行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　※
※**虛擬私有網路閘道** Layer 2/Layer3 **安全通訊協定之研究與設計**※
※The Study and Design of VPN Layer2/Layer3 Secure Communication Protocols※
※　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別： ¦**個別型計畫**　　æ**整合型計畫**
計畫編號： NSC　89-2213-E-009-153
執行期間： 89 **年** 8 **月** 1 **日至** 90 **年** 7 **月** 31 **日**
全程計劃： 89 **年** 8 **月** 1 **日至** 92 **年** 7 **月** 31 **日**

計畫主持人：謝續平　教授

本成果報告包括以下應繳交之附件：
æ**赴國外出差或研習心得報告一份**
æ**赴大陸地區出差或研習心得報告一份**
æ**出席國際學術會議心得報告及發表之論文各一份**
æ**國際合作研究計畫國外研究報告書一份**

執行單位：國立交通大學資訊工程研究所

中　華　民　國 90 **年** 7 **月** 12 **日**

行政院國家科學委員會專題研究計畫成果報告
虛擬私有網路閘道 Layer 2/Layer3 安全通訊協定之研究與設計
The Study and Design of VPN Layer2/Layer3 Secure Communication Protocols

計畫編號：NSC 89-2213-E-009-153
執行期限：89 年 8 月 1 日至 90 年 7 月 31 日
全程計劃：89 年 8 月 1 日至 92 年 7 月 31 日
主持人：謝續平 教授　國立交通大學資訊工程學系
計畫參與人員：何福軒、李富源、吳怜儀、鍾昌翰、吳裕國

中文摘要

在目前網路蓬勃發展的環境下，各個公司組織通常會建構內部網路(Intranet)以提供各式各樣的網路服務，例如資料的傳遞、網路電話、或者網路傳真的應用。因此，許多學者致力於開發一種節省成本，同時達到私密性的網路技術—虛擬私有網路(簡稱 VPN)，將私密封包包裹，透過隧道(tunnel)的方式來傳遞。VPN 主要可以分成兩大部分：建立虛擬通道的隧道技術，以及提供私密性的安全服務。因此，在本年度計劃中，我們著手討論三個重要的議題：首先，針對現有的隧道技術作分析與比較；接著，討論提供安全服務的身份認證協定；最後，考慮 VPN 與現有網路環境配合使用之情形，我們發現在 NAT (Network Address Translation)的環境下，會產生外部電腦無法主動連線至 NAT 內部、以及兩個 NAT 區域網路採用 VPN 連線時，會有私有 IP (Private IP)相衝突的問題。

關鍵詞

虛擬私有網路，隧道，IPSec，PPTP，L2TP，IKE，ISAKMP/OAKLEY，Kerberos，SNP，NAT

Abstract

Nowadays the Internet has been very popular. Corporations or organizations usually construct their own intranet for the use of many kinds of Internet applications such as data, voice, fax, etc. Many researchers devote themselves into the development of a new network technology, that is, virtual private network (VPN) to build up a private network among their intranets. VPN, a virtual tunnel technology for carrying private traffic, processes two main functions: tunneling protocols to provide virtual path and security services to support private characteristics. In this project, we consider three critical issues as the first step of total project: first, we compare main protocols providing tunneling mechanism. Second, we discuss several authentication protocols essential to provide security services. Finally, we debate the problems when applying VPN on NAT (Network Address Translation) environment.

Keywords

Virtual Private Network, tunnel, IPSec, PPTP, L2TP, IKE, ISAKMP/OAKLEY, Kerberos, SNP, NAT

1. Comparison of VPN Tunneling Protocols

At present, several protocols are designed to construct a virtual private network: Layer2 Forwarding (L2F) [Valencia98], Point-to-Point Tunneling Protocol (PPTP) [Hamzeh99], Layer2 Tunneling Protocol (L2TP) [Townsley99] at layer 2, IPSec at layer 3, and SOCKs [VanHeyningen99] at layer 7 of OSI model, etc. By several reasons, PPTP, L2TP, and IPSec protocols are suggested to be used, and will be dominant of VPN technology in future. However, all these protocols have some strengths, weakness, and suitable network architecture. We have done a survey and comparison of those protocols as a first step of our project.

A key point whether a protocol will survival or just disappear is the support behind it, either by vendors or standard formulating institutes. PPTP are already implemented by Microsoft on its window PC. Vendors who support PPTP are also going to construct L2TP products. Moreover, L2TP is now a standardized protocol by IETF. As like L2TP, IPSec protocol sets are also standardized.

Flexibility is also a concern. Because PPTP and L2TP are Layer2 VPN protocols, they can apply to several kinds of networks, Ethernet, ATM, frame relay, etc. However, IPSec is Layer3 protocols. Thus, IPSec can only construct above IP-based network, otherwise, we will need special devices to convert traffic into IP datagram.

Another scalability problem occurs when number of users increases. PPTP is limited to a small number of remote users. Although it can support Lan-to-Lan architecture, PPTP doesn't work as well as IPSec due to its authentication and tunnel control mechanism. L2TP improves some performance, but still limits to remote access users.

Cost needed to build up a PPTP for a corporation might be minimal, since one can only set up a PPP client and a PPTP server at corporate site and outsource most functions to an ISP. Simplified protocol can reduce network management cost and be widely used on small-scale environment, such as a company. On the other side, L2TP and IPSec protocols are more complex and every hosts need to have VPN functionality and may be costly.

As refer to security concerns, PPTP has weak authentication algorithm (PAP, CHAP [Simpson96], MS-CHAP) and no encryption mechanism. L2TP improve this weakness by including IPSec to strengthen data integrity, authentication, and key management. IPSec seems more secure, but its security hasn't been proved yet.

2. Comparison of VPN Authentication and Key Management Protocols

A complete design of VPN protocols should contain security mechanisms as well as tunneling functions. Therefore, we survey and compare several protocols suitable for a VPN network environment.

(1) Needham-Schroeder

Needham-Schroeder [Needham78] model was one of the very first models to provide authentication. This protocol uses a third-party authentication server to produce a session key.

When a client wants to construct a connection to a server, he or she first sends a request to authentication server for a session key. Then, both end use this key to establish their connection.

However, Needham-Schroeder can't resist replay attack .

(2) Kerberos

Kerberos [Steiner88] is a successor protocol of Needham-Schroeder model. It separates an authentication server in Needham-Schroeder into a Kerberos authentication server, and a ticket-granting server (TGS).

Once a user logs in the system, a request is sent to Kerberos server to grant a TGS ticket. If needing a specific service, a user first uses a valid TGS ticket to get another service ticket. Then use this service ticket to request service.

Using Kerberos, users only have to send secret once during logging which increase security strength of Kerberos. However, two types of tickets are expired by timestamp, which cause Kerberos vulnerable to replay attack if the client and server clock are not synchronized.

(3) SNP

SNP uses symmetric cryptography and minimizes messages to achieve authentication and key distribution. When a client wants to construct a connection to a server, he/or she first sends a request to authentication server for a session key. Then, both end use this key to establish their connection.

SNP including nonce instead of timestamp in Kerberos can prevent replay attack. Furthermore, it also provides data integrity by using symmetric key (for example: password) encryption.

However, SNP only uses password as the encryption and lacks for flexibility.

(4) IKE

IKE developed by IETF is one of main part of IPSec and a combination of Okaley and ISAKMP (Internet Security Association and Key Management Protocol). ISAKMP [Maughan98] provides a framework for authentication and key exchange but does not define them. On the other hand, Oakley ([Orman98]) describes a series of key exchanges.

IKE is flexible and secure because ISAKMP supports many kinds of key exchanging method, and once a new authentication technology is developed, it can be easily included by self if both endpoints of a tunnel have agreement in advance.

IKE can prevent several network attack by using Oakley. Oakley defines cookies to prevent clogging attack, nonce to prevent replay attack, and authentication during session key exchange to prevent man in the middle attack.

However, IKE defines two phases and three modes for authentication, and is complicated than the three protocols mentioned above. Moreover, IKE specification is hard to understand preventing the popularity usage.

(5) Comparison of Authentication and Key Management Protocols

Although IKE protocol sets are complex, it has already standardized by IETF. Further, IKE is secure, flexible, and compatible with IPSec tunneling protocols. It will be most suitable protocols for IPSec authentication.

3. A Debate on VPN and NAT Cooperation

(1) Solutions to IP Address Depletion

With the rapid growth of Internet services, IP address space is drying up soon. To deal with IP address depletion, many scholars do research on it and propose many solutions. The most important schemes of them are IPv6 (IP version 6) [RFC2460] and NAT.

IPv6, also called IPNG, is a new version of the Internet Protocol, investigated as the successor to IPv4. In order to solve the problem of IP address depletion, IPv6 extends the IP address space from 32 bits to 128 bits and combines IPsec mechanism within it.

While IPv6 really provides a long-term solution to the problem of IP address depletion, it requires

modifications to end hosts and costs too much to translation the current network environment from IPv4 to IPv6.

In contrast with IPv6, NAT by itself provides a transparent routing solution to end hosts that need to communicate to disparate address realms. NAT modifies end node addresses re-route and maintains states for these updates so that datagrams pertaining to a session are transparently routed to the right end-node in either realm.

In addition to providing a solution to the problem of IP address depletion, NAT hides internal network hierarchy from external network and offers a certain level of network security. For an organization such as a company or a campus, NAT is usually the simple and cheap solution to IP address depletion.

(2) VPN and NAT Cooperation Problem

Although NAT provides the features of transparent solutions to IP address depletion, there are really some problems caused by NAT. First, NAT hides internal network structure from external world so that internal services behind NAT are invisible to external realm. Second, NAT allows only uni-directional connections instead of bi-directional connections which prevents services from being contacted from outside world.

These properties of NAT prevent internal service from being reached from outside world. It seems that the services are hid behind NAT servers, and we denote such a problem as **hidden service problem.**

(3) Current Solutions to VPN and NAT Cooperation Problem

Currently, there are already papers or engineering reports proposed to solve Hidden Service Problem. Some of them focus on service probing while the others emphasize internal server connection ability, which means that sessions to internal servers can be initialized from external realm. We summarize as follows :

A. Service Probing

With rapid growth of Internet services, it is difficult that a host configures each desired service separately. SLP (Service Location Protocol) defined in [SLP99] is introduced to provide a framework for a host to configure Internet services dynamically.

To reach this goal, SLP involves three agents: DA (Delivery Agent), SA (Service Agent), and UA (User Agent). UA performs service discovery with service attributes on behalf of client software. SA advertises the location and attributes on behalf of services. DA aggregates service information into what is initially a stateless repository.

There are four SLP implementations: LDAP (Light Directory Access Protocol) [RFC2251] [VH99], DNS [RFC1035], Sun's Jini [JiniSpec] [JiniTech] [JiniArch] [SLPJini] and Berkery's SDS (Secure Service Discovery Service) [SDS99].

LDAPv3 is an Internet alternative to the standard X.500 Directory Access Protocol (DAP). LDAP servers provide LDAP clients a way to access objects by using some attributes in an entry and involve some X.500 security concepts. DNS is normally used to provide the mapping mechanism between FQDN and IP address.

Jini, developed by Sun, is purely based on Java and full of object-oriented concepts. In Jini, if Service Provider permits client's request, it returns not only the location and attributes of services but also the object handles by which clients use to contact with Service Provider. That is, Jini operating environment offers Jini Java-based clients decentralized and dynamic access to servers.

SDS adopts the concept of SLP and improves security and scalar problems in original SLP. A comparative table of SLP and the four implementations of SLP is organized as Table .

From the comparison shown in Table 1, we conclude that those implementations all are lack of some mechanisms to cooperate with NAT except to DNS. Although DNS scheme adopts DNS_ALG to cooperate with NAT, the solution only supports few one-line hosts at a time because it does not make effective use of IP address.

	LDAP	DNS	SLP	Jini	SDS
Directory structure	Fixed	Fixed	Dynamic	Dynamic	Fixed
Message authentication	Password	None	Certificate	Java RMI	Secure SDS communication
Query description	CN/C/DN	FQDN/IP	Service template	Object description	XML
Response	Object	IP/FQDN	URL	Object handle	URL
Scalar	Yes	Yes	Partial	Yes	Yes
Access restriction	ACL	NO/?	Scopes	?	?
Widely deployment	Yes	Yes	No	No	No
NAT	No	DNS_ALG	No	No	No

Table 1 Comparisons between SLP(s)

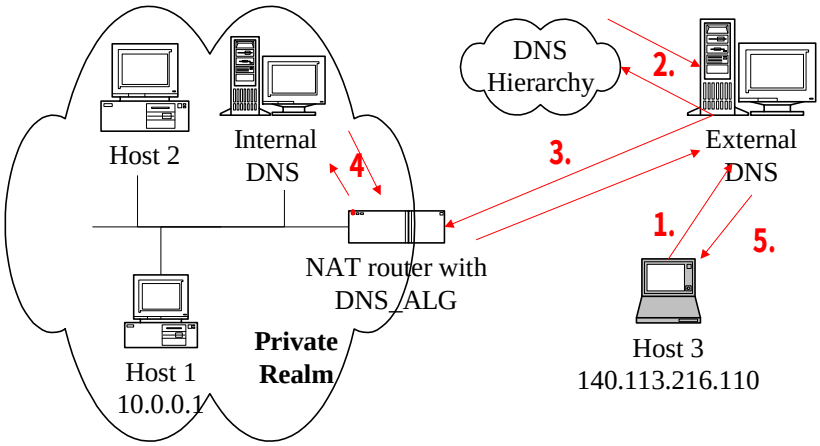

Figure 1 DNS Application Level Gateway

B. Internal Server Connection Ability

Three important schemes about internal server connection ability are discussed here. They are DNS Application Level Gateway, port forwarding and expanded NAT.

a) DNS Application Level Gateway

DNS Application Level Gateway (DNS_ALG), defined in [RFC2694] as an extension to NAT, is introduced to provide a transparent solution to hidden service problem. Functionally, DNS_ALG is a module within NAT servers, and NAT server will notify the module to perform DNS payload changes when NAT server intercepts a TCP or UDP packet with destination port set to 53 (53 is the common port for DNS service defined in /etc/services). DNS_ALG will interact with NAT server and modify payload transparently to alter address mapping of hosts as DNS packets cross one address realm into another.

The important assumption of DNS_ALG is that every host will resolve FQDN (Fully Qualified Domain Name), which stands for the globally unique identity of the host, by sending DNS queries to the proper DNS server before it begins the connections to the peers.

We introduce DNS_ALG with Figure 1. If Host A wishes to communicate with an internal Host B with its FQDN, it will issue a DNS query containing destination's FQDN to configured DNS server (Step 1). The configured DNS server will send client's DNS query to internal DNS server (step 2,3). NAT server will find that it is an incoming DNS query and notify DNS_ALG to handle it.

In step 4, DNS_ALG notices the query comes from external realms and requests NAT server to (a) setup a temporary binding for Host 1 (10.0.0.1) with an external address (140.114.10.1) and (b) initiate Bind-holdout timer. When NAT successfully sets up a temporary binding with an external address, DNS_ALG will modify response payload to replace the private address with its external assigned address and set the Cache timeout to be zero. In step 5, the DNS response is returned to querying Host 3. At last, inbound session to internal Host 2 can be initiated from external Host 3.

DNS_ALG scheme bases on current DNS structures and requires little modification to current communication peers. However, the scheme suffer the following two constrains:

First, it just provides internal server connection ability in one-level NAT case partially. For two-level NAT case, the first level NAT server will intercept the DNS query and notify DNS_ALG to handle with it. DNS_ALG will find the host belongs to the next level NAT realm and ignore the DNS request.

Second, when intercepting inbound DNS query, DNS_ALG will pick up an available IP address and assign it to the queried host. PAT (Port Address Translation) is an application of NAT, which means that NAT server only holds a single IP address and identifies different connections by ports. DNS_ALG will not work in PAT application.

b) Port Forwarding

The original name of port forwarding is IP substitution. Port forwarding by itself is a combination of routing by port and packet rewriting. For conventional routing, routers route packets to end hosts right according to the packets' destination address. Port forwarding examines the packet headers and rewrite IP headers if necessary. At last, port forwarding forwards the packets on to another host depending on the destination port.

In more detail, port forwarding forwards all packets intended for one forwarding port on the gateway from the external networks to route on a specified port on one of the internal machines. Figure describes the workflow of port forwarding with four steps. The web manager needs to inform network administrator to build the redirecting record in advance. If clients want to connect to internal web sever, he would connect inside by following the following steps as the four blue arrows.

Although port forwarding is a low cost solution, it suffers the two drawbacks: first, Port forwarding only supports applications, which won't change their communication port after the control connection is

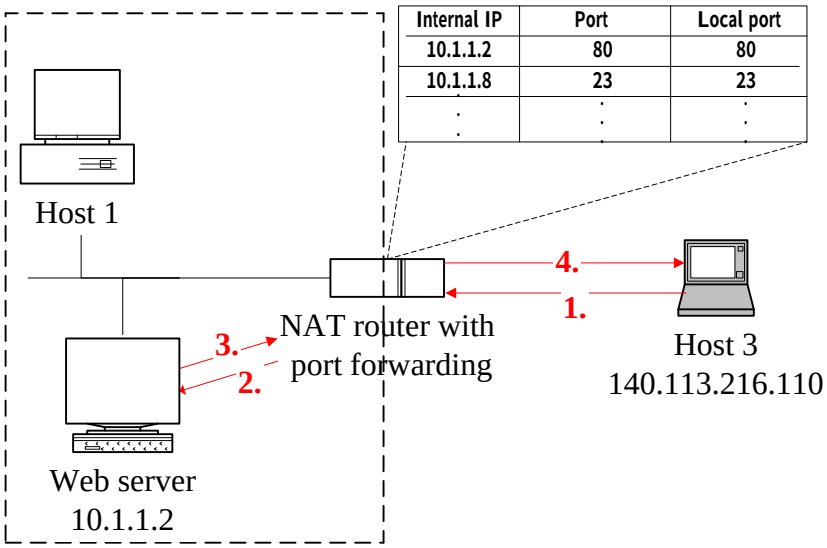

Figure 2 Port Forwarding

established. The applications with dynamic ports could not be handled with port forwarding.

Second, every server manager has to inform NAT network administrator in advance and provides no flexibility. In multi-level NAT case, the solution becomes not flexible because every server manager should inform every NAT network administrator in advance.

c) Expanded NAT

Another solution, expanded NAT, introduced in [ExNAT99] is designed for internal server connectivity by modifying NAT records. In their paper, they focus on NAPT (Network Address Port Translation), which shares different sessions with the same IP address but different port. Their discussion is divided into two parts: session from public network into private network and connection spanned on two private networks.

Their solution for case A is based on port forwarding, and is a static solution. Their solution for case B is IP-tunneling based, but they neglect the problem of private IP address conflict.

d) Summary

Although SLP implementation series really provide a flexible way for clients to configure various services, they lack some mechanism to cooperate with NAT. Port forwarding does not support dynamic-port applications, and DNS_ALG does not fit two-level NAT case. Therefore, neither of the above schemes is not a good solution for external clients to solve hidden service problem behind NAT.

(4) Future Work

When NAT has grown from experimental technology to practical applications, it is urgent that some scheme be proposed to solve the VPN and NAT cooperation problems indicated above.

Next year, we will propose a service probing protocol for hidden services behind NAT. The proposed protocol mainly assists clients to locate their desired services with their service descriptions. When matched services are found, our protocol is responsible to cooperate with NAT server with IP filtering to reserve or release mapping states according to their connections dynamically.

The protocol will be designed for multi-level NAT, and be suitable for current environments. Besides, we decide to group relational Probe servers into domains, and support service probing across different domains, which will makes our protocol fit variable applications.

4. Reference

[AH98] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998

[ESP98] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998

[Hamzeh99] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999

[Hanks94] S. Hanks, T. Li, D. Farinacci, P. Traina, "Generic Routing Encapsulation (GRE)", RFC 1701, Oct. 1994

[Harkins98] D. Harkins, D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, Nov. 1998

[Krawczyk96] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, Feb. 1997

[Madson98] C. Madson, N. Doraswamy, “The ESP DES-CBC Cipher Algorithm With Explicit IV”, RFC 2405, Nov. 1998

[Maughan98] D. Maughan, M. Schertler, M. Schneider, J. Turner, “Internet Security Association and Key Management Protocol (ISAKMP)”, RFC 2408, Nov. 1998

[Needham78] R. Needham, M. Schroeder, “Using encryption for authentication in large networks of

computers", Communications of the ATM, 1978

[Perkins96] C. Perkins, "IP Encapsulation within IP", RFC 2003, Oct. 1996

[Orman98] H. Orman, "The OAKLEY Key Determination Protocol", RFC 2412, Nov. 1998

[Rigney97] C. Rigney, A. Rubens, W. Simpson, and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997

[SA98] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[Simpson94] W. Simpson, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994

[Simpson96] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996

[Steiner88] J. G. Steiner, B. C. Neuman, J. I. Schiller, "Kerberos: An Authentication service for Open Network System," Proceedings of the Winter 1988 Usenix Conference, Feb. 1988

[Townsley99] W. Townsley, et al., "Layer Two Tunneling Layer Two Tunneling Protocol (L2TP)", RFC 2661, August 1999

[Valencia98] A. Valencia, M. Littlewood and T. Kolar, "Cisco Layer Two Forwarding (Protocol) L2F", RFC 2341, May 1998

[VanHeyningen99] M. VanHeyningen, "SOCKS Protocol Version 5", Feb. 1999

[Zorn98] G. Zorn, S. Cobb, "Microsoft PPP CHAP Extensions", Oct. 1998

[Zorn00] G. Zorn, "Microsoft PPP CHAP Extensions, Version 2", Jan. 2000

[RFC1631] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)", RFC1631, May 1994.

[RFC2663] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, Aug. 1999.

[RFC2460] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, Dec. 1998.

[VH99] Versna Hasller, "X.500 and LDAP Security: A Comparative Overview", IEEE Network, pp. 54-64, Vol. 13, Issue: 6, Nov.-Dec. 1999.

[RFC1035] P. Mockapetris, "Domain Nnames – Implementation and Secification", RFC1035, Nov. 1987

[TCP/IP] W. Richard Stevens, "TCP/IP Illustrated, Volumne1", Addison-Wesley, Reading, Mass, 1994.

[JiniSpec] SUN MICROSOFTSYSTEMS, "Jini technology specifications. white paper", http://www.sun.com/jini/specs/.

[JiniTech] SUN MICROSOFTSYSTEMS, "Jini technology architectural overview. White paper", http://www.sun.com/jini/whitepapers/architecture.html

[JiniArch] J. Waldo, "The JINI architecture for network-centric computing", Communications of ACM, pp. 76-82, Vol. 42, Issue: 7, Jul. 1999.

[SLP97] Guttman, E., "Service location protocol: automatic discovery of IP network services", pp. 71-80, Vol. 3, Issue: 4, July-Aug. 1999.

[SLPJini] Guttman, E. and Kempf, J., "Automatic discovery of thin servers: SLP, Jini and the SLP-Jini Bridge", IECON '99 Proceedings. The 25th Annual Conference of the IEEE, pp722-727, vol.2, Dec. 1999.

[SDS99] S. E. Czerwinski, B. Y. Zhao, and T. D. Hodes, A. D. Joseph, and R. H. Katz, "An architecture for a Secure Service Discovery Service", Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking , pp. 24-35, Aug. 1999.

[RFC2694] P. Srisuresh, G. Tsirtsis, P. Akkiraju, and A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)", RFC 2694, Sep. 1999.

[CBAC99] Cisco Cooperation, "Cisco IOS Firewall Feature Set and CBAC" http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/firewall.htm

[HJI96] H.Y. Yeom, J. Ha, and I. Kim. IP Multiplexing by Transparent Port-Address Translator, the Preceedings of the Tenth USENIX System Administration of Conference (LISA X) Chicago, IL, USA, Sep. 1996

[ExNAT99] E.S. Lee, H.S. Chae, B.S. Park, and M.R. Choi, "An expanded NAT with server connection ability", TENCON 99. Proceedings of the IEEE Region 10 Conference, pp. 1391-1394, vol.2, Sep. 1999.

[TO99] Terao, K., and Ono, S., "A shared secure server for multiple closed networks", Internet Workshop, 1999. IWS 99, pp. 32-39, Feb. 1999.

[PIXfirewall] Cisco Cooperation, "Cisco PIX firewall Series", http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm

[RFC793] Information Sciences Institute University of Southern California, "Transmission Control Protocol", RFC793, Sep. 1981

[RFC2608] E. Guttman, C. Perkins, J. Veizades, and M. Day, "Service Location Protocol, Version 2", RFC2608, Jun. 1999.

[RFC2251] M. Wahl, T. Howes, and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC2251, Dec.1997.