RE: Route Engine

* NSD: Network security daemon
* LSYSD: Logic system Daemon
* NStraced
* RPD: Routing Process Daemon

SPC: Security Process Card

SPU: Security Process Unit

PFE: Packet Forward Engine

CP: Central Point

* DCP: distribute central point
* APP-CP: application central point

IOC: Input Output Card

* NP

Session

* Flow session
* DCP session
* NP session

Session Key

* Source address
* Destination address
* Source port
* Destination port
* Protocol
* Session token (Zone ID plus VR ID）

First path

Fast path

Architecture:

APP-CP

RE

IOC

DCP

PFE

DCP

PFE

DCP

PFE

First Path:

APP-CP

RE

5

4 6

IOC

2

DCP2

PFE2

DCP3

PFE3

DCP1

PFE1

3,10

12 7 8.9

1 11 8

1: Pkt received in IOC

1. no **NP session**, forward to DCP based on Hash, supposing DCP1
2. No **DCP session**, create pending DCP session, queue the packet,

DCP session: Pending

DCP

S2C

C2S

1. send query message to APP-CP
2. App-CP do rate limit, gate/application lookup & determine which PFE should process the packet. By defauly, the local PFE will be selected.
3. APP-CP send query response to DCP1
4. DCP1 forward the packet to session SPU, supposing PFE1
5. PFE1 do SPU session lookup. No SPU session. Go first path to create SPU session
   1. Do ip-action
   2. Screen
   3. Create session

SPU session: Pending

SPU

S2C

C2S

* 1. Destination NAT
  2. Route lookup
  3. Policy lookup & session-init log
  4. Source NAT (pending packet here in case we need allocate NAT resource from App-CP)
  5. Service check
  6. Install CP session

1. DCP: update S2C wing, change session to VALID,
2. Send DCP session install ACK back to PFE1
3. On Receiving ACK, PFE1 will change SPU session from PENDING to VALID. Install NP session
4. Forward the packet out

Fast Path:

APP-CP

RE

IOC

DCP2

PFE2

DCP3

PFE3

DCP1

PFE1

2

4

1 3

1: Pkt received in IOC

1. Find NP session. Forward the pkt to PFE1 according to NP session
2. Do flow past process process according to SPU session matched
   1. TTL
   2. TCP process
   3. NAT
   4. Service process (ALG, UTM, GTP/SCTP, UserFW, AppFW, Dyn-app, Fwauth, etc)
3. Forward the packet out via IOC