Software Defined Secure Networks

José Fidel Tomás – fidel.tomas@juniper.net
Trends Impacting Enterprise Security

THREAT SOPHISTICATION
- Zero day attacks
- Advanced, persistent, targeted attacks
- Adaptive malware

CLOUD
- Virtualization and SDN
- Applications, data, management in the cloud
- Application proliferation

INFRASTRUCTURE
- Hybrid cloud deployments growing
- Device proliferation and BYOD
- IoT and big everywhere
Perimeter Oriented Security

- Hyper-connected Network
- Security at Perimeter
- Complex Security Policies
- Lateral Threat Propagation
- Limited Visibility
Software Defined Secure Network

Delivers Zero Trust Security Model

- Secure Network
- Simplified Security Policy
- Block Lateral Threat Propagation
- Comprehensive Visibility
Transformation to Software Defined Secure Networks

Uncoordinated and firewall focused

Orchestrated, holistic system encompassing security + infrastructure
Software Defined Secure Network

Policy

Create and centrally manage security policy through user-intent based system

Detection

Unify and rate threat intelligence from multiple sources

Enforcement

Enforce policy in near real time across the network; ability to adapt to network changes
SDSN Deployment Scenarios

**Campus & Branch**
- Quarantine infected end points
- BYOD and device profile based access control

**Data Center**
- Micro-segmentation
- Consistent security for
  - Private and hybrid cloud
  - SDN based workloads

**Service Provider**
- Mobile Edge Gateway
- Gi Firewall
Campus Network: Infected Host Workflow

**Policy**
- Policy defined in Policy Engine
- “Infected Hosts with Threat Level >8 should be quarantined”

**Detection**
- Sky ATP Threat Feeds
- Custom Feeds (e.g., Attivo, Vectra)

**Enforcement**
- Access and aggregation switches quarantine infected host
- SRX policy enforcement
Data Center Micro-segmentation

**POLICY**
- Policy defined in Policy Engine
  1. “IT Applications cannot access Finance Applications even if they share same VLAN”
  2. Traffic in and out of Infected Applications should be logged

**DETECTION**
- Sky detection applicable for infected applications scenario (#2 above)

**ENFORCEMENT**
- VM related traffic controls enforced in vSRX
- Physical to physical traffic controls in access/aggregation switches
Service Provider: Mobile Edge Computing

**MOBILE SP NETWORK**

**MOBILE HUB SITE**

**POLICY**
- Policy defined in Policy Engine
- “Attacks from infected mobile devices should be blocked in Mobile Hub site”

**DETECTION**
- Sky Infected Host feed
- Using 3rd feeds
- SRX data to Sky

**ENFORCEMENT**
- Contrail provisions vSRX in Service Chain
- Traffic from infected mobiles dropped by vSRX

**Dynamic Service Chain w/ vSRX**

**SDSN Policy Engine**

**SKY ATP**

**3rd Party Feeds**

**Contrail Service Orchestrator**
**SDSN Stage 1 – Design/Architecture**

- SDSN is both a Policy Controller and/or Feed Connector, based on License – Unicorn can be both or just Connector
- As Policy Controller – Introduce User intent Policy → Secure Fabric, Policy Enforcement Groups, switch support
- Support for SD+SKYATP or SD+SKTATP+SDSN
- SDSN downloads feeds from Cloud Server and support OnPrem custom feeds (OnPrem).
- SRX 1500 configured to download feeds from SKY ATP or Unicorn Connector (OnPrem mode).
- Other SRX (No SKYATP Support) configured to download feeds from SDSN OnPrem mode) – only support for C&C, GeoIP
- In SD+SKYATP+UNICORN –
  - Switch uService in SD manages switch filter configurations
  - Push Infested Host policy to switch, find endpoint, map IP-MAC.
Manage Your Migration and Upgrade - Juniper Professional Services

If you customers lack:
  Resources
  Domain expertise
  Experience deploying NGFW

Juniper Professional Services
  Reduce Risk
  Reduce Time to implementation

QuickStart Services:
  • SRX Series QuickStart Service
  • Junos Space Security Director QuickStart Service
  • JSA Security Analytics QuickStart Service
  • SKY-ATP Jumpstart Offer

Firewall Conversion Service
Thank you