3GPP TSG SA WG3 Security#33 **S3-030394**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.10 WLAN**

Source: **Siemens**

Title: **Profiling of IKEv2 and ESP for NAT traversal**

Document for: **Discussion and Decision**

Abstract

As identified in TS23.234, for both the establishment and the operation of an IPsec secured tunnel between UE and PDG, NAT devices need to be taken into account, in case of private IPv4 addresses in the WLAN access network. In its current version, TS 33.234 does not provide an appropriate discussion of this NAT issue.

This contribution, together with a related CR, provides a brief discussion of the relevant NAT issues as well as a section proposed to be added to TS 33.234.

1. Impact of NAT on 3G-WLAN interworking

In the 3G-WLAN interworking scenario, the UE operates with a set of two IP addresses (common for VPN access):

1. The UE is assigned an IP address in the WLAN access network (either allocated by the WLAN, or by the PLMN).
2. The UE then establishes an IPsec tunnel with the PDG and uses the address described above as outer address, and an IP address received during the tunnel establishment phase as inner IP address within the tunnel.

According to the tunnel requirements given in TS23.234 (v6.0.0), section 5.7.2, both IP addresses (inner and outer) can be IPv4 or IPv6 addresses.

In the IPv4 case, the (outer) address valid in the WLAN access network can be a private address allocated by the WLAN network. In this case, as TS23.234 states in section 6.4.3, a NAT is required between the UE and the VPLMN/HPLMN, i.e., between the UE and the PDG.

Hence, both the IPsec tunnel between UE and PDG and IKEv2 messages for establishment of this IPsec tunnel need to traverse a NAT, in the case of a private IPv4 address in the local WLAN.

Note: If this is either a public IPv4/IPv6 address, or an address that is routable in intermediate networks as well, no NAT is required.

In its current version, TS 33.234 does not provide a discussion of NAT issues. However, NAT needs to be considered for both the IKEv2, and the ESP part of the VPN solution. The appropriate sections for inclusion of this discussion in TS 33.234 are:

- Section 6.5: IKEv2 profile
  This section is required to cover a NAT traversal solution provided by IKEv2.

- Section 6.6: ESP profile
  This section is required to cover a NAT traversal solution for ESP

- Annex A3: IETF
  Informative discussion of the NAT traversal solutions for IKEv2/ESP may be added to this section

2. NAT-IPsec issues and solutions

NAT operation means to apply changes to IP addresses carried in the IP headers of packets traversing the NAT device, and to transport layer port information. This leads to a number of problems with IKE or ESP operation through a NAT, as the two solutions conflict in nature. An analysis of IPsec-NAT compatibility issues is given in [RFC3715].

To enhance the compatibility of IPsec and NAT implementations, the IKEv2 specification offers optional support for NAT traversal, see [IKEv2] section 2.23.

This support includes a mechanism for NAT detection that basically checks for a modification of IP source and destination addresses in the first IKEv2 exchange. If a NAT is discovered between IKEv2 initiator and responder, UDP encapsulation for ESP is negotiated within the IKEv2 SA negotiation for ESP. In addition, IKEv2 mandates that messages received must be accepted with any UDP port, not only UDP port 500. To exclude conflicts with IPsec-aware NATs, UDP encapsulation of IKEv2 and IPsec uses UDP port 4500 instead of 500 to avoid NAT-specific treatment. This means IKEv2 implementations need to listen on both UDP ports.
IKEv2 does not use IP addresses as IKEv2 endpoint identifiers to avoid conflicts with IP addresses carried in the IKEv2 messages.

Furthermore, ESP in tunnel mode can work with NATs (without port translation); however, if NAPT (including port translation) is in place, tunnel mode ESP cannot work through the NAPT. For ESP, [UDP-Enc] specifies the NAT-traversal solution corresponding to the UDP encapsulation that can be negotiated in IKEv2. For ESP tunnel-mode, encapsulation and decapsulation is described in [UDP-Enc].

3. Proposed solution for TS 33.234

As discussed in section 1, NAT traversal for IKEv2 and ESP tunnel mode is required in the case that a UE is provided with a private IPv4 address while roaming to a WLAN network.

It is therefore proposed to support NAT traversal for this scenario as specified for IKEv2 and ESP tunnel mode, and to add appropriate profiling to TS 33.234 sections 6.5 and 6.6. The text to be added is provided by the companion Siemens CR.

Adding the NAT traversal to TS.33.234 creates a dependency on [IKEv2] and [UDP-Enc]. As these specifications are currently classified as work in progress in the IETF, it needs to be verified that 3GPP Release 6 deadlines will be met by the IETF work. This, however, is not considered critical, as for IKEv2 the required specification is already provided by the base IKEv2 protocol, and [UDP-Enc] is expected to proceed in parallel to IKEv2 in the IETF IPsec group.

References

[IKEv2] Kaufman (ed.), March 2004: “Internet Key Exchange (IKEv2) Protocol”, IETF Internet-draft, draft-ietf-ipsec-ikev2-13.txt

[UDP-Enc] Huttunen, Swander, Volpe, DiBurro, Stenberg, Feb. 2004: „UDP Encapsulation of IPsec Packets“, IETF Internet-draft, draft-ietf-ipsec-udp-encaps-08.txt

[RFC3715] Aboba, Dixon, March 2004: “IPsec-Network Address Translation (NAT) Compatibility Requirements”, IETF RFC 3715