BCNET ANNUAL HIGHER EDUCATION

LEARN ENGAGE SHARE

Elevate your Security Posture with Juniper's Software-Defined Secure Networks

Bops Puliyanda, Product Manager, Juniper Networks



Trends Impacting Enterprise Security



THREAT SOPHISTICATION

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



- Virtualization and SDN
- Applications, data, management in the cloud

BCNET Conference 2016

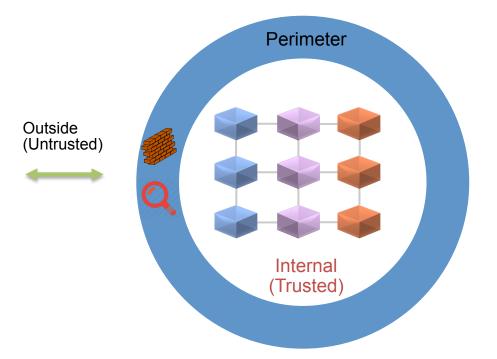
Application proliferation



INFRASTRUCTURE

- Hybrid cloud deployments growing
- Device proliferation and BYOD
- IoT and big data everywhere

Perimeter Oriented Security





Hyper-connected Network Security at Perimeter



Complex Security Policies



Lateral Threat Propagation

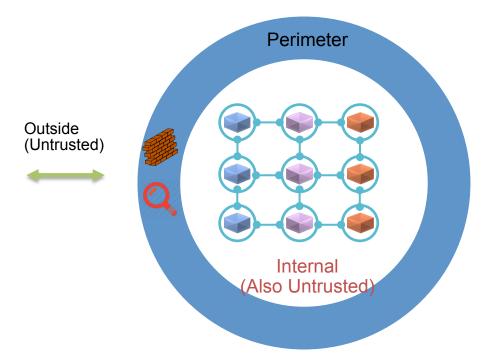


Limited Visibility



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

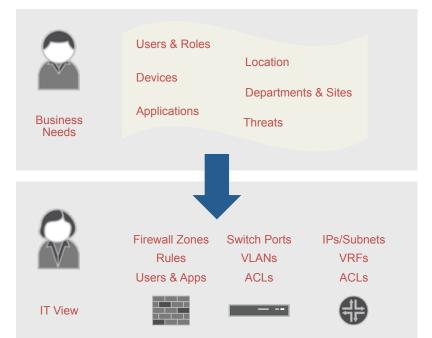




SDSN BUILDING BLOCKS



Framework



POLICY



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

DETECTION



Unify and rate threat intelligence, from multiple sources

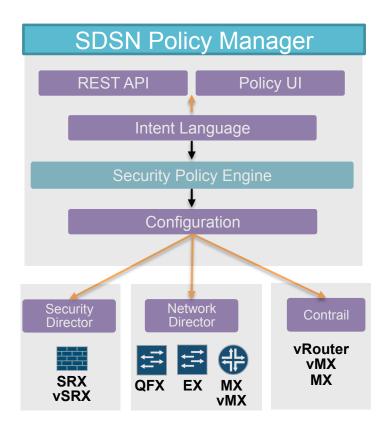
ENFORCEMENT



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



Global Policy Orchestration



Single policy across security and networking systems

Intent driven policy translated to configurations

Juniper and 3rd party support



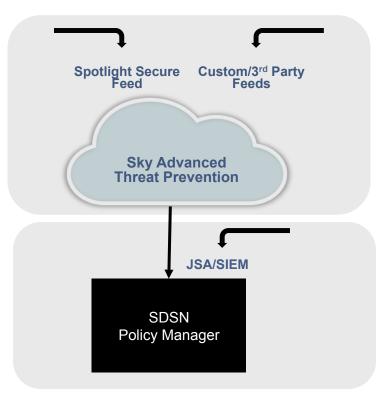
Sky Advanced Threat Prevention

| SKY ADVANCED THREAT PREVENTION | | | | | | | | | | bops | @juniper.net | juniper-it-svl | ి ~ |
|-----------------------------------|---------------------|----------------|------------------------|--------------|---------------------------|---------------------------------------|----------------------------|---|---|---|--------------|----------------|------------|
| Dashboard Moni | tor Devices | Configure | Administration | | | | | | | | | | |
| ard | | | | | | | | | | | | | |
| ATP | | | | | | | | | | | | C × Selec | ct Widgets |
| 111 | | | | | | | | | | | | | |
| urce Locations Ho | sts | Malware | File Cate gories | File Cat | e gorie s | | | | | | | | |
| &C Server & Malware To | p Compromised | Top Identified | Top Infected | Top So | anned | | | | | | | | |
| N 2007 | | | | | — | | | | | | | | |
| | =: | == | | | | | | | | | | | |
| () | 1 | | 0 | | | | | | | | | | |
| | | | | | | | | | | | | | |
| op Compromised Hosts | | | | | C&C Server and | I Malware Source Loc | ations | | | | | | |
| Host Thr | eat Lvi Blocker | d Status | State of Investigation | | | | Sh | ow: C&C Servers | Previous: | month 🛩 | | | |
| 192.168.239.98 | 10 Blocked | | Open | 6 | a | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | m 50 | | | | | | |
| 192.168.239.74 | 10 Blocked | | Open | | | | Ť | c ? | | | | | |
| 192.168.237.1 | 10 Blocked | | Open | | | | | \/s | | | | | |
| 192.168.236.136 | 10 Blocked | | Open | | | | | | | • | | | |
| 192.168.236.39 | 10 Blocked | | Open | | 1 | | 6 9 | 10 A | | and the second se | | | |
| 192.168.235.159 🕐 | 10 Blocked | | Open | | - Ar 200 | | | | 2 | | | | |
| 192.168.234.152 | | | Open | | | | V | | | 4 | | | |
| 192.168.186.249 🕐 | 10 Blocked | | Open | | | | | | The second second | • | | | |
| | | | | | | 1 | A 📑 | 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 | | | | | |
| Updated Feb 10, 2016 10:57:46 AM | | | | More Details | | | | - Aler | 74 - Carlos | | | | |
| | | | | | ~ | | K | L L L | a standard and | | | | |
| Fop Infected File Categories | | | | | | and the second | | SALAS - | V YS & | | | | |
| Show: Med, High Threat 🛩 | Previous: 1 month 🛩 | | | | | 275 | Contraction and the second | - Starter | S. Same | | | | |
| outable | | | | | | (Ser | . 7 | MAN 1 | The second second second second | | | | |
| - | | | | | |)~ | 5,- | TEAL | | | | | |
| library | | | | | Threat Count | Å. | 5 | | | × 1 | | | |
| ument | | | | | 1-49 | | | | | d' | | | |
| pdf | | | | | 50-99 | S. | 0 | | 5 | | | | |
| rchive | | | | | 500+ | | | | | | | | |
| Ok 2k | 4k | | | | - | | -10 ⁻ | | and the second and | | | | |
| Infected F | | | | | | | | | | | | | |
| Updated Feb 10, 2016 10:57:46 AM | More Details | | | La | t Updated Feb 10, 2016 10 | 57:45 AM | | | | More Details | | | |
| - | | | | | - | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

BCNET

JUNIPER

Unified Threat Detection



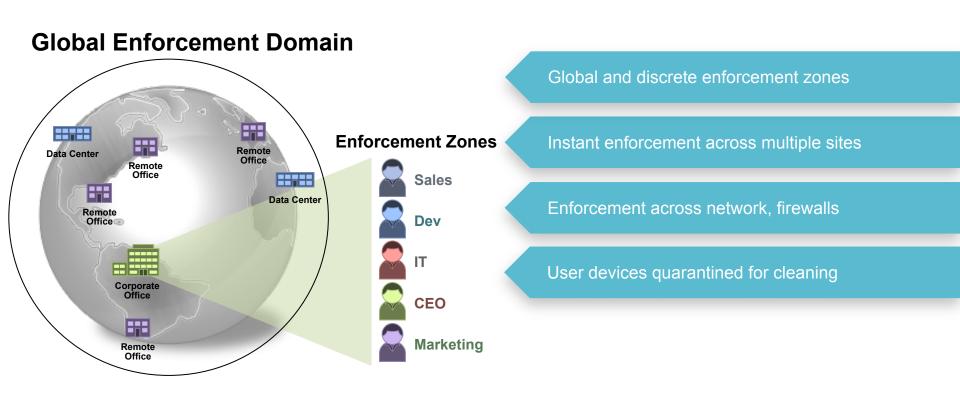
Open threat feeds platform: Juniper, third party, custom

Single view of threats for better visibility across enterprise

Unified feed curated for false positives and duplication, and given threat severity rating



Automated Enforcement







USE CASES



SDSN Deployment Scenarios



DATA CENTER

- Security for east-west and northsouth traffic
- · Consistent security for
 - On-prem and hybrid-cloud
 - SDN based workloads



- **CAMPUS & BRANCH**
- Quarantine infected end points
- Zero day attacks
- BYOD and device profile based access control

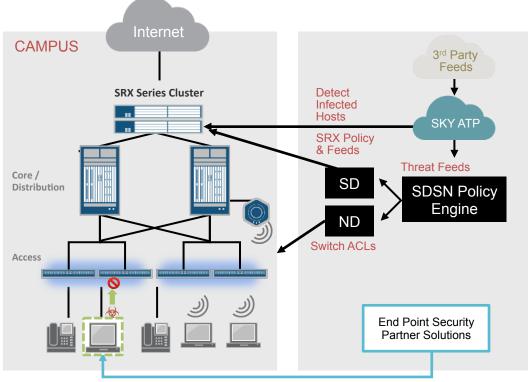
BCNET Conference 2016



- Mobile Edge Gateway
- Gi Firewall
- MSP: Tenant isolation

Campus Network

BCNET Conference 2016



Remediation of infection

POLICY

- · Policy defined in Policy Engine
 - "Infected Hosts with Threat Level >8 should be quarantined"

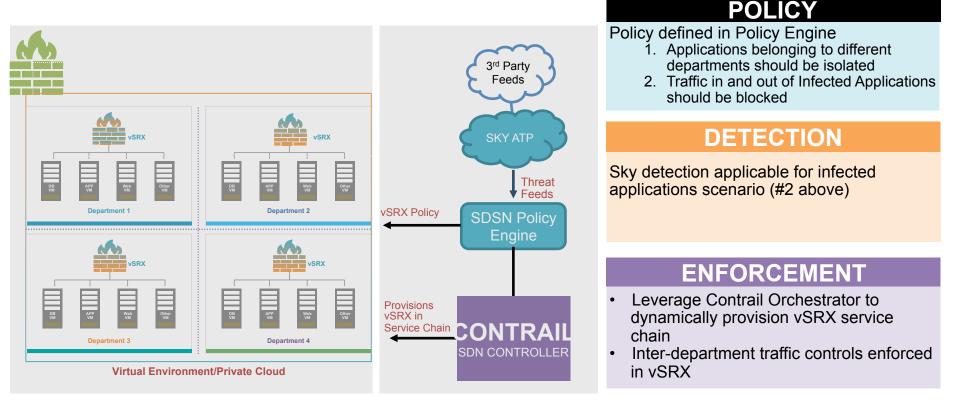
DETECTION

- · Sky Infected Host feed
 - Using 3rd party (e.g: Attivo, Vectra), and
 - SRX data to Sky

ENFORCEMENT

 Access and aggregation switches quarantine infected host

Enterprise Private Cloud



BCNET Conference 2016



POLICY WORKFLOWS



User-Intent – Presentation layer

Secondary

Constructs For Presentation Workflow Design

Building blocks for defining Intent

Primary

Examples of Intent

Example 1: Quarantine users in HR in Sunnyvale when infected with malware of threat score > 4

Additional Action Email Email ID

| Actions | Allow Block Quarantine Email Other | Example 1. Quarantine users in HK in Sunnyvale when infected with malware of threat score > 4 |
|------------|--|--|
| Groups | Departments Engineering Other | Action Quarantine Who |
| | Locations Sunnyvale Bangalore Other | HR Sunnyvale When |
| | Applications Other Social NW Apps Productivity Apps | Someone is infected with What Malware |
| Conditions | Someone Attempts Access Someone downloads Someone is infected with + Time/Schedule Time/Schedule Time/Schedule | Example 2: Block (and Email IT admin) when any user in Marketing contacts CnC Server of threat score > 6 |
| Feeds | CnC Malware Infected IPs Geo IP (Threat Level) (Threat Level) (Threat Level) | Action Block |
| Exceptions | Include Exclude | Who Marketing Someone tries to contact What CnC Server |
| | | |



User Intent – Policy definition

Define Campus

A user created object that represent a site (campus)

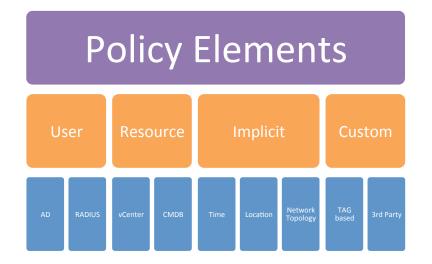
> Define department/group

User (HR-users), device (Windows machines), application (Web servers)

> Create threat management profiles

- Configure external threat sources
 - Sky ATP, Spotlight Cloud
- Configure malware detection profile

 Files to be examined by Sky ATP
- Configure infected host detection profile
 - \circ $\,$ Infected host detection by Sky ATP $\,$





User-intent – Policy definition

> Create and attach policy

- Rules
 - Block C&C servers based on threat management profile
 - Detect and block malware based on threat management profile
 - Identify and block/quarantine infected host
 - Track the infected host
 - DHCP server/ARP for IP-MAC binding
 - Detect MAC moves
- When
 - One-time, Always, Periodically
- Where
 - Policy Enforcement zone (A group within a site or a site/site-group)



Summary



Unified framework for policy and threat management

Every device in network (firewall, switch, router) can be an enforcement point

Security based on 'zero trust' paradigm

User-intent based policy definition





THANK YOU!

