3GPP TSG SA WG3 Security — S3#21 S3-010619

27 - 30 November, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#20 **S3-010489**

16-19 Oct, 2001

Sydney, Australia

Source: Nokia

Title: Proposed changes to 33.210 about defining the BG element

Document for: Discussion

Agenda Item:

This contribution proposes clarifications to the text concerning Border Gateway (BG) definition. It is edited with change marks against 33.210 v. 0.6.0.

5.6.2 Interface description

The following interfaces are defined for protection of native IP based protocols:

- **Za-interface (SEG-SEG)**

  The Za-interface covers all secure IP communication between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure tunnel between them. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be established as needed. The tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.

  One SEG can be dedicated to only serve a certain subset of all roaming partners. This will limit the number of SAs and tunnels that need to be maintained. ~~The number of SEGs within a network will normally be limited and should normally not be larger than the numer of BGs in the network.~~ The BG functionality is a subset of the SEG functionality. Thus, BG will be expanded with additional security functions whenever SEG is introduced to the security domain.

  All security domains shall operate the Za-interface.

[Editor's note: The intention here is to make Za mandatory provided that an operator has decided to implement NDS/IP. This I believe captures the current agreement in S3.]

- **Zb-interface (NE-SEG)**

  The Zb-interface is located between NEs and a SEG from the same security domain. The NE and the SEG are able to establish and maintain ESP-tunnels between them. Whether the tunnel is established when needed or a priori is for the security domain operator to decide. The tunnel is subsequently used for exchange of secured traffic between the NE and the SEG.

Normally ESP shall be used with both encryption and authentication/integrity, but an authentication/integrity only mode is allowed. All control plane traffic towards external destinations shall be routed via a SEG.

It is for the security domain operator to decide whether to implement Zb-interfaces or not.

- **Zc-interface (NE-NE)**

  The Zc-interface is located between NEs from the same security domain. The NEs are able to establish and maintain ESP-tunnels between them. Whether the tunnel is established when needed or a priori is for the security domain operator to decide. The tunnel is subsequently used for exchange of secured traffic between the NEs.

  Normally ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The ESP tunnel shall be used for all control plane traffic that needs security protection.

  It is for the security domain operator to decide whether to implement Zc-interfaces or not.

NOTE-1: The security policy established over the Za-interface is subject to roaming agreements. This differs from the security policy enforced over the Zb- and the Zc-interface, which is unilaterally decided by the security domain operator.

NOTE-2: There is normally no NE-NE interface for NEs belonging to separate security domains. This is because it is important to have a clear separation between the security domains. This is particularly relevant when different security policies are employed whithin the security domain and towards external destinations.

The restriction not to allow secure inter-domain NE-NE communication does not preclude a single physical entity to contain both NE and SEG functionality. A combined NE/SEG entity need not support an external Zb-interface provided that the entity itself is physically secured. The exact SEG functionality required to allow for secure inter-domain NE←→NE communication will be subject to the actual security policies being employed. Thus, it will be possible for roaming partners to have secure direct NE←→NE communication within the framwork of NDS/IP.