Dynamic Network Separation for IPv6 Network Security Enhancement

SUZUKI, Shinsuke
Central Research Laboratory
Hitachi, Ltd.
1-280 Higashi-Koigakubo, Kokubunji, Tokyo, 185-8601, Japan
suz@crl.hitachi.co.jp

KONDO, Satoshi
Trend Micro Inc.
Shinjuku MAYNDS Tower, 30F 2-2-1 Yoyogi Shibuya-ku, Tokyo 151-0053, Japan
satoshi_kondo@trendmicro.co.jp

Abstract

In the current Internet, a site is often secured by firewall, filtering bogus traffic from outside at the border of the site. This 'Border Defence Model', however, obstructs the deployment of IPv6 applications and services, since firewall denies the benefits of IPv6, such as end-to-end communication and IPsec.

To solve this problem, 'Quarantine Model' is proposed. In this model, network nodes are accommodated to separate network segments according to their security levels, and a different security policy is implemented on each network segment. This 'divide and conquer' framework provides more flexible and better network security for Quarantine Model.

This paper discusses how to conduct dynamic network separation, which is mandatory to Quarantine Model, and analyzes the pros and cons of separation methods.

1. Introduction

1.1. Limitation of Firewall

A network site is often secured by firewall to prevent network attacks from outside, such as intrusion attacks, viruses, or DoS attacks. To block these attacks, firewall divides internal and external networks at the the border of the network site, and blocks or allows incoming traffic based on the security policy of the site.

However, firewall-based network protection cannot cope with various kinds of recent security threats, such as insider attack owing to virus infection, disallowed communication using laptop PC, mobile phone, or wireless LAN. Firewall assumes there is no security issues inside the network site and every malicious packets comes through the border of the network site, which is no longer true now. Furthermore, firewall is an obstacle for the deployment of IPv6, because it negates the benefit of IPv6, such as direct end-to-end communication and IPsec.

These two issues stem from the nature of firewall: it must be located in the middle of communication. Hence, it is quite difficult to cope with the issues mentioned above using firewall, and a new security framework is necessary to provide security without spoiling the benefit of IPv6.

1.2. Quarantine Model

'Quarantine model' is proposed to overcome the limitation of firewall[12]. In this model, Quarantine Server monitors the security level of a node, and Policy Enforcer accommodates the node to a network segment according to the security level of the node. This monitoring and accommodation is periodically conducted, which brings about a more precise and refined network management compared to a firewall-based network protection.

Quarantine Model consists of two features: security level measurement and dynamic network separation.

The former can be implemented using the state-of-the-art security level measurement systems[13, 18]. Although they still have some operational issues, such as generalization of the vulnerability database and automatic discovery of network nodes, these issues are essentially irrelevant to security level measurement itself.

Regarding the latter feature, there are several methods. They are, however, not originally dedicated for such security enhancement.

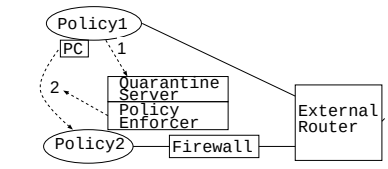

Figure 1. Overview of Quarantine Model

Therefore, this paper focuses on analysis of dynamic network separation methods, and considers the possible security issues.

2. Dynamic Network Separation

2.1. Possible Separation Method

To separate network connectivity, the Internet connectivity of a node has to be changed in one of the layers of the TCP/IP protocol suite. Considering the fact that the TCP/IP protocol suite consists of four layers, there are four corresponding separation methods.

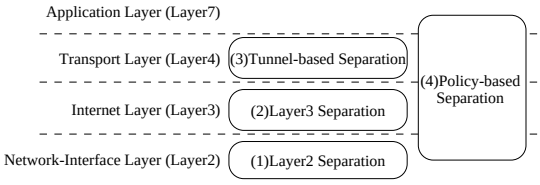

Figure 2. the TCP/IP Protocol Suite and Separation Method

(1)Layer2 Separation : Change the layer2 accommodating network, using logical layer2 networking protocol like IEEE802.1q VLAN. EAP[1] and IEEE802.1x are categorized here.

(2)Layer3 Separation : Change the layer3 accommodating network, by changing IP address of a node. In this method, different prefixes may be distributed to nodes in the same layer2 network segment. Hence, stateful address autoconfiguration[6] is required.

PANA[11] and Quarantine network[15] are typical examples in this category.

(3)Tunnel-based Separation : Change the tunnel server accommodating a node, through a tunnel management protocol. In this method, a node has to communicate via the assigned tunnel server through some layer4 tunneling session. Different from (1)Layer2 Separation , this method normally limits the protocol to be passed through the tunnel (e.g. IPv6 only, SIP only).

IPsec-VPN, SSL-VPN, and a tunnel-broker-based automatic IPv6 tunnel configuration [7] are typical examples in this category.

(4)Policy-based Separation : Change the communication policy in nodes, such as IPsec Policy and ACL, from a policy server. In this method, a node periodically obtains the communication policy from a policy server using some protocol like COPS[8], so that network administrators can control the behavior of a node from outside. The resolution of separation depends on the policy description given from network administrator.

Distributed Firewall[2, 16] and m2m-x[19] are categorized here.

2.2. Things to be Considered

Quarantine Model uses a node-identifier and a filtering-identifier to control network connectivity per node. The former identifies nodes within a network. The latter is used in a node-specific filtering rule, and the binding of these two identifiers is maintained in some manner. Therefore, it is essential in Quarantine Model to secure these identifiers and bindings.

Considering the importance of identifiers in Quarantine Model, this paper evaluates network separation methods in the following points of view.

(a) Removal of Previous Connectivity : whether a node can discard its previous connectivity, when a node is accommodated to a new network.

(b) Anti-spoofing : whether a node cannot override administrator's policy by spoofing its identifier.

(c) Management of Encrypted Communication : whether a network can control encrypted communications.

(d) Operation Cost : initial cost and running cost for identifier management.

2.3. Evaluation

Table 1 shows the evaluation results, followed by its explanation.

Table 1. Evaluation Result of Each Separation Method

Issue \ Method	(1)	(2)	(3)	(4)
(a)	OK†	OK	OK	OK
(b)	OK	OK†	OK	OK†
(c)	NG	NG	NG	OK
(d)	NG	OK†	OK	NG

(1)Layer2 Separation, (2)Layer3 Separation, (3)Tunnel-based Separation, (4)Policy-based Separation
(a) Removal of Previous Connectivity, (b) Anti-spoofing, (c) Management of Encrypted Communication, (d) Operation Cost
OK: state-of-the-art technology or implementations is enough.
OK†: same as above, but some operational hack is required.
NG: need a development or implementation of some new protocol to cope with the issue.

(a) Removal of Old Connectivity : (1)Layer2 Separation has one limitation; a node should retain an IPv6 address at least for two hours, even when it receives the IPv6 prefix with valid-lifetime=0 in stateless address autoconfiguration[17]. This may lead to a connectivity failure due to a wrong source address selection.

To cope with this issue in stateless address autoconfiguration, each layer2 network should have an accommodating router with different link-local address; when a link-local address of a default router becomes unreachable due to a network connectivity change, a node detects this unreachability using Neighbor Unreachability Detection (NUD)[14], and removes the prefixes obtained from this unreachable router.

Other separation methods does not have such limitation, since they administers IP address assignment statefully.

(b) Anti-spoofing : In (2)Layer3 Separation, a node can illegally obtain network connectivity by manual address configuration or forging its node-identifier for address assignment.

To completely remedy the former security hole, a router or a switch must filter packets if its source address is not included in the address management table of DHCP server[5]. For the latter security hole, an authentication framework is required in DHCP protocol itself[9].

From the operators' point of view, however, these threats can be alleviated by private-VLAN[10] or IGMP/MLD snooping[4]. Such technologies prevent a node from tapping packets from other nodes within the same network segment, which makes it difficult for a user to guess a network prefix or a node-identifier used by the other users.

In (4)Policy-based Separation, a node may overwrite the policy advertised from the server. The node, however, cannot obtain network connectivity completely unless the policy is also overwritten at the communication target node.

In (1)Layer2 Separation and (3)Tunnel-based Separation, a node cannot spoof network connectivity only by itself, because the accommodating switch or server need be changed.

(c)Encrypted Communication Management: Encrypted communication, especially IPsec, is originally designed to prevent forging and tapping in the middle of communication. Hence, only (4)Policy-based Separation can manage encrypted communication, e.g. contents-filtering, session management. Other methods cannot cope with this issue, since they filter traffic at the equipment in the middle of communication.

(d) Operation Cost : Table 2 shows what kind of identifier is used and how it is managed.

(1)Layer2 Separation normally manages only layer2-related information, such as VLAN-ID, MAC address, and authenticated user-ID. This is, however, not enough in the everyday security operation, since security incidents are often identified by layer3 address, layer4 protocol, and layer4 port number. Thus, layer3 address information has to be attached to this layer2-related information management.

Operation cost of (4)Policy-based Separation depends on the ability of the policy specification language; the more minute it is, the more complex and expensive policy management becomes. Current policy-base separation method focuses mainly on policy distribution, but not on policy management. Hence, this policy management needs further study in any implementation.

(2)Layer3 Separation and (3)Tunnel-based Separation does not need any additional management, since all the identifier that these methods requires are already managed in these separation protocols.

2.4. Discussion

When a network administrator needs to manage encrypted communication within a network, he/she needs to

Table 2. Identifiers and Their Management in Each Separation Method

Separation Method	Identifiers and Their Management
(1)	Node-ID = User-ID in Layer2 Authentication
	Filtering-ID = Layer2 address, IP address, VLAN-ID
	Binding Management = Layer2 management linked to Layer3 address assignment
(2)	Node-ID = DHCP Identifier
	Filtering-ID = IP Address, Layer2 address
	Binding Management = DHCP
(3)	Node-ID = User-ID in tunnel management protocol
	Filtering-ID = IP address, Tunnel Server
	Binding Management = Tunnel Session Management Protocol (e.g. TSP[3])
(4)	Node-ID = User-ID in Policy distribution protocol
	Filtering-ID = IP address, Layer2 address, etc
	Binding Management = Policy Management

(1)Layer2 Separation, (2)Layer3 Separation, (3)Tunnel-based Separation, (4)Policy-based Separation

adopt (4)Policy-based Separation, provided that the cost of the policy management is not so expensive compared to the expected security risk caused by the lack of encrypted communication management.

Otherwise, if the total amount of traffic from users does not exceed the forwarding performance of a tunnel server (about 100–500Mbps in general), tunnel-based separation method is the best method, since it does not have any other weak point compared to other methods.

In neither of the above environment, it depends on network administrators' priority to judge which is the best separation method, because all the methods have pros and cons. If operation cost is the most important point, (2)Layer3-based Separation is better than the other solutions. If complete security is the most important point, (1)Layer2 Separation and (4)Policy-based Separation are better than the other two.

3. Conclusions

This paper introduces Quarantine Model to overcome the limitation of firewall, which is an obstacle against the deployment of IPv6. Furthermore, it categorizes several dynamic network separation methods, and analyzes their pros and cons in terms of the identifier management. Based on this investigation, this paper proposes an appropriate method depending on the network environment.

4. Acknowledgment

I would like to show my special thanks to people in Secure6 Working Group of WIDE Project, Jordi Palet Martinez, and Ben Schultz, for their valuable comments.

References

[1] B. Aboba, L. J. Blunk, J. R. Vollbrecht, J. Carlson, and H. Levkowetz. "Extensible Authentication Protocol". *IETF RFC3748*, 2004.

[2] S. Bellovin. "Distributed Firewalls". *;login;*, pages 39–47, 1999.

[3] M. Blanchet and F. Parent. "IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)". *IETF draft-blanchet-v6ops-tunnelbroker-tsp-01.txt*, 2004.

[4] M. Christensen, K. Kimball, and F. Solensky. "Considerations for IGMP and MLD Snooping Switches". *IETF draft-ietf-magma-snoop-11.txt*, 2004.

[5] Cisco. "Configuring DHCP Snooping and IP Source Guard". *http://www.cisco.com/*, 2002.

[6] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Marney. "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". *IETF RFC3315*, 2003.

[7] A. Durand, P. Fasano, and D. Lento. "IPv6 Tunnel Broker". *IETF RFC3053*, 2001.

[8] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry. "The COPS (Common Open Policy Service) Protocol". *IETF RFC2748*, 2000.

[9] R. B. Hibbs, C. Smith, B. Volz, and M. Zohar. "Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Threat Analysis". *draft-ietf-dhc-v4-threat-analysis-02.txt*, 2004.

[10] S. HomChaudhuri and M. Foschiano. "Private VLANs: Addressing VLAN scalability and security issues in a multi-client environment". *IETF draft-sanjib-private-vlan-02.txt*, 2004.

[11] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy, and A. Yegin. "PANA Framework". *IETF Internet Draft, draft-ietf-pana-framework-00.txt*, 2004.

[12] S. KONDO, S. SUZUKI, and A. INOUE. "Quarantine Model Overview for IPv6 Network Security". *IETF draft-kondo-quarantine-overview-01.txt*, July 2004.

[13] Microsoft. "White Paper: Microsoft Baseline Security Analyzer V1.2". *http://www.microsoft.com/technet/*, June 2004.

[14] T. Narten, E. Nordmark, and W. Simpson. "Neighbor Discovery for IP Version 6 (IPv6)". *IETF RFC2461*, 1998.

[15] NEC. "Quarantine System Solution". *http://www.nec.co.jp/*, 2004.

[16] J. Palet, A. Vives, G. Martinez, and A. Gomez. "IPv6 Distributed Security Requirements". *IETF Internet Draft, draft-palet-v6ops-ipv6security-01.txt*, 2004.

[17] S. Thomson and T. Narten. "IPv6 Stateless Address Autoconfiguration". *IETF RFC2462*, 1998.

[18] J. A. Vidrine. "Vulnerability and eXposure Markup Language". *http://www.vuxml.org/*, 2004.

[19] T. Yamasaki. "IPv6, m2m-x & Net Appliance —New World of the Internet—". *Global IPv6 Summit in China 2004*, 2004.