SD-WAN Security and SASE

Charuhas Ghatge
Product Marketing, Nuage Networks

nuagenetworks
From Nokia

©2020 Nokia

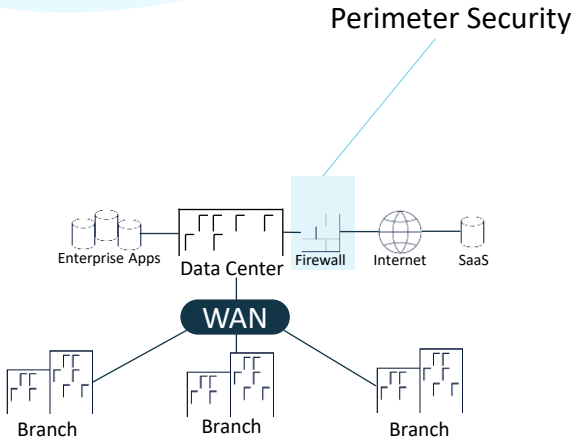
Agenda

- Security for SD-WANs
  - Branch Security Requirements
  - SD-WAN Security Paradigm – Prevent-Detect-Respond
  - Security Functions – IPS/IDS/Web Filtering, Security Monitoring and automated Response to threats
  - SD-WAN Security – Customer Verticals and Use Cases

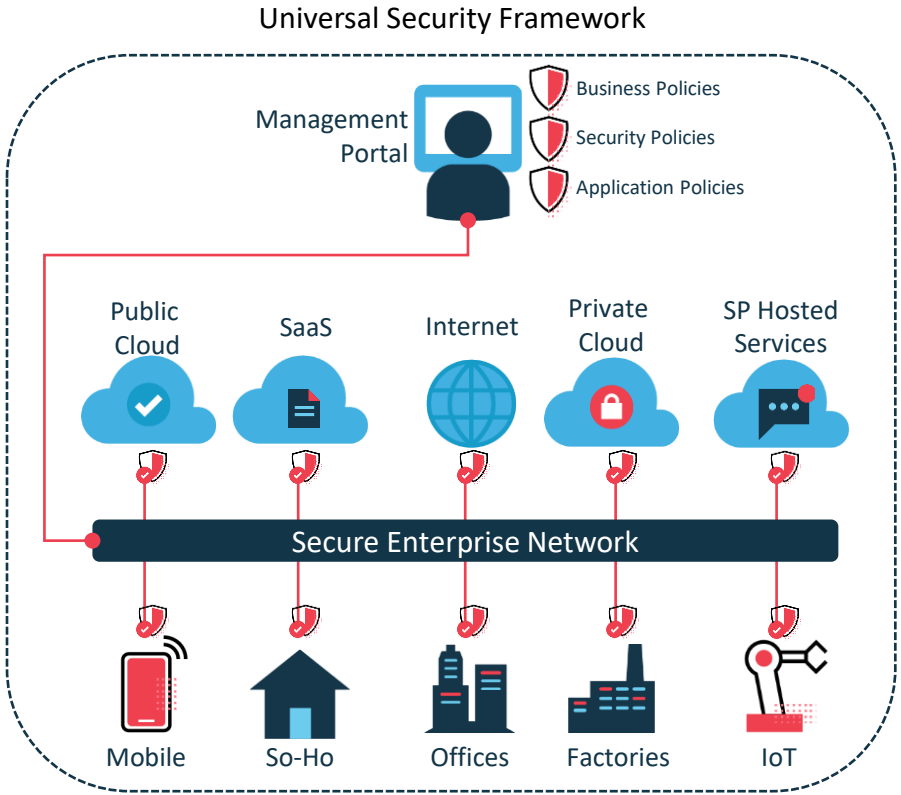
- Secured Access Service Edge (SASE)
  - What is SASE? Why is it needed?
  - Components of SASE
  - Deployment Considerations
  - A SASE Implementation

© 2020 Nokia

Enterprise Network Evolution



- Hub-spoke
- Branch-DC
- Centralized Security



© 2020 Nokia

Branch Security Needs to Evolve with Threat Landscape

Requires Automated, End-to-end approach based on Analytics

Prevent

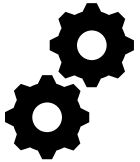
Need to secure local internet breakout access from branch (e.g., L3-7 Firewall, URL Filtering, IDS/IPS)

Prevent lateral malware spread from branch to DC

Detect

Need real-time visibility and monitoring for all traffic entering or leaving branch to detect emerging threats

Respond



Need to automate response to mitigate security threats in near real-time

© 2020 Nokia

Branch Edge Security Requirements

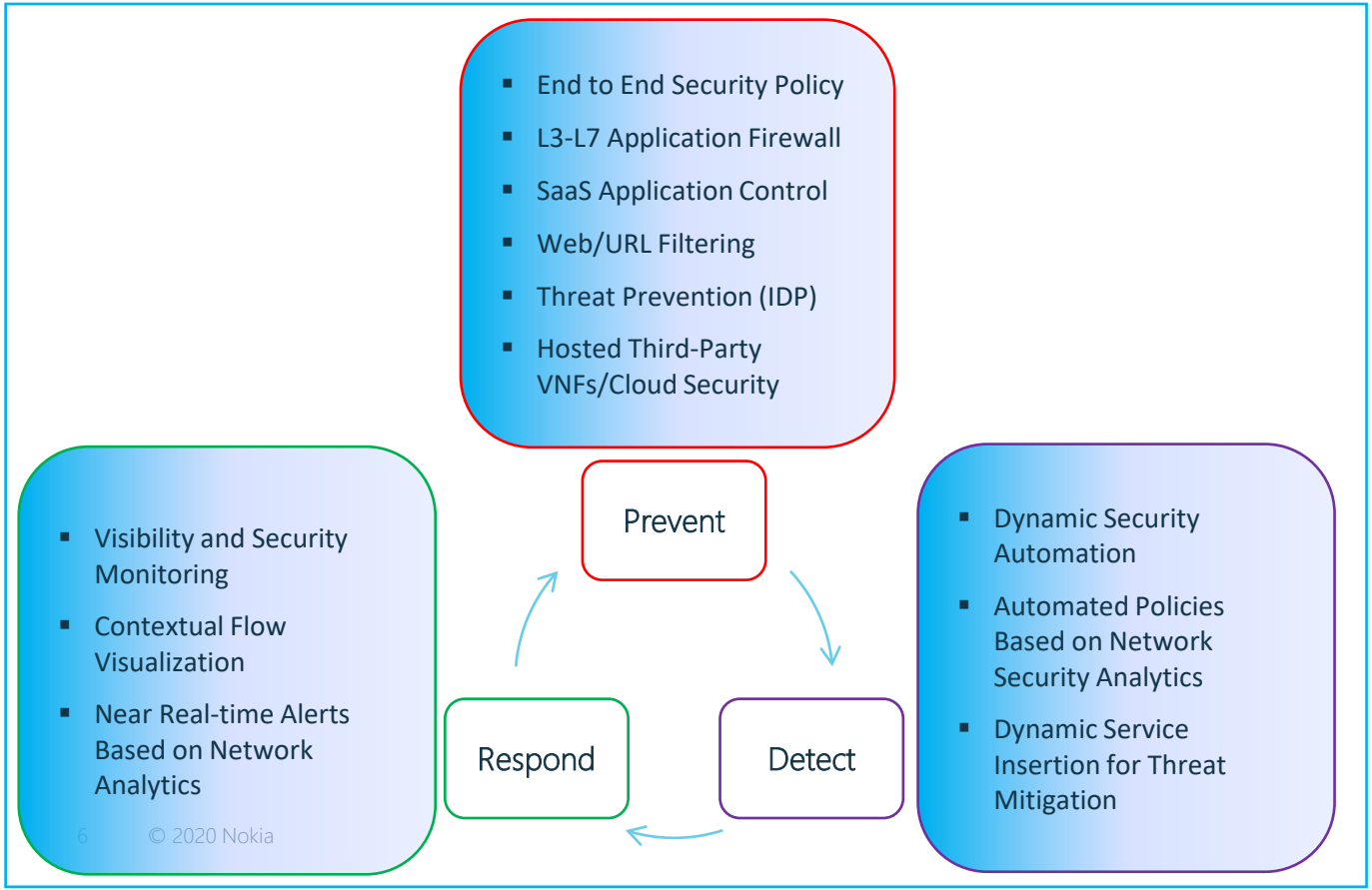
Advanced Security Features

Stateful Firewall	▪ Protect branch network access from outside ▪ Restrict branch user access to corporate network and internet using protocol/ports
L7 Application Control	▪ Restrict branch user access to select applications (e.g., allow Skype for Business, block Facebook)
URL/Web Filtering	▪ Limit branch user access to internet content, block malware ▪ White list access to cloud services ▪ Regulatory Compliance
Threat Prevention (IDP, Anti-Virus)	▪ Detect/block known threats from outside to branch as well as from branch to DC/internet ▪ Protect branch users from network based virus/malware (e.g.. via Web, Email, File downloads)
Real-Time Security Analytics and Automation	▪ Visibility into all traffic from branch to internet and DC/cloud ▪ Detect new zero day threats ▪ Automate response based on analytics to limit malware spread

© 2020 Nokia

Nuage SD-WAN Security

Key Features



Key Benefits

- ✓ Secure branch user to local internet breakout access
- ✓ Prevent unauthorized access to malicious web content
- ✓ End-to-End Segmentation and Security Policy for Threat Prevention and to prevent lateral spread of malware
- ✓ Fast Detection and Rapid Response based on Security Analytics

© 2020 Nokia

Embedded L3-L7 Firewall and SaaS Access Control

Advanced Security Features

L3-L4 Stateful Distributed Firewall

- Limit branch access to/from internet using stateful L3-4 security
- Validated by 3rd party for PCI-DSS v3.2 network firewall requirements
- Logging of ACL actions for compliance and auditing

L7 Application Control

- Restricts branch user access for specific application using L7 DPI
- Supports 1900+ application signatures
- L7 application classification for TLS traffic based on cname in certificates
- Visibility and logging L7 application information.

SaaS Application Control

Supports pre-defined SaaS services – Office365, Webex, Salesforce, Github, JIRA, Azure, AWS, Google

© 2020 Nokia

nuagenetworks

Web/URL Filtering

Block user access to inappropriate or malicious internet content

Use Cases

- Restrict local internet access from branch to cloud services/white listed websites
- Block branch user access to inappropriate or malicious content

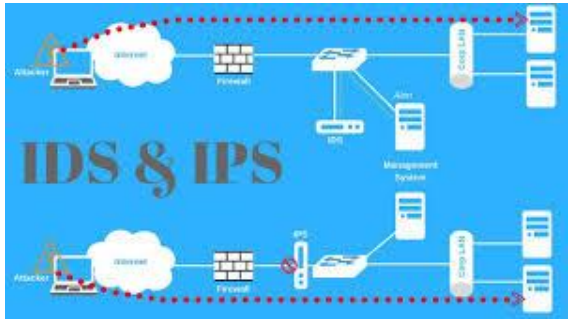
Key Features

- DNS based enforcement based on filtering DNS queries to the websites
- Content/Website Category based filtering (block malware, block adult content, block streaming media)
- Support for over 180+ website categories
- Supports daily update of pre-defined website categories
- Filtering based on custom website list (e.g., allow www.salesforce.com)
- Logging of blocked websites/categories
- Supported on all NSG physical form-factors as well as NSG-V

© 2020 Nokia

Threat Prevention – IDP (IDS/IPS)

Detect and Block Known Threats



Use Cases

- Detect/block known threats from outside to branch as well as from branch to HQ/DC/internet
- Targeted for medium/small sites with ~100s Mbps connectivity

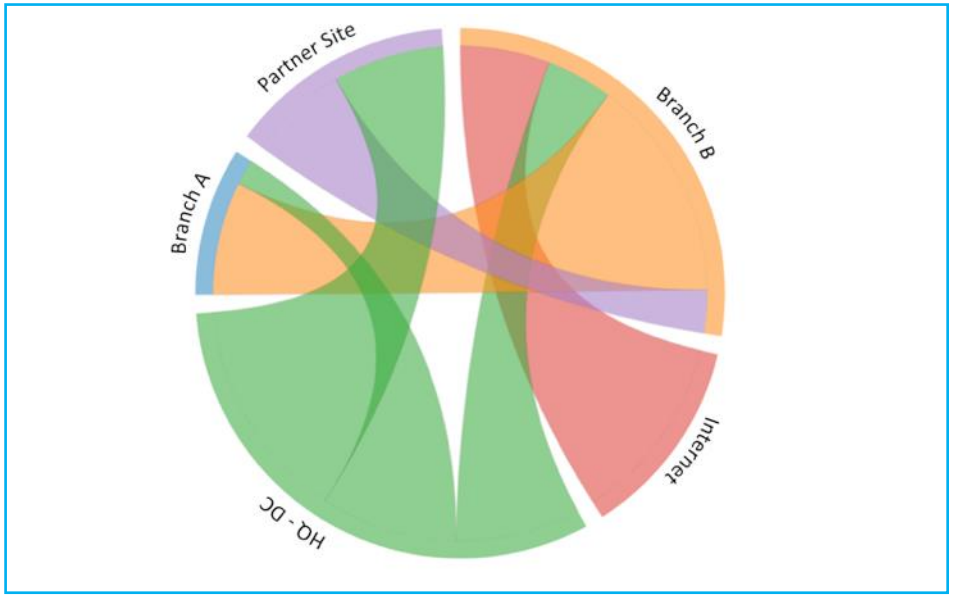
Key Features

- Embedded security capability in NSG
- Uses signatures of known attacks to match traffic that passes through the NSG in order to prevent attacks
- Signatures are divided into different groups containing relevant signatures - based on use case
- IDS/IPS policies defined and managed centrally by VSD GUI, API
- Stats/Reports on intrusion event details and rule hit count logging of blocked websites/categories
- Signatures updated dynamically from cloud and applied to NSG

© 2020 Nokia

Contextual Flow Visibility

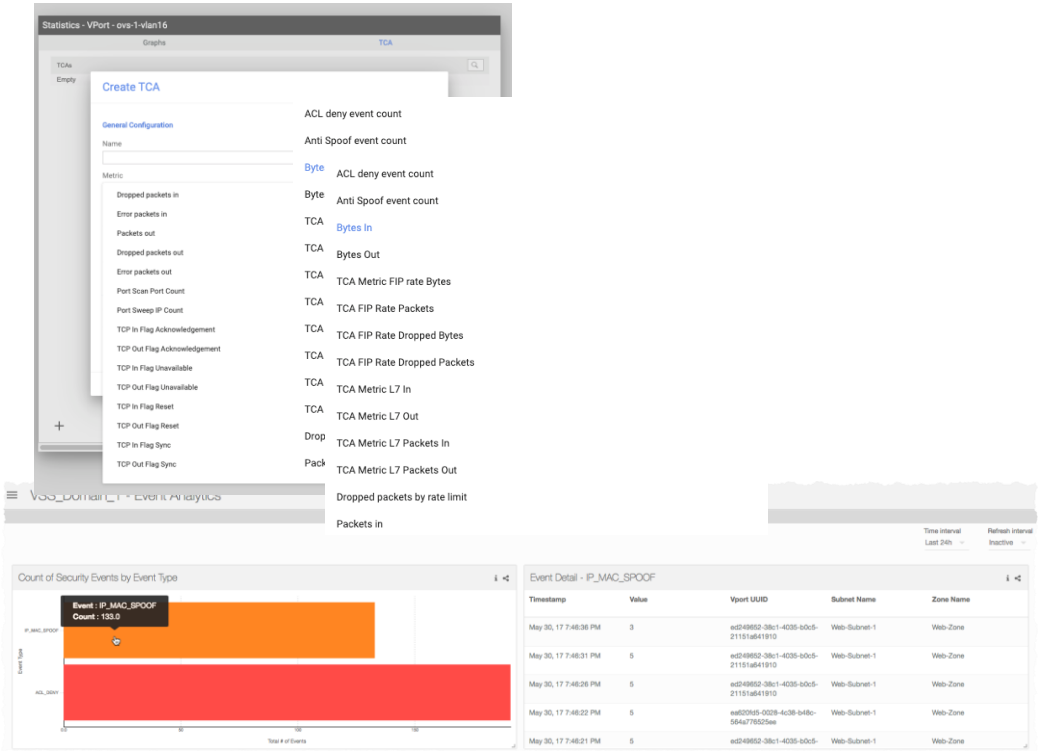
Overlay and Underlay



- Network security monitoring for compliance and audit
- Delivered as a managed cloud service to enterprises
- Shift from traditional box heavy branch (NGFW, Branch Routers) to a thin branch (with SD-WAN) and heavy cloud model
- Threat hunting
- Network forensics and troubleshooting

© 2020 Nokia

Real-Time Network Security Monitoring



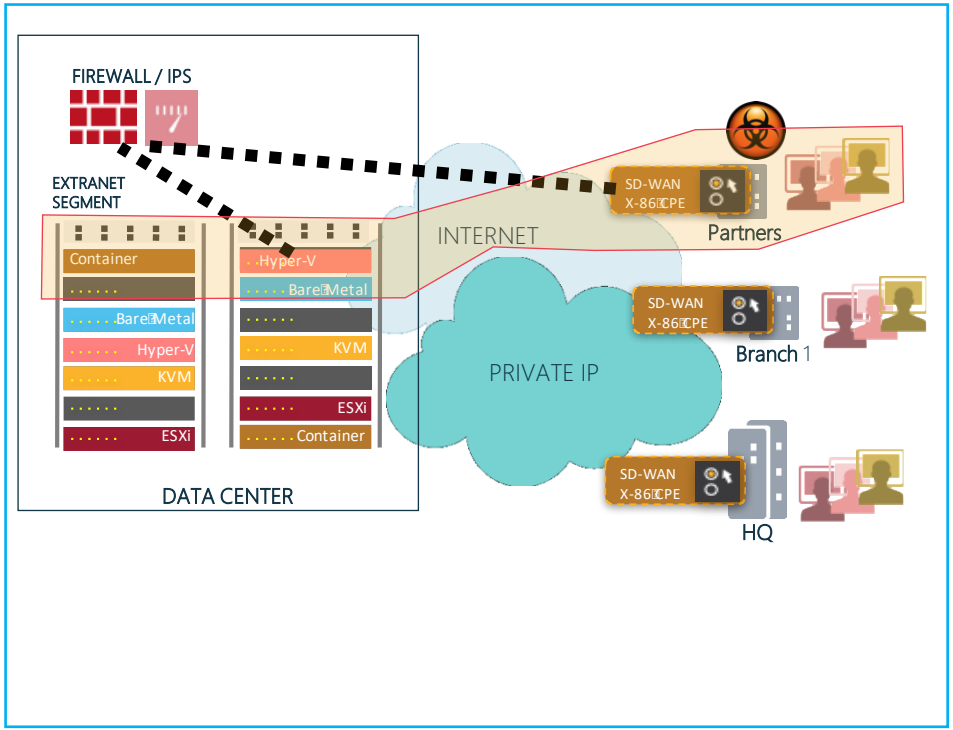
Threshold based Alerts and Security event Reports based on near-real time flow and ACL analytics to detect and alert on various security events:

- Port Scan Detection
- Port Sweep Detection
- Security Policy violations (ACL deny)
- TCP SYN/RST flood (TCP flag count)
- Volumetric DoS attack (Byte/Pkt count)
- Anti spoof

nuagenetworks

© 2020 Nokia

Automated Response



- Prevent malware from infected branch device from entering corporate network
- Leverage network security analytics to identify suspect end-points based on threshold alerts
- Dynamically insert security services (e.g., NGFW, IPS) for suspect traffic
- Security services can be hosted in the data center or the branch

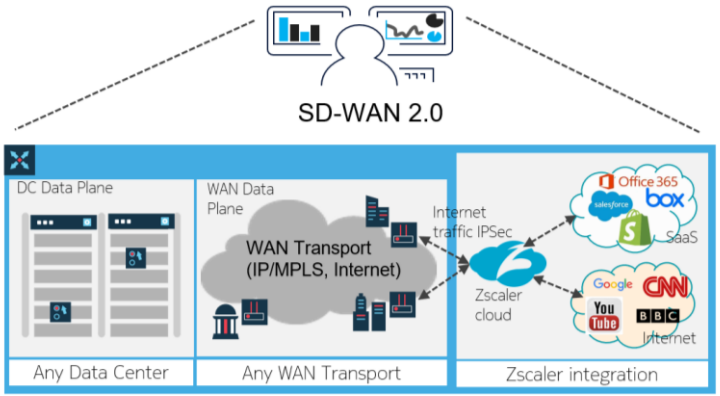
© 2020 Nokia

nuagenetworks

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

Flexible Deployment with Partner Eco-System

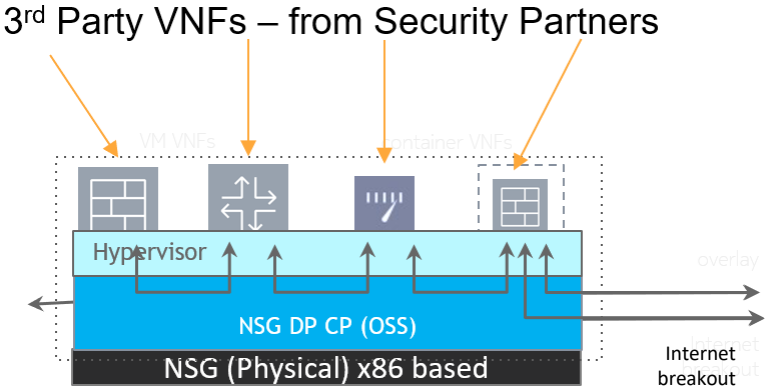
Security across entire IT landscape delivered as cloud-managed service



Cloud Security Services

Protect branch user access to internet via local breakout

- Limit access to specific cloud services via local breakout



3rd Party Hosted VNF and Service Chaining to HQ/DC (For example, Checkpoint)

- Hosting 3rd party VNF(s) on the branch CPE
- Service chaining to CSP Cloud VNFs or HQ/DC appliances
- An eco-system of security partners (NGFW/UTM)

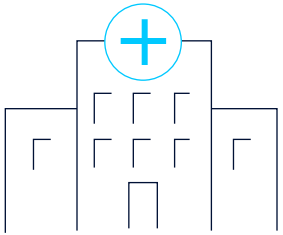
© 2020 Nokia

nuagenetworks

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries

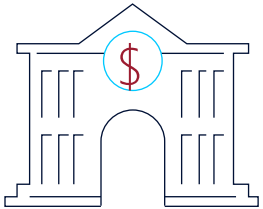
SD-WAN Security – Customer Use cases

Healthcare



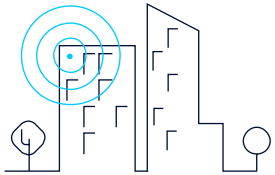
Identification of malware activity at branch site (doctor's office) based on Nuage embedded network traffic analytics

Financial/Banking



Securing guest user access to internet from a bank branch office using L3-7 firewall and embedded URL filtering

Managed Service Provider



Value added security services for SD-WAN using Nuage embedded security capabilities or using partner security VNF

© 2020 Nokia

Secured Access Service Edge (SASE)

nuagenetworks
From Nokia

©2020 Nokia

The SASE Story

- Why SASE - What Problem is being solved
- Evolution of Enterprise Networking & Security Needs

Why

- SASE Description, Status and Key Requirements
- What is SASE, Where is it on Hype Cycle, No Standards, 5-10 year Journey vs. a defined destination, major requirements (Gartner)

What

- Nuage does SASE
  - How we meet key requirements
  - Incremental Options and Benefits

How

- Deployment Considerations
- Consider the state of Industry, SD-WAN technology, Security technology, Enterprise.
- Need for flexibility: Rip and replace vs. evolution – undefined standards, dynamic and evolving threats, vendor lock-in, dynamic needs, flexibility.

When

- Nuage does SASE in detail
- SASE at the end points
- SASE at service edge and cloud

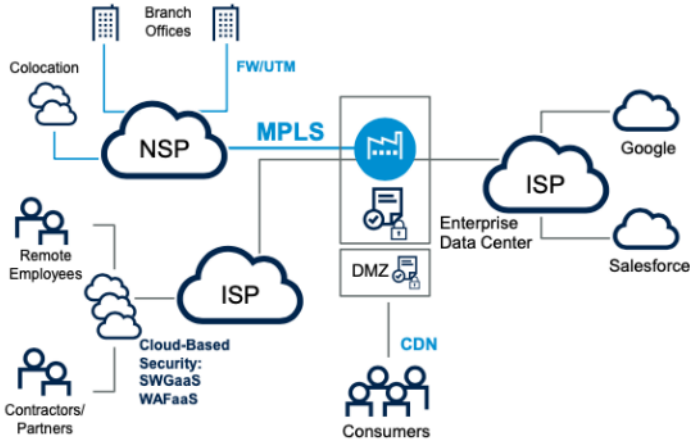
Who

© 2020 Nokia

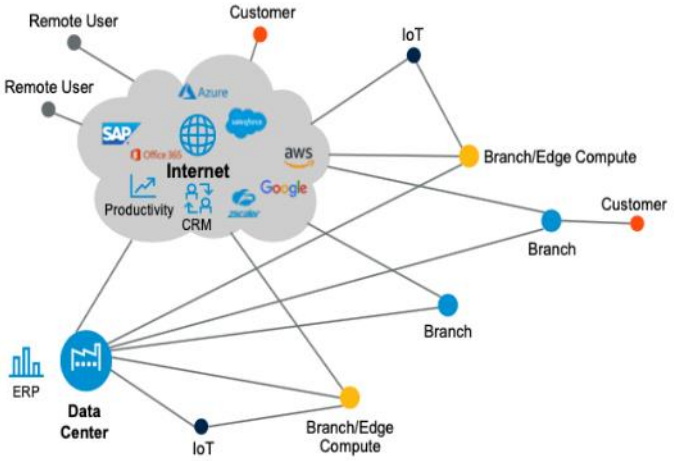
nuagenetworks

A new architecture is required to deal with both Security and Connectivity

Connect to Datacenter/HQ



Connect to Clouds (Private, SaaS, Public)



Connectivity from Anywhere

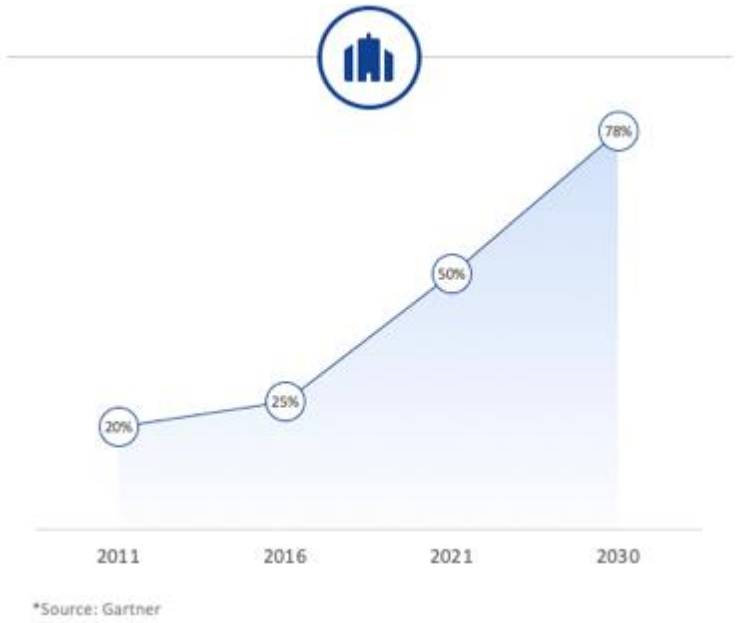
- Traditional Security (VPN) is overwhelmed
- IT Operations are stretched
- Growing Network performance and costs

Source: Gartner

© 2020 Nokia

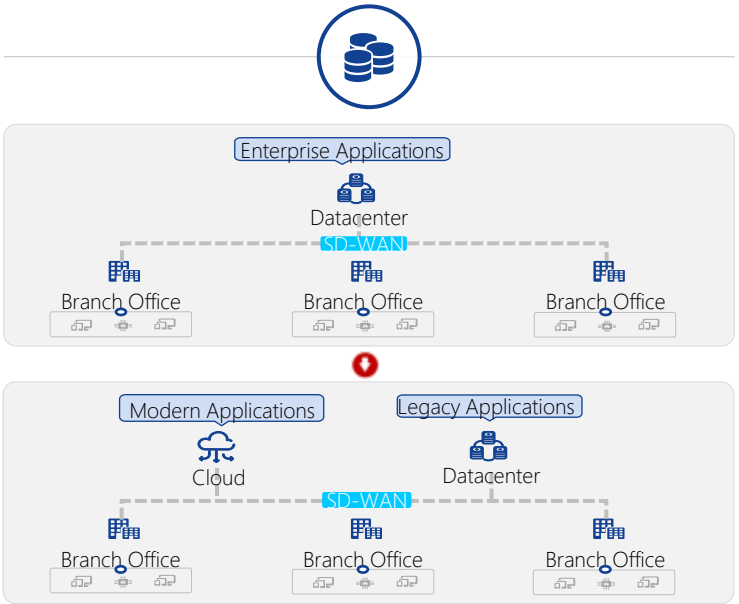
Migration of Enterprise to Cloud requires Cloud-Centric Connectivity & Security

Enterprise Applications Migrate to Cloud



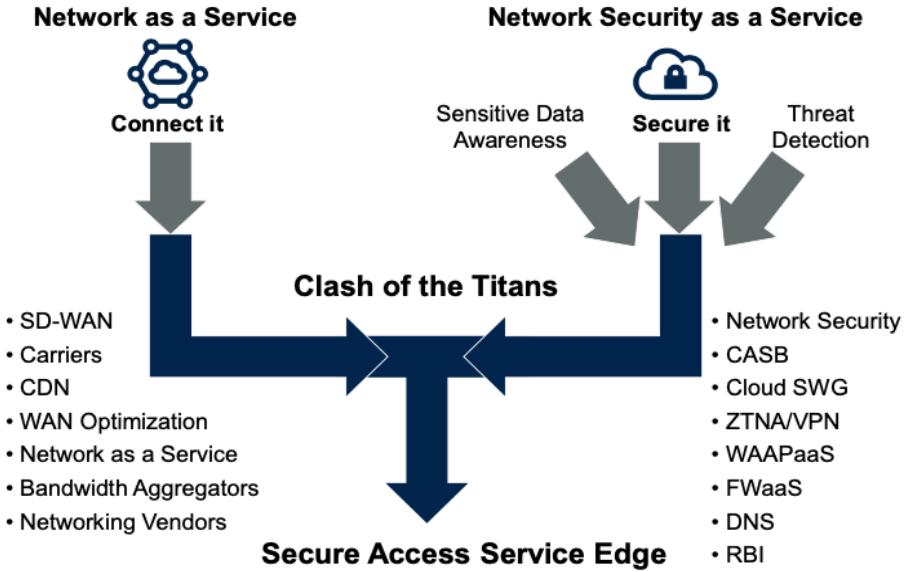
*Source: Gartner

SD-WAN architecture is evolving



© 2020 Nokia

What is SASE Framework and what are its potential Use Cases



SASE Use Cases

- Connect user from anywhere
- POP-centric Cloud access with assured SLA
- Secure WAN access with end-to-end security protection
- Enhanced Application experience
- Enterprise Digital Transformation
- Simplification of Security & Network Operations
- Migration and adoption of Cloud
- Networking for IoT and Industry 4.0

© 2020 Nokia

High level SASE requirements & recommended approach

Networking

- Performance based POP selection
- Application aware routing and traffic steering
- Full MPLS support for legacy Datacenter access

Security

- Access privileges are enforced at endpoint by policies including networking firewall and URL filtering
- SWG, CASB, NGFW, ZTNA, DLP and others are handled at the service edge

Management

- Easy provisioning and full visibility reports at all the networking levels.
- Multi-platform provisioning support

Vendor Strategy

- Multi security vendors support
- Multi Cloud vendors support

© 2020 Nokia

SASE Networking Requirements & vendor Implementation

Networking Requirements	Description	Vendor
Comprehensive Routing capabilities	Full stack of routing protocols to support switching and routing personalities	✓
Access and Connectivity to and from Anywhere	Seamless connectivity and policy management across fixed (internet, L2 and L3) and mobile WANs	✓
Performance based POP selection	Support for multiple paths and PoPs and performance-based selection ability	✓
Application aware routing and traffic steering	Providing optimal application experience based on application types	✓
Hybrid WAN support (e.g. Full MPLS/Ethernet) for legacy Datacenter access	Seamless integration of existing networking to access data center and apps	✓
Multi-Cloud & Hybrid Cloud connectivity	Policy based access to and across applications in private cloud and multiple public clouds	✓
Connectivity Security – VPN, IPSec	Embedded encryption and end point security	✓
WAN Optimization & Bandwidth Aggregation	Optimizing the use of available network for availability and performance	✓
SD-WAN Service Portal	Multi-tenant SD-WAN portal hosted by CSP for the visibility and control. Enabling co-management with enterprise	✓

© 2020 Nokia

SASE Security Requirements and vendor Implementation

SASE Requirements	Description	Vendor Implementation guidelines
IPS	Intrusion Prevention system	Preferably Native
IDS	Intrusion Detection System	Preferably Native
Firewall	Stateful Firewall	Preferably Native
Realtime Security Analytics & Automation	With end-to-end visibility and control for each application, the operator can detect, protect resources at a very granular level, and use automation to respond in real-time to threats.	Native, multi-tenant platform and should be cloud delivered (analytics and management can be hosted by SP)
SWG and DNS Filtering	Secure Web Gateway is used to protect users and devices from online security threats by enforcing internet security and compliance policies and filtering out malicious internet traffic.	Preferably Native
ZTNA	Zero trust network access is a set of technologies that operates on an adaptive trust model, where trust is never implicit, and access is granted on a "need-to-know," least-privileged basis defined by granular policies. A seamless and secure connectivity to private applications without exposing apps to the internet.	Provided via integration with specialized cloud security vendor
CASB	Cloud Access Security Broker - According to Gartner, a cloud access security broker (CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed.	Provided via integration with specialized cloud security vendor
DLP	Data Loss Prevention - DLP provides visibility across all sensitive information, everywhere and always, enabling strong protective actions to safeguard data from threats and violations of corporate policies.	Provided via integration with specialized cloud security vendor
FWaaS	Firewall as a Service	Policy Management layer for FWaaS should be multi-tenant and hosted in SP cloud.

© 2020 Nokia

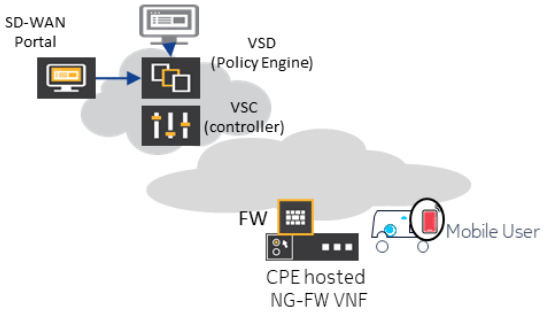
SASE Solution: Options to incrementally evolve towards SASE

1 Nuage SD-WAN embedded Security

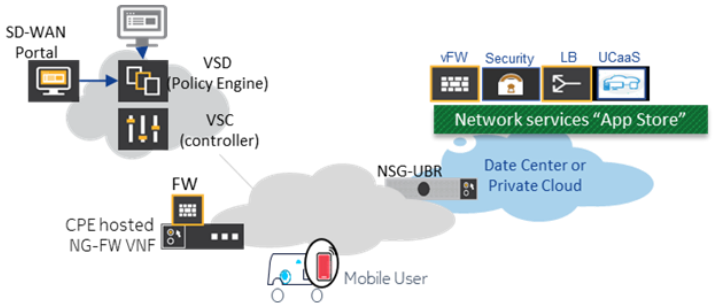
E2E L3-4 stateful micro segmentation	URL / Web filtering	IDS/IPS	Contextual visibility and security monitoring	Automate security policy based on alerts
L7 and SaaS application control	Host or Service chain to third party security functions	Anti-Virus DDOS protect user identity		
Prevent			Detect	Respond

Enabled by VSS Analytics

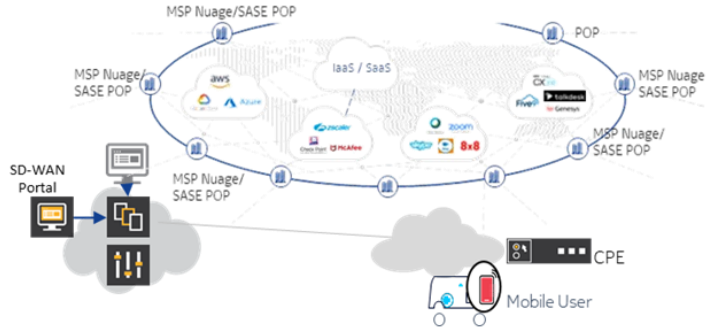
2 Augment with hosted 3rd party Firewall VNF on CPE



3 MSP's Cloud Security (SASE) through Service-Chain



4 Nuage SASE Platform



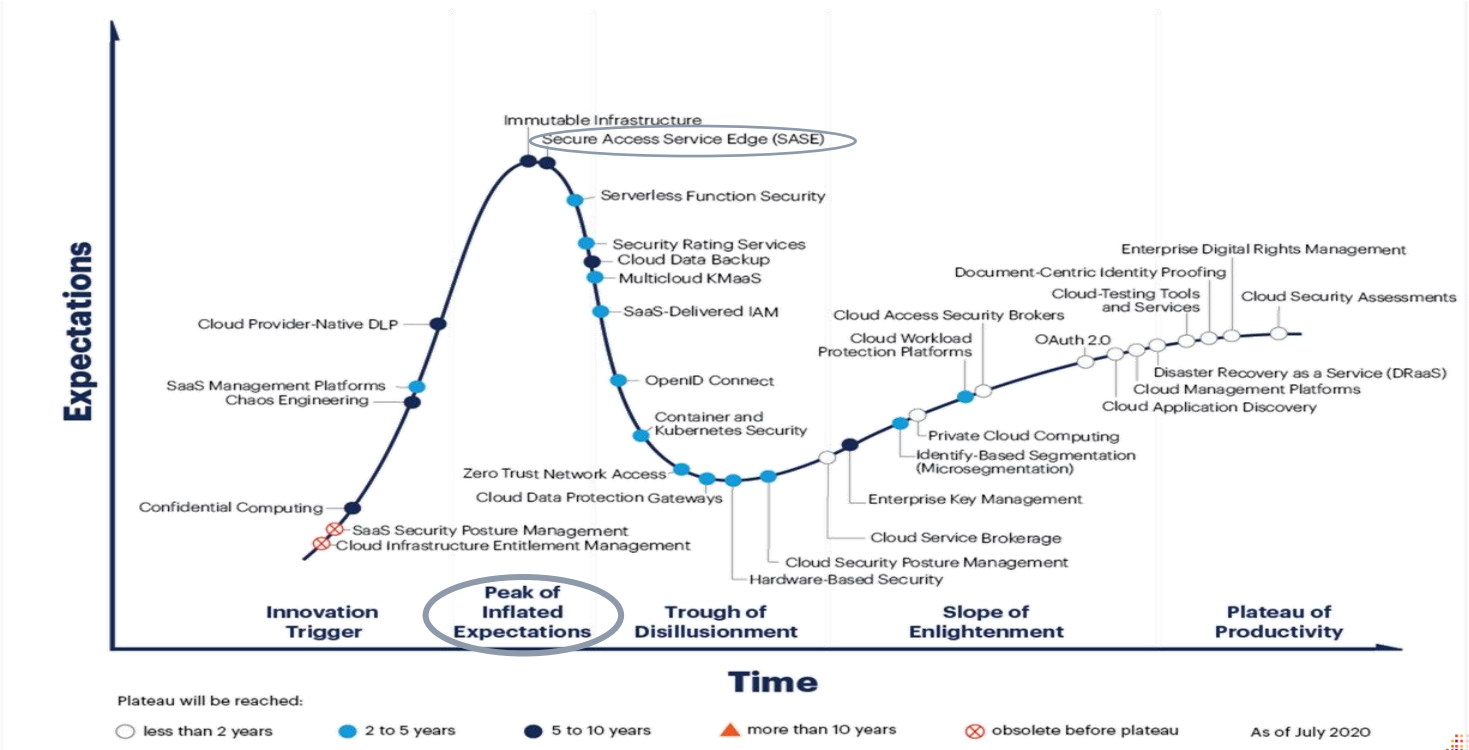
© 2020 Nokia

Deployment Considerations

© 2020 Nokia

Caveats on SASE @Peak of Inflated Expectation on Hype Cycle

SASE is at the Peak of Inflated Expectation on Gartner's hype cycle. Whereas, SD-WAN can be MEF certified, SASE standards are still being worked



© 2020 Nokia

SASE Deployment Considerations

Flexibility becomes critical in an evolving and dynamic space

- SD-WAN and Cloud Security solutions are widely deployed
- A rip-n-replace SASE deployment is not practical. Pragmatic solution requires utilizing investments
- A complete SASE solution from a single vendor would:
  - compromise completeness
  - reduce flexibility in a very dynamic space of enterprise security
  - risk the vendor lock-in
  - SD-WAN enjoys MEF standard, cloud security is evolving

- A good SASE solution should provide flexibility:
  - A highly scalable and feature-rich SD-WAN supporting connectivity from anywhere - SD-WAN is the foundation of SASE
  - Exhaustive native security functions within SD-WAN
  - Integration with cloud security platforms for advanced and evolving security functions
- This flexibility enables MSP to:
  - Create best-fit SASE solution for enterprise clients
  - Differentiate against single vendor cookie cutter solution

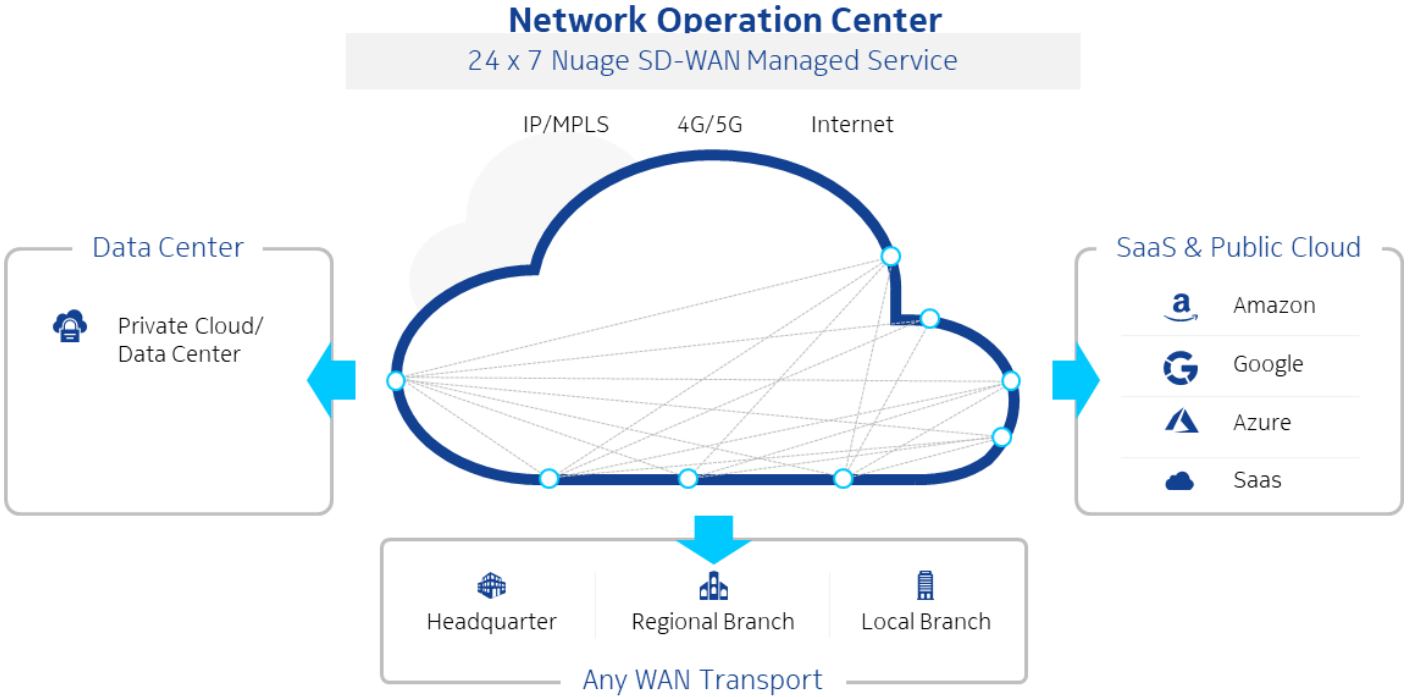
© 2020 Nokia

Details on Approach

© 2020 Nokia

Nuage does SASE: Nuage SD-WAN Managed Service Multi-Cloud Connectivity

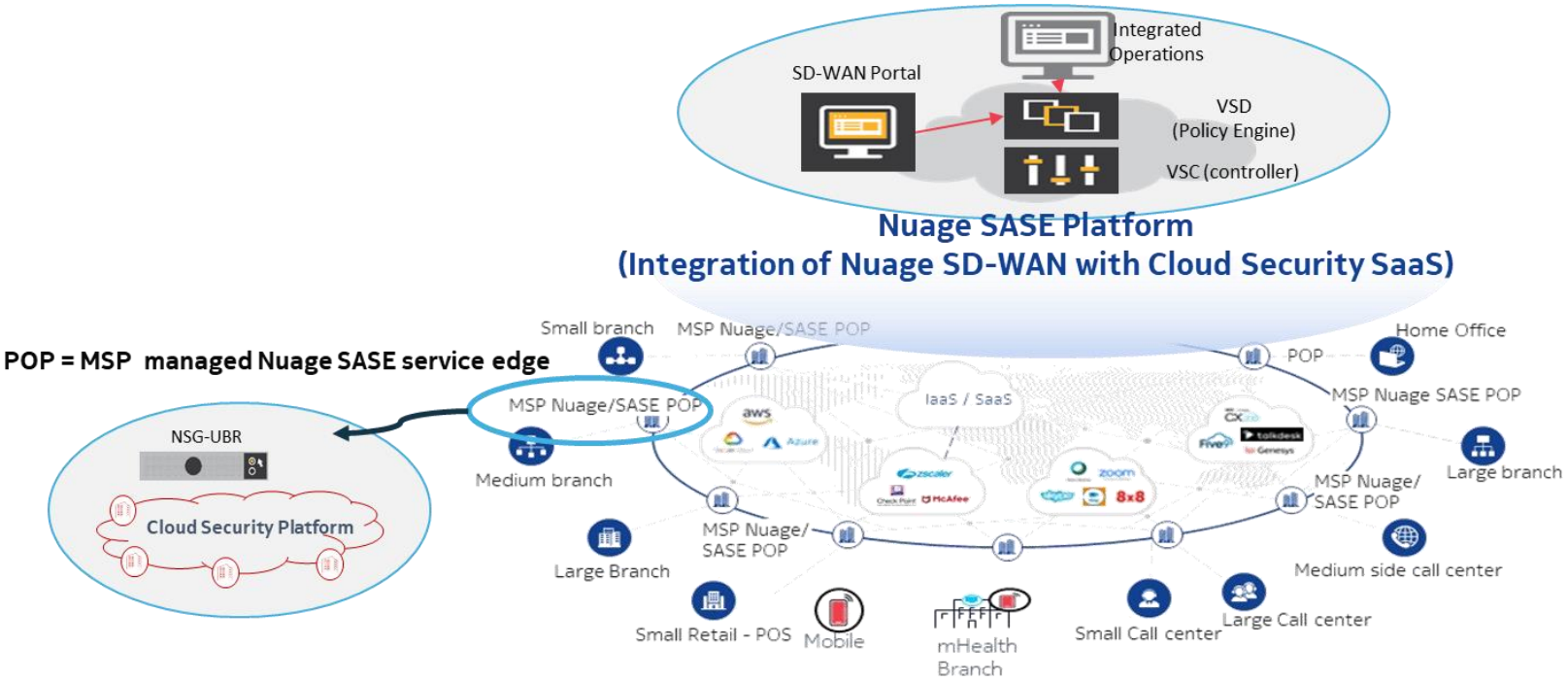
Secure Multi Cloud and Branch Connectivity by Nuage SD-WAN



© 2020 Nokia

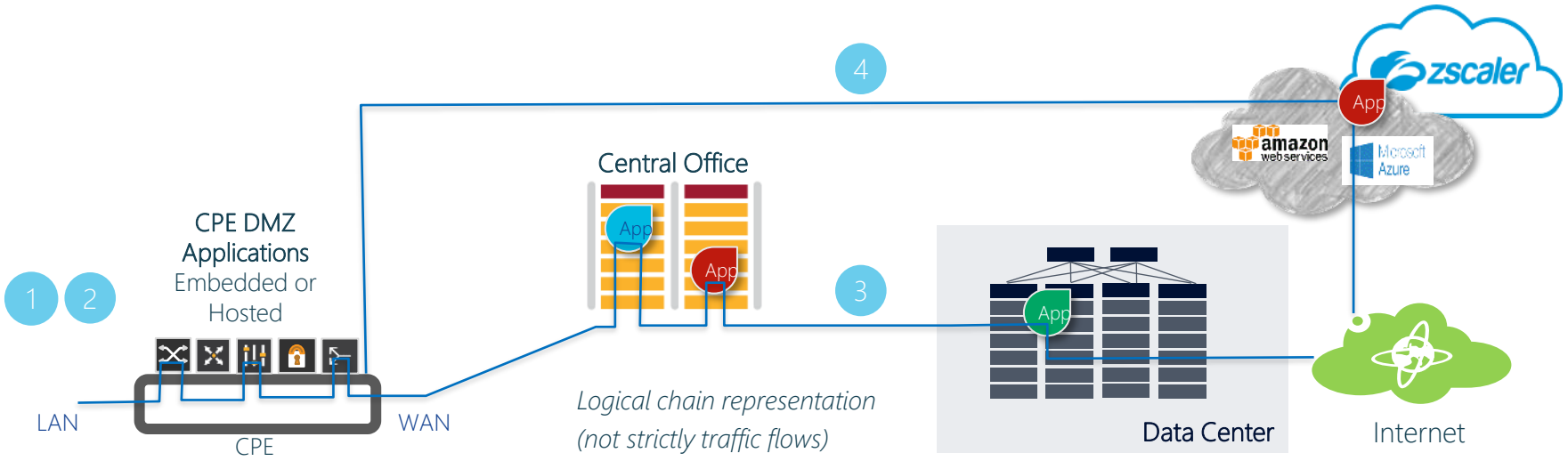
Nuage does SASE: Nuage SASE Platform for MSPs

Nuage SD-WAN Any Access Anywhere Connectivity + Nuage SASE Platform



© 2020 Nokia

Nuage SASE solutions offers multiple options



1 CPE and Nuage SD-WAN Embedded Functions

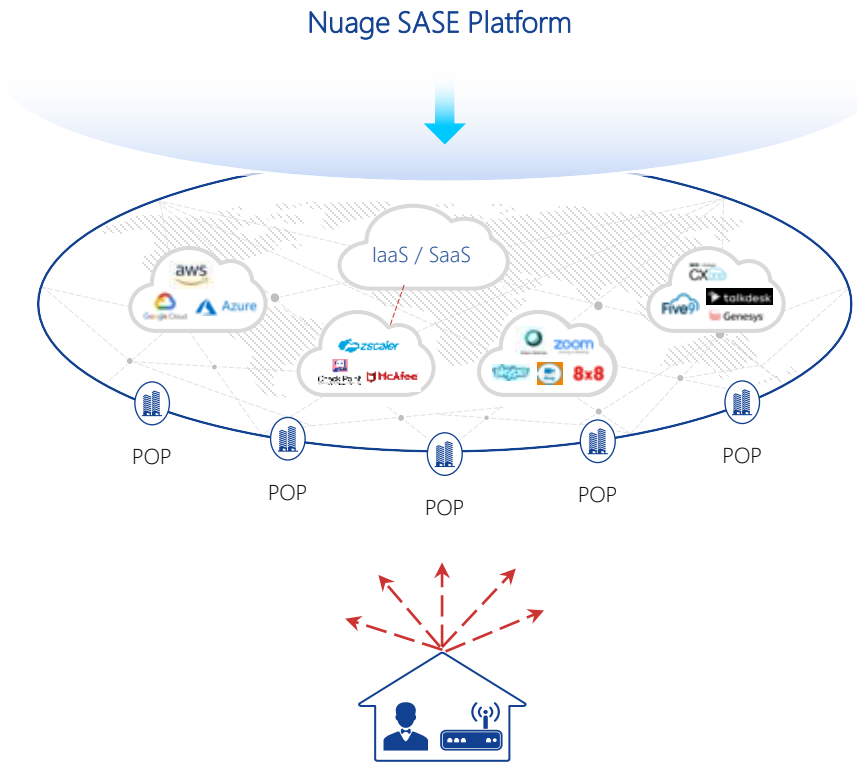
2 = 1 + CPE Hosted Firewalls
Breakout & Overlay Traffic using best-of-breed FW Solutions, Hub/Spoke model for vNF consumption

3 = 1 + Service Chaining to DC
Hosted Firewall Functions (Adv. Forwarding ACLs)

4 = 1 + Integration with Cloud Hosted Security Brokers
zScaler /PA(IKEv1/v2 based integration)

© 2020 Nokia
nuagenetworks

User Access from Anywhere with secure and highly available connectivity



User selects the SASE POP based on performance to reach Applications in the Cloud

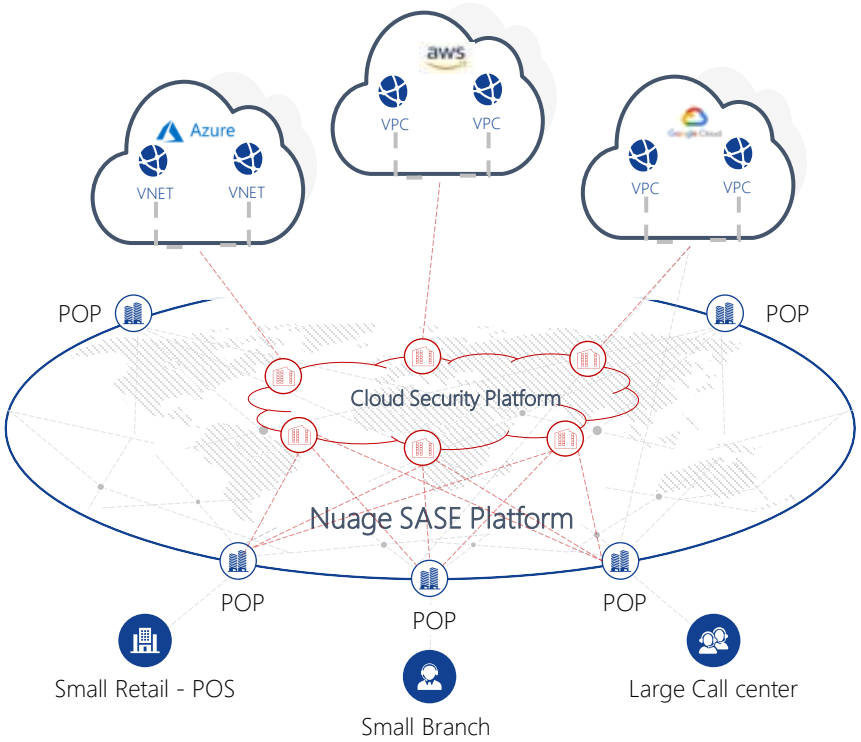
Networks performance — Select POP based on underlay quality (package lost, jitter and latency)

Gateway load — Balance the traffic to different POP if the gateway overloaded

Link resilience — If there are any peering link issue between POP to Cloud, redirect traffic to different POP

© 2020 Nokia

Connect to Clouds from Service POP via Security SaaS platform



01 Direct peering with Security SaaS platform POP

02 End-to-end traffic encryption from user to Nuage SASE POP

03 Enforce policy including both network Firewall and URL filtering at end points

04 Security SaaS platform handles SWG, CASB, NGFW, ZTNA, DLP and other security functions at their platform

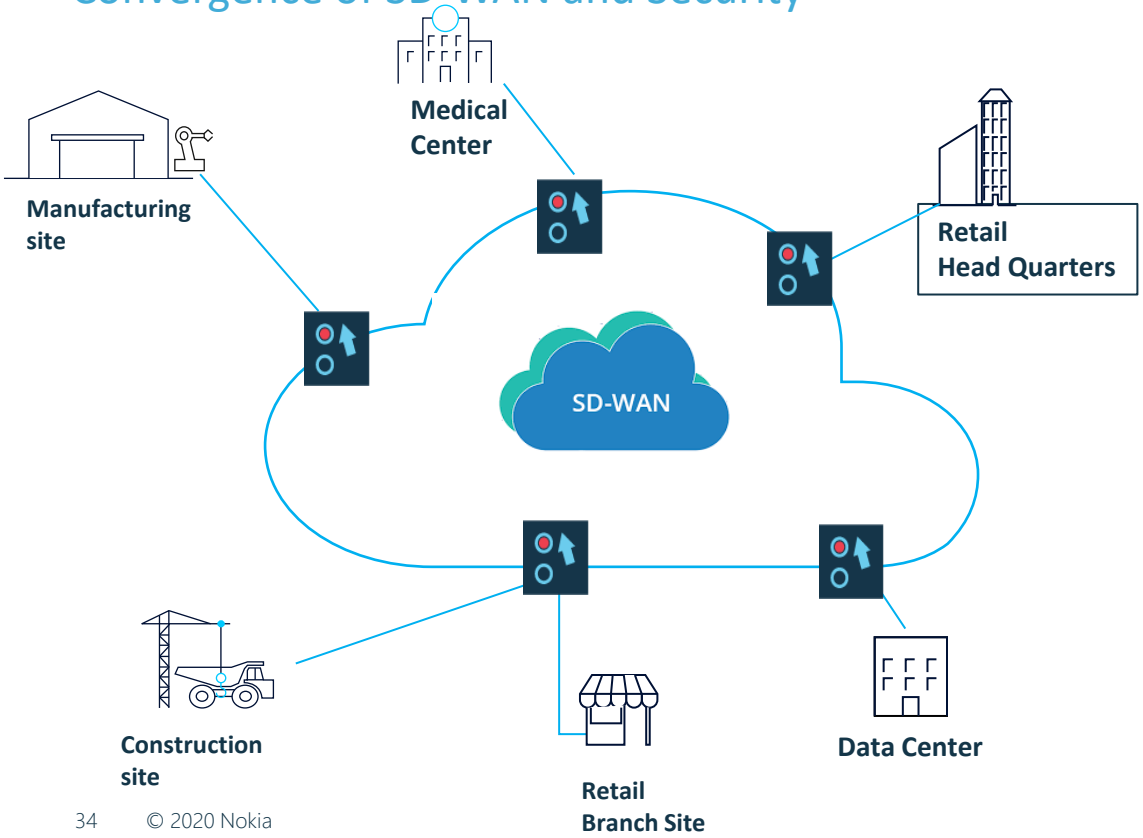
© 2020 Nokia

Summary

© 2020 Nokia

Foundation of SASE is SD-WAN

Convergence of SD-WAN and Security

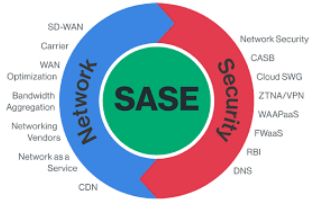


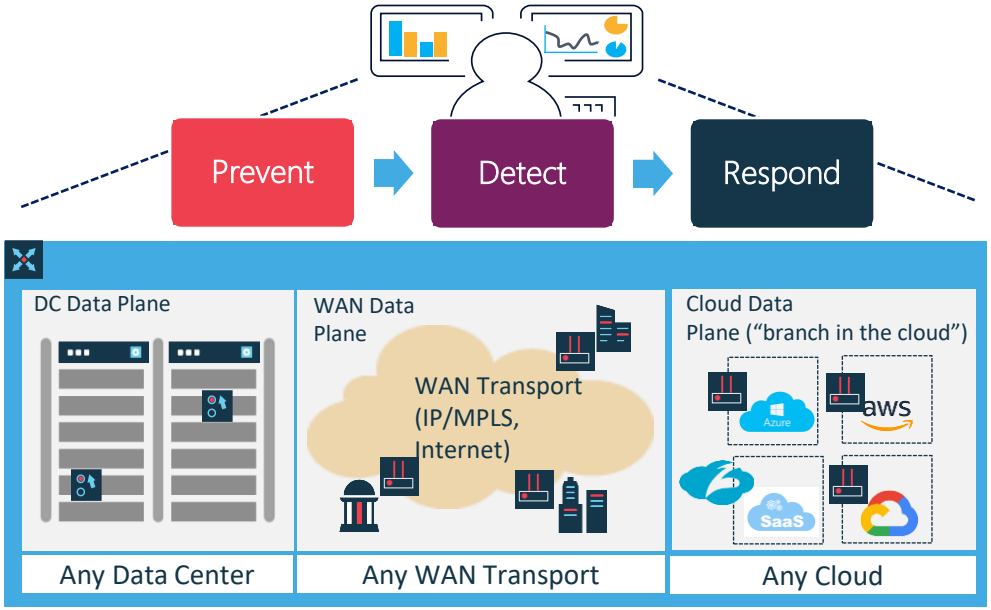
- Cloud delivered and managed SD-WAN service is the foundation of SASE
- Security is delivered on top of SD-WAN as a value added service
- Security defined in cloud enforced in the WAN-edge based on logical constructs and not using box-centric approach

© 2020 Nokia

Nuage SD-WAN and SASE

Security across entire IT landscape delivered as cloud-managed service





- ✓ Nuage SD-WAN 2.0 architecture provides the right architecture to deliver SASE
- ✓ Delivered as a Cloud Managed SD-WAN Service offered by 100+ Service Provider Partners Enterprises
- ✓ Offers Flexible Cloud Delivered Security Services including:
- ✓ Cloud Managed Embedded Security (NGFW, IDP, Web Filtering Analytics)
- ✓ 3rd Party Cloud Security Services Integration (zScaler)
- ✓ Hosted VNFs (UTM) in CSP Cloud

© 2020 Nokia
nuagenetworks

nuagenetworks

From Nokia

© 2020 Nokia