Software Defined
Secure Networks

Martti Saramies, Senior Partner Account Manager,
Juniper Networks
Software Defined Secure Network (SDSN)

- Unified Cybersecurity Platform by Juniper Networks
- Automated Enforcement and Remediation in Network Devices
- 3rd Party Compatibility
Software Defined Secure Network
SDSN Enforcement
Pervasive Security

- Consistent security for on premise & Cloud
- User and Application Mobility
- Enforcement at Network & Firewall Layers
- Eco-System Approach

Diagram showing access to users, devices, connectivity, public cloud, private cloud, data center, SAAS applications.
Product portfolio for end to end solution

Detection
• Leverage entire network and ecosystem for advanced threat intelligence and detection

Policy
User intent based policy model
Consistent policy enforcement across multiple enforcement domains
Robust visibility and management

Enforcement
• Utilize any point of the network including firewalls, switches, routers, 3rd party devices, and public cloud platforms as a points of enforcement

Network as a single enforcement domain - Every element is a policy enforcement point
SDSN Phase-1 (Dec 2017)
SDSN – Threat Remediation Use Case

Manual Threat Workflows

- Incident Response
- Net-Sec Operations
- Endpoint Security

Automated Threat Remediation

- Malware Detected
- SDSN Policy Controller
- Sky Advanced Threat Prevention
- Custom/3rd Party Threat Feeds
- JSA/SIEM

- WannaCry detected in 30 seconds

- Multiple Teams
- Threat Detection → Enforcement Delays
- Vendor specific threat feeds

- Cohesive Threat Management System
- Automation across Network & Security
- Open API and 3rd Party Threat Feed Collation
SDSN Phase-1 (FRS 2017)

Use Case: Threat Remediation of infected hosts

**DETECTION**
Sky ATP – Known & Day-0 Malware analysis, Sandboxing, Infected Host identification, Command & Control, GeoIP

**POLICY**
Simplified Threat Remediation Policy (Block, Quarantine, Track) defined in Security Director Policy Enforcer

**ENFORCEMENT**
Juniper: SRX, vSRX, EX and QFX

---

**Key Features**
- Security Fabric including Firewalls and Switches
- Infected Host Blocking
  - Perimeter Firewall level for north – south traffic
  - EX/QFX switches to protect from lateral movement of threats
- Infected Host Tracking
  - Track infected host movement in network, and
  - Quarantine or block infected hosts even if IP address changes

**Customer Benefits**
- Automates threat remediation workflows
- Real-time remediation of infected hosts
- Reduced time to remediate = Reduced exposure to attacks
- Leverage Network (EX/QFX) and Firewall (SRX/vSRX) to take remediation actions to address lateral movement of attacks inside the network in addition to limiting attacks from outside world
Understanding SDSN Phase 1

**Secure Fabric**
- SRX Firewalls
- Juniper EX and QFX switches

**Sky Realm**
- SRX and PE registered

**Threat Intelligence from**
- SKY ATP Cloud Feeds

**Enforcement**
- On SRX via Security Director
  - ATP policy pushed to SRX from SD
  - SRX pulls Infected host feed from PE
- On EX/QFX Switches
  - S/W micro service collects and Maintain IP/MAC binding of hosts
  - Commits a MAC F/W filter on switch for enforcement
SDSN Phase-2 (July 2017)
Policy Enforcer Phase 2 – Overview

**Threat Remediation**
- EX in Fusion Mode
- 3rd Party Switches
- Wireless & Trunk Port

**3rd Party Eco-System**
- 3rd Party Threat Feeds
  - Whitelist, Blacklist and Infected Host threat feeds
- 3rd Party Enforcement
  - Southbound API for 3rd parties

**Private Cloud**
- NSX – vSRX Micro-segmentation
  - vSRX Policies
Threat Remediaion Enhancements

Use Case: 3rd Party Switch and Wireless Support

**ENFORCEMENT**

**Juniper:** SRX, vSRX, QFX and EX (+Fusion Support)

**3rd Party:** Access Switches with Radius(AAA) configured

**Wireless:** WLAN Controllers with Radius(AAA) configured

---

**Key Features**

- Security Fabric to support 3rd party switches and wireless
- Infected Host Blocking
  - Juniper & 3rd party switches to protect from lateral movement of threats
- Infected Host Tracking
  - Track infected host movement in network, and
  - Quarantine or block infected hosts even if IP address changes

---

**Customer Benefits**

- Automates threat remediation workflows
- Real-time remediation of infected hosts
- Reduced time to remediate = Reduced exposure to attacks
- Network vendor agnostic mechanism for threat remediation
Custom Feed API Support

Use Case: Threat Remediation of infected hosts leveraging 3rd party threat feeds

DETENTION (Phase-1)
Sky ATP
- Command and Control
- Infected Host

Key Features
- Blacklist: Entities in blacklist always get blocked by SRX
- Whitelist: Entities in whitelist always get accepted by SRX
- Dynamic Address: Entities in Dynamic Address Group can be used in firewall policy of SRX
- Infected Host: Threat Prevention Policy enforced for entities identified as infected hosts

Customer Benefits
- Enables customers to leverage existing, trusted threat feed sources to take threat remediation actions w/ Policy Enforcer
  - Flexible mechanisms to synchronize threat information
    - Push to Policy Enforcer with "Threat Feed API", or
    - Configure Policy Enforcer to poll from remote feed server

ENHANCED DETECTION (Phase-2)
Now supports 3rd Party Feeds
- Blacklist
- Whitelist
- Dynamic Address
- Infected Host
Thank you

Martti Saramies
Sr Partner Account Manager
msaramies@juniper.net
Mob. +358 40 580 29 88