2005 version

IPv6 Deployment Guideline

Security edition

March 2005

IPv6 Promotion Council of Japan
DP-WG Security SWG

About this document

This document includes exhaustive coverage of the changes caused by “IPv6 technology in the migration process to IPv6, and analyzes the influences on security due to individual changes and discusses countermeasures and tasks ahead.

Description of security in Deployment Guideline of each SWG refers to the relevant part in this document. Security in the BCP and IPv6 propagation period described by each SWG working for large enterprises, local governments, SOHOs and households is analyzed and evaluated in Sections 4 and 5.

Table of Contents

1. Introduction

Purpose

The purpose of this SWG is to propagate IPv6 (deployment promotion) by organizing various issues and solutions regarding security by compiling them into a guideline, based on the consideration of the fact that “it is quite unlikely to migrate to IPv6 without consideration for security”. Concretely speaking, we organize and analyze the influence of IPv6, investigate and present the countermeasures and clarify the issues. Additionally, we examine the advantages of IPv6 resulting from changes in technical methods or increased options.

Security Advantages of IPv6

Before examining the countermeasures for IPv6 security, we present some security advantages of IPv6. The following are the advantages gained from usage of IPv6.

・The environments in which IPsec can be used for E2E will expand.
・Confidentiality (encryption) and integrity (detection of falsification) are improved.
・Uniqueness of addresses is guaranteed even in a closed network, making system administration easier.
・Availability (prompt detection of abnormalities) and integrity (decrease in inconsistencies in management) are improved.
・Specification and tracing of terminals become easier.
・Availability (prompt segregation) and integrity (prompt repair/recover) are improved.
・It becomes easy to construct a Plug & Play system including security measures.
・Compatibility level between availability (reduction in incorrect settings) and confidentiality (access control, etc.) is improved.

Targets of this Document

The following are the targets for this document (assumed readers) and roles of those targets.

Targets	Roles
SIer	IPv6 solution design/construction/usage guideline
Information system administrator	Usage guideline of IPv6 migration processes

Examination Range

The examination range of this document is as shown below.

・Influence on security from changes caused by IPv6 technology
・Security measures in the usage scenario of BCP and IPv6 deployment period, which is discussed in each SWG for local governments, large enterprises, SOHOs and households.

The examination items for security widely range and the countermeasures for them are integrated measures of “consciousness x policy x technology”. Investment in technology alone doesn’t help to improve security. We need to be aware that IPv6 will expand the “range” of usage flexibly, but on the other hand a clear usage process based on the user’s consciousness and policies become more significant.

The concepts behind security measures (from the following page) and the current (IPv4) security measures and trends (Section 2) are also included in this document as other content aside from IPv6 technology in order to supplement the understanding of readers, before examining issues mentioned above.

Security Measures Are …

Security measures are the integrated measures of Technology x Consciousness x Policy. Technology and system measures alone are not sufficient to cover overall security. Everything must be properly utilized in order to realize an effect. “Just one” countermeasure error, loophole or oversight will compromise integrity.

It is necessary to fully enforce security policy including usage and improve security consciousness and moral.

Security Measure Technology

As a security measure, it is important not to depend on technology and system too much.

No matter how rigid the security system is, it has no way of defending itself from an attack by people inside.

The main points of countermeasures are physical isolation, blocking and limitation of users/resource access control.

Regarding the security measures to be installed, it is crucial to understand what they can do and what they cannot do. It is essential that we do not expect to solve everything with just one security measure. It is possible to improve the overall security level by combining measures at multiple points.

Security Consciousness/Literacy

However rigid the system is, the security level may be compromised by a lack of awareness in the people who operate it. Therefore, it is important to improve the awareness of security issues.

For instance, we need to pay attention to the following points.

- Shared usage of accounts
- Simple passwords, or disclosure on post-its, etc. in places where anybody can see.
- Social hacking
- Request for reissuance of account
- Request for resetting of password
- Application for usage of server

Training and evaluation on a regular basis are crucial for maintaining security. Security disaster prevention drills, etc. should be performed strictly.

Security Policy

With regard to security policy, its definition is not the only important issue usage and application must also be considered. The point is how well we apply the security policy to users and machines.

It is also important to take a balance in expenditure for countermeasures according to the level of damage and loss in the event of an accident. There is no 100% safe security measure, and cost increases in proportion to safety. Therefore, we must consider the balance between the value of the system data we have to protect securely and required cost. Security measures for military and national security High security and high costs are necessary for military and national security.

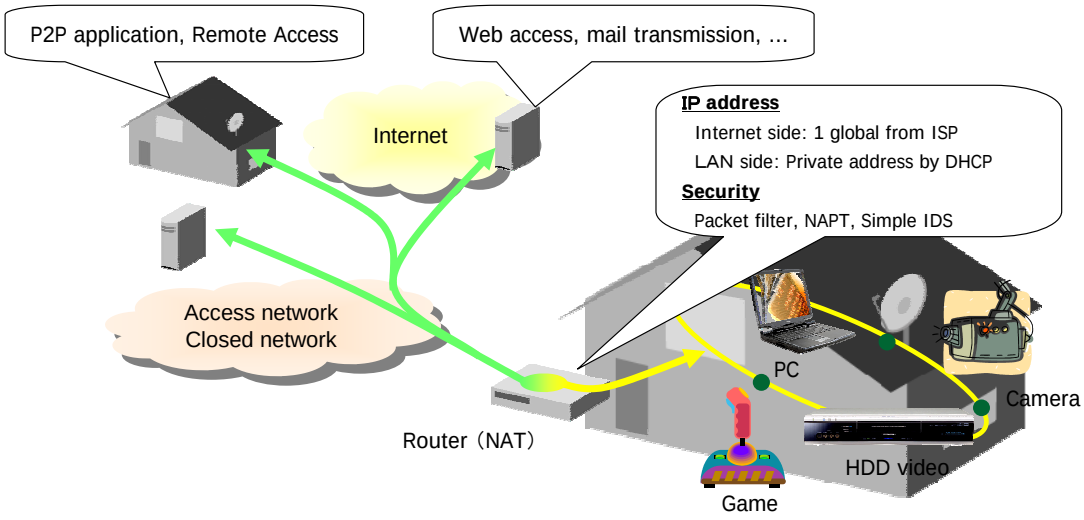
It is also important to remember to assess the cost required for actual security measures as well as the complexity of usage. For example, we need to assess whether the efficiency of regular business or operation will be affected by unnecessary security measures, how far we expect to ensure security, what level of risk we are able to accept.

2. Present Security Measures and Trends for (IPv4)

Present Security Measures ~ Home ~

The following Fig. shows a present home network connected to the Internet using IPv4.

- Typical example of IPv4 Home Network



There are access network terminal devices including a media converter and router, PC, game machines, AV machines, HDD video machines, network supporting cameras, network supporting sensors and home gateways as connection devices.

The home network may be hard wired or wireless (802.11a/b/g).

This network is mainly used for browsing the web, mail (usage as a client), messenger systems (using P2P), mail and web server in the household (some skilled users) and remote video booking (partially service-in).

The firewall using the router is the fundamental security measure. Packet filtering and NAPT function are the main configuration, and some routers are equipped with stateful packet inspection (SPI) function or simple IDS.

A personal firewall function is also incorporated in the PC, however, it is mainly used for scanning mail viruses.

Virus scanning is provided to households by ISP or ASP. Some skilled users access a server at home for video programming Dynamic DNS+Static NAT.

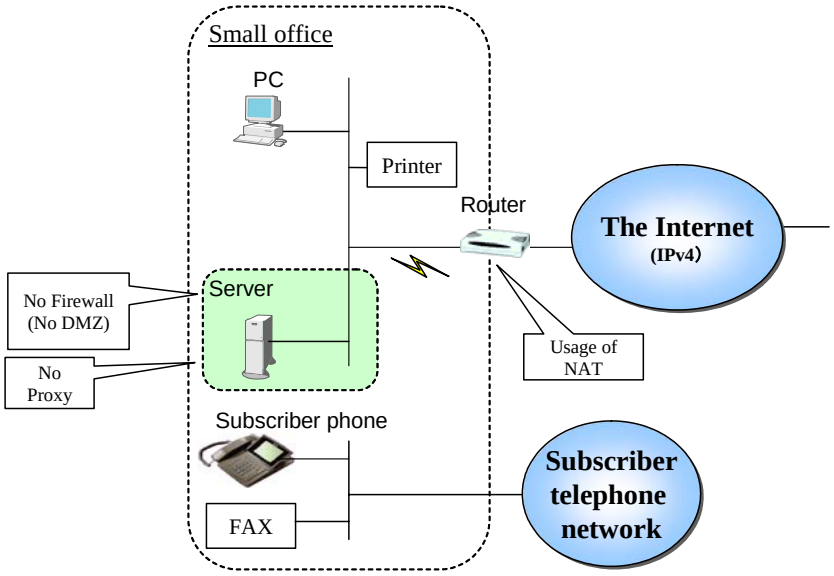
The present security of the home network can be analyzed as follows.

There is a limitation of incoming packets by NAT as a basic rule, therefore, most users are not able to go beyond default settings. Free spot will be mistakenly provided if Incidents if AP is left as the default setting. Non-PC (HDD video, network supporting camera, etc.) prevents the threat from networks by communicating with specific servers on the Internet (Proxy, regular mail Polling), however, security functions equivalent to those on the PC are not implemented in many cases. Therefore, once a worm, etc. enters the home network, the degree of damage becomes higher.

Present Security Measure ~ Independent SOHO ~

The following Fig. shows the configuration of network connection for independent SOHO.

- Typical IPv4 example of independent SOHO Network



The devices connected to the network in an independent SOHO are PCs, printers, dedicated terminals, business servers, NAT routers, etc.

The network is used for transmission of mail outside of the company, Internet browsing, usage of ASP or self constructed sales web sites.

Web browsing, mail, ASP, printing, real-time application, streaming and update tool applications are used.

The security measures are basically the same as those used for the home network.

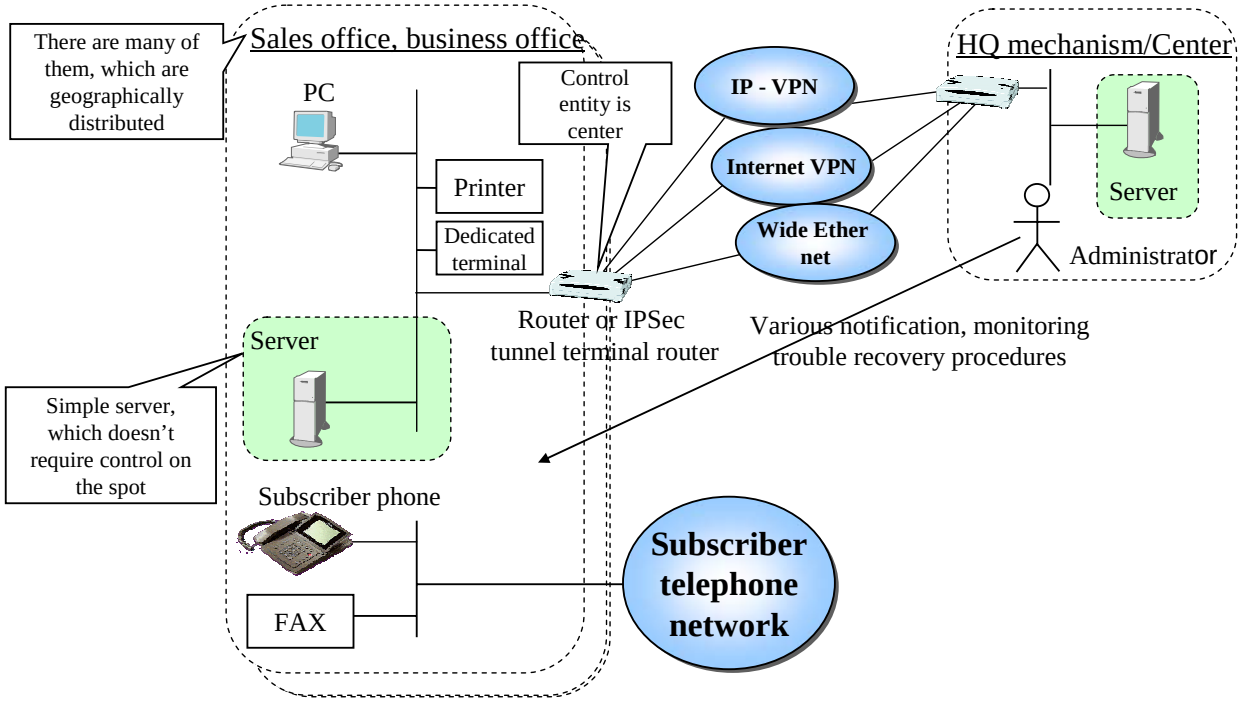
The security of an independent SOHO can be analyzed as shown below.

The technical skill level is probably better than that of the home network operator, however, halfway usage may allow greater damage than that to the home network through leakage of customer information, etc. Moreover, in the case that a self constructed web site for sales is present, a fixed global address is assigned to the NAT router, therefore you will be vulnerable to DoS due to the processing capability of the NAT router, and if security patch updates are erratic, information assets may leak from the LAN through illegal access code that comes through port No.80, etc.

Present Security Measures ~ Dependent SOHO ~

The following Fig. shows the connection configuration of a dependent SOHO.

- Typical IPv4 example of dependent SOHO (sales branch/business branch of company) network



The devices connected to the network in a dependent SOHO are PCs, printers, dedicated terminals, business servers, NAT routers (equipped with IPsec function) and so on.

The fundamental configuration of the network is the same as that of the independent SOHO, however, a dependent SOHO is connected with the enterprise center where the administrator is situated via IP-VPN, Internet VPN or wide area Ethernet network.

Apart from the linkage system with the center, the applications used for dependent SOHO are the same as those used for independent SOHO (Web browsing, mail, ASP, printing, real-time application, streaming, update tool, etc.).

It is possible to consider the dependent SOHO as a part of an enterprise Intranet as a basic rule, therefore, the same measures are used as those for terminals and servers on an Intranet (refer to Large Enterprise/Local governments segment).

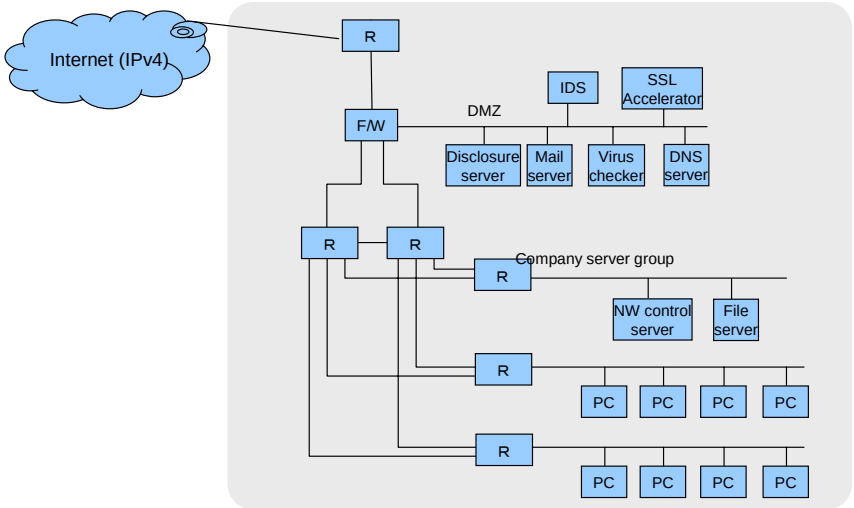
The security of the dependent SOHO can be analyzed as follows.

The contents are basically the same as those of an enterprise Intranet. However, when the Internet VPN is used, the tolerance of DoS against the global address on the WAN side is low due to the processing capability of the VPN router. Mistakes in description of the IPsec policy or simple setting of Preshared Key may allow VPN by illegal users.

Present Security Measures ~ Large Enterprises/Local Governments ~

The following Fig. shows the typical connection configuration of a large enterprise or local government.

- Typical IPv4 example of large enterprise/local government network



The following are the features of a large enterprise/local government network.

In a relatively large network where a special dedicated section administrates the overall network and there are more than several tens of users, an Intranet is used inside the organization. Such Intranets provide the mail or web application services inside and outside of the organization.

In this sort of organization, cost effectiveness is particularly sought after.

The security policy is maintained and controlled strictly by the network division. If any failure occurs in the network facilities, the degree of influence on society and the organization is rather large (redundant configuration, regular update of facilities).

The devices connected to the network are PCs, various servers, routers, switches, IDSs, firewalls, anti-virus gateways, etc.

The network is used for transmission of mail communicated inside and outside of the company, access to external web sites via proxy, sharing file/DB on the business server inside the company or access to mail/group ware (scheduler, etc.) from outside of the company.

As a security measure, first of all, the firewall is used to blocking access to the internal network. Connection from inside the company to outside of the company is made via a server (http/ftp proxy, mail, name resolution), so that the inner network is hidden and virus/content checks are performed. For remote access to mail/group ware, dial up to RAS or Internet VPN (SSL, IPsec) are generally used, and access is controlled by VPN connection authentication (mainly ID/Password are used).

The following is an analysis of the security of large enterprises and local governments.

For the present usage status, the internal and external networks don't always have to communicate each other directly, and the above mentioned countermeasure model is normally used. When the enterprise Intranet uses global addresses internally as well, http/ftp proxy is not setup in some cases (depending on policy).

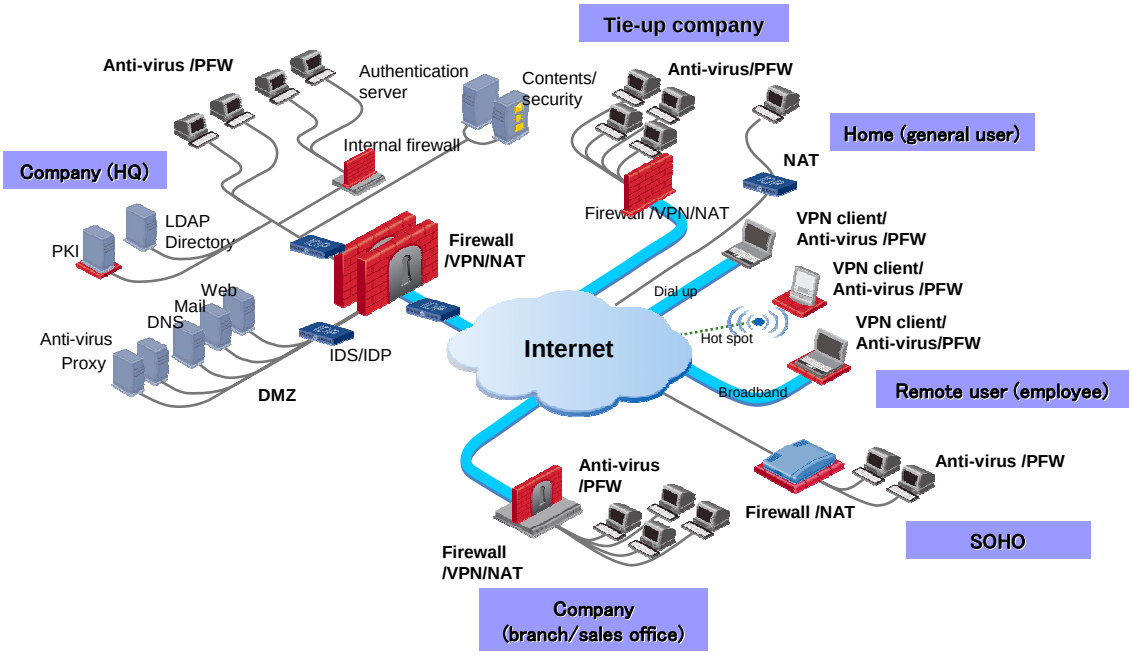
On the other hand, it is pointed out that the above mentioned model is vulnerable to internal damage, therefore it is necessary to prepare defense procedures to prevent the leakage of information caused by PCs taken in or out or damage from internal infection, such as encrypting the files themselves, limitation of operation and inspection of vulnerability.

Present Security Technology

For what sort of threats is the present security technology used? What are the added effects and risks resulting from the usage of such technology?

The security technology of IPv4 consists of the boundary firewall, PFW (Personal firewall), Proxy, IDS/IPS, anti-virus, NAT and VPN.

Usage environment of IPv4



The features of each area of security technology are as shown below.

Summary of Security Technology of IPv4

Name	Outline	Main products
Firewall	Router, server, etc. that is set in order to prevent illegal intrusion from outside (Internet) to inside (LAN). They are used to limit communication from outside to the minimum necessary and defend PC, etc. inside from external attack.	Check Point Firewall-1 Cisco PIX
PFW	The product to which the above mentioned firewall is installed on a client PC level. This is installed on a client PC in order to prevent illegal intrusion from outside to each client PC.	Trend Micro virus buster series
DMZ	This is a network situated inside Firewall and separated from outside (Internet) and inside (LAN). Connection to a server on DMZ is permitted by setting web server for external disclosure on DMZ, but a function to prevent connection to inside becomes executable.	
Proxy server	Server set to ensure security when making an external connection. This server accepts access requests (HTTP, FTP, etc.) from a client inside firewall and makes access to external resource by proxy of a client.	Squid DeleGate
IDS/IPS	IDS means Intrusion Detection System. This function detects illegal intrusion from outside (Internet) or unauthorized network or host and gives a warning to an administrator. IPS is a function for carrying out defense dynamically against illegal intrusion in addition to the function of IDS. When illegal intrusion occurs, this detects and blocks it.	TripWire Internet Security Systems RealSecure series

Summary of Security Technology of IPv4 (continued)

Name	Outline	Main products
Anti-virus	This software detects and destroys computer viruses breaking into a computer in order to cause damage to a computer, etc.	Trend Micro Virus buster series Symantec Norton AntiVirus series
NAT	This is a technology that converts private IP addresses used inside (LAN) to global address in order to connect to outside (Internet). It is not possible to connect to a computer under NAT transparently from outside, therefore NAT is now an effective security measure function.	Furnished on BB router, etc.
VPN	Normally encryption or authentication is not performed on the Internet, therefore the security level of the Internet is not very high. VPN is a technology used to carry out mutual connection between bases using this Internet line as though it were a dedicated line. VPN improves the security level and makes communication between bases by using encryption or user authentication methods regulated between mutual bases feeding encrypted packets to the Internet. Even if a packet is eavesdropped at the middle, because it is encrypted, the security level is ensured.	Furnished to a router made by NetScreen or sold by Cisco, etc.

The following is a detailed explanation of those technologies.

Boundary Firewall

The boundary firewall functions to stop unnecessary communication made from outside to inside in order to prevent illegal usage of the service operated by the machines inside, intrusion or attack. Incidental to this is the performance of segmentation or authentication of DMS, etc.

It is also necessary to prevent attacks from inside to outside (emission of virus with SMTP engine to outside, etc.), and the boundary firewall provides the function of permitting only necessary communications in response to this requirement.

As an additional effect, it becomes easier to monitor the communication status (centralized control) and the cost is also reduced compared with cases where countermeasures are taken for individual machines.

The risk is that damage caused by a PC brought in may be distributed, it's not possible to prevent intrusion (worm, virus) through a permitted service and it is not possible to inspect tunneled communication (passing straight through).

PFW (Personal Firewall)

The personal Firewall is furnished with a function to stop unnecessary/illegal communication in order to prevent illegal usage of the service run by the machines inside, intrusion or attack.

When illegal communication occurs, this firewall prevents one becoming an unwitting attacker, stops illegal communication with the outside or blocks communication from illegal programs.

As an additional effect, it is ready to handle internal attacks caused by a PC brought in

from outside.

The risk lies in the fact that security levels vary according to each individual, which makes it difficult to control and the cost increases according to the number of clients.

Proxy

The proxy performs filtering with the destination URL, IP, etc. in order to prevent connection to a dangerous site. It also checks the contents in order to prevent the download of dangerous files.

In order to prevent the collection of internal information, it is possible to conceal a client IP (topology).

Additional effects exist in that it is possible to control connections such as HTTP and FTP centrally and it is possible to increase the speed (cash) of access to contents.

The risks are that the burden is high and the service (protocol) is limited.

IDS/IPS

IDS (intruder detection system) or IDP (intruder detection protection) defends against DoS, port scan or illegal access from worms, etc. For detection and defense against illegal access, signatures (illegal access pattern files) are used. Defense with IDS requires a linkage with a firewall.

The risk is discontinuance of service due to error detection. The merits are that no measure can be used before a signature is issued and a measure can be used only on a segment for which IDS/IDP is set.

Anti-virus

The purpose of anti-virus products is to prevent infection from viruses and worms.

The risk is that there is a time difference till a countermeasure is prepared for a new virus and updates to the latest pattern can be easily omitted in the case of some terminals.

NAT

NAT prevents illegal usage of the service operated by a machine, intrusion and attack by blocking the connection made directly to inside. It also prevents leakage of internal information (used as information to carry out an attack) by concealing the client IP address

(topology).

Additional effects exist in that it can be implemented on inexpensive broadband router, therefore it is low cost and it is possible to increase the number of connecting terminals without changing the network (application receives a limitation).

The risks are that the damage caused by a PC brought in may be distributed, infection and attack by worms and viruses through the usage of websites or mail.

VPN

VPN is used to prevent eavesdropping, falsification and spoofing. Internet VPN with IPSec uses IKE and PKI authentication is carried out.

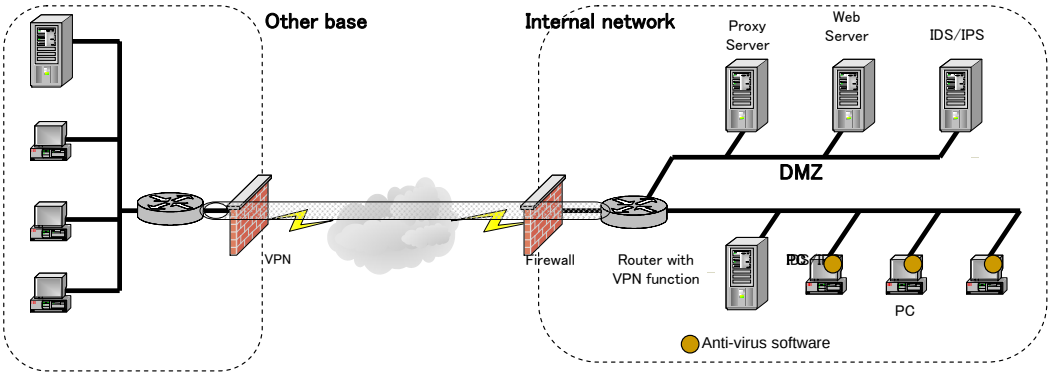
The advantage is that it is possible to use low cost WAN compared with dedicated line, and in the case of Internet VPN, it can be configured flexibly and promptly as long as there is a connection to the Internet.

The risks are that encryption may be compromised (as a possibility) and VPN gateway is vulnerable to DoS.

Security Technology Map

The technology explained above can be positioned as shown in the Fig. below.

・Security technology at each countermeasure point (layer) is shown below.



Layer	Security products
Internet layer	Firewall, VPN, NAT
DMZ layer	Proxy, IDS/IPS
Internal layer	IDS/IPS, anti-virus, PFW

Trend of Countermeasures

The following is an explanation of the transition of security technology and its recent trends according to the different categories shown below.

・From network layer to multi layer
・Sophistication of ID authentication
・Diversification of VPN
・Content security
・From post defense to pre-defense
・Sophistication of intruder detection
・Countermeasures are towards inside from boundary
・Distributed security and significance of control
・From single technology to architecture

From network layer to multi layer

Up to now, access has been controlled using the header information of the IP packet as the main condition. The main purpose of this was to protect networks from an attack by alteration or falsification of IP packet or a service disabling attack.

At present, attacks exploiting the vulnerability of applications and OS are increasing and rapidly becoming highly developed. Therefore, multi layer recognition and defense including at the application layer are required now. Which means that we can see a change from inspection of packets to inspection of streams.

Sophistication of ID authentication

The access range for enterprise networks, etc. has been expanded by providing remote access based on authentication as a condition. For this kind of authentication, static passwords, one-time passwords, 2 factors or tokens are used.

At present, the usage of certification (PKI) or biometrix is increasing. There is a growing awareness of the significance of authentication using a combination of items that only the person in question has. On the other hand, it is also required to share authentication information (single sign on) in multiple systems, belonging uniquely to a particular person.

Diversification of VPN

With regard to VPN, the encryption method used for products and algorithms are unique to a vendor, therefore it has been pointed out that it is difficult to secure compatibility and there is a limitation on export (import) due to key length.

However, the extension of Intranets by VPN between sites and remote access VPN is being actively performed, standardization of IPSec has been promoted and interoperability has improved. The extension to an Extranet is clarified as a need. Now the key length is extended and new encryption algorithms have appeared.

At present the trend is for an ever-increasing number of sites to require accurate and simple usage control of VPN, and VPN routing has become one of the issues. Moreover, there is a growing need to select the remote access implementation method, which is most suitable for individual access needs and conditions.

Content security

With regard to security at a content level, protection with anti-virus, URL filtering, filtering of unsolicited mail and malicious mail (JAVA/ActiveX) has been performed.

At present the trend is toward the use of information leakage prevention tools (checking the contents of mail), copyright protection technology (DRM, digital watermarking) and the usage of dedicated viewers that limit operations on contents.

From post defense to pre-defense

Up to now, defense based on a signature was performed after an attack was recognized, however, the period between discovery of vulnerability and actual attack is getting extremely short. There are also an infinite number of subspecies of virus, which makes prompt handling difficult.

The present trend is toward a focus on advance defense by solving vulnerability fundamentally, therefore it is required to perform update based on security knowledge including fundamental resolutions.

Sophistication of intruder detection

Intruder detection technology has developed considerably. The detection of intruders is not the only the function of some network type IDS or host type IDS products, but they are now furnished with a function as IPS to protect networks or hosts from illegal intrusion. There is also a tool called “Honey pot”, which invites illegal intruders to a virtual network.

The present trend is for evolution on a signature base from post measure to prior measure, however, for the success of this evolution, improvement of accuracy is also required at the same time.

Countermeasures are towards the inside from boundaries

Up to now, security measures have focused on the boundaries of a network. Based on this concept, anti-virus has been installed and IDS has been used for monitoring.

However, the present trend is that people have started to become aware of the occurrence of internal threats or damage caused by flow of information. In order to minimize the internal damage, the effectiveness of segmentation has been taken into account. Here, isolation is one of the themes.

Distributed security and the significance of control

In the case of enterprise networks, along with the change in network configuration, it is observed that security points have started to be distributed from a single boundary security point to multiple security points at branches, etc. Therefore, it is becoming necessary to operate multiple security functions and components. It is becoming more and more important to develop security in multiple stages of disclosure segment, inside and at end point.

As a present trend, a change is observed from one-on-one multiple control to one-to-many centralized control, and security control is required to cover the overall network. The necessity to smooth the security operation cycle is increasing as well.

From single technology to architecture

As a method of handling security, it used to be a basic rule to list up the functions for handling security problems. However, with this method, it was difficult to prevent occurrence of gaps.

Therefore, the present trend is for security to be designed to use architecture in which the contents of threats, source of occurrence, prior defense, minimization of damage, post handling, restoration and improvement are incorporated.

General statement/overview

As a recent trend for security measures, it is being recognized that multi layer security measures are necessary for application level threats. Inspection inside an application (tag, command) and blocking malicious code on port No.80 are considered more important.

Preemptive advance defense is required, and as part of this, vulnerable terminals are isolated through inspection.

Defense and separation not only at the boundary level, but also multi layer level including inside and end point is the recent theme of security measures, and people's awareness has shifted from boundary security measures to internal security measures and isolation of terminals attacked and infected is gaining more interest (minimization of damage).

On the other hand, it is emphasized how important it is to control measures precisely and promptly. It is necessary to perform centralized control using a policy, improve speed of detection at each security point and control the security operation cycle smoothly.

3. Analysis of IPv6 Security

The purpose of this section is to cover the possible influences of IPv6 on security as far as possible and to indicate that these influences may occur depending on how the security measure is used, so that the information can be used as a reference when considering the actual security measures.

In fact, not all measures are required. The content and level of the measures varies according to individual usage scenarios and the situation/policy of users.

Please refer to Section 4 for analysis and evaluation in individual usage scenarios.

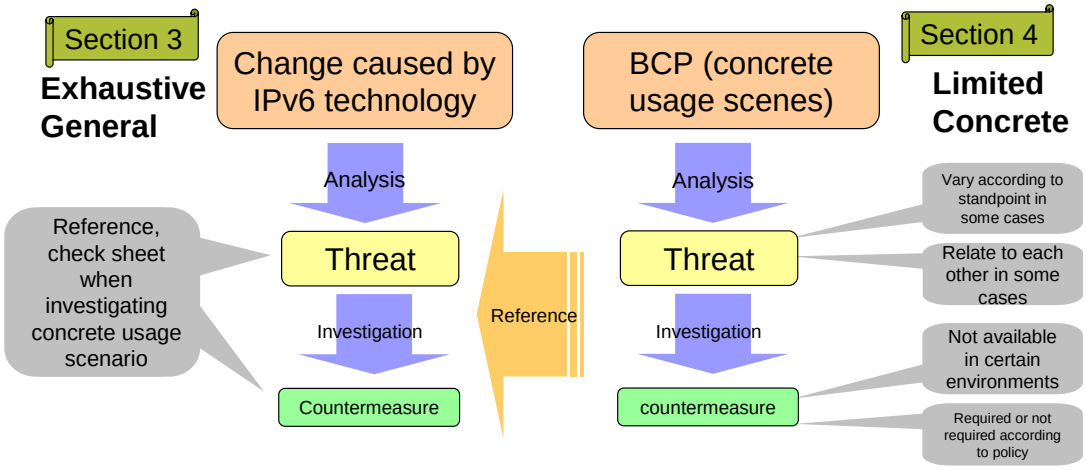
In this section, we analyze the changes resulting from “IPv6 technology”, which means that we talk about what will be changed by IPv6.

Here we analyze the influence (threats) made by individual changes to security, present countermeasure guidelines for such influences, describe concrete methods (examples) we are able to use as of now and present tasks and recommendations for IPv6 deployment period.

The difference between Section 3 and Section 4 is a difference in the method of approach. In Section 3, we analyze using items arising from IPv6 technology (change items) and in Section 4, we analyze using BCP (concrete usage scenarios).

Relationship between Section 3 and Section 4

- Difference of approach
  - Section 3: Analysis is performed on items (change item) caused by IPv6 technology
  - Section 4: Analysis is performed using BCP (concrete usage scenarios)



Changes Made by IPv6

The table shown below includes changes made by migration to IPv6 and threats on security due to those changes. A detailed explanation of individual items is given below the table.

Change by IPv6 (Part 1)

Item	Change	Sub-item	Threat
A	Direct reachability can be acquired by global address	A-1	Everybody can be a server (responder), therefore damage due to vulnerability of application is more actualized.
		A-2	Because it is possible to acquire direct reachability, the possible range suffering from DoS will spread inside of network.
		A-3	Usage environment of P2P application gets wider, but because the range of sender addresses and receiving ports is wide, it becomes more likely to suffer DoS.
		A-4	Encryption communication of E2E (Ipsec, etc.) will be easier, but because it is not possible to inspect inside a packet on a path, the risk of information leakage or worm infection may occur.
B	Information amount held by IP address itself incerases	B-1	Due to the uniqueness of the terminal when Eui-64 is used, it becomes easier to monitor the activity state of users.
		B-2	Frequency of human error at inputting IP address will get higher.

Change by IPv6 (Part 2)

Item	Change	Sub-item	Threat
C	Dedicated prefix environment gets wider	C-1	By attaching a string to communication log, privacy will leak.
		C-2	Probability of specification from outside gets higher and illegal accesses become more likely.
D	Anonymous address becomes available	D-1	It becomes difficult to control/specify the controlled individual.
E	Terminal is able to have multiple prefixes	E-1	Access control/operation is difficult, which encourages illegal access.
F	Terminal is able to have multiple interface IDs	F-1	Access control/operation is difficult, which encourages illegal access.

Change by IPv6 (Part 3)

Item	Change	Sub-item	Threat
G	ICMPv6 communication with E2E	G-1	It is possible to cause communication error by sending illegal NDP packet
		G-2	ICMPv6 Error is communicated with E2E, so it can become backdoor that network administrator can not control.
		G-3	RA has no authentication system, so net connection is made by L2 type intrusion which becomes a cause of illegal access.
H	Number of dual stack terminals (including translator, proxy) increases	H-1	If security level of IPv4 network to which pertinent terminal belongs and IPv6 network is different, damage using dual stack terminal as a platform will spread.
		H-2	If anti-virus software doesn't support IPv6, worm infection may occur using applications supporting dual stack.

Change by IPv6 (Part 4)

Item	Change	Sub-item	Threat
I	Tunnel protocol is introduced	I-1	Because of tunnel protocol, access control defined by boundary firewall may be ignored and reachability inside may be provided.
		I-2	Process ability is decreased due to DoS made to tunnel server
J	Usage environment of multicast will expand	J-1	Random attack by multicast transmission
		J-2	It becomes possible to attack aiming at a terminal by assuming a terminal address using a response to multicast.
		J-3	DDoS using a response to multicast becomes possible.
		J-4	By requesting a large amount of groups to join multicast, it is possible to flood multicast path table of router and to stop multicast communication.

Change by IPv6 (Part 5)

Item	Change	Sub-item	Threat
K	nonPC terminal (thin client) is connected to a net	K-1	It is difficult to handle a threat that exceeds implementation at shipping.
		K-2	It is difficult to implement sufficient security due to spec. problem of machine, therefore service cessation occurs easily.
L	Usage environment of mobile IP will expand	L-1	If Care of Address is outside of network, it gets difficult to control access.
M	Reverse resolution record for IP address doesn't exist in many cases	M-1	It is actually impossible to authenticate users by reverse resolution.

The following is a detailed explanation of individual changes and threats included in the table above. We use the configuration shown below for the explanation.

Outline

・Outline of threats is described.

・Cause-and-effect relationship between changes and threats. Where (occurrence point) and what sort of threat (assumed damage) could possibly occur.

Types of threat

・Types of threat (direct threats, not additional or secondary threats) are described using keywords. It's OK to select multiple keywords.

・Keywords: information leakage, spoofing, eavesdropping, service cessation, falsification, platform, intrusion of illegal code (worm), uncontrollability, undetectability, etc.

Analysis of threats

・The nature of the issue (what the cause is, whether the same threat occurs in IPv4 as well), occurrence frequency and significance of the damage are described.

・If a threat could become a merit under different circumstances or if seen in a different way, a comment about such a threat is made here wherever possible.

Guideline for measures

・The concept of the measure (idea) is described.

・Comments are included here if this concept gives (derives) any influence.

Implementation method

・In order to see the operability of the measure, supported products and resolution method

using existing procedure are described.

Issues and recommendations for IPv6 deployment period

・In the case that there is no implementation method, the issue is described here to indicate what sort of method is required in the future.
・Things required for IPv6 deployment period and recommendations are described.

A-1

Outline

Up to now, a terminal under NAT could only be an initiator, so even if the server application is started carelessly, it didn't receive any direct accesses. However, in the case of IPv6, when global unicast address is allocated to each terminal, each terminal can easily become a responder, therefore, there is a risk that the damage focusing on the vulnerability of the application will be actualized.

Types of threat

Intrusion of illegal code (worm)

Analysis of threats

The fundamental cause is whether update of security patch is performed properly. Therefore, the situation is the same for the connection at application level regardless of whether it is under NAT or not.
However, the range of address is wide, therefore, when a measure that is not easily specified by a third person (not registering with external DNS, not using easily targeted address (::80)) is used, it is possible to underestimate the threat.

Guideline for measures

Reduction of vulnerability by updating security patch. Limitation of communication origins by controlling access.
In the case of disclosed server, measures to prevent distribution of damage when infected are required, such as separation of segments.

Implementation method

It is required to update security patches and install IDS supporting IPv6 and firewalls supporting IPv6 application.

Issues and recommendations for IPv6 deployment period

It is necessary to have a firewall linked with IDS or IDP to support IPv6.

A-2

Outline

Because it is possible to get direct achievement, the range of receiving DoS will spread to the inside of the network.

Types of threat

DoS attacks

Analysis of threat

Because the address range is vast, it takes time to collect information (port scan, brute force attack) before DoS attack, therefore the efficiency is not good.

Guideline for measures

Monitoring of access made externally and blocking of specified packets are the basic measures.

Implementation method

Unnecessary access made externally is blocked using boundary router or firewall. It is important to collect information and watch for threats by logging and monitoring traffic from outside in order to execute the measures when unpredictable trouble occurs.

Issues and recommendations for IPv6 deployment period

It is required to have a firewall linked with IDS or in which IDP supports IPv6.

A-3

Outline

The usage environment of P2P applications will broaden, but because of the wide range of sender addresses and receiving ports, it becomes more exposed to DoS attacks.

Types of threat

DoS attacks

Analysis of threat

Because the address range is vast, it takes time to collect information (port scan, brute force

attack) before DoS attack, therefore it can be said that the efficiency is not good. Once you allow the intrusion, the damage may possibly spread to other Peers through analysis of internal segment and communication log.

Guideline for measures

A measure can be set according to the policy for monitoring access from outside, block a specified packet and separate a segment of a terminal when a terminal allows access from outside.

Implementation method

As described in “Guideline for measures”. It is important to collect information and watch for threats by logging and monitoring traffic from outside in order to execute the measures when unpredicted problems occur.

Issues and recommendations for IPv6 deployment period

It is required to have firewall linked with IDS or in which IDP supports IPv6. There is also a hopeful expectation on the stateful access control mechanism using a linkage between presence control mechanism and firewall.

A-4

Outline

Encryption communication of E2E (IPsec, etc.) will be easier, but it is not possible to inspect inside a packet on a path, therefore, there is a risk of allowing leakage of information or worm infection.

Types of threat

Information leakage, Intrusion of illegal code (worm)

Analysis of threat

Because IPsec is implemented as standard in the form of IPv6 protocol stack and the connection is not in NAT environment, which is the point of difference from IPv4, the usage frequency of IPsec will increase.

In the case of IPsec, the TCP/UDP header part is encrypted as well, therefore the existing access filter for these protocols will no longer be usable.

Guideline for measures

As a security policy of the organization, the communication destination is limited for IPsec communication with outside. However, this will cause the inhibition of distribution of

services that use IPsec for E2E, etc.

Implementation method

IKE and IPsec protocols with unnecessary communication destination are blocked using firewalls or boundary routers.

Issues and recommendations for IPv6 deployment period

Policy control solution for a terminal that permits IPsec and contents check mechanism (anti-virus, content filter) are required.

B-1

Outline

EUI-64 used as an interface ID is created based on the MAC address of the terminal, however, due to the uniqueness of EUI-64, it will be easier to monitor when and where a user activity takes place.

Types of threat

Compromised privacy

Analysis of threat

This threat can occur when you get an address using stateless address auto setting and connect the network at several points outside of the company. A likely case is that the activity state is analyzed by unwitting access to the specified host using header information of E-mail or HTTP mail display or the log of P2P application usage with an unspecified person.

Guideline for measures

It is important not to communicate with unspecified persons needlessly. It is also effective to hide unique interface IDs or delete IP address information from application usage log.

Implementation method

Anonymous address or DHCPv6 can be used. Or, a proxy can be used in order to hide a terminal address.

Issues and recommendations for IPv6 deployment period

Current state of implementation of application varies, but it is considered that RFC3484 accords permanent address priority over temporary address. It is preferable to have a system with which users are able to change source address according to the user's policy.

B-2

Outline

In the case of a system or device for which a user inputs an IPv6 address manually using a user interface, there is a possibility that the number of input mistakes increases compared with IPv4, which may cause a decrease in reliability for the system or provision of a port for illegal access.

Types of threat

Decrease in reliability for the system, widening the port for illegal intrusion

Analysis of threat

This depends on the user interface of system or device, but in the case of a system or device in which IP address is input frequently with user interface, there is a possibility of having an influence by incorrect input of address and causing abnormal operation of the system. If IP filter is input incorrectly for firewall or router, a port for illegal access may be provided.

Guideline for measures

It is necessary to eliminate unnecessary manual input of IP addresses. In the case of a system in which IP addresses are input frequently, it is recommended to use identifier (host name) corresponding to IP address in order to reduce human error. It is also effective to use a butting system with the connection terminal information such as Neighbor Cache.

Implementation method

The method relies on the user interface of the system or device, however, it is not too difficult. However, some current personal firewalls don’t distinguish IPv6 addresses (control only the service).

Issues and recommendations for IPv6 deployment period

In the deployment period of IPv6, it is recommended to use tools or user interface with which users don’t need to input IP addresses any more than necessary.

C-1

Outline

Even in a general ISP connection service, IPv6 address (prefix) is allocated in a fixed manner, therefore, there is a risk that the access state information of users is collected

based on IPv6 addresses.

Types of threat

Leakage of privacy (analysis of access trend)

Analysis of threat

Even in former dynamic address allocation using DHCP, it was not impossible to specify a user from IP address by checking a session log on the ISP side, however, if a session log is not disclosed, it is difficult for a third person to trace a user. When a prefix is allocated to individual users in the IPv6 service, it becomes easier for a third person to identify a user. It is also possible to specify area information or upper ISP easily using address aggregation structure of IPv6 addresses. Moreover, it is easy to put a string on information using fixed IPv6 address as a key through a method combined with putting a string on address information and mail account included in E mail headers and inviting access from URL links sent in SPAM mail.

With regard to unreliable external services, accessing using anonymous addresses can be used as one countermeasure. However, in the case that there are many terminals in the network segment with the same prefix inside a company, etc., it is possible to hide behavior or action of an individual terminal, but when it comes to home or SOHO, though it is effective to prevent specification of a terminal, the number of terminals in a prefix is not large enough to defend information on behavior of organization/home or network usage state being collected, therefore, no effect can be expected.

.

Guideline for measures

To prevent needless leakage of IP addresses outside.

Implementation method

When setting a mail server, it shall be set not to display the IP address of a client in the “Received” line of a mail header. Moreover, when setting a mail client, it shall be set not to display the IP address of a client in the “Message-ID” line of a mail header. Or, application proxy can be used to limit IP address when accessing externally.

Issues and recommendations for IPv6 deployment period

Along with the deployment of IPv6, the opportunities for an attacker to collect IPv6 addresses or select as the target of attack will increase. There is no change in the content and countermeasures for threats between migration period of IPv6 and deployment period of IPv6.

C-2

Outline

It is possible to attack by throwing a packet to the dedicated prefix.

Types of threat

Illegal intrusion, DoS(DDoS)

Analysis of threat

There is a risk of the address used conventionally such as <Prefix>::1 to be exposed to DoS attack. It is also possible to attack by creating a target list (128 bit address) through collection of IPv6 addresses organizationally. Possibility of brute force attack reaching the terminal is low, but it becomes a burden on the NDP solution itself on SOHO router, therefore, it has a chance to be DoS.

In the environment of IPv4, dedicated global addresses were limited to various servers, however, in the case of IPv6, the number of target nodes for this kind of attack will increase. Nonetheless, it is assumed that there are many vulnerable notes for which a security measure is not used properly on the network. There is a risk of the occurrence of a larger scale of distribution attack using these terminals as a platform such as DDoS attack.

.

Guideline for measures

It is necessary to use and control sufficient security measures using firewall, etc. for a terminal that has a dedicated address, which is reachable from the outside.

When using E2E communication at the same time, it is necessary to permit communication from external unspecified majority to the terminal inside the boundary. It is necessary to use the system to control the boundary firewall rules dynamically by, for example, permitting communication to inside dynamically and temporarily through monitoring session establishment/authentication sequence of E2E communication such as monitoring packets. Moreover, when the anonymous address is used in combination, it becomes possible to prevent the risk of DoS or attack on a specified terminal from outside to a certain degree.

Implementation method

Unnecessary access from outside shall be blocked using boundary router or firewall. When using E2E communication service, security measures shall be executed for the terminal side assuming that the communication is carried out directly to the devices inside the boundary from unspecified majority (firewall of host base, etc.). It is necessary to collect information and observe the state by logging and monitoring traffic from outside in order to execute a measure at the occurrence of unpredicted trouble.

With regard to access outside of the organization, it is possible to consider using the

anonymous address as a method of reducing the risk of receiving an attack, however, this method doesn't solve the problem completely. Moreover, in the case of application service demanding E2E communication, it is considered that the anonymous address will be a problem (it is necessary to re-register own address whenever anonymous address is changed, etc.).

Issues and recommendations for IPv6 deployment period

Along with the deployment of IPv6, the opportunities for the attacker to collect IPv6 addresses or choose the target for attack will increase. There is no change in the content or measure of threat between migration period to IPv6 and deployment period of IPv6.

D-1

Outline

When a user within an enterprise uses an anonymous address, it becomes difficult "to specify a user from various access logs", which used to be executed in the network control of IPv4.

Types of threat

Uncontrollability

Analysis of threat

Anonymous addresses are a method of making the tracking of a host difficult, in this method the host generates the lower 64 bits of the address using random numbers and changes it at certain intervals. When usage inside an enterprise is assumed, a user is not specified in communications outside of the company, but on the other hand, there will be a problem that it is difficult to specify a user when a problem occurs such as illegal access. For example, the 2 cases shown below may occur.

(1) When tracing an attempt to make illegal access from inside a company to a server in the enterprise is discovered.
(2) When illegal access occurs on a server outside of the company and the address prefix of the access destination is within the allocation range of ones own company.

Guideline for measures

A mechanism should be installed, with which it is possible to specify a user even if an anonymous address is used. Or it is recommended to set a rule not to use anonymous addresses inside the company. Anonymous addresses are furnished for Windows XP as

standard, however, it is possible to disable their use.

Implementation method

A function to control IPv6 anonymous addresses shall be added to the existing user control software in order to enable specification of a user from an access log. When IPv6 is used only inside the company, it is possible to prohibit the use of anonymous addresses.

Issues and recommendations for IPv6 deployment period

Even if a rule is set prohibiting the use of anonymous addresses, it is necessary to change the setting by a user thoroughly. Whatever the case may be, in order to perform strict operation, some kind of system to control IPv6 terminals inside the company is required.

E-1

Outline

When a terminal has multiple prefixes, access control/operation will be difficult, which may encourage illegal access.

Types of threat

Operation miss due to complication of setting, injection of illegal path information, packet eavesdropping, falsification, preparation for intrusion/attack, connection highjacking, DoS attack

Analysis of threat

When the address usage form in which there is one address for external access and there is a private address space inside the organization is used, just like in many organizations using IPv4, operation by allocating multiple IP addresses becomes possible and the number of address prefixes to be handled increases. If device setting, path information exchange and filtering are not performed as properly as or even more properly than operation with IPv4 for each address prefix, various security holes such as illegal access will occur.

The possibility of an increase in the number of incorrect settings or operation miss due to the complication of setting will increase.

In the multi home environment, it will be exposed more easily to the threat of DoS attack such as packet eavesdropping by redirecting to a third person, falsification, connection highjacking and flooding using intrusion path, which is difficult to trace.

In the case of an organization that performs sloppy management, if re-numbering and re-assignment becomes easier, it may interlock with the injection of illegal path and encourage attacks from inside to outside.

Guideline for measures

When the number of IP addresses to be handled increases, it becomes necessary to aim at integrative control such as interlocking with security devices including IDS or IPS and applications

Taking into account that a large scale security hole may occur if a system approach is not made beforehand, it is necessary to forecast influences such as personnel and system operation costs for analysis and handling measures for the occurrence of problems and to establish a method to handle the situation.

If policy control is not performed properly for a path, it may become a platform or a target for DoS attack itself, therefore monitoring is important.

When a multi-prefix and multi home environment is established, it is highly possible that an unexpected new type of attack may occur, so it is necessary to research various latest trends.

Implementation method

It is necessary to control prefixes exhaustively. After monitoring the inside and outside path control property, address and routing shall be designed. It is also required to use access control for each terminal and each prefix held by terminals and defense mechanism using a dynamic filter.

Issues and recommendations for IPv6 deployment period

It is considered necessary to realize the following measures in the future.

・Installation of appropriate authentication at updating path or establishing connection
・Installation of control and blocking method of bad RA transmission, etc.
・Appropriate mapping and control of locator/identifier
・Setting control at re-numbering and re-assigning and introduction of authentication
・Installation and usage of sufficiently evaluated application (implementation of source address section/RFC3484, etc.)

F-1

Outline

When a terminal has multiple interface IDs, access control/operation will be difficult and illegal access will be encouraged.

Types of threat

Uncontrollability of terminal, illegal intrusion

Analysis of threat

If it is not possible to monitor the state of a terminal Interface that has multiple IP addresses, it practically means that it is not possible to control the terminal. If a filter doesn't work properly, intrusion path is provided for illegal intrusion. A possibility of highjacking using auto setting mechanism illegally gets higher, and there is also a risk of being accessed by all connection destinations that use an interface.

Guideline for measures

It is necessary to perform terminal control and IP address control properly. It is also necessary to aim at performing integrated control by installing a dynamic filter based on the above mentioned control or linking security devices such as IDS and IPS or applications.

Implementation method

It is necessary to provide appropriate user education (terminal control, access control, usage rule of application, etc.). In addition, access control of each terminal and each prefix held by those terminals, introduction of defense mechanisms using dynamic filter, etc., introduction of hop limitation, introduction of privacy extension or setting/implementation using relationship between application and prefix appropriately are also considered as implementation methods.

Issues and recommendations for IPv6 deployment period

If the number of connection terminals increases along with the deployment of IPv6, damage will expand. There is no change in the contents or measures for threats.

G-1

Outline

When a malicious user flows an illegal ICMPv6 packet, communication in the segment is twisted or communication disability occurs.

Types of threat

Eavesdropping, service cessation, uncontrollability

Analysis of threat

Concretely speaking, the following attacks are assumed to occur.

・RA with prefix of segment is released all over the segment.
・NA with fake L2 address of default router is released to other user terminal.
・NS packet with faked L2 address part only from a certain terminal is released to a router.

・NA packet responding to NS packet for DAD is returned to other user terminal.
・NA packet responding to NS packet for NUD is returned to other user terminal.
・RA packet of which lifetime of default router is 0 is released to other user terminal.
・Redirect packet to illegal nexthop is released to other user terminal.
・RA including different prefix is released all over the segment.
・RA with faked only various parameters of RA (e.g. hoplimit) is released all over the segment.

These attacks are essentially the same as ARP/ICMPv4/DHCPv4 spoofing of IPv4. ICMPv6 packet is often broadcast to a link local/multicast address, therefore malicious users can easily get necessary parameters when attacking.
However, the problem occurs only in the Ethernet segment where users are able to communicate directly without using router, etc. Moreover, with direct communication between users as L2 for private VLAN or PPPoE, this problem doesn't occur either.

Guideline for measures

The release of ICMPv6 packets from a terminal to another user terminal shall be prevented. Or, a mechanism to authenticate ICMPv6 packets from a terminal shall be installed.

Implementation method

ICMPv6 packet filtering shall be performed on L2 device. Which means that, ICMPv6 packet between terminal storage ports is rejected (L3-4) or Private VLAN (L2) is used. In order to make a communication between terminals using global addresses, it is necessary "to use NDP proxy function" for terminal storage router or "to turn off ICMPv6 Redirect or turn off on-link flag of RA to be advertised". Terminal communication using link local address will no longer be possible.
If all ICMPv6 packets between terminals are rejected, normal operation of DAD is disturbed, so there will be a risk that duplication of address cannot be detected. However, when address duplication occurs, communication is not possible regardless of normal operation of DAD (because it is often implemented in a way that address is not created again after DAD fails). Therefore, it is expected that there will be no big problem for practical use (it is sufficient for a network administrator to be able to detect duplication of address).

Recommendations for the age of IPv6 deployment

It is also necessary to consider installation of SEND (Securing Neighbor Discovery). It is expected that prevention measures of address duplication through distribution of addresses using DHCPv6 will be implemented.

G-2

Outline

Under IPv6, fragment processing of packets or process for unreachable error is performed by a terminal. ICMPv6 Error packet required for control should be able to reach the terminal from arbitrary communication destination. If a network administrator doesn't perform filtering process for ICMPv6 Error packets at all in order to guarantee reachability, the ICMPv6 Error packet itself may become a back door which an administrator is not able to control (e.g., encoding confidential information to payload of ICMPv6 Error message, attacking inside from outside using ICMPv6 Error message).

Types of threat

Information leakage, service cessation

Analysis of threat

This is a problem unique to IPv6. However, if an attacker wants ICMPv6 Error to reach the attacking point, the attacker needs to know the IP address of the attacking point, therefore it is not easy to attack inside from outside (C-2).

Guideline for measures

It is necessary to make it impossible for an attacker to assume the target IP address for the attack. It should be prevented for ICMPv6 Errors with no calling or responding communication to go/come through the network boundary.

Implementation method

The range that can be communicated directly from the terminal shall be limited (communicate externally using IP address, port No., IPsec policy, Proxy).

When communicating externally from a terminal, anonymous address shall be used, and ACL for the address of EUI64 base shall be specified using personal firewall.

Recommendations for the age of IPv6 deployment

When carrying out stateful inspection using a boundary router, it is necessary to check the packet that is the source of occurrence of error included in payload part of ICMPv6 Error packet.

G-3

Outline

It is possible to get IPv6 global address or link local address through L2 type intrusion, which

means that if L2 type intrusion is made, illegal access results immediately.

Types of threat

Illegal access

Analysis of threat

The risks are the same as those from distribution of DHCPv4 address without authentication or illegal access by IPv4 link local address. The fact that intrusion is made in L2 type way will be an essential problem. Even if it is not possible to get an L3 address at all, it is possible to attack using eavesdropping or defective Ether Frame.

Guideline for measures

As a countermeasure, it is necessary to carry out access authentication of L2 in order to prevent illegal access even if an intrusion is made.

Implementation method

L2 security should be enhanced by physical guard or IEEE802.1x. Personal firewall on the terminal shall be used to minimize the accesses permitted from external terminals.

Recommendations for the age of IPv6 deployment

It is necessary to be able to perform DHCPv6 address distribution and DHCPv6 snooping. It is not possible to prevent attacks to link local address, but It is possible to prevent risk caused by getting the address more easily than by installing IEEE802.1x on all terminals.

H-1

Outline

If illegal intrusion is made from IPv6 (IPv4) network to the dual stack terminal, it can be used as a platform for a terminal connected to IPv4 (IPv6) network. So the risk of threat will widen. Moreover, when IPv4 and IPv6 are configured as separate networks, there is another possibility to be a threat such that terminals, which are not dual stack are used as a platform for each other if a translator (including web proxy) is set.

Types of threat

Platform, leakage of information

Analysis of threat

It is a problem to operate mixing IPv4 and IPv6, which have different policies. The causes of this problem may be that the mutual connection policy of the networks is not arranged

sufficiently, user uses the network without knowing it is “IPv6 ready” or that technically unsolved part (anti-virus soft, ID, etc.) of IPv6 network still remains. Even when IPv4 and IPv6 are configured as separate networks, if a translator is set at the middle and if the security measures are not furnished sufficiently, there is the possibility of causing a threat of networks being used as a platform by each other.

Guideline for measures

Administrator shall limit communication by permitting only appropriate communication in both directions on the firewall set at the IPv6 network boundary with outside. Administrator and end users shall use terminal firewall and security patches in a timely manner in order to improve the security of the dual stack terminal itself. Moreover, the administrator shall carry out security control of the translator itself (denying IPv4 map address or compatible address) in order to minimize influence range on non-dual stack IPv4 and IPv6 networks, and at the same time the administrator must limit communication via a translator and carry out control of the communication log passing through a translator appropriately.

Implementation method

Filtering setting shall be carried out on the firewall that makes connection with external IPv6 on a regular basis. Filtering shall be performed using adaptation of patches to dual stack terminal and terminal firewall on a regular basis. Moreover, security control of translator (denying IPv4 map address or compatible address) and log control via a translator shall be performed constantly.

Issues and recommendations for IPv6 deployment period

If the contents set for IPv4 (for IPv6) using firewall software for the terminal are applied automatically to IPv6 (IPv4) and the setting of one protocol can be changed as necessary, it is considered difficult to make a hole.

H-2

Outline

The current anti-virus software doesn’t related to IPv4/IPv6 with regard to file I/O, however, virus check of network part such as web or mail supports only IPv4 networks, therefore, it is not possible to handle a worm performing infective activity through an IPv6 network. As a result of the delay in development of anti-virus products supporting IPv6, there is a risk of infection by worm through an IPv6 network, which may encourage a worm to spread its activity range to the IPv4 network as well.

Types of threat

Intrusion of illegal code (worm)

Analysis of threat

Because worm measures are not developed for IPv6 networks, it is assumed that the infective activity of worms will be performed through IPv6 networks. Due to the delay in development of anti-virus products supporting IPv6, there will be a threat of worms spreading to terminals connected to IPv6 networks from infected machines, and at the same time, it is also assumed that IPv4 networks will become affected through a translator. Which leads further to the threat of expanded worm infection. On the other hand, another case can be assumed, where an access is made to IPv4 network through a translator and it is infected by a virus.

Guideline for measures

Administrators and end users shall update patches of terminal OS and carry out appropriate communication filtering using a firewall connected to an external IPv6 network. Moreover, the administrator shall investigate installation/implementation methods when anti-virus software supporting IPv6 networks becomes available. In order to minimize the influence range to non-dual stack IPv4 and IPv6 networks, the administrator needs to control the security of the translator itself (denying IPv4 map address or compatible address), and at the same time he/she needs to limit communication via a translator and control communication log via a translator appropriately. Of course, it is crucial to install anti-virus software supporting IPv4 on the terminal.

Implementation method

Virus handling software shall be updated on a regular basis and filtering shall be set on a regular basis on the firewall that makes a connection with external IPv6. Moreover, the installation of patches on the terminal on a regular basis, filtering on terminal firewall, installation of anti-virus soft supporting IPv4 and updating to the latest version shall be carried out. It is also required to carry out security control of the translator (denying IPv4 map address or compatible address) and log control via the translator constantly.

Issues and recommendations for IPv6 deployment period

When anti-virus soft supports IPv6 completely, the threats will be the same as those in the current virus measures for IPv4. Which means that updating anti-virus files to keep the latest state, not accessing doubtful sites or not opening suspicious attached files shall be used as countermeasures.

I-1

Outline

There is a risk of creating a path that ignores access limitation easily at the boundary firewall on existing network topology by turning protocol.

Types of threat

This is a threat for settings and operation, and it occurs at setting a tunnel for connection of IPv6 with the outside.

Analysis of threat

Because a path that allows free access remains in the internal segment, the network inside the organization is exposed to external attacks.

Guideline for measures

This threat can be prevented if the network is designed and controlled properly.

Implementation method

It is necessary to prepare measures such as access limitation or packet inspection for the tunnel server itself or on the path of tunnel server and internal segment. It is necessary to prohibit the creation of a tunnel end point on the terminal (Teredo of Windows XP), block tunnel protocol from tunnel server unless such a tunnel server is set properly, block unnecessary communication made externally with tunnel server or between tunnel server and internal segment or block communication that is counter to policy using access filter.

Issues and recommendations for IPv6 deployment period

Nothing in particular.

I-2

Outline

Degradation of traffic processing capability of tunnel server by sending large amounts of packets to a tunnel server is considered as a threat.

Types of threat

DoS

Analysis of threat

IPv6 connectivity will deteriorate. When a tunnel connection is used, tunnel server shall be

“Single point of failure” at all times.
A tunnel connection is a temporary usage status in the IPv6 migration period, therefore it is desirable to change to dual stack or native connection.

Guideline for measures

Authentication shall be carried out between tunnel server and client in order to limit usage of tunnel server from disallowed terminal. However, even in this case, if a terminal is infected with a worm, etc., it is not possible to prevent completely.

Implementation method

It is possible that it is effective depending on the tunnel protocol (DTCP) to be used or the use of other items (IPsec) together.

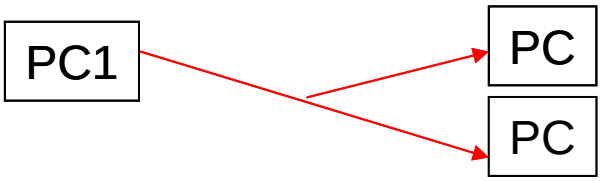
Issues and recommendations for IPv6 deployment period

Nothing in particular.

J-1

Outline

By sending a packet to a multicast address, it becomes possible to send an attack packet even if you don’t know the address of the other party.



Types of threat

Service cessation, illegal code intrusion

Analysis of threat

IPv4 multicast basically has the same problem, however, this sort of problem is not actualized yet because multicast is not used widely for IPv4.
In the case of a global multicast, the range of attack is wide, but very often no routing is made and even if it is made, it’s not easy to guess the routed multicast address, therefore it is not easy to attack in the same way as IPv4.
In the case of a link local multicast, the attack range is limited inside the segment, however, it moves even without routing. Moreover, many multicast addresses are known, therefore it is easy to attack (same as ARP storm attack).

Guideline for measures

One measure is to limit the number of multicast packets released to the minimum possible.

Implementation method

Source spoofing shall be prevented by Ingress Filter in terminal storage segment (enabling only global multicast). Multicast sender shall be limited by PIM Register ACL at Rendezvous-Point (enabling only global multicast in PIM-SM).

Intruder entry at layer 2 shall be prevented (effective for both global and link local multicasts (refer to G-3). Moreover, MLD snooping using layer 2 switch (effective for both global and link local multicasts) and prohibition of sending FF02::1 from a port other than a router using a layer 2 switch are included in the measures.

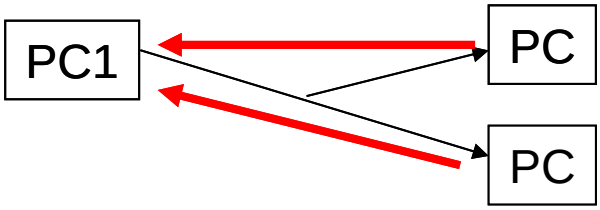
Recommendations for the age of IPv6 deployment

It is strongly desireable for small switches in particular to support MLD snooping (MLDv1 at minimum, MLDv2 if possible).

J-2

Outline

In a network where multicast is enabled, it is possible to guess the address or attributes of a terminal from unicast response of the terminal towards a packet addressed to multicast address (e.g. ECHO-REPLY to ICMPv6 ECHO, response to uPnP inquiry). It becomes easier to make an attack aimed at a terminal based on this information.



Types of threat

Illegal intrusion

Analysis of threat

Response to multicast causes provision of attack ammunition. It sometimes happens that multicast packets are addressed to a group that does not participate on the terminal (when other terminals in the same segment participate). Therefore, there is a possibility of the occurrence of this threat not only for link local multicasts. The same problem exists potentially in IPv4 (refer to J-1).

Guideline for measures

The countermeasure is for the network administrator to keep the release of multicast packets to the minimum possible. It is necessary to limit the participation of terminals in the multicast group to the minimum and to limit the responses of terminals to the multicast packet to the minimum.

Implementation method

As explained in “Implementation method” of J-1, it is important to release the minimum number of multicasts over the network.

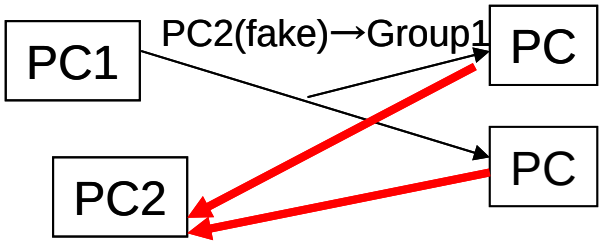
Recommendations for the age of IPv6 deployment

It should be possible to describe ACL for multicast packets and MLD reports using the personal firewall on the terminal.

J-3

Outline

In a network where multicasts are enabled, it is possible to make DDoS attack using a response to the packet (e.g. ECHO REPLY to ICMPv6 ECHO, Port Unreachable Error to UDP packet) by sending a faked multicast packet based on the address of the target terminal for the attack (PC2 in Fig. below) as a source.



Types of threat

Service cessation

Analysis of threat

This is an attack using a response to source spoofing and multicast. The same problem exists potentially in IPv4 (refer to J-1).

Guideline for measures

Source spoofing shall be prevented. Moreover, it shall be in such a way that the terminal issues the minimum possible responses to multicast packets (refer to J-2).

Implementation method

Source spoofing shall be prevented by Ingress Filter in terminal storage segment (effective only for global multicast). Moreover, responses to multicast packets shall be controlled by the measures shown in J-2.

Recommendations for the age of IPv6 deployment

Same as K-2.

J-4

Outline

When a large amount of multicasts join the Group, the multicast path table of a router overflows and the risk of proper multicast relay being disabled arises.

Classification of threats

Service cessation

Analysis of threat

This is an attack against the entry number of router. This is the same as IGMP join attack of IPv4 multicast or ARP storm attack of IPv4.

Guideline for measures

Unnecessary MLD Report shall be rejected using a router or prevented at the terminal from issuance.

Implementation method

MLD Report shall be rejected in ACL of router using a group address.

Recommendations for the age of IPv6 deployment

Nothing in particular.

K-1

Outline

If non-PC terminal (thin client) is connected to a net, it becomes difficult to handle a threat exceeding implementation at shipping.

Types of threat

There are all kinds of possibilities, however, in the sense that the vulnerability of non-PC platforms may be exploited in a malicious way, their use as platforms or for the intrusion of illegal code (worm) can be pointed out as possible threats.

Analysis of threat

In the built-in platform used on non-PC, security is not usually updated, therefore it is difficult to handle vulnerability if it is not discovered at shipping a product. Moreover, non-PC has no interface with which a user is supposed to update software, therefore it is not possible to take an urgent update measure other than by imposing a burden on the user such as collection by recall or taking the unit into a service contact. It can easily be imagined that customers get used to the existing usage form of the devices, therefore they don't understand the necessity and significance of the security update itself and use the device without using the latest security measures.

Guideline for measures

A passive handling method is to analyze the operation form of a non-PC terminal, and if it is sufficient that communication with the specified server is secured, it is possible to avoid the problem by blocking traffic from other than those servers or making communication through mutual authentication with those servers. Moreover, it is generally possible to improve

safety by limiting and authenticating a communication partner (server) using IPsec.
If a non-PC takes a form of action in which communication with an unspecified party is made, filtering shall be carried out by specifying the other party using stateful packet filter, on home router, etc.
Of course the ultimate resolution is to assure the framework that enables update of OS even in non-PC built in platform, however, this is not easy in terms of cost.

Implementation method

Communication partner of non-PC shall be limited, or packet flow to a non-PC shall be limited using stateful packet filter.

Issues and recommendations for IPv6 deployment period

It is necessary to construct and distribute the OS update mechanism of built-in platform.

K-2

Outline

There is a problem that if a non-PC terminal (thin client) is connected to a net, it becomes difficult to provide sufficient support for security.

Types of threat

When taking account the fact that non-PCs are weak at calculation, (in the sense that they are not suitable to use IPsec), we can point out that it is easily exposed to spoofing, eavesdropping, service cessation or falsification.

Analysis of threat

The problem is that low cost hardware with small calculation ability is assumed for non-PC, it is not possible to support security function sufficiently (IPSEC, TLS, SSL, etc.).

Guideline for measures

First of all, it is necessary for a vendor to judge what level of security mechanism is required for the relevant non-PC terminal. When judged necessary, the use of a lightweight solution such as using dedicated hardware or using a third person authentication method must be investigated.

Implementation method

When judged not necessary, there are other methods available; not to support security mechanism, using a dedicated chip or disclosure avoidance key encryption process using a third person authentication/key distribution mechanism.

In a link local segment, minimum security functions shall be used, and more safe encryption communication shall be used for communication with the outside using a security gateway implemented on other machines such as home router (advanced encryption algorithms shall be used between home router and server).

Issues and recommendations for IPv6 deployment period

It is desirable for third person authentication/key distribution mechanisms (Trusted 3rd Party Model, KINK. etc.) to become widely used.

L-1

Outline

When the usage environment of mobile IP expands, if Care of Address is outside of the network, it becomes difficult to control access.

Types of threat

This is a general threat of the remote access type, therefore, leakage of information, eavesdropping, service cessation, falsification or platform might occur.

Analysis of threat

With regard to threats caused by tunneling, the threats are the same as in item J and the countermeasures are the same as well. The following are the circumstances unique to MIP.

(1) There is no FW that is able to interpret extension option header used for MIP and FW rule becomes loose.

(2) If security GW is not “MIP aware”, registration packet cannot be fed to HA properly, and rule becomes loose again and security hole will result.

Guideline for measures

It is necessary to control access or inspect a packet on the path of the mobile node itself or on the path to mobile node and internal home agent.

Implementation method

MIP protocol packet shall be interpreted and blocked (IP filter) correctly in boundary firewall or internal router.

Issues and recommendations for IPv6 deployment period

It is necessary to clarify threats according to investigation about application of MIP and request vendors to implement a filter (supporting IPv6 extension option header of FW)

according to the result of clarification.

M-1

Outline

Some existing protocol implementation authentication communication partners using consistency of DNS reverse resolution records of IP addresses and normal resolution records responding to such records. It is difficult to implement this kind of protocol in IPv6.

Types of threat

Uncontrability, service cessation

Analysis of threat

This is a unique problem to IPv6. In the case of IPv4, the problem is handled by writing all dummy reverse resolution PTR records. When no response is made to DNS reverse resolution, log analysis becomes inconvenient. By waiting for DNS reverse resolution response, service RTT becomes larger.

Guideline for measures

DNS reverse resolution is originally a vulnerable authentication method, and it is a problem to complete authentication with this alone. Authentication should be performed using another method, and DNS reverse resolution should be used as a kind of reference for log analysis. In order to shorten the response time for DNS reverse resolution and to research the corresponding domain using an address, whois or so on can be used.

Implementation method

An authentication method other than DNS should be used. “lame delegation” of DNS reverse resolution should be prevented. Which means that, each site should remember NS setting of reverse resolution name space delegated from upper stream. DNS reverse resolution shall be disabled.

Recommendations for the age of IPv6 deployment

It is convenient for control if there is DNS server implementation that generates reverse resolution records dynamically and automatically (static automatic generation such as IPv4 is not ideal because it may lead to a significant increase in the number of DNS records). It is expected that inquiry frequency for whois server will increase, therefore, it is desirable to prepare a measure to distribute the load on the whois server.

Conclusion

Direct reachability, distribution of damage through dual stack, leakage of information by tunnel technology including IPsec and direct infection by worm can all be handled by appropriate settings and operation as of now.

There is no big difference between IPv4 and IPv6 with regard to “Guideline for measures” and “Methods”.

The level of support for IPv6 by security products and network devices hasn’t reached that of IPv4 yet.

It is necessary for support of IPv6 to be promoted with firewall linked with IDS, IDP, anti-virus and filtering of layer 3 packet using layer 2 device.

In some cases of multicast or firewall supporting Mobile IP, it may be necessary to enrich the functions of security products according to the usage method.

It is considered that unique countermeasures are required for non-PC according to the characteristics of each device.

With regard to privacy problems in the home environment caused by the spread of a dedicated address environment, some kind of countermeasure will be required.

4. Security Analysis of BCP

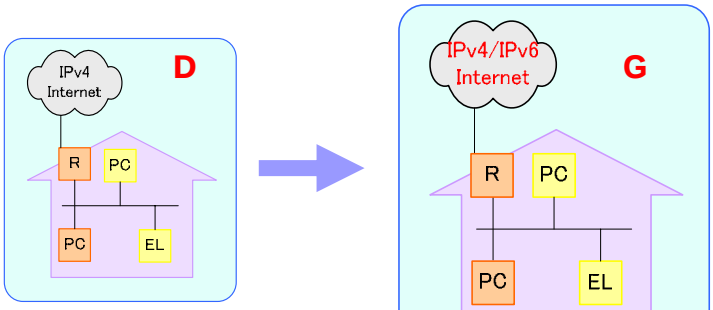
In this section, the security of BCP used in the home, large enterprise/local governments and SOHOs is analyzed and evaluated. Analysis is performed based on the scenarios shown below.

Home	Access from outside to a server at home (library of personal files)
Large enterprise	Installation of IP phone on an Intranet
Local government	Multicast assembly broadcasting using internal LAN (local government Intranet)
SOHO	Maintenance of shop terminal

Security of BCP ~ Home ~

The home scenario assumed here is the Deployment period model G of home SWG.

This model subscribes to IPv6 service and is connected with dynamic address of IPv4 with dedicated address of IPv6. IPv6 supporting OS used on a PC is already purchased.



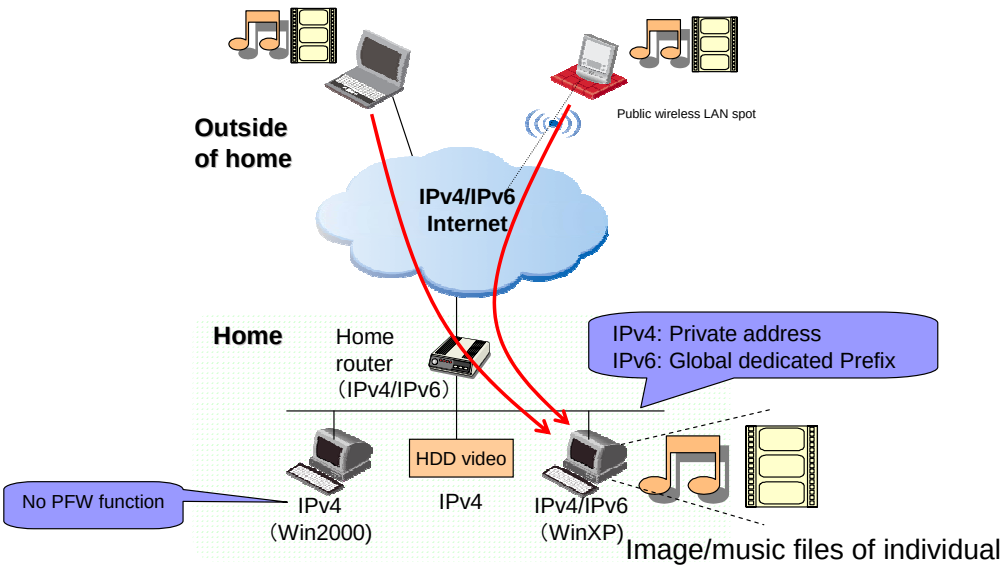
Model D

Model G

IPv4 is available as before, and there is a PC (Windows 2000) and an HDD video that support IPv4. It is considered that IPv6 is used for downloading personal images and music library through accessing the home file server (IPv6PC, WebDAV) from outside of home.

As security policy, access from outside is limited to only https connection to IPv6PC. Moreover, accessible filters and files are limited. However, IP address for outside point is not dedicated.

Security of BCP ~ Home ~ (continued)



Security Analysis and Evaluation

Analysis

Because it is possible to access to (H-2) (A-2)IPv6PC directly from outside, the threat of illegal intrusion to IPv6PC or infection by worm get higher. When this threat occurs, damage will probably spread to relatively vulnerable IPv4 machines and non-PC, therefore it is important to prepare measures for IPv6PC.

(A-2) is used for accessing from yourself (at outside point) to yourself (inside home), and the terminal address is shown publicly from information on the path, therefore there is a threat of illegal access being made to each device connected with v6.

With regard to access from (C-2) public wireless LAN spot, if security measures are not prepared using WEP, etc., the address or dedicated prefix are shown publicly, therefore there is a threat of illegal access made to each device connected with v6.

In many cases, Home router is default and prefix is ::1, therefore there is a risk of becoming a target for attack. If the Home router is taken over, it is may be used as a platform to

collect internal information or intrude into vulnerable machine.

Evaluation

Risk level: Low

It is possible to reduce threats using the measures shown below. It is possible to expect improved security compared with a similar way of using for IPv4.

Setting at terminal

・On personal firewall, external connection shall be set only to https service.
・Authentication at application level and limitation of file operation shall be carried out.

Access control with Home router

・In addition to access control with IPv6PC, the Home router shall be used to control access in order to prevent illegal intrusion from outside.
・Connection to Home router shall be made only from inside. (against highjacking of Home router)
・Filter to IPv6PC using Home router shall also be defined. Basically, all access from outside shall be prohibited and only those necessary can be opened individually.
・SPI function on Home router shall be used.
・There is a method to limit internal access to the connection between Home router and external terminal using VPN.

No terminal address shall be given to a third person carelessly

・No registration with disclosed DNS.
・Name resolution from outside shall be carried out using Hosts file.
・Address shall be changed on a regular basis (manual setting).

Related subitems

A-1,A-2,B-2,C-1,C-2,G-2,H-1,H-2

Security of BCP ~SOHO~

The assumed scenario is that IPv6 is installed for maintenance of shop terminals.

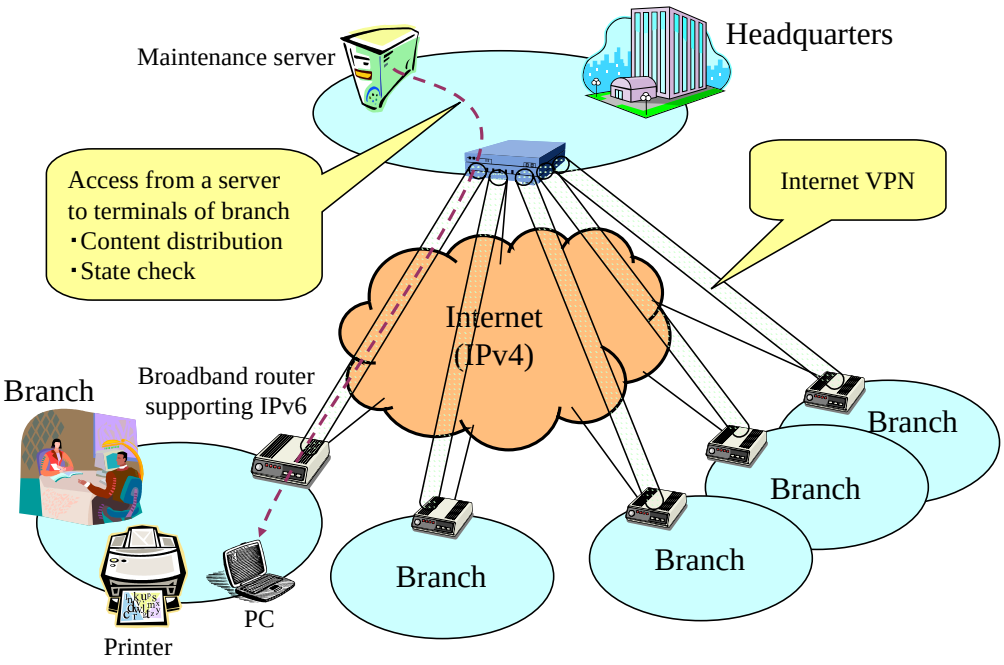
The problem with the operation of shops is that it's not possible to station IT staff on the spot, it requires man-hours for maintenance of terminals, there is a burden from merger and

abolition of shops and it requires man-hours for set up. In order to solve these problems, an auto maintenance system for terminals shall be installed. Then the purpose becomes to distribute contents to terminals directly by pushing and to obtain terminal state from the server dynamically.

As system requirements to realize this, it becomes necessary to operate IP addresses in a fixed manner in order to specify a terminal directly from a server. Moreover, for simplification of operation, it is necessary to assign auto address.

As security policy, network is used in a closed environment for maintenance use, and IPv6 is only used for maintenance. Internet is used via headquarters, and no internet communication is performed using IPv6. This is installed for maintenance purposes, no IPv6 communication between shops is performed either. IPv6 communication between shops is filtered. IPv6 communication is allowed only for setting and controlling terminals by administrator.

Security of BCP ~SOHO~ (continued)



Security Analysis and Evaluation

Analysis

It is not necessary to consider anything but security between server and terminal. There is no communication with the Internet and no communication between offices. However, inside the office, auto terminal setting is used, therefore security should be considered for it. For instance regarding the fact that RA has no authentication mechanism. This is the same

level of security problem as IPv4. When an anonymous address is used, it becomes difficult to perform remote maintenance, therefore an anonymous address cannot be used.

Evaluation

Risk level: Low

It is not easy to take a measure of L2 level, therefore some kind of security function is required for gateway. The risk level is the same as that of IPv4. Apart from the above mentioned measures, illegal terminals (NDP, online terminal) shall be removed. Anonymous addresses are not used for application of remote maintenance.

Related subitems

The following items affect the general Intranet, but they can be ignored in this case according to the initial premise.

A-1, A-2, A-4, B-1, B-2, C-1, C-2, E-1, F-1

The following items remain as security issues.

D-1, G-1, G-2, G-3

Security of BCP ~ Large Enterprise ~

As assumed scenario, IPv6 is installed on the occasion of the installation of IP phone in order to simplify the subnet design.

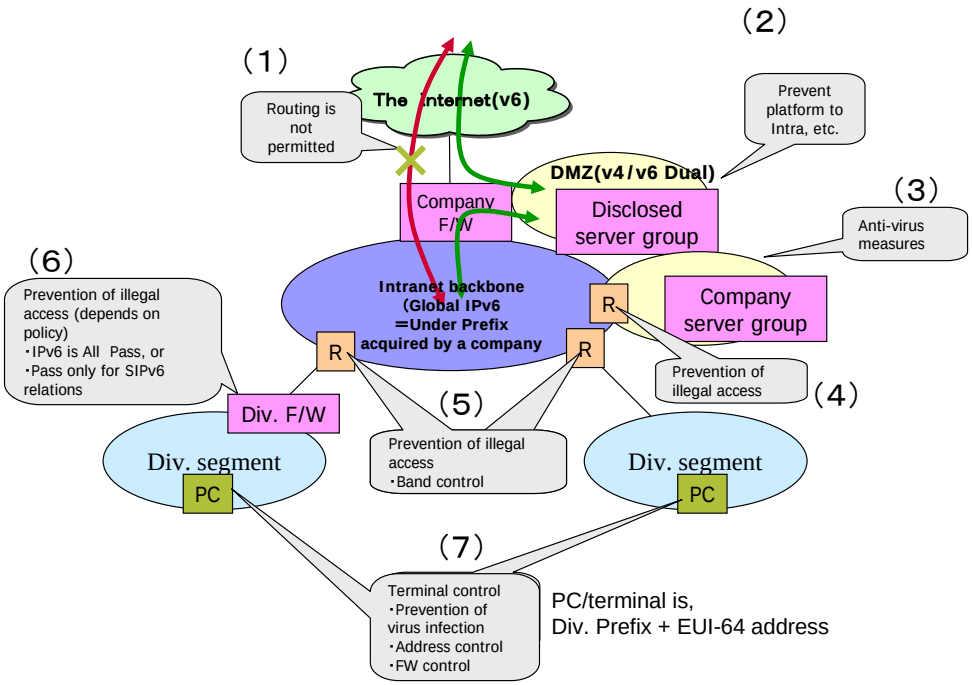
This organization acquires official global addresses, however, the organization is separated from the outside in the meantime. Because the main purpose is to construct a seamless Intra VoIP network without via NAT.

When hardphone and PC based soft phone are installed for IP phone, the demand for addresses increases.

As security policy, boundary router blocks v6 communication with inside Intranet and Internet. IPv6 communication from outside is allowed only to DMZ. For division firewall, division administrator chooses one of 2 policies. IPv6 is either All Pass (assuming that there is no threat from inside of Intranet) or only port related to SIP/RTP Pass.

Appropriate control shall be performed for a client. This control includes virus measures using inspection VLAN, etc., setting control of personal firewall, control of address (IP-MAC corresponding table: control measures when using anonymous addresses) and detailed terminal control using agent soft, etc.

Security of BCP ~ Large Enterprise ~ (continued)



Security Analysis and Evaluation

Analysis

(A) Risk of direct infection increases. Therefore, the prevention measures against bringing in an infected terminal must be enhanced (same as IPv4). However, it is possible to keep the risk of specification by port scanning at a low level.

(B-1) Terminal control gets easier in enterprise network, so that there are some advantages.

(B-2) Operation miss → it is considered that the risk of operation miss is low in the case of this BCP.

(D-1) Anonymous address shall be set at OFF, or terminal shall be controlled using a method such as installing agent for a client.

(G-3) The same system as IPv4 including layer 2 authentication shall be installed.

(H-1) In the case of BCP, access from outside is made through DMZ, and it shall be covered with the measure in H-2.

(H-2) Appropriate control of internal server and translator is required.

(K-2) In the case of BCP, access is made only from Intranet, so only inside is the target of threats.

Evaluation

Risk level: Small

Related subitems

A: Basically the same as v4.

B-1,B-2,C-2, D-1, G-3,H-1,H-2,K-2

Security of BCP ~ Local Governments ~

The assumed scenario is that this local government aims to be open administration and pursues the realization of local government service using IT technologies and focusing on disclosure of information to citizens and close communication with them. Therefore, the internal LAN of internal Intranet is utilized to realize an assembly broadcasting system at low cost. Then, IPv6 is installed at the time assembly image is distributed by multicast.

As security policy in this case, there is a limitation of distribution range. Distribution range shall be limited to internal LAN for the time being. With regard to branch offices related to the local government, distribution will be investigated according to band area, line type and equipment conditions. Distribution outside will be investigated for the future according to restriction of each local government.

The other issue is limitation of IPv6 supporting application. IPv6 service available for each terminal shall be limited to objective application (image distribution, etc. in this case) for a while.

Existing service shall be used as it is in IPv4, and if it is possible to expect additional merits, handling of IPv6 will be considered.

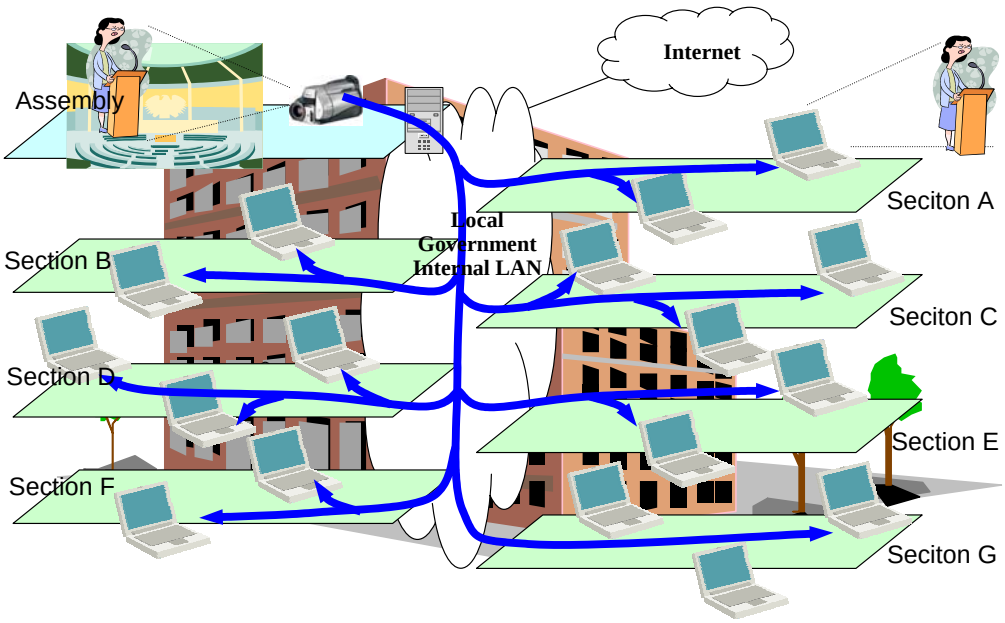
With regard to the new service to be introduced, usage of IPv6 shall be promoted actively.

The application of authentication is also an option. This is because it may become necessary to have a system where only specified users/terminals are able to hear according to the contents of stream data. It is preferable that distribution range is controlled and limited expressly by a network administrator, and it is also desirable to be able to prevent fake distribution servers.

Security of BCP ~ Local Governments ~ (continued)

- State of assembly is audited on PC terminal of each clerk using multicast

→Making internal LAN to support IPv6



Security Analysis and Evaluation

Analysis

Attack using only IPv6 multicast must be a target for consideration. Because IPv6 communication with the outside is out of the target for service and all IPv6 traffic from outside is rejected by the boundary router, the only concern should be internal attack. IPv6 unicast is also out of the target for service. Because there is no problem if IPv6 global address is not distributed to terminals

With regard to link local/unicast attack closed in a link, it shall be handled by rejecting all IPv6 packets issued by the target except MLD (this is performed using a personal firewall in an IPv6 terminal or L2 device that directly stores a terminal).

Evaluation

Risk level: Low

Authentication method of stream data

For authentication related to distribution, DRM (authenticated in streaming application) shall be used first of all. As access authentication, HTTP access (IPv4) to meta data of stream shall be authenticated.

Unintentional multicast/traffic measure

There is a problem of narrow band link flood caused by flowing into narrow band link (e.g.wireless LAN), however, (J-1) unintentional flow in shall be prevented by MDL snooping. Intentional flow in shall be prevented by dividing into segments in layer 3 method holding a router in between (to stop multicast in the segment, or to limit access to stream meta data).

The possibility of streaming from a fake distribution server will never occur because the IPv6 global address is not distributed to a terminal.

Entry number attack measures for multicast routers

Refer to countermeasures in J-4.

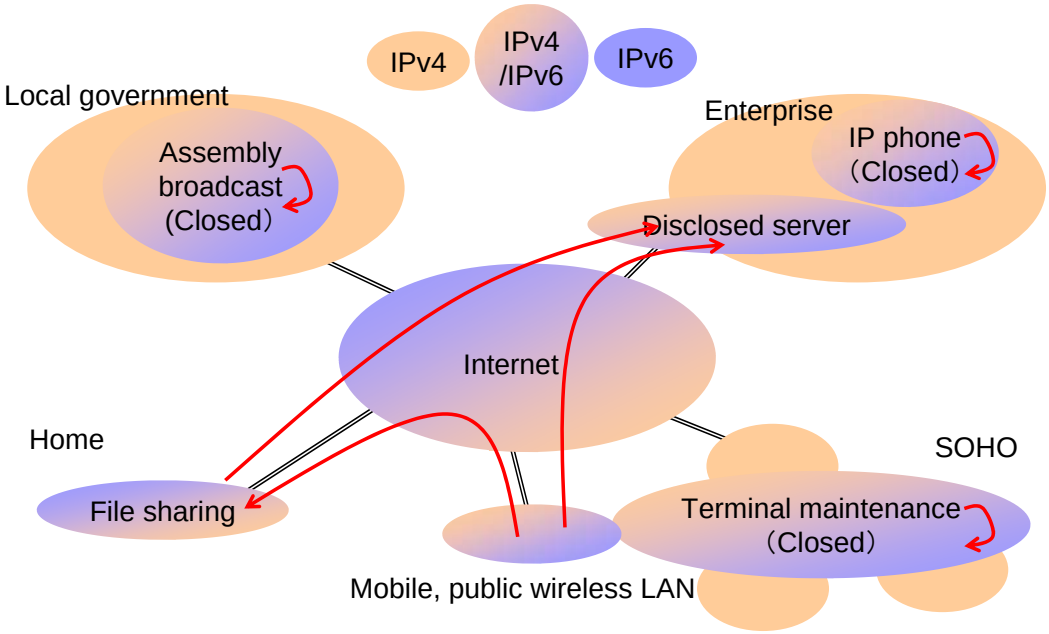
Related sub-item

J-1, J-4

5. Security in IPv6 Deployment Period

Analysis and Issues

State after BCP



Assumptions for IPv6 Deployment Period

In IPv6 the deployment period, installation of BCP cases will expand. Closed IPv6 systems will expand and mutual connection between closed systems will be promoted along with the increase in the number of terminals. Then, during the deployment period, usage is migrated from dual stack usage to IPv6 only usage. The main purpose of this migration is to reduce control/operation cost. There will be a movement from using the version for each application to integration to IPv6 (web, mail).

Moreover, usage of IPv6 will expand by fusion with new technology. Services for non-PCs such as IPv6 connection of home appliances or mobile terminals will start, and the usage service of IC tag and sensor information for provision of traceability, statistic information or information according to individual attributes will be promoted.

Upgrading of IT usage for business operation will lead to deployment of IPv6. Activation of business collaboration using P2P applications will be promoted, and the purpose of IT usage will shift from “improvement of business efficiency” to “acquisition of customers” and “improvement of service quality”.

Security in IPv6 Deployment Period

This section presents an analysis of the issues of security in the IPv6 deployment period that can be assumed for the home, large enterprises/local governments and SOHO based on the scenarios shown below.

Home

Based on the home network model K, L and O of IPv6 deployment period, access from outside (VTR booking, in-house camera) shall be performed.

SOHO

Connection of non-PC equipment, external linkage and outsourcing of business shall be performed.

Large enterprises/local governments

Dual stack is adopted overall, business application is shifted to IPv6 (P2P application, etc.) and various devices including non-PC are connected. Multihome (multi prefix) is also necessary.

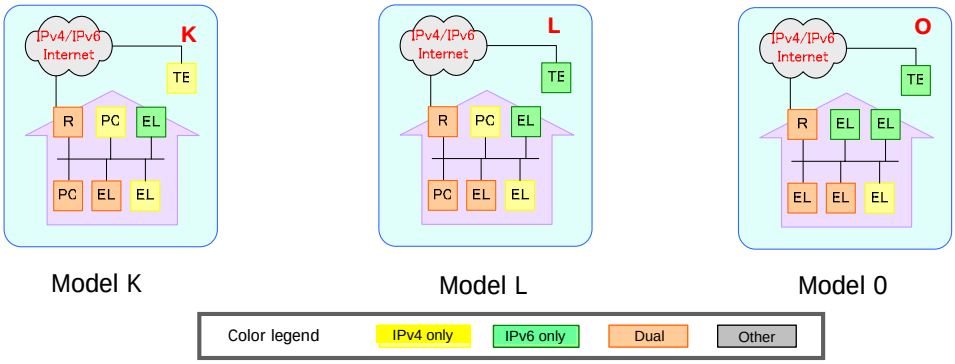
Subitems of related Section 3 are described below.

Security in IPv6 Deployment Period ~ Home ~

Home networks in the IPv6 deployment period can be classified into 3 models as shown in the Fig. below. The following is an analysis of the security of each model.

<explanatory notes>
R: Router M: Modem, Media converter
B|R : IPv4 router equipped with IPv6 bridge
EL : Home electric appliance PC : Personal Computer
TE : Remote terminal

- Home network in IPv6 deployment period
  - Model K:
    - Multiple number of PCs/ELs in home, some PCs are dual, some are IPv6 only and external equipment is IPv4
  - Model L:
    - Multiple number of PCs/ELs in home, some PCs are dual, some are IPv6 only and external equipment is IPv6
  - Model O:
    - Multiple number of ELs in home, some are IPv4 only, some are IPv6 only, and router (dual) is necessary.



Model K Model L Model 0

Model K

Devices to be connected

PC/game machine/non-PC equipment (AV, home electric appliances, IP camera, IP phone) and IPv4 external equipment (mobile phone, PC (PDA)) are connected.

Application to be used

Booking VTR using a mobile phone, viewing images from an in-house camera using an external device

Analysis of security

It is difficult to ensure sufficient security when making a connection with non-PC such as VTR or in-house camera, therefore, it is necessary to complete sufficient measures (illegal access measures, encryption, anti-virus) before the stage of actual access.

For connection from outside, IPv4 is used, therefore, if only IPv6 is used for devices at home, a translator is required. It is important to take the above mentioned measures for this translator and on either side of it. If a translator is inside the home or is a home router, measures for IPv4 shall be relied on.

Related subitems for Section 3

A-1, A-2, A-3, B-2, C-1, C-2, F-1, G-2, H-1, H-2, K-1, K-2

Model L

Devices to be connected

PC/game machine/non-PC equipment (AV, home electric appliances, IP camera, IP phone) and IPv6 external equipment (PC (PDA)).

Application to be used

Booking VTR using a mobile phone, viewing images from an in-house camera using an external device

Analysis of security

The difference from Model K described on the previous page is that direct connection becomes available with IPv6, however, it is the same in that measures including those for illegal access, encryption and anti-virus should be taken before connecting with nonPC.

Related subitems for Section 3

A-1, A-2, A-3, B-2, C-1, C-2, F-1, G-2, H-1, H-2, K-1, K-2

Model O

Devices to be connected

Game machine/non-PC equipment (AV, home electric appliances, IP camera, IP phone)

Application to be used

TV and video are used. The TV is used to view images from an in-house camera.

Analysis of security

This is the case where only non-PC equipment exists inside home, however, as long as there is a threat from an external PC, etc., this case is the same as Model K and L.

Or, for direct P2P communication between non-PCs, a system is required so that the access control files of both PCs and the necessary communication modules are provide continuously from the control server.

Related subitems for Section 3

A-1, A-2, A-3, B-2, C-1, C-2, F-1, G-2, H-1, H-2, K-1, K-2

Security problems at Home (common concerns)

With regard to security at home in the IPv6 deployment period that we introduced according to each case, the following can be pointed out as common concerns.

Problem regarding user's operation capability

Insufficient awareness on the part of the user, insufficient skill of the user, filter/limitation application miss due to incorrect input of address may be a problem.

Problems of security policy for equipment at home

The problem is that there is no common security policy between equipments at home or between equipment providers, and security policy varies according to the capability of individual equipment such as PC, AV machine, white goods, sensors.

Cost problems

When introducing into the home, the cost of the product must be low. This is the reason why there are many CPE, etc. with low functionality.

Threats to security (common matters)

If an effective measure is not used, illegal access becomes easier or the risk of being used as a platform gets higher. Moreover, there is a possibility that threats become more apparent, such as that countermeasures are not used promptly and therefore damage is spread further.

Issues for security measures (common matters)

It is necessary to reach a consensus regarding default settings between equipment providers, network providers and service providers.

Another issue is to provide a setting interface that is easy to use and is sophisticated, and it is necessary to encourage the changing of passwords or to devise interactive GUI, etc.

Necessary tools include a name resolution tool responding to usage purpose or inspection tool inside home, etc.

It is also considered effective to incorporate security measures suitable for the usage purpose of nonPCs in the service.

It is necessary to investigate the provision of a boundary service on the network side, for instance detection and blocking of errors such as IDS/IPS, or isolation and blocking when the home is used as a platform.

Security in IPv6 Deployment Period ~SOHO~

In the SOHO IPv6 deployment period (independent SOHO), the network is formed as shown below.

Because there are many addresses and auto setting is enriched, various items are connected by IPv6. PC, printer, IP phone, PDA, copy machine, FAX, white board, projector, PC peripheral machines, security camera, time card, etc.

Linkage with external nodes will increase as well. As a background, an environment for easy linkage with the outside will be arranged, including the arrangement of security infrastructure supporting P2P communication. Moreover, we can point out that the outsourcing of business operations will be promoted. These are the configuration of the order/booking system (web based system is already used), reception of inquiry/support, telephone, TV phone, collaboration (this will spread through deployment of IPv6) and so on. Real-time performance of the business gets higher, which will promote deployment of IPv6.

Analysis of security

Here, it is necessary to monitor the possibility of mutual connection with organizations with different security policies. When the outsourcing of business is promoted and business tie-ups with joint ventures are promoted, mutual connection will be formed with organizations that have different security policies, therefore it is necessary to have a clear guideline and countermeasures based on customer information leakage measures (P mark system, etc.).

First of all, it is necessary to prepare anti leakage measures for the information assets for each business partner. As countermeasures, prohibition of bringing PCs in/out, separation of network segments, separation of communication (equivalent to telephone/TV conference) and collaboration (exchange of cooperatively developed data, etc.) business can be considered.

Moreover, the ability to take security measures (technology, consciousness, policy) of the same level as those of the business partners also becomes an issue.

However, due to characteristics of general SOHO, there are some restrictions. This depends on the scale and steadiness of the SOHO, but generally speaking, SOHOs have the characteristic that they are not good at estimating the effect of investment for countermeasures mid term and they don't have a dedicated administrator, therefore it is considered difficult to maintain sufficient investment for security measures and to make limited installations.

Related subitems for Section 3

There are all kinds of possibilities according to the IPv6 technology used.

Security Issues

Issues other than technical issues

Establishment of security policy, creation of documents and improvement of awareness of employees through security education are all relevant issues.

Technical issues

Compared with the home, it is more promising in terms of technical operation skill, however, as technical issues, we can point out that because there is no dedicated administrator, countermeasures may not be taken promptly, and they may not all appreciate the versatility of countermeasure technology (it varies according to each business partner).

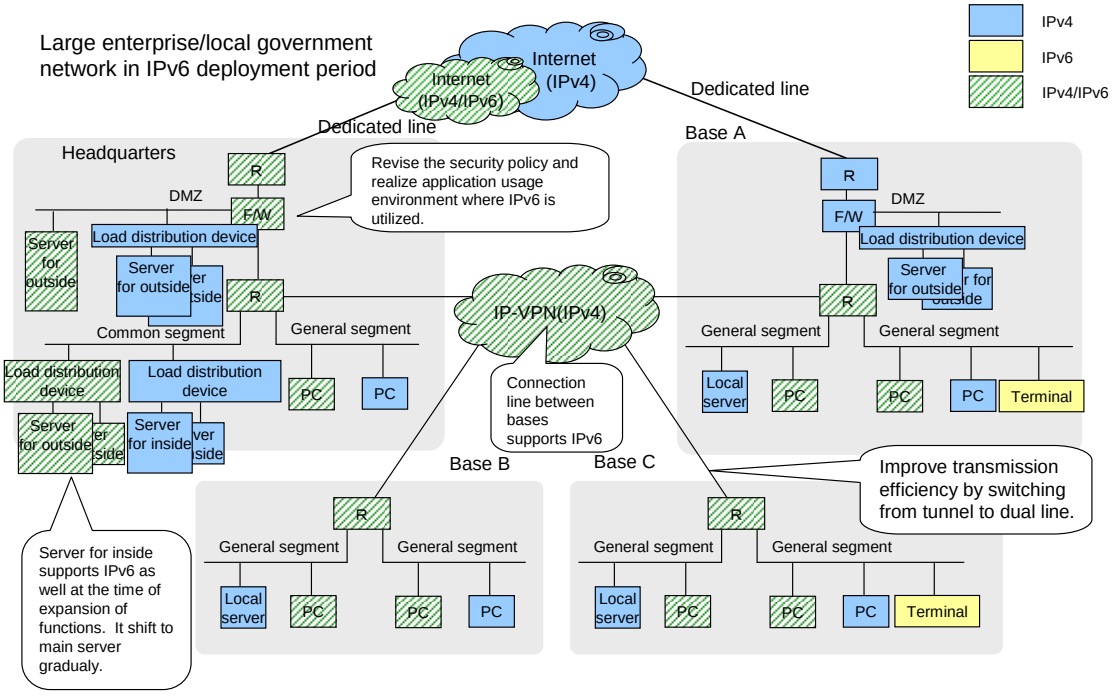
Due to the above mentioned issues, a system provided by a third party including the security service of the third party (ASP, etc.) and business Extranet configured by a business partner may be used in many cases.

Security in IPv6 Deployment Period ~ Large Enterprises/ Local Governments ~

Large enterprises and local governments in the IPv6 deployment period will install IPv4/IPv6 dual stack network environment entirely and shift to application usage environment focused on IPv6 step by step. P2P application will be used for business operation (SIP base), VoIP (extension line, external line), TV conference, file sharing and IM will be used. Legacy application is connected through a translator.

It is also assumed that various machines will be connected to a network. They are member PC, printer, non-member PC/PDA, whiteboard, copy machine, lighting, air conditioner, sensor, monitoring camera and TV.

Multi home (redundant external connection) or multi prefix is also installed.



The following points are examples of RFP from administrator.

・Plug&Play, Secure (there shall be a system in which once a user connects to a terminal, safe communication means is provided only for the appropriate party without setting.)
・Traceable (administrator should be able to identify owner and location of a terminal easily.)
・Manageable (administrator should be able to control setting of end users as a batch.)

Analysis of security

When a product complying with the above mentioned RFP examples is released, usage of P2P application for business and connection of non-PC equipment will be more realistic compared with the present state. There is a sign of the release of IPv4 products that are close to the RFP examples. However, in the case of the Centric control model shown in the RFP example, there is a risk of the spread of damage (disabled usage, leakage of control data, etc.) when vulnerability of control tool itself is actualized, therefore it is necessary to prepare an alternative measure for minimization of damage and recovery.

Related subitems for Section 3

A-1, A-2, A-3, A-4, B-1, B-2, C-1, C-2, D-1, E-1, F-1, G-1, G-2, G-3, H-1, H-2, K-1, K-2

Security issues

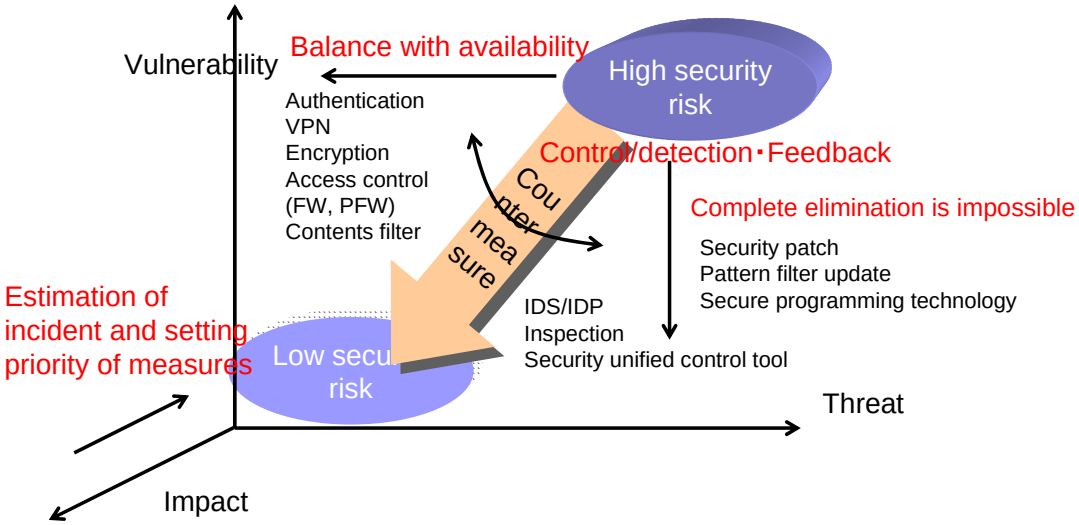
The release of the products shown below, which comply with the above mentioned RFP examples and state of IPv6 deployment period is an important issue.

・Integrated security control linked with security GW device according to the features of non-PC
・Access control corresponding to the selection of source address in multi prefix environment
・Detection and blocking of attacks that aim at vulnerability of P2P application
・Multi stage access control linked with the presence of information

Moreover, accumulation of experience in operating the above mentioned products is also required. At the beginning it is required to clarify operation issues by limiting segments and to feed back those issues into security education and operation policy.

Security measure guideline in IPv6 deployment period

- Risk = Vulnerability (weak point of a thing) x threat (that attacks a thing) x impact (influence degree of an incident)
- Security measures of IPv6 are basically an extension of the current trend in security measures (IPv4)



As shown in Fig. above, “risk = vulnerability x threat x impact” will remain as it is, and security measures for IPv6 represent an extension of the current trend in security measures (IPv4).

Consideration of Security in IPv6 Deployment Period

In order to take a balance between the 3 big factors for security; safety of information assets (prevention of data falsification, detection/recovery), confidentiality (encryption control, leakage measure) and convenience (availability) at the highest level, it is necessary to make equal investment in consciousness, policy and technology, and IPv6 is just one of the technical methods available.

However, when the usage of P2P application and non-PC equipment is promoted by IPv6, there is a possibility that this balance of achievement level may change. A certain administrator said, “it is absolutely out of question to connect to the Internet” 10 years ago, but you can not know how useful it is if you don’t use it.

There is no difference in technical security measure items between IPv4 and IPv6. The same illegal access, encryption and anti-virus measures are required.

With regard to firewalls in the age of IPv6, the boundary model of the firewall type is considered effective even for IPv6. However, along with the diversification of communication, countermeasures at multiple points and integrated control systems will be

required in the future.

How about the issue of whether a paradigm shift will occur with IPv6?

When IPv6 is more widely distributed, the number of machines using IP will increase, however, compared with IPv4, [number of machines using IP / IP address space] will become dramatically more sparse. Along with the diversification of the users' sense of value (privacy, convenience), items and usage of items will also diversify accordingly, and the targets of attackers may shrink (decrease in motivation). The final right of choice belongs to the user.

Due to the above mentioned situation, there is a possibility of the occurrence of a paradigm shift against security.

Tips

Investigation Example of Security Measures in IPv6 Deployment Period

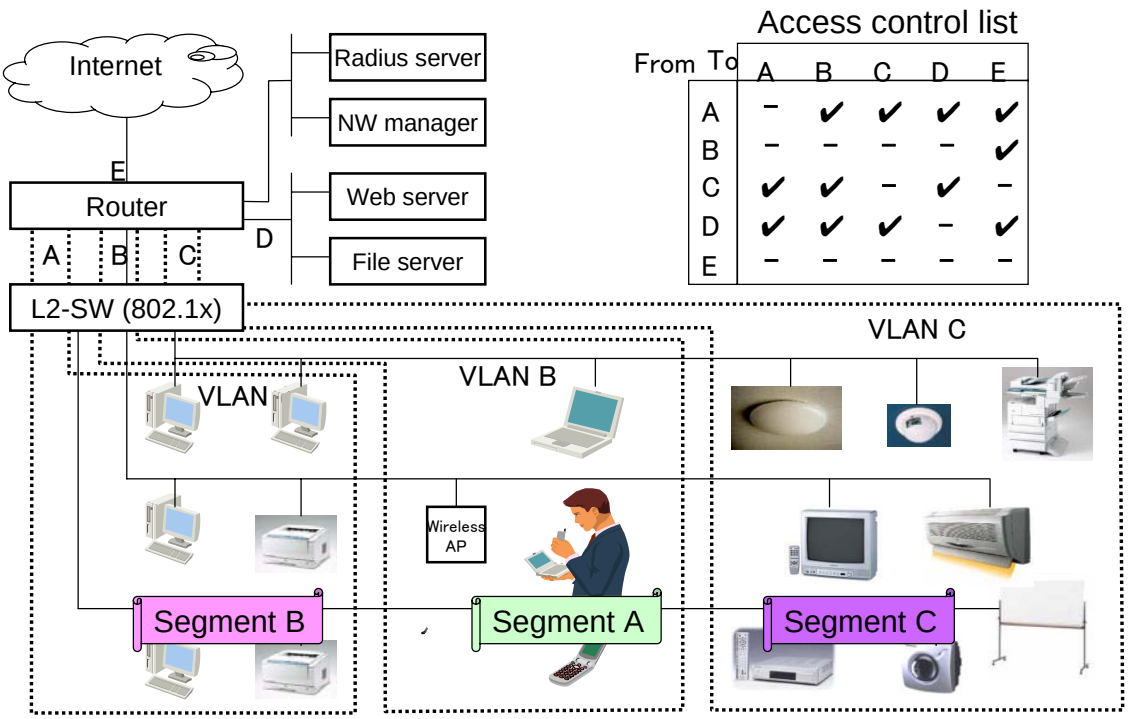
1. Clear segmentation

We can think of classifying machines into segments according to the different possible measures and threat levels in the network.

The example in the Fig. below shows that segment A is a terminal group that permits incoming, segment B is a group of terminals only for outgoing and segment C is a group of non-PCs.

The effects expected through segmentation are that it will enable the minimization of the spread of damage when an incident occurs and the total operation cost can be reduced compared with the case of mixed installation.

Concept of segmentation and access control



2. Investigation for segment A

Access origin shall check whether access is controlled at multiple procedure/measure points. IP filtering, session control such as SPI and authentication of application level shall be carried out at boundary and end point.

The expected utility of IPv6 is that because the address space is broader, the threat of brute force attacks by a third party will decrease.

3. Investigation for segment B

In this segment, the same measures as the existing IPv4 measures are effective. As long as the same measures as the existing ones (IPv4) (web, mail) are used, this segment doesn't always have to make external routing for IPv6. The existing measures are used only for communication with the internal server (web, mail, DNS), and in this case, IPv6 is used for communication on the internal network.

4. Investigation into mutual connection between segment A, B and segment C

The necessity shall be investigated according to the purpose, whether it is necessary to connect them directly or whether measures are taken to stop the spread of vulnerability of PC to non-PC. It is necessary to limit connections via proxy and gateway devices without direct routing.

5. Mutual connection between segment A and segment B

If there is no need, direct routing shall be not carried out. You can limit connection to that via proxy and GW device. Or, you can allow communication after inspection.

Investigation State of IPv6 Security by IETF

As of December 13, 2004, the following IPv6 security related RFC or Internet drafts of IETF exist.

IPv6 Neighbor Discovery trust models and threats
RFC3756
IPv6 Transition/Co-existence Security Considerations
draft-savola-v6ops-security-overview-03.txt
IPv6 Security Problem Statement

draft-vives-v6ops-ipv6-security-ps-02.txt
Security Considerations for 6to4
RFC3964
Fire walling Considerations for IPv6
draft-savola-v6ops-firewalling-03.txt
IPv6 distributed security requirements
draft-palet-v6ops-ipv6security-01.txt
Quarantine Model Overview for IPv6 Network Security
draft-kondo-quarantine-overview-01.txt
Threats relating to IPv6 multihoming solutions
draft-nordmark-multi6-threats-02.txt
Secure Neighbor Discovery (SEND)
draft-ietf-send-ndopt-06
Cryptographically Generated Addresses (CGA)
draft-ietf-send-cga-06.txt

The Concept of Security Model in IPv6 Deployment Period

The following are the possible security models in the IPv6 deployment period.

Thin Client Model (doesn't have vulnerabilities)

In this model, terminal connects to a control server at booting and when a program is required, the up-to-date version is obtained from a control server occasionally and operation is performed. This model contributes to reduce vulnerability.

Tamper proof model (detects a danger and drops)

Purpose of this model is to prevent the taking out of confidential information illegally, and the contents and programs are encrypted, and they are decrypted and used as necessary. In the case of a non-PC base, this model has the mechanism to destroy itself when illegal access is detected.

Stealth model (hides existence)

In this mode, the control server mediates and service matching or notification of address of another party is carried out. This mode aims at disturbing specification by a third party

by changing the IP address (interface ID) on a regular basis according to an acquired random number.

Investigation members

Nakai (Chair, NTT communications Corporation)

Arano (Intec Net Core)
Ishihara (KDDI Corporation)
Ishihara (Toshiba Corporation)
Inoue (Toshiba Corporation)
Inomata (Fujitsu Limited)
Uesugi (Hitachi, Ltd.)
Ujo (Checkpoint)
Oka (Toshiba Solutions Corporation)
Kitsuta (Checkpoint)
Kubota (Matsushita Electric Industrial Co., Ltd.)
Kondo (Trend Micro Incorporated)
Kondo (NEC Corporation)
Saiki (NS Solutions Co., Ltd.)
Sakauchi (NEC Corporation)
Sato (NS Solutions Co., Ltd.)
Shimada (Fujitsu Access Ltd.)
Shimizu (Toshiba Solutions Corporation)
Suzuki (Hitachi, Ltd.)
Takahashi (Trend Micro Incorporated)
Takizawa (Fujitsu Access Litd.)
Tsukioka (Hitachi, Ltd.)
Hashimoto (Mitsubishi Research Institute Inc.)
Hirabayashi (Mitsubishi Research Institute Inc.)
Hirayama (Trend Micro Incorporated)
Hiroumi (Intec Net Core)
Furukawa (Fujitsu Access Ltd.)
Murata (Matsushita Electric Industrial Co., Ltd.)
Yokota (Matsushita Electric Industrial Co., Ltd.)
Yoshimoto (Checkpoint)