Network Working Group
Internet Draft
Document: draft-gupta-ospf-ospfv3-auth-01.txt
Expires: January 2003

M. Gupta
Nokia
N. Melam
Nokia
July 2002

Authentication/Confidentiality for OSPFv3

Status of this Memo

Abstract

This document describes means/mechanisms to provide authentication/confidentiality to OSPFv3 using IPv6 AH/ESP Extension Header.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [5].

Table of Contents

1. Introduction

In OSPFv3 for IPv6, authentication fields have been removed from OSPF headers. When running over IPv6, OSPF relies on the IPv6 Authentication Header (AH) and IPv6 Encapsulating Security Payload (ESP) to ensure integrity, authentication and/or confidentiality of routing exchanges.

This document describes how IPv6 AH/ESP extension headers can be used to provide authentication/confidentiality to OSPFv3.

It is assumed that the reader is familiar with OSPFv3 [1], AH [4], ESP [3], the concept of security associations, tunnel and transport mode of IPsec and the key management options available for AH and ESP (manual keying and IKE) [2].

2. OSPFv2 to OSPFv3

Security concerns MUST be taken away from OSPFv3 protocol and IPv6 stack MUST provide inherent security to OSPFv3 by using AH/ESP extension headers. It means OSPFv3 protocol MUST not receive any unauthenticated packets. As OSPFv2 has its own security mechanisms, no inherent security needs to be provided by the IPv4 stack. As OSPFv2 is only for IPv4 and OSPFv3 is only for IPv6, the distinction between the packets can be easily made by IP version.

Authentication and confidentiality, if provided, MUST be provided to the entire OSPFv3 header and data. Authentication to the selected portions of IPv6 header, selected portions of extension headers and selected options may also be provided optionally.

3. Authentication

Transport mode SA is the security association between two hosts or security gateways that are acting as hosts. SA must be tunnel mode if either end of the security association is a security gateway. OSPFv3 packets are exchanged between the routers but as the packets are destined to the routers, the routers act like host in this case. So

transport mode SA MUST be used in order to provide required security to OSPFv3.

In order to support OSPFv3 authentication, "ESP with NULL encryption" MUST be supported in transport mode. "AH" in transport mode SHOULD also be provided. AH in transport mode provides authentication to higher layer protocols, selected portions of IPv6 header, selected portions of extension headers and selected options. ESP with NULL encryption in transport mode will provide authentication to only higher layer protocol data and not to the IPv6 header, extension headers and options.

OSPF packets received in clear text and OSPF received with incorrect AH ICV MUST be dropped when authentication is enabled.

4. Confidentiality

Providing confidentiality to OSPFv3 in addition to authentication is optional. Confidentiality must be implemented using ESP extension header of IPv6 if it is being provided. ESP with non-null encryption in transport mode MUST be used for the providing confidentiality to OSPFv3.

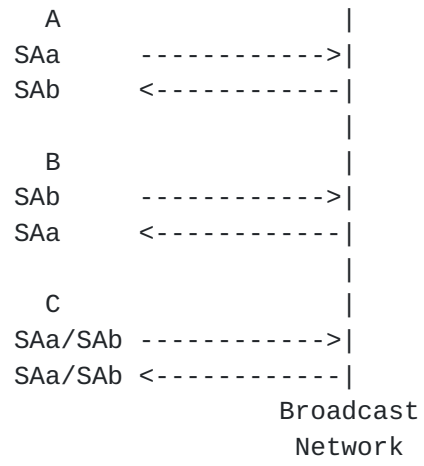
5. Authentication and Encryption Algorithms

hmac-md5-96 must be implemented as the authentication algorithm and DES-CBC must be implemented as the encryption algorithm.

6. Key Management

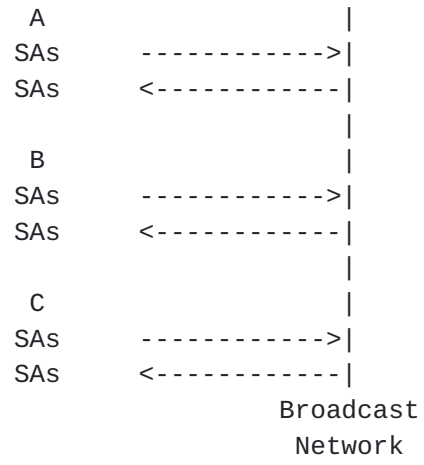
OSPFv3 exchanges both multicast and unicast packets. While running OSPFv3 over a broadcast interface, the authentication/confidentiality required is "one to many". Since IKE is based on the Diffie-Hellman key agreement protocol and works only for two communicating parties, it is not possible to use IKE for providing the required "one to many" authentication/confidentiality. Manual keying MUST be used for this purpose. In manual keying SAs are statically installed on the routers and these static SAs are used to encrypt/authenticate the data.

Since security associations (SAs) are directional, generally different security associations are used for inbound and outbound processing for providing higher security. The following figure explains that it is not possible to use different security associations for inbound and outbound processing in order to provide the required "one to many" security.



If we consider communication between A and B in the above diagram, everything seems to be fine. A uses security association SAa for outgoing packets and B uses the same for incoming packets and vice versa. Now if we include C in the group and C sends a packet out using SAa then only A will be able to understand it or if C sends the packets out using SAb then only B will be able to understand it. Since the packets are multicast packets and they are going to be processed by both A and B, there is no SA for C to use so that A and B both can understand it.

The problem can be solved with the following figure where all of them use the same SA for incoming and outgoing direction.



So, all the adjacent routers on a broadcast medium MUST use the same SA and the same SA MUST be used for inbound and outbound processing.

7. SA Granularity and Selectors

Different SA for different interfaces MUST be supported. In the outgoing path, IPv6 source address, OSPF protocol and egress

interface ID MUST be used as selectors to locate the SA to be

applied. In the incoming path, OSPF protocol, SPI and ingress interface ID MUST be used to locate the SA to be applied. Any incoming OSPF protocol packets on the given ingress interface that fail the confidentiality/authentication checks MUST be dropped.

8. Virtual Links

Different SA than the SA of underlying interface MUST be provided for virtual links. Packets sent out on virtual links use unicast site local or global IPv6 addresses as the IPv6 source address and all the other packets use multicast and unicast link local addresses. This difference in the IPv6 source address should be used in order to differentiate the packets sent on interfaces and virtual links.

As the end point IP addresses of the virtual links are not known at the time of configuration, the secure channel for these packets need to be setup dynamically. The end point IP addresses of virtual links are learnt during the routing table build up process. The packet exchange over the virtual links starts only after the discovery of end point IP addresses. In order to provide security to these exchanges, the routing module should setup a secure IPsec channel dynamically once it acquires the required information.

9. IPsec rules

The following set of rules can be installed in a typical IPsec implementation to provide the authentication/confidentiality to OSPFv3 packets.

Outbound Rules for interface running OSPFv3 security:

No.	interface	source	destination	protocol	action
1	iface	fe80::/16	any	OSPF	apply
2	any	src/128	dst/128	OSPF	apply

Inbound Rules for interface running OSPFv3 security:

No.	interface	source	destination	protocol	action
3	iface	fe80::/16	any	ESP or AH	apply
4	iface	fe80::/16	any	OSPF	drop
5	any	src/128	dst/128	ESP or AH	apply
6	any	src/128	dst/128	OSPF	drop

For outbound rules, action "apply" means encrypting/calculating ICV and adding ESP or AH header. For inbound rules, action "apply" means decrypting/authenticating the packets and stripping ESP or AH header.

Rules 4 and 6 are to drop the OSPFv3 packets without ESP/AH headers.

Rules 2, 5 and 6 are meant to secure the packets being exchanged over virtual links. These rules are dynamically installed after learning the end point IP addresses of a virtual link. These rules are installed on all the interfaces.

Rules 1, 3 and 4 are meant to secure the unicast and multicast packets that are not being exchanged over the virtual links. These rules are interface specific.

10. Replay Protection

As it is not possible as per the current standards to provide complete replay protection while using manual keying, the proposed solution will not provide protection against replay attacks.

Security Considerations

This memo discusses the use of IPsec AH and ESP headers in order to provide security to OSPFv3 for IPv6.

The use of manual keying does not provide very high level of security as compared to IKE but the security provided should be adequate for a routing protocol.

References

1. Coltun, R., Ferguson, D. and Moy, J., "OSPF for IPv6" RFC 2740, December 1999

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

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

4. Kent, S. and Atkinson, R., "IP Authentication Header (AH)" RFC 2402, November 1998

5. Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

Acknowledgments

Authors would like to extend sincere thanks to Marc Solsona, Janne Peltonen, John Cruz and Dhaval Shah for providing useful information and critiques in order to write this memo.

Authors' Addresses

Mukesh Gupta
Nokia
313 Fairchild Drive
Mountain View, CA 94043
Phone: 650-625-2264
Email: Mukesh.Gupta@nokia.com

Nagavenkata Suresh Melam
Nokia
313 Fairchild Drive
Mountain View, CA 94043
Phone: 650-625-2949
Email: Nagavenkata.Melam@nokia.com