Network Working Group
Internet Draft
Document: draft-ietf-ospf-ospfv3-auth-04.txt
Expires: June 2004

M. Gupta
Nokia
N. Melam
Nokia

December 2003

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 [N5].

Table of Contents

1. Introduction

In Open Shortest Path First - Version 3 (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 [N1], AH [N4], ESP [N3], the concept of security associations, tunnel and transport mode of IPsec and the key management options available for AH and ESP (manual keying [N2] and Internet Key Exchange (IKE)[I1]).

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 Security Association (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 hosts 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 or with incorrect AH Integrity Check Value (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 providing the confidentiality to OSPFv3. The user MUST be able to configure the encryption key and the authentication key separately.

5. IPsec Requirements

In order to implement this specification, the following IPsec capabilities are required.

Transport Mode
: IPsec in transport mode MUST be supported.

Traffic Selectors
: The implementation MUST be able to use interface index, source

address, destination address, protocol and direction for choosing the right security action.

Manual key support
: Manually configured keys MUST be able to secure the specified traffic.

Encryption and Authentication Algorithms
: The implementations MUST be conformant to the RFCs that describe mandatory-to-implement algorithms for use with ESP and AH.

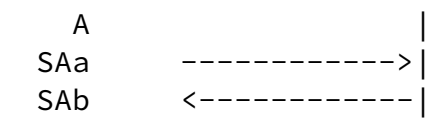
Dynamic IPsec rule configuration

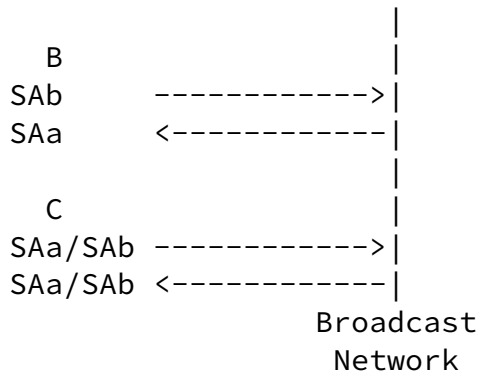
Routing module SHOULD be able to configure, modify and delete IPsec rules on the fly. This is needed mainly for securing virtual links.

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.

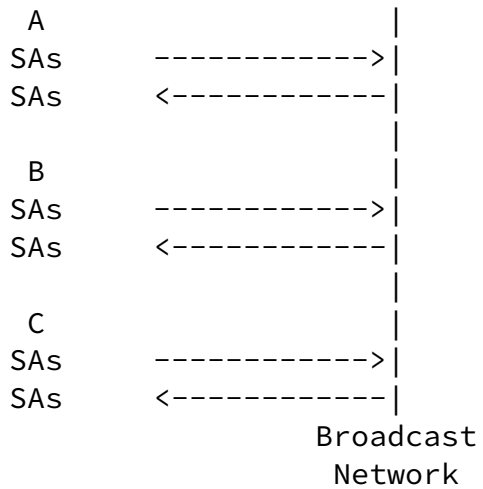
As security associations (SAs) are directional, generally different security associations are used for inbound and outbound processing for providing higher security. The following figure explains that it is not possible to use different security associations for inbound and outbound processing in order 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 neighbor routers on a network/subnet MUST use the same SA and the same SA MUST be used for inbound and outbound processing.

7. SA Granularity and Selectors

The user SHOULD be given a choice to share the same SA among multiple interfaces or using unique SA per interface.

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 is 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 needs to be set up 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.

According to the OSPFv3 RFC [N1], the virtual neighbor's IP address is set to the first prefix with the "LA-bit" set from the list of prefixes in intra-area-prefix-LSAs originated by the virtual neighbor. But when it comes to choosing the source address for the packets that are sent over the virtual link, the RFC simply suggests using one of the router's own site-local or global IPv6 addresses.

In order to install the required security rules for virtual links, the source address also needs to be predictable. So the routers that implement this specification MUST change the way the source and destination addresses are chosen for the packets exchanged over virtual links when the security is enabled on that virtual link.

The first IPv6 address with the "LA-bit" set in the list of prefixes advertised in intra-area-prefix-LSAs in the transit area MUST be used as the source address for packets exchanged over the virtual link. When multiple intra-area-prefix-LSAs are originated they are considered as being concatenated and are ordered by ascending Link State ID.

The first IPv6 address with the "LA-bit" set in the list of prefixes

received in intra-area-prefix-LSAs from the virtual neighbor in the transit area MUST be used as the destination address for packets exchanged over the virtual link. When multiple intra-area-prefix-LSAs are received they are considered as being concatenated and are ordered by ascending Link State ID.

This makes both the source and destination addresses of the packets exchanged over the virtual link, predictable on both the routers for security purposes.

9. Changing Keys

To maintain the security of a link, it may be desirable to change the key values from time to time. The following three-step procedure MAY be provided to rekey the routers on a link without dropping OSPFv3 protocol packets or disrupting the adjacency.

(1) For every router on the link, create an additional inbound SA for the interface being rekeyed using a new SPI and the new key.

(2) For every router on the link, replace the original outbound SA with one using the new SPI and key values. The SA replacement operation should be atomic with respect to sending OSPFv3 packets on the link so that no OSPFv3 packets are sent without authentication/encryption.

(3) For every router on the link, remove the original inbound SA.

Note that all the routers on the link must complete step 1 before any begin step 2. Likewise, all the routers on the link must complete step 2 before any begin step 3.

One way to control the progression from one step to the next is for each router to have a configurable time constant KeyRolloverInterval. After the router begins step 1 on a given link, it waits for this

interval and then moves to step 2. Likewise, after moving to step 2, it waits for this interval and then moves to step 3.

In order to achieve smooth key transition, all the routers on a link should use the same value for KeyRolloverInterval, and should initiate the key rollover process within this time period.

At the end of this procedure, all the routers will have a single inbound and outbound SA for OSPFv3 on the link with the new SPI and key values.

10. 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::/10	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::/10	any	ESP or AH	apply
4	iface	fe80::/10	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 insecure 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 MUST be installed on at least the interfaces that are connected to the transit area for the virtual link. These rules MAY alternatively be installed on all the interfaces. If these rules are not installed on all the interfaces, clear text or malicious OSPFv3 packets with same source and destination addresses as virtual link end point addresses will be delivered to OSPFv3. Though OSPFv3 drops these packets because they were not received on the right interface, OSPFv3 receives some clear text or malicious packets even when the security

is on. Installing these rules on all the interfaces insures that OSPFv3 does not receive these clear text or malicious packets when security is turned on. On the other hand installing these rules on all the interfaces increases the processing overhead on the interfaces where there is no IPsec processing otherwise. The decision of installing these rules on all the interfaces or on just the interfaces that are connected to the transit area is a private decision and doesn't affect the interoperability in any way. So this decision is left to the implementers.

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.

11. 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.

Fields LS age, LS Sequence Number and LS checksum in LSA header are kept intact in OSPFv3. Though these fields do not provide the complete protection, they certainly help 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.

Normative References

N1. Coltun, R., Ferguson, D. and J. Moy, "OSPF for IPv6", RFC 2740, December 1999

N2. Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

N3. Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

N4. Kent, S. and R. Atkinson, "IP Authentication Header (AH)", RFC 2402, November 1998.

N5. Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

Informative References

I1. Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

Acknowledgments

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

We would also like to thank IPsec and OSPF WG people to provide valuable review comments.

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