RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: SPO-F03

Network of Steel – Designing Ultra-Resilient Networks to Counter Mega Scale Cyber Attacks

Amritam Putatunda

Cyber-Security Evangelist
Ixia

What this session will cover

- Key aspects of network security
- Assessment based Policy Configurations and Purchase decisions
- In the event of eventuality -Visibility to increase network Resiliency

What this session will not cover

- End point/Auth security methods
- Scareware / Consequence
- Lower layer(Dot1X, IPsec) security

Why Steel?

- Strong
- Trustworthy
- Resilient
- At times vulnerable

Prelude: Know who you are and what your worth.

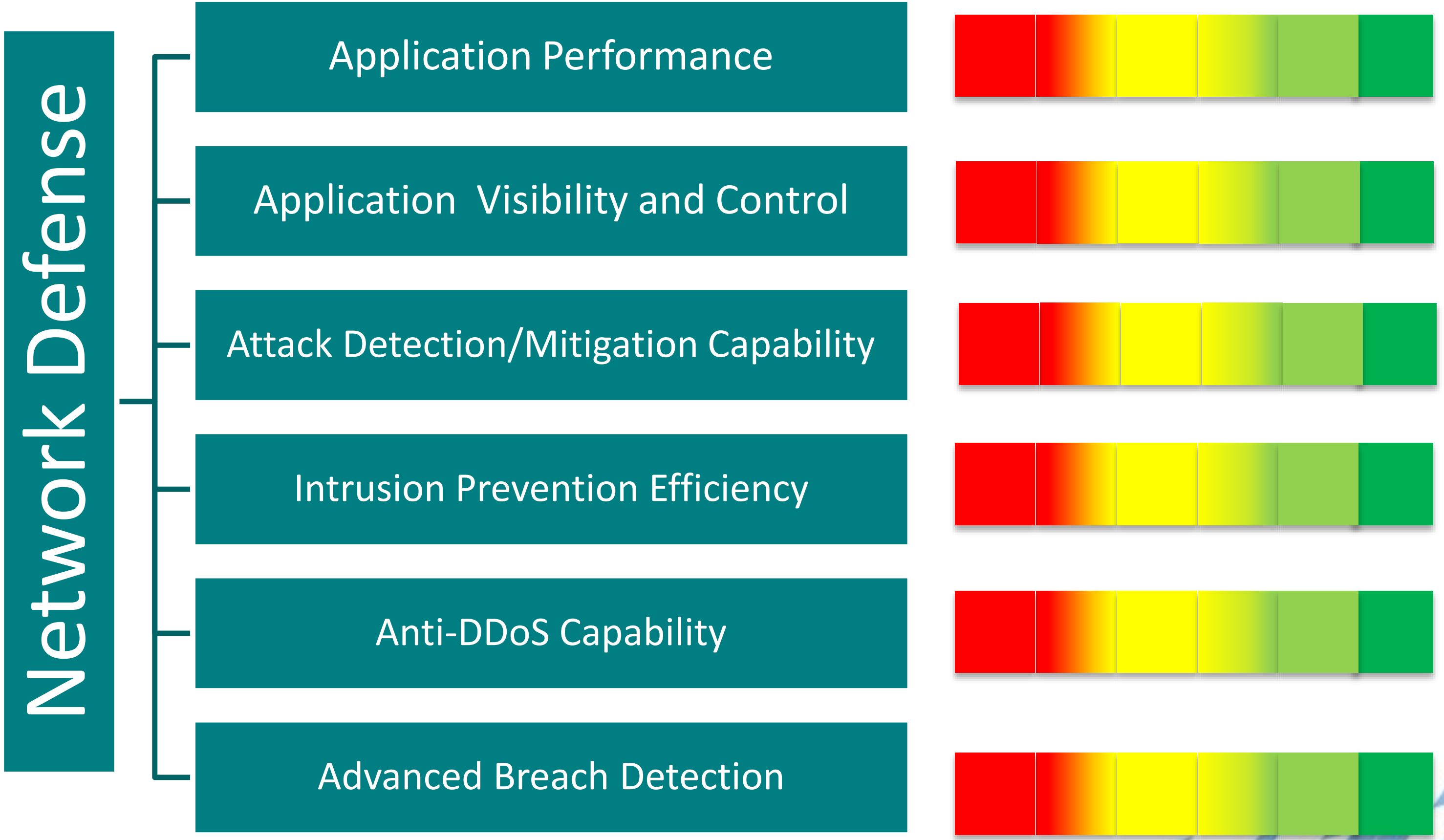
Cost of Breach

Your present Security Posture

Data driven Implementation

Resiliency with Visibility

Designing Network of Steel-Key Areas of Focus



Network Defense

- Application Performance
- Application Visibility and Control
- Attack Detection/Mitigation Capability
- Intrusion Prevention Efficiency
- Anti-DDoS Capability
- Advanced Breach Detection

How is it Done?

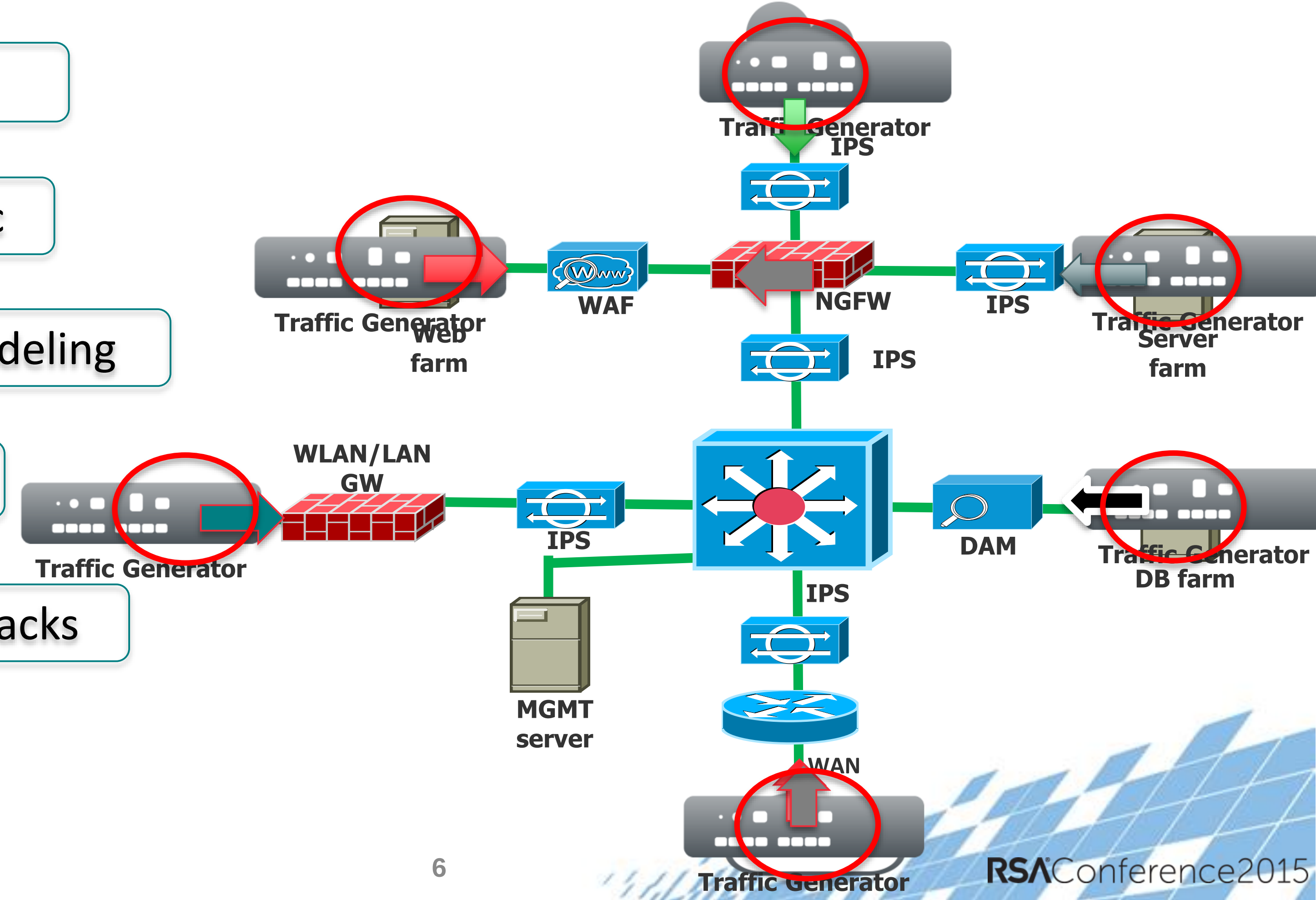
Network Traffic

Application Traffic

User Behavior modeling

Attacker traffic

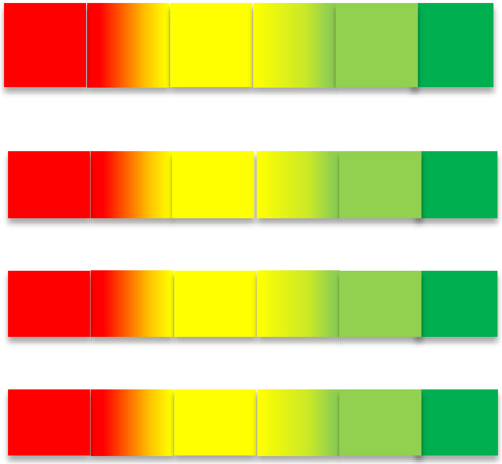
Mix of Apps & Attacks



#1 Application Performance

Key Assessment

- Theoretical Max performance
- Ideal performance with application mix
- Major traffic blockage points



Recommendations

- Application rules and policy analysis
- Result Based recommendations

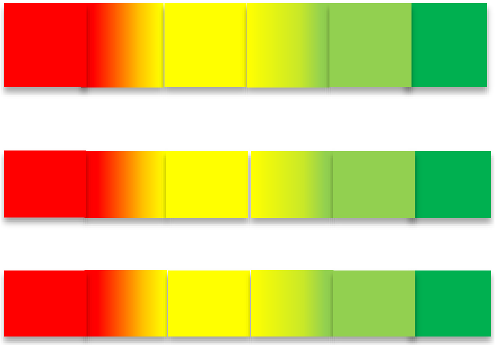
- Wan Optimizers
- App Delivery Cntrolers
- Server Load Balancers

#2 Application Visibility and Control

Key Assessment

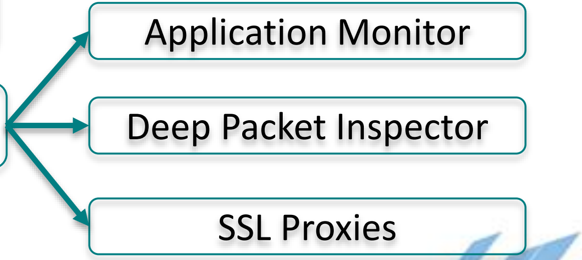
Applications Detection Capability

Application Control capability



Recommendations

Tailor made application rules



Application visibility implementation

Application Monitor

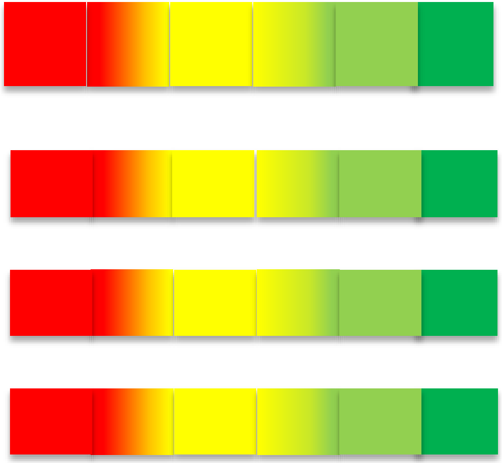
Deep Packet Inspector

SSL Proxies

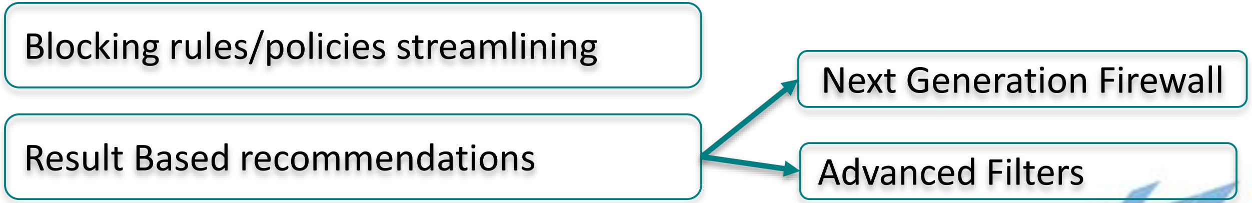
#3 Attack Mitigation Capability

Assessment

- Signature detections for Malwares
- Signature detections for Vulnerabilities
- Detection efficiency under evasion



Recommendations



Blocking rules/policies streamlining

Result Based recommendations

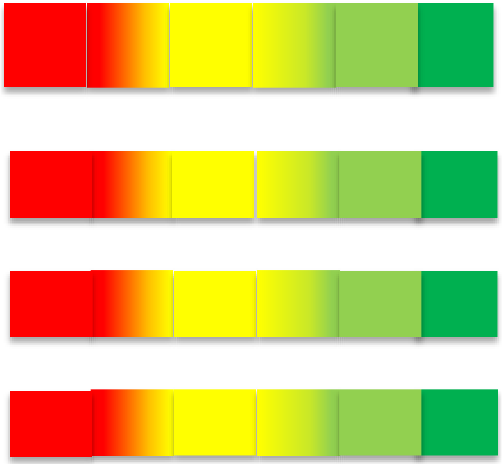
Next Generation Firewall

Advanced Filters

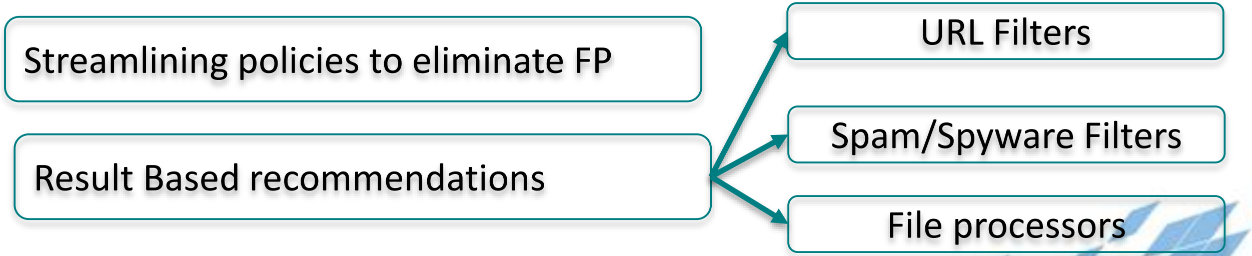
#4 Intrusion Prevention Efficiency

Assessment

- URL Filtering abilities
- Bot to C&C transaction detection
- Ability to eliminate False Positives



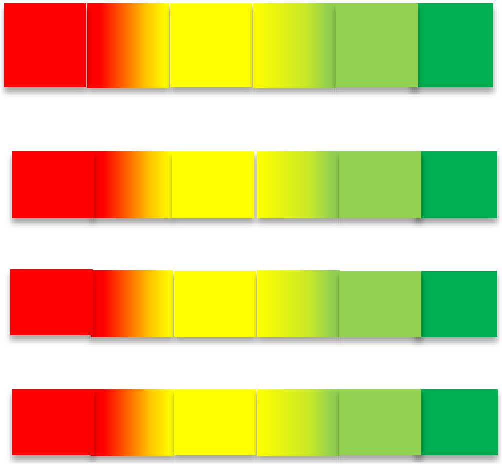
Recommendations



- Streamlining policies to eliminate FP
- Result Based recommendations
  - URL Filters
  - Spam/Spyware Filters
  - File processors

#5 DDoS Capability

Assessment



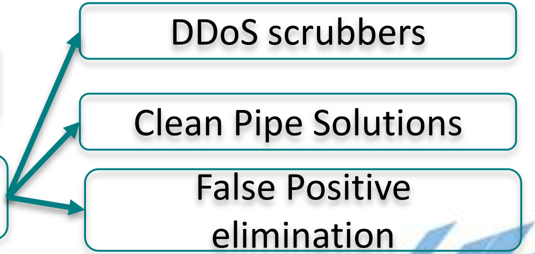
Volumetric DDoS mitigation ability

Low and Slow DDoS mitigation ability

Application DDoS mitigation ability

Recommendations

Server session/memory limit settings



Result Based recommendations

DDoS scrubbers

Clean Pipe Solutions

False Positive elimination

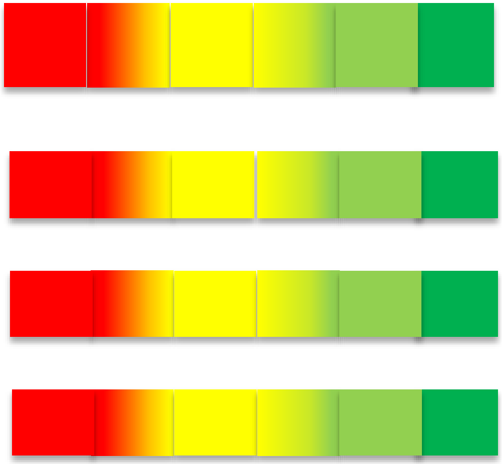
#6 Advanced Breach Detection/Mitigation

Assessment

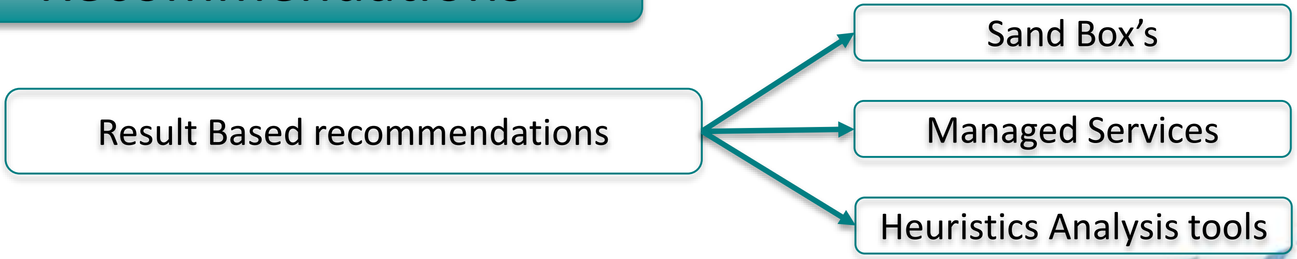
Attacks hidden within apps

Advanced Targeted/persistent attacks

Kill Chain Life Cycle analysis



Recommendations



Result Based recommendations

Sand Box’s

Managed Services

Heuristics Analysis tools

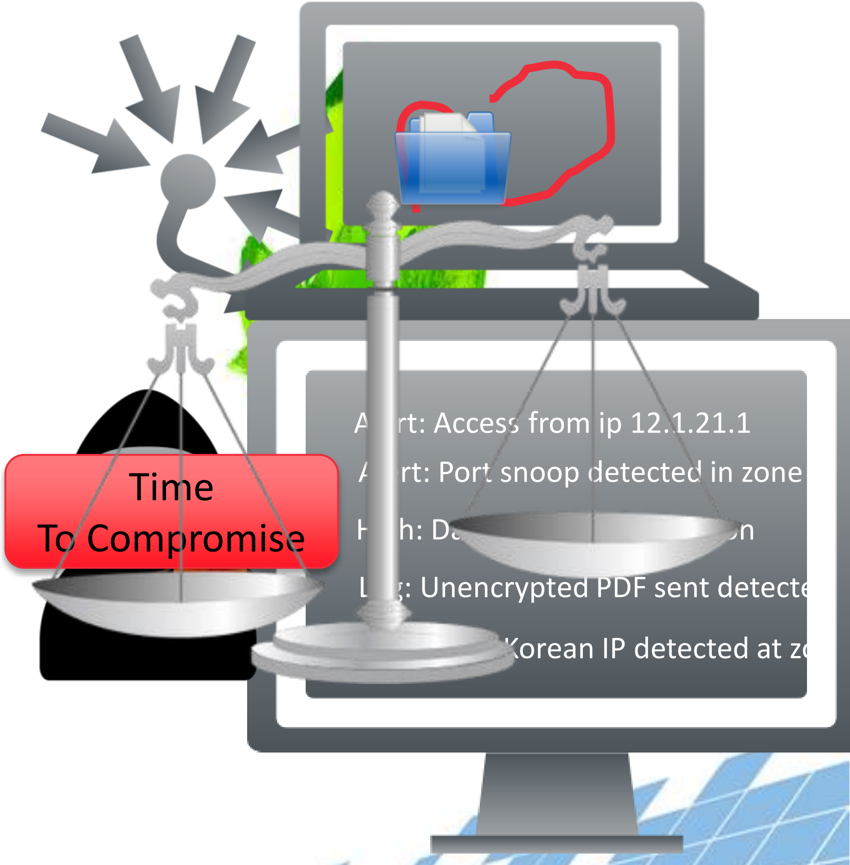
In the Event of a Breach

Every defense has its own weaknesses

Endpoints can be compromised and footprints erased

Log Everything-Once Logged in network it stays forever

Enhance Resiliency



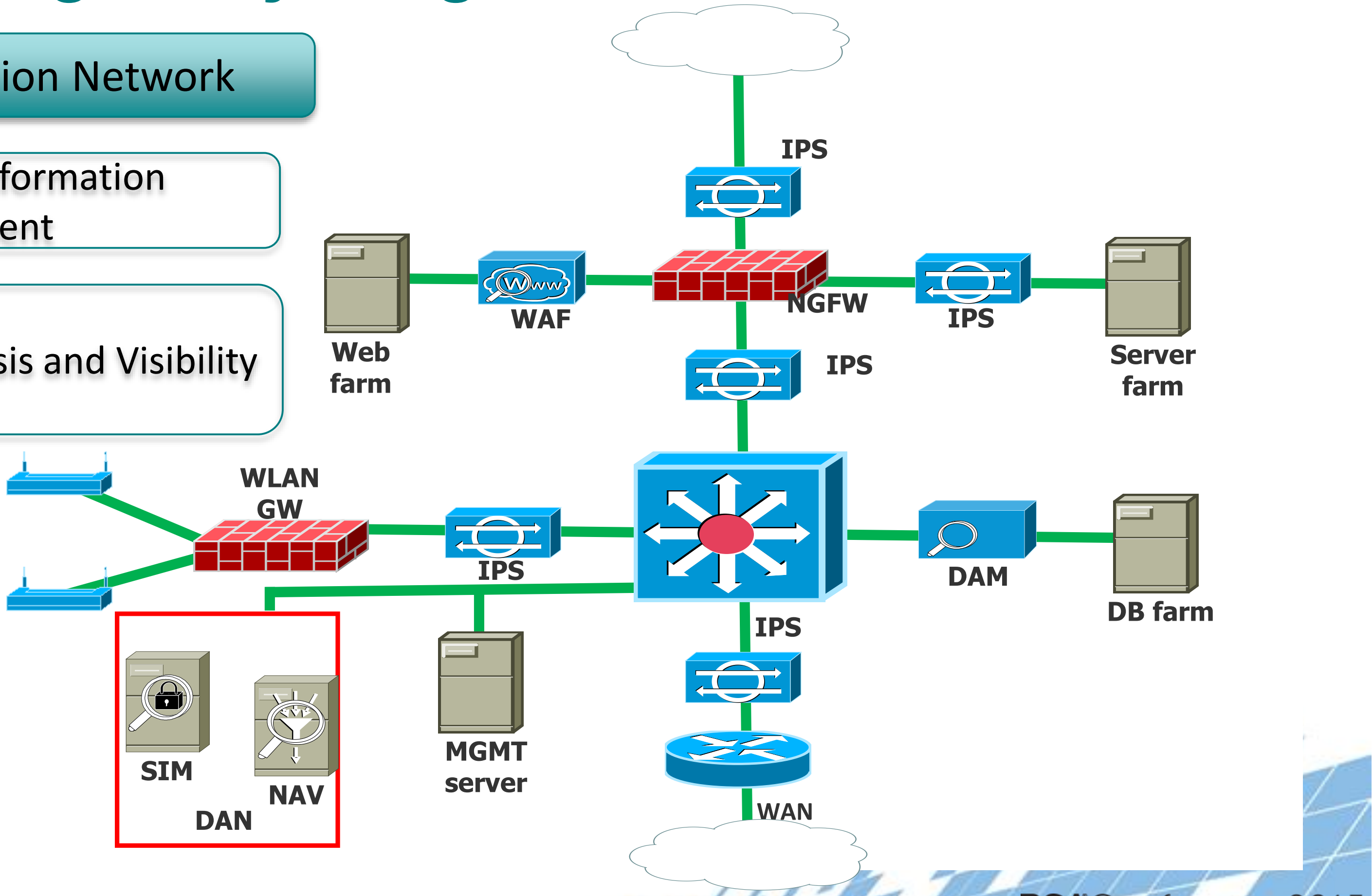
```
A  rt: Access from ip 12.1.21.1
A  rt: Port snoop detected in zone
H  h: D                          n
L  : Unencrypted PDF sent detecte
          Korean IP detected at zo
```

Inspect and log everything

DAN – Data Acquisition Network

SIM – Security Information Management

NAV – Network Analysis and Visibility

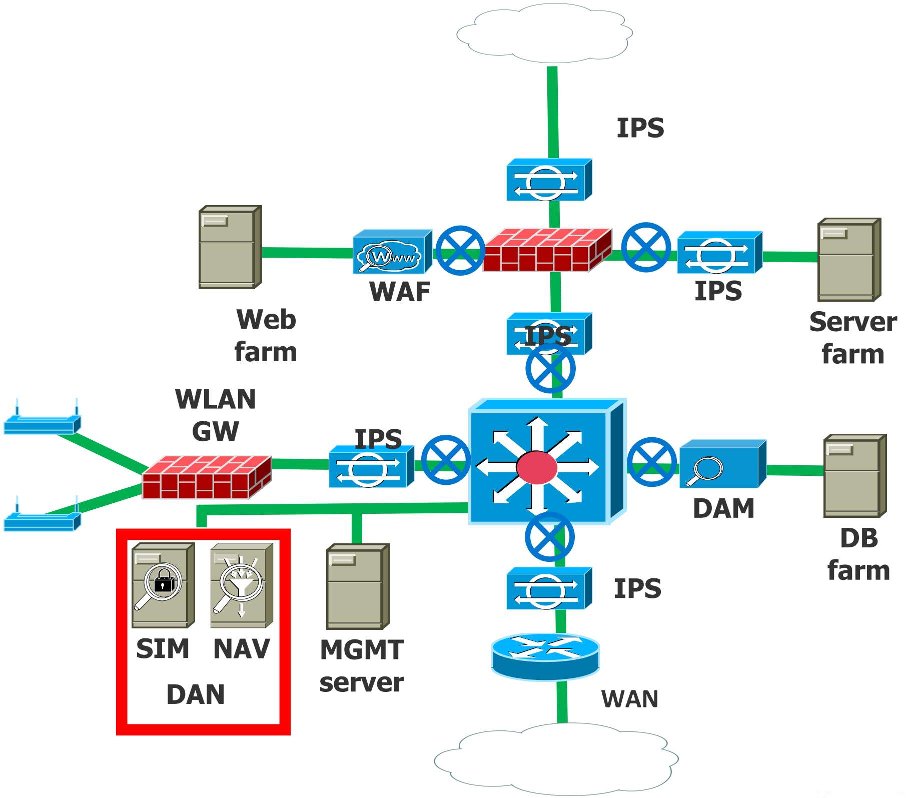


Building a DAN

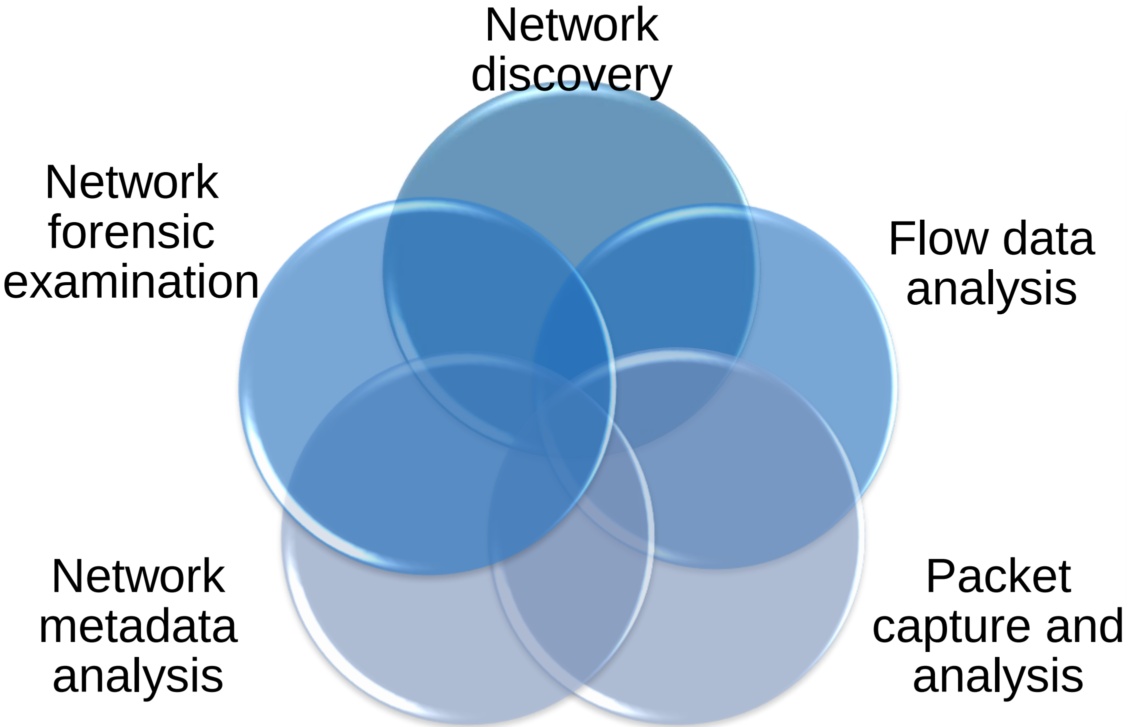
SPAN Ports are ineffective

TAP all internal traffic

Send everything intelligently to SA



Network Analysis and Visibility (NAV) is a diverse set of tools with similar functionality


Network discovery
Network forensic examination
Flow data analysis
Network metadata analysis
Packet capture and analysis

Provides scalable insight into the network

- Verifies access and behavior.
- Reconstructs and reviews application level traffic.

Sends a message to potential malicious insiders

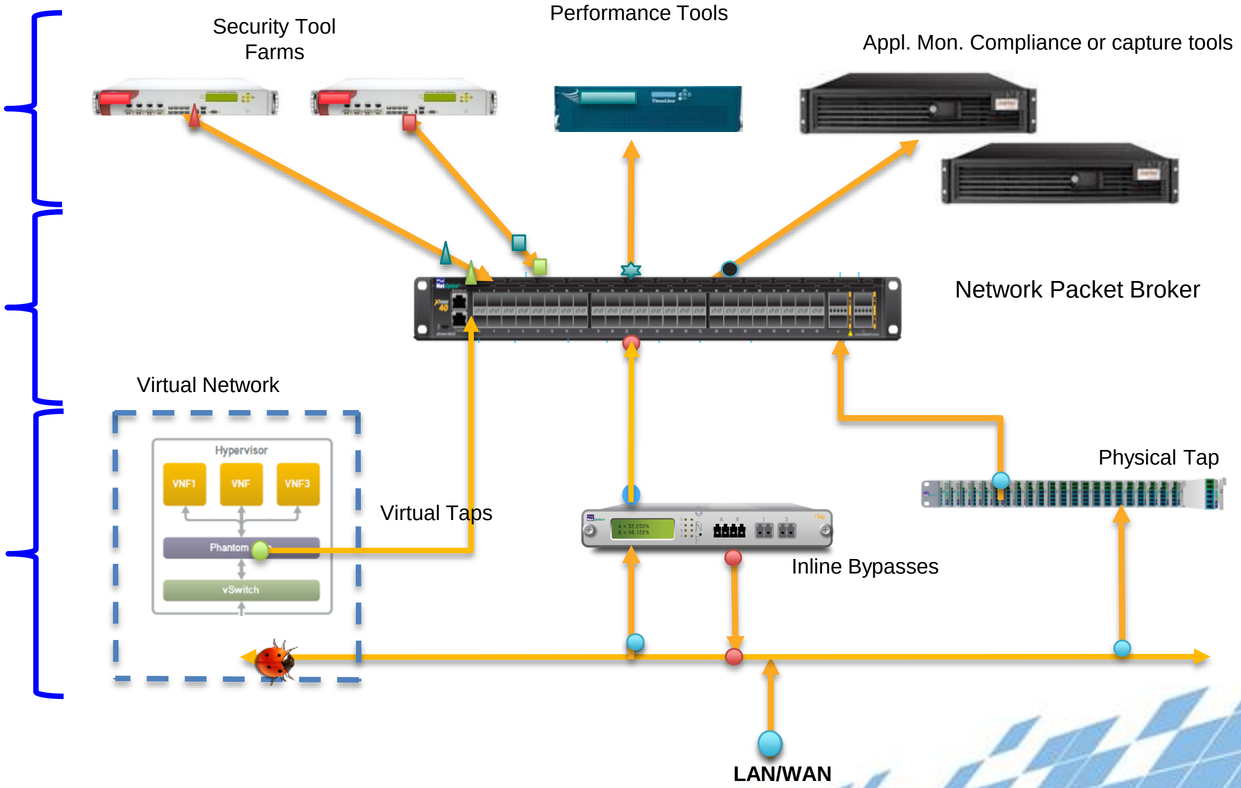
- Changes user behaviors.
- Reduces temptation

Visibility Architecture Data Flow

Monitoring Layer tools provide analytics and performance metrics

Control Layer
NPBs for filtering, load balance, aggregation, regeneration

Access Layer Virtual Taps
Physical Taps



To Summarize

Understand your network status and present needs

Remove assumptions and focus on Data Driven Investments – **Trust but Verify**

Be prepared for eventuality – RESILIENT Architecture

Implement Complete visibility and Intelligent logging to ensure there’s no place to hide