

Campus Firewall Deployment

Steven Bourque

23 January 2014

Hardware

Juniper SRX 3600

SRX3600 SERVICES GATEWAY

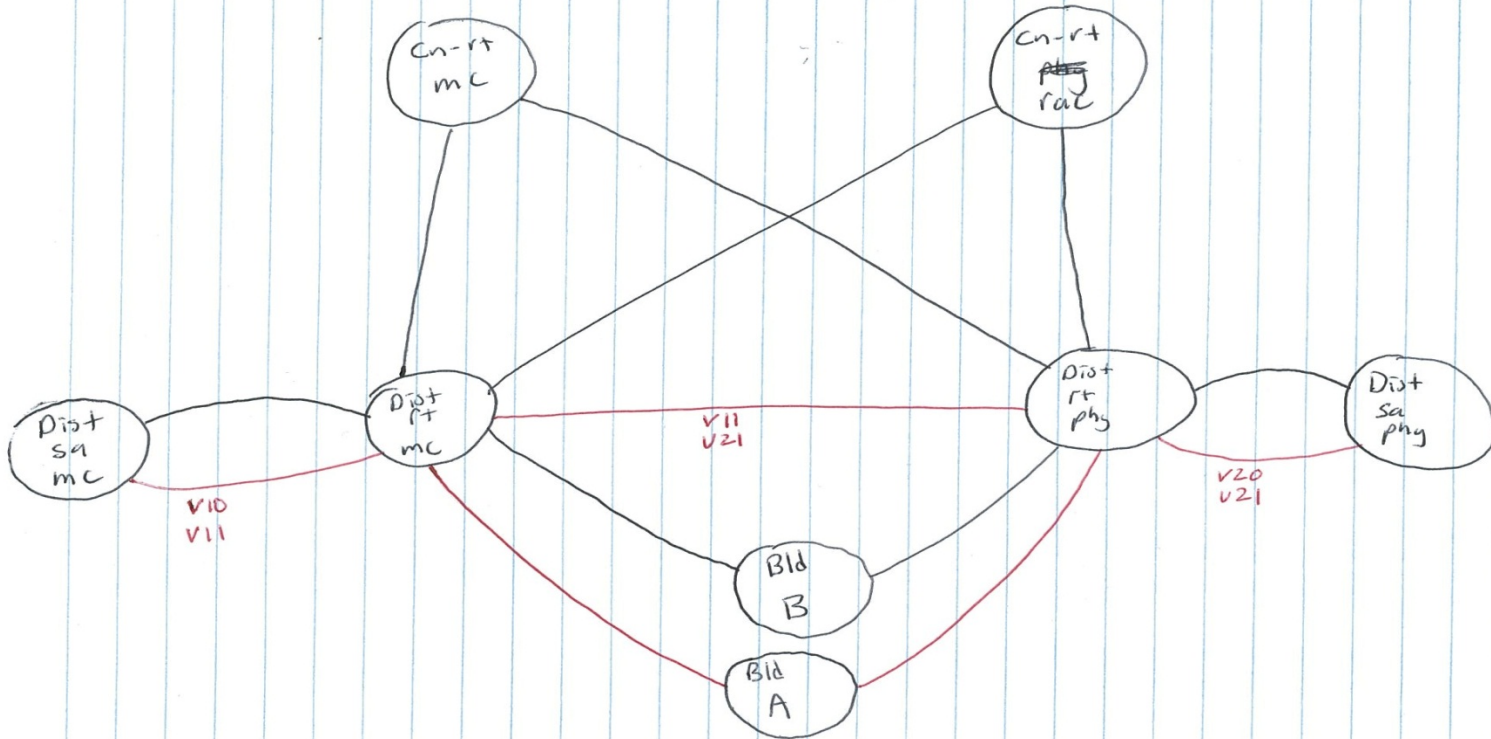
The SRX3600 Services Gateway is designed to secure enterprise, service provider, and mobile operator, data centers and server farms, as well as aggregating security services across the network infrastructure.



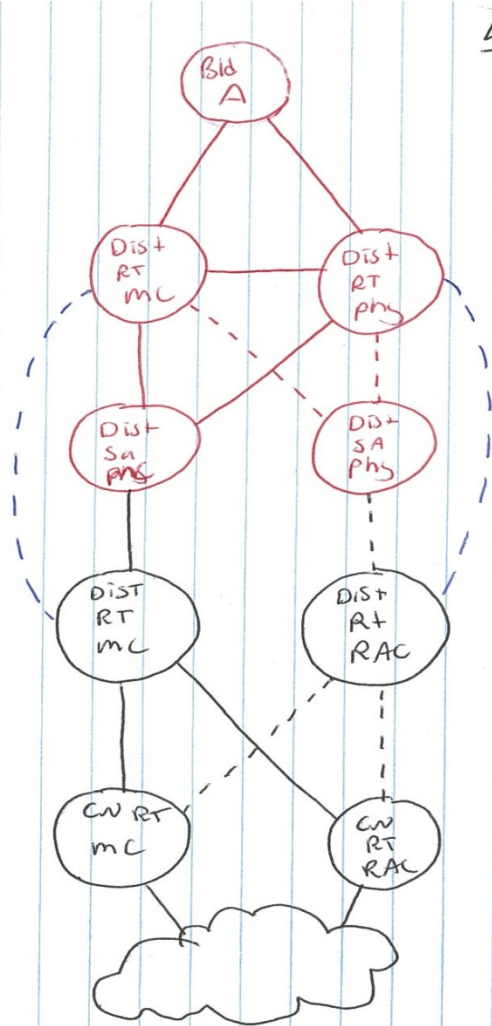
- 2x Service Processing Cards (SPC-1-10-40)
- 1x Network Processing Card (NPC)
- 1x Routing Engine (RE-12-10)
- 1x Switch Fabric Module (SFP-12GE)
- 1x 10GE I/O Card (2XGE-XFP)
- 1x 1GE I/O Card (16GE-SFP)
- 4x Power Supplies

Physical Diagram

Physiade — = Untrust (URF Campus)
— = Trust (URF Campus)



Logical Diagram



Logical

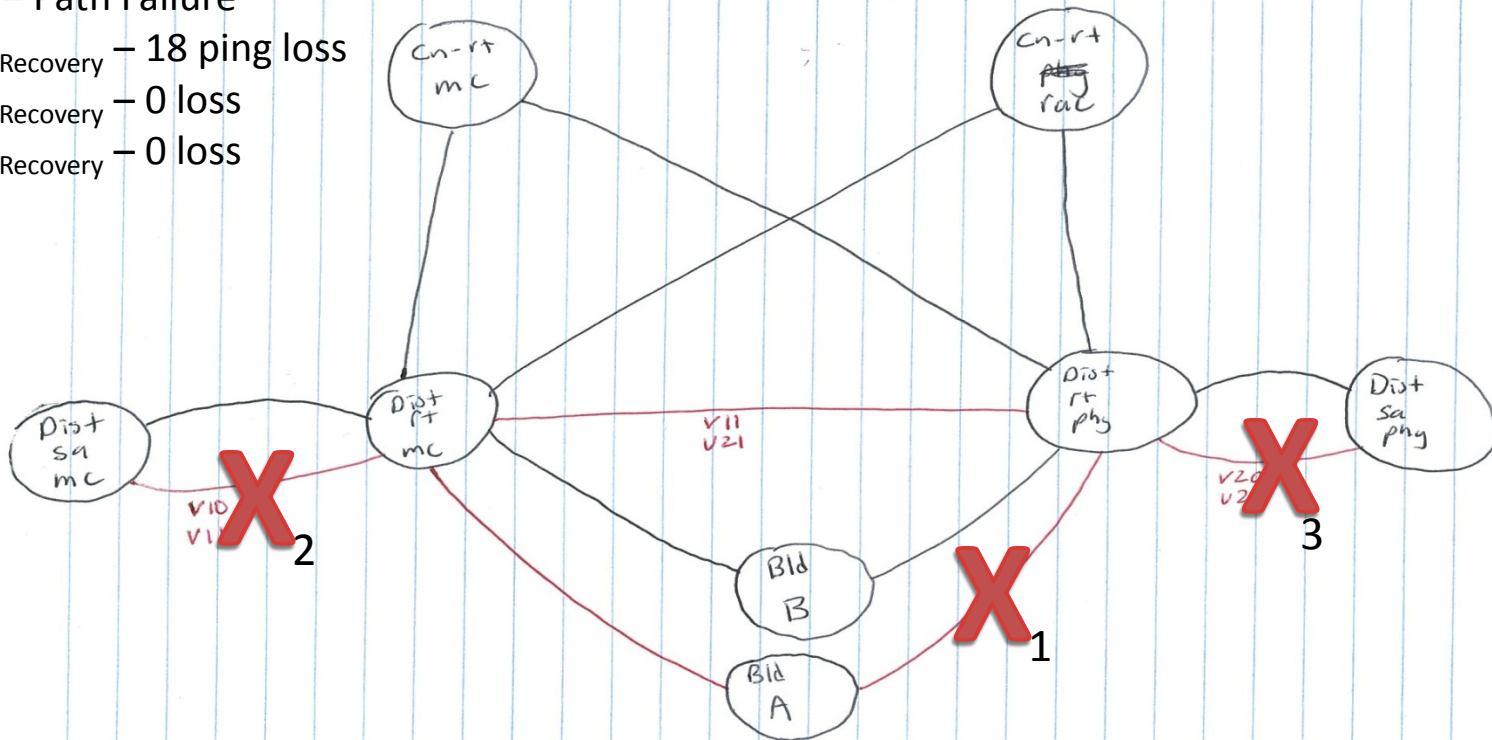
- Primary Trusted Path
- - - Alternative Trusted Path
- Primary Untrusted Path
- - - Alternative Untrusted Path
- Primary path between:
 APs 172.22.0.0/20 to 30
 to Aruba Controllers 172.16.2.192/27
 and
 IP phones 172.30.120.0/17 to 30
~~to~~ to
 IP Phones 172.30.120.0/17 to 30
 PBX 172.16.18.0/27
- - - Alternative path to above

Physical Diagram

User Traffic Tests

- X_1 - 1 ping loss
- X_2 - 5 ping loss
- X_3 - Path Failure
- $X_{3 \text{ Recovery}}$ - 18 ping loss
- $X_{2 \text{ Recovery}}$ - 0 loss
- $X_{3 \text{ Recovery}}$ - 0 loss

Physical — = Untrust (URF Campus)
— = Trust (URF Campus)



Physical Diagram

IP Phone Call Tests

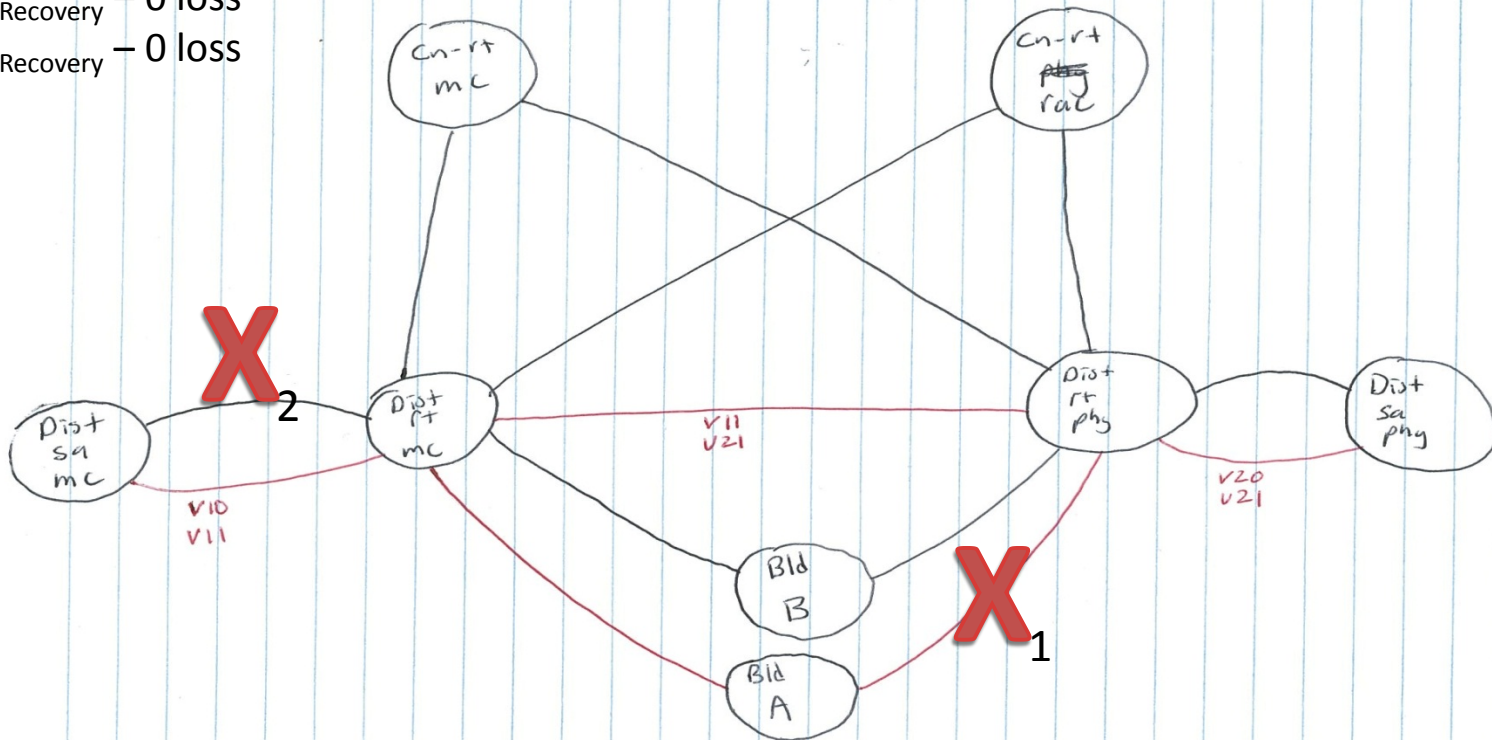
X₁ - 2 ping loss, 2s call silence, call remains connected

X₂ - 0 ping loss

X₂ Recovery - 0 loss

X₃ Recovery - 0 loss

Physiade — = Untrust (URF Campus)
— = Trust (URF Campus)



Physical Diagram

AP Traffic Tests

X₁ - 0 loss

X₂ - 0 loss

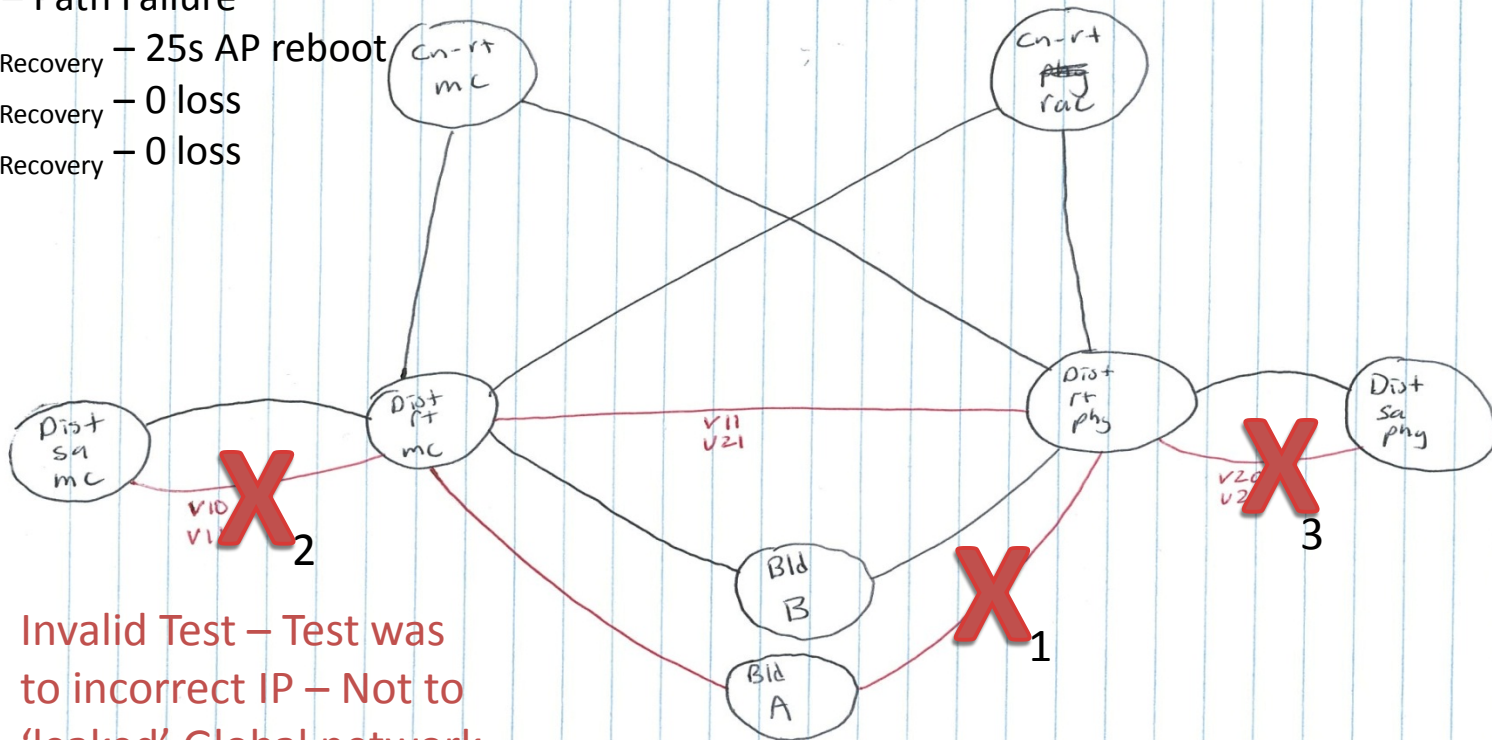
X₃ - Path Failure

X₃ Recovery - 25s AP reboot

X₂ Recovery - 0 loss

X₃ Recovery - 0 loss

Physiade — = Untrust (URF Campus)
 — = Trust (URF Campus)



Invalid Test - Test was to incorrect IP - Not to 'leaked' Global network

To Do

- Migrate all current building routed links into Global VRF on dist-rt-* - ETA
- Migrate dist-rt-* uplinks into Global VRF
- Apply any policy exceptions
- Test additional failure scenerios
- Test IPv6 and Multicast Failures
- As-rt-mc will be first building behind firewall