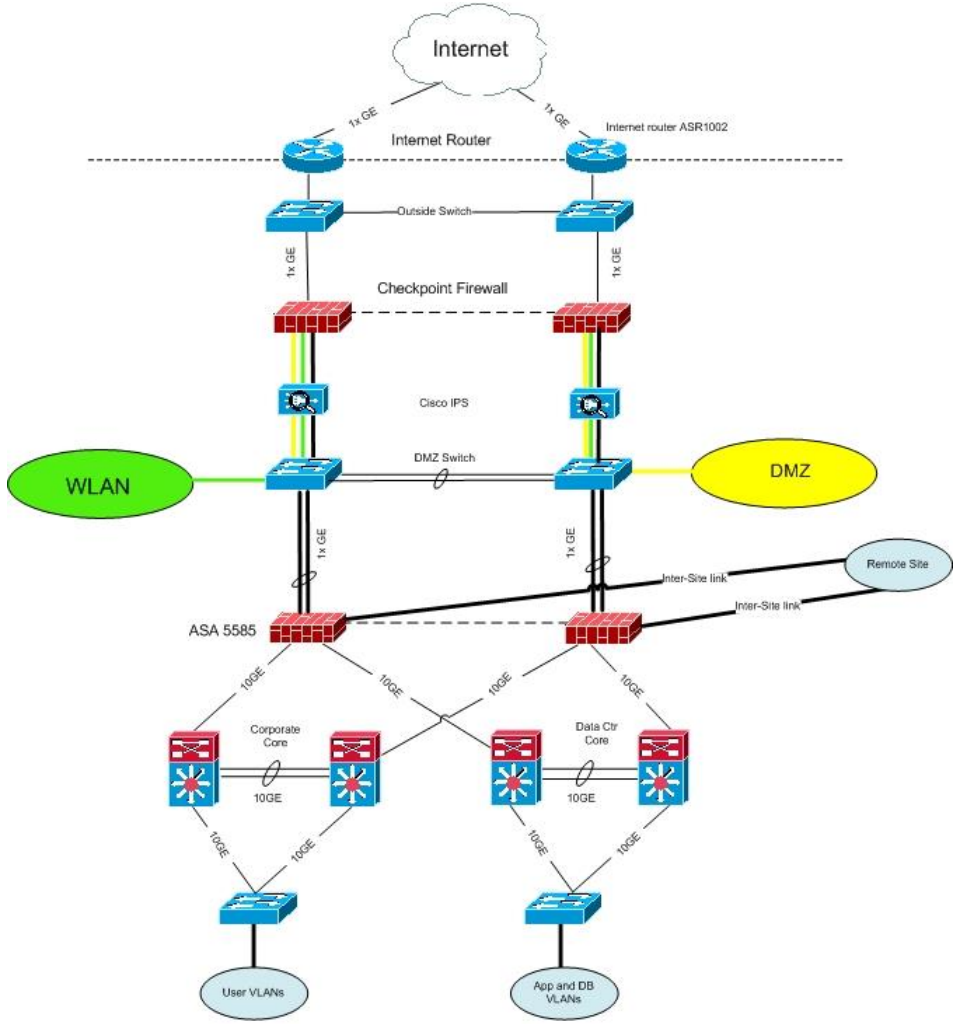
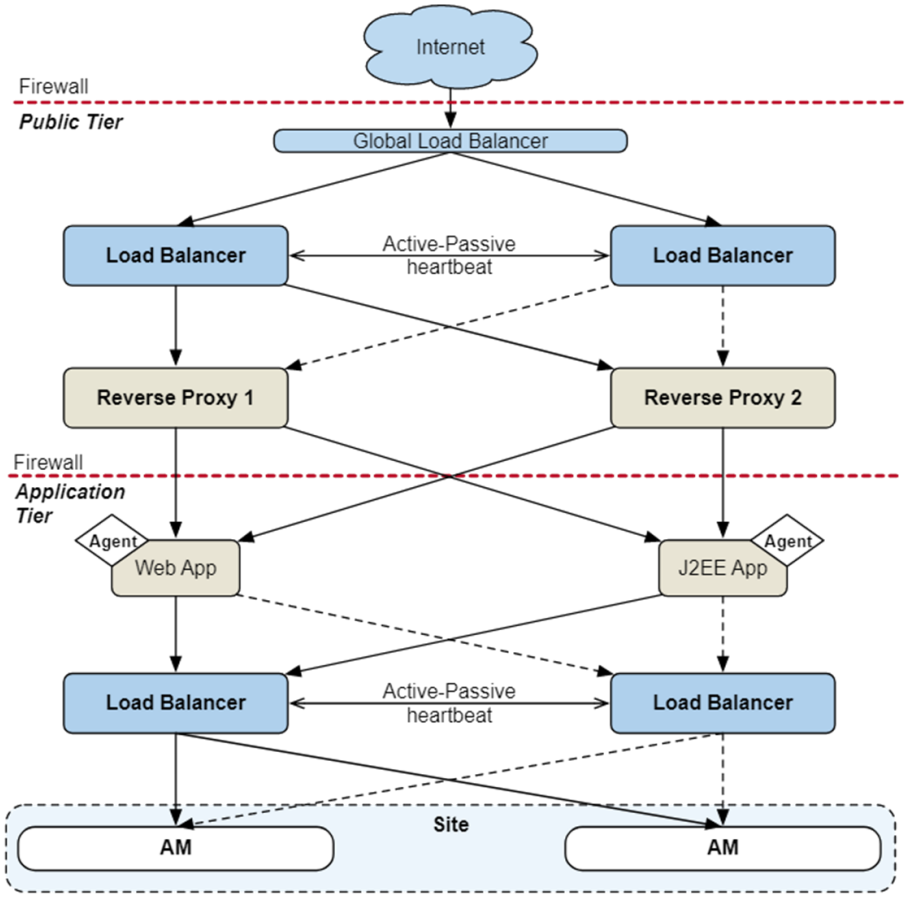
hosting IDC security project(Multi-Tier)



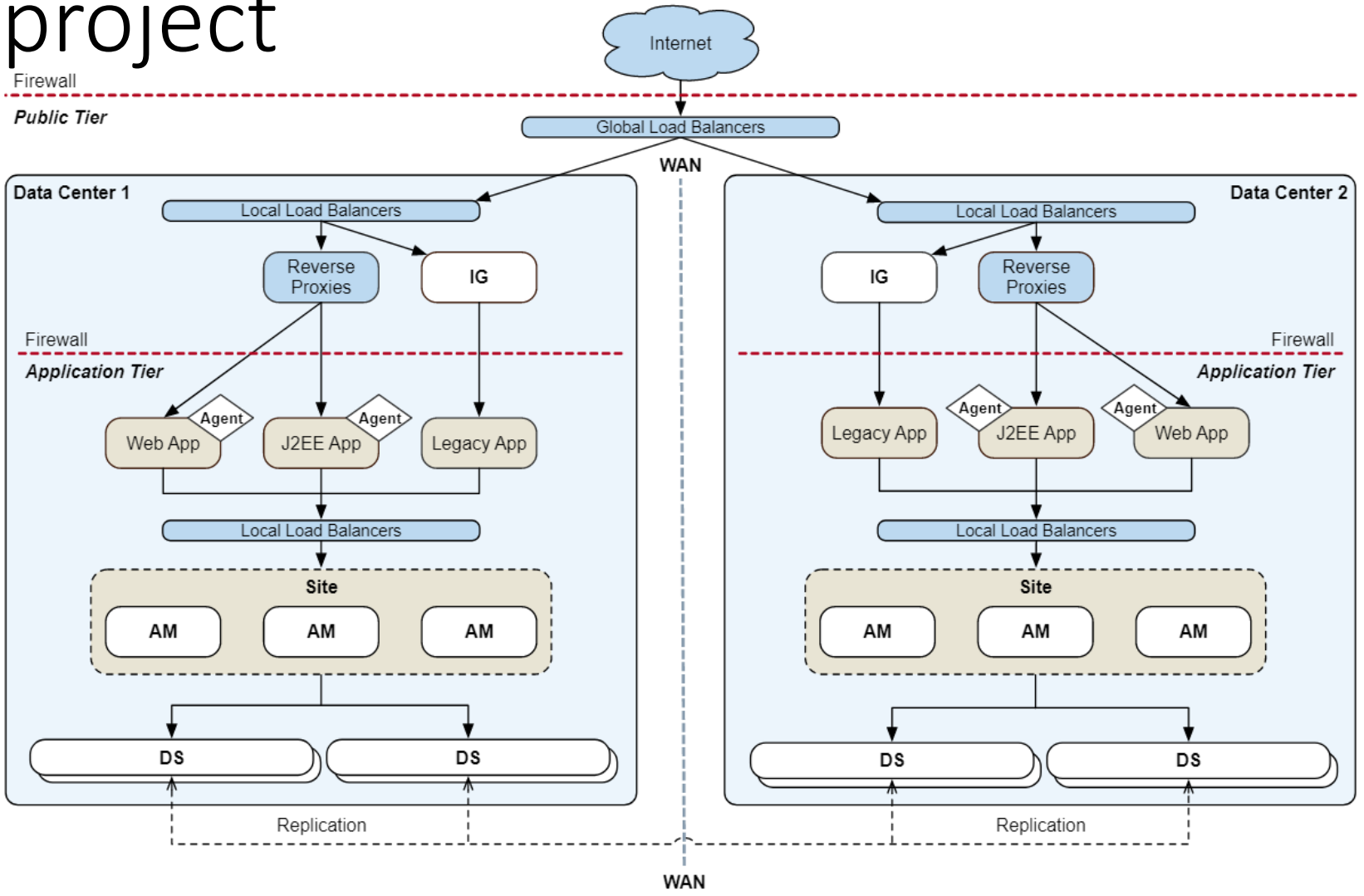
Multi tier firewall (Cisco, Juniper/netscreen, checkpoint)
IPS (Snort, Cisco IPS)
Load balancer/SSL accelerator (alteon/Cisco CSS)

Banking (online banking—ESI1) project



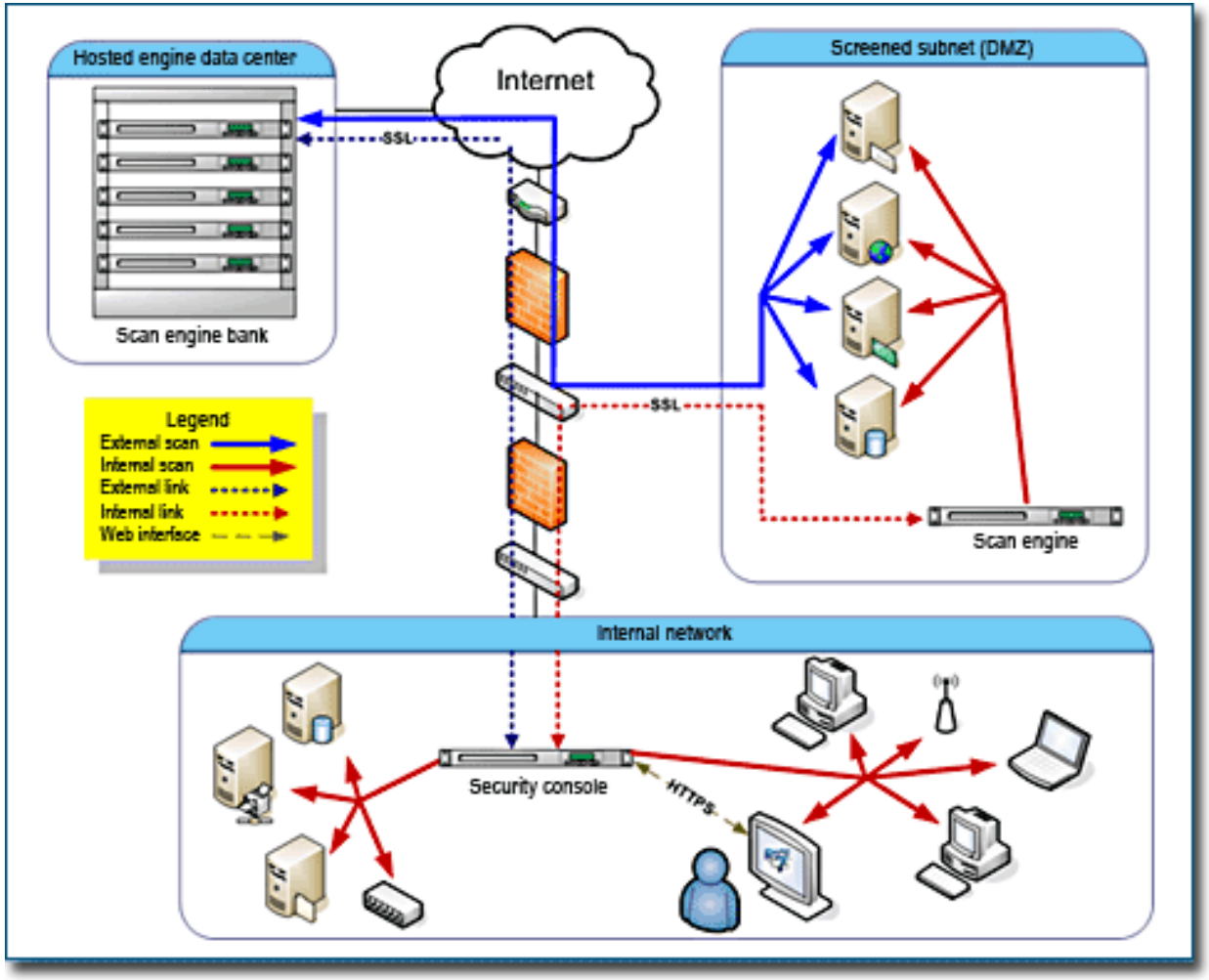
- Firewall(checkpoint NG, juniper SRX)
- Load balancer/SSL acceleration (Alteon, F5 LTM/GTM, Citrix netscaler)
- secure proxy (IBM webseal/reverse, bluecoat SG/forwaring)
- IPS (IBM ISS prevention, checkpoint smartdefense IPS-1)
- Identity manager/Access manager (IBM TIM/TAM, oracle OIM)
- XML secure GW (IBM datapower)
- vulnerability scanner (IBM Qradar, rapid7)

Banking ESI-1 security TAM infrastructure project

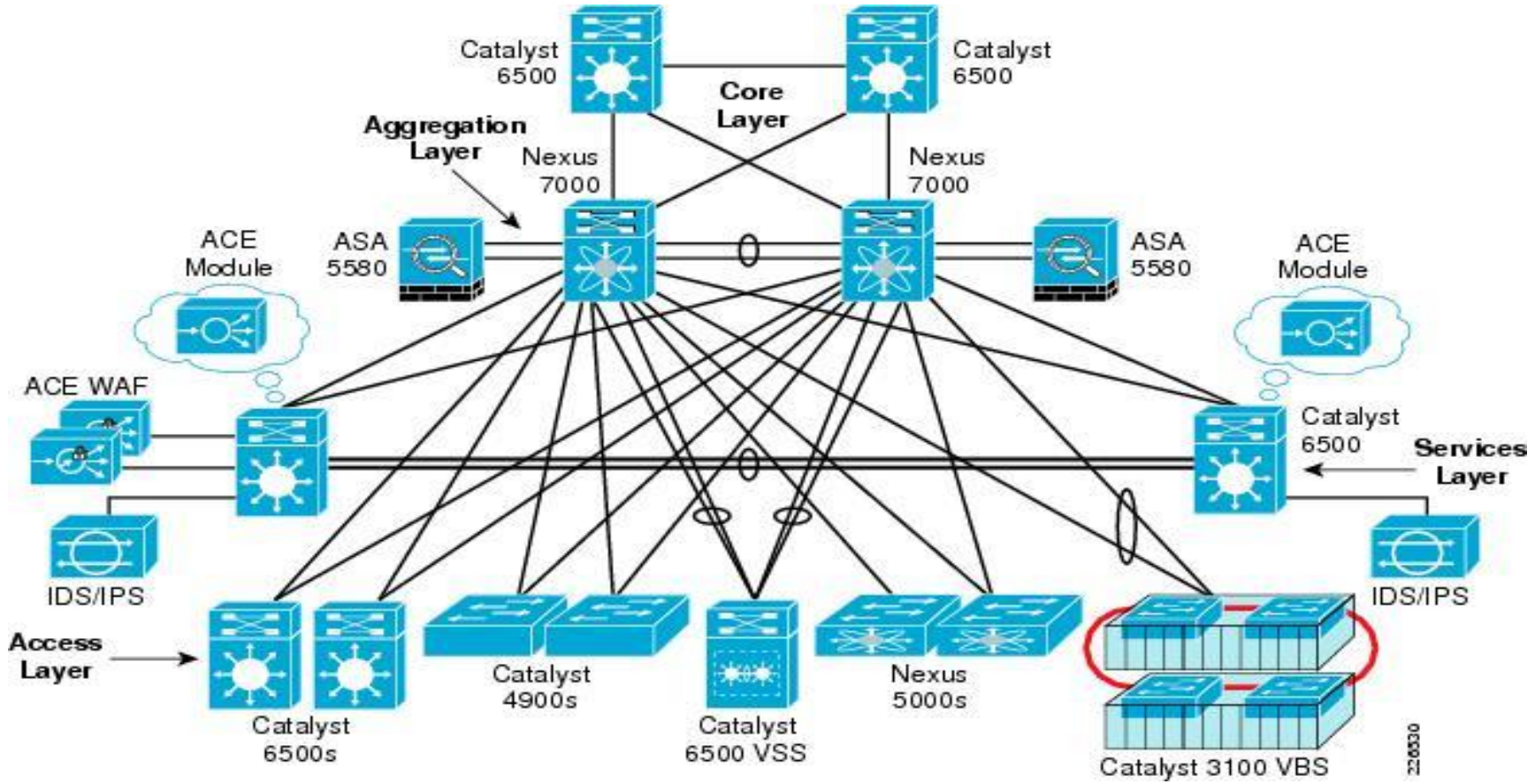


- **TAM access management**
  Cookie Reset.
- Authentication-Only Mode
- Not-Enforced Lists.
- URL Checking and Correction.
- Attribute Injection.
- Notifications.
- Cross-Domain Single Sign-On (CDSSO)..
- POST Data Preservation.
- Continuous Security.
- Conditional Redirection.

Banking vulnerability scanner project

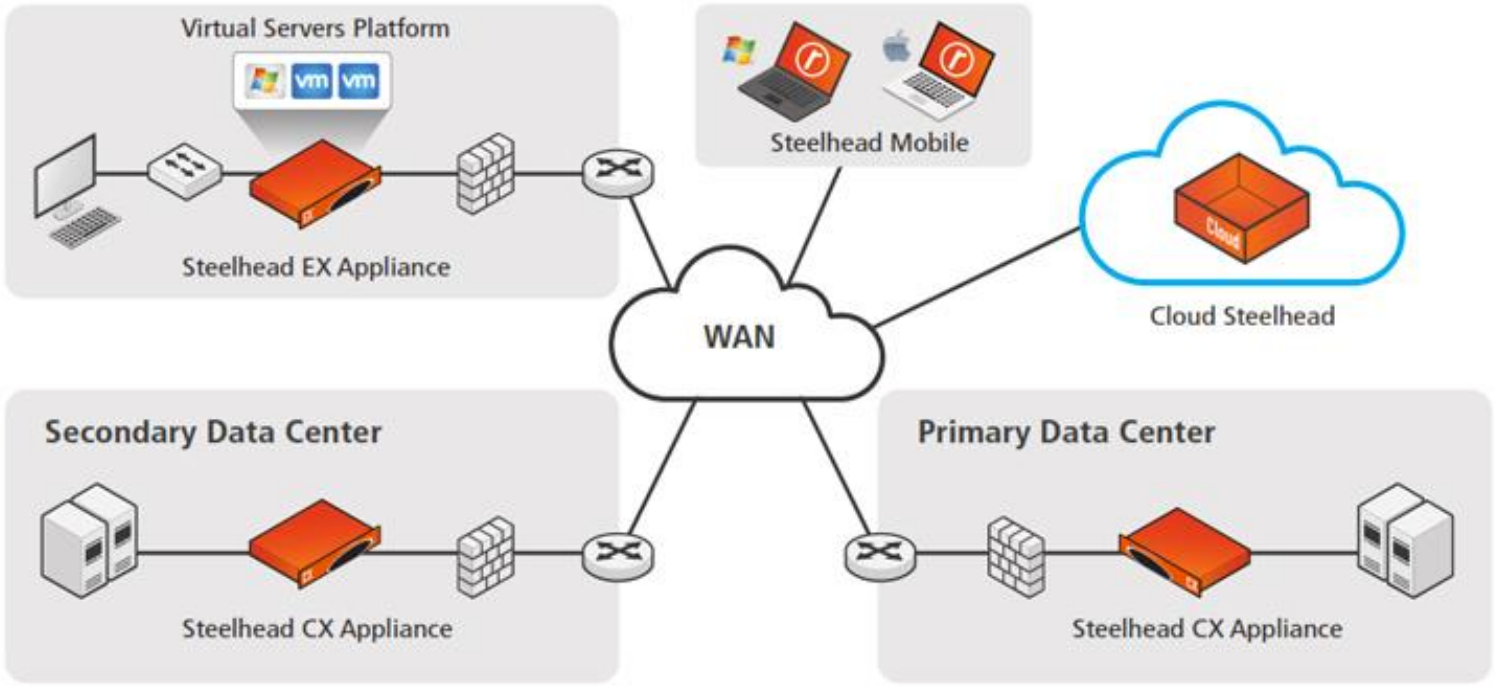


IB New DC segregation project (Warwick+Shatian PDC/BDC)



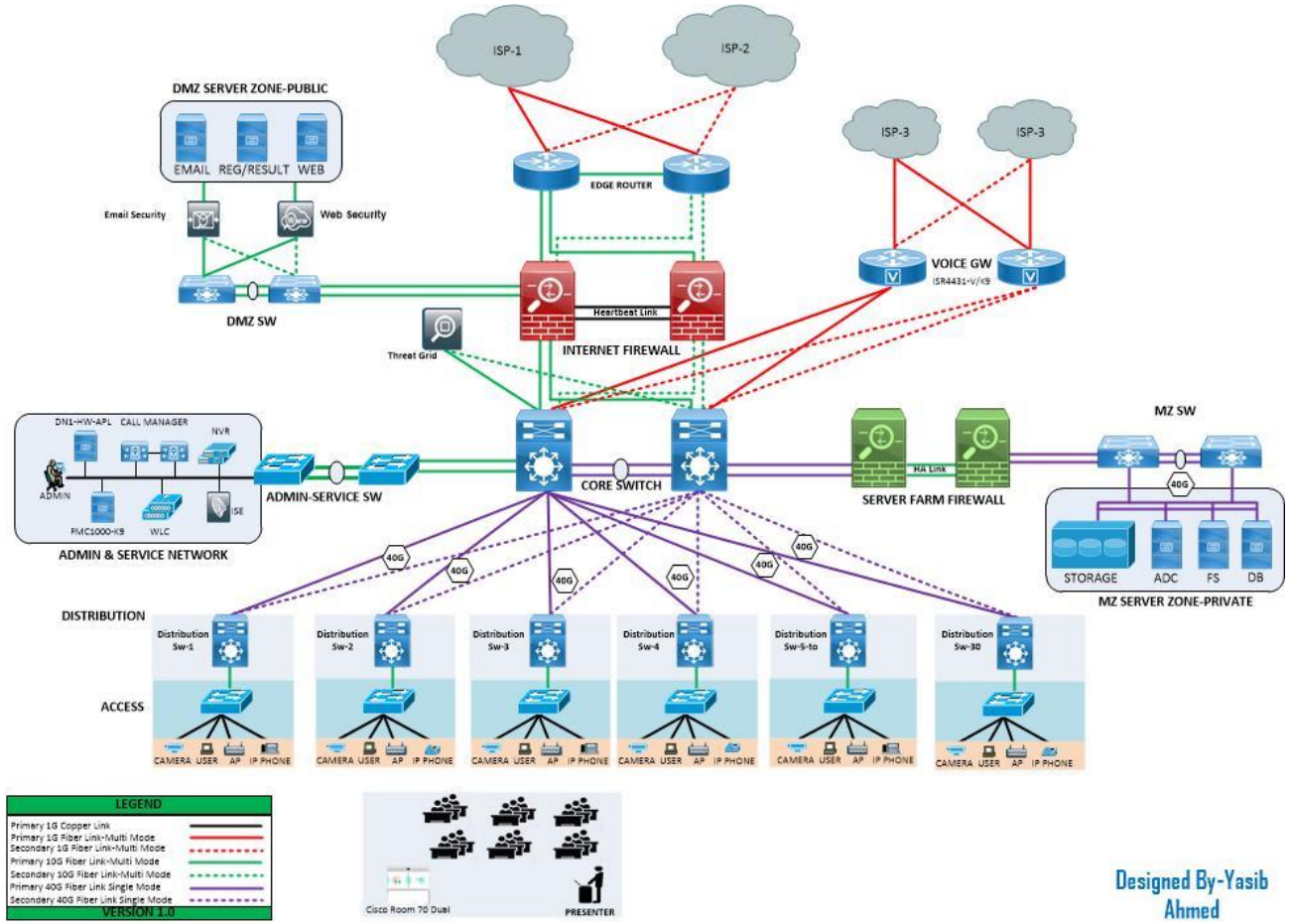
SD-WAN WAN optimization project

FIGURE 1. ACCELERATE EVERYWHERE: STEELHEAD CX SERIES IN A RIVERBED DEPLOYMENT



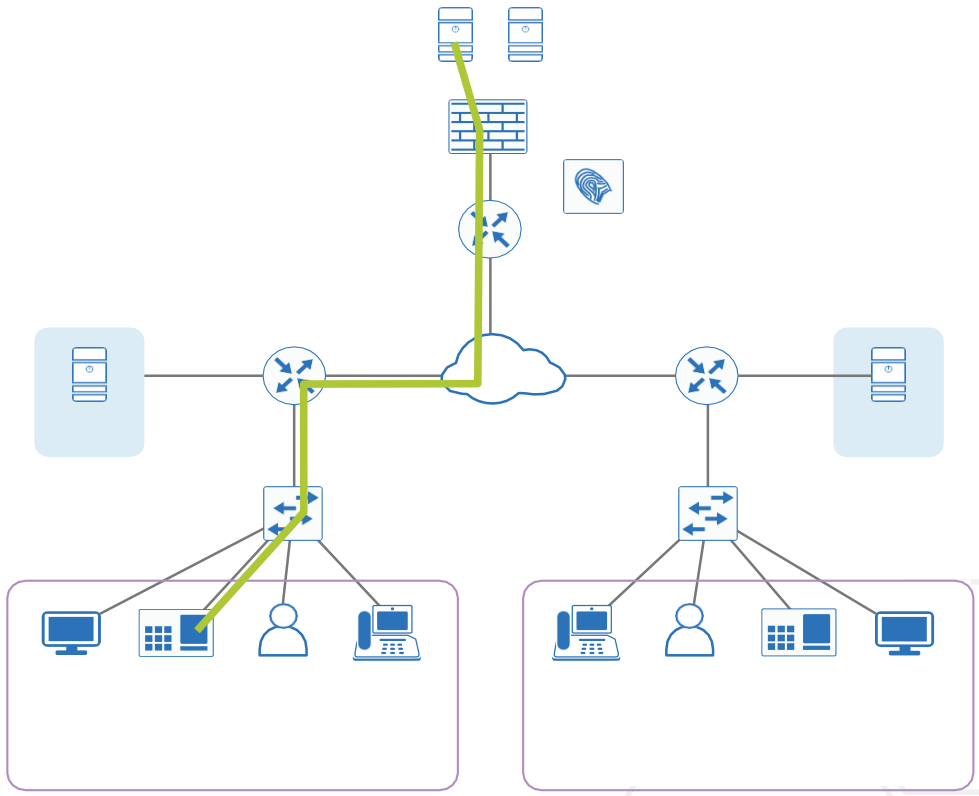
WAN Optimization traffic
MS-Exchange/email
NFS/CIFS
VDI
applications fit-for caching
WCCP protocol

Investment banking security segregation project

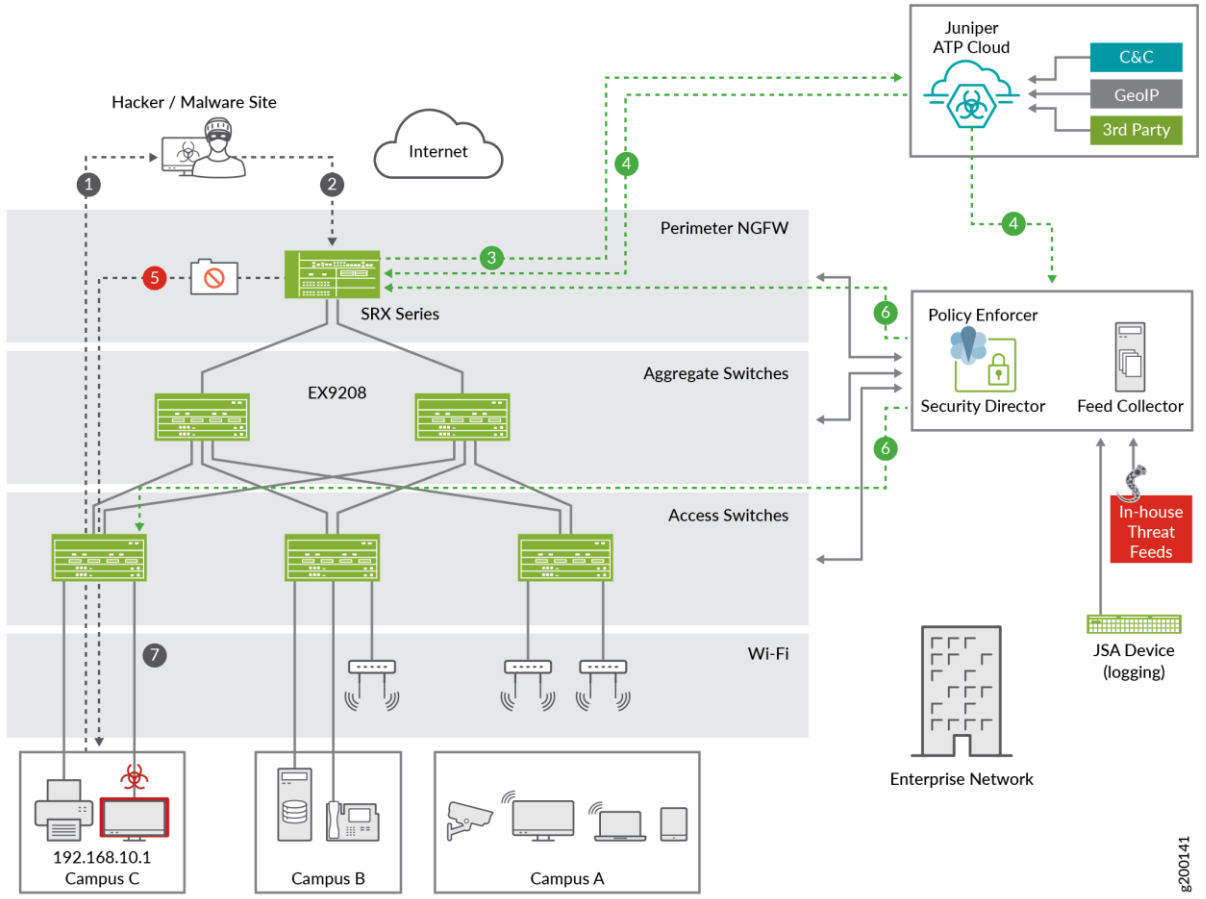


IB SG Internal trading security segregation

- Trading floor segregation design

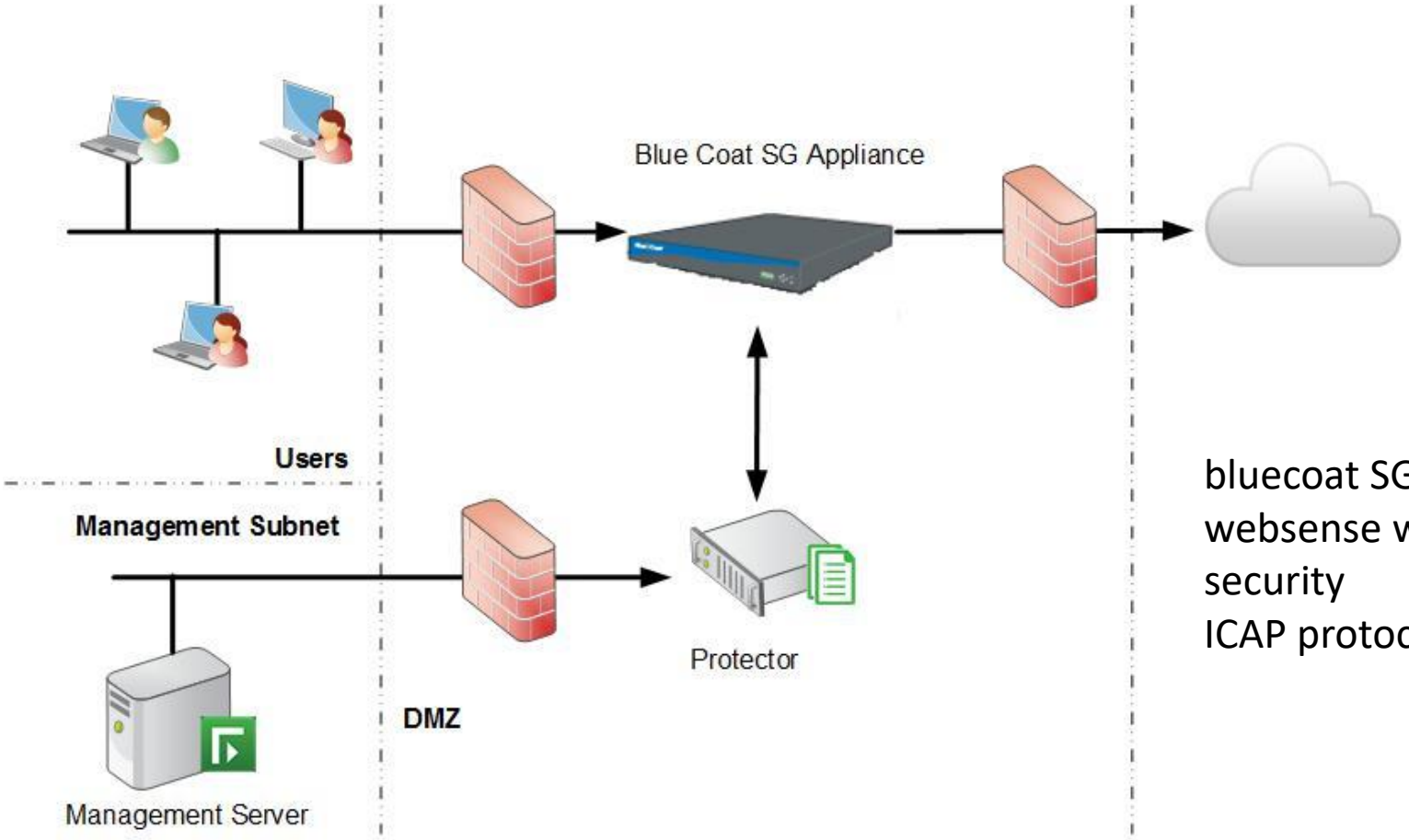


IB SEA SIG(secure internet GW) project stage1



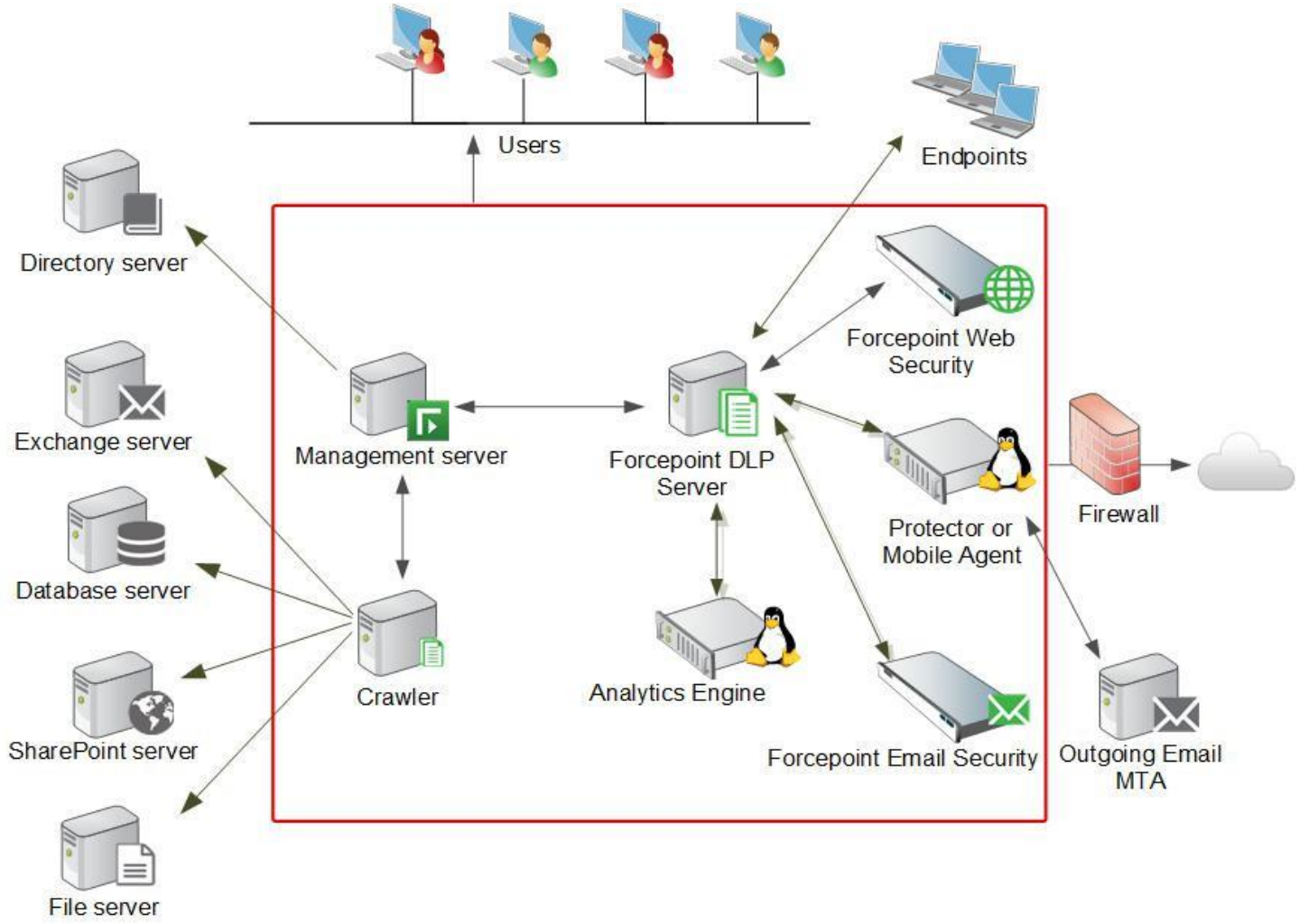
Juniper NGFW/IPS
policy director, JSA(security analytics engine)

IB SEA SIG DLP project stage2



bluecoat SG forward proxy
websense web content security
ICAP protocol

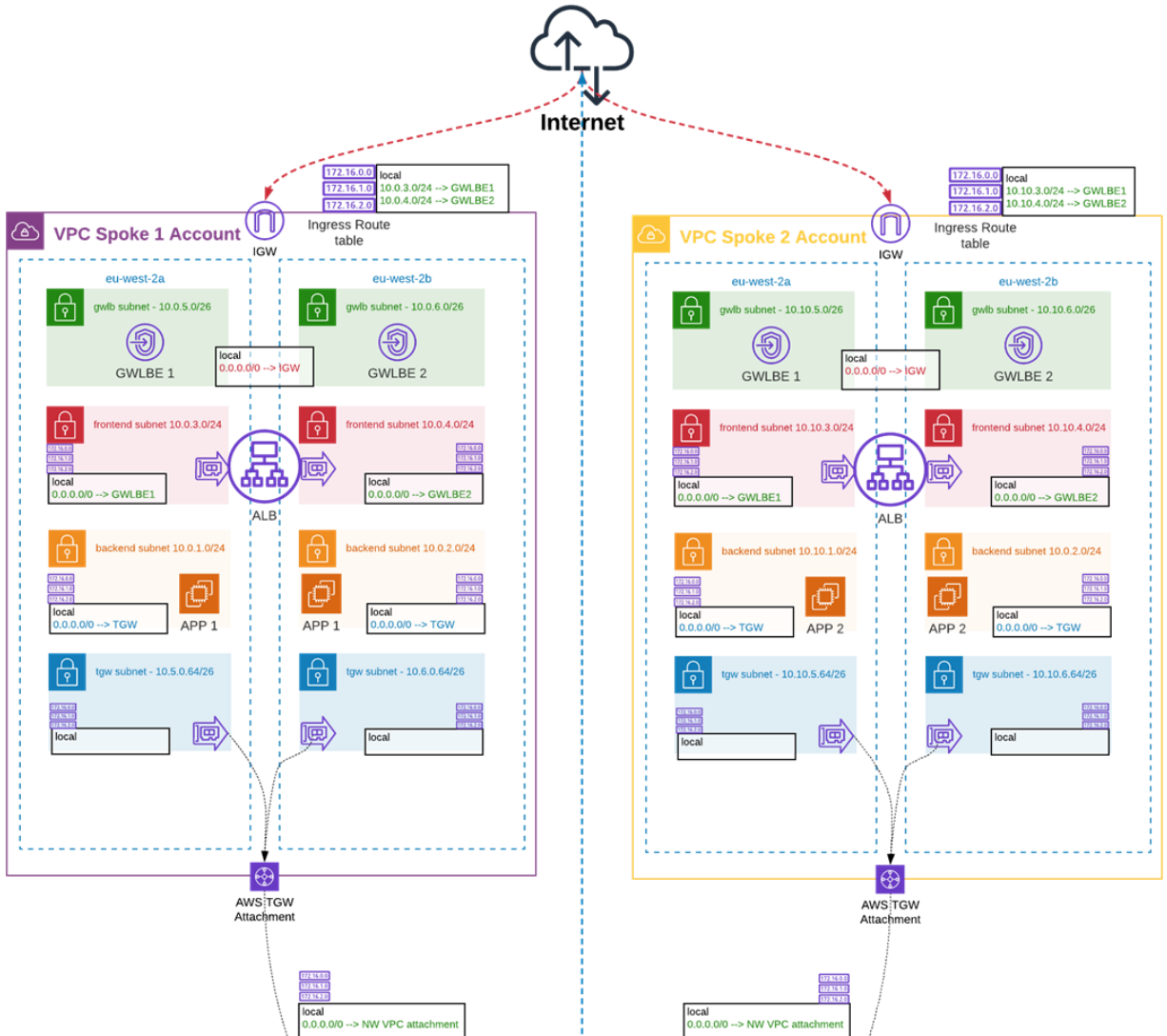
IB SG SIG DLP project(stage 3)



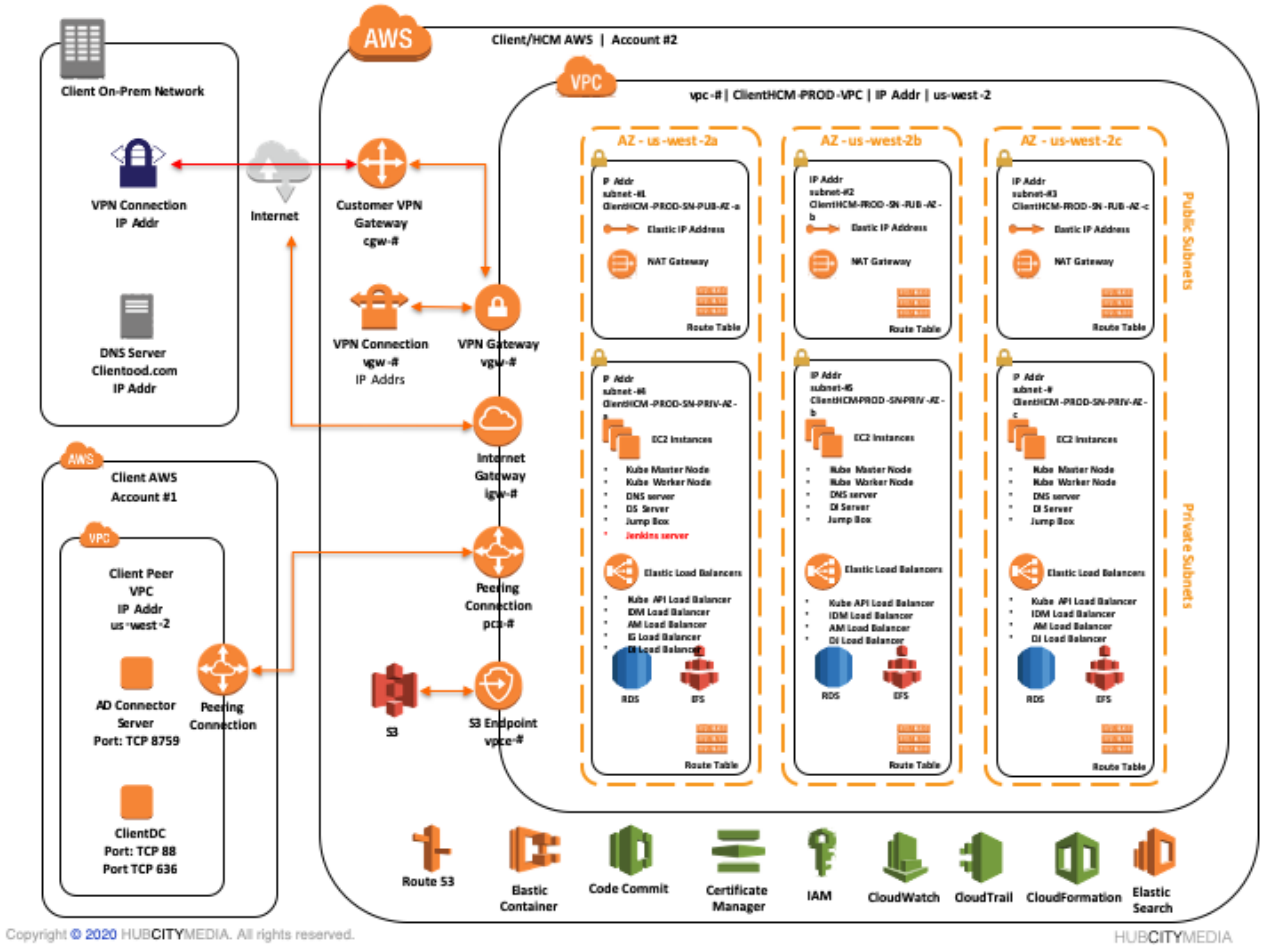
Websense solution

- DLP appliance
- Web security
- Email security
- Anti Malware security
- Analytics
- Data discovery/crawler
- Management

AWS cloud security enhancement project



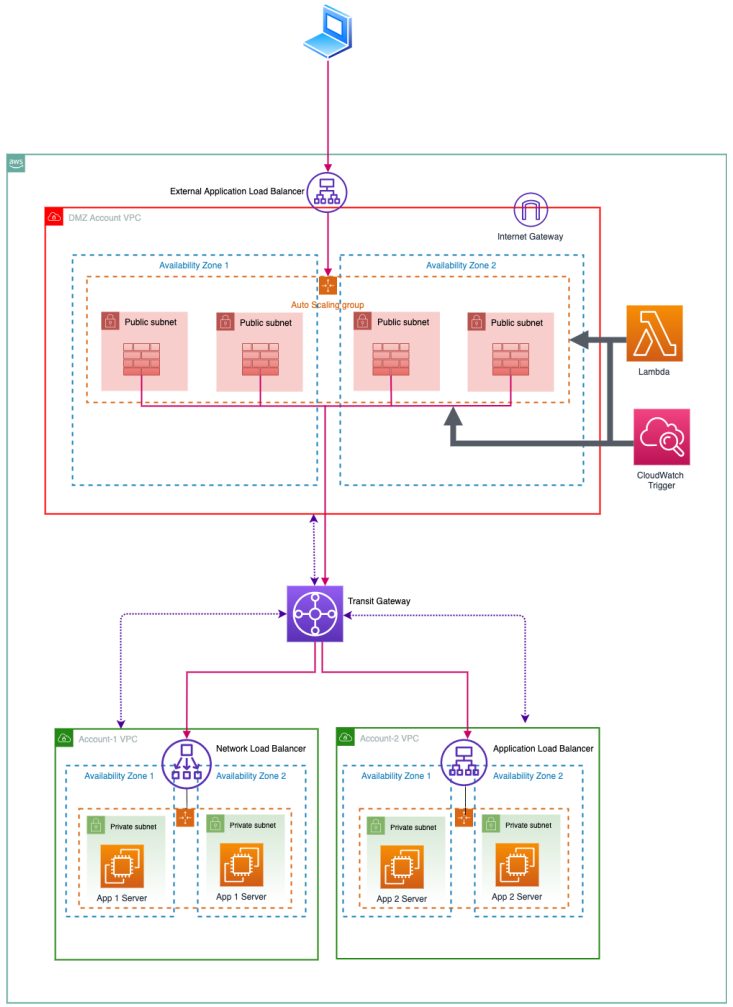
AWS cloud Identity+ Access manager project



HUBCITYMEDIA

AWS default solution
Federal SSO
SAML2.0+ IAM SSO connector

AWS marketplace security (BYOL) project

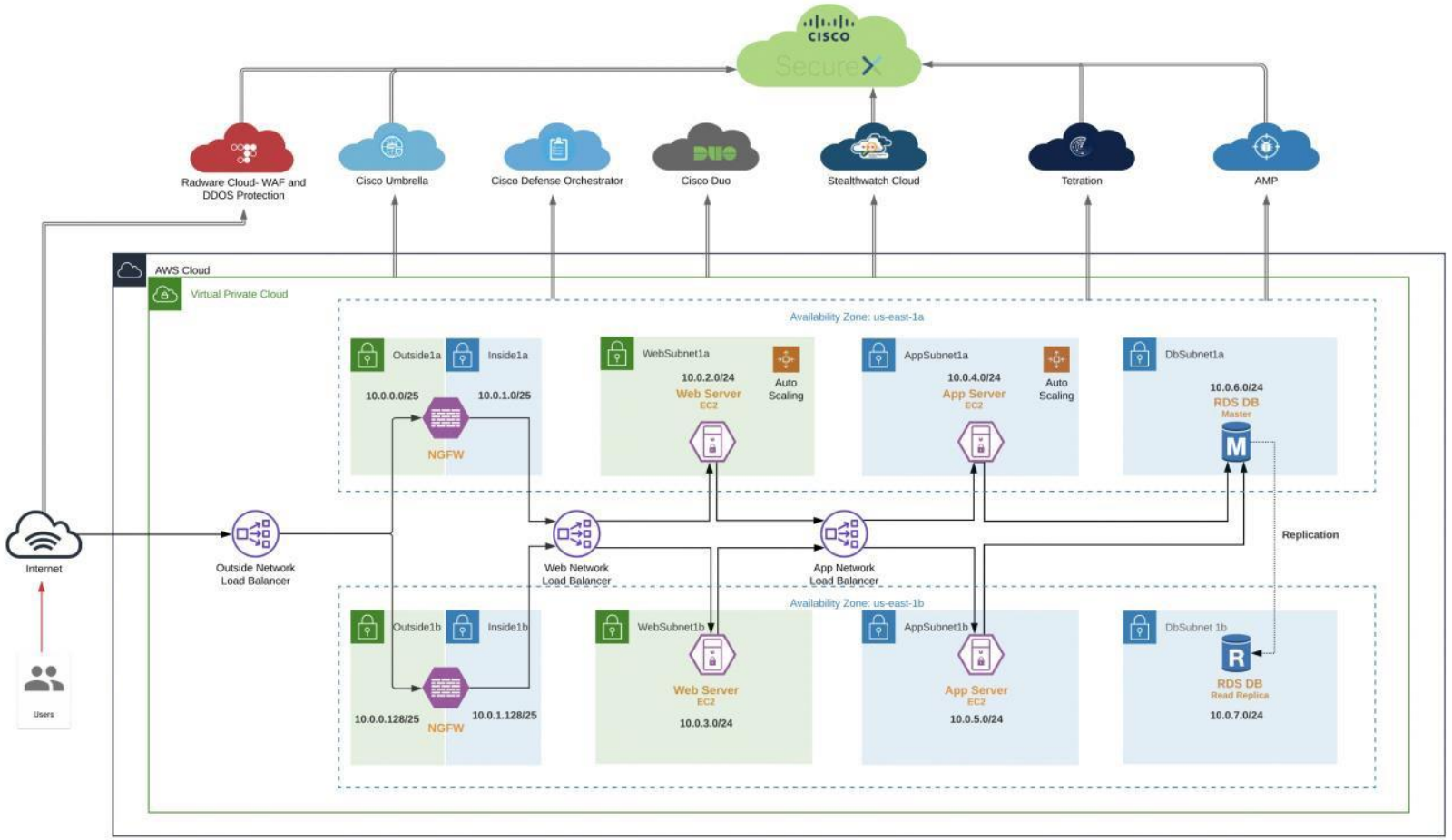


Replaced the default AWS open source security solution
With AWS VPC marketplace vendor vcloud solution
Virtual appliance

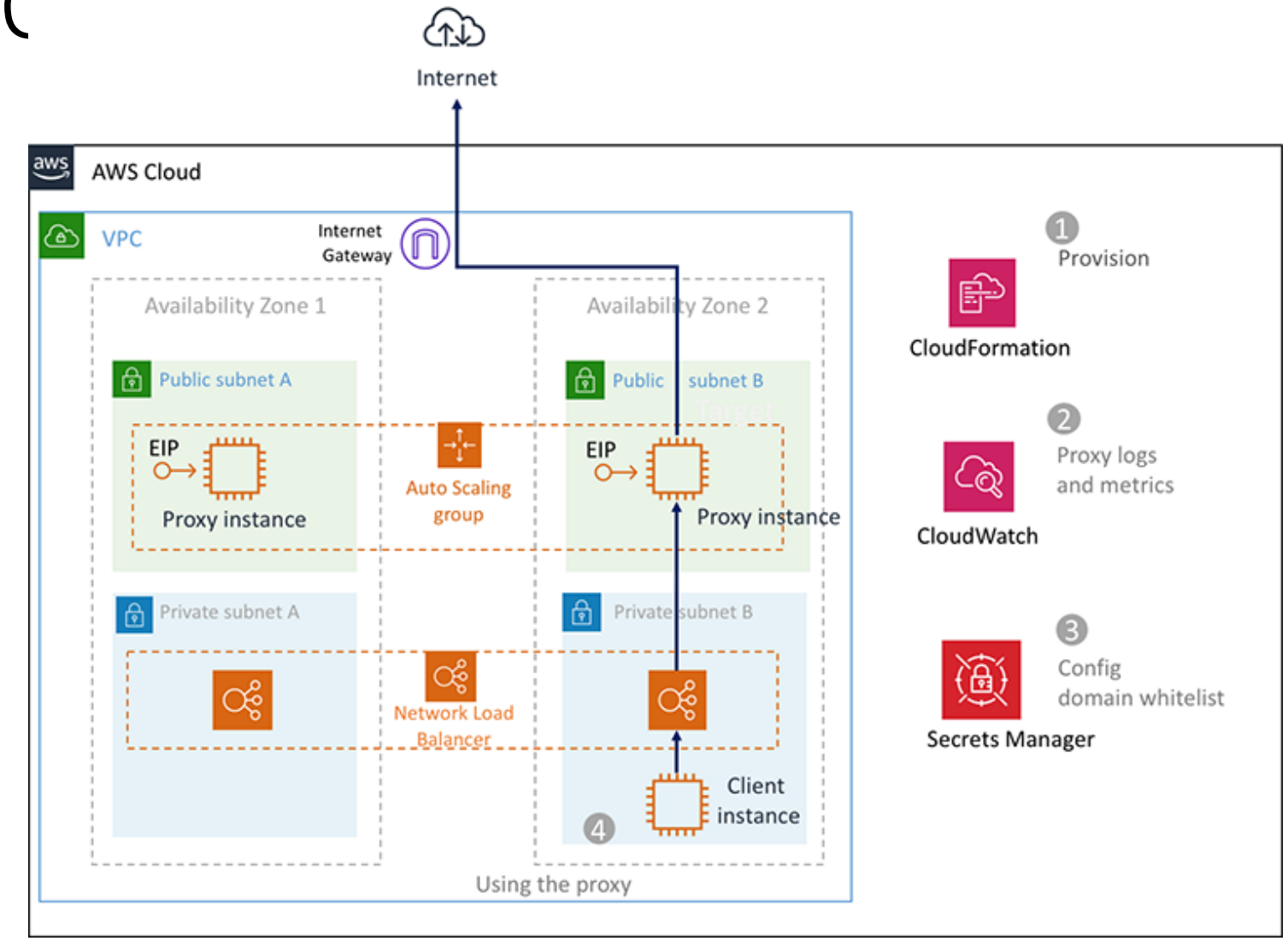
- Cisco(FW+IPS+Content security)+ secure
- Critix netscalerADC
  Symantec SG virtual proxy appliance)
- Cisco security

- Dedicated security VPC was designed and implemented for each region as centralized security control and traffic inspection

cisco cloud security deployment

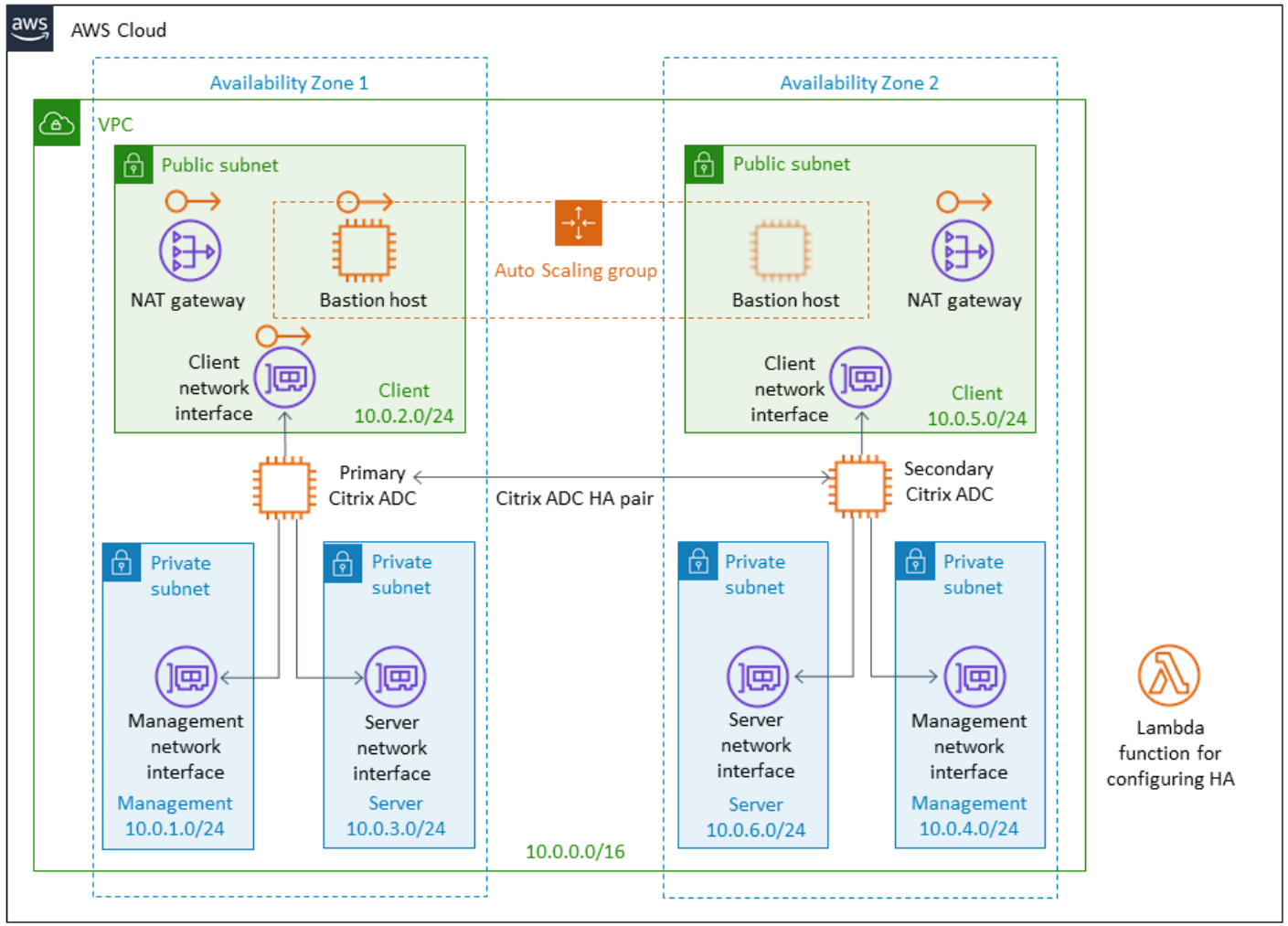


AWS engress outbound proxy virtual appliance (BYO



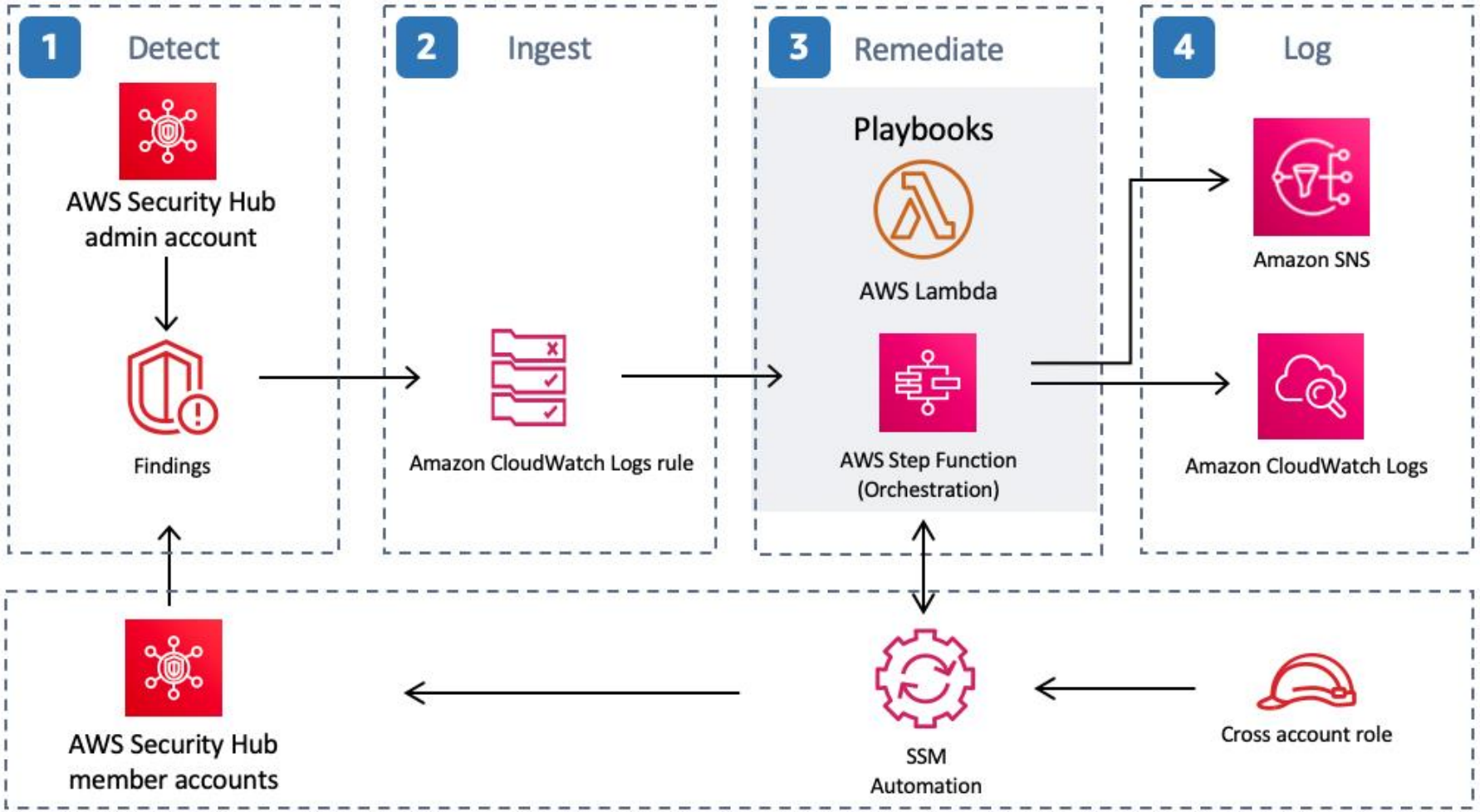
forward proxy

AWS critix ADC/netscaler deployment



load balancer citrix ADC netscaler

AWS security hub integration



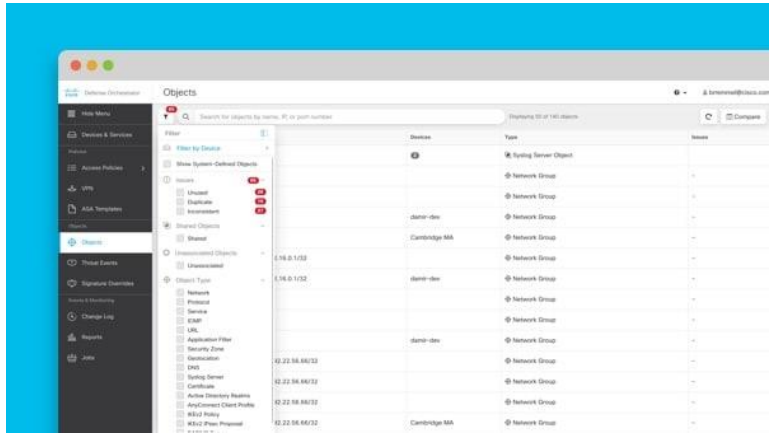
Appendix: legacy premise DC security vendor

Security vendors

- Firewall/IPS/malware(UTM): Cisco IOS, juniper JunOS SRX and virtual firewall vSRX, checkpoint quantum FW, symantec

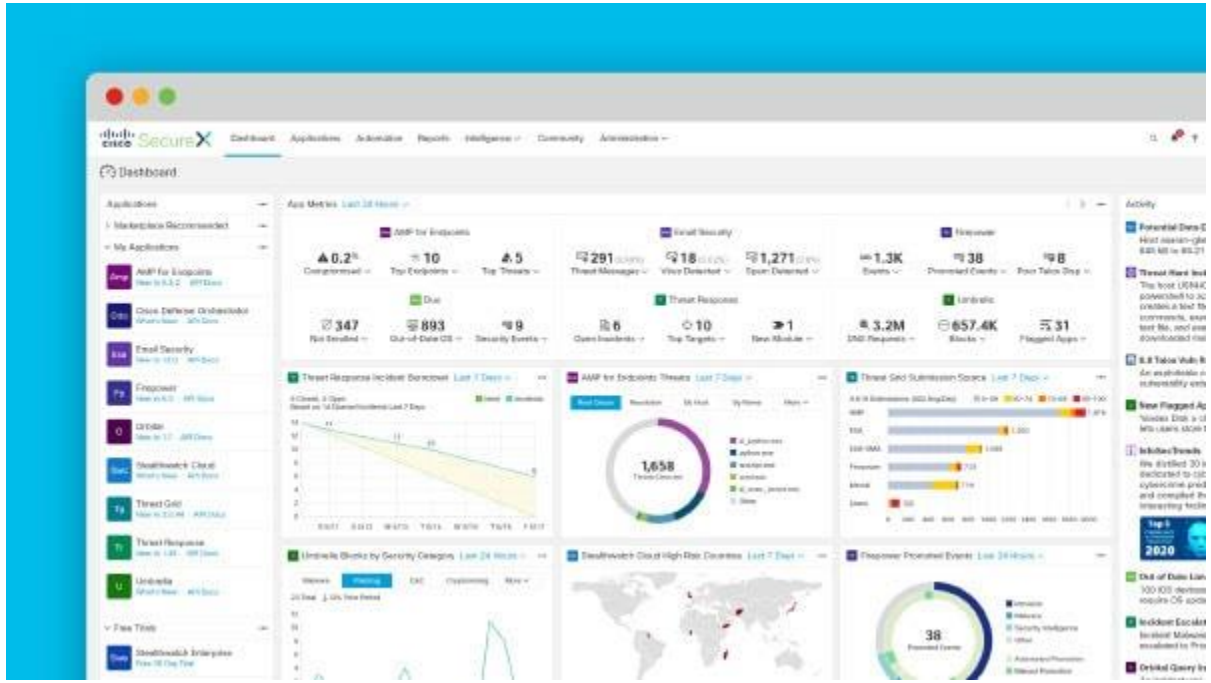
Security Management solution

- Cisco Defense Orchestrator



Firepower Management Centre

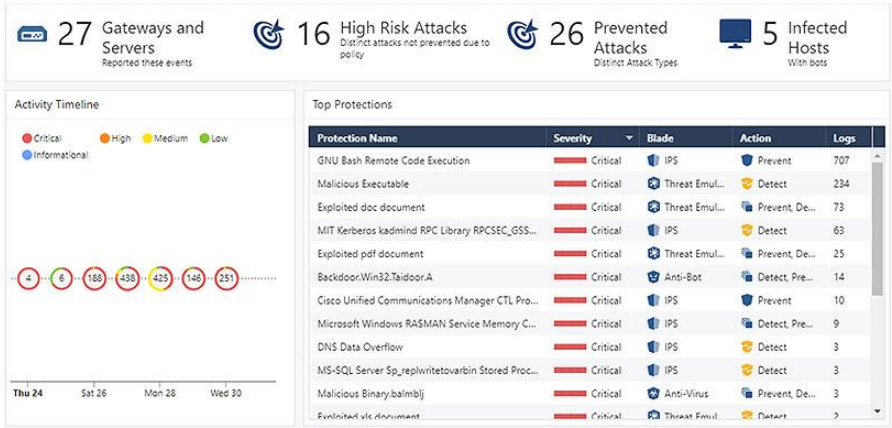
- Cisco SecureX



Checkpoint

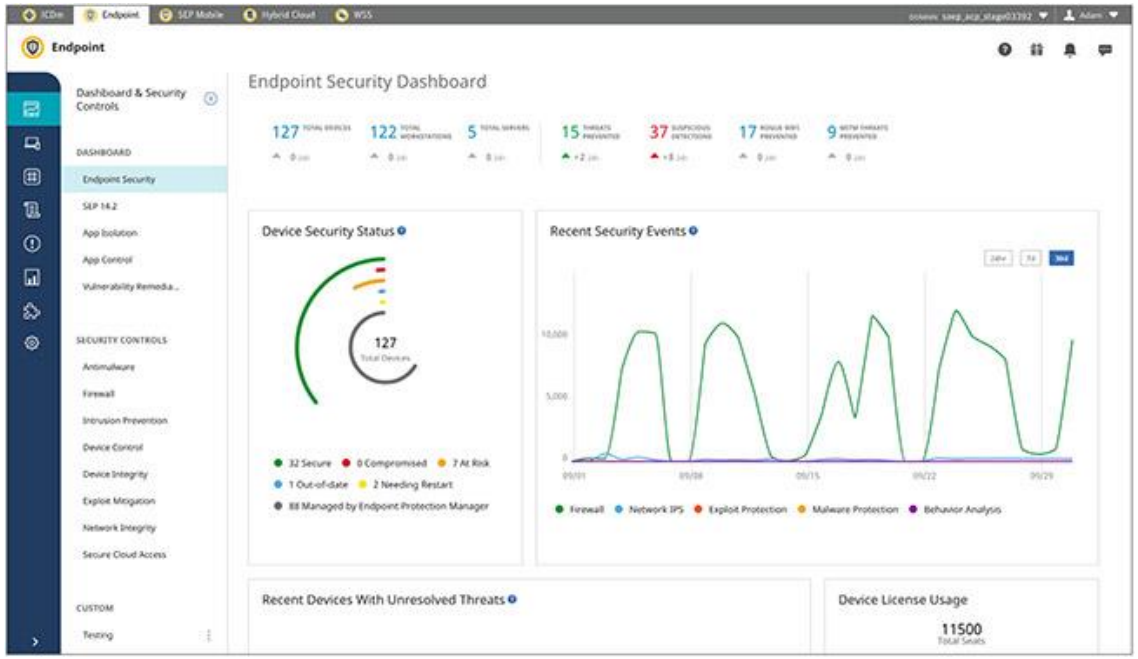
- Checkpoint smart event

Checkpoint smart-1 security management



- Juniper JSA secure management

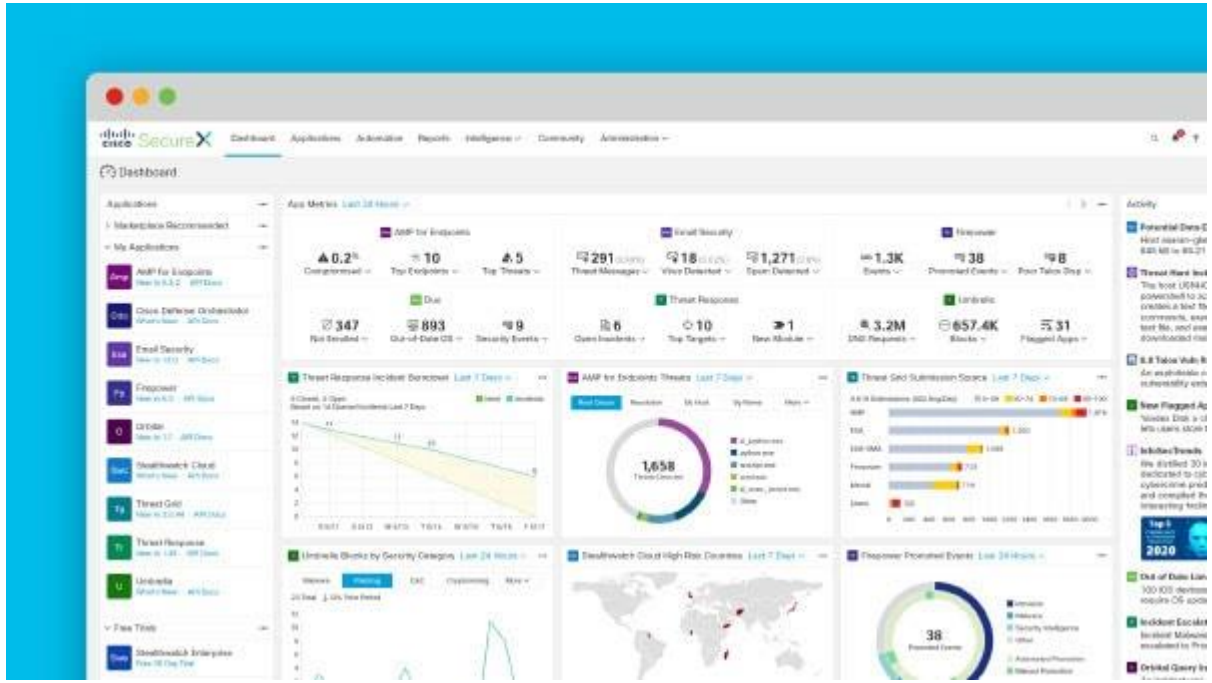
- Symantec director



Cisco umberla End point security management

Security analytics manager

Agentless, scalable, and integrated security- don’t use agent software



- Cisco Advanced Melware protection (AMP)/content filter security
- Juniper AEP
- Symantec
- Checkpoint

Malware security

Email security

Web security

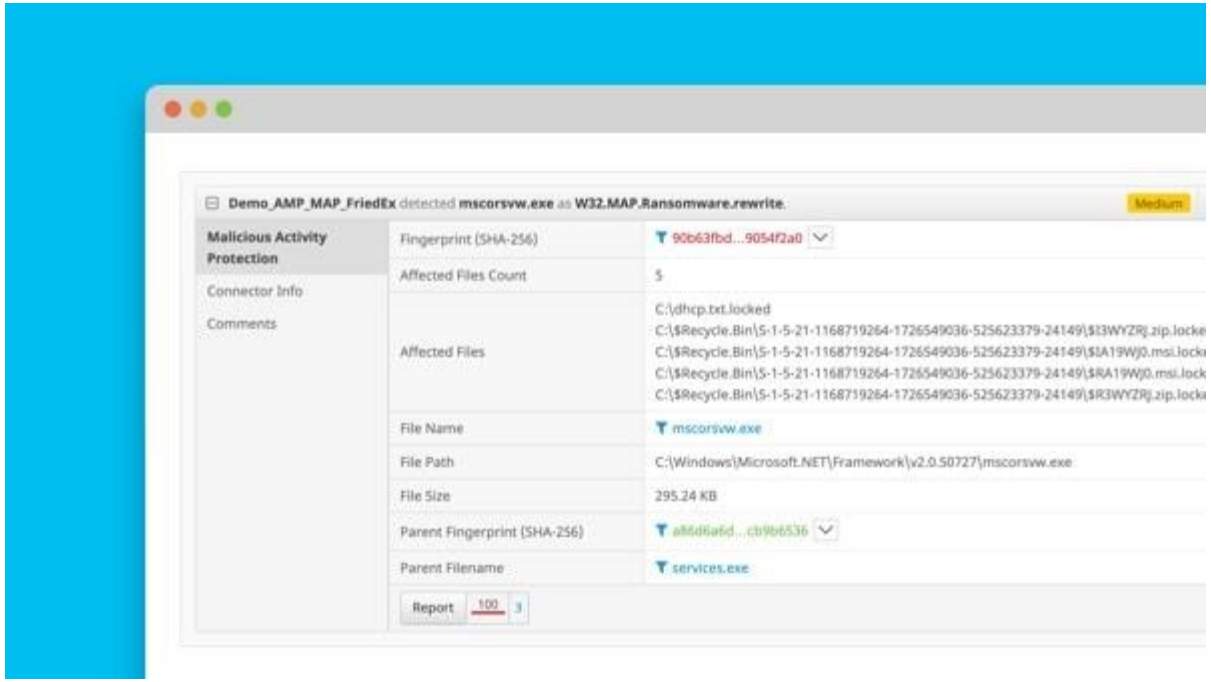
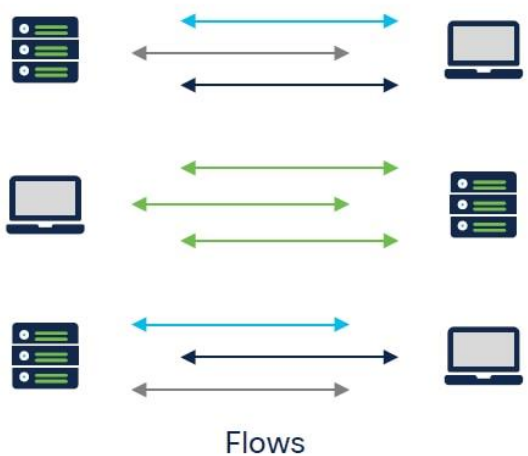


Figure 2. Anomaly detection using behavioral modeling

Collect and analyse telemetry

Comprehensive data set optimized to remove redundancies



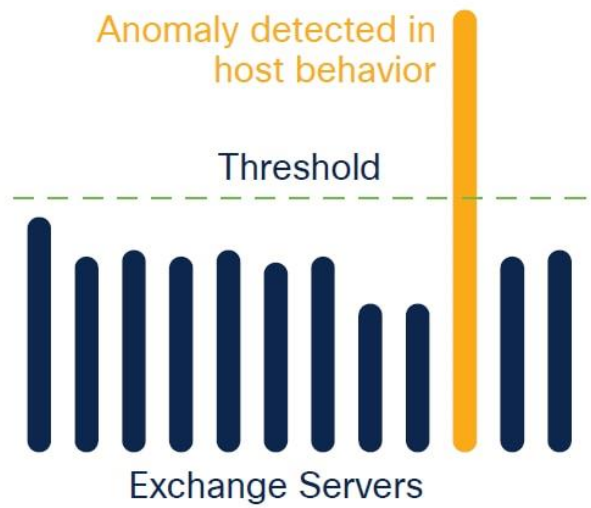
Create a baseline of normal behavior

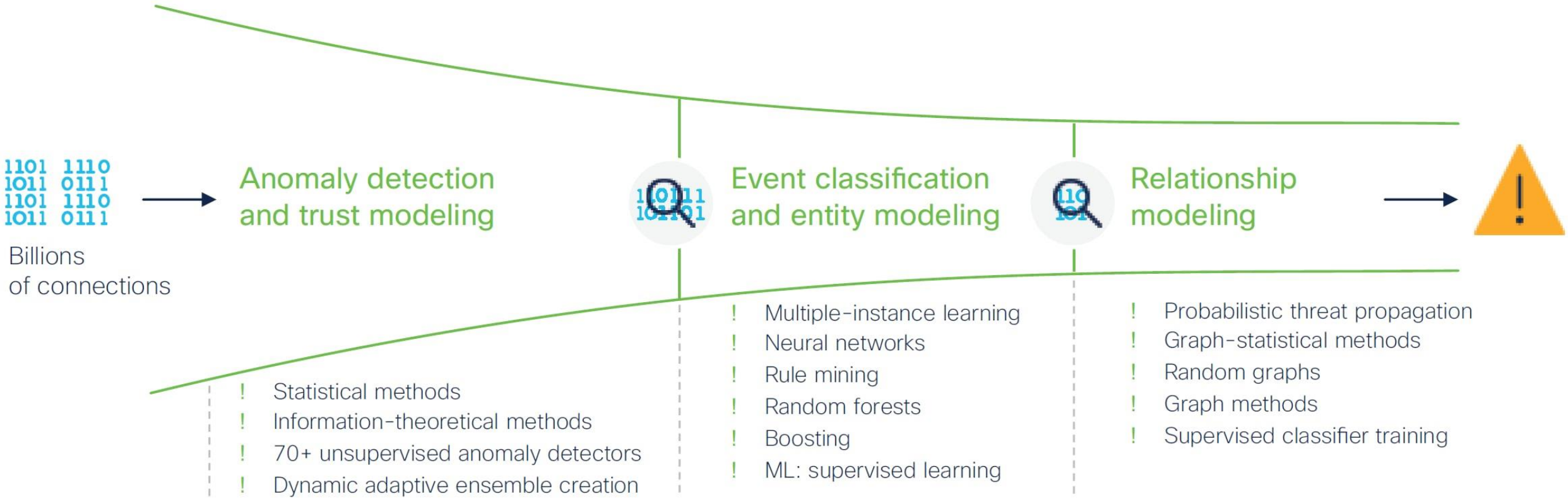
Security events to detect anomalies and known bad behavior

Security Observations		
Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

Alarm on anomalies and behavioral changes

Alarm categories for high-risk, low-noise alerts for faster response




1101 1110
1011 0111
1101 1110
1011 0111
Billions
of connections
Anomaly detection
and trust modeling
Event classification
and entity modeling
Relationship
modeling
! Statistical methods
! Information-theoretical methods
! 70+ unsupervised anomaly detectors
! Dynamic adaptive ensemble creation
! Multiple-instance learning
! Neural networks
! Rule mining
! Random forests
! Boosting
! ML: supervised learning
! Probabilistic threat propagation
! Graph-statistical methods
! Random graphs
! Graph methods
! Supervised classifier training

Global threat intelligence

(powered by Talos)

Intelligence of global threat campaigns mapped to local alarms for faster mitigation

Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

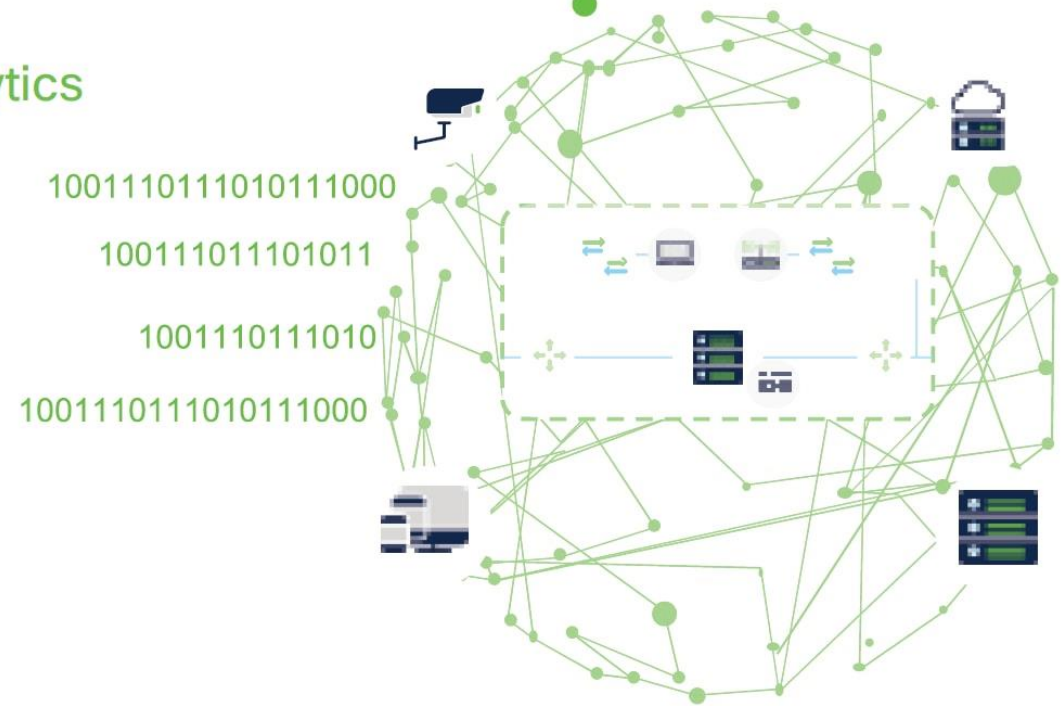
Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Network Analytics

Data collection

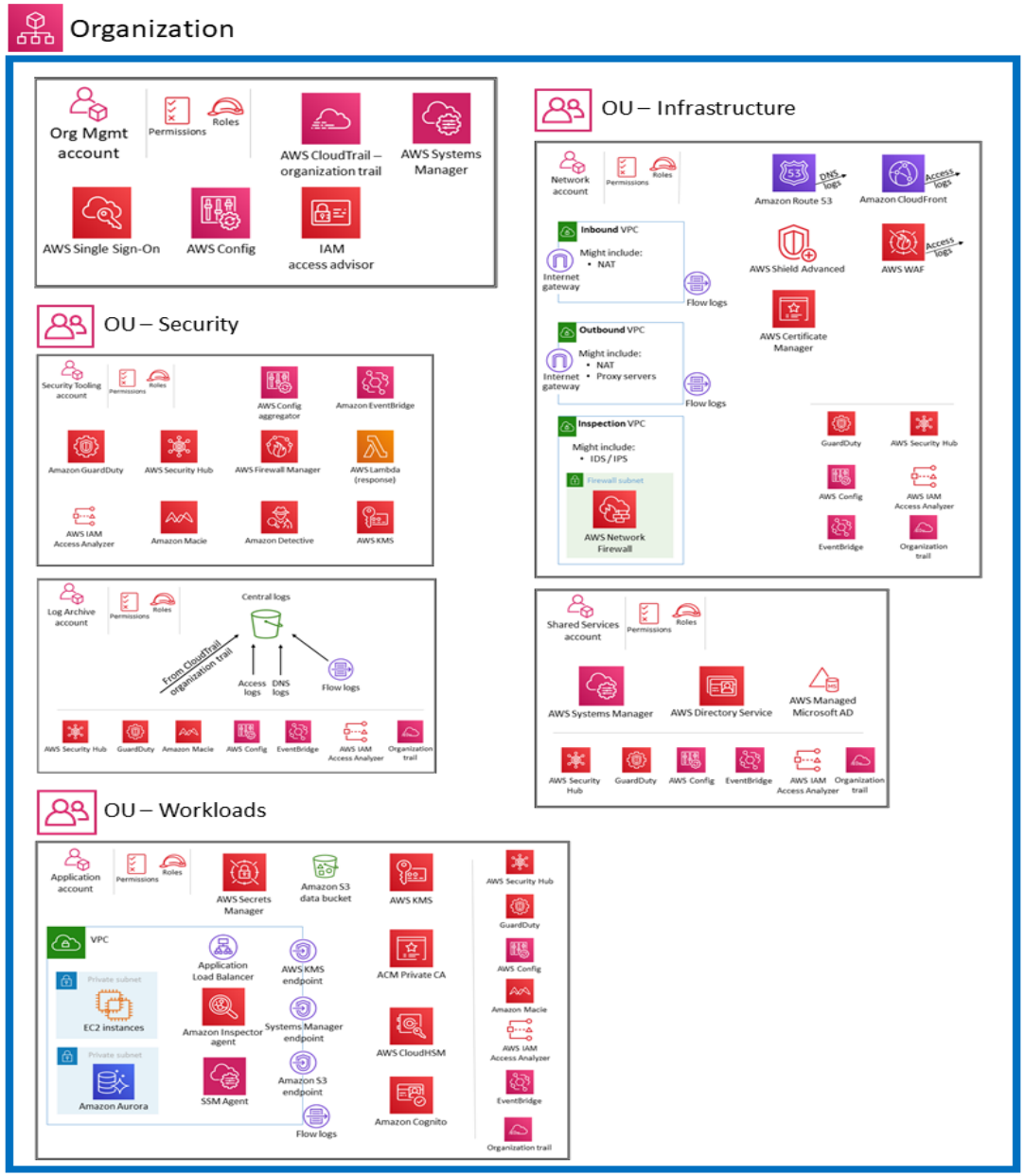
Rich telemetry from the existing network infrastructure



Encrypted Network Analytics

Malware detection without any decryption using enhanced telemetry from the new Cisco devices

Security design- business flow (Internal/ external/ third-party)



AWS AWS Security Reference Architecture