3GPP TSG SA WG3 – S3 #17bis **S3z010018**

April 23 – 24, 2001

Madrid, Spain

Source: Motorola Inc.

Title: NDS architecture for IP-Based protocols

Document for: Discussion/Decision

Agenda item: tbd

Abstract

In this contribution, we propose that for IP native protocols, a centralized inter-domain SA negotiation be re-instated for R5. Furthermore, NDS architecture should not limit the existing options of IPsec modes. In particular, it should support the transport mode to provide end-to-end protection when the IP protocol is allowed.

1. Introduction

In the current TS 33.200 v0.3.2 (see [2]), for native IP based protocols, the security architecture is based on hop-by-hop security. It uses chained tunnels so that only security gateways can directly communicate with other security domains. For network entity NE_A in one security domain to communicate with network entity NE_B in another security domain, each IPsec protected packet has to pass three tunnels to reach its destination, which implies three ESP encryption (authentication)/decryption (verification) procedures. (see Figure 1)

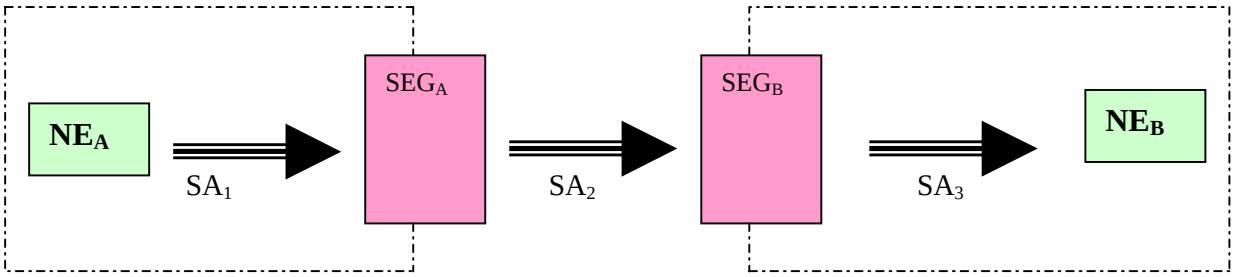

Figure 1. Chained Tunnels

In section 2, we will review the history in SA3 on NDS architecture discussions. From the review, we will see that some of the reasons to eliminate other options do not exist any more. In section 3, we will present an NDS architecture, which will include the current chained-tunnels as one of the options. In section 4, we will further provide the rationale to support this more general architecture.

2. Review of NDS architecture discussions in SA3

SA3 had employed a security architecture called “two tiered” key management before meeting #16. In the “two tiered” key management, each network or security domain has a centralized inter-domain Key Administration Center (KAC). In order to establish a Security Association (SA) between a network entity NE_A in domain A and a network entity NE_B in domain B, KAC_A will negotiate SA with KAC_B by using IKE (see [1]). Then KAC_A and KAC_B will distribute the SA or SAs to NE_A and NE_B. The communications

between NE_A and NE_B will be protected by IPsec. It is very important to notice that under such an architecture, as one of the options, security gateways can also be used to tunnel the packet from one network to another network. This provides flexible options to apply IPsec mode. (see Figure 2)

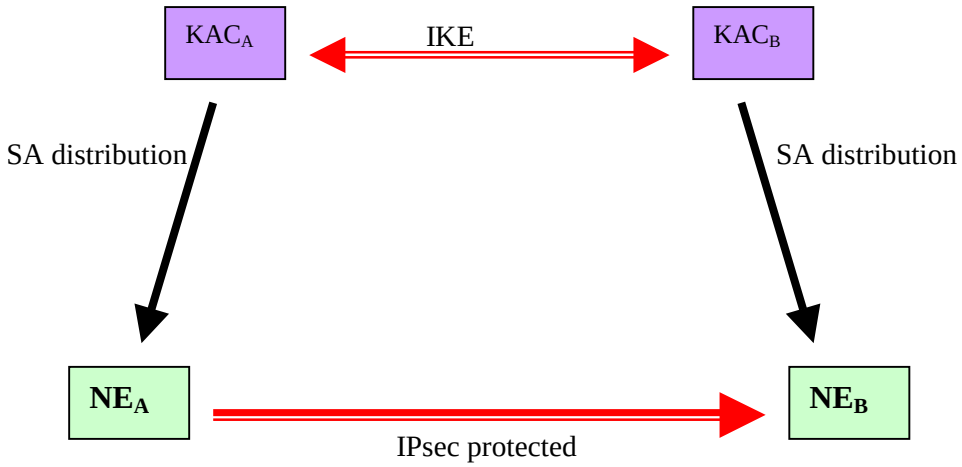

Figure 2: NDS architecture with two tiered key management

At SA3 Network Domain Security ad hoc meeting in Munich last November, Siemens contribution Sz000023 pointed out a "problem" with the aforementioned architecture. With the "problem", IKE seems to be unable to support KACs to negotiate SAs for network entities. The main reason is that by standard IKE negotiation, there is no way the initiating KAC can deliver two IP addresses of NE_A and NE_B to the responding KAC.

In order to make progress on the NDS work item, contribution S3-000670 at SA3 meeting #16 suggested today's NDS architecture as we presented in section 1 to avoid the "problem" discovered by contribution Sz000023.

However, at SA3 meeting #16 (November of 2000, Sophia Antipolis), Siemens' other contribution S3000686 pointed out that by IKE quick mode, the two IP addresses can be delivered to the responding KAC by client negotiation mode. For convenience, we quote IETF RFC 2409 quick mode part as follows:

Quick Mode is defined as follows:

```
    Initiator                                   Responder
   -----------                                  -----------
    HDR*, HASH(1), SA, Ni
      [, KE ] [, IDci, IDcr ]           -->
                                        <--     HDR*, HASH(2), SA, Nr
                                                  [, KE ] [, IDci, IDcr ]
    HDR*, HASH(3)                       -->
```

In the protocol, IDci and IDcr represent the "client initiator" and "client responder" identities. Siemens contribution S3000686 presented this solution to SA3 as follows:

"IKE quick mode supports two optional ID payloads for exchanging additional identities. Updating S3-

z000021 which described the exchange of a single ID payload per peer within IKE quick mode as being supported, it seems to be possible as well that the initiating IKE peer uses both payloads to send two IP addresses. Therefore this simple example should be supported by IKE."

However, Siemens contribution S3000686 pointed out another problem. Specifically, in the case that KACs negotiate SAs for Security Gateways for the purpose of tunneling, it will require that the initiating KAC send additional information besides the IP addresses of SEG_A and SEG_B in order to distinguish between the different tunnels used for different pairs of NEs.

We note that there seems to be no reason to distinguish among multiple tunnels for different NEs. Furthermore, in the current TS 33.200, it is pointed out that "This tunnel (the inter-SEG tunnel) is subsequently used for forwarding secured traffic between security domain A and security domain B." Thus, it appears that only a single tunnel is needed.

Therefore, we have addressed the main problems that seemed to prevent the use of KACs to negotiate SAs for network entities.

3. NDS Architecture

In this contribution, we propose the following NDS architecture (see Figure 3).

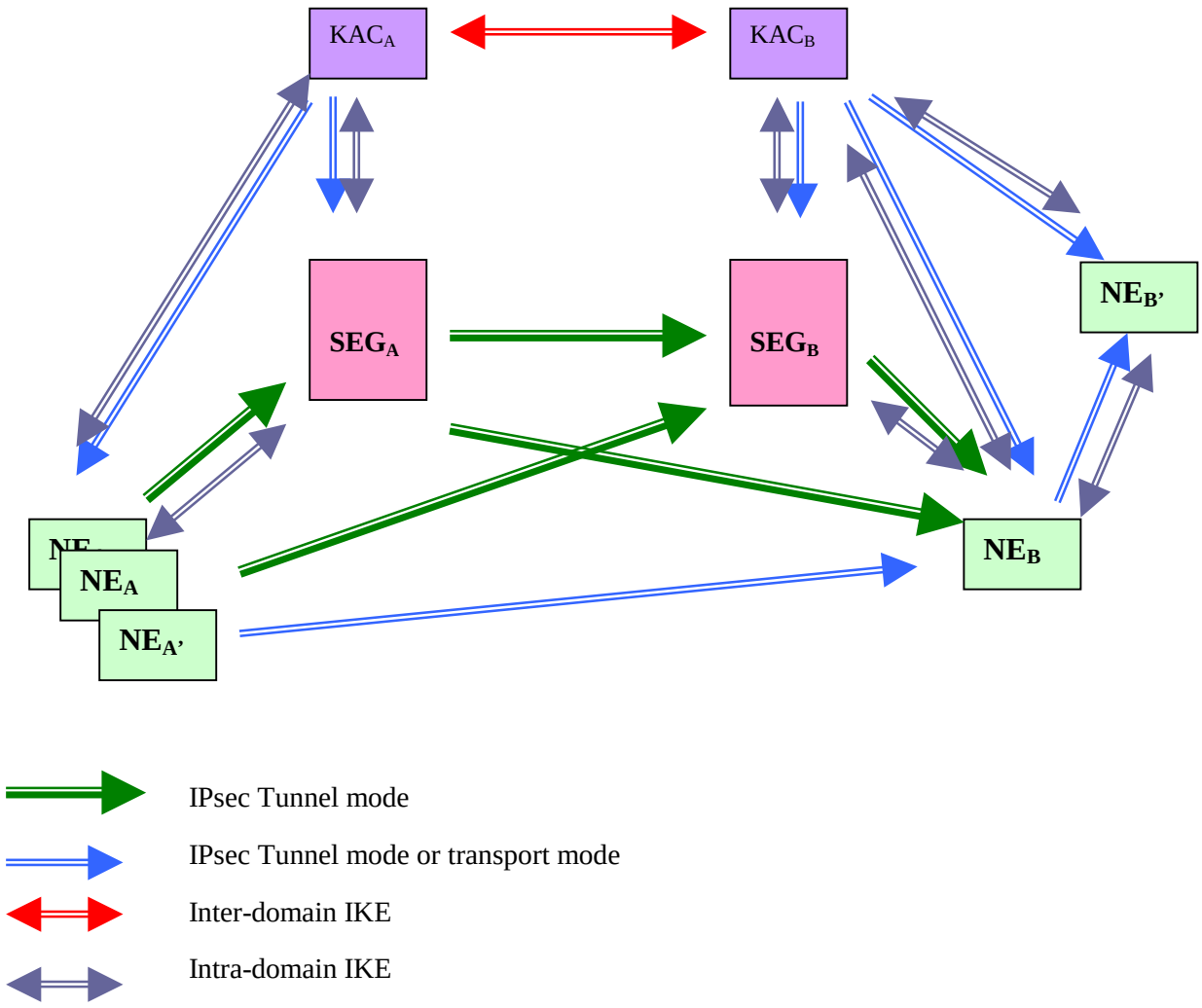

Figure 3. NDS architecture to support different modes with centralized inter-domain SA negotiation

This architecture is very similar with what we had been using before SA3 meeting #16. Therefore, we will not explain each of the interfaces. This architecture employs a centralized inter-domain SA negotiation. The following options should be supported.

1. Transport mode for both intra- and inter-domain signals, if there is no SEG involved and if network protocol is allowed.
2. Tunnel mode, if there is an SEG involved.
3. Different combinations of tunnels.

4. Rationale

4.1 The number of security gateways grows quickly

The current TS 33.200 is based on an assumption that the number of security gateways will remain "low enough" to enable the use of "pre-shared secrets" for entity authentication. However, anticipated expansion of 3G networks will cause the number of security gateways to increase very quickly.

When the number of security gateways experiences even moderate growth, the distribution of "pre-shared secrets" among all the security gateways will become prohibitive. For example, in some heavy populated metropolitan areas, each network operator may assign one security gateway per city to tunnel IP packets for inter-domain control signals. Thus, if there are n cities and k operators, then there are kn^2 "pre-shared secrets" to be distributed.

The dynamic business scenario demands a frequent update of the keys. Whenever a new operator either enters the market or goes out of the business, all the security gateways have to be involved in the key updating process.

4.2 Centralized inter-domain SA negotiation limits the "many-to-many" situation

One of the rationales for the "chained tunnel" architecture is to limit the "many-to-many" situation. However, as we have discussed, the number of security gateways is likely to grow quickly. The real complexity is brought about by the need for a "many-to-many" set of inter-domain pre-shared secrets for IKE phase 1 SA negotiations. The use of centralized inter-domain KACs to negotiate SAs will limit the "many-to-many" pre-shared secrets. This in turn simplifies the architecture to achieve a scalable approach.

Therefore, the use of KACs to negotiate SAs is based on exactly the same idea as for MAPsec in the current TS 33.200.

4.3 The KAC function of negotiating SAs for clients is defined in IKE

In IETF RFC 2409, client mode is defined to negotiate SAs for other network entities. It is said that

> Client negotiation is supported. Client mode is where the negotiating parties are not the endpoints for which security association negotiation is taking place.

Therefore, the KAC function of negotiating SAs has been defined in IETF even though it was not named explicitly as KAC. Therefore, KAC functionality is supported by IETF IKE.

4.4 KACs negotiates SAs for MAPsec

In TS33.200, for SS7 and mixed IP/SS7 based protocols, KACs are employed to negotiate MAPsec SAs for network entities for inter-domain communications.

It seems appropriate to continue this practice for the IP domain.

4.5 Network-wide security policies should be handled by KACs

In TS33.200, security policies are administered by security gateways for the IP domain. However, it seems reasonable that network operators would seek methods whereby they could perform updates to their security policies in a reliable, timely, and uniform manner. For this to be successful, a centralized entity needs to be established for this purpose. We assert that the KAC could act as this centralized entity, and administer network-wide security policies for all NEs and SEGs in its domain.

4.6 Support heterogeneous IP protocols for Release 5

One of the reasons for adopting the chained tunnels is that for IPv4, because of the shortage of available addresses, the UMTS networks domain control plane security architecture has to allow NATs to be present in the networks. The use of NATs inherently prevent end-to-end security.

For Release 5, it is expected that IPv6 and IPv4 may co-exist in a network domain. In some cases, it may be possible to use transport mode from one network entity to another that belong to different security domains. Furthermore, it may also be possible that the chained tunnels only involve one security gateway but not two.

In this case, allowing a flexible combination of chained tunnels along with transport mode will support the co-existence of IPv4 and IPv6 in network domains for Release 5.

5. Conclusions

The preceding discussion leads us to the following conclusions:

- The problems that were believed to prevent the use of KACs to negotiate SAs for network entities can be avoided.
- The function of negotiating SAs for clients has been defined in IETF.
- The use of centralized inter-domain SA negotiation makes the “many-to-many” situation more manageable and scalable.
- The centralized inter-domain SA negotiation allows the KAC to be the unique network policy management unit.

References:

[1] “The Internet Key Exchange”, IETF RFC 2409, November 1998.

[2] “Network Domain Security”, 3G TS 33.200 v0.3.2.