**3GPP TSG SA WG3 (Security) –S3 #31** **S3-030763**
**18-21 November 2003**
**Munich, Germany**

| | |
|---|---|
| **Agenda Item:** | **6.10 – WLAN Interworking** |
| **Source:** | **Huawei Technologies Co., Ltd.** |
| **Title:** | **Comments on S3-030741: Security Considerations on resolution gateways** |
| **Document for:** | **Discussion and Decision** |

# 1. Introduction

This contribution provides comments on the S3-030741, an analysis of the security properties of SA2 proposed architecture and some alternatives/options within it.

Two of the sections are addressed and commented: section 5 and 6 of S3-030741

# 2. Functional decomposition of PDG

In the liaison from SA2 (S3-03xxxx, S2-033813), the possibility of separating the PDG into two components is suggested. The two components would be:

- The 'W-APN Resolution Gateway', which processes tunnel establishment messages, and
- The 'Packet Data Gateway', which processes tunnel data messages

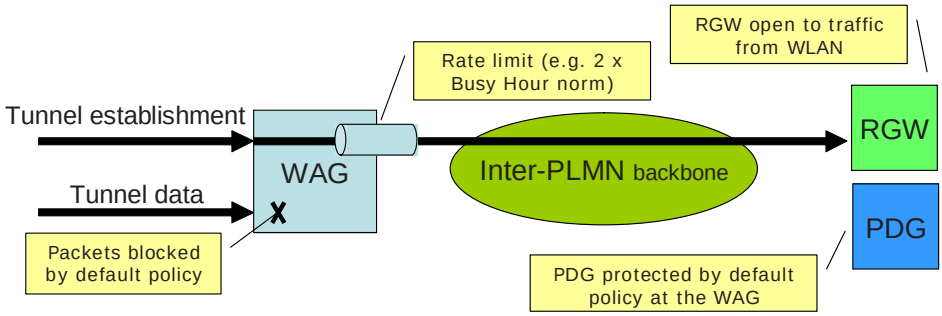
**[Comments 2.1:**

**the W-APN Resolution Gateway', mainly processes service authentication, authorization& W-APN resolution, the processing of initial tunnel establishment messages is to optimize the signal interactions, the further tunnel maintenance messages do not necessarily go through the RGW anymore, can just directly to go between PDG and UE, or be "in-band" in the tunnelled traffic.**

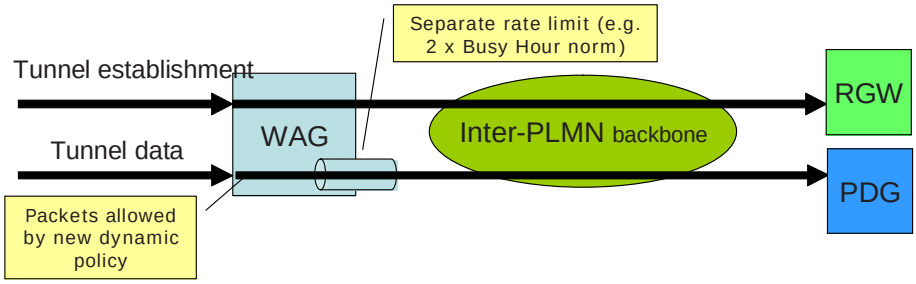
**]**

The consequence of this separation is illustrated below:

**Before/during tunnel establishment**




**After tunnel establishment**




In summary, the PDG is protected from 'unauthorised' traffic from the WLAN until after Tunnel Establishment. It has been suggested that this results in less stringent robustness requirements on the PDG and is therefore a security advantage.

Additionally, the address of the PDG is not supplied to the user until they have been authenticated and authorised, which is seen by some as an advantage (but see comments in (3) above).

**[Comments 2.2:**

**This summary should be formulating this way to be more objective:**

**1. The PDG is protected from 'unauthorised' traffic from the WLAN until after Tunnel Establishment. This improves the security situation of PDG, and results in less stringent robustness requirements on the PDG.**

**2. The configuration of PDGs, seems here be simply understand as only address of one or several PDG, this is not true, it is the whole information of the arrangement that the services are deployed to PDGs and the address of the PDGs, it is taken as confidential business information by some operators, should not expose to public DNS which can be query by any user from any device, mobile or fixed line, internet.**

**]**

# 3. Comments on the proposal

We make the following comments on the proposal outlined above and in the SA2 liaison:

- Tunnel data packets will be addressed to a different Destination Address from Tunnel Establishment packets. As a result, they may appear to come from a different Source Address due to presence of a NAPT. Any filters for Tunnel Data cannot therefore be based on Source Address, greatly simplifying the task of spoofing Tunnel Data packets for any attacker.

**[ Comments 3.1:**

**This is not valid. After the UE is authorized and tunnel is established, the RGW do not need to involve, the UE directly communicates with PDG. The filters of cause can base on the source address. The filter is not applied base automatically base on the establishment flow to decide the source and destination, but applied base on the police application request from PDG or AAA server, after the UE is authorized and tunnel is allocated.**

**So, nothing is compromised on this point.. ]**

- The proposal represents a departure from the operation of standard VPN concentrators, which might be expected to be adapted for the PDG function – it therefore increases the expected costs of PDGs. In fact, this seems the main concern with the solution proposed by SA2.

**[Comments 3.2:**

**This is valid, if the tunnel establishment have to be broker by RGW, we need evaluate the efforts for current tunnel protocol to support tunnel broker**

**]**

The most economical solution from an implementation point of view may in fact be to set up two tunnels, one between UE and RGW and one between UE and PDG. But this would clearly be undesirable from a performance point of view. There may also be interoperability problems if tunnel re-direction solution was allowed to co-exist with the two-tunnel solution as the UE would have to know which solution to apply.

**[ Comments 3.3:**

**This is not valid. Why we need two tunnels?**

**If the RGW need to broke the tunnel after it authenticated and authorized the UE to a PDG, it only broke the initial tunnel establishment messages, after tunnel is established, it do not need to involve anymore.**

**Even if the tunnel establishment can not be broke by the RGW, two tunnels are not necessary, only two interactions may be necessary:**

**1. UE contact RGW for the authentication authorization&PDG resolution, it can get a TID as specified by the GBA mechanism also PDG address can be sent to UE as a authorization result.**

**2. Then, with the PDG address (and TID) it contact PDG for service, establish a tunnel.**

**]**

- The proposal relies on separating the physical resources which deal with the 'unauthenticated' tunnel establishment messaging from that which deals with tunnel data. The objective is that overload of the former will not affect the operation of the latter. However, such segregation of resources is possible within a single piece of equipment as an implementation choice.

**[Comments 3.4:**

**But then you need all PDG to be enhanced, we agree some of PDG can combine with RGW but we don't think all PDG should do that. Additionally, this comments seems out scope of SA3,**

**If we imagine PDG can be enhanced to handle any kind of attack without help from other entity, then there is no security problem with any architecture. However, we have to acknowledge the RGW architecture can mitigate the security threat to PDGs, only RGW (serves many PDGs) need to be enhanced to handle one kind of attacks. Thus improve the whole network security management.**

**]**

- The proposal suggests that a single RGW may serve many PDGs. However, such a RGW then becomes a single point of failure

**[Comments 3.5**

**This is not true, the RGW only involve in the authentication authorization& WAPN resolution, and initial tunnel establishment messages (if tunnel establish broke is possible), does not involve in the further tunnel data traffics and interaction between UE and PDG.**

**Furthermore, with this logic, is AAA server a single point of failure? Do you want one AAA should serve only one PDG, or combine AAA into PDG?**

**]**

- The rate limit applied at the WAG for Tunnel Data traffic is expected to be much higher than that applied to Tunnel Establishment packets. It is not clear that the relatively low volume of tunnel establishment packets is something that the PDG needs to be 'protected' from.

**[Comments 3.6**

**For the first sentence: If all of the users are legal, this is true; but when there is attack crisis, this is not true. We are talking about the security, the case of attack crisis, the traffic of attacking can be much higher than any of normal traffic , it depend on what attack is used. Lets analysis the effects of different attack:**

**1. Spoofed tunnel data attack:**

**The PDG can be protected to be accessed by the valid tunnel data, by the policy base on the tunnel id and destination address and/or source address. If attack is from spoofed tunnel id and then Such spoofed packets would be quickly detected at the PDG and the Tunnel aborted as a result. This only constitutes a DoS attack against the legitimate owner of the aborted tunnel.**

**PDG can quickly detect a data is forgery, because it have the keys share with UE, and do not need to check all the data, but some header security parameters, then it cost very limited time and resource.**

**2. Tunnel establishment attack: much danger than the tunnel data attack:**

**When process with a tunnel establishment it have to interact with AAA for authentication and authorization, then AAA may need to contact with HSS for new vectors, the AAA need to derive keys, interact with the UE for authentication, the PDG have to save the request and wait the process, attack requests then consume lot of its resource.**

**Additionally, attackers do not need bother to spoof authorized tunnel header parameters—it may not be so easy to spoof and construct a forgery data.**

**]**

- The proposal requires the parameters of an IPsec security association, including the keys derived during tunnel establishment, to be passed from RGW to PDG, which although possible, may have security implications which are not usually considered in the design of tunnel establishment protocols.
- It is not clear what the protocol for the transport of security association parameters should be.
- Furthermore, the security association transferred from the RGW to PDG would have to be "patched" by replacing the RGW's IP address with that of the PDG. Consideration would also have to be given to the SPIs. In order to ensure uniqueness of the SPIs at each PDG, the RGW would have to maintain SPI state across all PDGs. It is unclear how this could be achieved as the RGW would not be notified by the PDG about the deletion of an IPsec tunnel. If the PDG patched the SPI it is not clear how the new SPI could be communicated to the UE.

**[Comments 3.7:**

**The above 3 comments are not valid, they addressed only one possible implementation, is valid only to one of the interaction options among the RGW, PDG and AAA server. As show in ANNEX. Figure 1.**

**With annex1.2 (figure2) the RGW do not need to be involved. Only act as a transfer proxy, between the UE and PDG.**

**So these are not valid comments against RGW.**

**]**

- The fact that the PDG address is not supplied to the user until after authentication/authorisation is a minor advantage, since it does not affect the vulnerability of the device, it just places an additional (small) hurdle in the way of an attacker

**[Comments 3.8:**

**This is not the real advantages of RGW combine tunnel establishment, the essential security advantages are:**

**1. Even the UE have the PDG address, it can not contact the PDG, before it is authenticated and authorized to do so. Only authorized tunnelled data is allow to reach PDG.**

**2. (1)Avoid the sequence problem addressed by GBA system, which maybe a potential security problem with the UE DNS client based APN resolution in TS23.234( ANNEX E, A model in which users obtain a PDG address through DNS and establish a tunnel with this PDG using standard IP VPN procedures). (2)Ease the security maintains of whole architecture, not need to deal with all PDGs for some kind of attacks.**

**3. enables the control of service applicator source: keep the network configuration confidential in reasonable extent: the UE can only know what it is authorized to know;**

**If the UE is not subscribed several services he can not know where the services are provided. if it is open to public DNS, then, even the UE did not authorized to know some information, it can, so it can easily get the whole configure information; Moreover, it is also possible, any kind of internet user also can know it from public internet, just through several public DNS queries.**

**Note: it is also acknowledged in SA2 RGW architecture have the advantage of WAPN resolution: enable diff-serve strategy, AAA can allocate different PDG to a same service request from different user (e.g. prepaid user vs. VIP user). The DNS query based mechanism can not do this.**

**A main issue in point is supporting of tunnel broker with proper tunnel protocol. It will be helpful if SA3 can provide some guidance, if not out scope of SA3.**

**RGW without tunnel establishment function:**

**Even If the tunnel broker can not be realized or too expensive to be realize, to separate the service authentication, authorization&APN resolution to RGW; PDG deal with the tunnel establishment also have the security advantage:**

**1.since the UE is authenticated and authored by the RGW+AAA, the PDG can detect the validity of the tunnel establishment request quickly with the TID as specified in GBA (not need to interact with AAA, then AAA interact with HSS for vectors, AAA derive keys), then of cause mitigates the Dos attack effects to PDG.**

**2. Same with second advantage of above mechanism ease the security management of the whole architecture.**

**3. Same with third advantage of above mechanism: enables the control of service applicator source: keep the network configuration confidential in reasonable extent**

**]**

**[Comments 3.9: For conclusion:**

**Based on the above considerations, we conclude that the proposal to separate the RGW and PDG has obvious security advantages:**

1. **mitigates the DoS attacks threat to PDG**
2. **In line with the SA3 GBA, have the advantages of separating service authentication and authorization with service data tunnel traffics interaction.**
3. **enables the control of service applicator source: keep the network configuration confidential in reasonable extent**

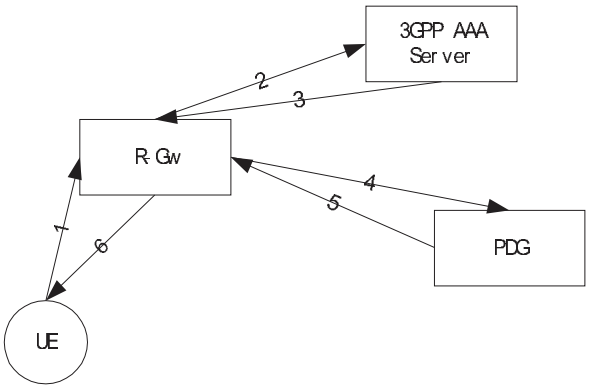
**For the combine of tunnel establishment in RGW, the first advantage is stronger, but seems need develop broker support for the current tunnel protocols, we agree that this advantages need to be evaluated with the additional cost and complexity introduced. . In particular, SA3 need help consider the availability and possibility of solutions for a separation of tunnel establishment protocol endpoint and tunnel endpoint.**

**SA3 should encourage separating at least service authentication authorization from PDG to keep the architecture in line with GBA.**

**]**

# ANNEX for comments 3.7 : POSSIBLE RGW interaction procedures

## 1.1. R-Gw transfers the derived keys for PDG:




1. Upon received a tunnel establishment request from the UE, the W-APN Resolution Gateway a service authorization request to the 3GPP AAA Server, including the requested W-APN and user identity from the tunnel establishment request. Additional exchanges between the WLAN UE and the 3GPP AAA Server (via the W-APN Resolution Gateway) may be required to complete authentication of the user.

2. The 3GPP AAA Server authorizes the service to the WLAN UE and a PDG to serve the UE for this service

3. The 3GPP AAA Server respond to the RGw, including the authorized PDG address and the related security information (e.g. derived key materials) to the PDG.

4. The W-APN Resolution Gateway then includes the necessary information requests allocation of the necessary tunnel resources at the PDG (e.g. SPI or port number allocation).

5. The PDG allocate the tunnel resources and respond to the W-APN Resolution Gateway.

6. The W-APN resolution Gateway responses to the WLAN UE, including the PDG address and tunnel attributes, and necessary security parameters to the WLAN UE

## 1.2. R-Gw do not transfer the derived key for PDG

1. Upon received a tunnel establishment request from the UE, the W-APN Resolution Gateway a service authorization request to the 3GPP AAA Server, including the requested W-APN and user identity from

the tunnel establishment request. Additional exchanges between the WLAN UE and the 3GPP AAA Server (via the W-APN Resolution Gateway) may be required to complete authentication of the user.

2. The 3GPP AAA Server authorizes the service to the WLAN UE and a PDG to serve the UE for this service

3'. The 3GPP AAA Server send message to authorized PDG, to request allocation of the necessary tunnel resources at the PDG (e.g. SPI or port number allocation).

4'. The PDG allocate the tunnel resources and respond to the 3GPP AAA Server.

5'. The 3GPP AAA Server respond to the W-APN Resolution Gateway, with the PDG address, tunnel and security parameters for the UE..

6. The W-APN resolution Gateway forward the response to the WLAN UE, including the PDG address and tunnel attributes, and necessary security parameters to the WLAN UE