



Intranet Security Solution

1. Introduction

With the increase in information and economic exchange, there are more and more enterprises need to communicate with their partners, suppliers, customers or their branches in different places through intranet.

There are some specific requirements of intranet network. For example, it needs WAN link and backup line for the connection, data and voice integration transmission, high reliability of the network and low cost for the TCO.

Because of the requirement of information security and control, it needs some features listed and explained as follows.

Information Hiding

It is unnecessary to use real identity to communicate with the opposite side. With network address translation, users can access exterior networks with public address only (with interior address hidden). Except for connection initiated by the interior network, exterior users cannot access interior resources directly through address translation.

Data Encryption

Data transmission in the public network cannot be free from wiretapping. In order to avoid information leakage caused by data wire tapping, it is necessary to encrypt the transmitted information, with only the opposite in communication having the right to decrypt it. With encryption on the transmitted message by router, data will be guaranteed with privacy and integrity as well as message content reality even transmitted on the Internet. For VPN built on public network, data encryption can ensure security of messages in tunnel transmission.

2. Technologies of Quidway® Series Routers

Quidway® series routers provide abundant features used for the Intranet connection including different WAN interface, user authentication, authorization and data protection, QoS and VPN.

2.1. Backup Center

In order to promote network reliability, Quidway® series routers brings out proper concept of backup center. The backup center has the following characteristics.

- It can provide backup interface for any interface of the router except the dialing interface.
- Any interface of the router can be used as backup interface of other interface or logical link.
- It can provide backup for certain logical link of an interface. The backup interface can be either an interface or certain logical channel of the interface. Here the logical channel may be virtual circuit of X.25, frame relay, ATM and ADSL or certain dialer map of the dialing interface.
- One master interface may have multiple backup interfaces. When the master one breaks off the multiple backup interfaces will be in substitute according to their PRI.
- Interfaces with multiple physical channels (such as interfaces of BRI and PRI) can provide backup for multiple master interfaces.
- The master and backup interfaces can share load. When flow of the master interface reaches the threshold, backup interface will be started up. The backup interface will be closed if flows of the master and backup interfaces are lower than another configured threshold.

2.2. AAA (Authentication, Authorization, Accounting)

AAA provides user authentication, authorization and accounting.

- Authentication: user (including login user and PPP access user etc) should be authenticated before being allowed to access network resources. The authentication may adopt either user database maintained by the router itself or the user database maintained by RADIUS server.
- Authorization: it uses a group of attributes to describe user authorization information in order to determine practical access authorizations of users. The authorization information is stored in the database maintained by RADIUS. For access users, the attribute of "filterID" can be used to decide which type of principles should be adopted to filter user messages.
- Accounting: it allows tracking and auditing on network resources accessed by user. After accounting function of AAA is opened, the network access server will send user activity information to RADIUS server in certain charging format. The information will be saved on the server, used for analysis on network operation and creating user bills etc.

AAA provides a mainframe of identity authentication and access control. It utilizes protocols of RADIUS, TACACS+ and Kerberos to realize network access control. Quidway® series routers apply RADIUS protocol, which is in most expansive use.

2.3. VPN

VPN (Virtual Private Network) develops rapidly with the Internet. Modern enterprises utilize more and more Internet resources for sales promotion, marketing, after-sale service, training and cooperation, etc. Many enterprises are inclined to replace their private data network with the Internet. Compared with original Intranet, VPN is a logical network using virtual links of the Internet to transmit private information.

Let's take this enterprise as an example. The interior network set up on VPN is shown as Figure 1.

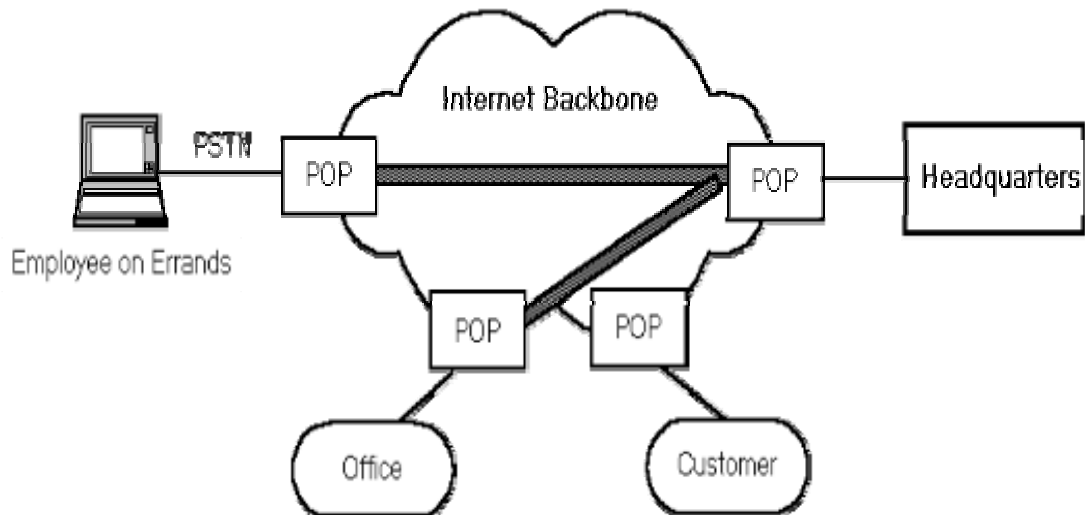


Figure 1 VPN application

As shown in the figure, interior resources occupier is connected to POP (Point of Presence) server of local ISP through PSTN for mutual communication. If adopting traditional WAN technology, dedicated line must be placed to achieve the same objective. With VPN employees on errands and distant customers can access enterprise interior resources without access authorization of local ISP. This is very important for fluid employees on errands and customers in extensive distribution.

To set up VPN, an enterprise simply put a server supporting VPN (such as a router supporting VPN) at the place of resources sharing. After connecting to local POP server through PSTN resources occupier will directly call remote VPN server of the enterprise, with the same call manner as that of PSTN connection. The left work will be completed by NAS (Network Access Server) of ISP.

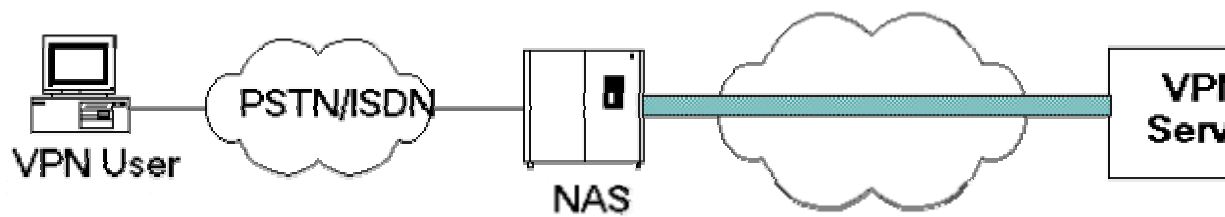


Figure 2 VPN access

NAS mainly uses tunneling technology, which aims at transmitting one type of packets in another type of network. As shown in Figure 2, user dials in NAS of ISP through PSTN. NAS identifies the user of VPN user through username or access number and sets up connection (tunnel) with destination VPN server of the user. User message will be encapsulated into IP packet and transmitted to VPN server from the tunnel. After receiving the packet VPN server will unpack it and read the content. The reverse process is similar. Both ends of the tunnel can encrypt the packet so that other users of the Internet cannot read it. As to user the tunnel is logical extension of PSTN link, with the same operation as that of physical link.

Protocols supporting tunneling in layer-2 include PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) and L2TP (Layer-2 Tunneling Protocol). L2TP integrates advantages of the former two protocols, accepted by enormous companies.

Tunneling protocols in layer-3 include IPSec and GRE. IPSec can guarantee data security of transmitted private information by encryption. For more details please refer to next section.

Quidway® series routers support L2TP, IPSec and GRE.

3. Solutions

3.1. SMB Solution

Considering of branches in different locations, Quidway® series routers provide interconnection solution for security Intranet construction (as shown in Figure 3). Interconnection through DDN dedicated line belongs to traditional Intranet solution of different branches. However, with the development of enterprise with various branches over the world, security problem of remote data transmission between LANs is attracting more and more sights. IPSec of Quidway® series routers provides data protection, which can guarantee privacy, integrity and reality of data in remote interconnection of different branches so as to implement secure Intranet. Similarly, as shown in Figure 3, it can also apply packet filtering and NAT to realize interior security of LANs. This is very important for institutions such as bank. For example, the bank headquarters settles with branches in specified time period only, which can be realized by duration packet filtering.

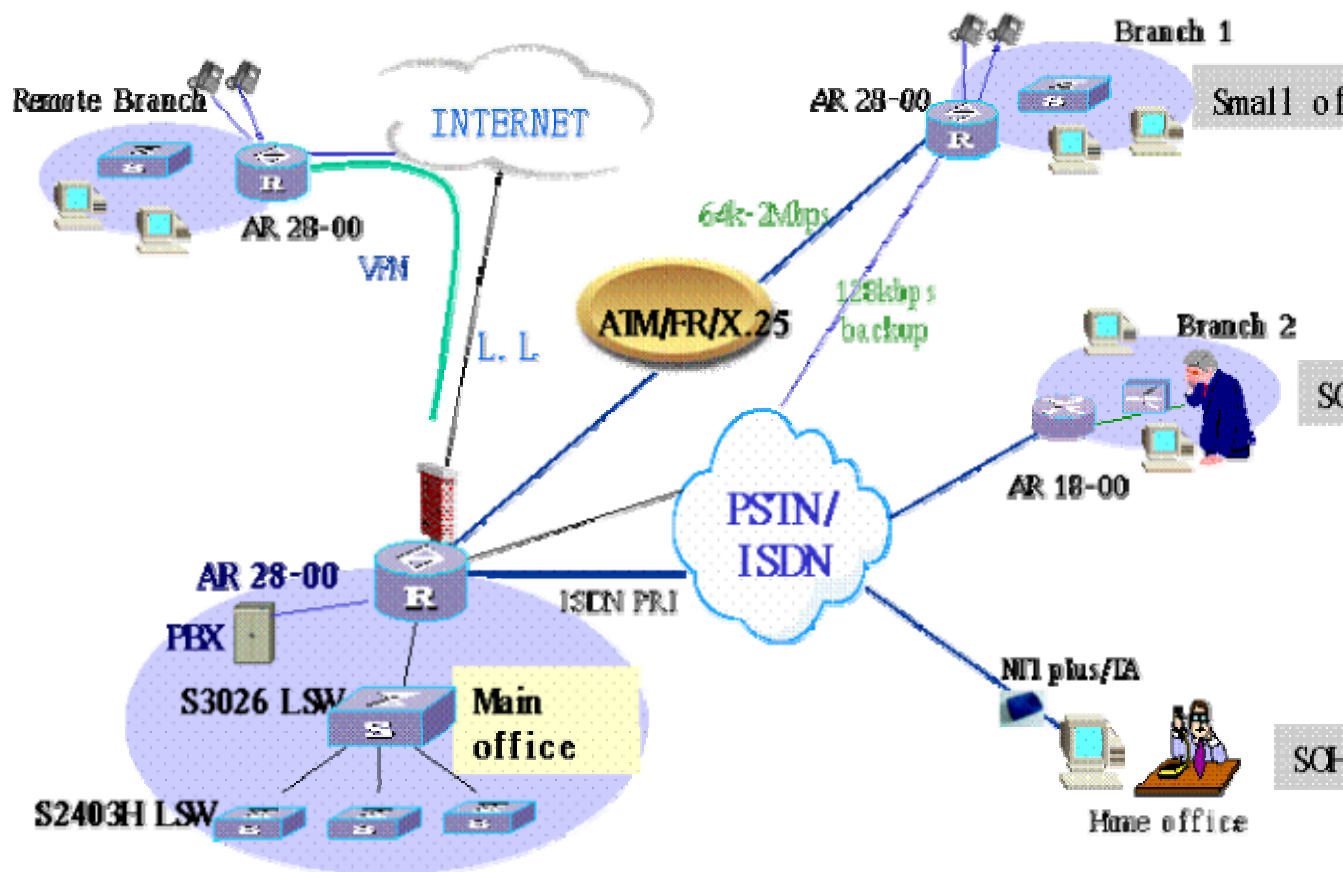


Figure 3 SMB solution of Quidway® series routers

3.2. Large Enterprise Solution

It is very expensive to interconnect branches through DDN dedicated line so it can satisfy neither demand of large-scale organization nor demand of employee on errand accessing interior network. Quidway® router supports tunneling technologies of GRE and L2TP, utilizing public network to set up VPN to make up for the above shortage. However, these tunneling protocols cannot provide corresponding data security guarantees because they do not provide encryption protection. For example, L2TP may take authentication algorithm such as MD5 in channel negotiation but have neither encryption nor authentication on data transmission so that it is easy to be wiretapped. When combined with IPsec it is able to encrypt message to realize secure VPN. Yet IPsec can implement secure VPN independently.

Security VPN solution of Quidway® router is shown in Figure 4.

- Employees on errand can access the headquarters through local Internet.
- Offices and branches interconnect with the headquarters through GRE or IPsec, with data encrypted in transmission.
- Branches can interconnect with each other or the Internet through NAT.

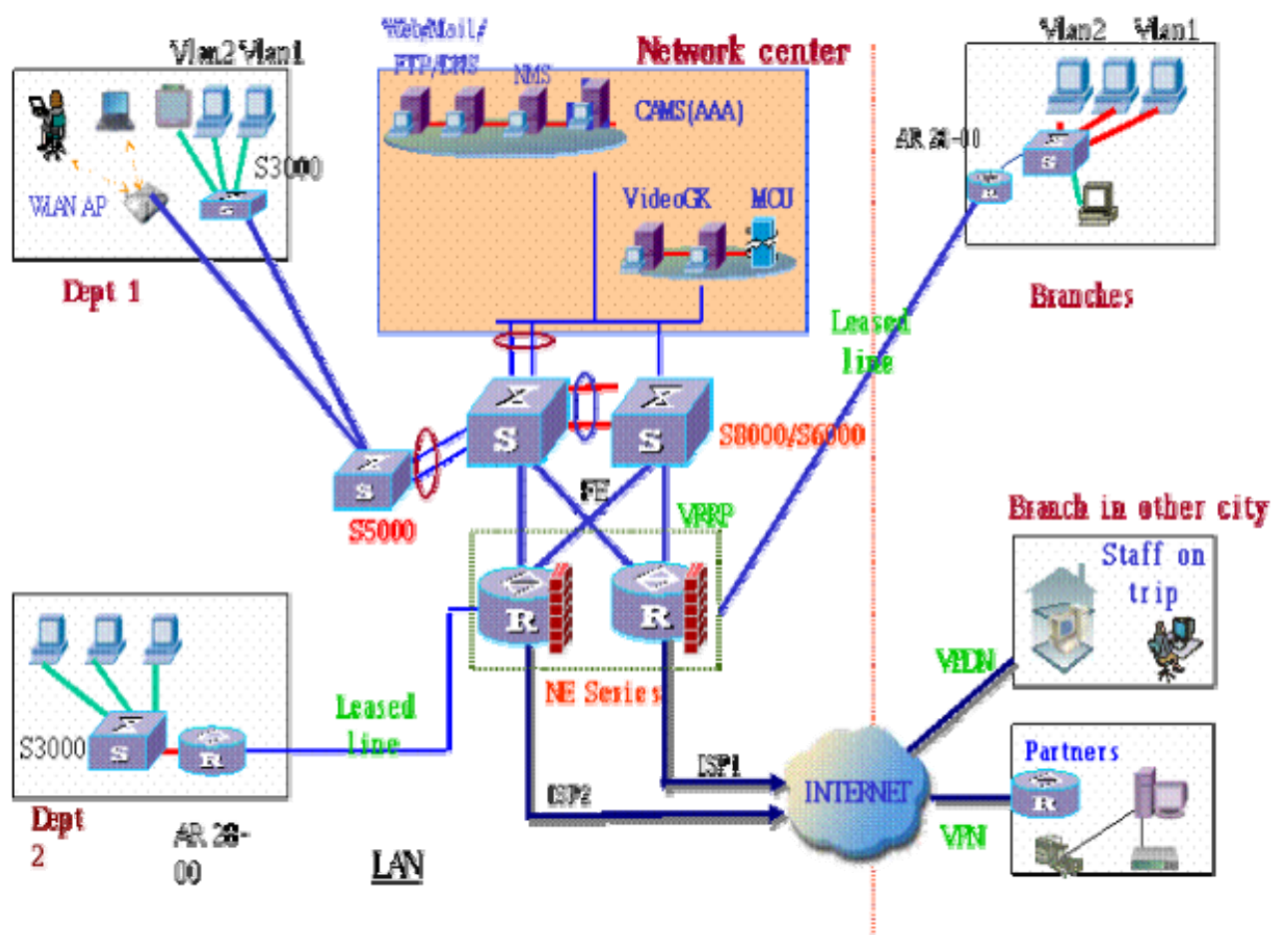


Figure 4 Large enterprise solution of Quidway® series routers