dhc
Internet-Draft
Intended status: Informational
Expires: April 16, 2011

Ma
CNNIC

October 13, 2010

Extended DHCPv6 for Piggybacking Security Association Configuration
draft-madi-dhc-dhcpv6-psac-00

Abstract

IPSec [RFC2401]is pervasive in many scenarios to build the channel of security mechanism to protect the communication between the host and the local servers, such as DNS recursive name server [RFC1304]. In the public wireless access environment, an extra trust relationship configuration between the roaming host and the local server, manually or by IKE [RFC2409], is indispensible.

DHCP is typically the first protocol executed by a mobile host when it enters a new network, so this document present an extension to DHCPv6 to piggyback the parameters needed for IPSec, avoiding the delay invited by manual configuration of security association or IKE interaction for IPSec.

Table of Contents

1. Introduction 4
2. Terminology 4
3. Requirements and Considerations 5
4. Design Overview 5
5. Extended DHCPv6 Operation 6
5.1. Message and Option Definitions 6
5.1.1. Messages 6
5.1.2. Options 7
5.1.3. Status Codes 12
5.1.4. Transmission and Retransmission Parameters 13
5.2. Message Validation 13
5.2.1. SOLICIT 13
5.2.2. SACONFIGURATION 14
5.2.3. SACONFIGURATION-REPLY 14
5.3. DHCP Server Solicitation 14
5.4. SACONFIGURATION Behavior of DHCP Server 15
5.4.1. Creation of SACONFIGURATION 15
5.4.2. Transmission of SACONFIGURATION 16
5.4.3. Receipt of SACONFIGURATION-REPLY 16
5.5. Target Server Behavior 16
5.5.1. Receipt of SACONFIGURATION Messages 17
5.5.2. Transmission of SACONFIGURATION-REPLY Messages 17
5.6. The extension brings to the DHCP exchange 17
6. Security Considerations 18
7. IANA Considerations 18
8. References 19
8.1. Normative References 19
8.2. Informative References 19

1. Introduction

There are an increasing number of mobile hosts who, roaming across different access domains, want to resort to the shared key based method to gain secrecy and integrity of the data exchange with the local server of the access network, the communication between the DNS stub resolver and the local DNS recursive name sever as an example. IPSec, for instance, is pervasive in many scenarios to build the channel of security mechanism. And IPSec architecture has a security policy database that specifies which traffic is protected and how, which could be established with a manual configuration of security associations or with IKE [RFC5996]. As for the mobile host, its security association with the local server is usually established by IKE, which leads to an extra interaction delay. Even the delay MAY not be taken into consideration, IKE is not necessarily not be supported everywhere.

DHCP allows a computer to be configured automatically, eliminating the need for intervention by a network administrator. For IPv4, DHCPv4 is typically the first protocol executed by a mobile host when it enters a new network. Even in the era of IPv6, according to the point of view of Ralph, DHCP service is typically provided by a centralized service composed of fewer managed components [21], so DHCP server misconfiguration is less likely than delivery of misconfigured Route Advertisements. Since DHCP also takes the responsibility in configuring the IP address of the local server, the security association information between the host and the specific local server, such as SIP server and DNS recursive name server, could be piggybacked via DHCP messages, avoiding the delay invited by manual configuration of security association or IKE interaction for IPSec.

This document describes the extension to DHCP to integrate security association construction course into the DHCP interaction to build the trust relationship between the roaming host and the specific local server of the access network.

2. Terminology

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 [RFC2119].

DHCPv6 terminology is defined in [RFC3315]. Terminology specific to the extension of DHCPv6 can be found below:

Throughout this document, "DHCP" refers to DHCP for IPv6. DHCP terminology is defined in [RFC3315] and IPSec terminology is defined

in [RFC2401]. Terminology specific to the extension of DHCP can be found below:

SA - SA is short for Security Association and defined in IPSec specification [RFC2401].

SPI - SPI is short for Security Parameter Index and defined in IPSec specification [RFC2401].

target server - A local server of the access network, DNS recursive name server for instance, which is to be configured the security association with a specific host, by DHCP. The target server works as a DHCP client listening for DHCP messages on UDP port 546.

requestor - A host that wants to establish security association with a specific local server. The requestor works as a DHCP client requesting the configuration parameters for security association.

SA binding - SA binding is employed by DHCP server to manage the SA information which is indexed by the tuple [requestor's DUID, target server's DUID, SPI].

3. Requirements and Considerations

Although DHCP is being challenged by the SLAAC [RFC4862], yet this document is intended to take the position that DHCP is indispensible and necessary to the network administrative need.

DHCP server and the target server are usually deployed within one same organization and public key schemes are not necessary, trust relationship based on preshared secret could be established between them by administrator's manual configuration to gain secrecy and integrity. Accordingly, the extension in this document takes the position that DHCP service is indispensible and there is secured channel between DHCP server and the target server.

To realize the very function of the extended DHCP, the host in question MUST have the ability to generate asymmetric key pair, the public key of which is used to encrypt the symmetric key to be shared with the target server.

The extension of DHCPv6 SHOULD go with stateful service DHCPv6 provides.

4. Design Overview

The focus of this document is to extend DHCP to piggyback SA information for the entities that want to employ IPSec, providing a

quick configuration for security parameters. It is especially appropriate for processes and devices that already interpret DHCP messages.

With the extended DHCP, the host especially the roaming host is able to build trust relationship with the target server, the service from which is desired to be provided in a security channel. Accordingly, the host called requestor in this document is on the initiative in the course of the SA establishment in SOLICIT message. The DHCP server configured to take the responsibility responds. The requestor SHOULD also present its public key to DHCP server for encrypting the symmetric key as an element of SA, and the DHCP server MUST provide the symmetric key in cipher text together with other parameters of the very SA.

If selected by REQUEST message, the DHCP server will determine which target server will be configured with SA parameters according to the SA establishment request indicated by the requestor in a new defined option. Then the DHCP server sends message to convey the SA to the selected target server and waiting REPLY message to make sure whether the SA parameters have been configured successfully or not. To guarantee the confidentiality of the symmetric key, the access key SHOULD be encrypted by pre-shared key.

Once the DHCP server gets the confirmation of SA configuration from the intended target server, it responds to requestor in REPLY message that includes SA parameter shared between the requestor and the target server whose service is wanted to be secured by the requestor.

If needed, the DHCP serve MAY choose to update a current SA by sending RECONFIG-INIT message to the requestor.

5. Extended DHCPv6 Operation

5.1. Message and Option Definitions

5.1.1. Messages

Extended DHCP for Security Association Configuration specified in this document uses the Client/Server message formats described in [RFC3315], Section 6. Two new message codes are defined:

SACONFIGURATION (TDB by IANA)) - A DHCP server sends a SACONFIGURATION message to a target server to configure the SA parameters that are indicated in an option called OPTION_SA.

SACONFIGURATION-REPLY (TDB by IANA) - A target server sends a REGISTRATION-REPLY message to a DHCP server the SA from which has

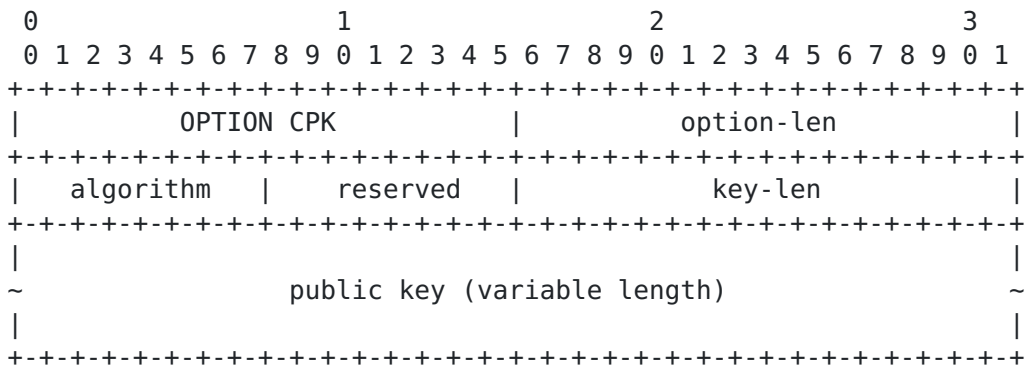
been configured successfully.

5.1.2. Options

5.1.2.1. Client Public Key Option

The Client Public Key Option is used to specify the public key associated with the client that sends the option. The Client Public Key Option SHOULD be bound to the DUID of the client.

The format of the Client Public Key Option is:



option-code OPTION_CPK (TDB by IANA).

option-len 4 + length of public key field.

algorithm the algorithm used to perform the encryption of the shared key.The algorithm are:

RSA(1), defined in [RFC3447].

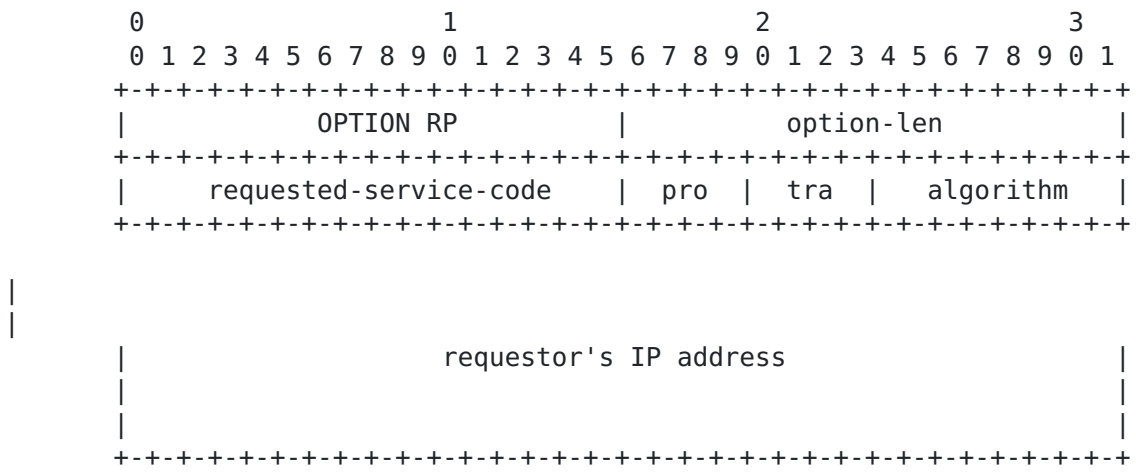
key-len length of the public key.

public key This is a variable-length field containing the public key of the DHCP client.

5.1.2.2. Requestor's Parameters Option

The Requestor's Parameters Option is used to specify the security parameter provided by the requestor, with which the SA will be established. The Requestor's Parameters Option must be encapsulated in the Options field of an SA Request Option.

The format of the Requestor's Parameters is:



option-code OPTION_RP (TDB by IANA).

option-len 20.

requested-service-code To indicate which service is wanted to be secured according to the requestor. The requested-service-code is consistent with the option-code which means if the host wants to use IPSec with a DNS recursive name server, it set the requested-service-code as the option-code for the addresses of DNS recursive name servers.

pro To specify the security protocol IPSec employ.

AH(1).

ESP(2).

tra To specify which traffic, INBOUND or OUTBOUND will be processed from the point of view of the requestor.

INBOUND(1), traffic from the target server to the requestor.

OUTBOUND(2), traffic from the requestor to the target server.

Two-Way(3), all traffic between the requestor and the target server.

algorithm The algorithm employed by IPSec:

HMAC-MD5-96(1), defined in [RFC2403]

HMAC-SHA1-96(2), defined in [RFC2404]

DES(3), defined in [RFC1829]

3DES(4), defined in [RFC1851]

DES-CBC(5), defined in [RFC2405]

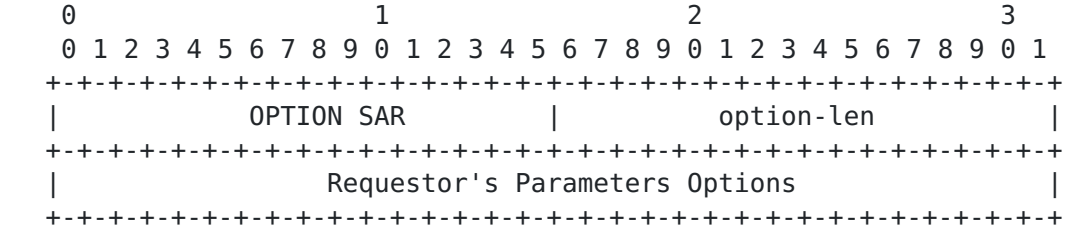
AES(6), defined in [RFC3686]

requestor's IP address To indicate which address of the requestor will be involved in SA. If the address is of all-zero and the requestor's has one or more assigned address from the DHCP server, the DHCP server will select an involved address for the requestor.

5.1.2.3. SA Request Option

The SA Request option is used to encapsulate SA Requestor's Parameters Option(s) to indicate which local service is required to be secured by the requestor and the related parameters.

The format of the SA Request Option is:



option-code OPTION_SAR (TDB by IANA).

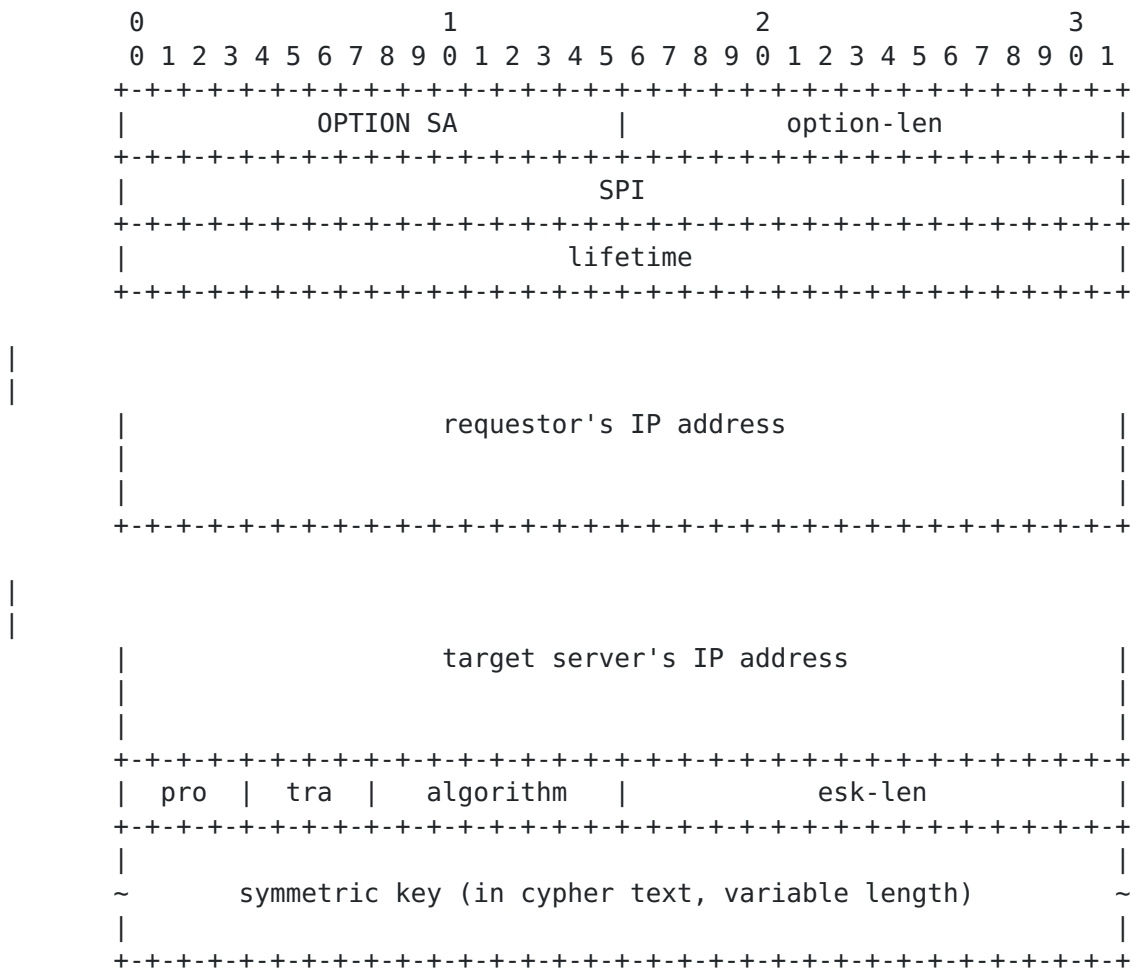
option-len 20 * number of Requestor's Parameters Options.

Requestor's Parameters Options Different Requestor's Parameters Options intended for target servers of different local services.

5.1.2.4. SA Option

The SA Option is used to specify the SA parameters shared between the requestor and a specific target server.

The format of the SA Option is:



option-code OPTION_SA (TDB by IANA).

option-len 44 + length of symmetric key field.

SPI Security Parameter Index created by the DHCP serverand defined in IPSec specification [RFC2401].

lifetime The valid lifetime for the SA, expressed in units of seconds.

requestor's IP address A copy of the requestor's IP address field in the Requestor's Parameters Option included in SOLICIT message or REQUEST message.

target server's IP address To indicate which address of the target server will be involved in SA. The addresses of a specific target server SHOULD be maintained by the DHCP server.

pro A copy of the pro field of Requestor's Parameters Option included in SOLICIT message or REQUEST

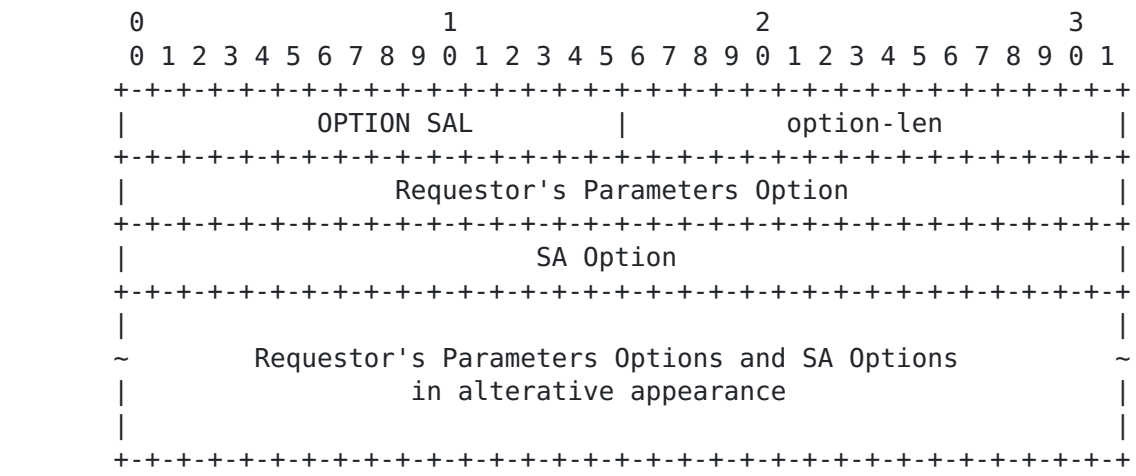
message.

tra	A copy of the tra field of Requestor's Parameters Option included in SOLICIT message or REQUEST message.
algorithm	A copy of the algorithm field of Requestor's Parameters Option included in SOLICIT message or REQUEST message.
esk-len	The length of the encrypted symmetric key.
symmetric key	The encryption of the key shared by the requestor and the target server to use IPSec.

5.1.2.5. SA List Option

The SA List Option is used to contain one or more SA Options in response to the SA request indicated in the SA Request Option included in SOLICIT message from the requestor. In the SA List Option, the Requestor' parameters Option and the SA Option give the alterative appearances to indicate their correlation.

The format of the SA List Option is:



option-code OPTION_SAR (TDB by IANA).

option-len 20 * number of Requestor's Parameters Options + the total length of all SA Options.

Requestor's Parameters Option A copy of Requestor's Parameters Option of the SA Request Option included in SOLICIT message or REQUEST message.

SA Option A SA Option in response to a specific Requestor's Parameters Option included in SOLICIT message or REQUEST message.

5.1.3. Status Codes

Some status codes defined in [RFC5007] are redefined in the messages newly defined in this document, together with the new status codes, they are defined:

NotConfigured (9) - The status code is originally defined in [RFC5007] and redefined with the massage defined in this document. The intended SACONFIGURATION-receiver is not configured to provide secured service based on IPSec.

NotAllowed (10) - The status code is originally defined in [RFC5007] and redefined with the massage defined in this document. The sender of SACONFIGURATION is not the authorized DHCP server to configure SA for IPSec. The authentication of the DHCP server MAY be based on Authentication of DHCP Messages specified in Section 2.3.1 of [RFC3315].

InappropriateAddress (TBD) - The requestor's IP address in the

Requestor's Parameters Option is not a authorised one for the requestor or the target server's IP addressis in the SA Option is not one of the valid IP address of the target server.

UnsupportedAlgorithm (TBD) - The algorithm specified in the Requestor's Parameters Option is not supported by the target server whose service is wanted to be secured.

MalformedSACONFIGURATION (TBD) - The SACONFIGURATION is not valid; for example, the required symmetric key field is missing from the SA Option. This status code is used only in SACONFIGURATION-REPLY message.

FailedSACONFIGURATION (TBD) - The SACONFIGURATION interaction between the DHCP server and the target server is failed for some reasons. This status code is used only in REPLY message from DHCP server to the requestor.

5.1.4. Transmission and Retransmission Parameters

This section presents a table of values used to describe the message transmission behavior for IP address registration.

Parameter	Default	Description
SAC_TIMEOUT	1 sec	Initial SACONFIGURATION timeout
SAC_MAX_RT	10 secs	Max SACONFIGURATION timeout value
SAC_MAX_RC	5	Max SACONFIGURATION retry attempts

5.2. Message Validation

The Message Validation specified in this document follow the basic message validation principles in [RFC3315], Section 15. Requestors, target servers and DHCP servers SHOULD discard any messages that contain options that are not allowed to appear in the received message.

5.2.1. SOLICIT

Extended DHCP for Security Association Configuration with the Local Server in the Access Network mandates the confidentiality of the shared symmetric key. The requestor MUST include Client Public key Option for encrypting the shared symmetric key. DHCP Servers MUST discard any received SOLICIT messages that meet any of the following conditions:

o the message does not include an OPTION_SERVERID option.

5.2.2. SACONFIGURATION

The target server MUST discard any received SACONFIGURATION messages that meet any of the following conditions:

o the message does not include an OPTION_SERVERID option.

o the message includes an OPTION_CLIENTID option but the contents of the OPTION CLIENTID option does not match the target server's identifier.

o the message does not include a SA Option.

DHCP servers, relay agents and the non-requestor DHCP clients MUST discard any received SACONFIGURATION messages.

5.2.3. SACONFIGURATION-REPLY

The target server MUST discard any received SACONFIGURATION-REPLY messages that meet any of the following conditions:

o the message does not include an OPTION_CLIENTID option.

o the message includes an OPTION_SERVERID option but the contents of the OPTION_SERVERID option does not match the server's identifier.

o the message does not include a SA Option.

o the "transaction-id" field in the message does not match the value used in the original message.

Target servers (on the DHCP server port, 546 [RFC3315]), relay agents and DHCP clients MUST discard any received SACONFIGURATION-REPLY messages.

5.3. DHCP Server Solicitation

This section describes how the SA configuration with the target server in the access network will affect DHCP Server Solicitation specified in [RFC3315], Section 17.

Once a host especially a mobile one intends to establish a SA with a local server in the access network to secure one certain service such as DNS recursive resolution service, it will include a SA Request Option together with the Client Public Key Option in its SOLICIT message.

Once informed by SA Request Option included in the SOLICIT message,

the DHCP server will decide whether to provide the service for SA establishment according to its policies configured by the administrator of the access network. If a DHCP server takes the responsibility in managing SA establishment for the requestor and the target server, it responds, via the ADVERTISE message, to the requestor it is able to find a proper IP address for IPSec as the requestor's agent.

On receiving the ADVERTISE messages from several DHCP servers, the requestor selects one according to its local policies and then multicast the REQUEST message including the SA Request Option. Once the selected DHCP server gets the REQUEST message, it decides which IP address will be involved in the intended SA establishment according to the requested-service-code of the Requestor's Parameters Option in the SA Request Option.

Then DHCP server initiates SACONFIGURATION exchange with the target server. Once the SACONFIGURATION has been confirmed from the intended target server, DHCP server sends Reply message to the requestor.

The DHCP server use the SA binding to manage the SA parameters shared between the requestor and the target server. The SA binding is indexed by the tuple [requestor's DUID, target server's DUID, SPI].

The SACONFIGURATION mechanism is not compatible with Rapid-commit mode specified in [RFC3315], Section 17.1.1.

5.4. SACONFIGURATION Behavior of DHCP Server

Once receiving a REQUEST message with SA Request Option, the DHCP server then initiates the SACONFIGURATION exchange with the target server.

This section describes how DHCP Server initiates exchange with a specific target server in SACONFIGURATION.

5.4.1. Creation of SACONFIGURATION

The DHCP server sets the "msg-type" field to SACONFIGURATION. The DHCP server generates a transaction ID and inserts this value in the "transaction-id" field. The DHCP server MUST include an OPTION_ SERVERID option to identify itself to the target server which works as a DHCP client. The DHCP server MUST include a SA Option specified in Section 5.1.2.4.

5.4.2. Transmission of SACONFIGURATION

According to the requested-service-code of the Requestor's Parameters Option in the SA Request Option included in the REQUEST message and the address list of one certain local service, the DHCP server is able to choose an IP address of a proper target server for the requestor to establish SA.

The DHCP server transmits SACONFIGURATION messages according to Section 14 of [RFC3315], using the following parameters:

IRT SAC_TIMEOUT

MRT SAC_MAX_RT

MRC SAC_MAX_RC

MRD 0

If the message exchange fails, the DHCP server takes an action based on the local policy of the access network. Examples of actions the DHCP server might take include:

o Inform the client of the failure with denying offering service.

o Inform the client of the failure while assigning IP address as usual.

5.4.3. Receipt of SACONFIGURATION-REPLY

A successful SACONFIGURATION-REPLY is one without an OPTION_STATUS_CODE option (or an OPTION_STATUS_CODE option with a success code). Then the DHCP server responds to the requestor in the REPLY message with SA List Option to indicate the SA to be established between the requestor and one certain target server.

An unsuccessful SACONFIGURATION-REPLY is one that has an OPTION_STATUS_CODE with an error code. Depending on the status code, the DHCP server may try a different target server (such as for NotAllowed, and NotConfigured), try a different or corrected SACONFIGURATION request (such as for MalformedSACONFIGURATION and FailedRegistraion), or terminate the SACONFIGURATION request.

5.5. Target Server Behavior

A Target Server sends SACONFIGURATION-REPLY messages in response to valid SACONFIGURATION messages it receives to inform the DHCP server that the information conveyed by the SA Option has been configured.

5.5.1. Receipt of SACONFIGURATION Messages

Upon receipt of a valid SACONFIGURATION message, the target server updates the SA database it maintains and returns a SACONFIGURATION-REPLY.

No matter whether the SA establishment has been successfully built, the target server configures itself the SA. Once the lifetime of the SA index by SPI expires, the target server removes this SA.

With SPI field of the SA Option, SAVP decides how to deal with the binding request described in SACONFIGURATION message:

o If the SPI is new to the target server, the target server records the SA parameters included in the SACONFIGURATION message.

o If the SPI has been maintained by the target server, the target server overwrites the SA parameters index by the SPI as an update.

The target server constructs a SACONFIGURATION-REPLY message by setting the "msgtype" field to SACONFIGURATION-REPLY, and copying the transaction ID from the SACONFIGURATION message into the transaction-id field. If the SA intended to be configured is not a proper one, the target server adds the error status code according to Section 5.1.3 and sends the SACONFIGURATION-REPLY to the DHCP server.

If the target server fails to configure SA for some unknown reasons, the target server MAY discard the SACONFIGURATION message or MAY add an OPTION_STATUS_CODE option with the FailedSACONFIGURATION status code and send the SACONFIGURATION-REPLY to the DHCP server.

5.5.2. Transmission of SACONFIGURATION-REPLY Messages

The target server sends the SACONFIGURATION-REPLY message as described in the "Transmission of Reply Messages" section of [RFC3315].

5.6. The extension brings to the DHCP exchange

As in Section 5.1.2, some new defined options MUST be supported for the DHCP server solicitation. And on the receipt of REQUEST message containing the SA Request Option from the requestor, the DHCP server initiates the SA establishment exchange with the intended target server before it assigns IP address and other network parameters for the requestor.

The IP address registration exchange happens every time the DHCP server updates the lease on IP address assigned, which means once the

DHCP server is ready to reply to the RENEW or REBIND message, the IP address registration exchange takes places before sending the these very messages for DHCP client.

6. Security Considerations

The original intention of the extension to DHCP for piggybacked SA configuration makes security consideration a necessity. As mentioned before, the symmetric key to be used for IPSec should be in a confidential form. By the virtue of the Client Public Key Option, the DHCP server is able to use client's public key to encrypt the symmetric key and included it in SA Option. As for the very symmetric key transmission between the DHCP server and the target server, administrator MAY choose to make a key pre-shared between the DHCP server and the target server, or MAY employ the public key scheme for the encryption of the symmetric key shared between the DHCP server and the target server.

7. IANA Considerations

IANA is requested to assign the following new DHCPv6 Message types in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:

SACONFIGURATION

SACONFIGURATION-REPLY

IANA is requested to assign the following new DHCPv6 Option Codes in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:

OPTION_OPTION CPK

OPTION_OPTION RP

OPTION_OPTION SAR

OPTION_OPTION SA

OPTION_OPTION SAL

IANA is requested to assign the following new DHCPv6 Status Codes in the registry maintained in http://www.iana.org/assignments/dhcpv6-parameters:

InappropriateAddress

UnsupportedAlgorithm

MalformedSACONFIGURATION

FailedSACONFIGURATION

8. References

8.1. Normative References

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2403] Madson, C. and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC1829] Karn, P., Metzger, P., and W. Simpson, "The ESP DES-CBC Transform", RFC 1829, August 1995.

[RFC1851] Karn, P., Metzger, P., and W. Simpson, "The ESP Triple DES Transform", RFC 1851, September 1995.

[RFC2405] Madson, C. and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

8.2. Informative References

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

Author's Address

Di Ma
CNNIC
4, South 4th Street,Zhongguancun,
Beijing
China(100085)

Phone: +86 010 58813216
EMail: madi@cnnic.cn