Approach to Next-Generation Corporate Networks

● Akihiro Inomata   ● Hiroyuki Nakahara   ● Noriyuki Fukuyama
● Masafumi Katoh

The proliferation of the Internet has created a network society in which high-speed networks can easily be used in a cost-effective manner. However, the advantages of low price and easy use have also resulted in negative consequences such as increased criminal activity on the Internet and lower reliability. Measures to guarantee secure network use in mission-critical areas will become essential. Fujitsu's FENICS network service for enterprises uses advanced network security technologies such as Dynamic VPN and NetSpanner to ensure that products and services can be used in a secure network environment. This paper describes the current status of network use and security-related problems and introduces Fujitsu's technical approach to these issues.

1. Introduction

Network use has expanded into many aspects of daily life and business.[1] This trend is accelerated by technological innovation and social maturity, and as a result, the following developments will occur in homes, enterprises, social/entertainment venues, and other areas.

1) Many functions will be realized on networks. For example, some of the functions of banks, schools, and hospitals will be performed over networks in the form of electronic commerce, electronic banking, telelearning, and telemedicine.

2) The culture of physically possessing content (e.g., on devices such as CDs, DVDs, and HDDs) will shift to a culture of accessing and using it over a network. For example, software, music, and movies will be downloadable as required. Also, methods for handling the huge amounts of content that will be made available will become common.

3) A ubiquitous computing society will be realized. Many goods will be individually controlled using IC tags, and cameras and other sensors will be commonly used for security monitoring.

When such a society is created, networks, including enterprise networks, will become much more important. As a result, they will need to be more flexible, secure, and reliable.

This paper describes the overall concept of a highly flexible, secure, and reliable enterprise network. It also introduces a technical approach that is based on Fujitsu's FENICS (Fujitsu Enhanced Information and Communication Services) business-oriented network service.

2. Enterprise networks

Enterprise use of networks is spreading along with the advance of the Internet. The networks of 10 years ago connected a mainframe computer to terminals by using a special protocol such as Fujitsu Network Architecture (FNA) or were mostly used for file and printer sharing. However, the explosive growth of the Internet has led enterprises to embrace Internet-based network technology because Internet systems are inexpensive to purchase and are easy to operate and expand. Thanks

FUJITSU Sci. Tech. J., **42**,4,p.547-553(October 2006)

547

to the recent availability of open servers and various Web services, mission-critical tasks such as accounting and providing customer services are being done using Internet technology.

Concerning network infrastructures, TCP/IP has become popular and enterprise network facilities have mainly turned to using routers and layer 2 switches. Network services that connect different bases in an enterprise have shifted to IP-Virtual Private Network (IP-VPN) services based on Internet technology, wide-area Ethernet service, and so on. Moreover, more and more enterprises are using less-expensive Internet VPNs that use cryptography.

On the other hand, certain Internet defects are becoming clear. For example, because anyone can use the Internet, network crimes such as information leaks and abuses are easy to commit.

The network system is unstable because the Internet does not guarantee the stability and performance of low-cost broadband lines. To expand the use of networks to mission-critical fields such as medical services and banking, a more stable and secure network framework must be realized while retaining the convenience and low cost of the current system.

3. Dynamic VPN

As described in the previous section, future networks need improved security. The present Internet technology is based on the view that people are fundamentally good. However, anyone can communicate freely at any point on a network, and this convenience has led to increased network abuse. To realize secure communications, communication lines must be connected only to the intended receivers and then disconnected after the intended calls have ended. Therefore a system that controls access is needed.

Basically, anyone can communicate freely in a network, and networks are controlled by restricting access. However, the security risk to networks is increasing, and we should therefore shift the emphasis away from access restriction toward

access permission. To do this, it is necessary to control access individually for each terminal or application software. Application software based networks are controlled as client-server systems, with the control parameters being set in the servers. In a network containing multiple servers, conventional access control is complicated and difficult to implement because control parameters must be set individually for each server. Moreover, it is costly to develop access control software that does not require such settings.

Based on the above issues, such a network should satisfy three conditions:
1) It must keep the system secure.
2) It must adapt to changes such as changes in the network infrastructure.
3) It must be easily accessible anywhere on the Internet.

To meet these conditions, Fujitsu has developed a secure solution technology called Dynamic VPN and offers it as a product and service.

This technology has the following features:
1) Access points and connections/disconnections are controlled according to a security policy.
2) The network is controlled by a single center based on the security policy and modified as required.
3) Automatic setting of encrypted communication, user IP address, and other functions and information.

This technology is installed on Fujitsu's GeoStream Si-R series of routers and realizes the advanced functions in cooperation with FENICS service servers. **Figure 1** shows the sequence for a connection between bases that conform to the security policy. The sequence is as follows:
1) When base A tries to access base B, the router asks the center server for permission to access base B.
2) The server judges whether to permit this access by referencing the security policy database at the center.
3) If permission is granted, the router at the destination site is asked to establish the
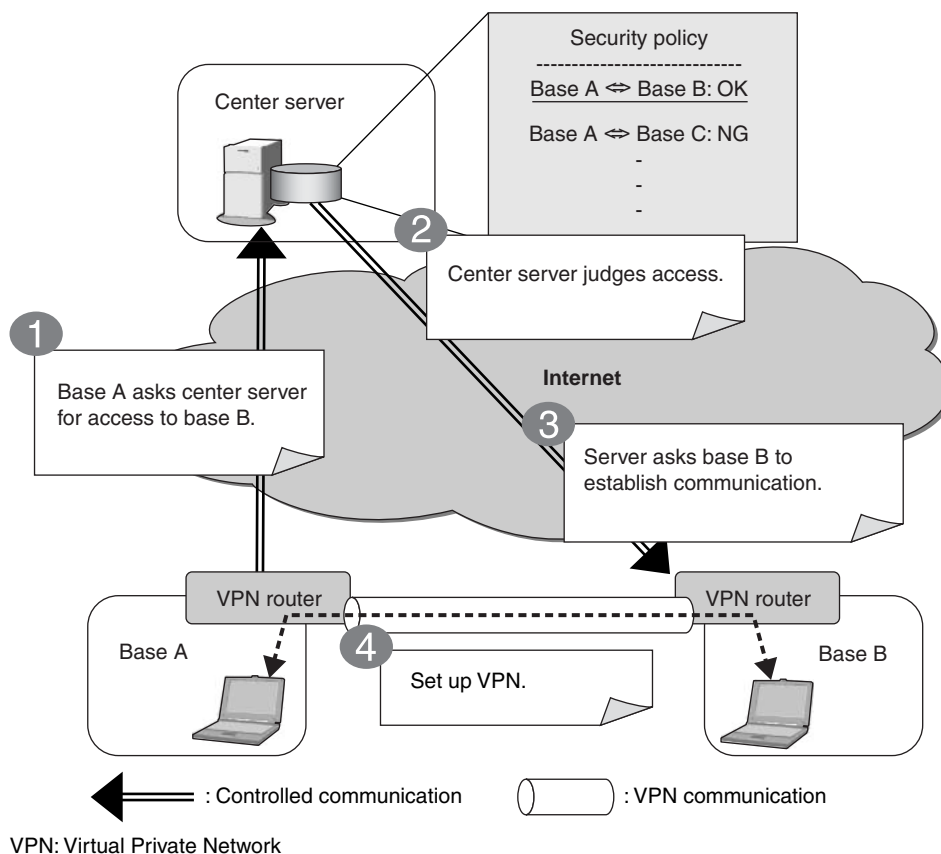
548

FUJITSU Sci. Tech. J., **42**,4,(October 2006)

Figure 1
Sequence for connection between bases participating in security policy.

communication.

4) Each site exchanges communication parameters (encrypted key, IP address) and establishes the communication.

By using this technology, connection/disconnection can be judged not only according to the sender's request but also the center's request. Users can perform encrypted communication based on a security policy without regard to security. When there is a communication request, it is confirmed that the newest security policy is reflected to the centrally controlled security policy information. The centralized control of the center can reduce the operation load of maintaining the latest security policy and can reflect the latest security policy in real time.

VPN terminals generally consist of a hub and spoke system. If the volume of communication or number of users exceeds the hub's capacity, the communication speed of paths in the network goes down. However, by using this technology, because communication between sites is achieved by directly interconnecting sites on demand via a VPN router, the communication load on the hub is reduced and a reduction in communication speed is prevented (**Figure 2**). This technology is also used for multimedia communication between sites and to reduce the communication load on the center when content is delivered to multiple sites. Fujitsu plans to expand this secure technology to include direct communications between terminals.

4. Maintaining network health

Enterprises cannot confidently use a network unless it guarantees stable communications, and this stability is being adversely affected by the following changes:
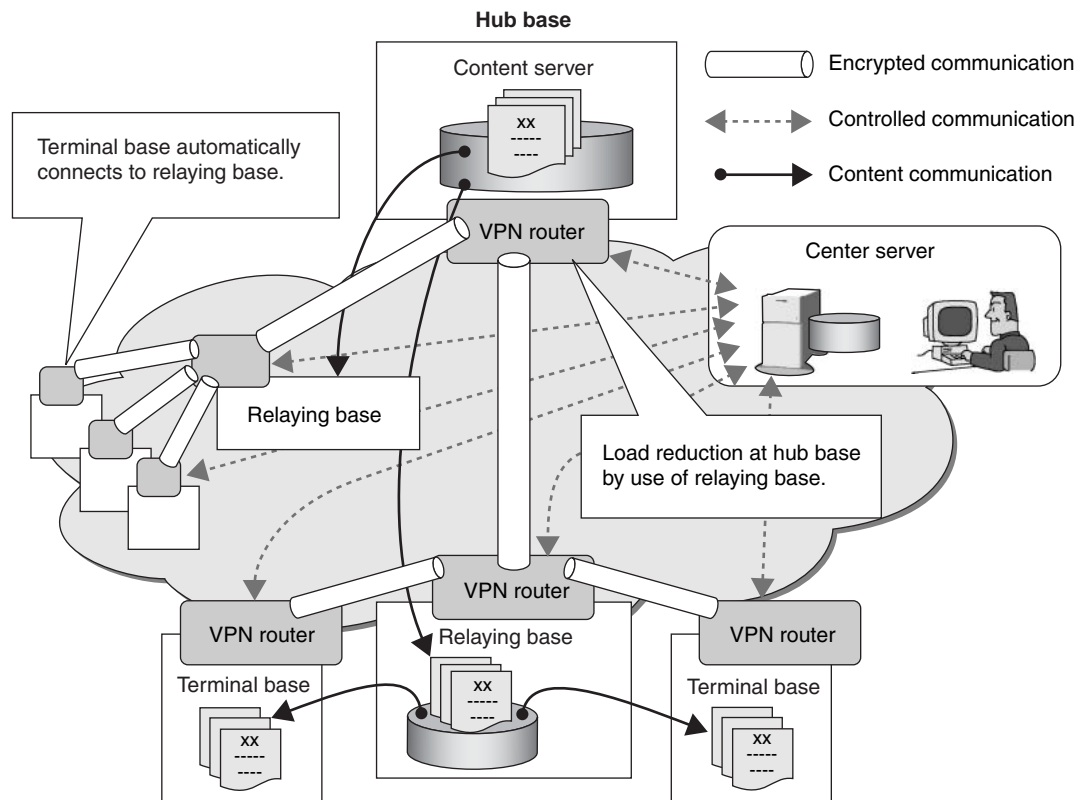
Figure 2
Reduction of communication load.

1) Conventional exclusive-line services have mostly been replaced with inexpensive broadband connections (Internet VPN).

2) Because IP technology makes it easy to introduce new equipment, there are frequent changes to system configurations and the amount of terminal equipment and application software being used has increased. Consequently, system structures have become complicated.

Although networks have been modified to match these changes, sometimes their performance is poor; for example, communication speed is very low. As a result, at those times, they cannot be put to practical use.

This performance deterioration can be so severe that, at worst, it becomes impossible to execute certain jobs and the seriousness of the matter becomes apparent. However, the root cause of these failures is difficult to identify, and

it will take time to recover the performance of networks.

In the case of normal operation and management technology, a network is diagnosed to classify the cause of performance deterioration by using, for example, the ping program to monitor the communication status and whether the network is reachable or SNMP to obtain data about the utilization rate and error rate. To investigate a cause, a system administrator depends on know-how and experience, and it takes considerable investment to train system administrators and then maintain their skills.

Fujitsu's FENICS network service includes access to a 24/7 call center that helps customers resolve problems they encounter. When an alarm is generated in a customer's system, the local information about the trouble is collected by the center and then the trouble is resolved. In some cases, when the network performance deterio-

rates, some local network data (traffic data) is needed to find a solution. However, if the local network configuration or network management system is complicated, finding a solution can sometimes take a long time.

In these complicated situations, it is necessary to visualize the operating status of the network equipment and servers, and we have developed various technologies to enable this visualization.[2)-4)] For example, we have developed NetSpanner, which is technology for network performance management that has a network service performance analyzer and tuner (**Figure 3**).

Based on this technology, we have also developed a network stabilizing function that is installed on a GeoStream Si-R series router in a business hub and a server in a center. This is a powerful function that quickly locates failures in a network by combining passive and active mode

analyses. In the passive mode analysis, this function examines communication data at a center in which a large amount of data is concentrated and then determines the communication performance between the center and each base. In the active mode, this function performs test communications between a center and each base and judges whether a failure has occurred in a base zone or a zone between a center and base. Normally, the network is monitored in the passive mode, and if a failure cannot be located in this mode, the active mode is used to make a zone judgment. This method is effective not only for troubleshooting but also for preventing failures from occurring.

Figure 3 shows the monitoring network performance using NetSpanner. For example, when the network is monitored in the passive mode and a packet loss occurs, by analyzing the packet spans between before and after the packet loss, the NetSpanner function judges whether the
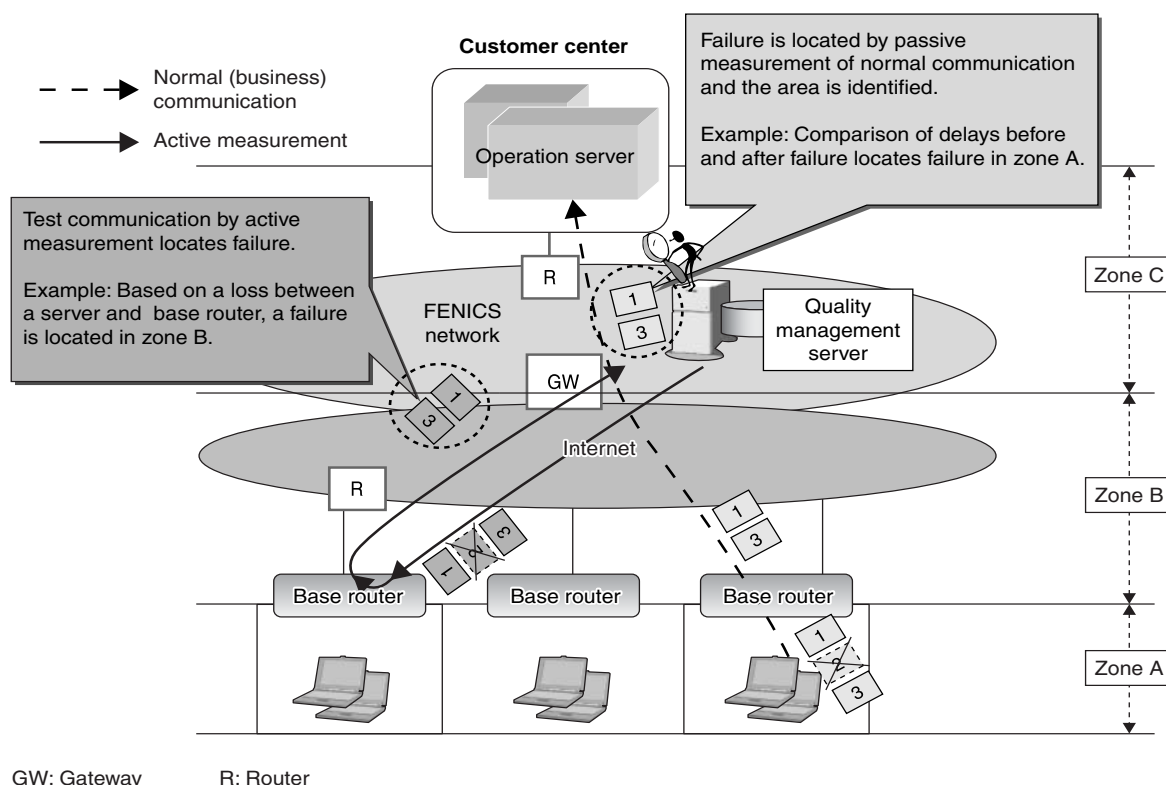
Figure 3
Monitoring network performance using NetSpanner.

FUJITSU Sci. Tech. J., **42**,4,(October 2006)

551
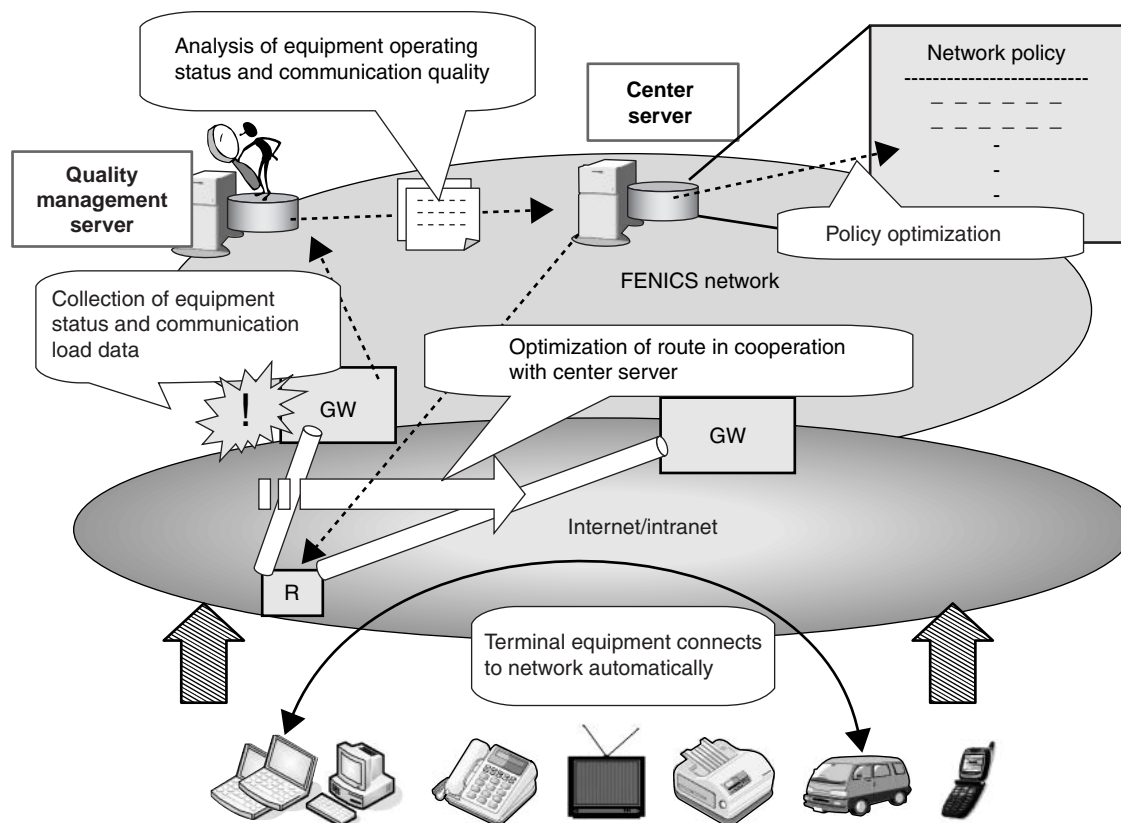
Figure 4
Future network.

failure occurred in the base zone (zone A) or in the internet (zone B). (In the figure, the failure is located in zone A.) In the active mode, by analyzing packets going to and coming from the base router, the function locates the failure zone or failure direction. (In the figure, the failure occurs in the path from the quality management server to a base router and is located in zone B.)

Basically, a router has all the necessary functions for analyzing, and there is no need to add analyzing equipment at a base. However, when there is a severe load, good router performance can be maintained by adding a server to perform TCP sequence analyses and search for problems such as duplex mismatches.

5. Future network
In the future, by developing and applying its network technology, Fujitsu plans to realize a

secure and autonomous network and use it to provide network services and solutions that will reduce the cost of operation management and enhance value. Some examples of these services and solutions are as follows (**Figure 4**):

1) Automatic optimization
    The communication (transfer) quality and trends of communication rates are analyzed, and the network automatically optimizes the topology of the VPNs in the network and the routing details.
2) Plug and play network
    A secure network can be automatically set up simply by adding terminals.
3) Automated recovery function
    This function automatically performs recovery using cold-standby equipment, isolates a failed node, and establishes roundabout routes.