BCNET ANNUAL HIGHER EDUCATION IT CONFERENCE

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

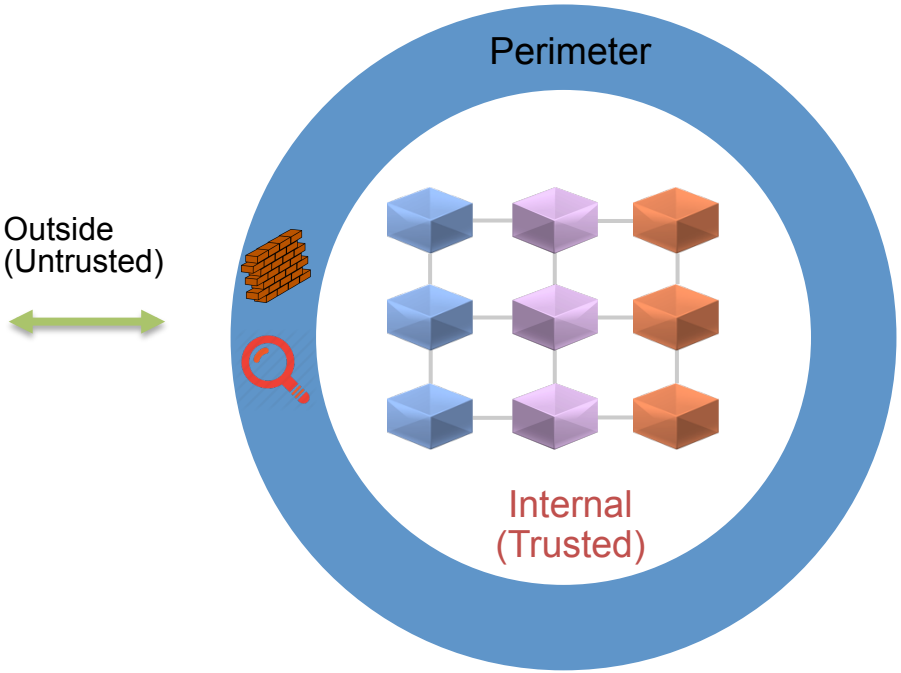
CLOUD

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

INFRASTRUCTURE

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

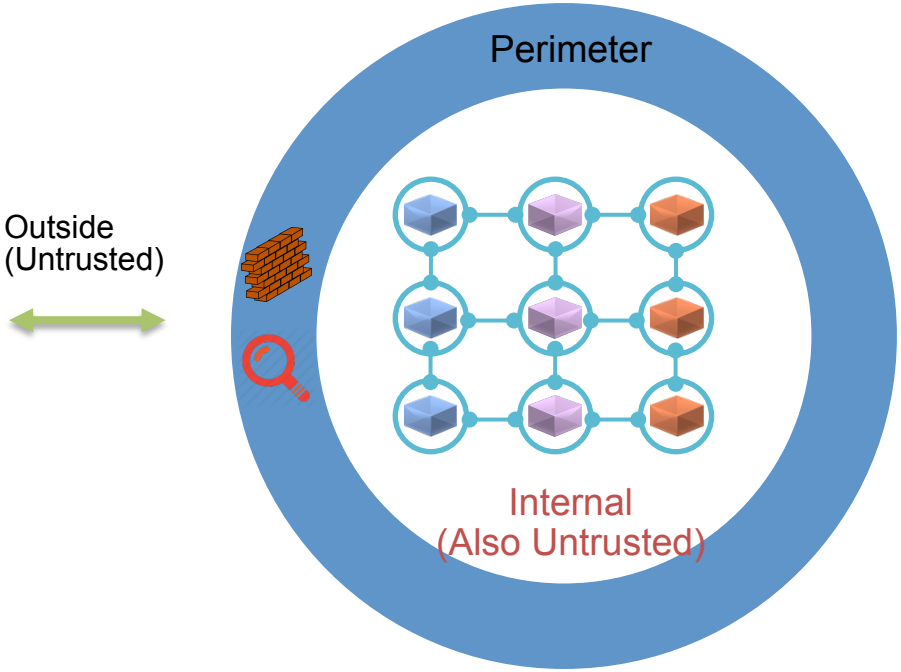
Perimeter Oriented Security



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

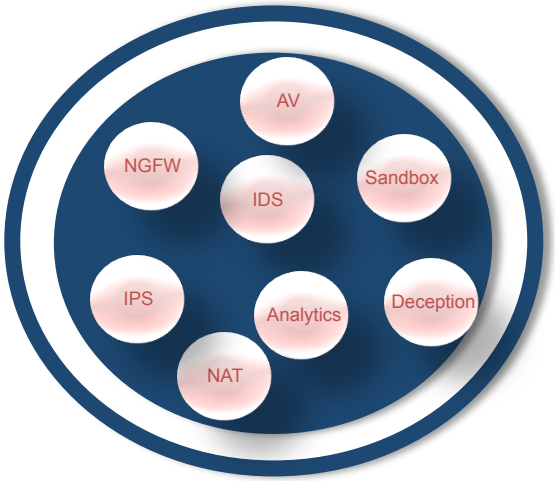
Software Defined Secure Network

Delivers Zero Trust Security Model



- Secure Network
- Simplified Security Policy
- Block Lateral Threat Propagation
- Comprehensive Visibility

Transformation to Software Defined Secure Networks

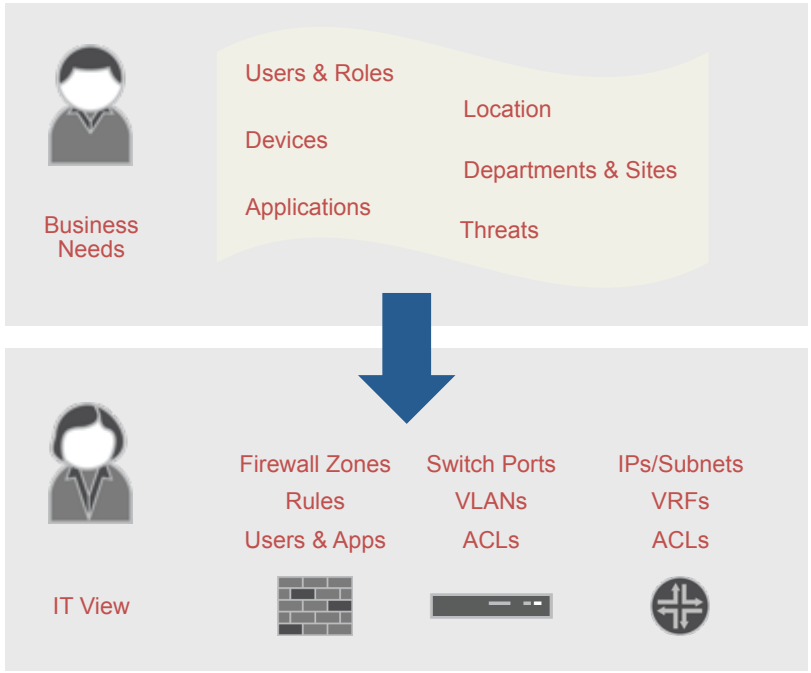


Uncoordinated and firewall focused

Orchestrated, holistic system encompassing security + infrastructure

SDSN BUILDING BLOCKS

Framework



POLICY

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

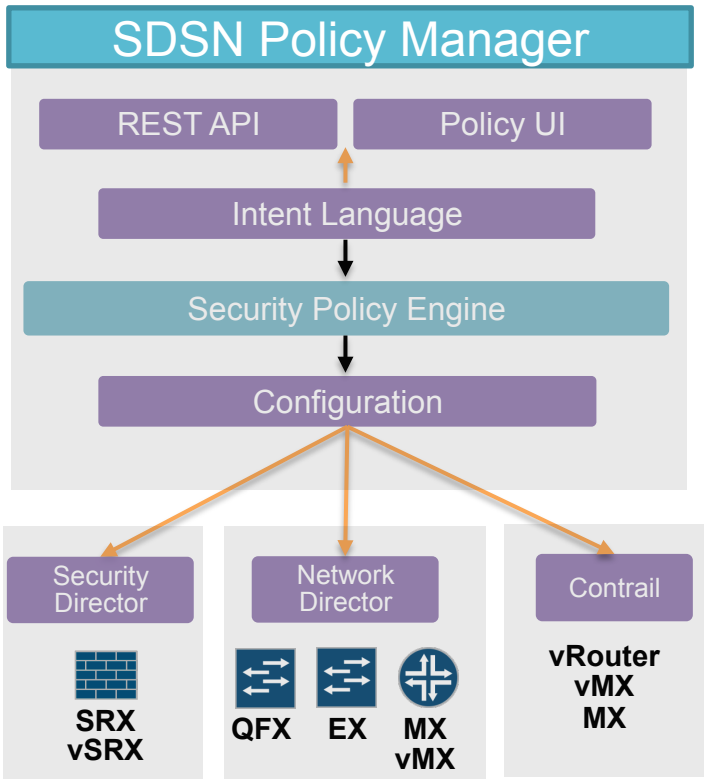
DETECTION

Unify and rate threat intelligence, from multiple sources

ENFORCEMENT

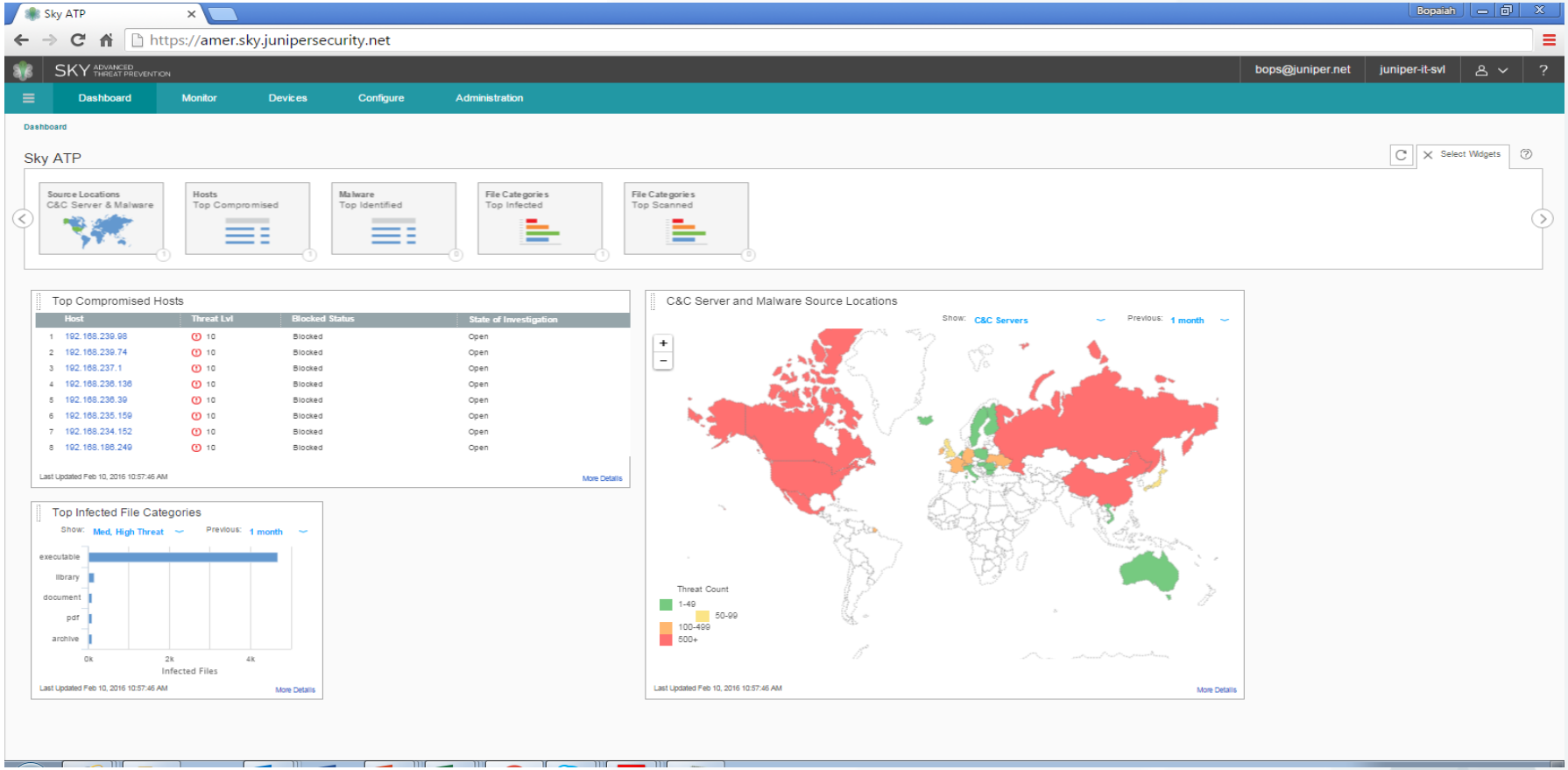
Enforce policy in near real time across the network; ability to adapt to network changes

Global Policy Orchestration

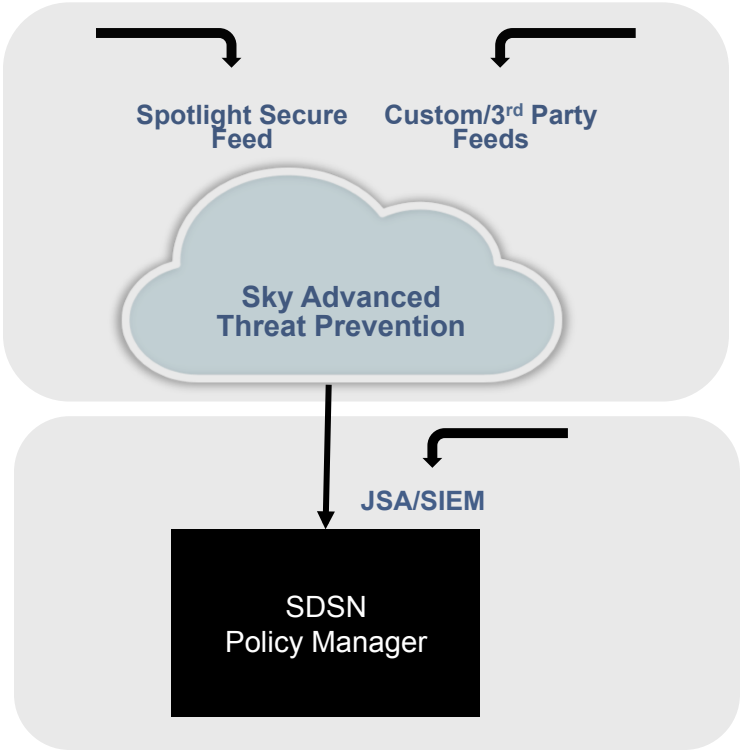


- Single policy across security and networking systems
- Intent driven policy translated to configurations
- Juniper and 3rd party support

Sky Advanced Threat Prevention



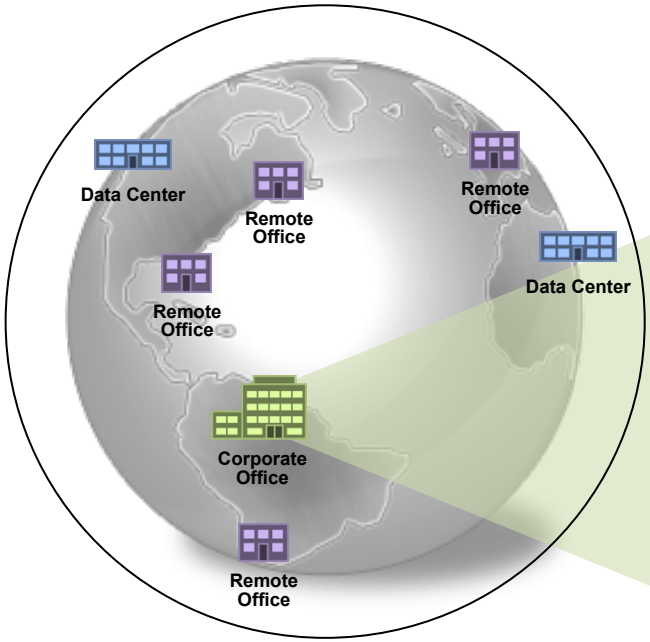
Unified Threat Detection



- 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

Global Enforcement Domain



Enforcement Zones

- Sales
- Dev
- IT
- CEO
- Marketing

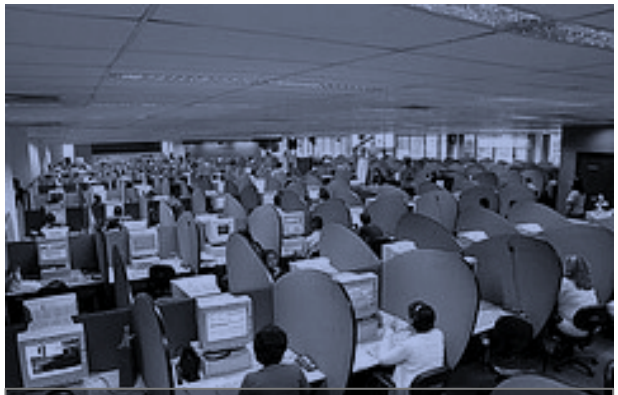
- Global and discrete enforcement zones
- Instant enforcement across multiple sites
- Enforcement across network, firewalls
- User devices quarantined for cleaning

USE CASES

SDSN Deployment Scenarios

DATA CENTER

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



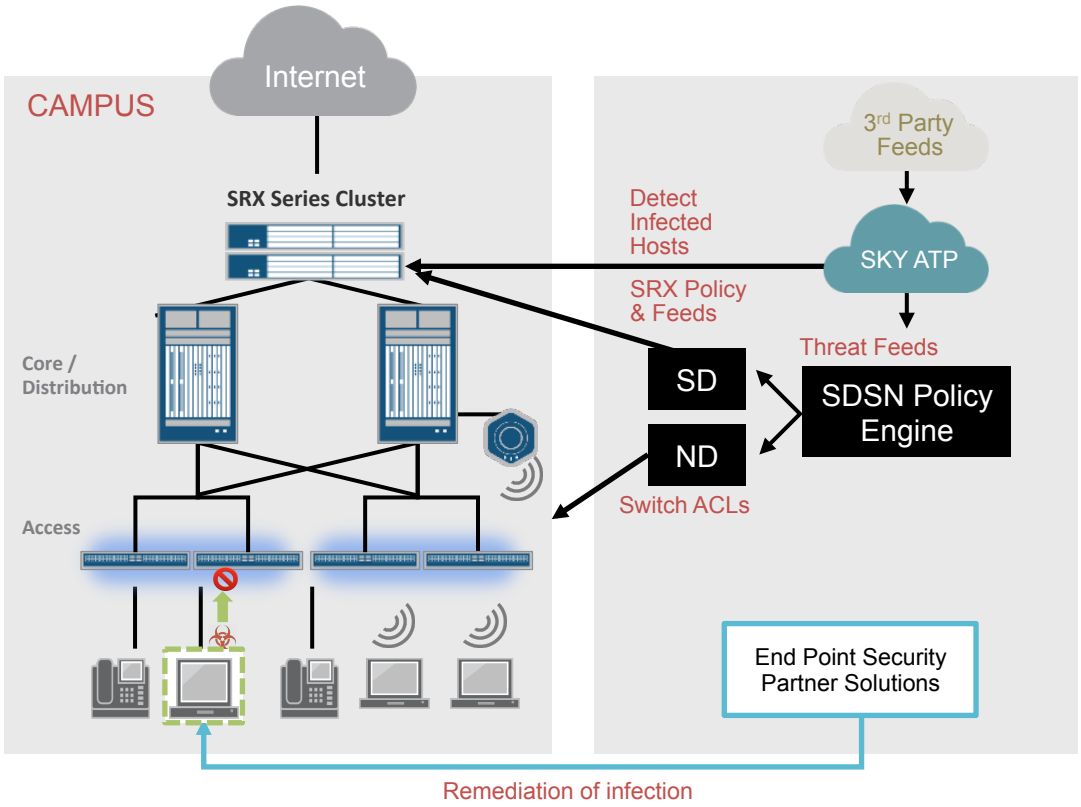
CAMPUS & BRANCH

- Quarantine infected end points
- Zero day attacks
- BYOD and device profile based access control

SERVICE PROVIDER

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

Campus Network



POLICY

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

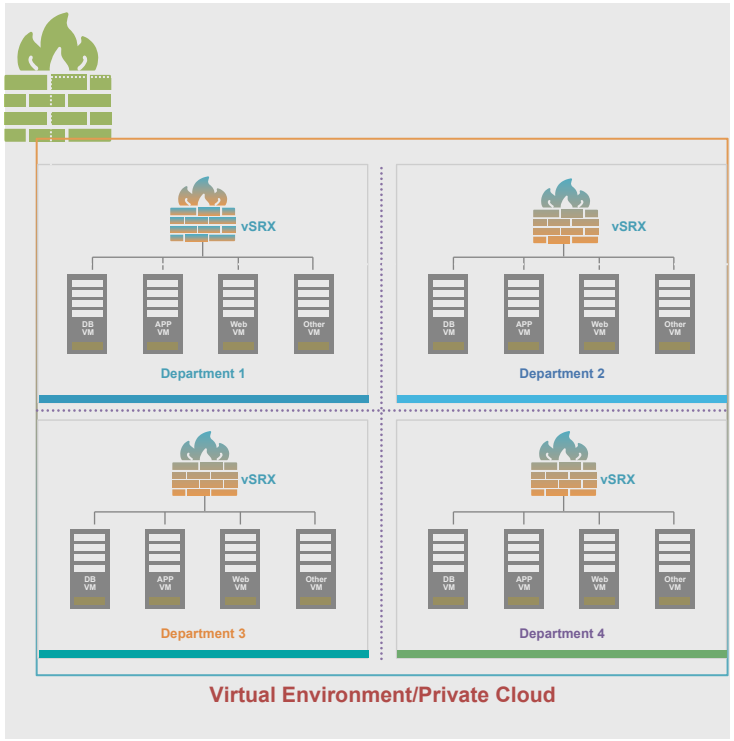
DETECTION

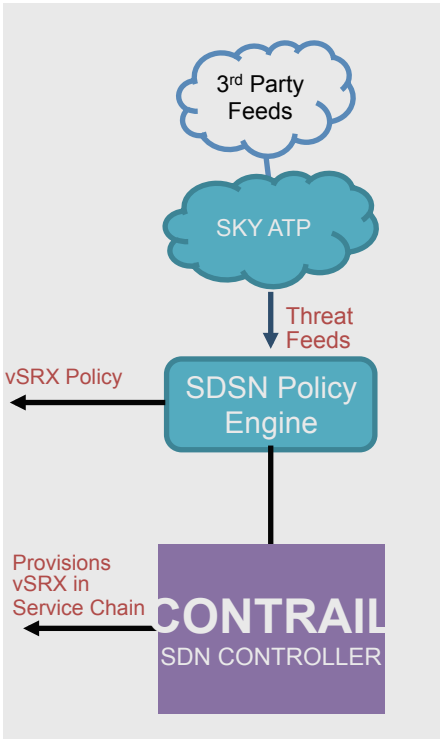
- Sky Infected Host feed
  - Using 3rd party (e.g: Attivo, Vectra), and
  - SRX data to Sky

ENFORCEMENT

- Access and aggregation switches quarantine infected host

Enterprise Private Cloud





POLICY

Policy defined in Policy Engine

1. Applications belonging to different departments should be isolated
2. Traffic in and out of Infected Applications should be blocked

DETECTION

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

ENFORCEMENT

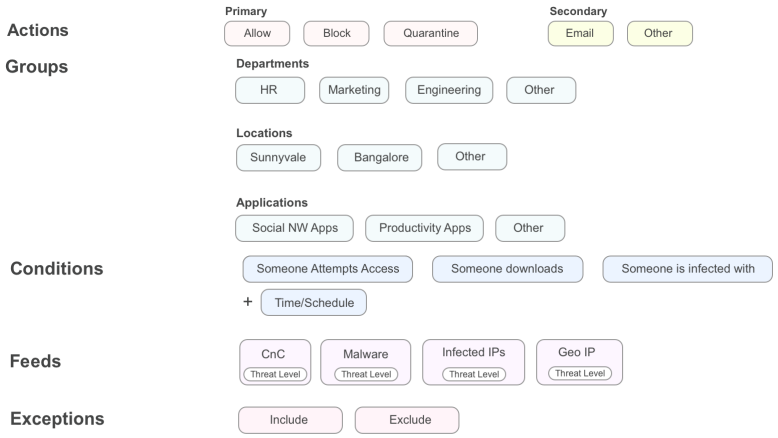
- Leverage Contrail Orchestrator to dynamically provision vSRX service chain
- Inter-department traffic controls enforced in vSRX

POLICY WORKFLOWS

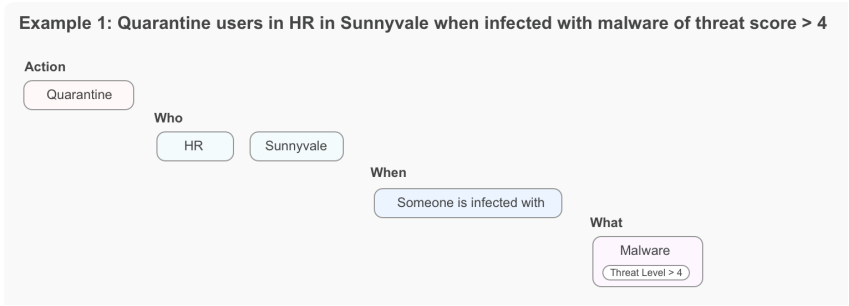
User-Intent – Presentation layer

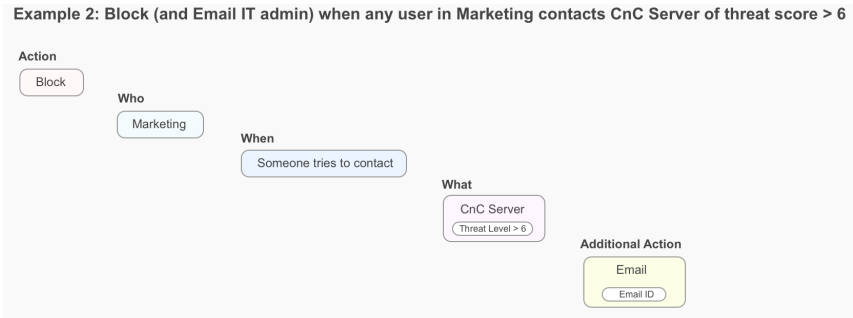
Constructs For Presentation Workflow Design

Building blocks for defining Intent



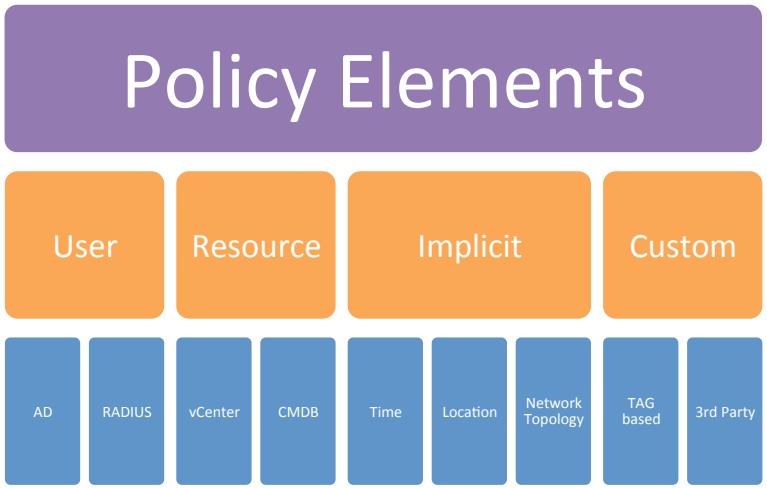
Examples of Intent





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
    - 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!

BCNET
Conference 2016