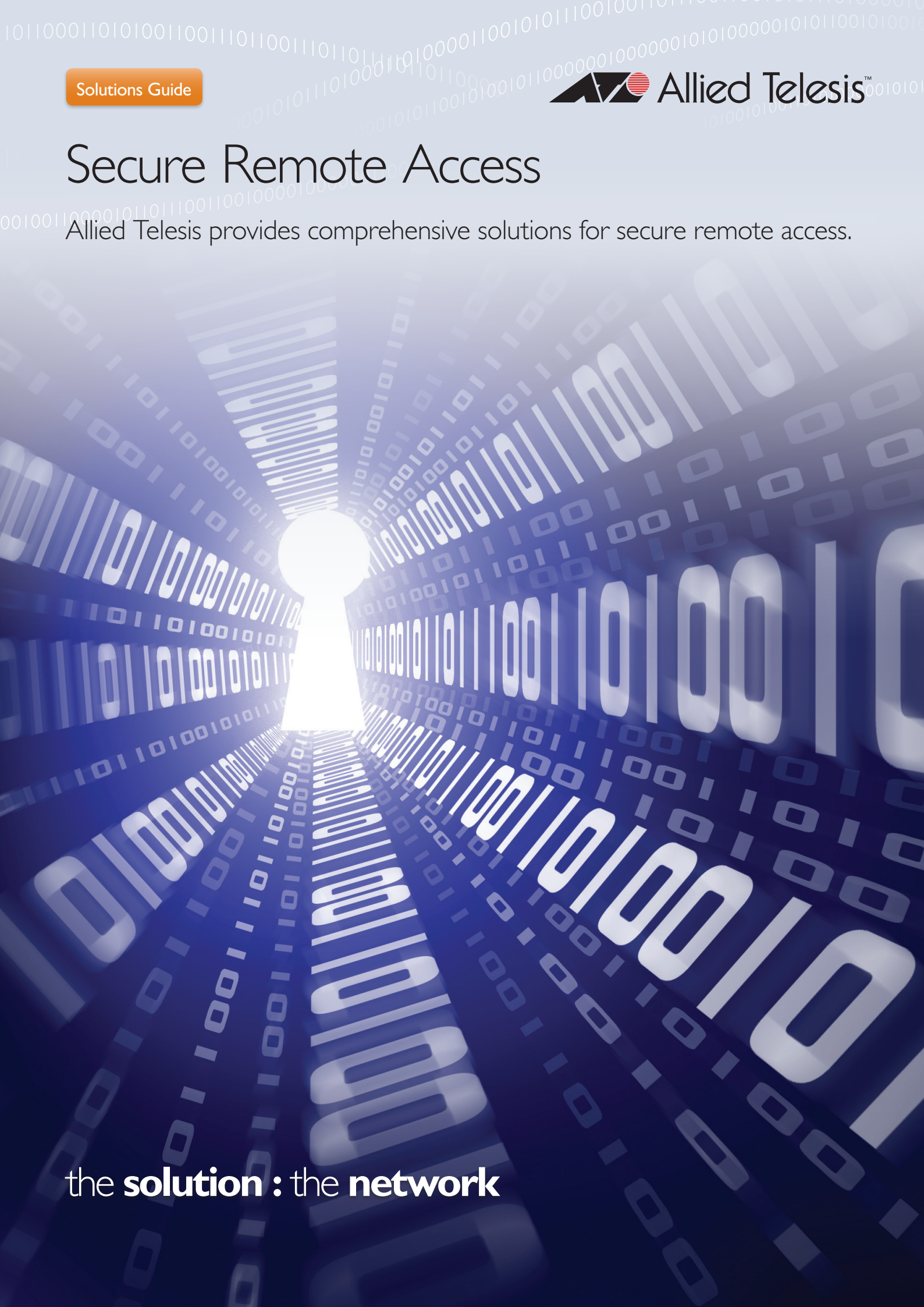
Solutions Guide

Allied Telesis

Secure Remote Access

Allied Telesis provides comprehensive solutions for secure remote access.



the **solution** : the **network**

Introduction

The world is generating electronic data at an astonishing rate, and that data is increasingly underpinning so much of what happens in our lives.

In the last few decades, a virtuous cycle has occurred:

- The ease with which electronic data can be gathered, stored and accessed has benefited, and transformed, many spheres of human activity.
- This in turn has stimulated yet more ways to collect, provide, and use data.

In a remarkably short space of time, we have moved from a world in which information was stored on paper and kept in filing cabinets and folders, to a world in which all information — immense amounts of information — exists in "the cloud".

Storing, accessing, and updating paper-based data was a slow, expensive process. By contrast, interaction with cloud-based data can be incredibly convenient. As a result, many of the ways in which society and business now operate are dependent on access to electronic data. That data must also be available, accurate, and able to be accessed easily and securely.

Allied Telesis secures data connectivity

Allied Telesis provides comprehensive network security solutions — securing the internal LAN infrastructure, the interface to the Internet, and connections across the Internet. Our security technology has evolved with the Industry throughout the decades we have been in business. We have extensive experience in end-to-end network security, and a strong track record in safeguarding our customers' networks.

Working away from the office has increased in popularity, and the desire to connect smaller branch offices to the corporate LAN has greatly increased. Allied Telesis provides powerful solutions for secure remote connectivity to company information from anywhere, at any time.

This document showcases a number of secure remote access solutions and technologies.

Allied Telesis security appliances

AR Series VPN Routers

Allied Telesis multiservice VPN routers have a modular design to allow a wide range of WAN connectivity options, simply by changing the Port Interface Card (PIC). Connectivity options include Ethernet, xDSL, ISDN, Frame-Relay and more. Allied Telesis routers provide extensive IPsec-based VPN capability, allowing the interconnection of offices, remote teleworkers, and other users who require secure access to a corporate network.

AR Series Next-Generation Firewalls

Allied Telesis Next-Generation Firewalls (NGFWs) provide the ideal integrated security platform for today's networks. Next-Generation Firewall and threat protection is combined with routing and switching, to provide an innovative high-performance solution. Application and Web control ensures Enterprises can control applications and how they are used, as well as manage web traffic for productivity, legal and security purposes.

As well as control of business traffic and applications, our NGFWs offer VPN solutions for companies to provide secure remote access to their online resources.

Secure inter-branch connectivity

Allied Telesis secure VPN routers and NGFWs provide powerful VPN solutions to connect corporate offices, whether it be for securely connecting branch offices to a head office, or for businesses extending their LAN across more than one location.

IPsec site-to-site VPN

Allied Telesis security appliances implement highly secure VPN connections using advanced encryption algorithms. Multiple simultaneous site-to-site VPN tunnels can be employed, and at the same time multiple remote user VPNs can support out-of-office workers (described in the "Secure remote access for users" section).

Configuring tunnels between offices is a simple process of following the steps in a GUI application embedded in the routers. Once VPN connections are configured and running, no maintenance is required. Encryption keys are renegotiated on a regular basis to keep one step ahead of snoopers.

To eliminate the risk of initial encryption keys, known as "pre-shared keys", being leaked, the routers can use digital certificates for authentication. The VPN network can be fully integrated with a certificate server system to receive certificate revocation lists, and so on.

A full range of other security options is available: extended authentication of VPN peers, anti-replay protection, keep-alive monitoring, and much more.

Flexible data tunnelling options include:

- **Tunnelling multicast data:** multicast-based server applications and for remote video cameras.
- **Mixed IPv4 and IPv6 tunnelling:** providing IPv4 in IPv6 tunnelling, and IPv6 in IPv4 tunnelling.

Allied Telesis VPN technologies adhere closely to published standards, and have proven interoperability with a multitude of other VPN devices.

Inter-office VPN connections

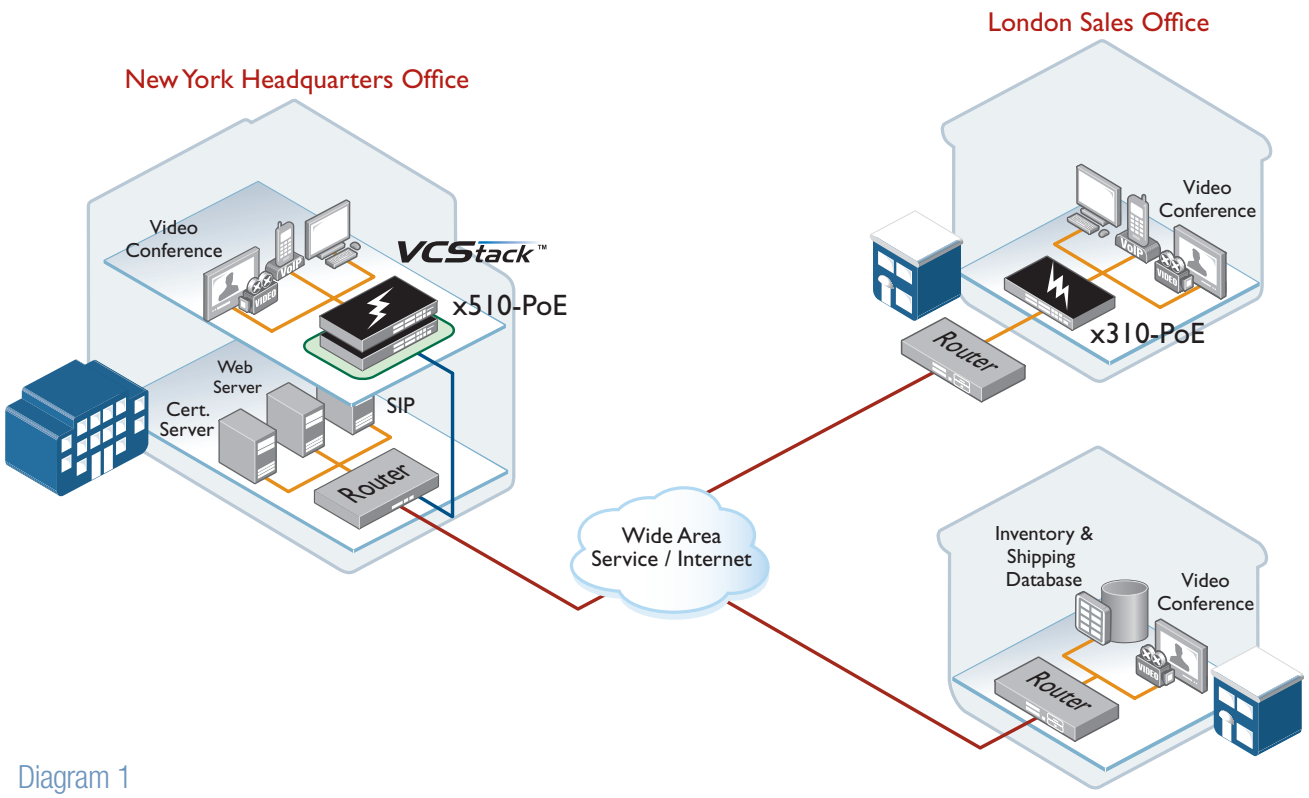


Diagram 1

In the scenario shown in diagram 1, the head office Allied Telesis router will provide a highly available, data-symmetrical connection to the Internet over a leased line or Ethernet connection. The connection ensures sufficient bandwidth for all traffic. The Allied Telesis routers act as secure VoIP gateways, allowing the corporate VPN network to be used for voice, video and data services.

The Quality of Service (QoS) capabilities of the Allied Telesis routers mean they can easily manage the prioritization and bandwidth allocation for different types of traffic. Real time VoIP and video applications can operate effectively over the same connection that is carrying bulk data, for example file transfers, email, or web browsing. QoS protects voice and video streams from surges in the bulk data load, giving a smooth user experience.

A wide range of WAN connectivity options are available in Allied Telesis modular VPN routers including ADSL, SHDSL, E1, T1, X.21, V.35, Frame Relay, X.25, PPP, PPPoE, PPPoA and 10/100/1000 Ethernet. A highly distributed organization can utilize the best connectivity options that are available at different locations.

Corporate LAN extension

Using Allied Telesis security appliances to bridge Ethernet LANs across a wide-area connection is an effective means of simplifying a multiple site network, providing the same network environment for staff at both locations. The equipment attached to the networks at both sites can operate as though connected to the same Layer 2 LAN, and no special configurations are required to allow for a Layer 3 network environment.

Using bridging to unify multi-site LANs is particularly valuable when there are multiple VLANs in use, as shown below in diagram 2. Each VLAN can simply extend across the multiple sites, and the access policies and addressing schemes defined for each VLAN apply equally at each site. As users move from one office to another, they see the same identical network environment whenever they connect.

A Layer 3 hop between the sites would completely break the uniformity of the VLANs, and greatly complicate the task of providing an equivalent connectivity experience throughout a given VLAN, regardless of physical location. Therefore, bridging of tagged VLANs is a very valuable network service. Some service providers do offer such a capability, but at considerable cost. Businesses can avoid this cost by using the tagged VLAN bridging functionality of Allied Telesis routers, and extending VLANs across multiple sites while using a standard wide area connection.

The number of bridged VLANs, and the VLAN IDs of the bridged VLANs, is entirely under your control. There is no need to put requests into the service provider to change the service configuration.

This solution provides true LAN extension with full security, fully under your control, using standard Internet connections.

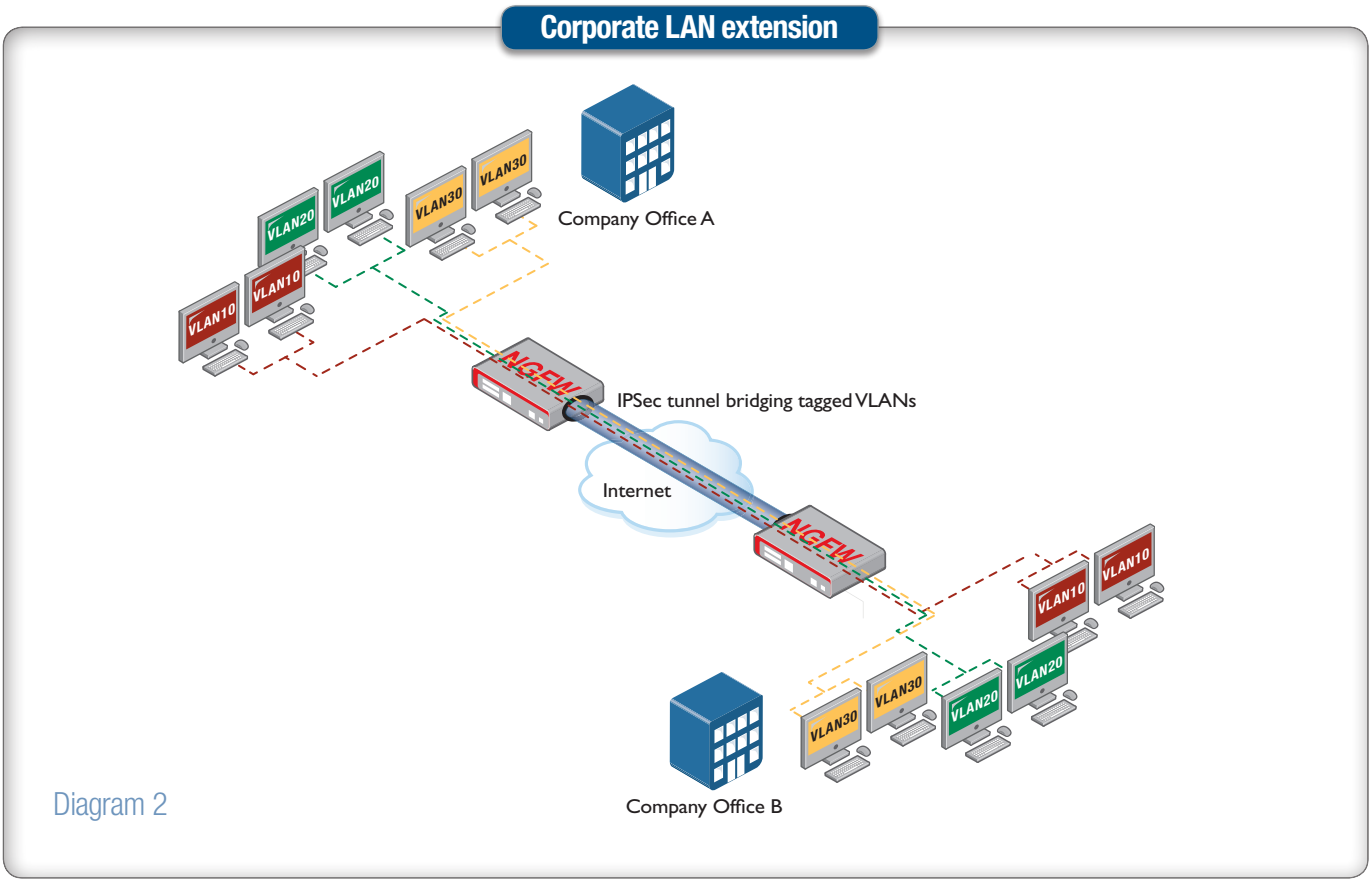


Diagram 2

Secure remote access for users

Today's business environment has an ever increasing need for remote access to the corporate LAN. Staff may have days when they work from home, and travelling professionals require instant access to online company resources.

To securely support this growth in remote network access, Allied Telesis secure VPN routers support IPsec VPNs, and our NGFWs support SLL VPNs for out-of-office users.

IPsec VPN access from home or a hotel

The scenario shown in diagram 3 illustrates our secure VPN routers providing company network access for two different types of teleworkers—home workers and travelling professionals. All the security and powerful features of an Allied Telesis IPsec VPN are employed to provide remote users with safe and reliable business connectivity.

Home teleworker

A home-based, data-only teleworker uses an Allied Telesis ADSL router to connect to the office over a broadband Internet connection. The teleworker's company PC is running VPN software, which is terminated by an Allied Telesis secure modular VPN router at the office.

The teleworker may also share the broadband Internet connection with other family PCs, linked via wired or wireless LAN connections. Because the VPN is software based and only enabled on the work PC, any other network users are prohibited from accessing the corporate network.

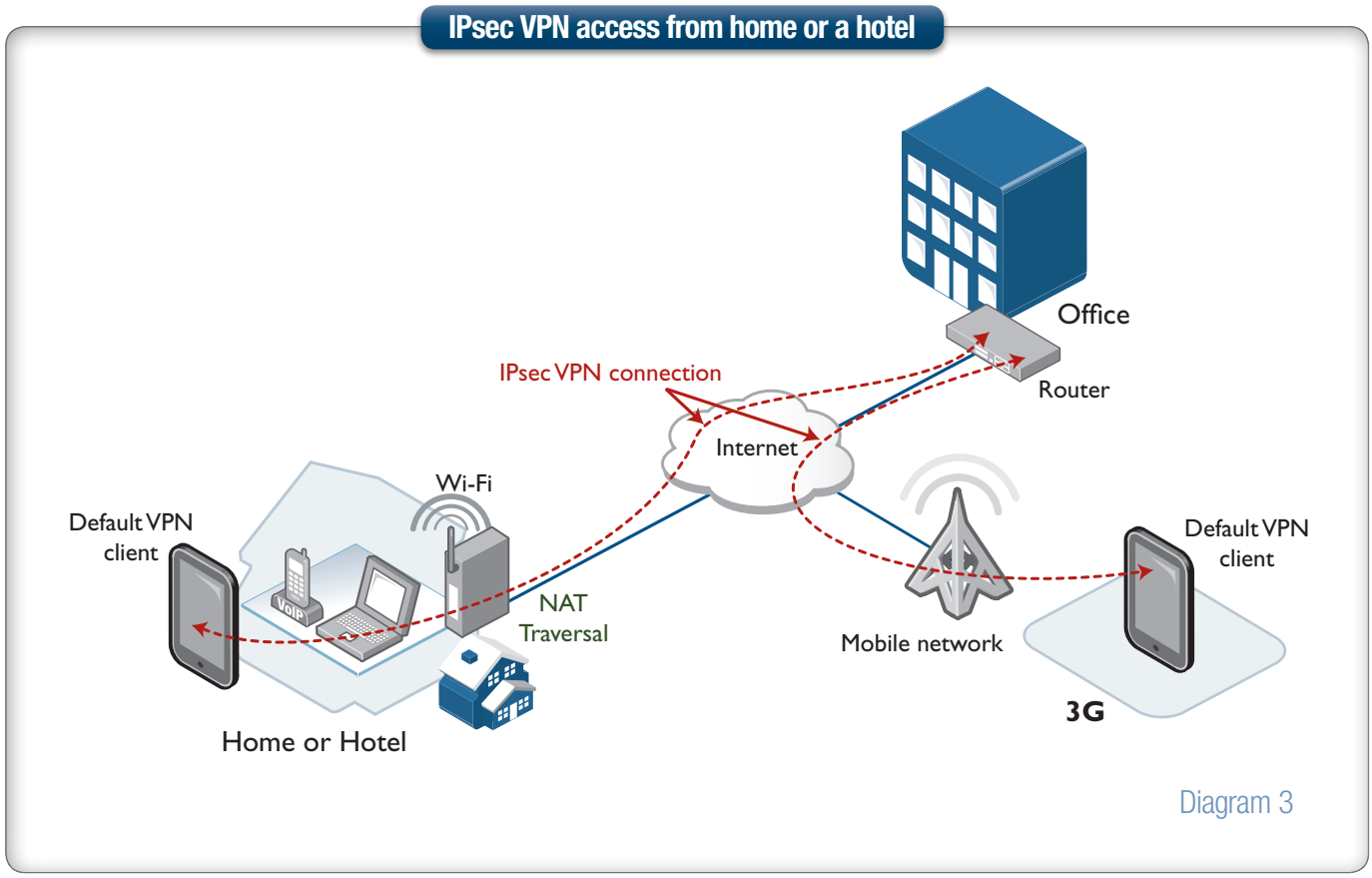


Diagram 3

Professional teleworker

The professional teleworker requires both data and a low cost digital voice connection or Voice over IP (VoIP). The Allied Telesis head office VPN router is acting as a secure VoIP gateway. QoS capabilities within the router prioritize the delivery of high quality digital voice.

Example IPsec VPN network for medical professionals

Combining the abilities of IPsec VPNs, to provide both site-to-site branch office and remote user connectivity, allows medical professionals to have access to the hospital network from their consulting rooms, as well as when visiting patients' homes, as shown in diagram 4.

With a simple lightweight smartphone or tablet, medical personnel can remotely access records held on hospital database servers while on home visits. The device is unobtrusive during the consultation, and does not rely on Internet connectivity at the patient's home.

Medical practitioners can always connect securely to national or regional medical data systems. Allied Telesis secure VPN routers have proven their reliability and security in medical applications.

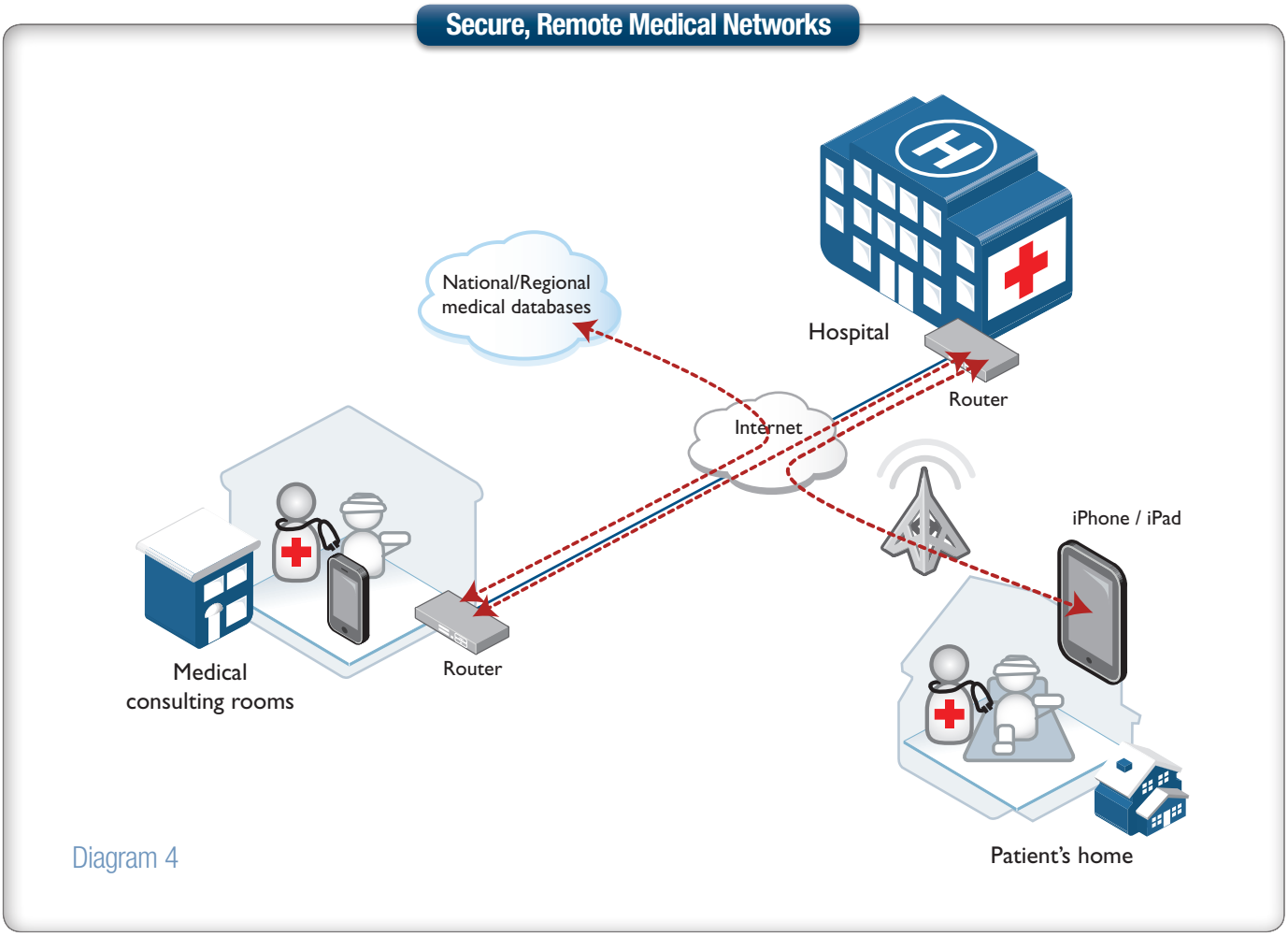


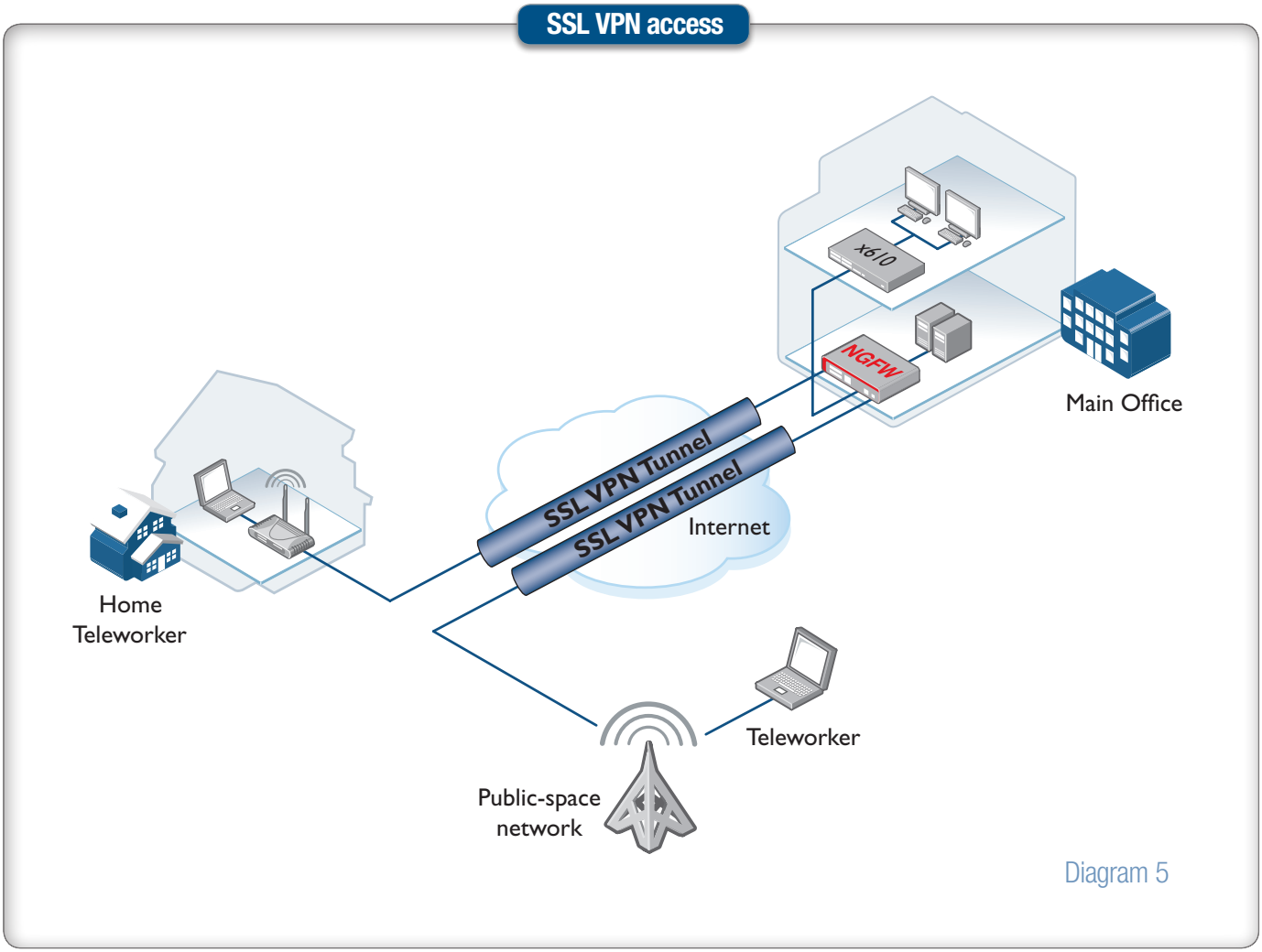
Diagram 4

SSL VPN access

Allied Telesis Next-Generation Firewalls (NGFWs) support SSL VPNs, which are a convenient alternative to IPsec VPNs for remote access to business networks.

Users simply utilize the OpenVPN client on their computer, tablet or other mobile device. Using the HTTPS protocol, SSL VPNs are compatible with the security policies of almost all network installations. This makes them ideal for travelling staff, who may need to access the corporate network from a variety of public space networks as well as from home, as shown in diagram 5.

Whereas firewalls in residential, hospitality or public networks will often frustrate mobile users by unwittingly blocking transfer of IPsec traffic, it is almost unknown for SSL VPNs to be blocked.



User identification and authentication, full Ethernet bridging, and NAT traversal are all inherent in the operation of SSL VPNs. There is no extra protocol layering, complexity and processing overhead, as is the case with IPsec VPN.

To provide advanced SSL VPN capabilities, the Allied Telesis solution incorporates a client side agent application, as shown in diagram 6. This has the following advantages:

- It is independent of web browsers, and their inherent security vulnerabilities.
- It uses Layer-2 tunneling mode, to enable secure LAN extension over the Internet.
- There is a choice of UDP or TCP transport.
- It contains a high level of application flexibility.

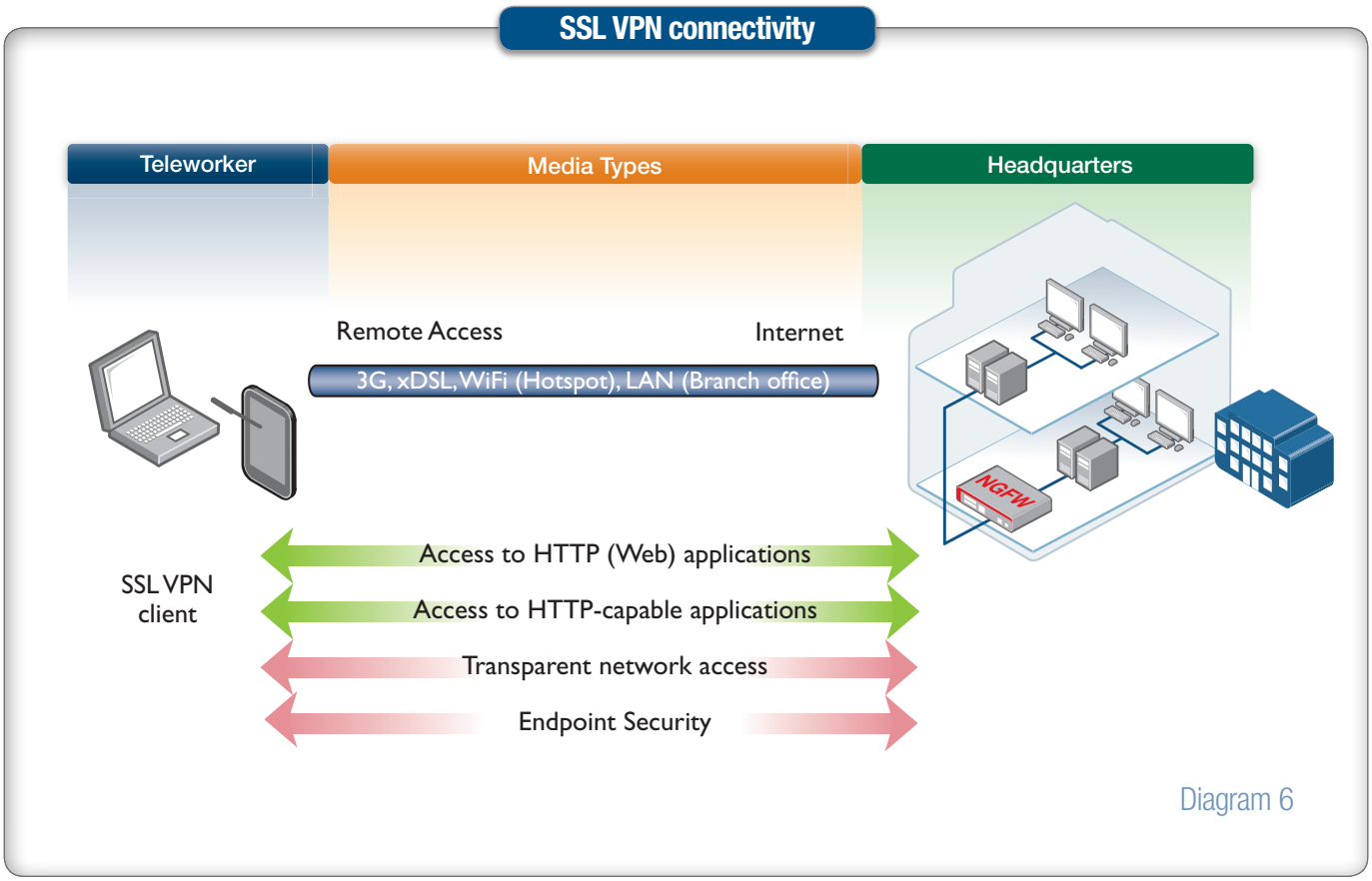


Diagram 6

Summary

Allied Telesis comprehensive network security solutions have evolved to keep pace with the way we conduct business and live our lives. As remote network access and user mobility have increased, our technologies have kept pace with modern corporate practices.

Our secure VPN routers and Next-Generation Firewalls (NGFWs) make it easy to connect branch offices to a head office, or extend the corporate LAN, so all employees have full network access from all company locations. Powerful remote access solutions ensure workers always have access to online resources and applications.

Allied Telesis solutions support secure business data access from anywhere, at any time.

About Allied Telesis, Inc.

Founded in 1987, and with offices worldwide, Allied Telesis is a leading provider of networking infrastructure and flexible, interoperable network solutions. The Company provides reliable video, voice, and data network solutions to clients in multiple markets including government, healthcare, defense, education, retail, hospitality, and network service providers.

Allied Telesis is committed to innovating the way in which services and applications are delivered and managed, resulting in increased value and lower operating costs.

Visit us online at **alliedtelesis**.com

Allied Telesis™ the **solution** : the **network**

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com

C618-31047-00 REV B