# (U//FOUO) Net Defense from Encrypted Communications

February 2012

# Increment 3 Requirement

SYSREQ10322.2
(S//REL) TURMOIL shall reinject decrypted IP traffic into BLUESNORT for malicious network activity detection.

# Three-Feather Solution

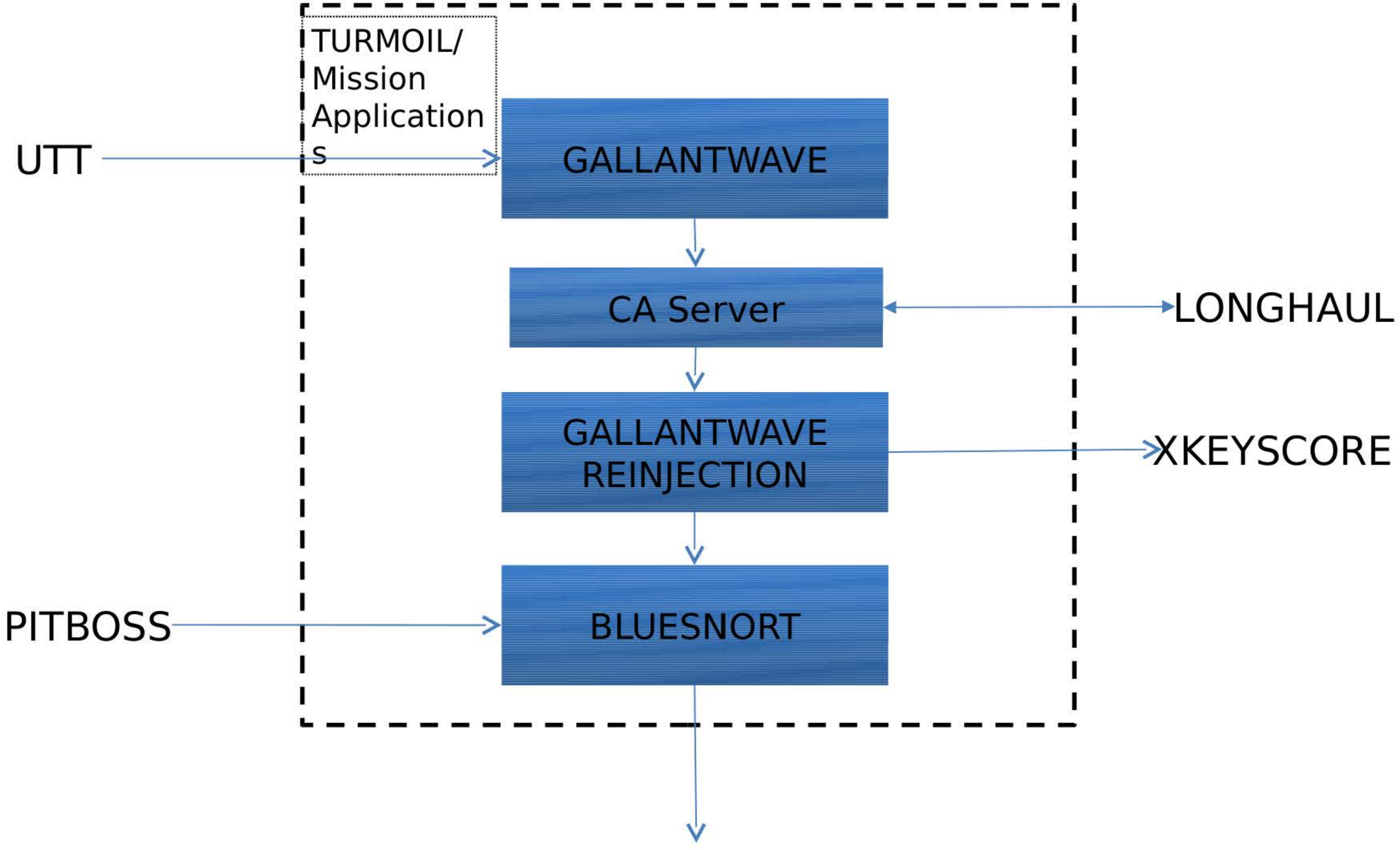
1. *GALLANTWAVE application*
   - *Same module supports NetDef and SIGINT*
   - *Supports dynamic update of targeting via UTT*
   - *Supports static target updates*

2. *GALLANTWAVE Reinjection application*
   - *Same module supports NetDef and SIGINT*
   - *Supports re-injection of decrypt into TURMOIL for detection by BLUESNORT*

3. *BLUESNORT in Stage 1 Prime application*
   - *Emits events off decrypted, re-packetized, reinjected data*

# HIGH Level Data Flow

## Net Defense and SIGINT sites



TIPS (Bluesnort Events)

# Status

- Running on MHS DEV ESO T5 and T22
- Transform, Reinjection, Signature Hits confirmed
- Signatures need further development to produce true hits vs. false positives
- NTOC POC reviewing XKS hits to generate new signatures.

# Issues/Risks

1. *CA Servers at Net Defense Sites*
   a) *ITx Connectivity to LONGHAUL*
   b) *NTOC requires stand-up of separate dev and live ITx fabric*
      i. *- H/W funding may be needed*
      ii. *- Need paperwork for update to firewall – submission expected by 25 Feb*
   c) *Expected completion was 29 Feb; now delayed to TBD*
   d) *SSH connectivity*
   e) *Short term: via BLUEBOX CA Servers at Pentagon - done*
   f) *Longer term: via deployment of servers within the NTOC enclave that connect to CA Servers in the field*
2. *GALLANTWAVE Targeting Challenges*
   a) *MAILORDER/Ni-FI not yet available*
   b) *Mitigation:  Manually load static targeting files*

# CA Capabilities Planned for NCC-3 Test Events

| Capability | DT/OA 2 (June 2012) | | DT/OA 3 (June 2013 ) | |
|---|---|---|---|---|
| | Defensive Sensor | SIGINT Sensor | Defensive Sensor | SIGINT Sensor |
| CA Reinjection | No | DGO | TTENT | DGO |

# Near-term Schedule

| Capability | Date |
|---|---|
| GW-R Gate 2 | Done (15 Feb) |
| GW-R Gate 3 | Done (29 Feb) |
| GW-R Gate 5 | 31 Mar |
| GW-R Deploy to U sites | May |
| ITx Dev Fabric at NetDef sites | 29 Feb + |
| CA Server ssh connectivity | Done via Bluebox |
| Initial Live Dev Test TURTLEZOO | ~May |
| GW-R Core 4.0 | May |
| GW Core 4.0 | May |
| ITx Live Fabric | TBD |

# Players

[redacted]

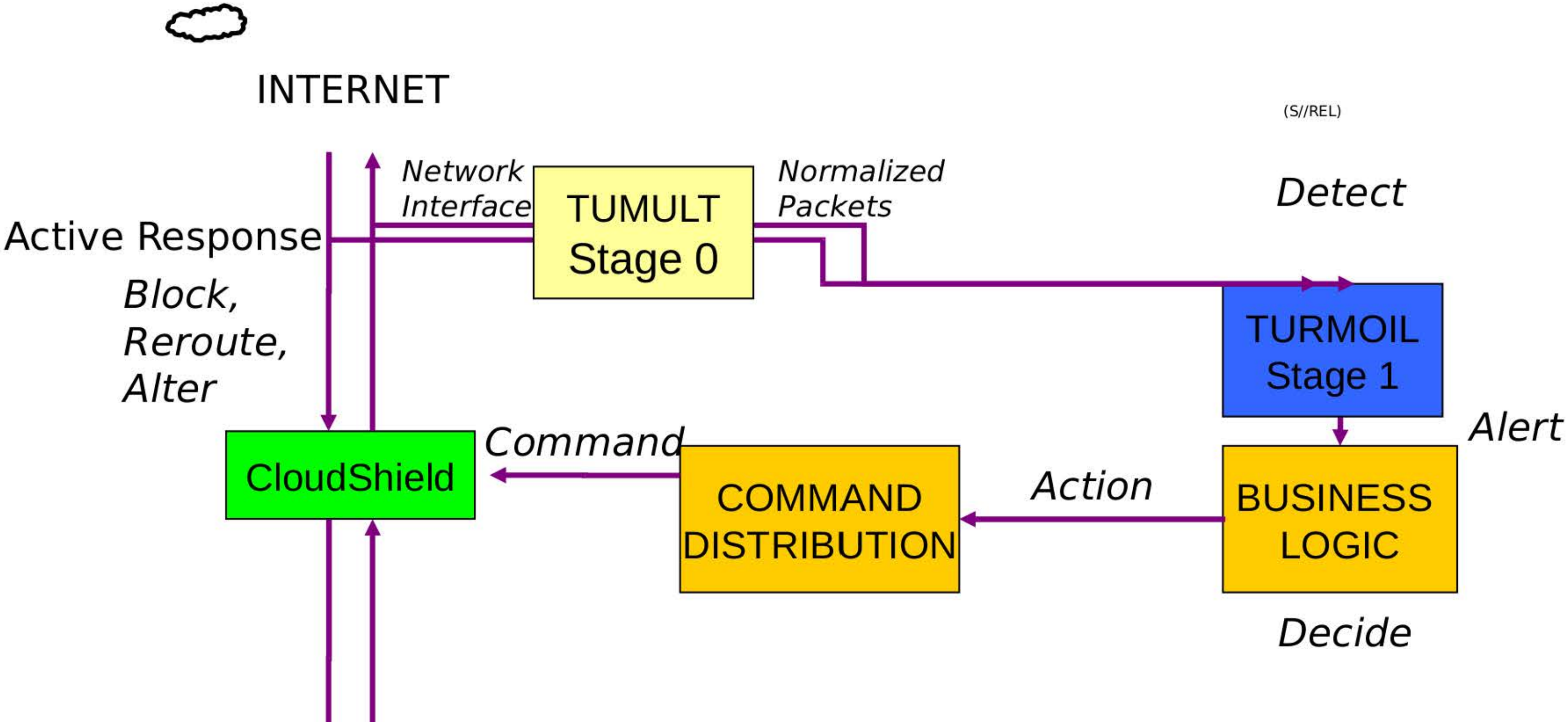
# BACKUP SLIDES

# CCA Capabilities Planned for NCC-3 Test Events

| Capability | DT/OA 2 (June 2012) | | DT/OA 3 (June 2013) | |
|---|---|---|---|---|
| | Defensive Sensor | SIGINT Sensor | Defensive Sensor | SIGINT Sensor |
| NETFLOW | Full Netflow | Pretty Good Netflow | Full Netflow | Full Netflow |
| BLUESNORT (updates) | Yes | No | Yes | Yes |
| FULL SNORT | Yes | No (Core 4) | Yes | Yes |
| POPQUIZ | No | No | Yes | Yes |
| Performance Testing | Yes | No | Yes | Yes |
| Wireless reinjection | N/A | Yes | N/A | Yes |
| CA Reinjection | No | Yes | Yes | Yes |
| Cyber Tasking | Yes | Partial | Yes | Partial |
| Updated Cloudshield Interface | Partial | N/A | Yes | Yes |
| Metrics and Monitoring | Yes | No | Yes | Yes |

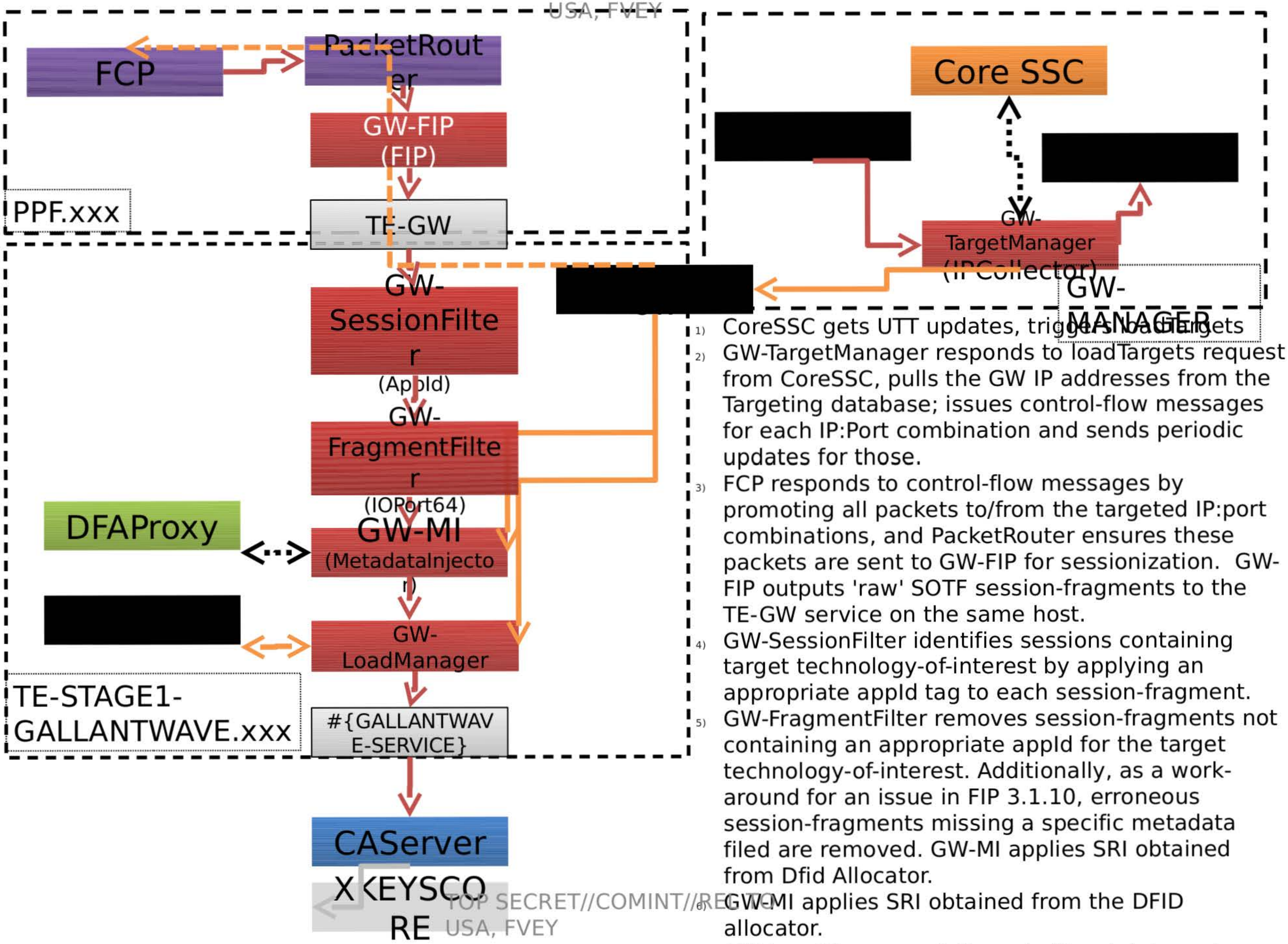
🟧 *Orange items are being revisited. Requirements without explicit TML Core 4 dependency need mission documentation to justify not being covered in DT/OA 2.*

# (S//REL) Dynamic Defense Logical Diagram



Legend:

| | | | |
|---|---|---|---|
| TUMULT<br>(T113) | TURMOIL<br>(T112) | TUTELAGE<br>(T111) | NTOC<br>(VSPO) |



[redacted]

[redacted]

[redacted]

[redacted]

1) CoreSSC gets UTT updates, triggers loadTargets

2) GW-TargetManager responds to loadTargets request from CoreSSC, pulls the GW IP addresses from the Targeting database; issues control-flow messages for each IP:Port combination and sends periodic updates for those.

3) FCP responds to control-flow messages by promoting all packets to/from the targeted IP:port combinations, and PacketRouter ensures these packets are sent to GW-FIP for sessionization. GW-FIP outputs 'raw' SOTF session-fragments to the TE-GW service on the same host.

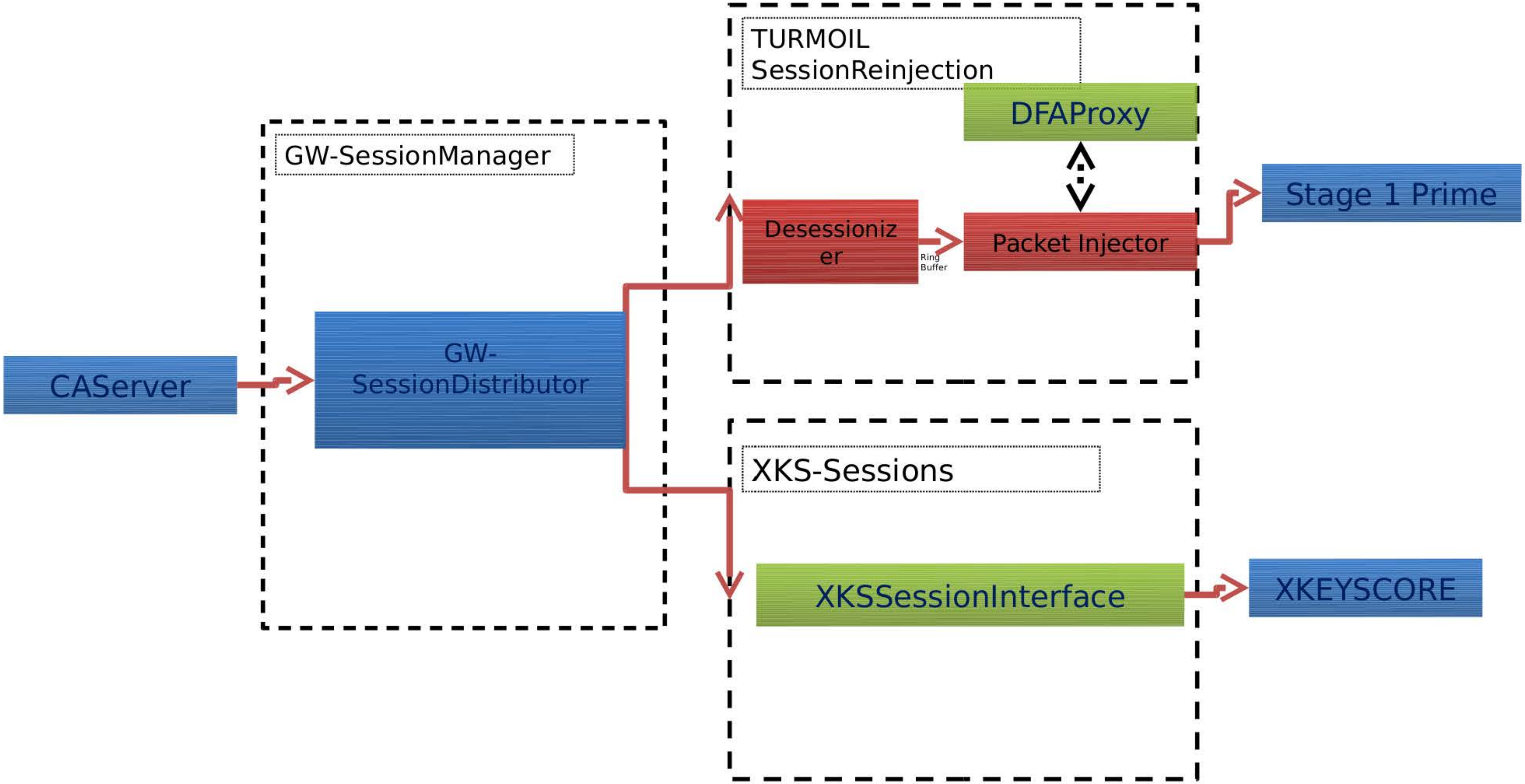
4) GW-SessionFilter identifies sessions containing target technology-of-interest by applying an appropriate appId tag to each session-fragment.

5) GW-FragmentFilter removes session-fragments not containing an appropriate appId for the target technology-of-interest. Additionally, as a work-around for an issue in FIP 3.1.10, erroneous session-fragments missing a specific metadata filed are removed. GW-MI applies SRI obtained from Dfid Allocator.

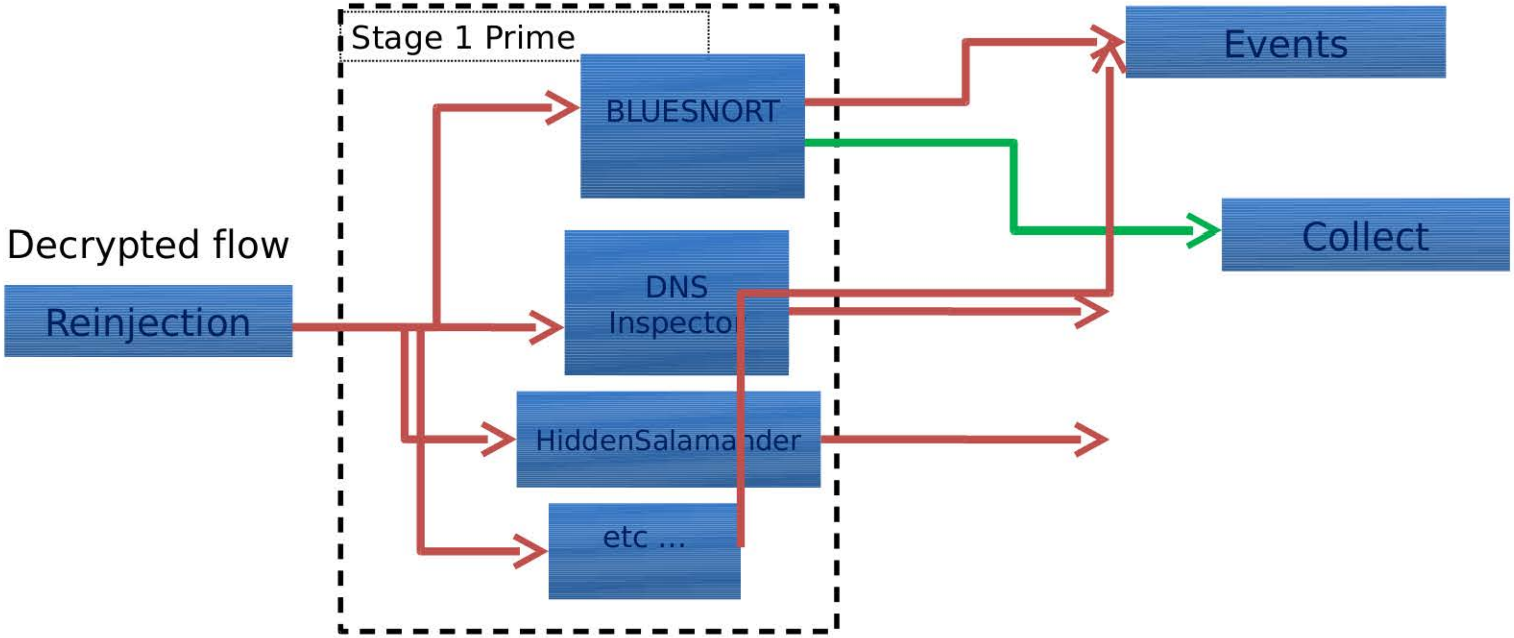
6) GW-MI applies SRI obtained from the DFID allocator.

GW-LoadManager delivers buffered data, upto a

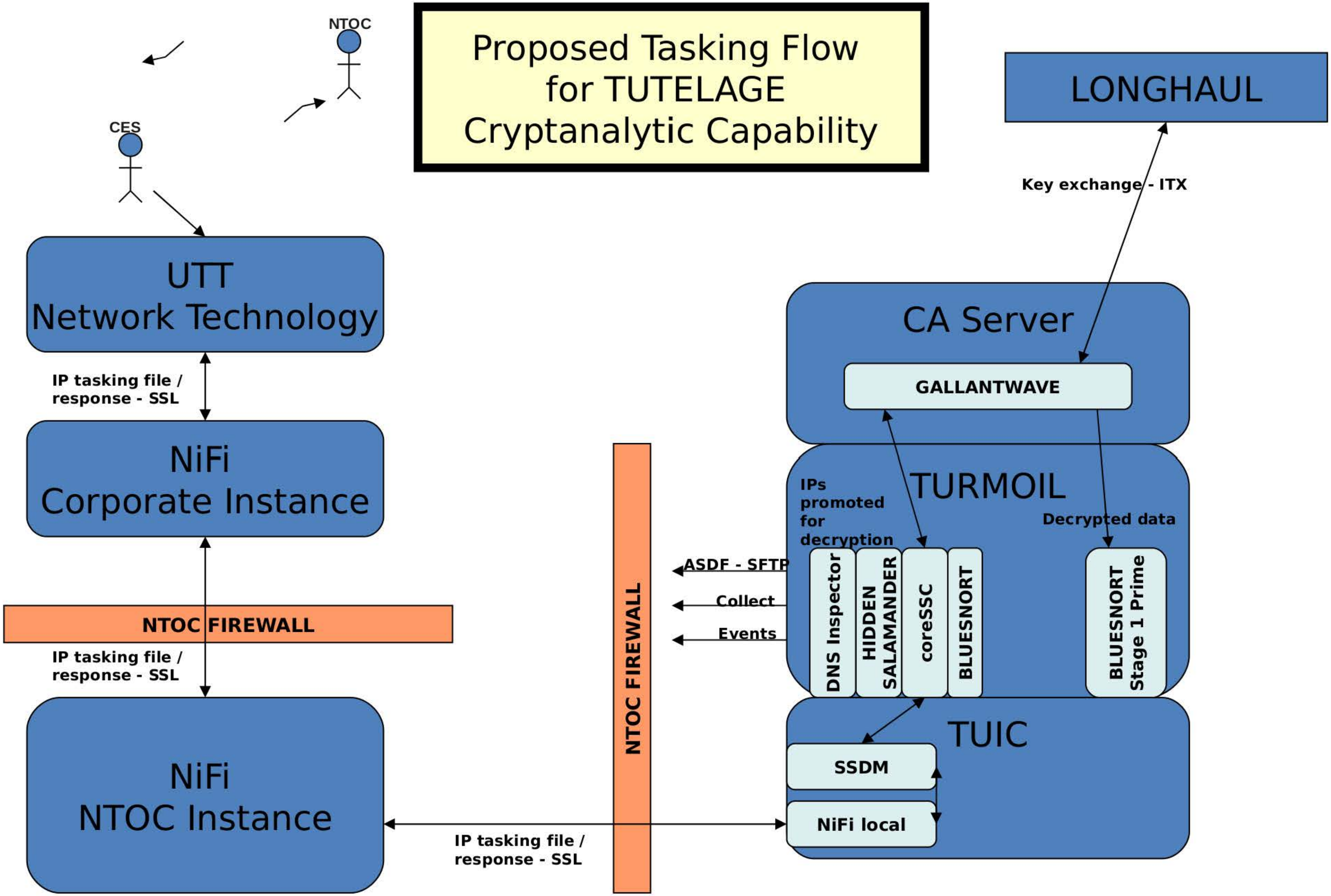
# Delivery to both XKEYSCORE and Stage 1 Prime Reinjection



# TURMOIL
# Stage 1 Prime Reinjection



# Proposed Tasking Flow for TUTELAGE Cryptanalytic Capability


NTOC
CES
UTT
Network Technology
IP tasking file /
response - SSL
NiFi
Corporate Instance
NTOC FIREWALL
IP tasking file /
response - SSL
NiFi
NTOC Instance
IP tasking file /
response - SSL
NTOC FIREWALL
LONGHAUL
Key exchange - ITX
CA Server
GALLANTWAVE
TURMOIL
IPs
promoted
for
decryption
Decrypted data
ASDF - SFTP
Collect
Events
DNS Inspector
HIDDEN
SALAMANDER
coreSSC
BLUESNORT
BLUESNORT
Stage 1 Prime
TUIC
SSDM
NiFi local