

# MX Edge Security Solution for Cloud, Mobility & Wireline Providers

Eric Sandoval

Chief Network Security Architect – Cloud, Mobility, Wireline

# LEGAL DISCLAIMER

This statement of direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

This presentation contains proprietary roadmap information and should not be discussed or shared without a signed non-disclosure agreement (NDA).

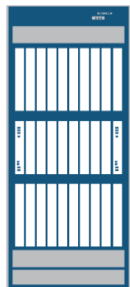
# Agenda

- Common large Provider deployment Issues
  - NOT for Small or Medium Enterprise type deployments
- MS-MPC (2<sup>nd</sup> Generation)
- NPU (Network Processing Unit) Load Balancing
- Packet Walk Through
- Customer X & Y Traffic Profile
- Multi-dimensional Scale Test Results
- HA Inter-Chassis Clustering
- DDOS Enhancement
- Command and Control
- Application Awareness
- Use Cases

# Common Firewall Production Issues

- Scaling of Firewall
  - IPv4 Stateful Firewall + NAT
  - IPv6, Stateful Firewall
- Packets Per Second (PPS)
- CPS
- Sessions
- ISSU
- HA with Fast Convergence
- Future Proofing Platform

# NEXT GEN SERVICES BLADE MS-MIC/ MS-MPC



MX2020



MX2010



MX960



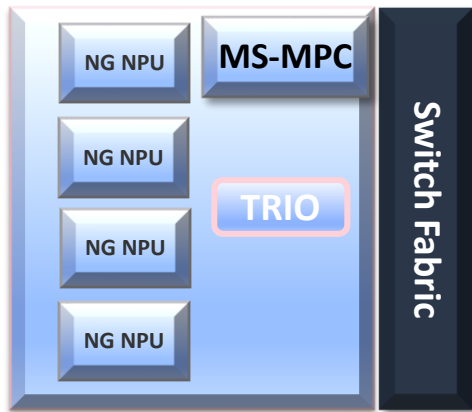
MX480



MX240



MX104



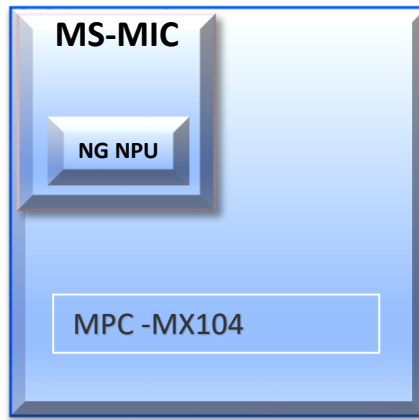
## Services – (SFW, NAT, IPSEC, IDP)

### MS-MPC

- SFW 37G IMIX / Card
- IPSEC 21G IMIX / Card
- Sessions 60M / Card
- CPS 560k / Card, Linear scale

### MS-MIC

- SFW 7G IMIX
- IPSEC 3.4G IMIX
- Sessions 7M
- CPS 390k



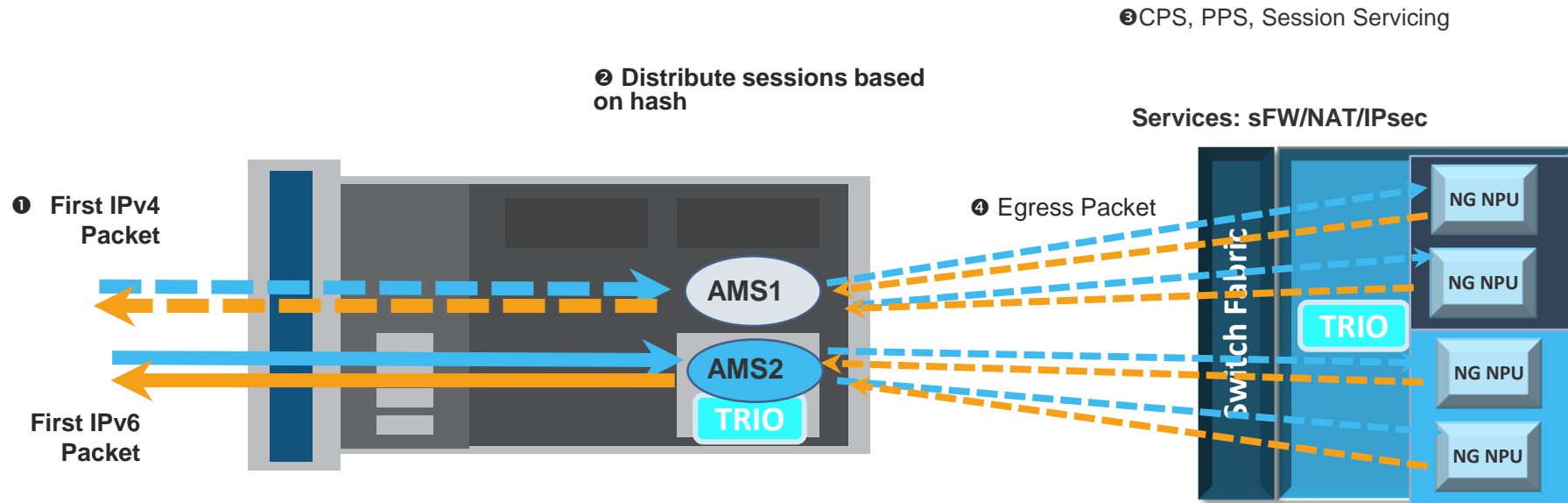
# NPU Load Balancing Sessions

- AMS (Aggregated MultiServices)
  - Grouping of NPU in which to be load-balanced
  - Group NPU in any combination
    - Intra Card or Inter Card

Example: 2x AMS groups across 8 MS-MPC cards



# MX/MS-MPC DATA PLANE – PACKET FLOW



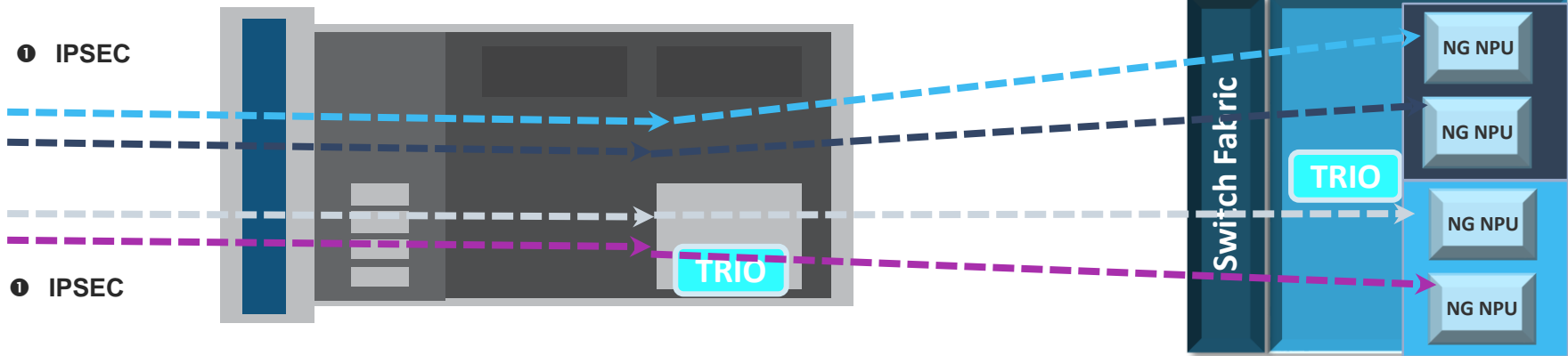
# MX/MS-MPC DATA PLANE – PACKET FLOW

IPSec remote IKE Gateways

- Known remote IP address (static)
- Unknown (DEP)

CPS, PPS, Session Servicing  
**Encryption/Decryption**

Services: sFW/NAT/IPsec





# Customer X Year 2020 Expected Traffic Profile

- 640 Byte average TCP packet size
- 300G of traffic
  - 50% IPv4 + NAT
  - 5% IPv4 without NAT
  - 45% IPv6 no NAT
- 150M Session
- 60M PPS
- 400K CPS
- Cone NAT on 2% of IPv4 traffic

# Customer Y Current Test Traffic Profile

- 100M sessions at a minimum.
- 1M CPS
- 200Gbps
- Average packet size is 640Bytes.
- Failover and operational less than 5 seconds
- No loss of sessions

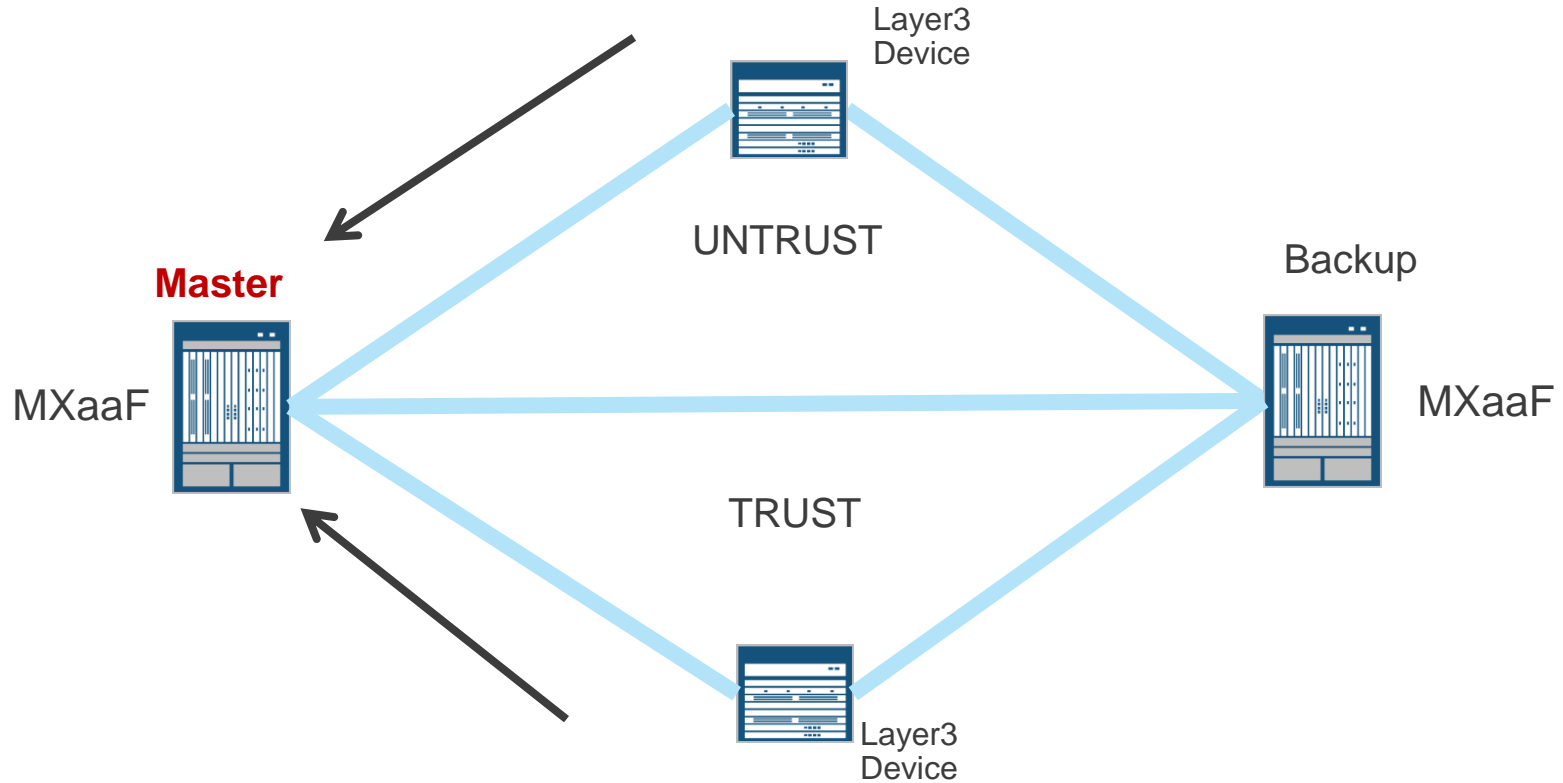
# MX / MS-MPC Scale Testing Achieved IPv4/NAT+v6

- 396Gbps
- 71MPPS
- 168M sessions
- 1.25M CPS
- Average packet size is 640Bytes.
- Very Fast Failover convergence
- No loss of sessions

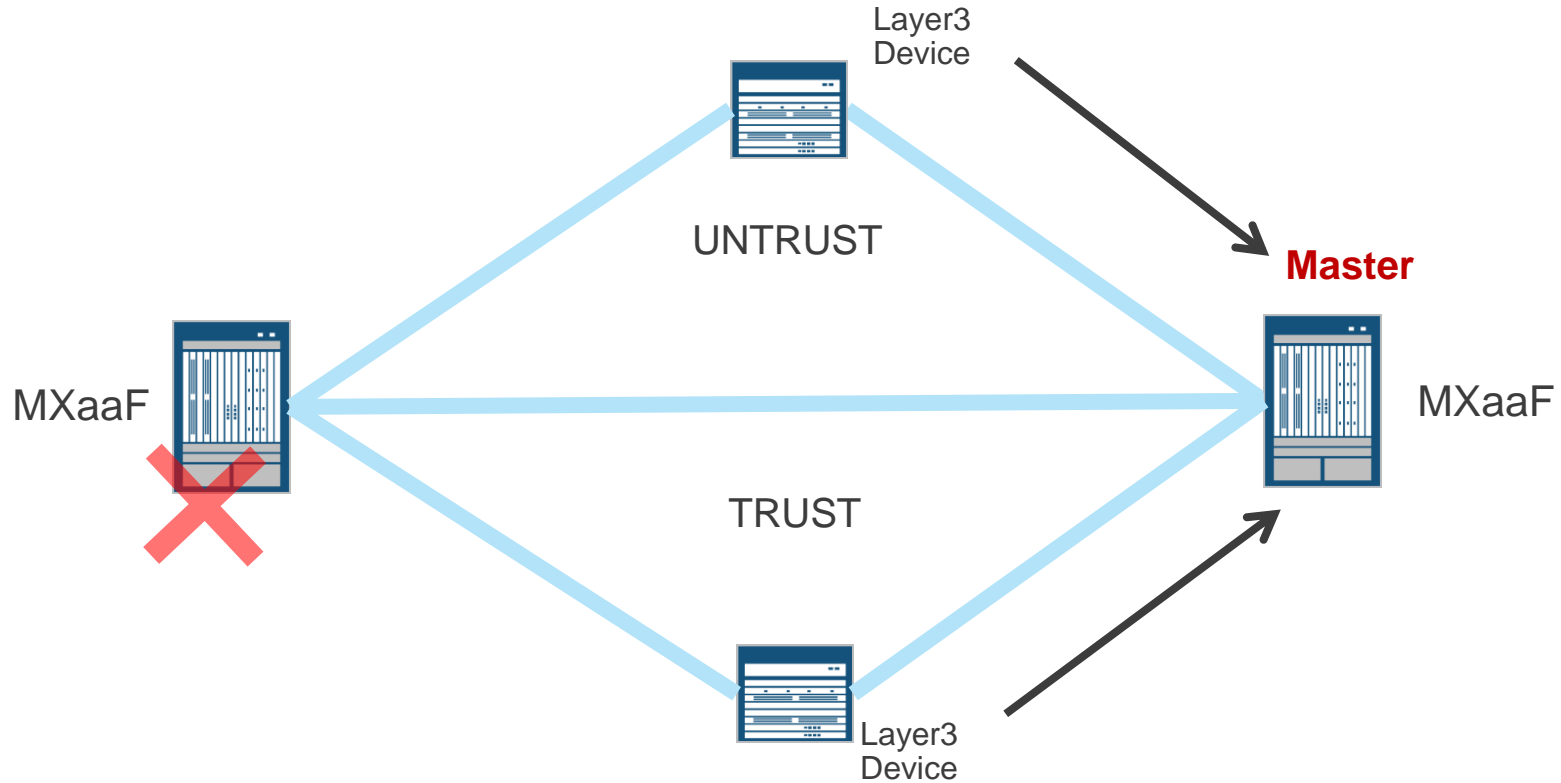


# Stateful High Availability

# Stateful High Availability



# Stateful High Availability



The background is a dark, teal-colored abstract image. It features a central circular structure with concentric rings and a pointed tip, resembling a stylized eye or a network hub. Radiating from this center are numerous curved, wavy lines that create a sense of motion and depth. The overall aesthetic is modern and technological.

# Volumetric DDOS

# MX Multi Stage DDOS Mitigation

PFE stateless filtering



MS-MPC



IDS



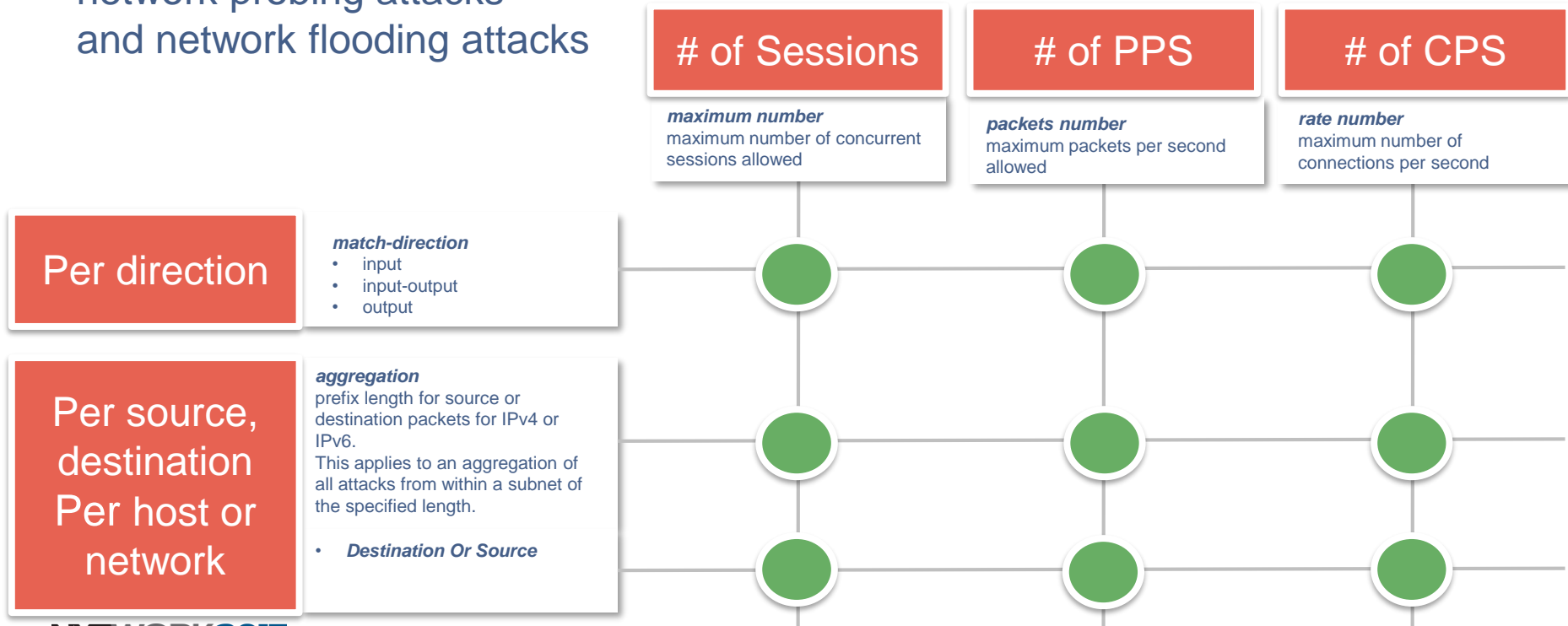
IDS - Dynamic Filter on PFE

- Prevents illegal TCP flags and illegal flag combinations
- Using policer in PFE, allows stateless rate limiting of Packets/sec (per protocol)
- Line rate processing
- CPS rate limiting / CPU threshold at NPU [MS/AMS] level
- Configuring different AMS bundles to isolate attack to single AMS bundle
- Granular level detection & prevention of attacks like Network Probing, Flooding, Header anomalies & Suspicious packet pattern. N;1 or 1:N (#sessions, PPS, Protocol)
- Early Detection of attack traffic on NPU and dynamically install Implicit stateless firewall filter on the PFE
- This filter dynamically gets uninstalled once the attack stops/subsides



# MX Screens - DDoS Customization

You can customize the following IDS rule options for protecting against network probing attacks and network flooding attacks

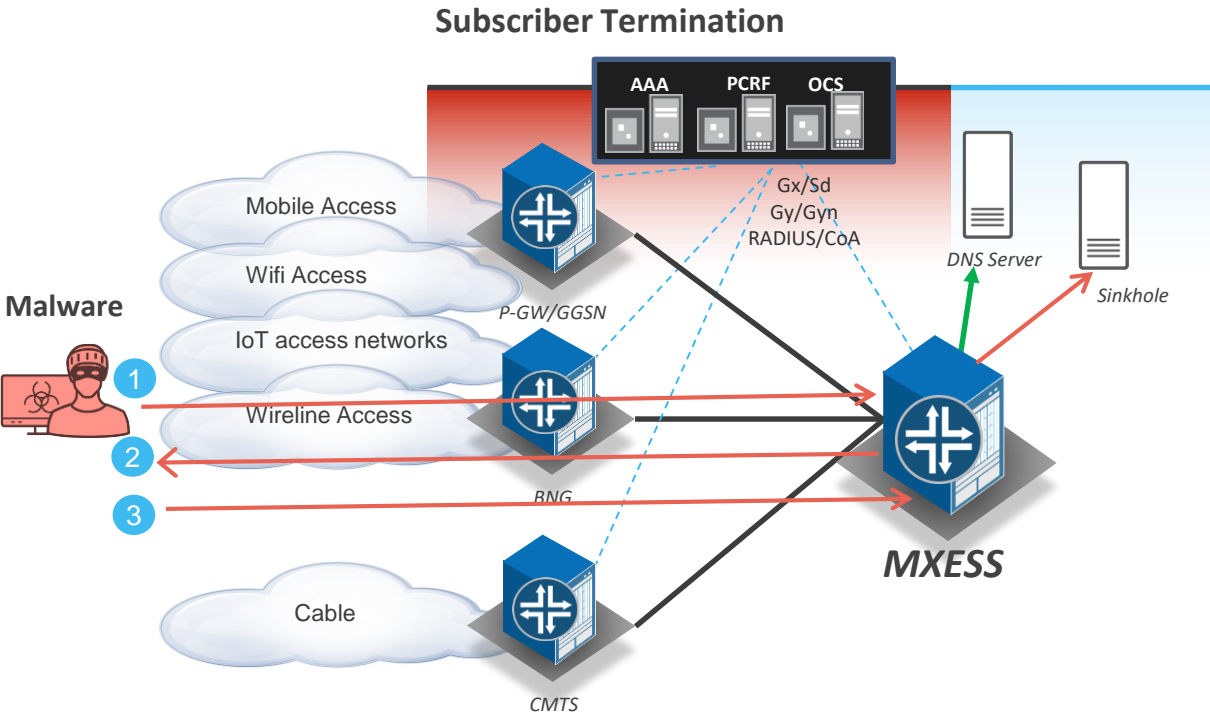




---

# Command and Control

# Command and Control – DNS Sink-Holing



- 1 Compromised host requests for a black-listed domain
- 2 MX intercepts the DNS request and responds with a sink hole IP
- 3 Compromised host's traffic is directed to the sink hole



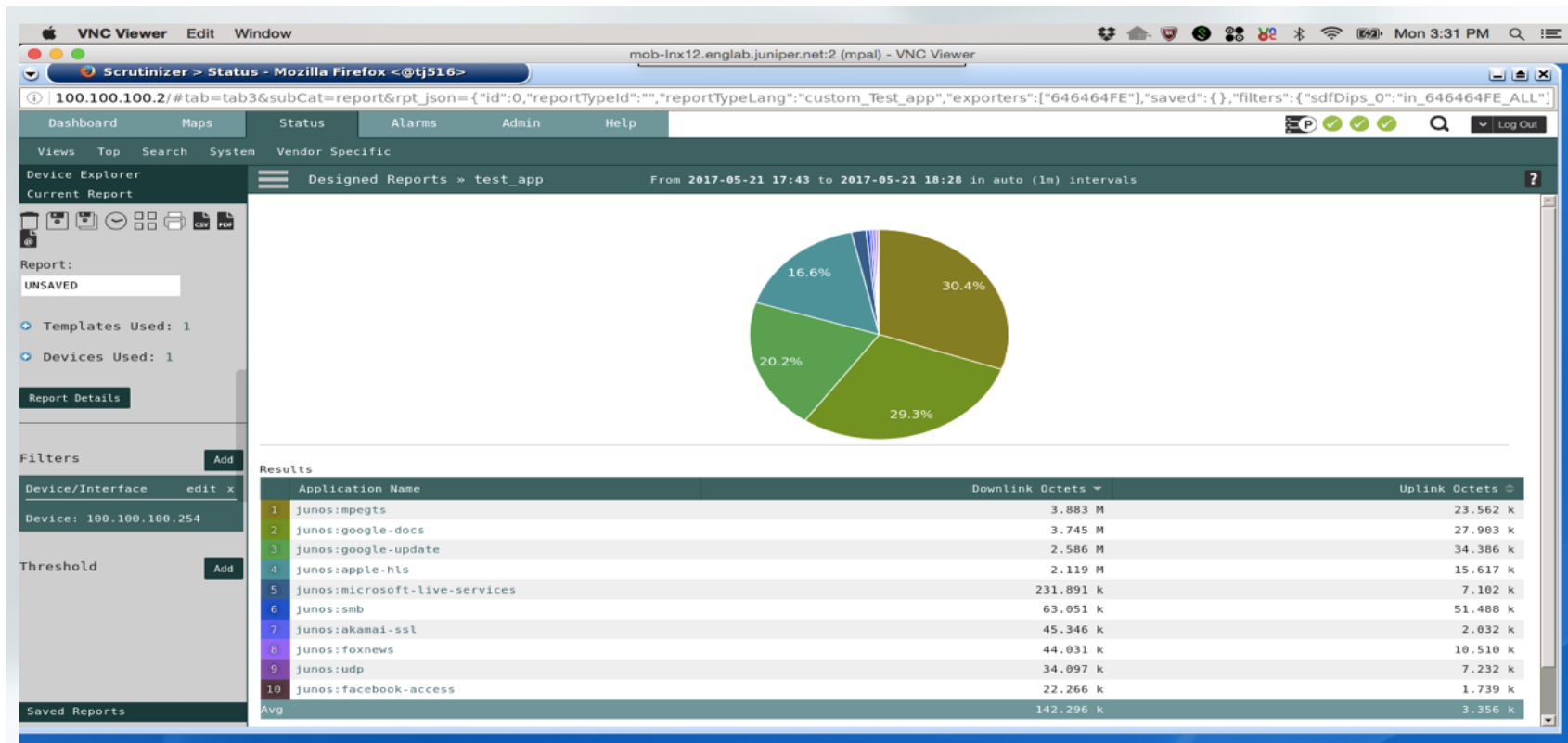
# Application Awareness

# Sample output from MXESS

```
regress@liquidmini> show services application-identification statistics applications
Last Reset: 2017-05-22 15:11:32 PDT
```

Application	Sessions	Bytes
junos:addthis	2	5911
junos:adobe	6	67672
junos:adobe-updater	3	23696
junos:akamai-ssl	20	1230626
junos:amazon	50	7695000
junos:amazon-adsystem	28	117241
junos:amazon-aws	97	9284981
junos:amazon-video	2	22308
junos:aol	1	1481
junos:apple-hls	4	6911796
junos:bing	4	11091
junos:brightcove	6	146243
junos:cloudflare	3	142325
junos:cnn	315	16240170
junos:criteo	12	63765
junos:dns	1793	738089
junos:doubleclick	33	111163
junos:epm	1	1280
junos:facebook-access	26	1744751
junos:foxnews	218	9670562
junos:freewheel	3	3603
junos:google	39	611894
junos:google-accounts	1	7830
junos:google-adservices-ssl	39	592702
junos:google-analytics-tracking	4	41823
junos:google-appengine	23	169659
junos:google-docs	1	3772526
junos:google-static	33	357602
junos:google-syndication	105	1338276
junos:google-update	2	15721085
junos:http	1192	16371935
junos:http-video	4	21946
junos:https	1014	21290725
junos:hulu	20	738712

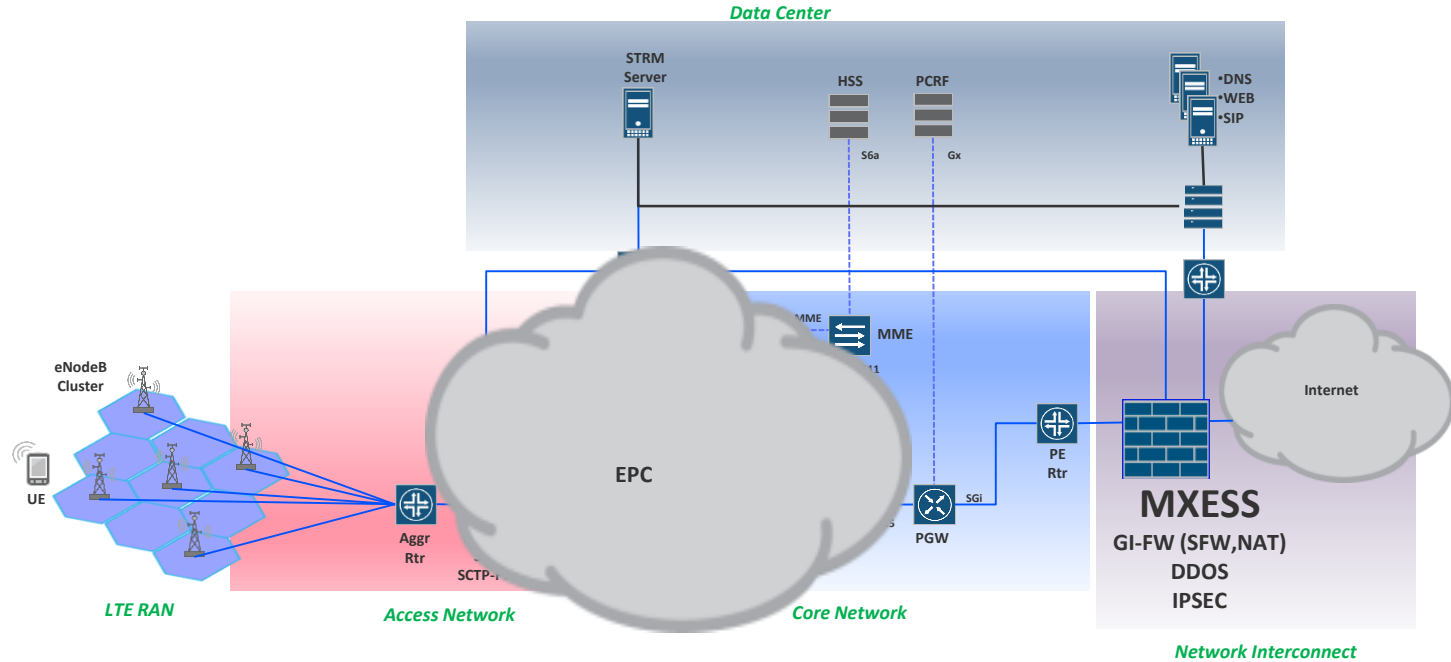
# Reporting



---

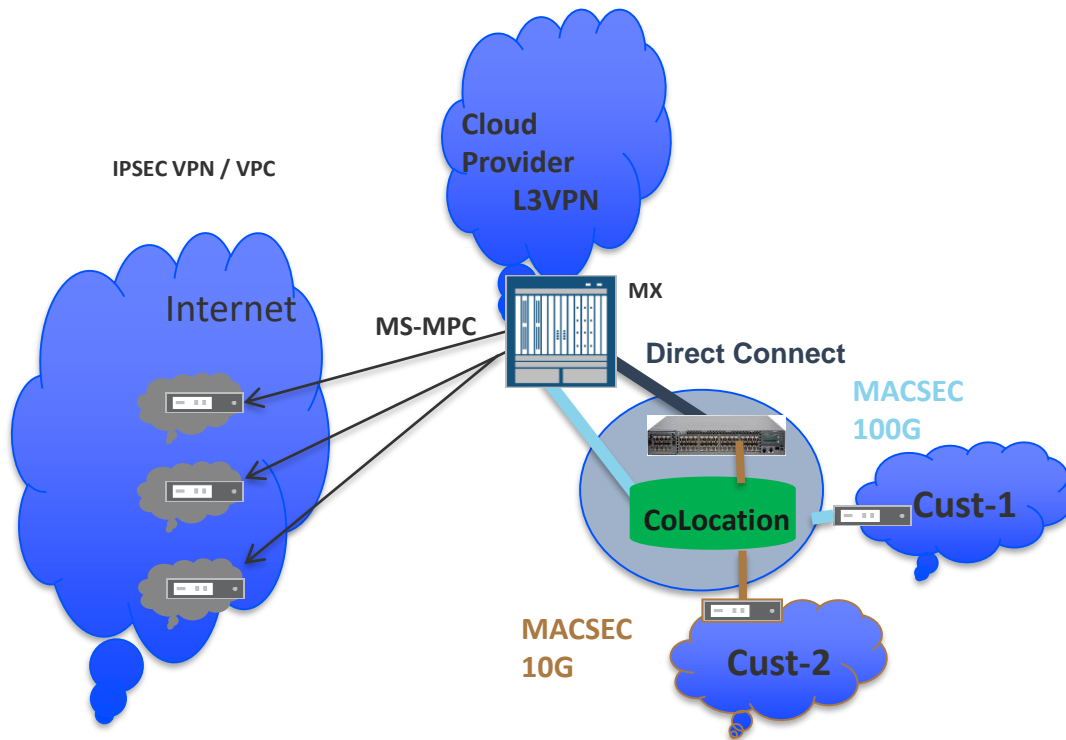
# Use Cases

# LTE Network Security Architecture

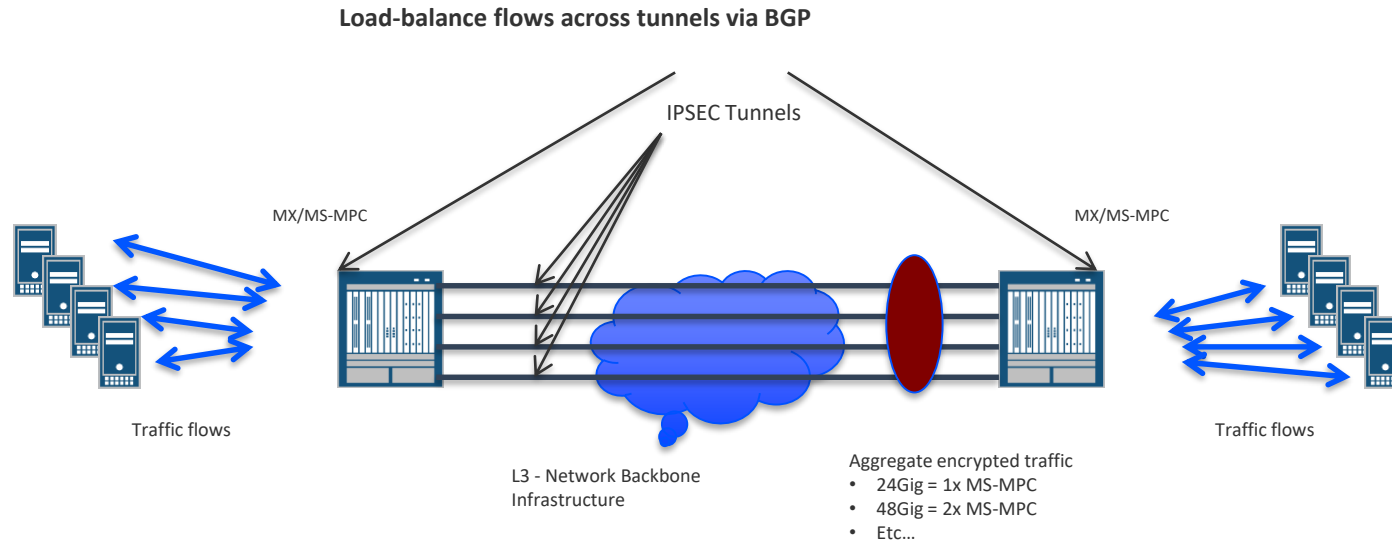




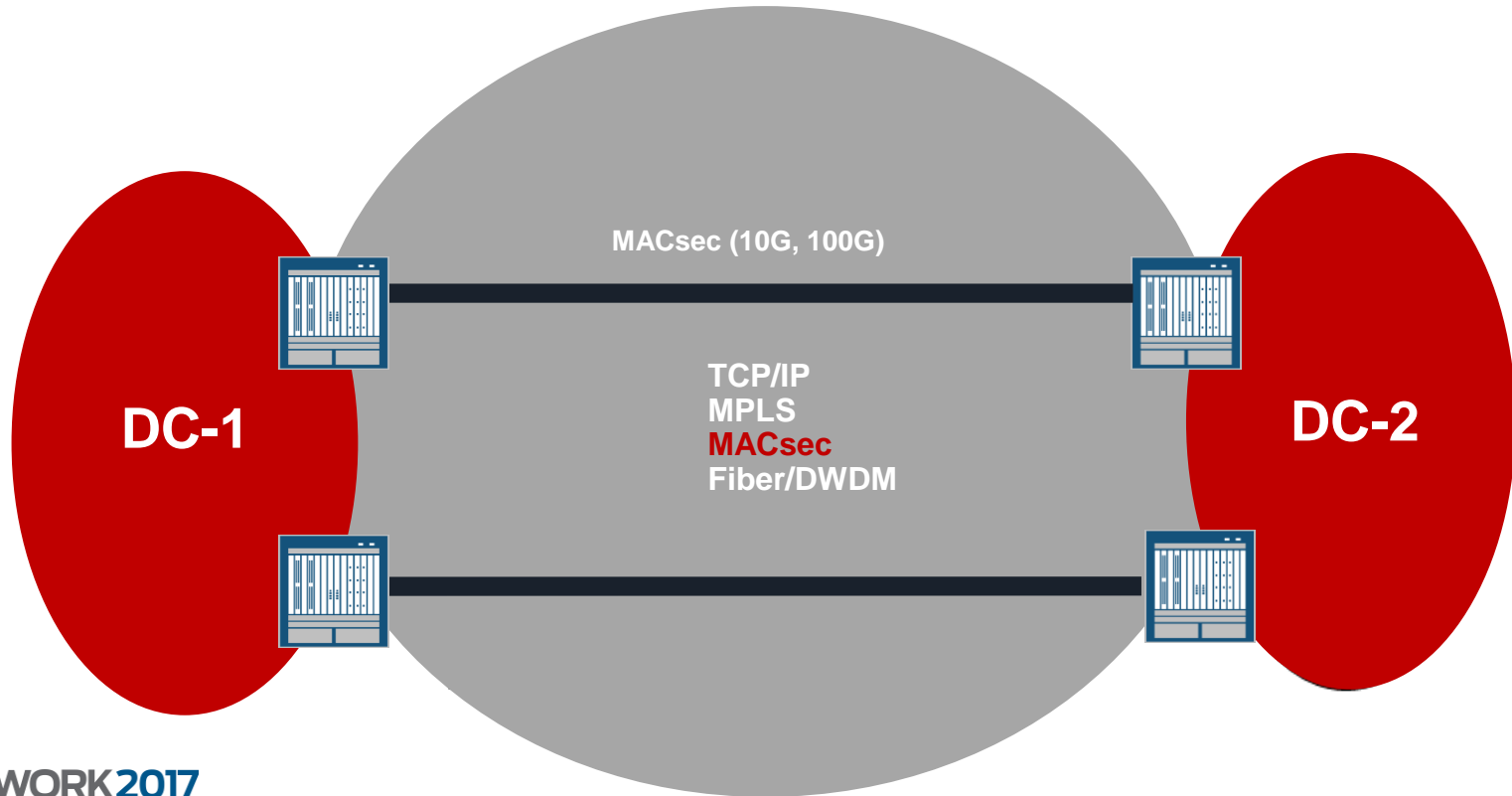
# Cloud Edge Security Services



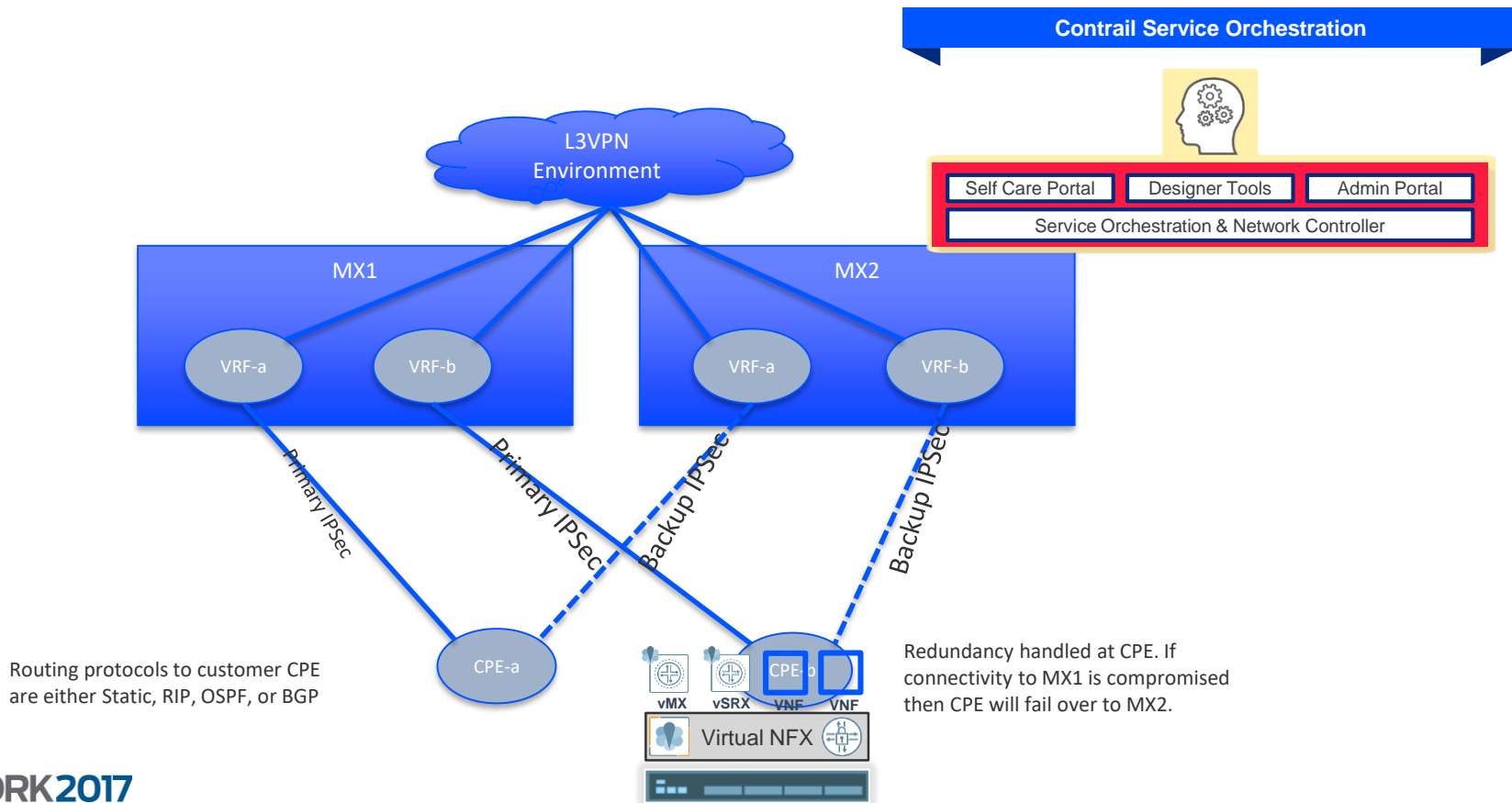
# IPSEC: Juniper Fat-Pipe Solution (MX/MS-MPC)



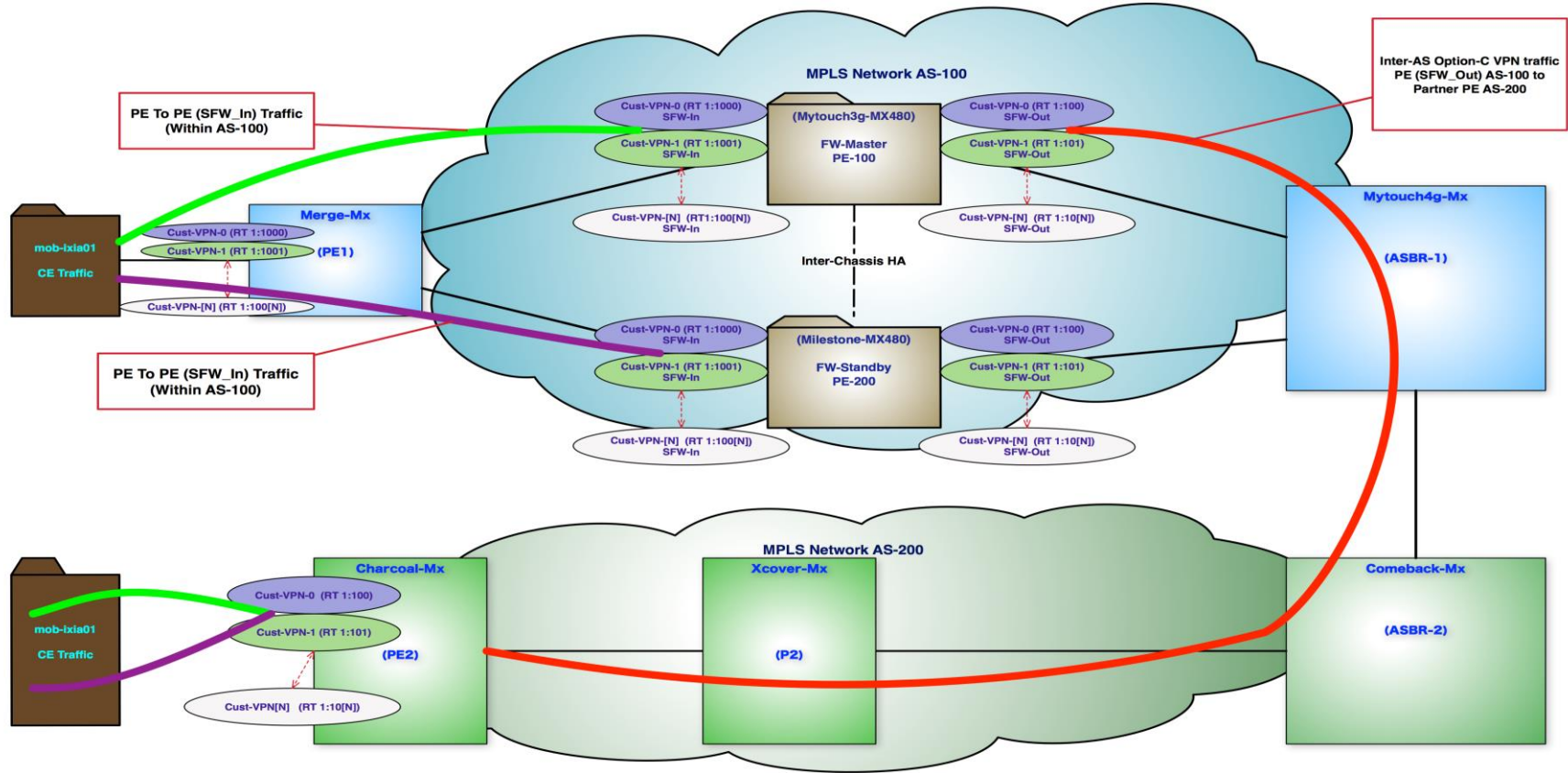
# Data Center to Data Center MACsec Transport



# IPSEC: Dual-homed, Dynamic or Static



# Inter-AS Option C Inline Stateful Firewall + NAT



## 1. Manage both MX and SRX in the same view



















NSM Migration

Update Changes

Resynchronize with Network

Upload Keys

More

	Device Name	IP Address	Connection Status	Managed Status	Platform	Configuration Status	RAM	Device Family
	> 10.213.49.41	10.213.49.41	 up	 SD Changed	VSRX	 In Sync	 	junos-es
	VSRX-10.213.49.25	10.213.49.25	 up	 SD Changed	VSRX	 In Sync	 	junos-es
	brainstorm	10.213.0.195	 up	 SD Changed	MX960	 In Sync	 	junos

0 Selected

1

<

1

of 1

>

Display 50

# Summary

- MESS Leader in Small or Large Scale Performance
- Inline Services enablement .vs. Off-Ramp
- Could Leverage existing MX deployments (Consolidation)
- PROVEN SOLUTION
  - Hardened in the most STRENUOUS Multi Dimensional Networks

# Thank you

