Published as: Ahmad AlSa'deh, Feng Cheng, Sebastian Roschke, and Christoph Meinel, IPv4/IPv6 Handoff on Lock-Keeper for High Flexibility and Security, in Proceedings of 4th IFIP/IEEE International Conference on Network Technologies, Mobility and Security (NTMS'11), IEEE Press, Paris, France, February 7-10, 2011.

IPv4/IPv6 Handoff on Lock-Keeper for High Flexibility and Security

Ahmad AlSa'deh, Feng Cheng, Sebastian Roschke, Christoph Meinel
Hasso Plattner Institute, University of Potsdam
P.O.Box 900460, 14442, Potsdam, Germany
{ahmad.al-sadeh, feng.cheng, sebastian.roschke, christoph.meinel}@hpi.uni-potsdam.de

***Abstract*— In response to the emerging deployment of IPv6 on network devices, this paper proposes the integration of IPv6 on Lock-Keeper, an implementation of a high level security system for preventing online attacks. It is designed to permit the secure data exchange over physically separated networks in an IPv4-based environment. A new intercommunication module is added to manage IPv4/IPv6 handoff inside the Lock-Keeper, which provides several benefits. First, the Lock-Keeper gains the flexibility to work in IPv4/IPv6 environments. Second, an application layer gateway to bridge IPv4 and IPv6 networks is achieved. Third, the IP-layer protocol isolation is realized inside the Lock-Keeper to enhance the security of the protected network by exchanging data between physically separated networks using different IP protocols.**

Keywords-network security; physical separation; protocol separation; Lock-Keeper; IPv4/IPv6 transition

I. INTRODUCTION

The depletion of IPv4 addresses was the main motivation behind designing IPv6. It provides a 128-bit address space instead of a 32-bit address space in IPv4. So, IPv6 will have enough unique addresses for variable types of products, such as smart phones, IP TV, automobiles, etc. Moreover, IPv6 expands and optimizes some features of IPv4 to make it more powerful. IPv6 was designed with stateless address autoconfiguration, mandatory IPSec for security, enhanced mobility, simple header structure, Quality of Service (QoS) provisioning, and more.

The consumption of IPv4 addresses seems to be accelerating. Less than 2% of the IPv4 address space remains to be assigned, and the available address space will be used up by 2012 [1]. Consequently, the migration to IPv6 has become inevitable and fundamental to boost the future growth of Internet. Therefore, several governments around the world take initiatives to promote the migration to IPv6. Also, most of networking equipment vendors and software developers support IPv6 in their products. And now most of mainstream operating systems support IPv6 by default.

In response to the emerging deployment of IPv6 on network devices, in this paper, IPv6 is integrated to the network security device named "Lock-Keeper" [2]. The Lock-Keeper system has been offered as a high level security product to prevent online attacks against an internal IPv4-based network. It works as switch and permits data exchange between two physically separated networks without establishing direct physical connections [3, 4]. Fig. 1 shows the abstract principle of Lock-Keeper's operation. The Lock-Keeper system consists of four components: INNER, OUTER, GATE, and a switch module. To support IPv6 on Lock-Keeper, a new IPv4/IPv6 handoff transformation mechanism is implemented for managing the IPv4/IPv6 intercommunication process inside the Lock-Keeper.

Several benefits are obtained by integrating IPv6 into Lock-Keeper. First, the Lock-Keeper gains the flexibility to support both IPv4 and IPv6 users and to work with both IPv4-only networks and IPv6-only networks. The second benefit comes from the fact that IPv6 is not "backward compatible" with IPv4. This restriction of direct communication between IPv4 and IPv6 can be employed to enhance the security of Lock-Keeper by combining "physical separation" and "IP protocol separation" for network protection. IP protocol separation can be used to prevent IP-based online attacks from outside by stopping one protocol at the border of a network site and using the other to carry the data to the internal network. Other benefits, such as realizing the application layer gateway to bridge IPv4 and IPv6 networks is also achieved. These benefits are gained without noticeable effect on the transmission delay through the Lock-Keeper, since the Lock-Keeper delay is dominated by other factors, such as a switching mechanism delay and queuing delay rather than the processing time of IPv4/IPv6 handoff intercommunication.

The rest of this paper is organized as follows: Section II reviews the existing IPv4/IPv6 transition mechanisms. Section III introduces the concept of network security by separation at the physical layer and by using the Lock-Keeper device. Section IV illustrates how IPv4/IPv6 handoff

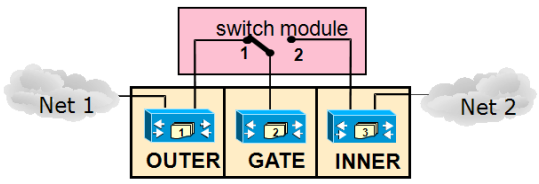


Figure 1. Lock-Keeper components

is done inside the Lock-Keeper. Section V presents two practical case studies of an IPv6 deployment on Lock-Keeper. Section VI concludes the paper.

II. Review of IPv4/IPv6 Transition Mechanisms

Despite the fact that IPv6 still maintains much of IPv4's semantics and two protocols have similar functionalities, IPv6 is incompatible with IPv4. IPv6 has its own address family, forwarding table, and routing algorithms. Moreover, IPv6 headers and IPv4 headers do not inter-operate since some fields are removed, changed, added or expanded. The interoperability and reliability are identified as the key prerequisites for adoption of IPv6. Therefore, many transition mechanisms have been proposed by the Internet Engineering Task Force (IETF) and other researchers in order to ensure smooth migration from IPv4 to IPv6 networks. In fact, it is impossible to migrate from IPv4 to IPv6 in an instant and it is expected that current IPv4 and IPv6 networks will co-exist with each other for several years or even decades.

The existing transition mechanisms can be mainly categorized under three categories: dual stack, tunneling, and translation [5, 6]. Dual-stack mechanisms [7] are operating the two protocol stacks in parallel to allow the network node to communicate either by IPv4 or IPv6. In Tunneling, IPv6 nodes communicate with IPv4 by encapsulating IPv6 datagrams within IPv4. Several tunneling mechanisms have been presented: IPv6 over IPv4 [8], IPv6 to IPv4 automatic tunneling [9], and Tunnel Broker [10]. In IPv4/IPv6 translation mechanisms, the basic function is to translate the IP packets. Several translation mechanisms are proposed, such as BIS (Bump In the Stack) [11] and NAT-PT (Network Address Translation-Protocol Translation) [12, 13].

All these solutions only address the backward compatibility. Thus, IPv4 nodes still cannot communicate with IPv6 nodes, since they do not know how IPv6 works. To solve this problem, a Bi-Directional Mapping System (BDMS) was proposed in [14] to deal with IPv4/IPv6 address mapping transition. Benefit from the flexibility of the Lock-Keeper architecture and the integration with Dual-stack mechanism, the data could be exchanged inside the Lock-Keeper by using two different IP protocols via a simple bi-directional IPv4/IPv6 handoff intercommunication module. Section IV shows the details of IPv4/IPv6 handoff process inside the Lock-Keeper.

III. Network Separation for Security

As pointed out by Rushby and Randell [15], the basis of protection is separation. A network site can be secured by being separated from other networks. Based on the TCP/IP model, one can separate network access in four ways, corresponding to each layer: at physical layer, at network layer, at transport layer, and at application layer. The most powerful and secure way of separation will be at the physical layer.

A. Physical Separation and Lock-Keeper

Based on the principle, "to secure a network is to separate it", the Lock-Keeper has been proposed as an efficient approach to guarantee a high level of security and prevent online attacks by physically separating the communicated networks without losing the ability of secure data exchange between these separated networks [3, 4]. Lock-Keeper works as a sluice on the border of the protected network [4]. Because of such physical network separation, it can be guaranteed that hackers and malign data have no chances of breaking into the internal network by any means of online attacks. Currently, the commercial version of Lock-Keeper has already been developed and is now vended by Siemens [2]. Two different types of Lock-Keeper are available, the SingleGate and the DualGate [16] Lock-Keeper. To briefly explain how the Lock-Keeper works, a SingleGate Lock- Keeper system is introduced.

As shown in Fig. 2, a SingleGate Lock-Keeper system consists of three independent active computers: INNER, OUTER, and GATE. Besides, a switch module is realized on a Printed Circuit Board (PCB). The INNER computer is connected to the internal high security network, the OUTER computer on the opposite side is connected to an external, less secure network (e.g., the Internet), and the GATE computer provides the actual sluice function. The patented switch module is for switching the connections at the hardware layer between INNER-GATE and OUTER-GATE. In this way, the GATE is connected to just one side at a time, either INNER or OUTER.

In addition to the hardware components, a software component called the Lock-Keeper Secure Data Exchange (LK-SDE) runs on the Lock-Keeper system. Currently, LK-SDE software includes four application modules, the File eXchange (File-X) Module, the Mail eXchange (Mail-X) Module, the Database Replication (DBRep) Module, and Web Services (WS) Module [17]. Normal application protocols, such as FTP, SMTP, HTTP, etc., are stopped by these application modules, and then the standard file-based Lock-Keeper Message Containers (LKMCs) carry the data for the respective services. A "Basic Data Exchange Module" is responsible for transferring the LKMCs by using the "Pull-Push" mechanism to avoid the possibility of outside hosts establishing a direct connection to GATE [3]. Since the GATE is also a normal PC, it is possible to add other security software, e.g., virus scanning software, mail analysis tools, or content filtering methods to prevent offline attacks. IPv6 can be integrated into the Lock-Keeper components: INNER, OUTER and GATE to gain more flexibility to work in IPv4/IPv6 environments, in addition with other benefits like enhancing the security by achieving IP protocol separation.

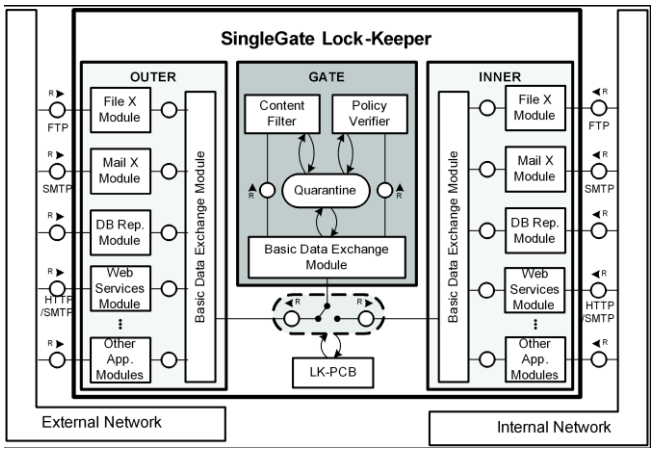


Figure 2. Conceptual architecture of the SingleGate Lock-Keeper

B. Protocol Isolation for Security

Generally, network layer separation can be done by subnetting, which creates different networks. Two nodes in different subnets communicate with each other through the gateway only. Another idea of "Protocol Isolation" for security is introduced by Microsoft [18] to protect entire LANs from the external Internet. In this model, an Internet server with two network adapters has been used. One of these adapters is connected to the Internet using the IP protocol, and the other is connected to the LAN which runs another protocol such as the IPX protocol. Fig. 3 shows this model for protocol isolation. The resources on the server are accessible from both directions, but the data cannot be passed through, i.e., Internet users can reach the server, but cannot access the Intranet because it requires IPX. The advantage of protocol isolation model is that the LAN users can share information with Internet users without exposing the LAN to unauthorized users [18]. On the other hand, one limitation of this model is that the LAN users cannot directly access the Internet.

However, our idea for doing the IP protocol isolation benefits from the differences between IPv4 and IPv6. Since IPv4 and IPv6 cannot directly "speak" with other, this method will be more powerful than subnetting to protect a network. To achieve the IP protocol isolation without losing the ability to transfer the data through the Lock-Keeper, a new IP-Based eXchange (IP-BX) module is added to manage the intercommunication process between IPv4 and IPv6 on Lock-Keeper.

IV. IPV4/IPV6 HANDOFF INSIDE THE LOCK-KEEPER

On each component of Lock-Keeper, there is a separated network card. These three network cards are connected by the LK-Switch Module and responsible for the data transmission inside the Lock-Keeper system. Besides, on INNER and OUTER, there are two additional network interfaces, respectively exposing services to internal and external users. Each interface could have IPv4, IPv6, or both. So, there are many possibilities for IP combinations on Lock-Keeper to support IP protocol isolation and to achieve the IPv4/IPv6 handoff. By properly configuring the Lock-Keeper network interfaces, the packets could pass through the Lock-Keeper using different IP protocols. The most flexible one is to enable both IPv4 and IPv6 on all interfaces as shown in Fig. 4. In this case, the Lock-Keeper will gain high flexibility to work in IPv4/IPv6 networks at both sides, OUTER and INNER.

Fig. 5 shows more IPv4/IPv6 configuration combinations on Lock-Keeper. The "X" in the Fig. 5 means that the protocol is not supported at the corresponding network interface. The most interesting configuration cases are shown in Case 1 and Case 2. In these cases, the Lock-Keeper can communicate with IPv4 and IPv6 at both sides, INNER and OUTER. Besides achieving high flexibility, a virtual barrier is created on the GATE. So, messages will be carried through the Lock-Keeper parts using two different IP protocols. In Case 1, IPv4 is used for GATE-OUTER communication, while IPv6 is used for GATE-INNER communication. In Case 2, GATE/OUTER communicate by using IPv6 while GATE/INNER communicate by IPv4. Accordingly, an isolation protocol region will be created at the GATE to enhance the Lock-Keeper security. However, these cases require small modification on GATE's LK-SDE software modules to support IPv6.

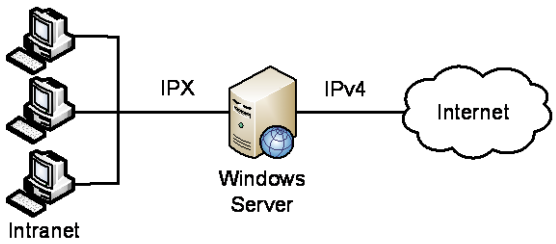


Figure 3. Microsoft protocol isolation model for security

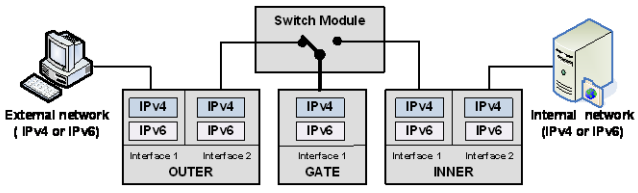


Figure 4. Enabling IPv4/IPv6 on all network interfaces of Lock-Keeper

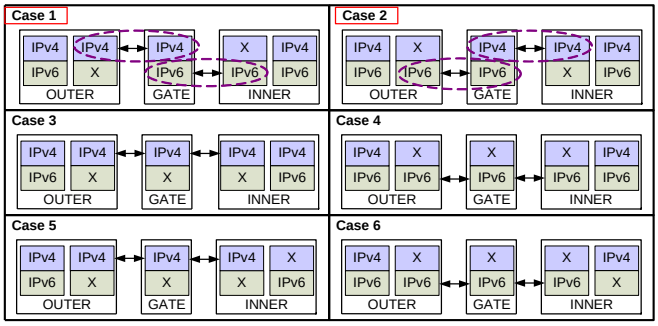


Figure 5. Some other possible IP configurations on Lock-Keeper

The Cases 3 and 5 do not need modifications to GATE's LK-SDE software modules. These cases provide the flexibility to communicate with IPv4 or IPv6 at the external side of the OUTER. At the same time, IPv6 traffic is stopped at the OUTER. And IPv4 is used for the communication between GATE-OUTER and GATE-INNER. This could be an advantage, since IPv4 security tools, which are integrated on GATE, are more mature than IPv6 security tools which are still under development and testing. Case 5 allows the INNER to communicate only by IPv6. The Cases 4 and 6 mainly depend on IPv6 protocol for the Lock-Keeper internal communication and these cases need modifications to GATE's LK-SDE software modules to support IPv6.

It is recommended to enable IPv4 and IPv6 on the external interface of OUTER to permit any authenticated external user with IPv4 or IPv6 to communicate with the Lock-Keeper easily. However, this flexibility should not introduce new security issues since running the two protocols can open new doors for the hackers to attack on both IPv4 and IPv6. In this case, handling the vulnerabilities of both protocols have to be taken into consideration simultaneously.

To mitigate this vulnerability, a new IP-Based eXchange (IP-BX) module is added on OUTER of the Lock-Keeper. This Module manages the intercommunication process between IPv4 and IPv6. The functionality of this module is to receive the IPv4/IPv6 packets and then checks the "Version" field value in IP header. Base on the "Version" field value, IP-BX module selects the proper IP protocol to carry data. For example, if the data received by IPv6 at the OUTER, IP-BX module can decide to use IPv4 for GATE-INNER communication. In this way, the network protocol separation is achieved to enhance security by exchanging data between physically separated networks using different IP protocols.

IP protocol isolation security is a powerful solution in mixed IPv4/IPv6 networks. Because IPv4 firewalls cannot be deployed for IPv6, both IPv4-based and IPv6-based firewalls are needed to be configured and managed carefully. Otherwise, the internal networks can be vulnerable to some attack due to IPv6 protocol misused. For example, the IPv4 tunnel can potentially bypass an IPv6-unaware firewall. The IP-BX module can be easily modified to achieve IP protocol isolation according to the Lock-Keeper interfaces configuration. Even in case of enabling IPv4 and IPv6 on all of the Lock-Keeper interfaces, the IP protocol isolation is still possible if the IP-BX works according to the algorithm which is shown in Fig. 6.

V. TESTING AND EVALUATION

The practical deployment of IPv6 on Lock-Keeper is realized and tested by using two case studies based on FTP protocols. The first one is Windows Secure CoPy (WinSCP) [19] which is an open source SFTP and FTP client for Microsoft Windows. The other is Very Secure File Transfer Protocol Daemon (vsftpd) [20] which is also an open source package for Linux. Two experiments are carried out, the first one by using internal IPv4 server, and the second one by using internal IPv6 server. For the two experiments, IPv4 and IPv6 are enabled and configured on the external interfaces of OUTER and INNER. Other interfaces are kept working with IPv4-only.

A. *Internal IPv4 SFTP Server*

As shown in Fig. 7 (a), an external user connected to an external interface of the OUTER uses a WinSCP client to exchange data with an internal IPv4 SFTP server. At "Interval 0", an IPv6-user provides the correct authentication information, username and password. "Interval 1" shows the successful login to exchange data with the internal IPv4 SFTP server through the Lock-Keeper. In this case, IPv6 is used just for the communication between the external user and the external interface of the OUTER. IPv4 is used for the communication between GATE-OUTER, GATE-INNER, and the INNER-Internal SFTP server.

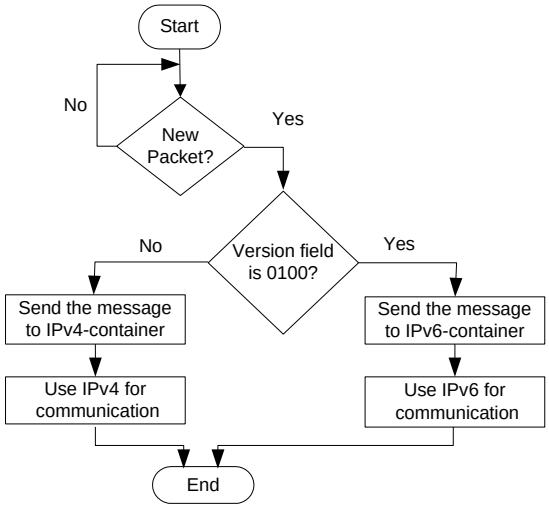
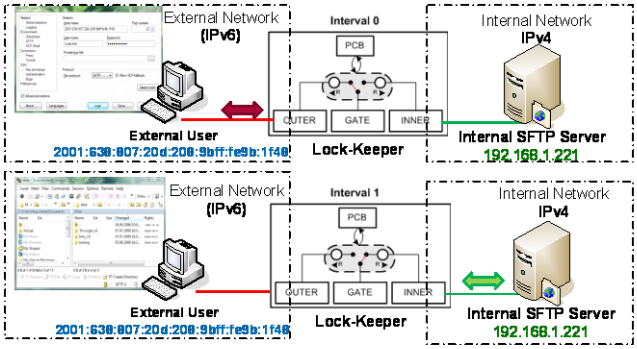
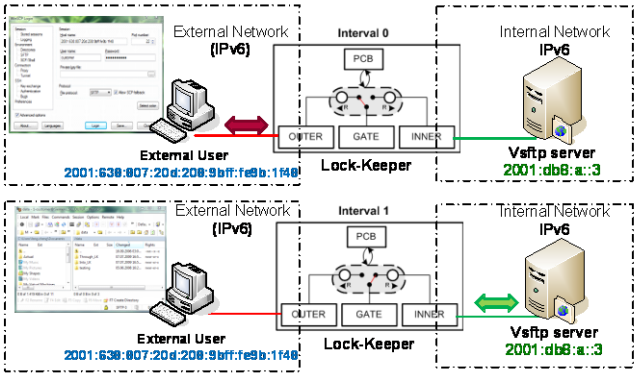


Figure 6. IP-Base eXchange module functionality



(a) IPv6 external user exchange data with internal IPv4 server through the Lock-Keeper with IPv4 on the GATE



(b) IPv6 external user exchange data with IPv6 internal server through the Lock-Keeper with IPv4 on the GATE

Figure 7. A practical deployment of IPv6 on the Lock-Keeper

B. *Internal IPv6 FTP Server*

To test the possibility of accessing an internal IPv6 FTP server, vsftpd was configured to listen on an IPv6 socket only. This means that vsftpd will not be able to listen on IPv4 in conjunction with listening on IPv6 at the same time since the parameters for listening on IPv4 and IPv6 are mutually exclusive. Fig. 7 (b) shows that the authenticated external IPv6 user gets access for exchanging data with the internal IPv6 FTP server. In this scenario, IPv6 is used for OUTER- External User and INNER-Internal FTP server communication, while IPv4 is used for GATE-INNER and GATE-OUTER communications.

C. *Experiments Discusion and Evaluation*

These two experiments clearly show how the Lock-Keeper gains the flexibility to support IPv6 and how the IP protocol separation is achieved inside the Lock-Keeper. Moreover, the application layer IPv4/IPv6 conversion is also achieved since IPv6 has a new socket API with 128-bit address structure instead of 32-bit in IPv4 and it is obvious that IPv6 addresses cannot be stored by IPv4 address structure.

Even though IPv6 data header length is twice as that of the IPv4 header implying that IPv6 has a higher overhead than IPv4, the time delay through the Lock-Keeper is almost identical in both cases, i.e., with original IPv4-only and with integrating IPv6. By experiment, we found that the Lock-keeper has about 0.08 % increases in the transfer time than with IPv4-only when an external user uses IPv6 to get 1GB file form IPv6-internal server. IPv4 outperforms IPv6 by only about 0.001% for transferring 10KB file. For smaller file sizes, the transfer times are roughly equal. Fig. 8 shows the percentage increase in transfer time through the DualGate Lock-Keeper by integrating IPv6 comparing to the original IPv4-only Lock-Keeper when transferring different file sizes.

The above results have been possible since IPv6 header structure is designed to get a simplified standard format which can be processed faster than IPv4 headers. Moreover, the switching mechanism, queuing delay, and scanning time inside the Lock-Keeper from the significant portion of the total transfer time rather than the processing time. Furthermore, the IP-BX module benefits from Lock-Keeper architecture to do IPv4/IPv6 handoff in a simple way without doing complete header processing and transformation between the two IP versions.

D. *IPSec with the Lock-Keeper*

Due to the physical separation, it is impossible for the external host to establish a direct connection to the internal network behind the Lock-Keeper. The Lock-Keeper breaks the connectivity and used different IP protocols to transfer data between its components. The Lock-Keeper Secure Data Exchange (LK-SDE) works as a proxy to manage the intercommunication between the Lock-Keeper components. However, it is still possible for the external user to use end-to-end security scheme, IPSec, which depends on the source and destination address, with the external interface of the OUTER.

Although IPSec provides confidentiality, integrity, and authenticity protection of IP packets, it is not a protection against application attacks. So, the security tools integrated to the GATE are very important for doing the “offline” scanning to ensure that there is no malicious data go into the internal network. Consequently, using IPSec with the Lock-Keeper will introduce a more secure system which provides confidentiality, integrity, and authenticity, as well as application-layer security.

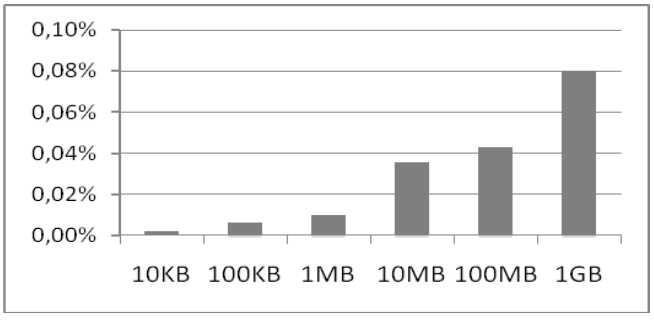


Figure 8. Percentale increase in transfer time for different file sizes due to integrating IPv6 on Lock-Keeper comparing to the original Lock-Keeper.

VI. CONCLUSION

IPv6 is a viable solution to IPv4 addressing space depletion problem. Accordingly, IPv6 is being integrated into more and more new products. However, the migration to IPv6 may take many years and new products should be able to communicate with both IPv4 and IPv6 during the coexistence period.

Consequently, we integrate IPv6 on the Lock-Keeper to extend it to work in both IP4/IPv6 environments in a secure way. An IPv4/IPv6 isolation mechanism based on the protocol separation is used to permit the secure data exchange over physically separated networks. The validation of the proposed solution is achieved through a practical deployment of IPv6 on Lock-Keeper system.

The contributions of this paper can be summarized as:

- Increasing the usability of the Lock-Keeper to work with both IPv4 and IPv6.
- Enhancing the security of the Lock-Keeper protected network by integrating an IPv4/IPv6 protocol handoff mechanism.
- Providing a physical separation based IPv4/IPv6 isolation approach.
- A prototype to prove concepts and test the practical deployment of IPv6 is realized on the Lock-Keeper system.

We tested IPv6-involved FTP applications. However, other IPv6-based applications, such as Web server and Mail server can be easily integrated on Lock-Keeper.

REFERENCES

[1] IPv4 Address Report, Dec. 2010, http://www.potaroo.net/tools/ipv4

[2] Lock-Keeper Website, Dec. 2010, http://www.lock-keeper.org/

[3] F. Cheng, and C. Meinel, "Research on the Lock-Keeper Technology: Architectures, Applications and Advancements," International Journal of Computer and Information Science 5(3), 2004, pp.236–245.

[4] F. Cheng, and C. Meinel, "Lock-Keeper: A new implementation of physical separation technology," In: Paulus, S., Pohlmann, N., Reimer, H. (eds.) Securing Electronic Business Processes: Highligths of the Information Security Solutions Europe Conference, (ISSE 2006), Friedrich Vieweg & Sohn Verlag, 2006, pp. 275–286.

[5] D. S. Punithavathani and K. Sankaranarayanan, "IPv4/IPv6 Transition Mechanisms European Journal of Scientific Research, Vol.34 No.1, 2009, pp.110-124.

[6] J. Bi, J. Wu, and X. Leng. "IPv4/IPv6 Transition Technologies and Univer6 Architecture," IJCSNS International Journal of Computer Science and Network Security, Vol. 7(1), January 2007, pp. 232-243.

[7] E. Nordmark and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," RFC 4213, October 2005.

[8] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels," RFC 2529, March 1999.

[9] C. Huitema, "An Anycast Prefix for 6to4 Relay Routers," RFC 3068, June 2001.

[10] A. Durand, P. Fasano, I. Guardini, and D. Lento, "IPv6 Tunnel Broker," RFC 3053, 2001.

[11] K. Tsuchiya, H. Higuchi and Y. Atarashi, "Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS) ," RFC 2767, February 2000.

[12] C. Aoun and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status," RFC 4966, July 2007.

[13] G. Lee, M. Shin, and H. Kim, "Implementing NAT-PT/SIIT, ALGs and Consideration to the Mobility Support in NAT-PT environment," Proceedings of the 6th International Conference on Advanced Communication Technology, 2004, pp.433-439.

[14] R. AlJa'afreh, J. Mellor, M. Kamala, and B. Kasasbeh, "Bi-Directional Mapping Systen as a New IPv4/IPv6 Translation Mechanism," In Proceedings of the 10th International Conference on Computer Modeling and Simulation (ICCMS 2008), Cambridge, England, UK, April 2008, pp. 40-45.

[15] J. Rushby and B. Randell, "A distributed secure system," In Proceedings of the EEE Symposium on Security and Privacy (S&P 1983 I), Oakland, California, USA, April 25– 27, 1983. pp. 127–135

[16] F. Cheng, P. Ferring, C. Meinel, G. Mü llenheim, and J. Bern, "The DualGate Lock-Keeper: A Highly Efficient, Flexible and Applicable Network Security Solution," in Proceedings of the 4th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2003). Luebeck, Germany. October 16-18, 2003.

[17] F. Cheng, M. Menzel, and C. Meinel, "A Secure Web Services Providing Framework based on Lock-Keeper," In Proceedings of 10th Asia-Pacific Network Operations and Management Symposium (APNOMS2007), Springer LNCS 4773, Sapporo, Japan, October 2007.

[18] Windows NT Server Resource Kit, 2010 Microsoft Corporation, http://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/inet/security.mspx?mfr=true

[19] WinSCP, 2010, http://winscp.net/eng/index.php

[20] Vsftpd, 2010, http://vsftpd.beasts.org/