INTERNET-DRAFT
<draft-ietf-aft-socks-multiple-traversal-00.txt>
Expires in six months

M. Kayashima
M. Terada
T. Fujiyama
T. Ogino
Hitachi Ltd.
21 November 1997

SOCKS V5 Protocol extension for Multiple Firewalls Traversal

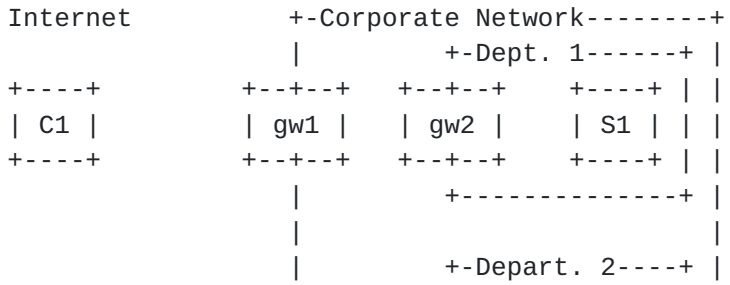
Status of this Memo

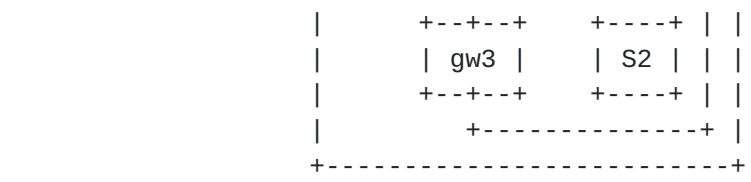
Abstract

This document provides the extended specification of SOCKS Version 5 which enable to use multiple firewalls traversal. In this protocol, client does subnegotiation with all servers on the communication path, and each server relays the connection after subnegotiation.

Propose

The network firewalls are currently being used for corporate networks, but there is a need to provide access control for departments in organizations as shown below.





The department firewalls, gw2 and gw3 are used for a fail safe system against intruders on the Internet, and they are used to provide access control for other departments members.

In this environment, the connection from the Internet client to department servers must traverses multiple firewalls. And the client authentication with each firewall may be used different method. For example, a firewall which protects corporate network needs strong authentication, because it is a gate of the Internet. But a firewall which protects department network uses more weak and convenient authentication method such as username/password.

Procedure for TCP-based client

This extended protocol is used for TCP-based clinets. When a TCP-based client wishes to establish a connection to an object that is reachable only via multiple firewalls which are located like a cascade.

In the SOCKS V5 protocol, the sequence between SOCKS client and SOCKS server is followed:

(1) Method specific subnegotiation
(2) Request Command
(3) Reply

In the extended protocol, client repeats these sequence with all SOCKS server which is located on the route of server. Method specific subnegotiation and Request Command is not extended from SOCKS V5 protocol.

To recognize the end of repeat, Reply packet is extended as follows:

VER	REP	RSV	ATYPE	BND.ADDR	BND.PORT	NXT.ADDR	NXT.PORT
1	1	X'00'	1	Variable	2	Variable	2

This packet format has two new fields; NXT.ADDR and NXT.PORT.

Where:

- REP Reply field:
  The reply code is extended with multiple firewalls traversal.
  o X'09' Connect next-hop SOCKS server
- NXT.ADDR Next-hop SOCKS server address
- NXT.PORT Next-hop SOCKS server port

The NXT.ADDR is next-hop SOCKS server address. The NXT.PORT is a port which is used at next-hop SOCKS server. If destination host is behind other SOCKS servers, the SOCKS server selects next-hop SOCKS server, which is located at the route of client and destination host, and can be connected to it. If SOCKS server can connect destination host directly, NXT.ADDR field and NXT.PORT field set to X'00'.

The reply code in REP field is extended for multiple firewalls traversal. X'09' is new value to express that the client MUST connect next-hop SOCKS server.

When the client receives this REP code, the client starts same sequence with next-hop SOCKS server. This sequence repeated while the client receives the reply code of X'09'.

If each subnegotiation method includes encapsulation for purposes of integrity checking and/or confidentiality, following request/reply packet and next subnegotiation packets MUST be encapsulated in the method dependent encapsulation. Each SOCKS server encapsulates request/reply packet for itself and subnegitiation packets for next hop SOCKS server. Other packets are relaied by SOCKS server without encapsulation.

Connection setup sequence

This section provides an example of connection setup sequence when the Internet client C1 establishes a connection with department server S1 via corporate firewall gw1 and the department firewall gw2.

(1) Sequence with gw1
- C1 connects to gw1.
- C1 does subnegotiation with gw1 directly.
- C1 sends Request to gw1.
- gw1 search destination. If gw1 is reachable the destination server, then gw1 send Reply to C1.

(2) Sequence with gw2
- gw1 connects to gw2.
- C1 does subnegotiation with gw2. This sequence is relayed by gw1.
- C1 sends Request to gw2.

- gw2 search destination. If gw1 is reachable the destination server, then gw2 send Reply to C1.

Security Considerations

This document describes a protocol for the multiple traversal of application layer firewalls. The security of such traversal is highly dependent on the particular authentication and encapsulation methods provided in a particular implementation, and selected during negotiation between SOCKS client and each SOCKS server.

References

[RFC 1928] Leech, M., Ganis, M., Lee, Y., Kuris, R. Koblas, D., & Jones, L., "SOCKS Protocol V5," April 1996.

Author's Address

Makoto Kayashima
Hitachi Ltd. Systems Development Laboratory
292 Yoshida-cho, Totsuka, Yokohama, Kanagawa 244, Japan
kayashi@sdl.hitachi.co.jp

Masato Terada
Hitachi Ltd. Systems Development Laboratory
292 Yoshida-cho, Totsuka, Yokohama, Kanagawa 244, Japan
terada@sdl.hitachi.co.jp