3GPP TSG SA WG3 Security — S3#18 **S3-0100202**

21-24 May, 2001

Phoenix, Arizona

Source: Nokia

Title: Proposed changes to 33.200 about firewalls

Document for: Discussion/decision

Agenda Item: tbd

This is a re-submission of the document S3z010028 which was not handled in Madrid meeting. That is why it is against the old version of the specification. Still the proposed changes are valid.

This contribution proposes enhancements on text about firewalls. It is edited with change markers against 33.200 v. 0.3.5.

C.2 Filtering routers and firewalls

In order to strengthen the security for IP based networks, border gateways and access routers would normally use packet filtering strategies to prevent certain types of traffic to pass in or out of the network. Similarly, firewalls are used as an additional measure to prevent certain types of accesses towards the network.

The rationale behind the application of packet filters and firewalls should be found in the security policy of the network operator. Preferably, the security policy should be an integral part of the network management strategy as a whole.

While network operators are strongly encouraged to use filtering routers and firewalls, the usage, implementation and security policies associated with these are considered outside the scope of this specification.

Simple filtering may be needed before the Security Gateway (SEG) functionality. IPSec ESP in tunnel mode should be accepted. All traffic coming from non-operator addresses must be rejected.