IPCOM EX Series for Realizing Network Stability and Safety

● Shoji Temma

(Manuscript received June 8, 2007)

Stability and safety are essential requirements in today's enterprise IT systems. This paper discusses network stability and safety in the WAN edge and server-front areas relative to the network infrastructure used for configuring enterprise IT systems. The paper then describes the obstacles to achieving stability and safety in these areas, and how to overcome those obstacles. The concept of integration for Fujitsu's NETWORK SERVER IPCOM EX series is then discussed from the standpoints of design, installation, and troubleshooting, with mention made of the improved stability, simplicity, and safety of the IPCOM EX series. The paper concludes by showing how the IPCOM EX series provides stability and safety in citing examples of application in WAN edge and server-front areas.

1. Introduction

It is essential for enterprise IT systems to be capable of readily handling new businesses, M&A, and alliances. Consequently, enterprise IT systems must be provided with stable networks through which to interlink the systems. Also, with the widespread proliferation of the Internet, enterprise IT systems must now more than ever be provided with stable services on a year-round 24/7 basis. As such, the need for stable and safe enterprise IT systems has been steadily growing.

This paper discusses the network stability and safety necessary for enterprise IT systems relative to networks used for configuring these systems. This paper cites examples of application to illustrate the roles and functions of Fujitsu's NETWORK SERVER IPCOM EX series that was developed to easily provide the levels of stability and safety required.

2. Network stability and safety

This section defines the areas used to achieve network stability and safety. This section also discusses the obstacles to ensuring the stability and safety needed by each area, as well as the network functions employed to overcome those obstacles.

2.1 Definition of areas used to achieve network stability and safety

Figure 1 shows the key areas in which to achieve network stability and safety.

1) WAN edge area (W)

The WAN edge area is used to connect enterprise IT systems and global networks such as the Internet and intranet. Stability and safety are essential for the WAN edge area in terms of communicating with applications through global networks. For Internet connections in particular, safety is essential in protecting the enterprise IT systems against a sudden increase in the number of accesses and acts of illegal access.

2) Server-front area (S)

The server-front area is an entry point for accessing server farms and backbone LAN connections. Stability and safety are essential for

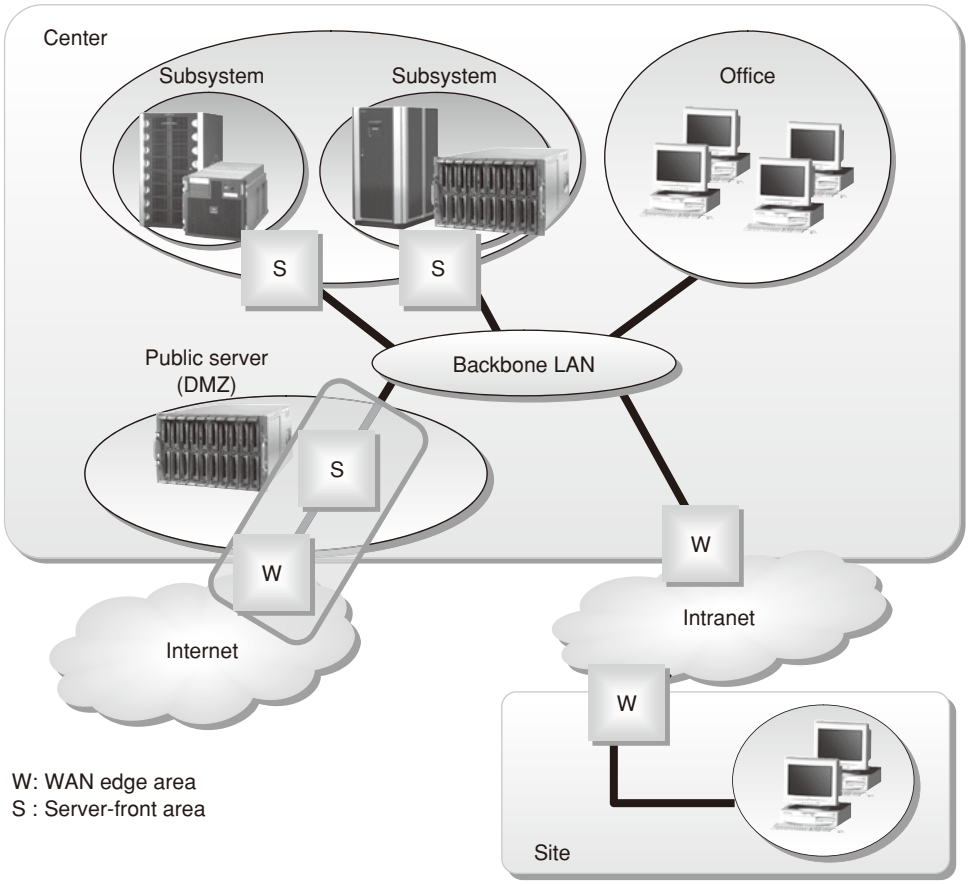


Figure 1
Key areas for stability and safety.

the server-front area relative to accessing applications provided by the server farms.

The following section cites examples of obstacles that hinder the stability and safety of these areas, and the network functions used to overcome these obstacles.

2.2 WAN edge area stability and safety

2.2.1 WAN edge area stability

As described above, the stability required for the WAN edge area means stable communication with applications through networks.

IP networks handle not only transaction data, but image and voice data as well. As a result, IP networks face more obstacles regarding stability than communication on private circuits. Examples of such obstacles and the functions used to overcome those obstacles are listed below.

1) Examples of obstacles hindering stability
- Failure of a device (e.g., router) or line used to connect to networks
- Access line failure
- Rapid increase in amount of communication through specific applications

2) Functions for achieving stability

To prevent the obstacles described above from affecting enterprise IT systems (in not stopping services), the following functions are required:
- Link load balancing function

By connecting enterprise IT systems to the Internet or intranet through multiple lines and making all connected lines available, the link load balancing function enables communication

to continue by using the remaining normal lines, even if communication is interrupted by failure of a connection device such as a router, or due to Internet or intranet failure.

- Layer 7 bandwidth control function

When the layer 7 bandwidth control function detects a sudden increase in the amount of communication traffic for a given application while monitoring communication, it restricts the application traffic to the prescribed amount in order to protect the communication capabilities of other applications. In contrast to the QoS function (also called the shaping function) provided by a router to control only the amount of traffic output to a global network, the layer 7 bandwidth control function can control the amount of traffic input to and output from a global network (bidirectionally). As such, the layer 7 bandwidth function can also be used to handle any sudden increase in the amount of input data.

2.2.2 WAN edge area safety

Due to the particular demands for safety regarding Internet connections as discussed above, the following assumes an Internet connection in discussing the obstacles that hinder safety, and the network functions used to overcome those obstacles.

1) Examples of obstacles hindering safety

- Unauthorized access to a server (illegal access)
- External intrusion by programs executing irregular operations (such as due to a virus)
- Unauthorized Internet (Web server) access from inside the company
- Activities such as viewing (theft) or rewriting (altering) communications data

2) Functions for achieving safety

To address the obstacles described above, the following functions can be used to protect enterprise IT systems:

- Firewall function

The firewall function blocks unauthorized access of specific addresses and ports to protect the system against illegal server access.

- Anti-virus function

The anti-virus function compares the communications data with data files in which the specifics (patterns) of computer viruses have been recorded, and then deletes the communications data or outputs a warning for any virus detected in the data.

- Web content filter function

The Web content filter function imposes restrictions on viewing Web sites so that inappropriate information on the Internet cannot be accessed to protect against information linkage on the Web.

- Virtual Private Network (VPN) function

By encrypting communications between a center and a site or between personal computers within a site, the VPN function protects communication data against external theft or alteration virtually as if the data were on a private circuit.

2.3 Server-front area stability and safety

2.3.1 Server-front area stability

The stability required for the server-front area means the stable access of applications provided by the servers.

1) Examples of obstacles hindering stability

- Server failure or stopping due to periodic maintenance
- Deteriorated response due to a sudden increase in load due to requests concentrated on a specific server
- Deteriorated response due to a sudden increase in communication traffic for a specific application such as video delivery.

2) Functions for achieving stability

Maintaining stable access to applications in case the obstacles above require the following functions:

- Server load balancing function

The server load balancing function monitors the status of servers and distributes access requests to servers with lower loads to prevent

Table 1
Areas and functions for achieving stability and safety.

Area for achieving stability and safety		WAN edge	Server-front
		Area used to connect to global networks such as the Internet and intranet	Entry area for accessing server farms
Stability	Essential stability	Stability of communications with applications through the network	Stability of application access
	Functions for achieving stability	Link load balancing function layer 7 bandwidth control function	Server load balancing function Accelerator function
Safety	Essential safety	Protection of systems against illegal access, data theft, and alteration	
	Functions for achieving safety	Firewall function, anti-virus function, Web content filter function, VPN function, etc.	

a concentration of access requests on a specific server.

By monitoring the status of servers, the server load balancing function can distribute access requests to another server and prevent services from being stopped, even if a server fails or is stopped for maintenance.

The server load balancing function can also restrict the number of access requests sent to a server for ensuring more stable access.

- Accelerator function

When high-load processing is executed on a server, the server load may suddenly increase due to a concentration of access requests. If such processing operations occur on a server, the accelerator function offloads the demands of high server load processing to a network device. For example, encryption processing is considered high-load processing for a server in Secure Socket Layer (SSL) communication. By offloading SSL processing to a network, a more stable response can be achieved.

2.3.2 Server-front area safety

1) Examples of obstacles hindering safety

- Unauthorized access to a server (illegal access)
- Transmission inside the company of programs executing irregular operations (due to a virus, etc.)
- Unauthorized Internet (Web server) access from inside the company
- Activities such as viewing (theft) or rewriting (altering) communications data

2) Functions for achieving safety

The causes of obstacles described above are the same as those for WAN edge area safety. Therefore, the same functions as those for achieving safety for the WAN edge area are required.

Because the causes of obstacles that hinder safety occur not only from outside, measures for overcoming obstacles inside the company are also required. Public systems are now being constructed with a firewall installed for each application system and communications data encrypted within a data center.

Table 1 lists the stability and safety required for the WAN edge area and server-front area, and the functions for achieving such stability and safety.

3. IPCOM EX series approach

The functions needed for achieving the stability and safety described in the previous section form the basis of constructing and operating an enterprise IT system. To enable the easy and speedy utilization of these functions, “integration” has been adopted as the basic concept of IPCOM (**Figure 2**).

In addition to the basic functions for achieving stability such as the layer 7 bandwidth control, link balancing, and server load balancing functions used in conventional devices,[1),2)] the IPCOM EX series integrates new functions for

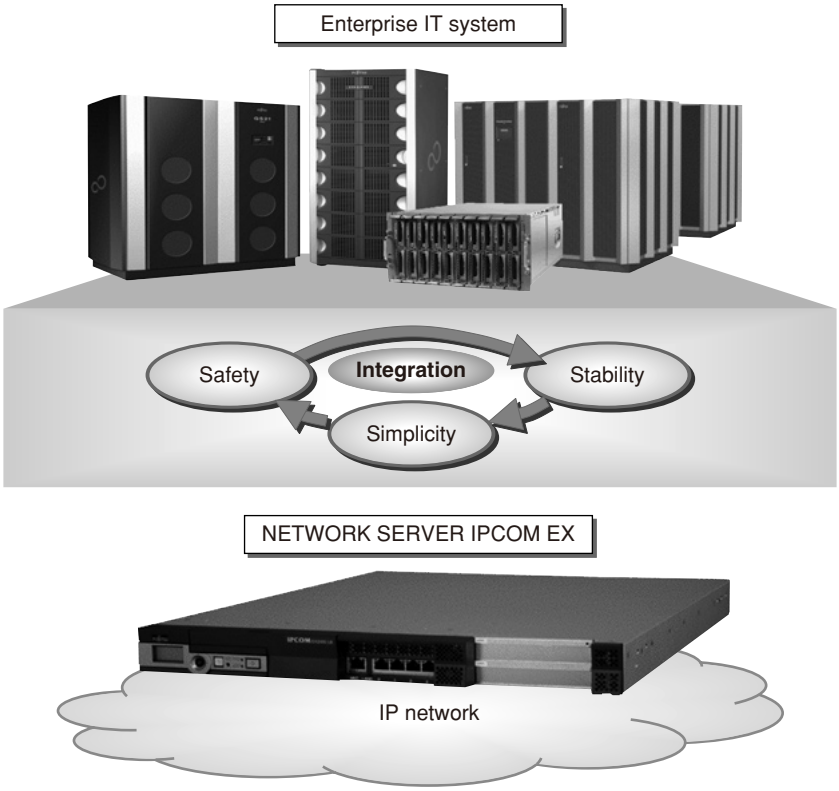


Figure 2
"Integration" — basic concept of IPCOM.

achieving stability. These functions include the anti-virus and Web content filter functions that are indispensable for achieving stability.

Regarding the product lineup, product lines have been prepared for all applicable areas and functions from the standpoint of various combinations between the areas and functions needed for achieving stability and safety as discussed above. By enabling step-by-step upgrading of the products after purchase and installation, the product lineup is intended to simplify use.

Figure 3 shows the IPCOM EX lineup.

3.1 Merits of integration

The merits of integration can roughly be divided into two points: the simplicity of design and installation, and the simplicity of operation and troubleshooting.

The following describes both points.

1) Simplicity of design and installation

As mentioned above, several functions are needed to achieve stability and safety. This was typically achieved by combining several devices. Regarding design and installation, the following are required:

- Assurance of compatibility between functions provided by the devices
- Assurance of alternate routes in case of device failure
- Setup of various devices and training on device operations

Combining several devices increased the amount of work required including complex design and verification, resulting in a system lacking stability. However, integrating the required functions to reduce design and installa-

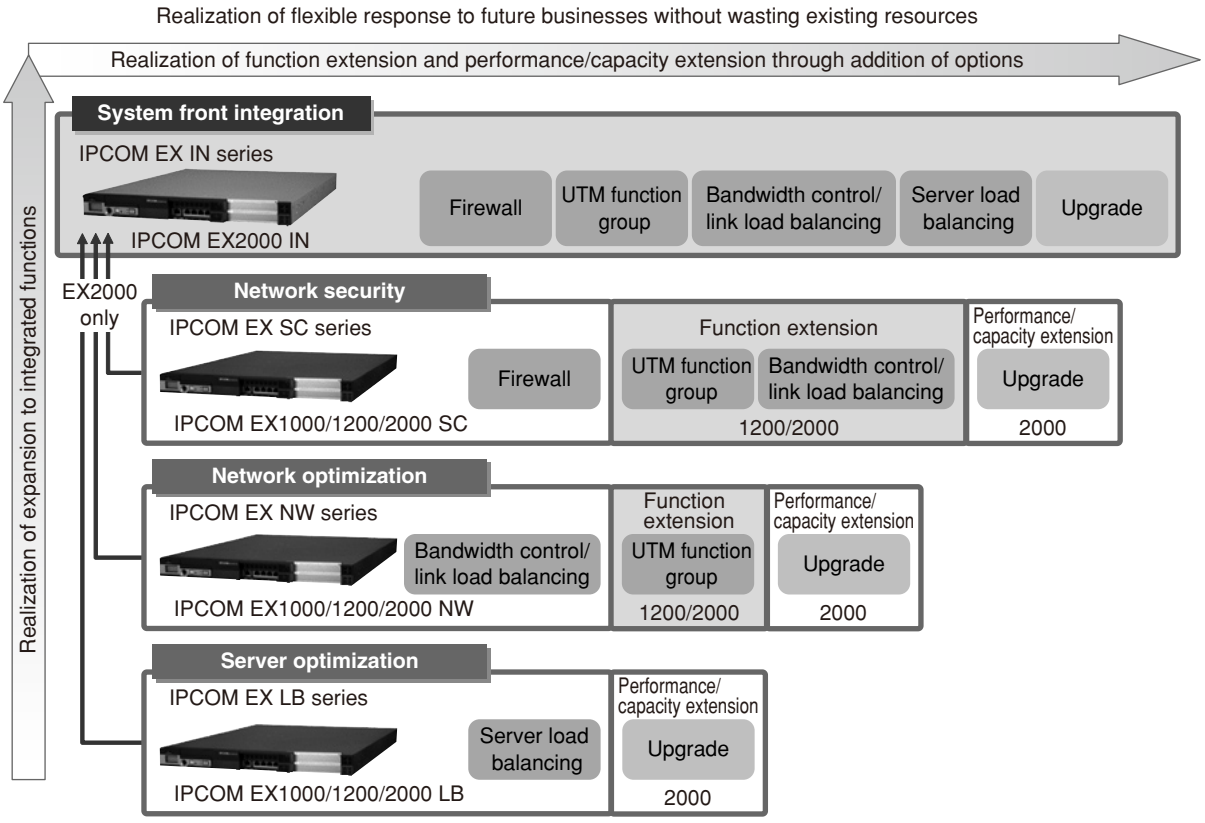


Figure 3
IPCOM EX series lineup.

tion work enabled the following [**Figure 4 (a)**]:

- The devices assure compatibility between the functions.
- The design is simple with no need to consider alternate routes.

2) Simplicity of operation and troubleshooting

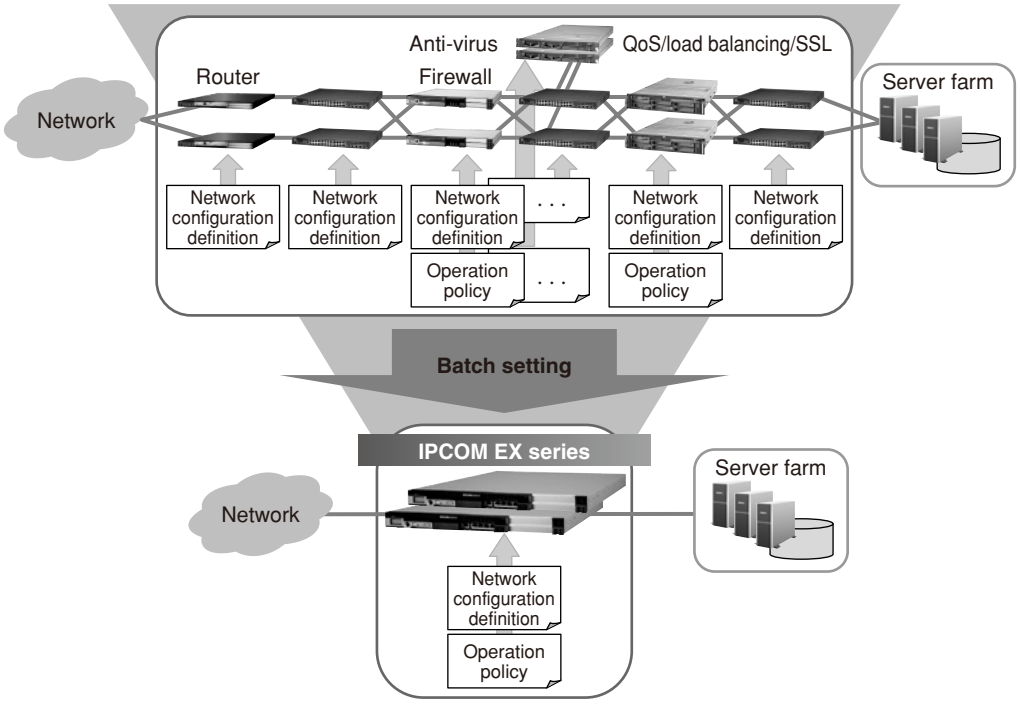
Any attempt to achieve stability and safety through a combination of various devices will inevitably increase the number of devices. As a result:

- It will be difficult to isolate the range of influence in case of device failure.
- Troubleshooting will be complicated.
- When there are different device vendors, mutual cooperation between the vendors will become necessary. However, such mutual cooperation as the vendors inspecting the devices will involve further complications. This problem can be resolved through integration because one vendor equals one device [**Figure 4 (b)**].

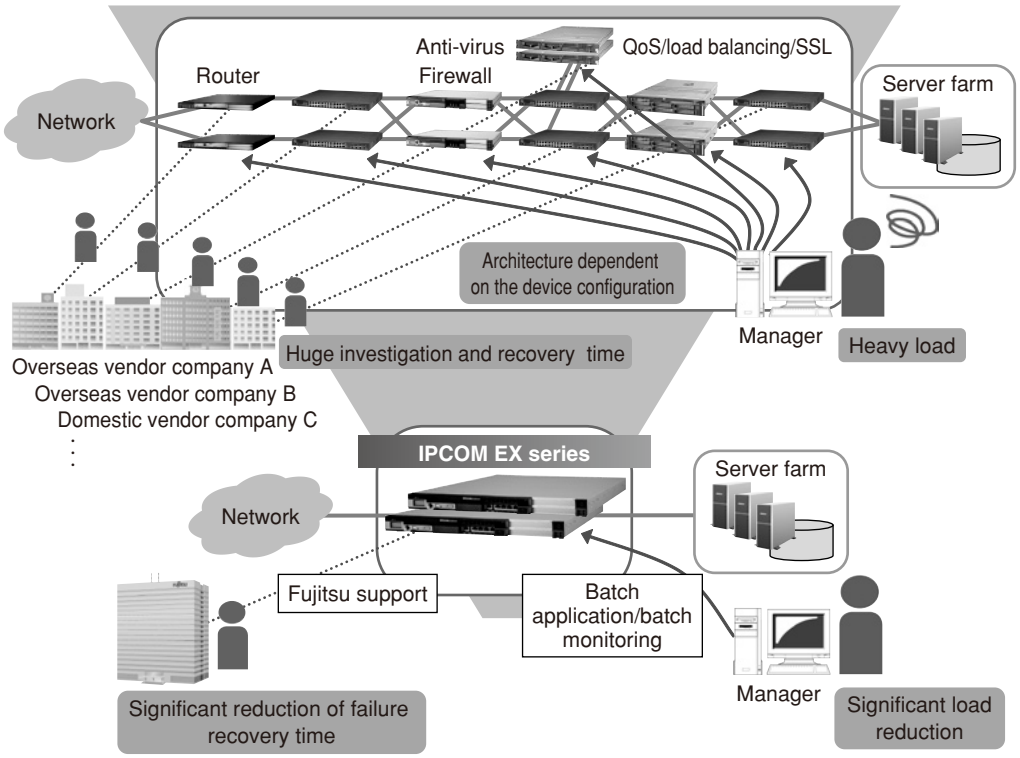
3.2 Merits of step-by-step upgrading

From the standpoints discussed in the previous sections, the product lineup has been expanded along with the basic concept of integration from the initial shipment of products being adopted for IPCOM. The following describes the integration adopted for the IPCOM EX series.

As a business grows, the enterprise IT system should be able to expand systematically to match that growth. For such an enterprise IT system, arranging all the functions considered necessary in the initial stage of configuring the system will increase the initial investment. It may also result in wasted investment if the system design must be changed. And with regard to the network infrastructure of enterprise IT systems,



(a) Reduction of design and/or installation work



(b) Simplicity of operation and troubleshooting

Figure 4
Merits of “Integration” in design and/or installation.

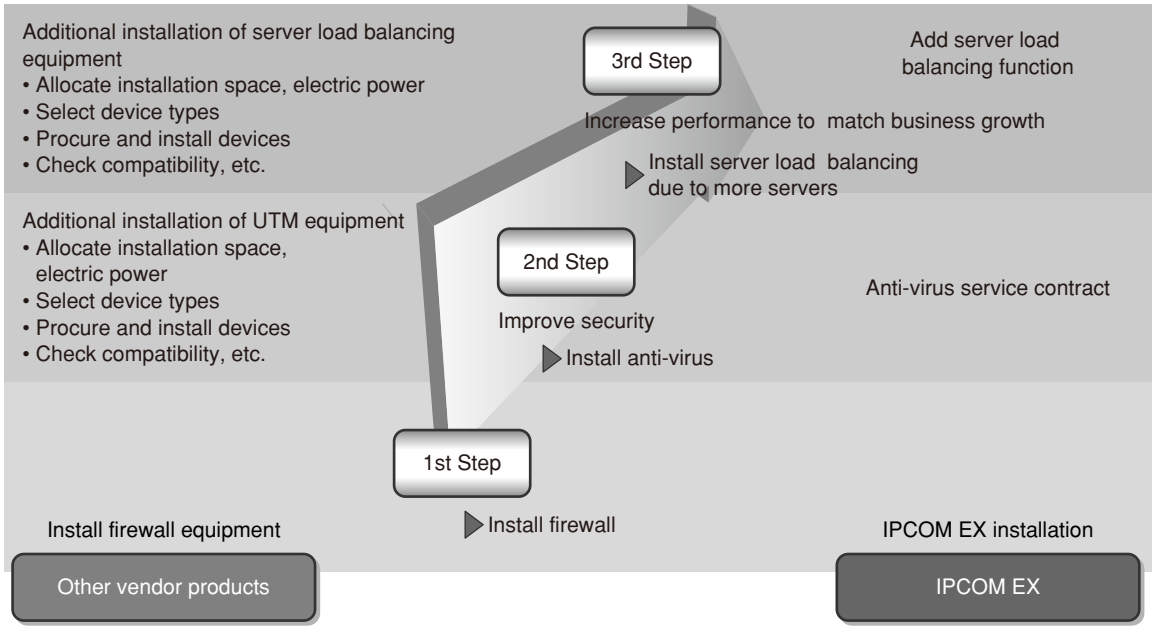


Figure 5
Example of step-by-step upgrade.

stopping the services for long periods in order to add new functions considered necessary would not be tolerated.

To resolve such problems, the IPCOM EX series provides a mechanism for step-by-step upgrading of the functions of the devices installed.

Figure 5 shows an example of the step-by-step upgrading of a system where a firewall was initially installed, followed by the addition of an anti-virus function and server load balancing function.

In a system that includes the products of other vendors, it will be necessary to add a device whenever functions are added. Work will be required to match the newly designed system, beginning with the allocation of installation space and electric power to the confirmation of functional compatibility between newly installed and existing devices in the system.

For the IPCOM EX series, however, the required functions can easily be added by simply setting up an additional license, and without having to stop the system. Moreover, the system can be upgraded within a short period of time.

4. IPCOM EX series enhancements

This section discusses the enhancements made to the IPCOM EX series.

1) Improved safety

Enterprise IT systems must now confront an increasingly diverse range of security threats for the WAN edge area. In addition to a firewall (including some intrusion prevention system [IPS] functions), the IPCOM EX series also supports the anti-virus and Web content filter functions not conventionally supported, and covers the functions required for Unified Threat Management (UTM).

2) Improved simplicity

The appearance of blade servers triggered the integration of servers into a center. Along with this development, security threats have become localized at individual locations. Therefore, applying concentrated countermeasures in the server-front area where the security threats are focused is a particularly effective and

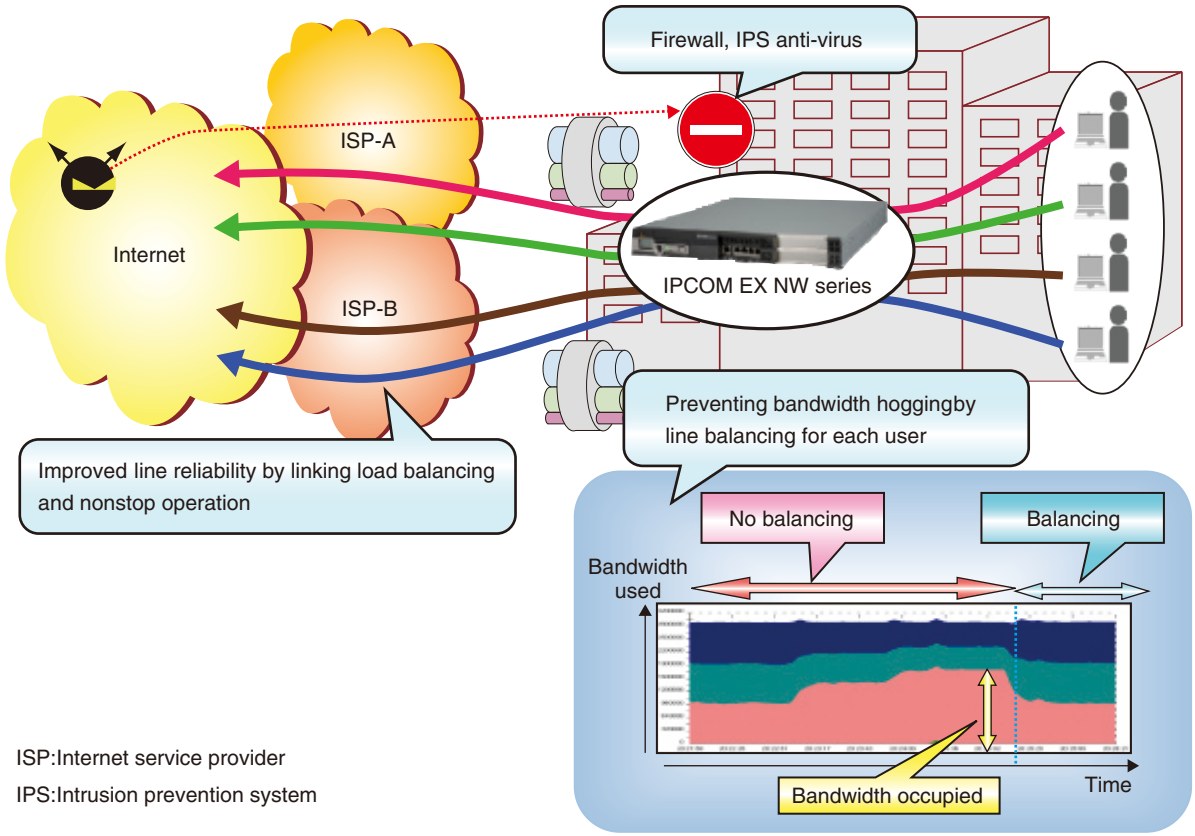


Figure 6
Example of IPCOM EX series application in WAN edge area.

efficient means of protection. The IPCOM EX series integrates the industry's first server load balancing function and UTM function in order to enhance and complete the security functions in the server-front area.

3) Improved stability

Given the need for year-round 24/7 nonstop services, stopping the system for long periods to improve security functions would not be tolerated. Even for such security improvements, the IPCOM EX series offers improved stability by enabling the addition of functions without having to stop the devices. The functions required can be added by simply activating the licenses (option) of function modules installed in advance.

As previously described, the IPCOM EX series has realized the following (ratios of reduction at our company) by improving the three points above based on the concept of integration.

- 40% reduction in initial costs
- Reduction in installation space and power consumption to 1/8
- 50% reduction in support costs

5. Examples of IPCOM EX series applications

This section introduces some examples of IPCOM EX series applications in the WAN edge area and server-front area.

1) IPCOM EX series application in the WAN edge area

Figure 6 shows an example of applying the IPCOM EX series in a network to which an office and the Internet are connected. The example illustrates how the stability of a system capable of handling access line failures or any sudden

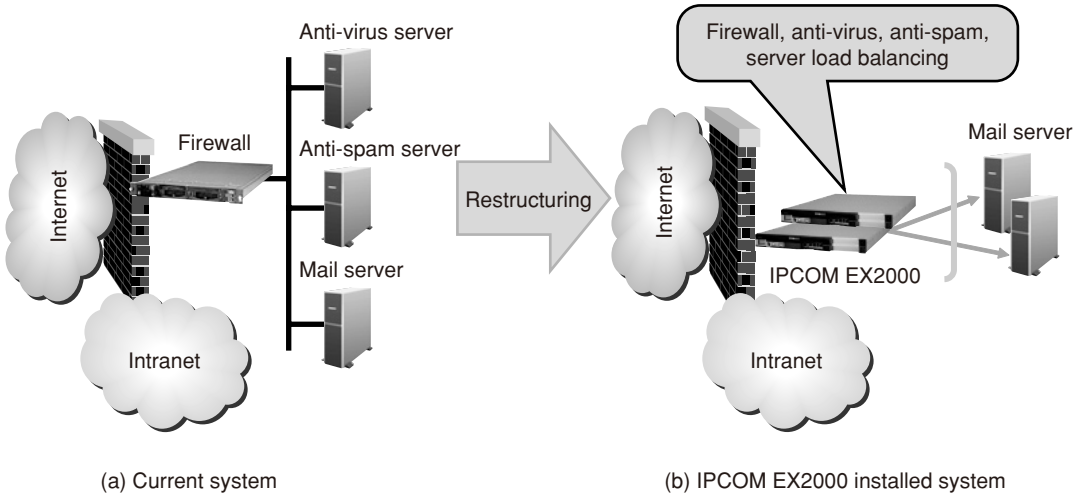


Figure 7
Example of IPCOM EX series application in server-front area.

increase in communication traffic is assured through the use of the following two functions of the IPCOM EX series:

- Link load balancing
- Layer 7 bandwidth control function

The example also illustrates how the safety of a system capable of handling any security threats from the Internet is assured through the use of UTM functions (firewall, IPS, anti-virus, and Web content filter). The concept of IPCOM EX series integration has enabled the above functions to be realized using a single device, and thus affords simple system construction.

2) IPCOM EX series application in the server-front area

Figure 7 shows an example of applying the IPCOM EX series in an e-mail system. The example illustrates how the concept of IPCOM EX series integration has enabled the firewall, anti-virus, and anti-spam functions conventionally provided by the server to be realized by using a single device. By installing the IPCOM EX series, such work as setting up a server for multiple devices or customization can be simplified on one IPCOM EX series device. Moreover, even if the amount of e-mail increases and additional servers must be installed in the future, the servers can be installed without having to stop the e-mail system.

6. Conclusion

We have introduced examples of the IPCOM EX series relative to the stability and safety of enterprise IT networks using network functions.

We will continue making further improvements to IPCOM based on the concept of integration through ongoing efforts toward improving the stability and safety of enterprise IT systems.

References

1) S. Temma: Simple High-Reliability Network Servers. (in Japanese), *FUJITSU*, **56**, 1, p.47-53 (2005).
2) Nikkei BP: Fujitsu's New Challenge. (in Japanese), Tokyo, Nikkei BP, 2004, p.111-116.

Shoji Temma, *Fujitsu Ltd.*

Mr. Temma received the B.S. and M.S. degrees in Computer System Engineering from Hiroshima University, Hiroshima, Japan in 1981 and 1983, respectively. He joined Fujitsu Ltd., Kawasaki, Japan in 1983, where he has been engaged in research and development of communication processors for mainframes, and since 2001, he has also been engaged in R&D of IPCOM.