APEX
Active/Passive Exfiltration

"go apex"

[redacted]

STDP: S32354 & T112, NCSC/C91

August 2009

This presentation is classified

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Motivation: CES needs VPN keys!

NCC Increment 3 Planning

1. NCC CA Service Requests (Decrypt) per hour (aggregate for all VPN exploitation-enabled systems).

Q4 FY09 (Risk Reduction)	**1,000**
Q4 FY10	**10,000**
Q4 FY11	**100,000**

2. NCC front end systems shall fully process (i.e. decrypt and re-inject) at least 20% of CA service requests (~20% Reinject Rate?)
3. For tasked IP addresses, NCC front end systems shall identify relevant IPSec sessions and generate attack requests (Rates?)
4. NCC front end systems shall buffer VPN data for up to 15 minutes (900 seconds) while waiting for response from Attack Orchestrater (AO)
5. After successful key recovery and decryption PIQ services shall re-inject decrypted VPN for Stage1 & Stage2 processing
6. Aggregate VPN buffering and processing rate per TML system (**Assumptions – LPT? T16? U64?**)

Q4 FY09 (Risk Reduction)	4 VPN Systems	**25 Concurrent VPN Flows / System**	**100 Mbps Aggregate VPN Data / System**
Q4 FY10	10 VPN Systems	**100 Concurrent VPN Flows / System**	**100 Mbps Aggregate VPN Data / System**
Q4 FY11	100 VPN Systems	**100 Concurrent VPN Flows / System**	**500 Mbps Aggregate VPN Data / System**

- CES receives VPN IKE packets from passive collection (TURMOIL) and recovers VPN keys.
- TURMOIL receives VPN ESP packets and decrypts them using the keys recovered by CES.
- But there are many VPNs that TURMOIL(s) can't see.

Motivation: Leverage TAO

- TAO/DNT active implants have a powerful Man-in-the-Middle capability to access data deep within target networks.
  - They can select packets and exfiltrate them back to the Common Data Receptor (CDR) at the Remote Operations Center (ROC).
  - HAMMERSTEIN: target any 5-tuple packet
    - {SrcIP, SrcPort, DstIP, DstPort, Protocol}
      - IKE: VPN key exchanges
      - ESP: VPN encrypted tunnels
  - HAMMERCHANT: target VoIP phone numbers
    - Process SIP/H.323 VoIP signaling
    - Forward targeted phone call RTP media sessions
- But CDR has limited input bandwidth.

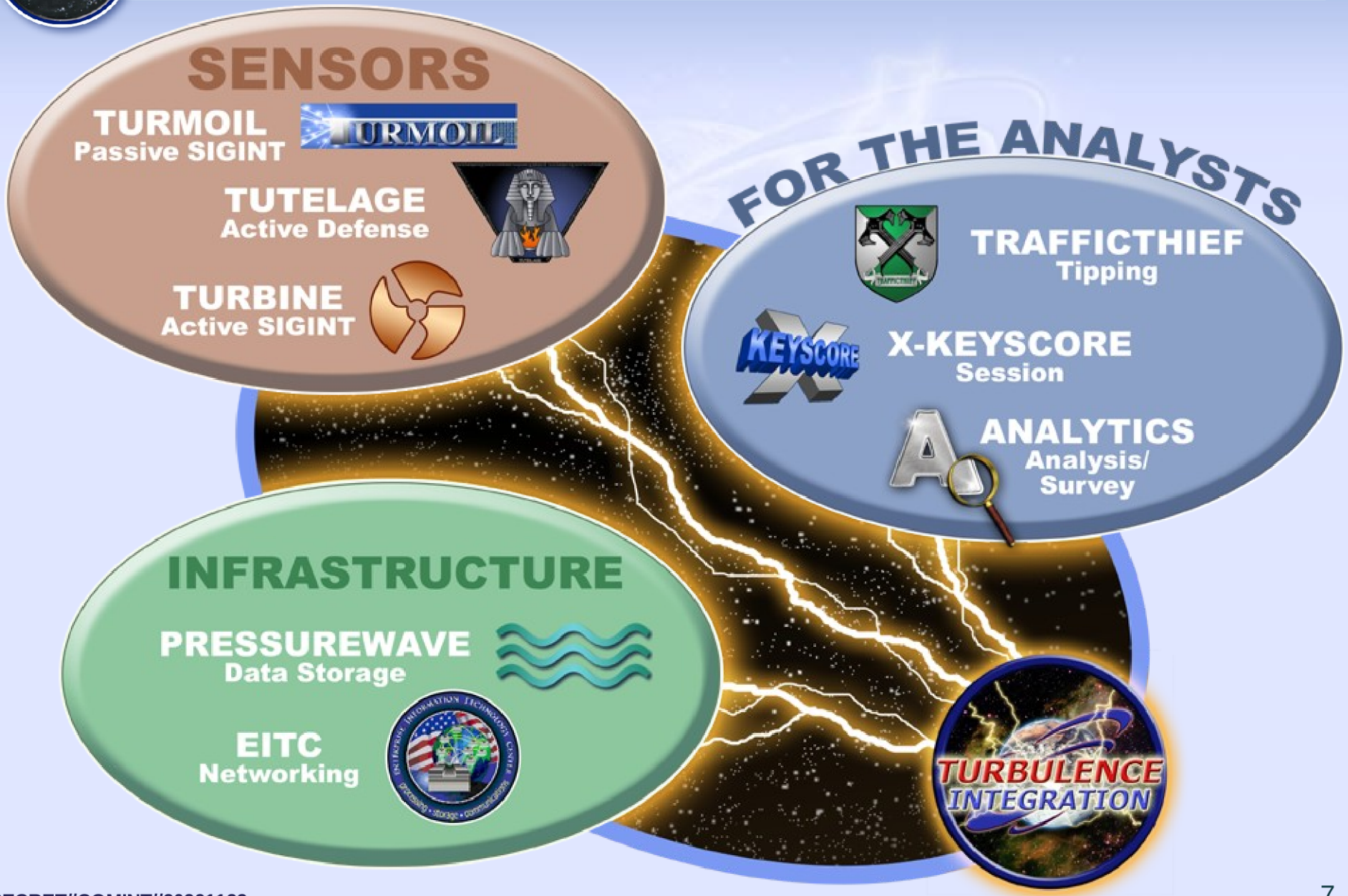
Hmmmm…

Maybe… Combine Active & Passive?

Agenda

- Motivation: Why?
- TURBULENCE High Level Concept: What?
- Details: How?
  - FASHIONCLEFT Exfiltration Protocol
    - Definition
    - Processing Required
  - Turmoil Architecture
  - Turmoil Implementation
    - Packet Reinjection: Stage 1 Prime
    - Packet Processing Framework: AEG/SEG
    - Packet Routing: different Transform Engines
- Complexity
- Challenges
- Phased Development

(U) TURBULENCE Architecture



(U) Sensors: Passive Collection

Accesses

- TURMOIL
- TUTELAGE
- Implants (TAO)

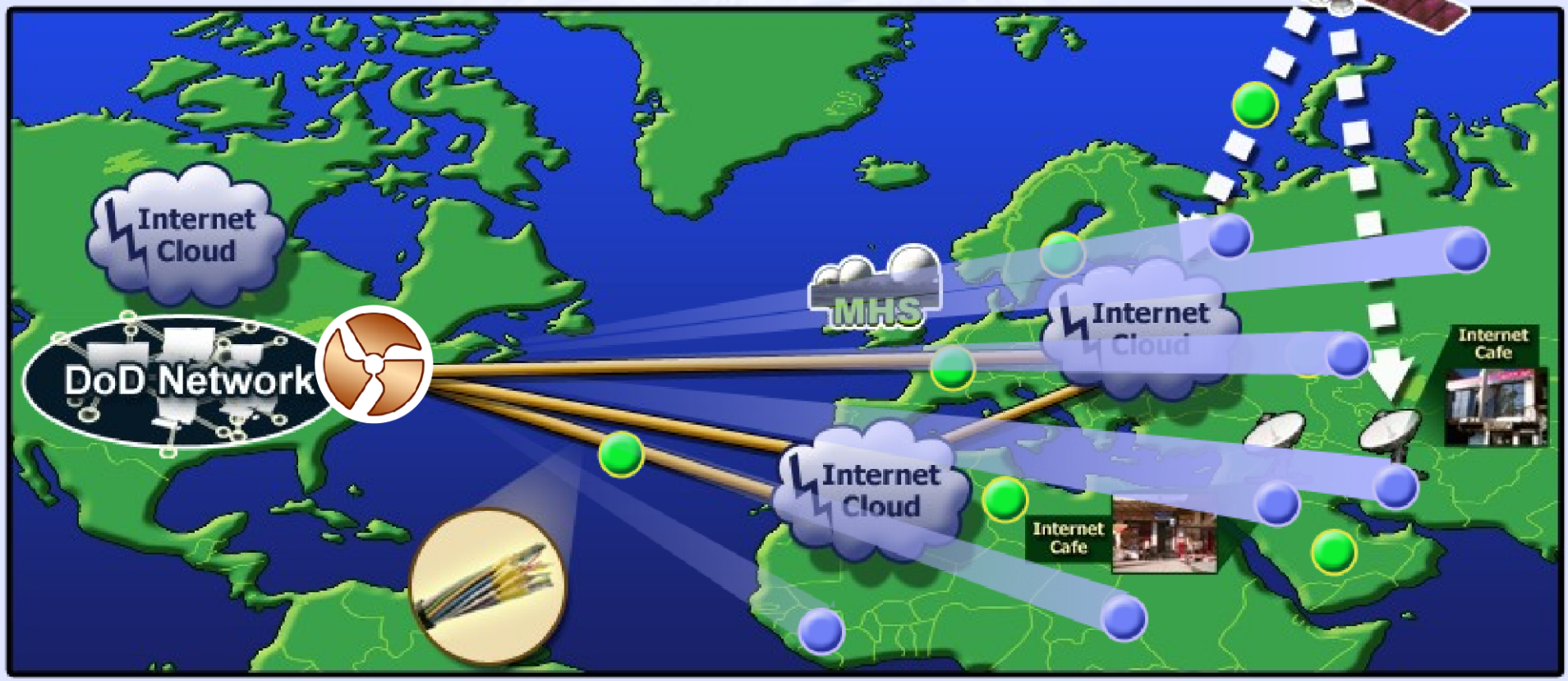
TURMOIL (S//SI//REL) High-speed passive collection systems intercept foreign target satellite, microwave, and cable communications as they transit the globe.

(U) Sensors: Active Mission Management

Accesses

- TURMOIL
- TUTELAGE
- Implants (TAO)

(TS//SI//REL) TURBINE enables the automated management and control of a large network of active implants



APEX VPN IKE Mission

Internal Network

The Internet

VoIP server or VPN

TAO Inside

Exfil Path

Tailored Access Office Remote Operations Center

Tasking

Tasking

URMOIL SSO

MHS

TURBINE NSAW

PRESSUREWAVE

POISON N

TOYGRIPE

Analyst Tools

APEX VoIP Mission

Exfil Path

Tasking

FASHIONCLEFT Exfiltration Protocol

FASHIONCLEFT

- **Definition:** *TAO/DNT protocol used by implants to exfiltrate collected network packets to the Common Data Receptor (CDR, aka FLAXENPRECEPT).*

- Provides support for:
  - Metadata Authentication/Integrity + AntiReplay + Encryption
  - Data Encryption
  - Uses 1024-bit RSA, 128-bit RC6, SHA-1

- Based on DNT standards:
  - FOGYNULL (DNT Exfiltration Protocol)
  - FUNNELAPS (DNT Exfiltration Data Format)
  - SHELLGREY (DNT Exfiltration Metadata Format)

How To Exfiltrate IP Packets

1. Select packet based on tasking.
2. Make a copy of the selected packet.
3. Modify packet IP destination address.
4. Modify other protocol fields (IP, UDP, TCP) as needed to bypass firewalls and to tag packets for ID.
5. Optionally encrypt/munge Transport layer payload.
6. Send modified Data Packet (DP) to new destination.

Receiver: Needs Metadata

- Metadata explains how to:
  1. Identify an exfil packet and the implant source.
  2. Recover original IP destination address.
  3. Recover other original protocol fields (IP, UDP, TCP).
  4. Contains Key to decrypt/unmunge transport layer payload.

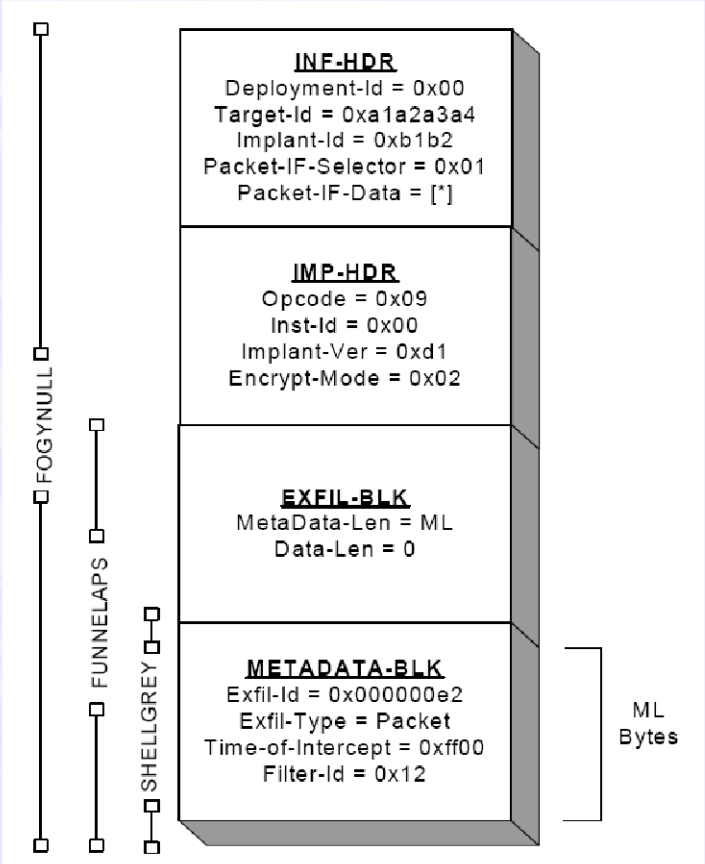
- Metadata sent in a Session Announcement (SA)
  - SAs is an IP/UDP packet sent to a destination IP/port.
  - Multiple copies of SA sent to mitigate dropped SA packets.

- Receiver is dynamically configured with:
  - SA IP/ports, Infrastructure & Implant Private Keys
  - Processing Mode: Reconstruct or Reinject

FASHIONCLEFT

Session Announcement Format

- IP Header
- UDP Header
- SA Payload in UDP Transport Layer
  - Infrastructure Header (128 bytes)
    - RSA Encrypted w/ Infrastructure Public Key
    - Contains SHA-1(INF-HDR), CryptoId
      - CryptoId = {DeploymentId, TargetId, ImplantId}
  - Implant Header (128 bytes)
    - RSA Encrypted w/ CryptoId 's Public Key
    - Contains SHA-1(IMP-HDR)
    - 128-bit CV, MI, and CRC-16 checksum for Exfil/Metadata Block
  - Exfil/Metadata Block (variable)
    - RC6 Encrypted w/ CV & MI
- Minimum packet length = 344 bytes



FASHIONCLEFT

Session Announcement Processing

1. Look for SA packets:
   1) at destIP/destPort; protocol=UDP,
   2) that are at least 344 bytes long, and
   3) whose first 128-bytes of Transport Payload “look random”.
   - (Easy/quick initial checks)
1. RSA Decrypt INF-HDR w/ Infrastructure Private Key.
   - Authenticate w/ SHA-1
   - (Slow secondary check; can’t withstand much non-SA traffic on IP/port)
1. RSA Decrypt IMP-HDR w/ CryptoId ’s Private Key.
   - Authenticate w/ SHA-1
1. RC6 Decrypt Exfil/Metadata w/ CV and MI
   - Perform CRC-16 integrity check.
1. Anti-Replay Check & New Session/Retransmit Check
2. Extract Metadata and create Collection Filter rule for DPs
   - Metadata contains either 5-tuples or pattern/mask/offset that match DPs
   - `PpfEvent.DfceCF.tuple (5-tuple)`

FASHIONCLEFT

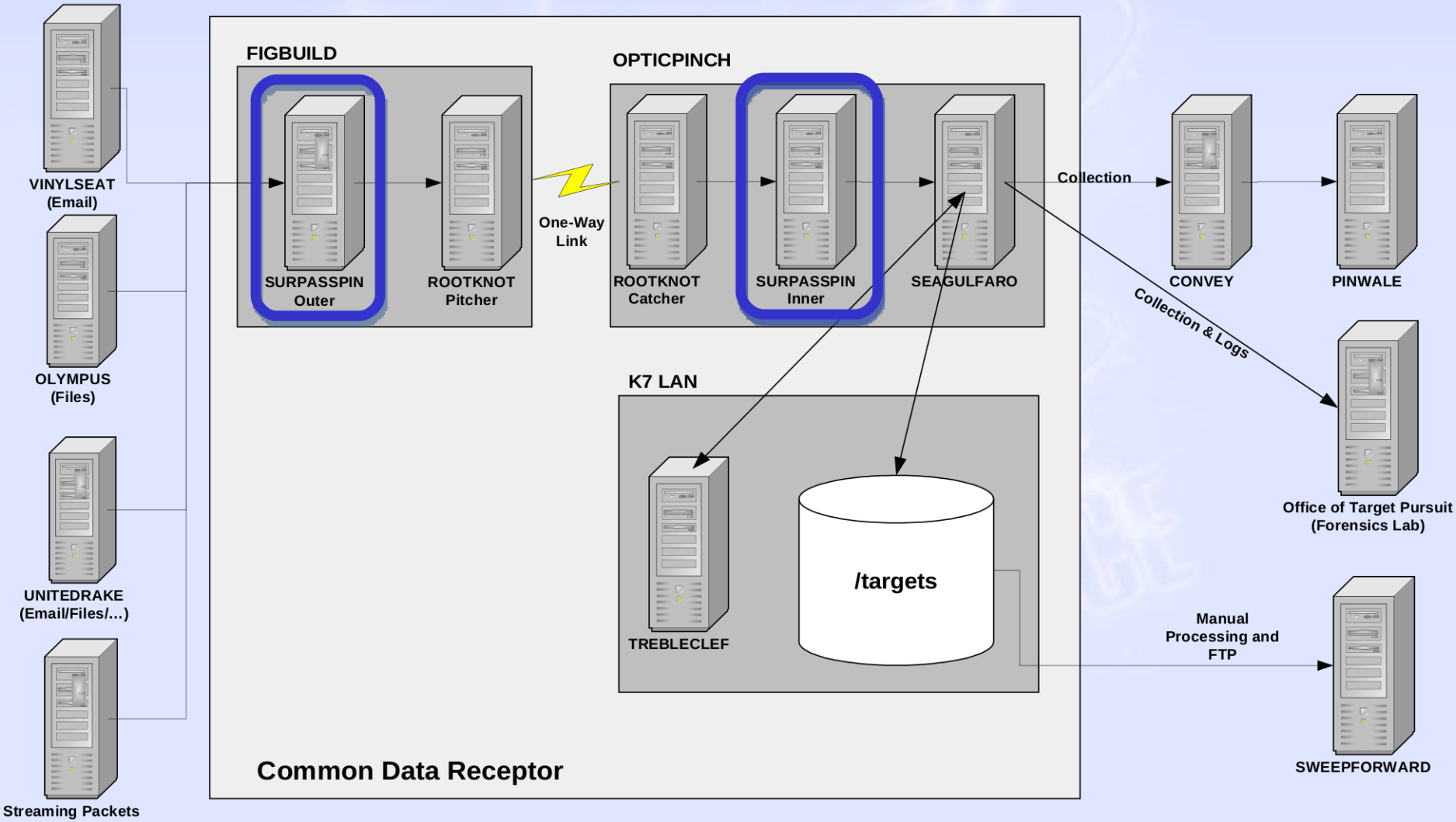
Data Packet Processing

1. Identify an exfil packet that matches DP filter rule.
2. Modify to original IP destination address.
3. Modify to original protocol fields (IP, UDP, TCP).
4. Decrypt/unmunge transport layer payload.
   - Have now recovered the original captured packet.

1. Associate metadata with recovered packet.
   - agentCaseNotation, Turmoil link caseNotation
1. Perform protocol specific processing.
   - Pre-selected: forward all traffic to TUBE/PWAVE
   - Re-inject back into Turmoil Stage-1

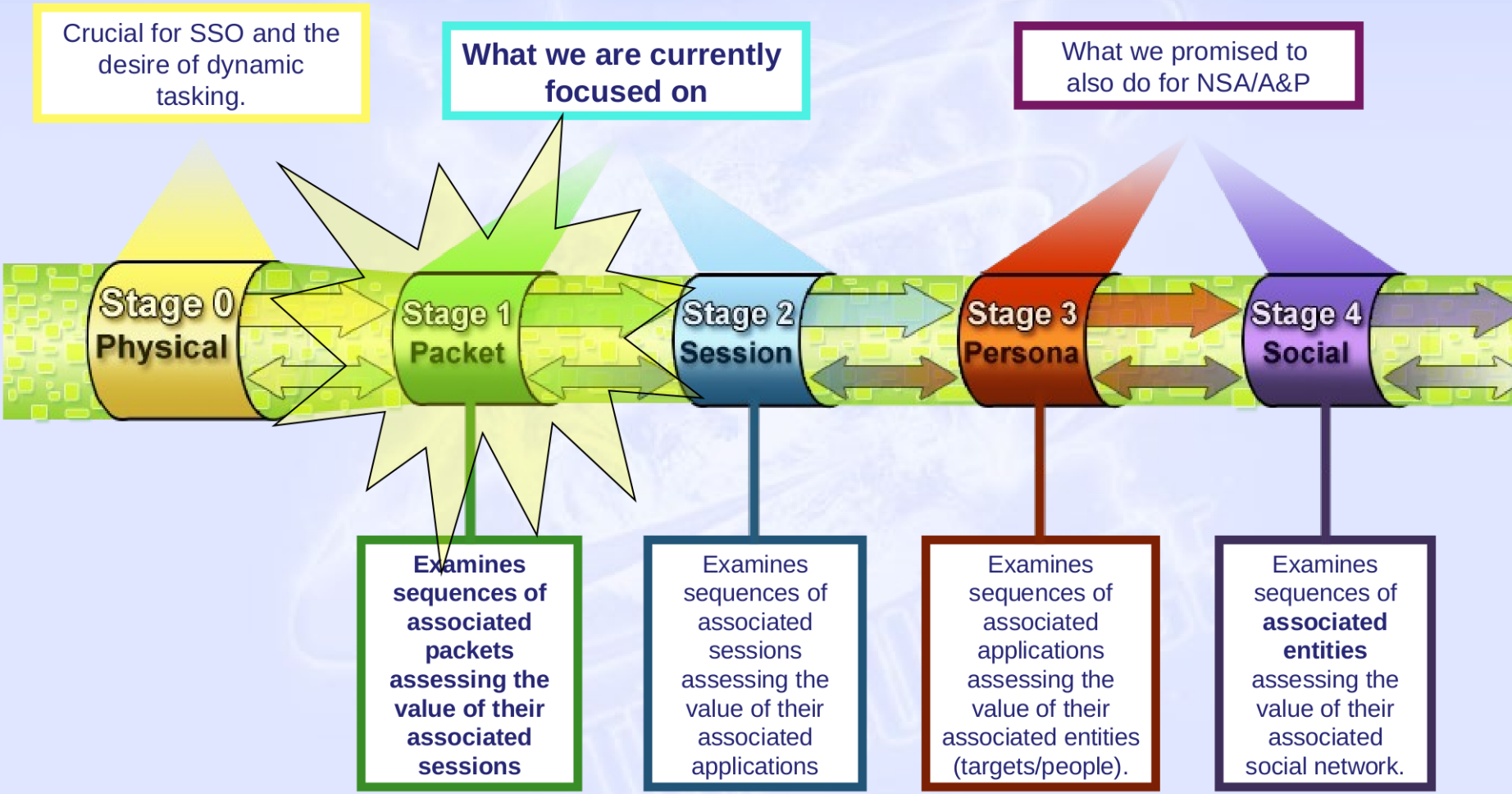
TAO Remote Operations Center

Common Data Receptor

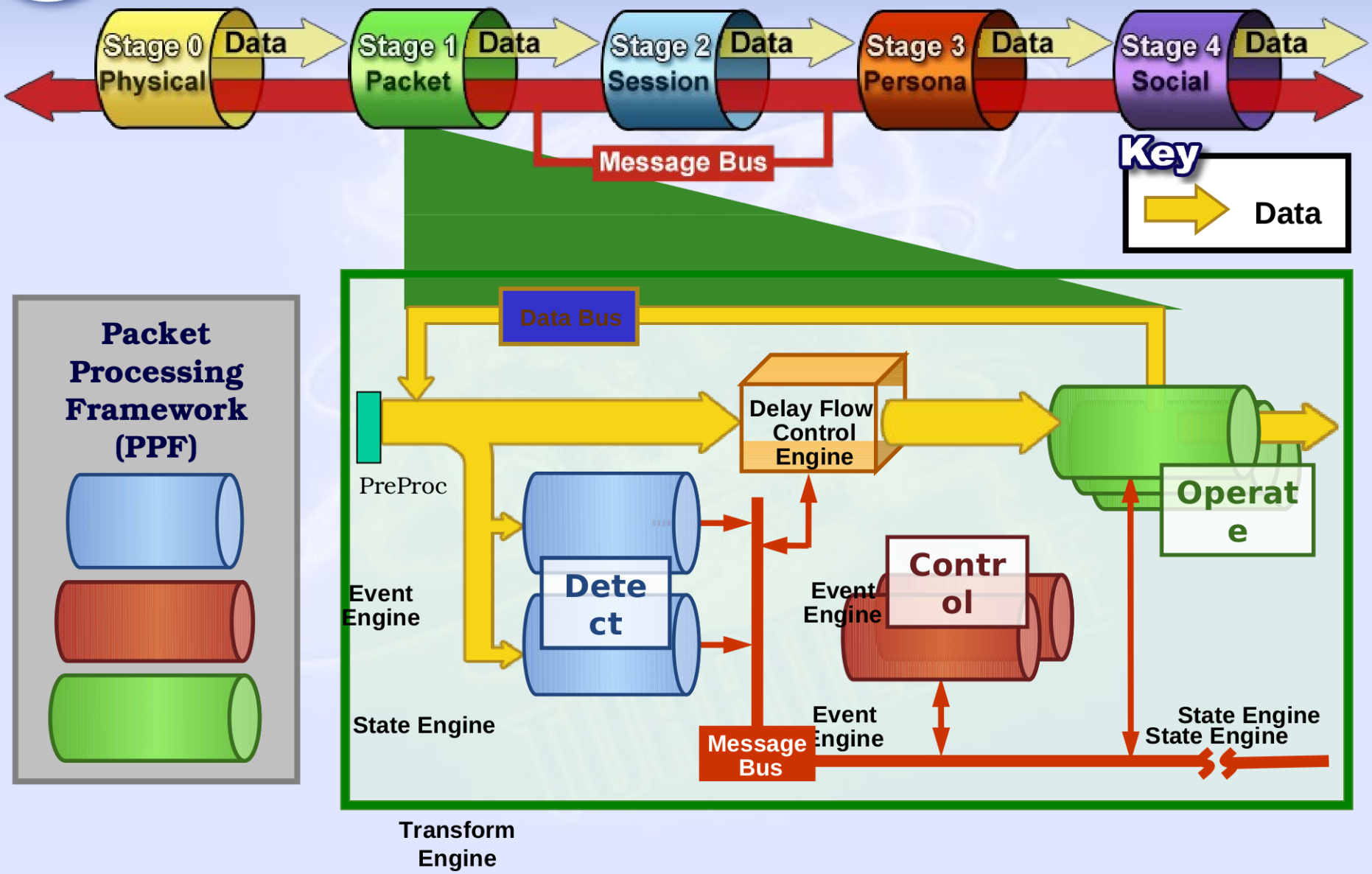


TURMOIL Architecture

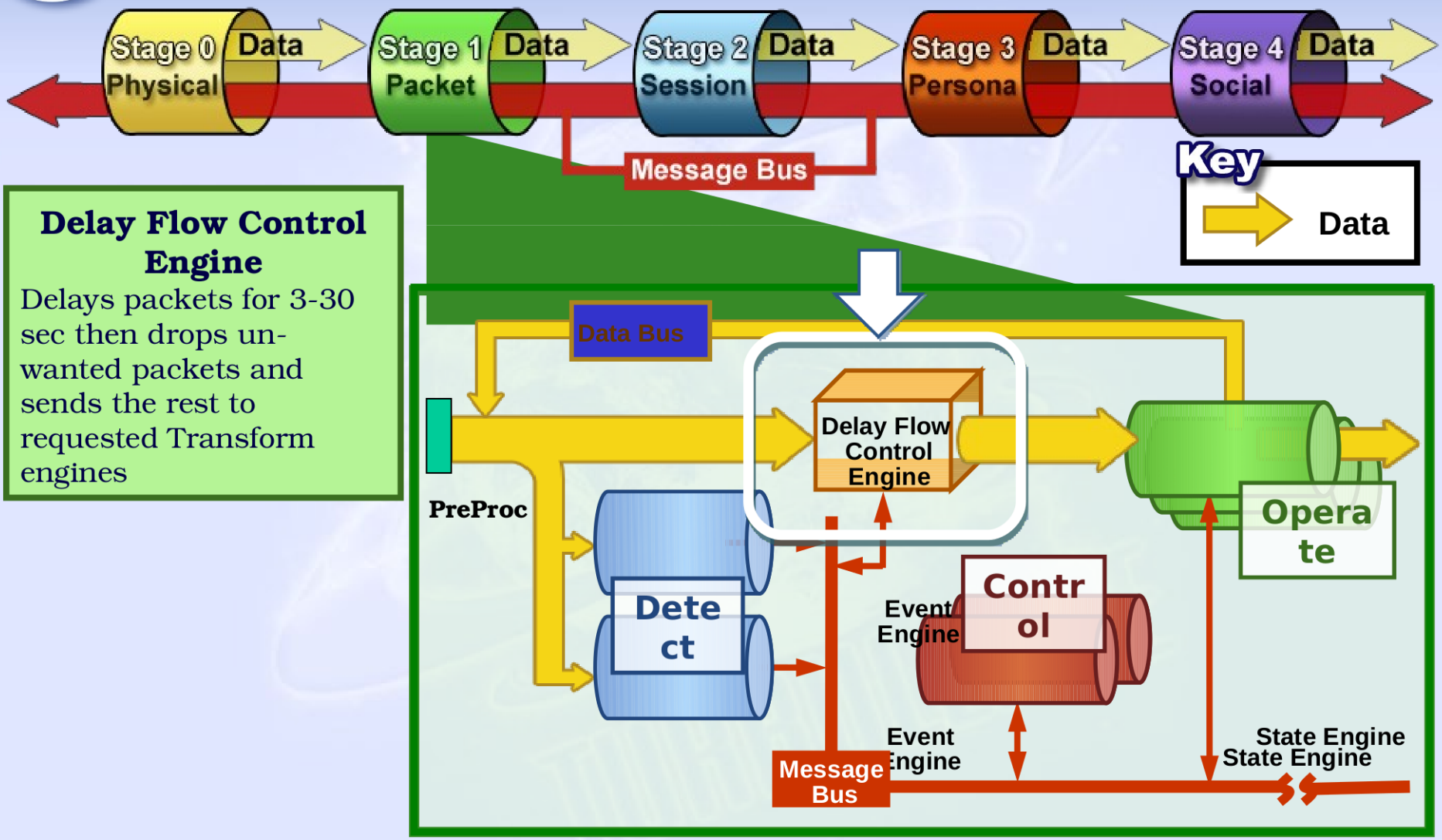
TURMOIL Architecture



Inside Stage 1



Inside Stage 1



Delay Flow Control Engine

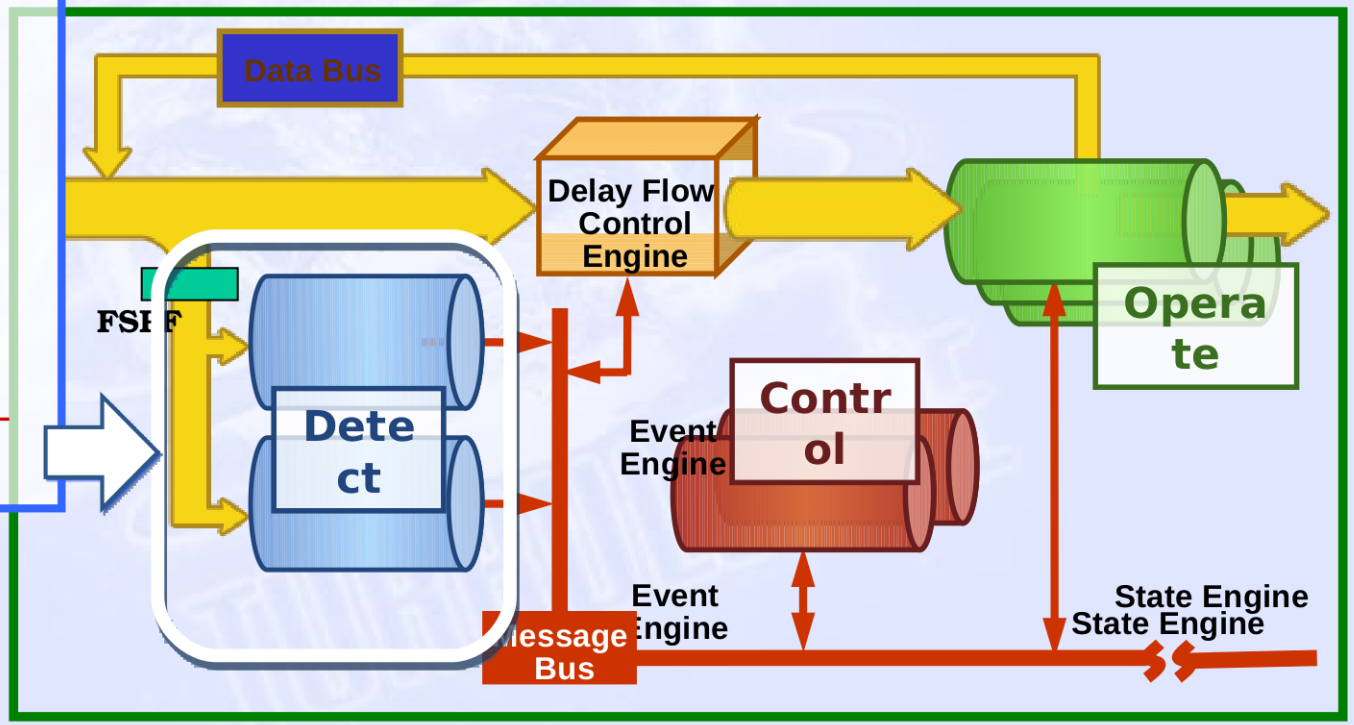
Delays packets for 3-30 sec then drops un-wanted packets and sends the rest to requested Transform engines

Event Engines: Detect

- **Stateless -** does not store data or metadata
  (Atomic Event Generator = AEG)
- Evaluation of traffic
- Publish observations
- Each engine can be specialized and optimized based on incoming speed
  - Software and/or Hardware

Examples:

1. Detect VPN setup:
   IKE key exchange.
2. Detect VPN tunnel:
   ESP packets.
3. Detect VoIP signaling:
   H.323, SIP, Skype, etc.
4. Detect FASHIONCLEFT Session Announcement.



State Engines: Control

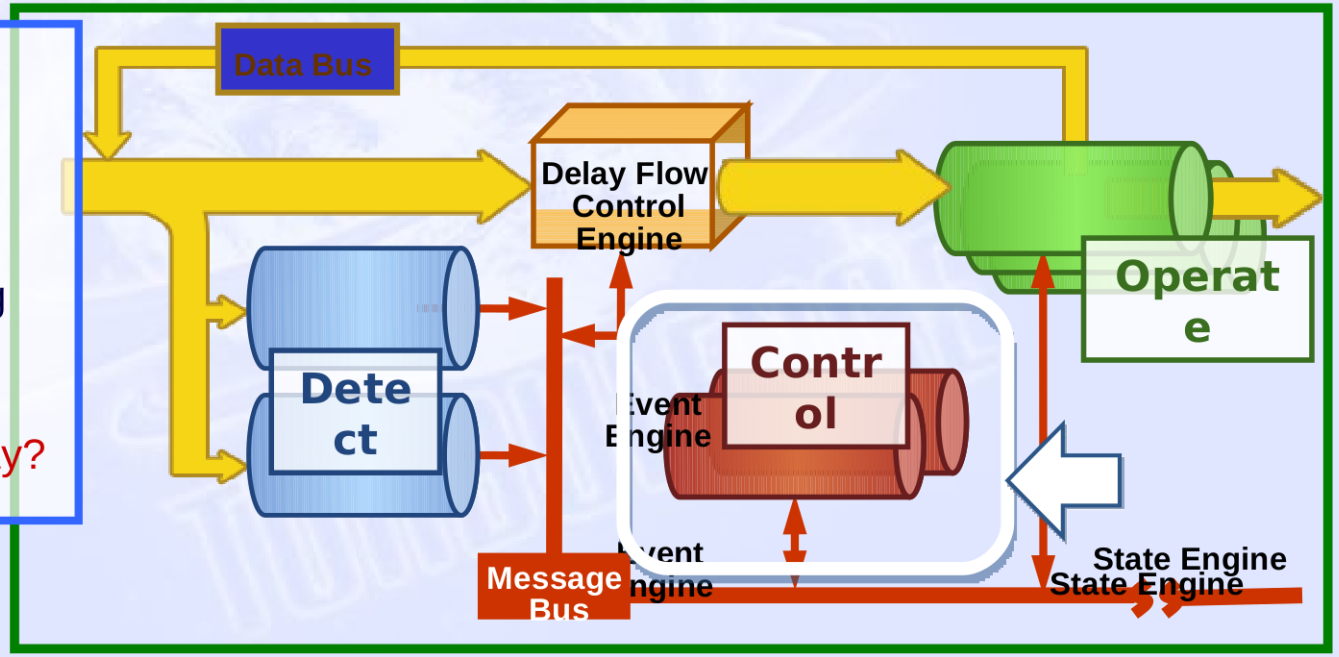
- Receives published events from Event Engines and makes processing decisions.
- Choreographs activity for data flows (Stateful Event Generator = SEG)
  - Correlates multiple published events
  - Starts/stops transform processing engines
  - Publishes decisions about the flow
- Each State Engine can be specialized and optimized

Examples:

1. Associate VPN IKE/ESP traffic with recovered VPN keys.

2. Associate VoIP signaling w/ phone call.

3. Track FASHIONCLEFT SA's: new, keepalive, replay?



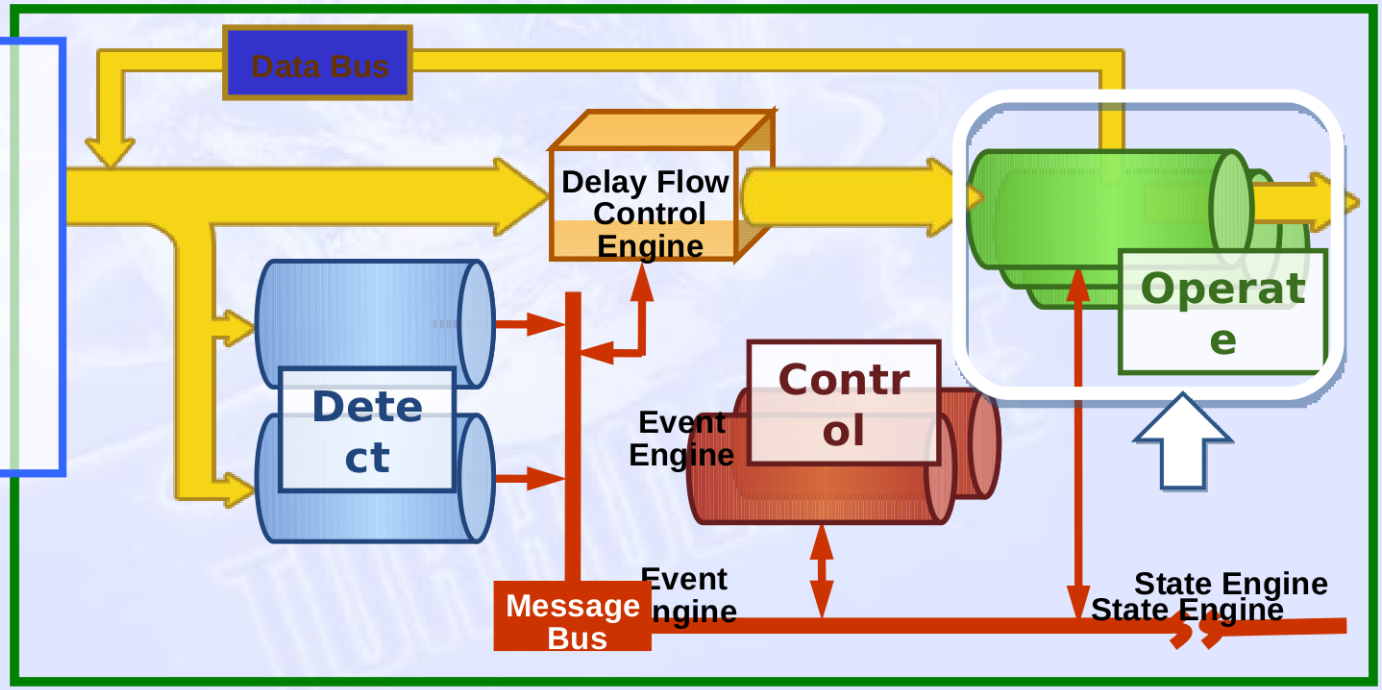
Transform Engines: Grooming

- Receives orders from State Engines
- Operation applied to a data object that does not change its level of abstraction.
  - Packet ➡ Packet(s)
  - Session ➡ Session(s)
- Groomed data object can then be ***re-injected*** or ***sent forward***

Examples:

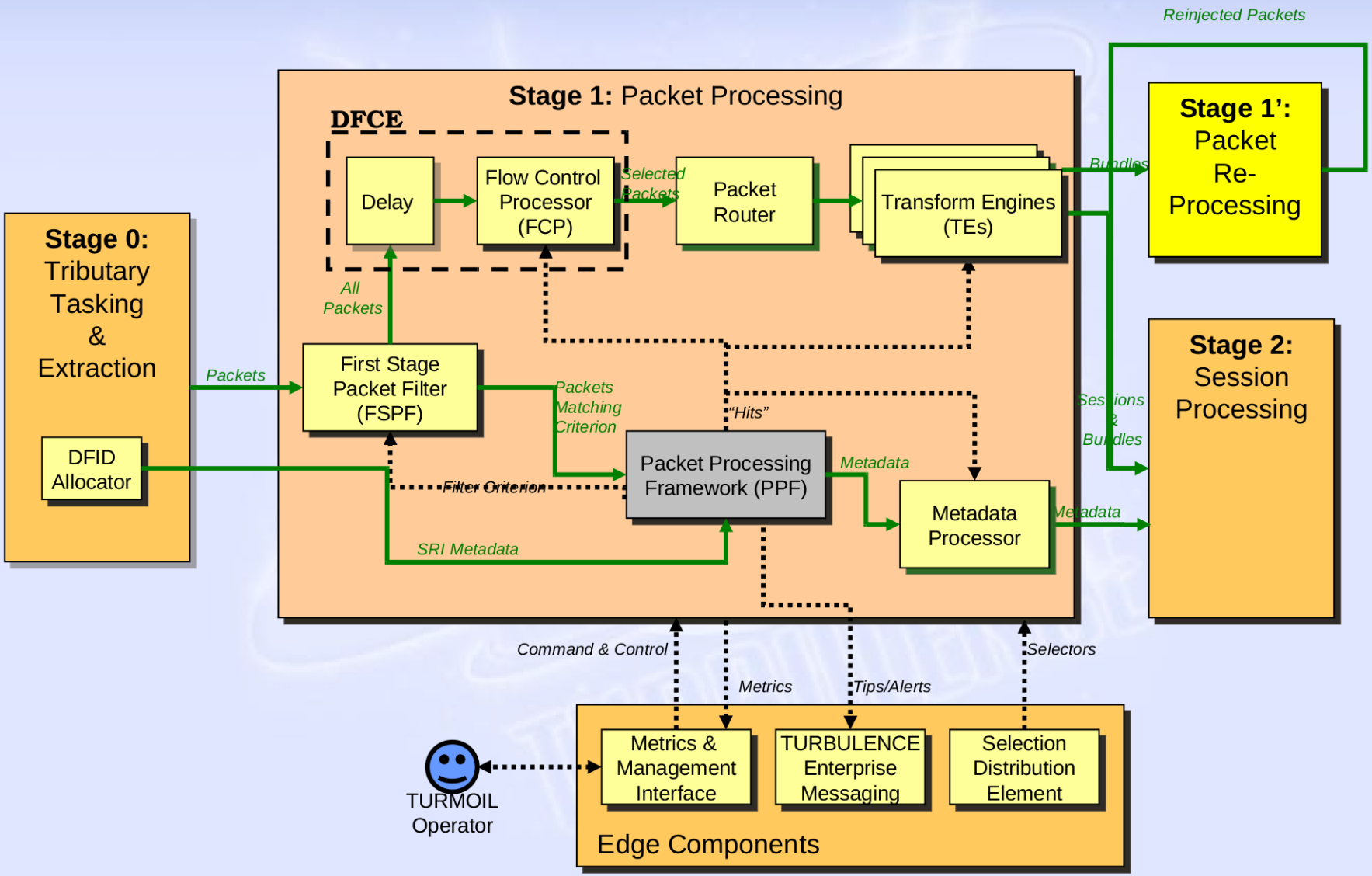
1. Decompress/decrypt packet.

2. Reconstruct original packet from FASHIONCLEFT Data Packet.

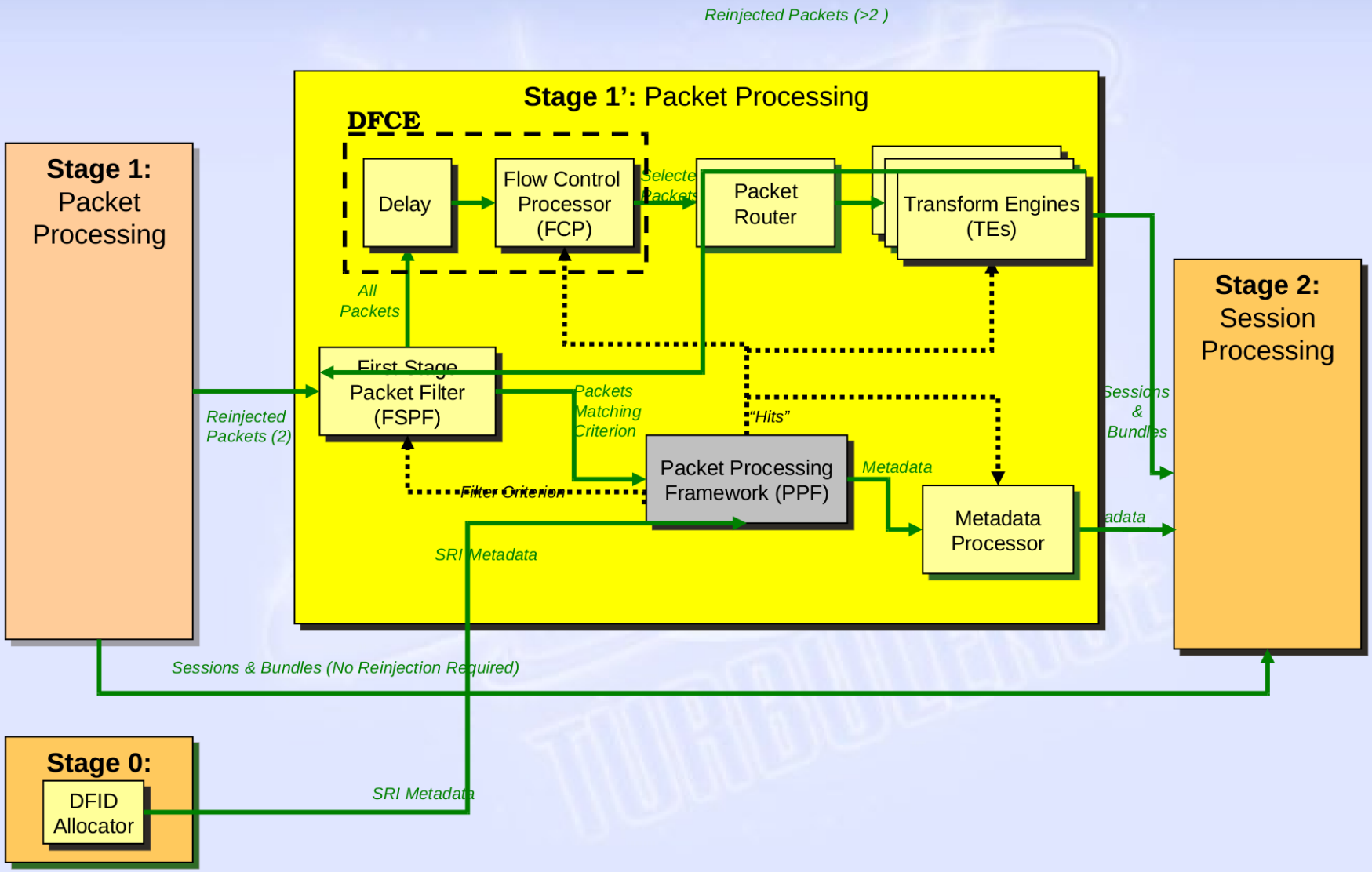


TURMOIL Implementation

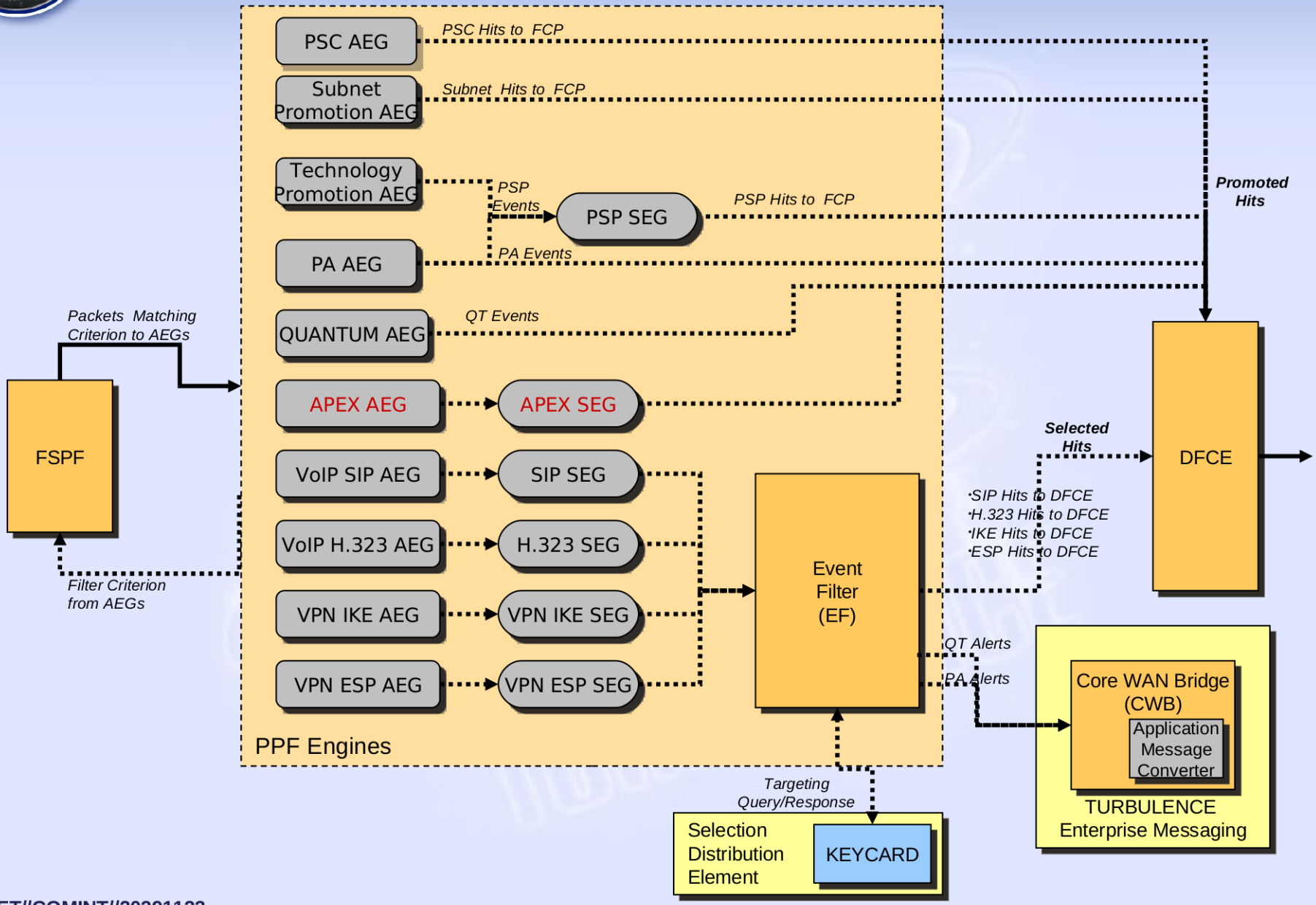
TURMOIL Stage 1 with Stage 1'



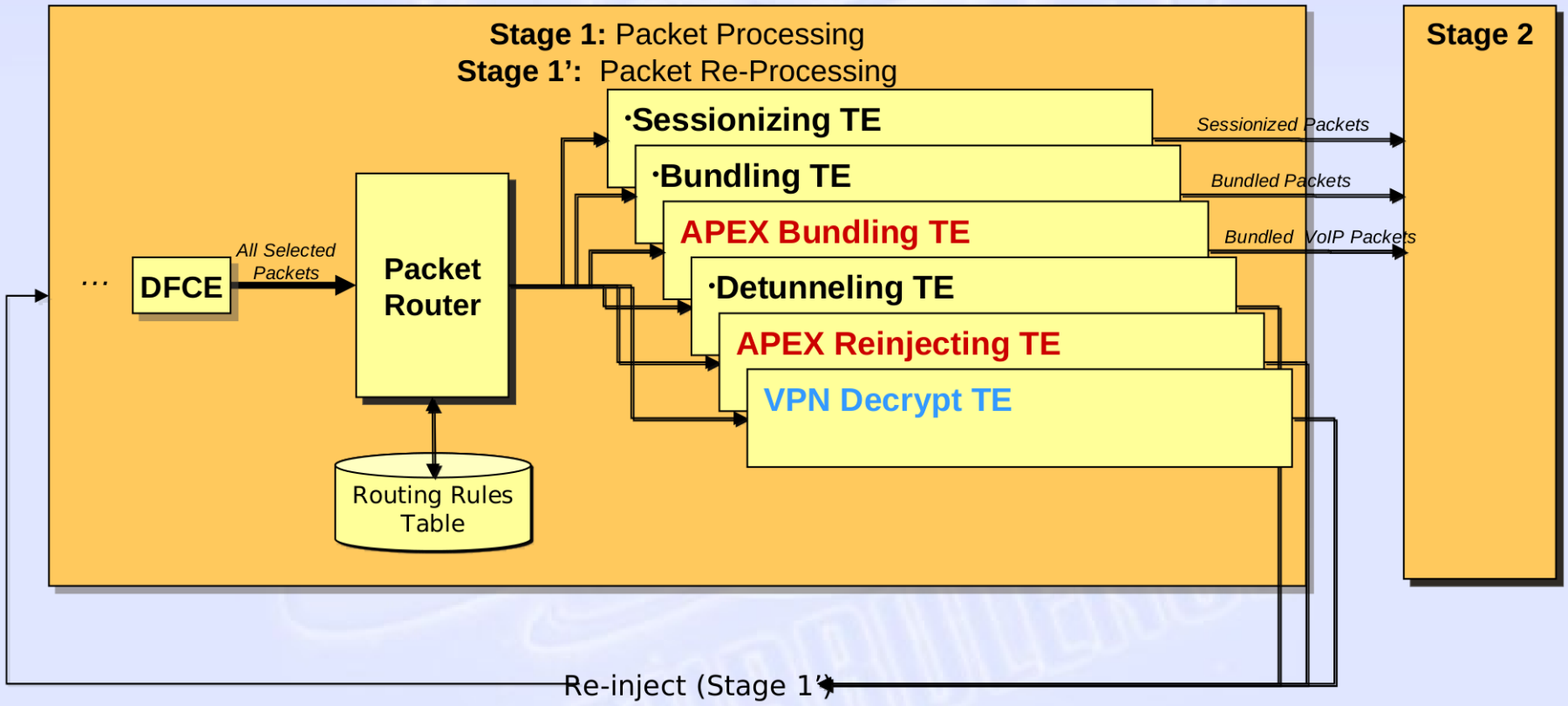
TURMOIL Stage 1' (Stage One Prime)



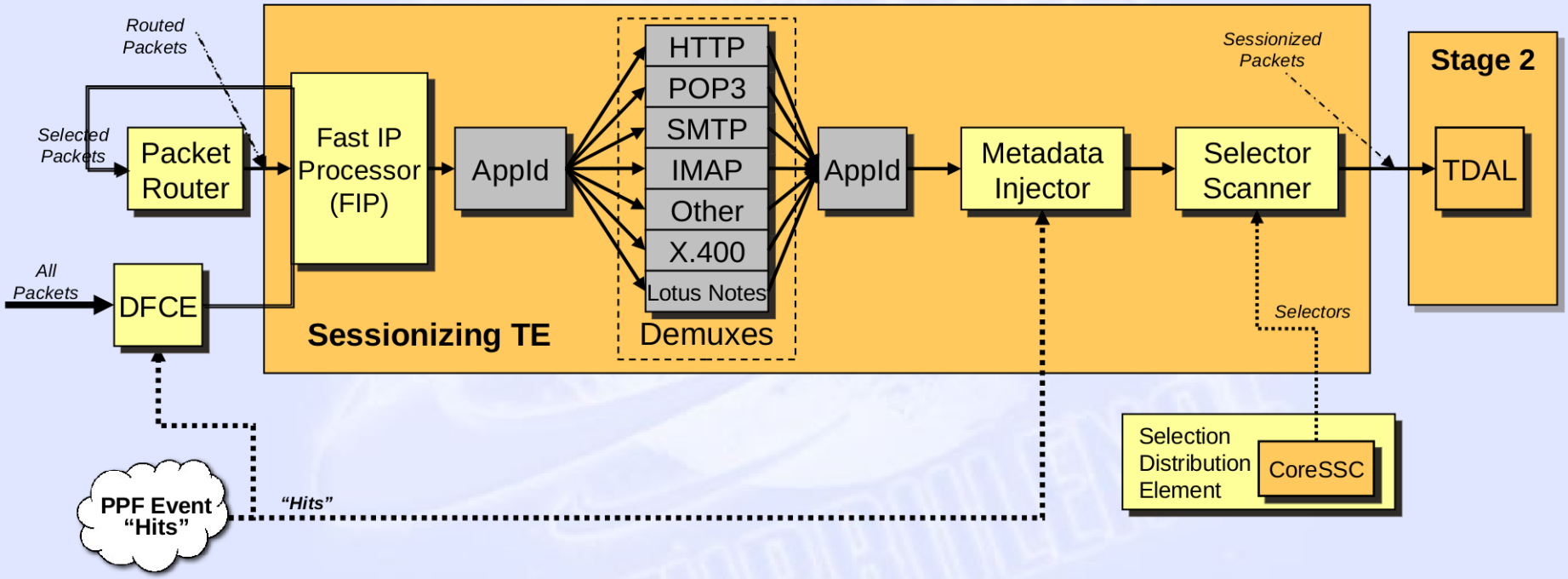
TURMOIL Stage 1 PPF Engines



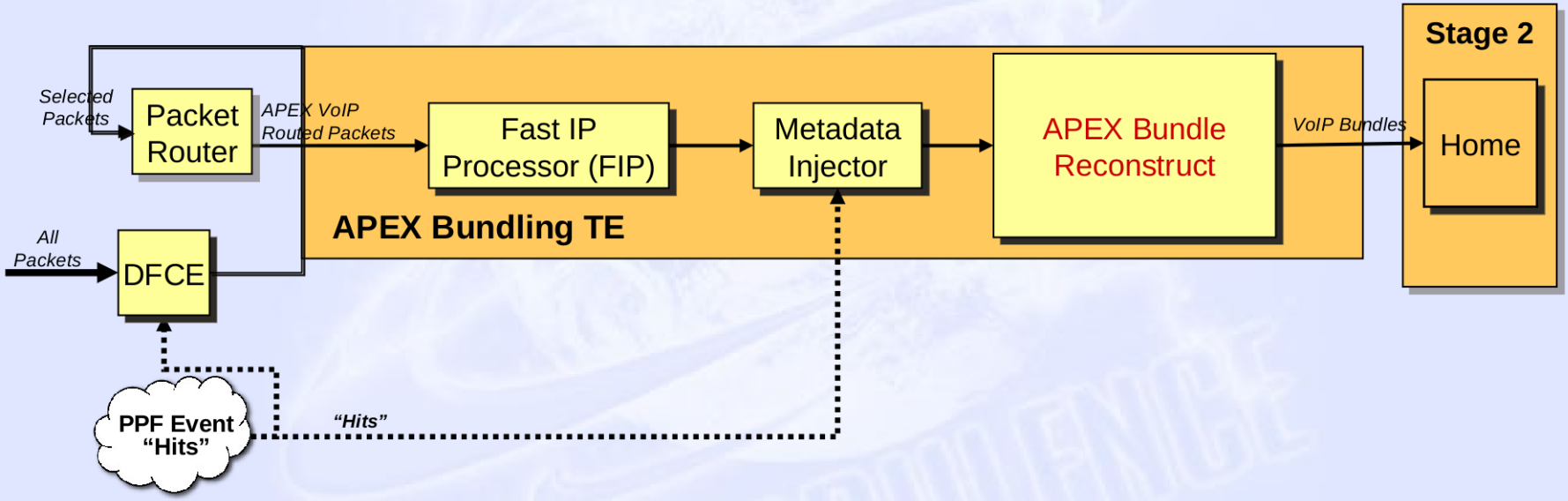
TURMOIL Stage 1 Packet Router



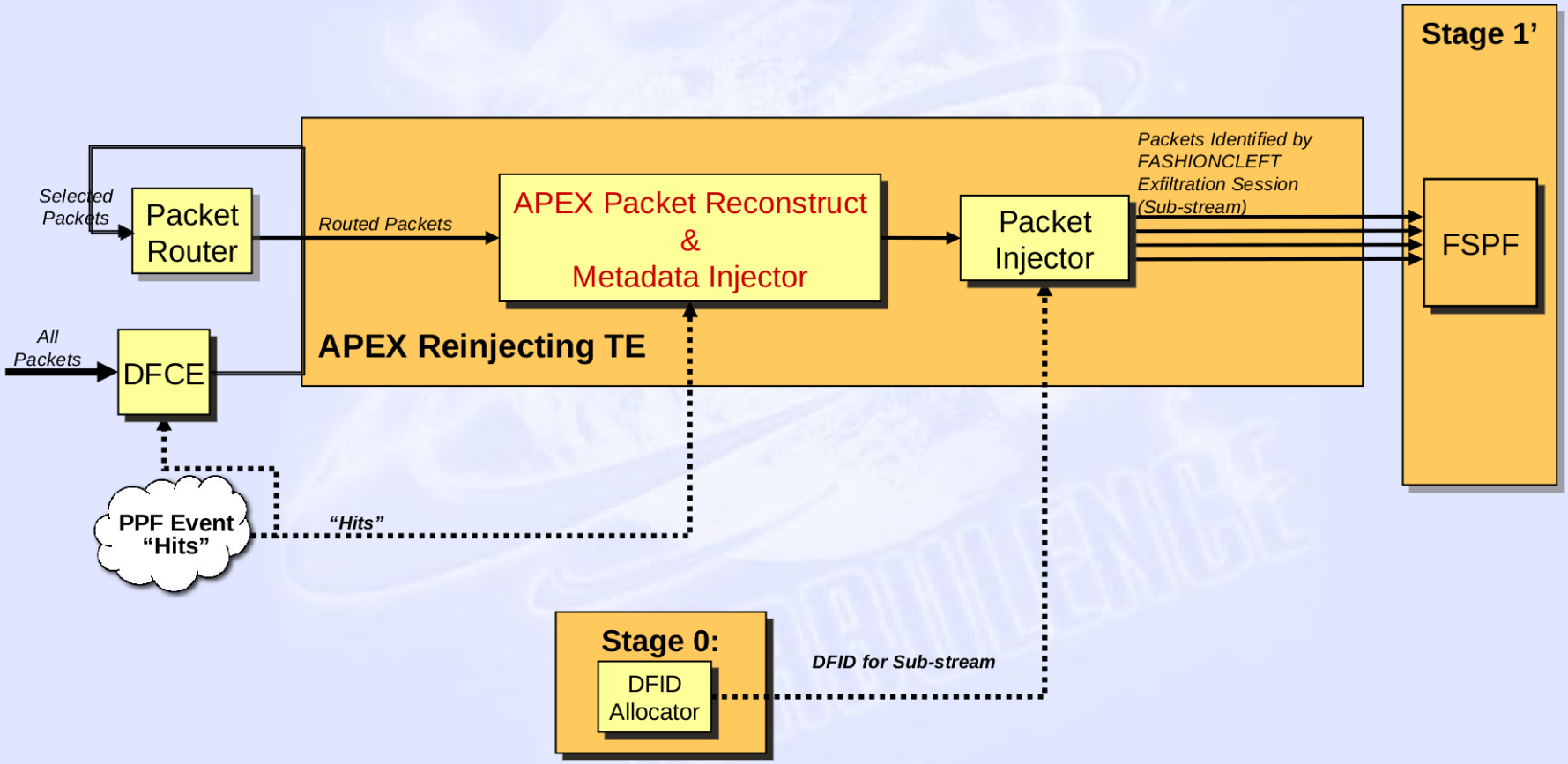
TURMOIL Stage 1 Sessionizing TE



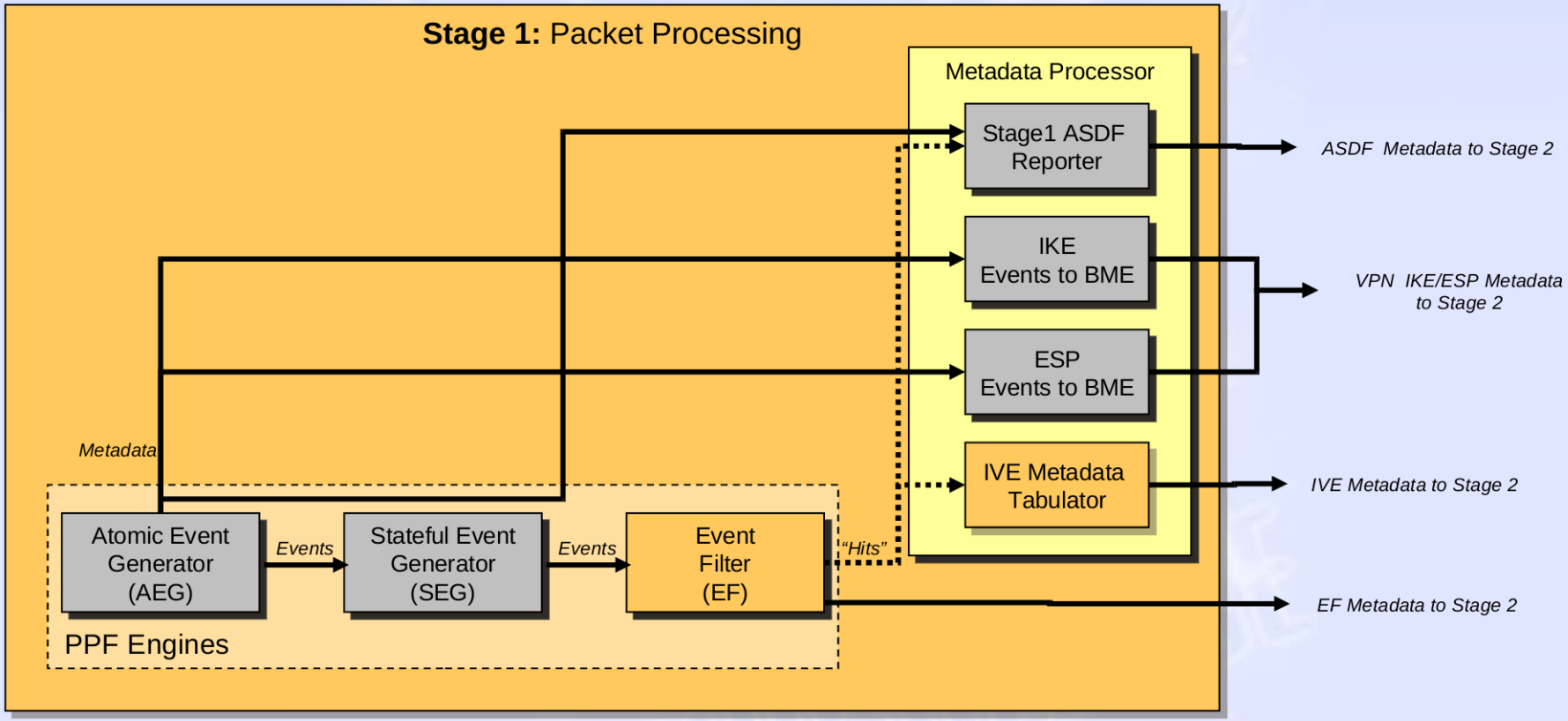
TURMOIL Stage 1 APEX Bundling TE



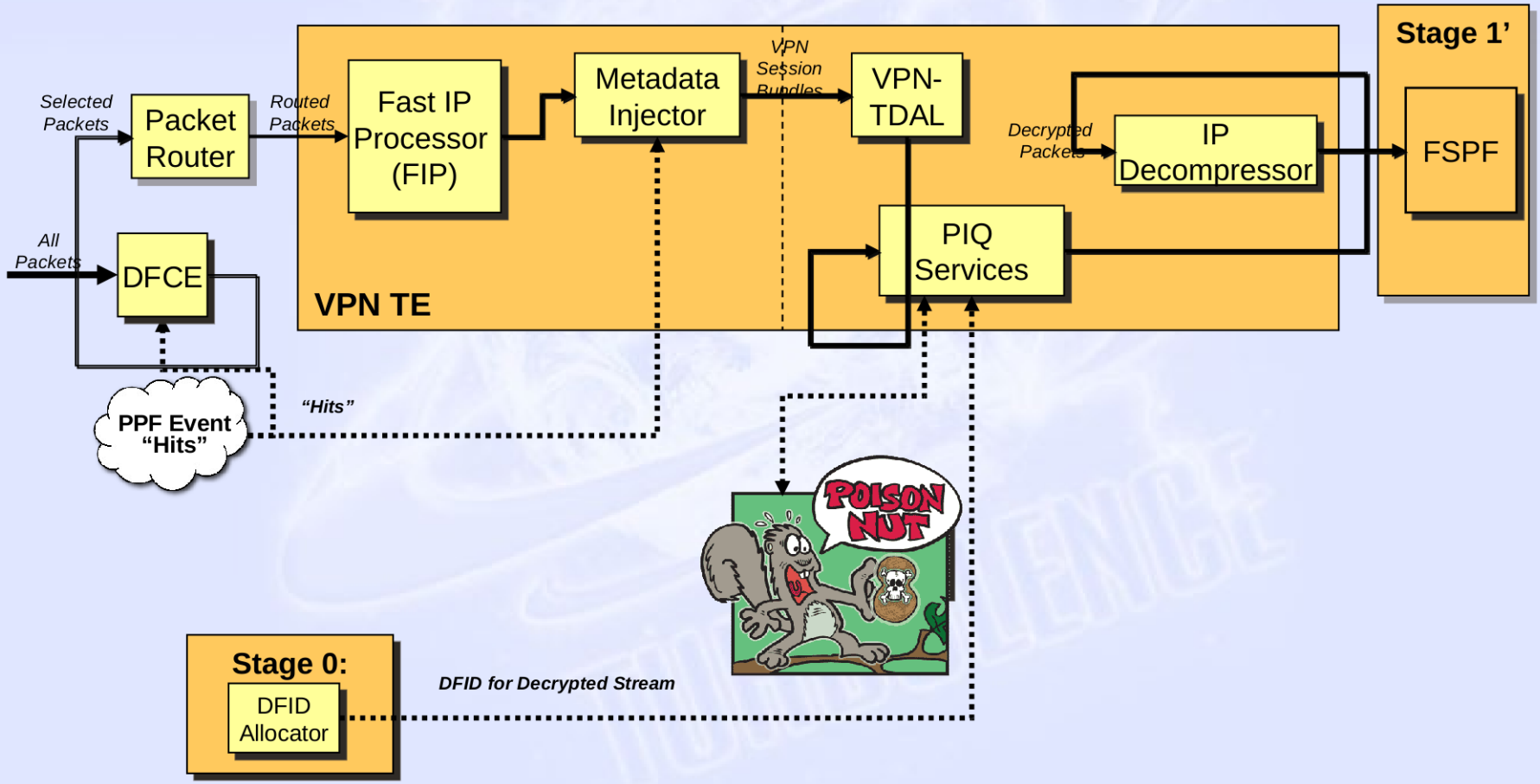
TURMOIL Stage 1 APEX Re-Injecting TE



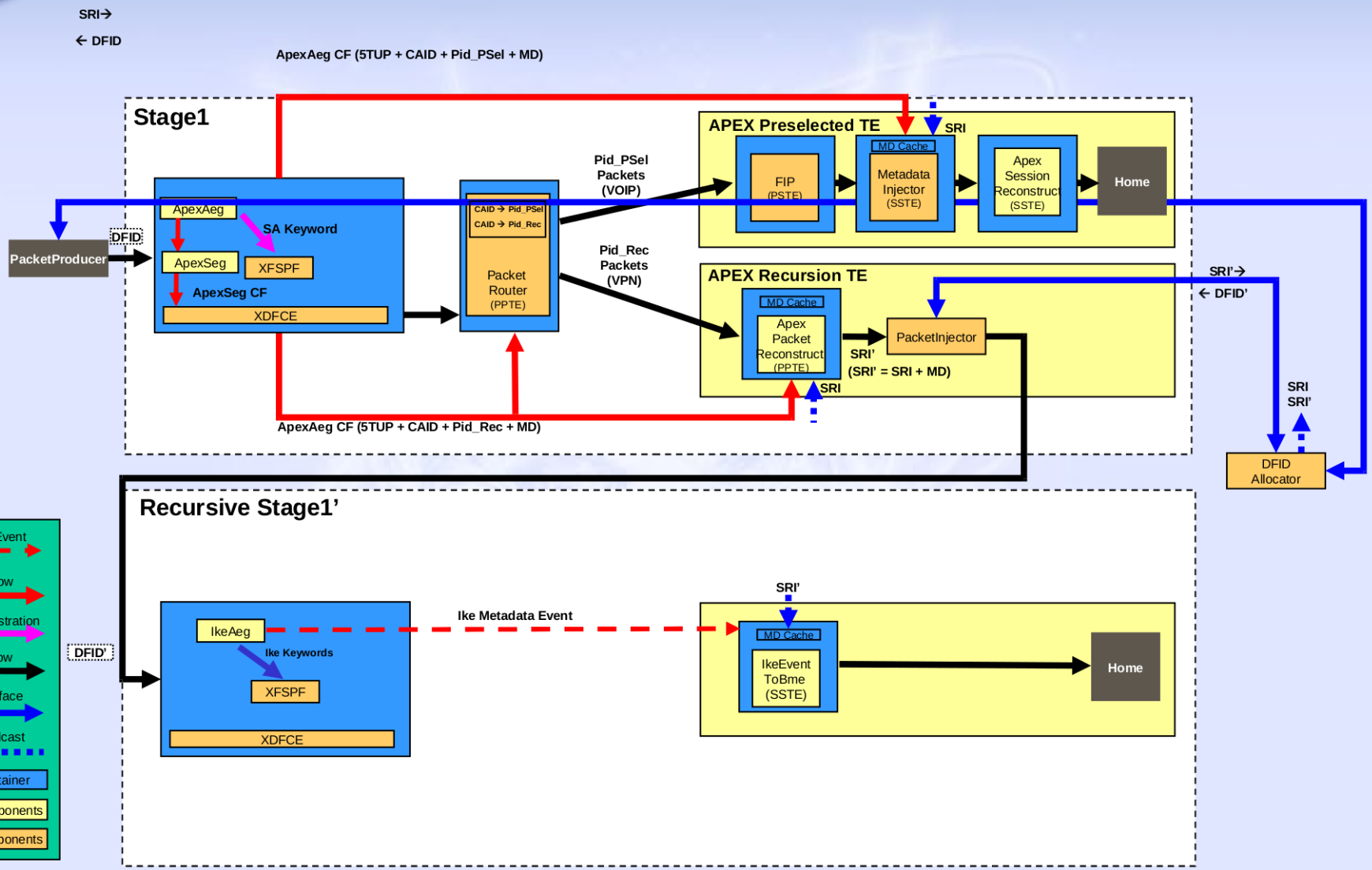
TURMOIL Stage 1 Metadata Processor



TURMOIL Stage 1 VPN TE



APEX Spin 15 Design

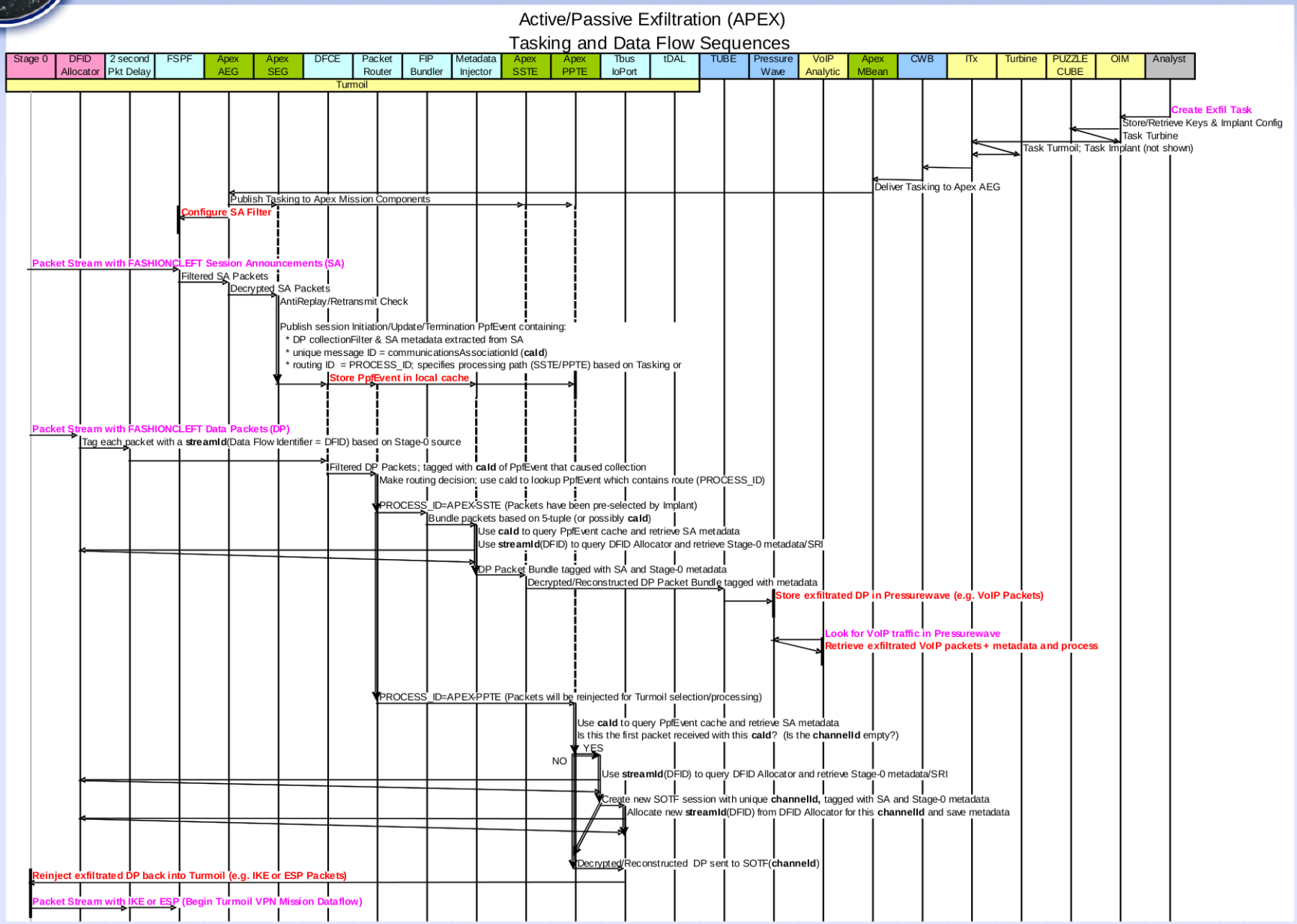


Complexity

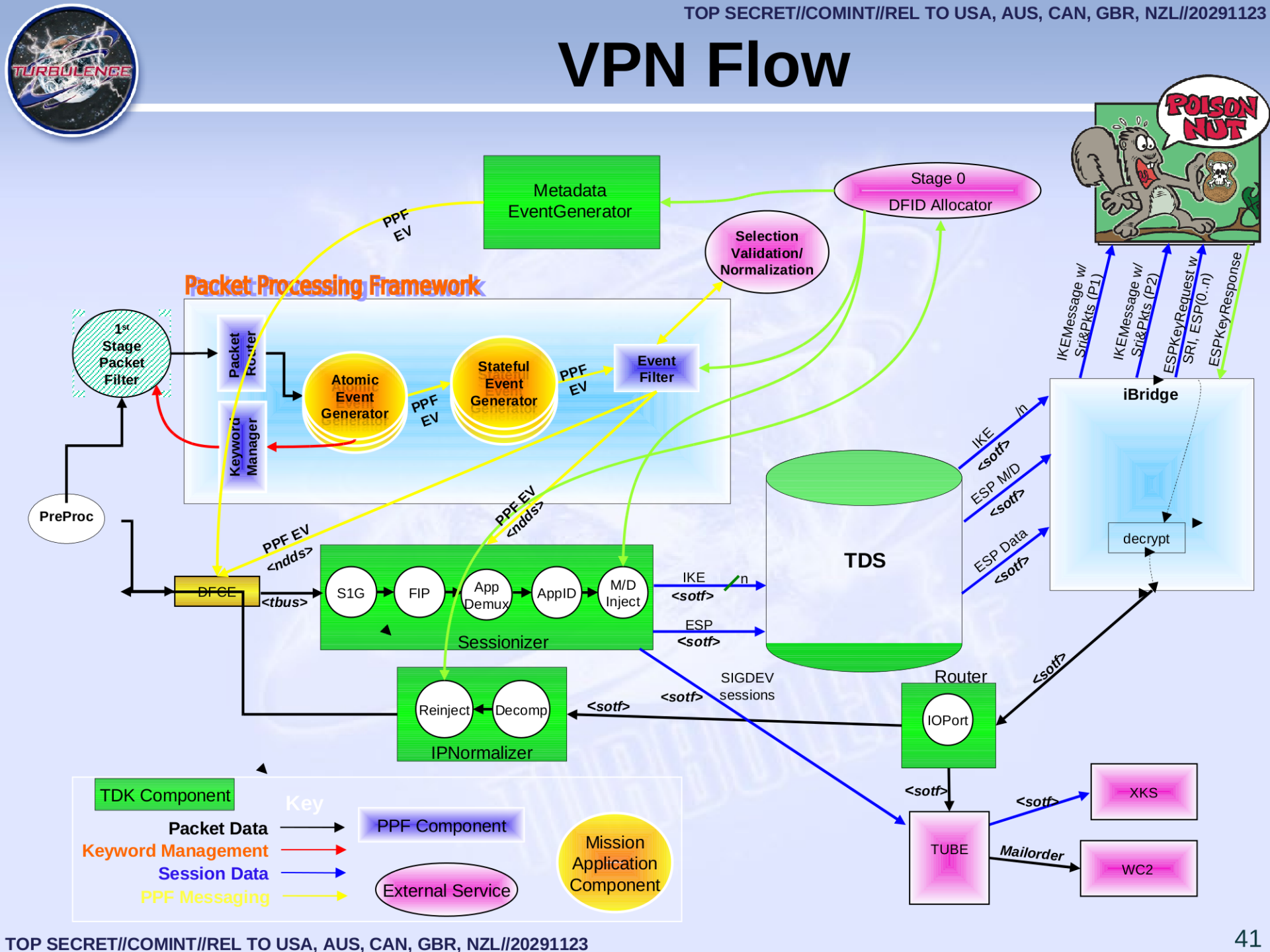
Complexity

- APEX Sequence Diagram
  - Tasking
    - Look for: FASHIONCLEFT Session Announcements.
  - Recognize SA
    - Look for: FASHIONCLEFT Data Packets
  - Recognize DP
    - Route DP to Bundling or Packet Reinjection TE
    - Reconstruct, Attach Metadata, Output/Reinject
- VPN Dataflow & Sequence Diagram
  - Recognize VPN IKE Packets
    - Send all IKE Metadata to CES TOYGRIPPE database
    - Send targeted IKE to CES POISON NUT for VPN key recovery.
  - Recognize VPN ESP Packets
    - Save targeted ESP in *big* buffer and request VPN key from CES.
    - If receive VPN key, decrypt and Reinject.

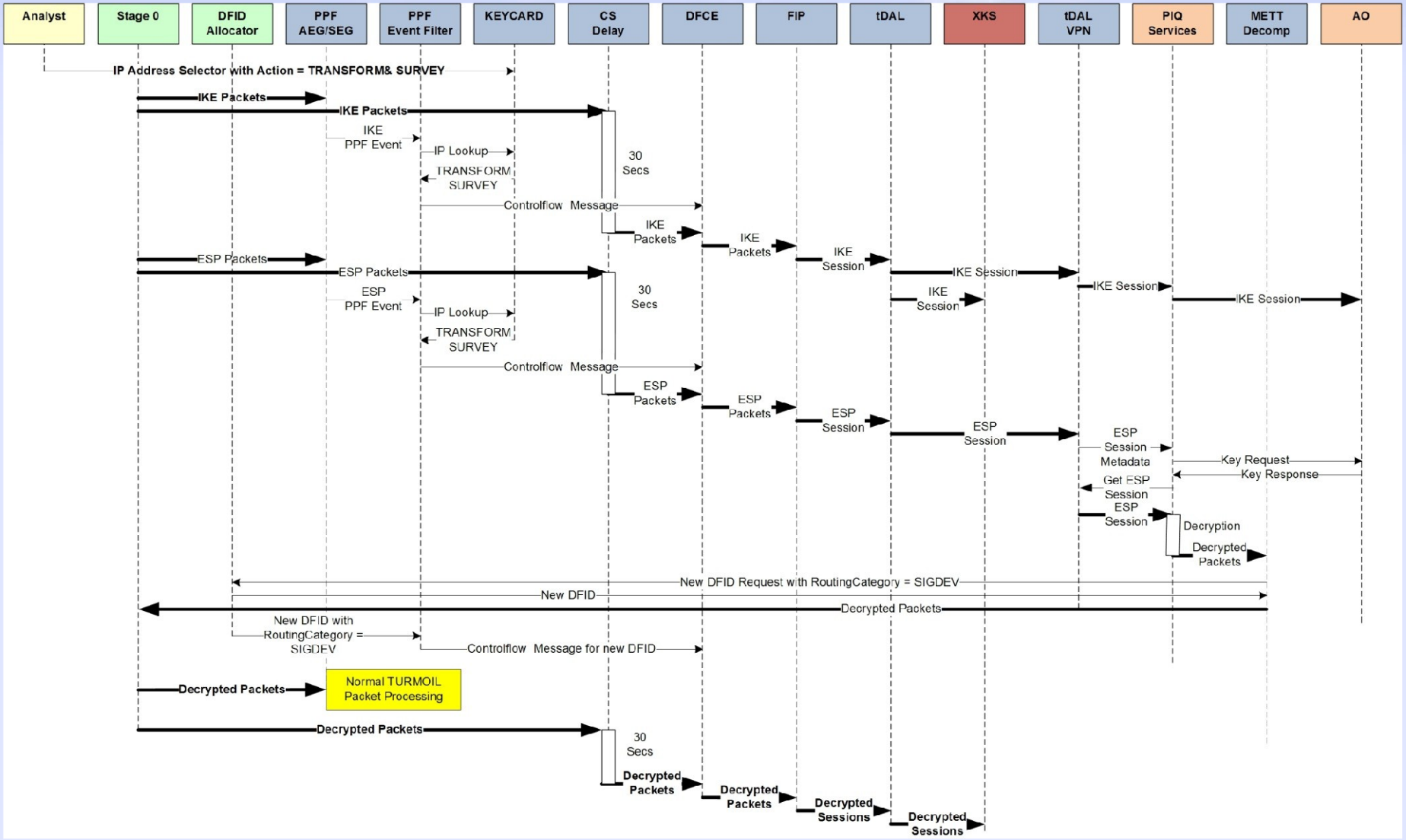
APEX Tasking & Data Flow Sequences



VPN Flow


Metadata EventGenerator
Stage 0
DFID Allocator
Selection Validation/ Normalization
POISON NUT
Packet Processing Framework
1st Stage Packet Filter
Packet Router
Atomic Event Generator
Stateful Event Generator
Event Filter
Keyword Manager
PPF EV
IKEMessage w/ Sri&Pkts (P1)
IKEMessage w/ Sri&Pkts (P2)
ESPKeyRequest w/ SRI, ESP(0..n)
ESPKeyResponse
iBridge
decrypt
PreProc
DFCE
<tbus>
<ndds>
S1G
FIP
App Demux
AppID
M/D Inject
Sessionizer
IKE
ESP
<sotf>
TDS
IKE In
ESP M/D
ESP Data
Router
IOPort
SIGDEV sessions
Reinject
Decomp
IPNormalizer
TUBE
XKS
WC2
Mailorder
Key
TDK Component
Packet Data
Keyword Management
Session Data
PPF Messaging
PPF Component
External Service
Mission Application Component

VPN Decrypt Sequence Diagram



Challenges

Challenges

- SIGDEV
  - Find target networks/devices with desired traffic.
    - TAO/R&T
  - Exfiltration path discovery from device to Turmoil.
    - COALSHOVEL
- End-to-End Metadata & Processing
  - Provide CES with appropriate metadata for VPN mission.
  - Provide TUBE/PRESSUREWAVE with appropriate metadata for VoIP analytic.
  - Two Case Notations:
    - Link collected by Active Implant: “new” agentCaseNotation
    - Link collected by Passive System: “current” caseNotation.

Challenges

- Classification & Legal Authority
  - Some TAO implants/accesses are compartmented.
    - *The highest priority VPNs are likely on compartmented accesses.*
  - We'd like to exfil packets to high-bandwidth SSO sites
    - *Ensure compliance with FISA / FAA / PAA / USSID SP0018.*

- Future Automation
  - Turbine tasks both Active & Passive collectors
  - Automated Path Discovery
  - Dynamically task Active system using Passive selectors
    - Exfil VoIP signaling to Turmoil for selection:
      - task selected calls for exfil.
    - Exfil VPN ESP tunnel starts to Turmoil for selection:
      - task exploitable tunnels for exfil.
    - Apply automated OPSEC policy to manage exfil bandwidth & CPU utilization on implanted device.

APEX Phased Development

- Command & Control
- VPN
- VoIP

APEX Command & Control Phases

- **C&C Phase 1:** Manual Configuration (Spin 15)
  - HAMMERMILL is configured via existing command interface.
  - Simultaneously TURMOIL APEX is provided a configuration file for this HAMMERMILL mission.
  - A human is responsible for keeping the two in sync.

- **C&C Phase 2:** Semi-automatic Configuration
  - TURBINE receives mission parameters and automatically configures both the HAMMERMILL implant and the TURMOIL APEX components.
  - TURBINE-HAMMERMILL interface uses CHIMNEYPOOL RPC commands and requires HAMMERMILL version 2.5.
  - TURBINE-TURMOIL interface uses ISLANDTRANSPORT.

- **C&C Phase 3:** Dynamic Targeting
  - TURBINE sets initial configuration as in Phase 2.
  - Exfiled traffic is evaluated by TURMOIL components+KEYCARD for selection decisions.
  - TURMOIL messages to TURBINE to dynamically target a particular flow through the implant.
  - Example:
    - TURMOIL receives an IKE key exchange (and possibly a few initial packets)
    - TURMOIL evaluates the IP addresses to decide if the VPN being set up corresponds to a target
    - If so, TURMOIL message to HAMMERMILL via TURBINE to capture/exfil corresponding ESP traffic.
  - This phase must be managed so that router exfil does not exceed the tolerable bandwidth limits set by OPSEC and operational concerns. TURBINE may need to implement additional workflows to monitor and control exfil volume.

Tasking ICF (Implant Control File)

```
#  TEST-APEX-1 INFRASTRUCTURE CONFIGURATION FILE
ICF_NAME        TEST-APEX-1
ICF_DTG         Wed Jan 28 14:38:59 2009
ICF_INFO        Test ICF for Apex Development
IMPLANT_ID      0x0001
IMPLANT_VER     1
TARGET_ID       0x00000002
DEPLOYMENT_ID   0x00000003
TARGET_CN       TESTTECHNIQUE_TESTHOST
TARGET_IP       10.0.0.1
TARGET_HOST     TESTHOST
#
# IMPLANT_LP[1-9]  [<Tunnel-Id>:]<ip-address>[:port(s)]
# Tunnel-Id: 1-TCP_Redir, 2-Fashioncleft, 3-HTTP_BT_S, 4-UDP_S
# ./genkey -l 128
IMPLANT_LP1     2:10.1.1.2:10002
IMPLANT_RC6_CV1 5366fbe1 7f7a05fd 33d66a6f 3581de48
#
IMPLANT_RSA_INF
RSANAME TEST_APEX_INF_KEY-1
RSAINFO Wed Jan 28 14:38:59 2009, [redacted] ./rsagenkey v2.0
RSASIZE 1024
RSAMOD 32
  0xdb532e9d, 0x93c792fc, 0x4459fc40, 0x07744c65, ...
RSAMU 33 ...
RSAPRIV 32 ...
RSAPUB 32 ...
#
IMPLANT_RSA_IMP
RSANAME TEST_APEX_IMP_KEY-1
...
```

Tasking XML (FlashHandle Mission Manager)

```
<?xml version="1.0" encoding="UTF-8"?>
<dci>
    <header>
        <fullyQualifiedId>
            <protocol>
                <protocolName>FN</protocolName>
                <protocolVersion>2.0</protocolVersion>
            </protocol>
            <targetId>2</targetId>
            <techniqueId>1</techniqueId>
            <techniqueVersion>1</techniqueVersion>
            <instanceId>0</instanceId>
        </fullyQualifiedId>
        <configurationVersion>2</configurationVersion>
        <revisionDate>2009-01-30T12:19:05.910-05:00</revisionDate>
    </header>
    <commands>
        <command name="fogynullControls" identifier="FN_CONTROL">
            <parameters>
                <parameter name="replayPrevent">1</parameter>
                <parameter name="historyLimit">100</parameter>
                <parameter name="antiDelay">0</parameter>
                <parameter name="timeWindow">1800</parameter>
            </parameters>
        </command>
        <command name="implantLp" identifier="IMPLANT_LP">
            <parameters>
                <parameter name="tunnelId">2</parameter>
                <parameter name="ip">10.1.1.2</parameter>
                <parameter name="port">10002</parameter>
            </parameters>
        </command>...
```

Tasking XML (Turbine → ITx → Turmoil)

```
<?xml version="1.0" encoding="UTF-8"?>
<task:message schemaVersion="1.0" xmlns:task="urn://control.exo/TaskingInterface/v1">
    <task:taskAdd>
        <task:msgUuid>00110000-1111-2222-3333-444455556666</task:msgUuid>
        <task:timestamp>2</task:timestamp>
        <sessionConfigTask>
            <taskSecurityMarking classification="TS" coi="COMINT" disseminationControls="REL"
                sCIcontrols="SI" releasableTo="USA AUS CAN GBR NZL" legalAuthority="RAWSIGINT" />
            <header> ... </header>
            <commands>
                <fogynullControls>
                    <replayPrevent>1</replayPrevent>
                    <historyLimit>100</historyLimit>
                    <antiDelay>0</antiDelay>
                    <timeWindow>1800</timeWindow>
                </fogynullControls>
                <apexControls>
                    <taskUuid>00010001-1111-2222-3333-444455556666</taskUuid>
                    <agentUuid>80010001-1111-2222-3333-444455556666</agentUuid>
                    <agentCaseNotation>UA.AAABBBCCCMM1</agentCaseNotation>
                    <processingMode>Reinject</processingMode>
                </apexControls>
                <implantLp>
                    <tunnelId>2</tunnelId>
                    <ip>10.1.1.2</ip>
                    <port>10002</port>
                </implantLp>
            </command>...
```

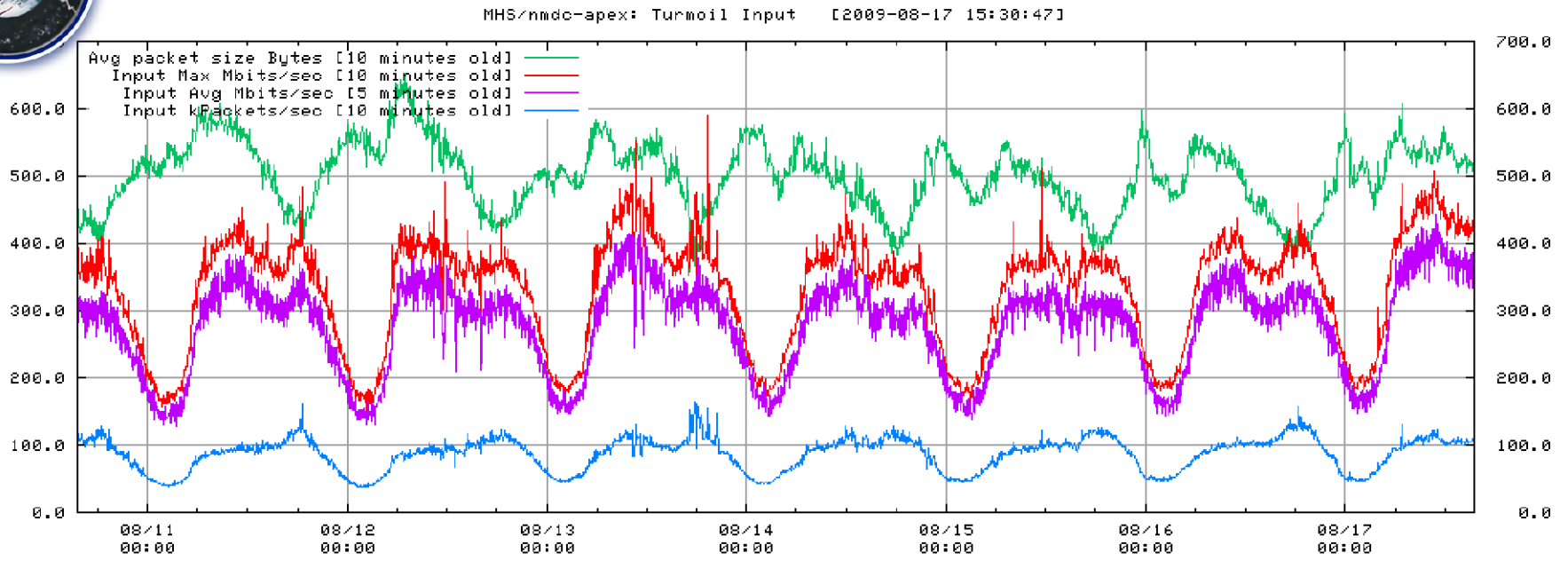
APEX VPN Phases

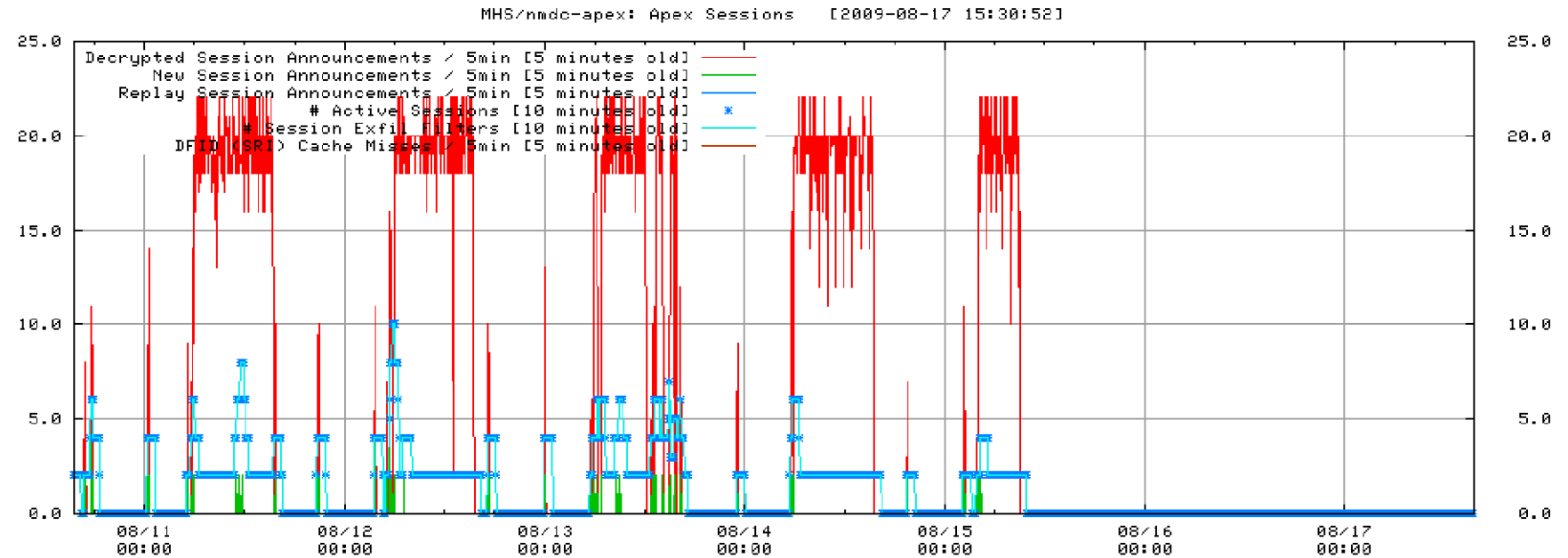
- **VPN Phase 1:** IKE Metadata Only (Spin 15)
  - IKE packets are exfiled to TURMOIL APEX.
  - APEX reconstructs/reinjects IKE packets to the TURMOIL VPN components.
  - TURMOIL VPN extracts metadata from each key exchange and sends to the CES TOYGRIPPE metadata database. This database is used by SIGDEV analysts to identify potential targets for further exploitation.
- **VPN Phase 2:** Targeted IKE Forwarding (Spin 15)
  - TURMOIL VPN looks up IKE packet IP addresses in KEYCARD.
  - If either IP address is targeted, the key exchange packets are forwarded to the CES Attack Orchestrator (POISON NUT) for VPN key recovery.
- **VPN Phase 3:** Static Tasking of ESP
  - HAMMERSTEIN receives static tasking to exfil targeted ESP packets.
  - APEX reconstructs/reinjects ESP packets to the TURMOIL VPN components.
  - TURMOIL VPN requests VPN key from CES and attempts decryption.
- **VPN Phase 4:** Dynamic Targeting of ESP
  - Based on the value returned by KEYCARD, the ESP for a particular VPN may be targeted as well.
  - TURMOIL sends to HAMMERSTEIN (via TURBINE) the parameters for capturing the ESP for the targeted VPN.

APEX VoIP Phases

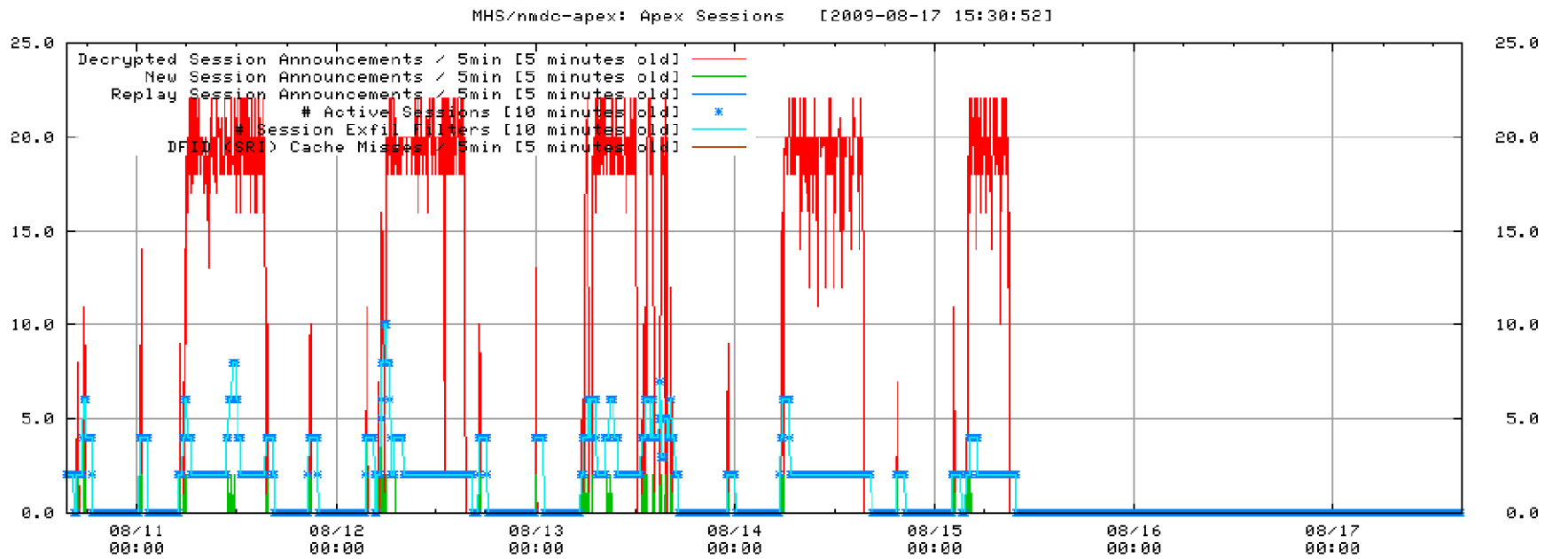
- **VoIP Phase 1:** Static Tasking of VoIP (Spin 16)
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates only targeted VoIP RTP sessions to TURMOIL.
  - APEX reconstructs and bundles the voice packets into a file, attaches appropriate metadata, and delivers to PRESSUREWAVE.
  - This triggers a modified VoIP analytic to prepare the VoIP for corporate delivery.
- **VoIP Phase 2.** VoIP Call Survey
  - HAMMERCHANT monitors VoIP SIP/H.323 signaling and exfiltrates all call signaling metadata to TURMOIL.
  - APEX inserts call signaling metadata into an ASDF record and publishes it to the TURMOIL AsdfReporter component for target SIGDEV.
- **VoIP Phase 3.** Dynamic Targeting of VoIP
  - HAMMERSTEIN captures/exfils all VoIP signaling
  - APEX reconstructs/reinjects the signaling to the TURMOIL VoIP components.
  - TURMOIL VoIP extracts call metadata and sends to FASCIA; checks KEYCARD for hits.
  - If called/calling party is targeted for active exfil, then TURMOIL sends to HAMMERSTEIN (via TURBINIE) the parameters to capture the targeted RTP session.
- Implementation of VoIP Phase 2 and 3 will be driven by mission need.
  - Phase 3 leverages all TURMOIL VoIP signaling protocol processors to expand beyond SIP and H.323 (e.g. Skype) without additional development on the implant.

Performance & Status Metrics





Performance & Status Metrics



Questions?

"go apex"

apex chat room on LINKUP

[redacted]

STDP: S32354 & T111, NCSC/C91

[redacted]