UNLEASH THE POWER OF LIMITLESS CONNECTIVITY
Security & Privacy

SD-WAN Security and SASE

Charuhas Ghatge
Product and Solutions Marketing
Nuage Networks by 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
Enterprise Network Evolution

Universal Security Framework

- Hub-spoke
- Branch-DC
- Centralized Security
Branch Security Needs to Evolve with Threat Landscape

Requires automated, end-to-end approach based on Analytics

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
</tr>
</thead>
</table>
| ![Lock Icon](image)  
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 | ![Magnifying Glass Icon](image)  
Need real-time visibility and monitoring for all traffic entering or leaving branch to detect emerging threats | ![Gears Icon](image)  
Need to automate response to mitigate security threats in near real-time |
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
SD-WAN Security

Key Features

- End to End Security Policy
- L3-L7 Application Firewall
- SaaS Application Control
- Web/URL Filtering
- Threat Prevention (IDP)
- Hosted Third-Party VNFs/Cloud Security
- Visibility and Security Monitoring
- Contextual Flow Visualization
- Near Real-time Alerts Based on Network Analytics
- Prevent

- Dynamic Security Automation
- Automated Policies Based on Network Security Analytics
- Dynamic Service Insertion for Threat Mitigation
- Respond

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
- Detect
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 embedded security capabilities or using partner security VNF
Secured Access Service Edge (SASE)

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

- 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)

- Vendor SASE implantation
  - How they can meet key requirements
  - Incremental Options and Benefits

- 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.

Why | What | How | When
New architecture needed for security and connectivity

Connect to Datacenter/HQ

Connect to Clouds (Private, SaaS, Public)

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

Source: Gartner
Migration of Enterprise to Cloud requires Cloud-Centric Connectivity & Security

Enterprise Applications Migrate to Cloud

SD-WAN architecture is evolving

*Source: Gartner*
SASE Framework and its 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

Navigating the SASE Framework:

**Network as a Service**
- Connect it
  - SD-WAN
  - Carriers
  - CDN
  - WAN Optimization
  - Network as a Service
  - Bandwidth Aggregators
  - Networking Vendors

**Network Security as a Service**
- Secure it
  - Sensitive Data Awareness
- Threat Detection
  - Network Security
  - CASB
  - Cloud SWG
  - ZTNA/VPN
  - WAAPaaS
  - FWaaS
  - DNS
  - RBI

Clash of the Titans

Secure Access Service Edge
# SASE Networking Requirements & vendor Implementation

<table>
<thead>
<tr>
<th>Networking Requirements</th>
<th>Description</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive Routing capabilities</td>
<td>Full stack of routing protocols to support switching and routing personalities</td>
<td>✔️</td>
</tr>
<tr>
<td>Access and Connectivity to and from Anywhere</td>
<td>Seamless connectivity and policy management across fixed (internet, L2 and L3) and mobile WANs</td>
<td>✔️</td>
</tr>
<tr>
<td>Performance based POP selection</td>
<td>Support for multiple paths and PoPs and performance-based selection ability</td>
<td>✔️</td>
</tr>
<tr>
<td>Application aware routing and traffic steering</td>
<td>Providing optimal application experience based on application types</td>
<td>✔️</td>
</tr>
<tr>
<td>Hybrid WAN support (e.g. Full MPLS/Ethernet) for legacy Datacenter access</td>
<td>Seamless integration of existing networking to access data center and apps</td>
<td>✔️</td>
</tr>
<tr>
<td>Multi-Cloud &amp; Hybrid Cloud connectivity</td>
<td>Policy based access to and across applications in private cloud and multiple public clouds</td>
<td>✔️</td>
</tr>
<tr>
<td>Connectivity Security – VPN, IPSec</td>
<td>Embedded encryption and end point security</td>
<td>✔️</td>
</tr>
<tr>
<td>WAN Optimization &amp; Bandwidth Aggregation</td>
<td>Optimizing the use of available network for availability and performance</td>
<td>✔️</td>
</tr>
<tr>
<td>SD-WAN Service Portal</td>
<td>Multi-tenant SD-WAN portal hosted by CSP for the visibility and control. Enabling co-management with enterprise</td>
<td>✔️</td>
</tr>
<tr>
<td>SASE Requirements</td>
<td>Description</td>
<td>Vendor Implementation guidelines</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention system</td>
<td>Preferably Native</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td>Preferably Native</td>
</tr>
<tr>
<td>Firewall</td>
<td>Stateful Firewall</td>
<td>Preferably Native</td>
</tr>
<tr>
<td>Realtime Security</td>
<td>With end to end visibility and control for each application, the operator</td>
<td>Native, multi-tenant platform and should be cloud delivered (analytics and management can be hosted by SP)</td>
</tr>
<tr>
<td>Analytics &amp;</td>
<td>can detect, protect resources at a very granular level, and use automation</td>
<td></td>
</tr>
<tr>
<td>Automation</td>
<td>to respond in real-time to threats.</td>
<td></td>
</tr>
<tr>
<td>SWG and DNS</td>
<td>Secure Web Gateway is used to protect users and devices from online security</td>
<td>Preferably Native</td>
</tr>
<tr>
<td>Filtering</td>
<td>threats by enforcing internet security and compliance policies and filtering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>out malicious internet traffic.</td>
<td></td>
</tr>
<tr>
<td>ZTNA</td>
<td>Zero trust network access is a set of technologies that operates on an</td>
<td>Provided via integration with specialized cloud security vendor</td>
</tr>
<tr>
<td></td>
<td>adaptive trust model, where trust is never implicit, and access is granted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on a “need-to-know,” least-privileged basis defined by granular policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A seamless and secure connectivity to private applications without</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exposing apps to the internet.</td>
<td></td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker - According to Gartner, a cloud access</td>
<td>Provided via integration with specialized cloud security vendor</td>
</tr>
<tr>
<td></td>
<td>security broker (CASB) is an on-premises or cloud-based security policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>enforcement point that is placed between cloud service consumers and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cloud service providers to combine and interject enterprise security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>policies as cloud-based resources are accessed.</td>
<td></td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention - DLP provides visibility across all sensitive</td>
<td>Provided via integration with specialized cloud security vendor</td>
</tr>
<tr>
<td></td>
<td>information, everywhere and always, enabling strong protective actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to safeguard data from threats and violations of corporate policies.</td>
<td></td>
</tr>
<tr>
<td>FWaaS</td>
<td>Firewall as a Service</td>
<td>Policy Management layer for FWaaS should be multi-tenant and hosted in SP cloud.</td>
</tr>
</tbody>
</table>
SASE Solution: Options to incrementally evolve towards SASE

<table>
<thead>
<tr>
<th>1</th>
<th>SD-WAN embedded Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2E L3-4 stateful micro segmentation</td>
<td>URL / Web filtering</td>
</tr>
<tr>
<td>L7 and SaaS application control</td>
<td>Host or Service chain to third party security functions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>Augment with hosted 3rd party Firewall VNF on CPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN Portal</td>
<td>VSD (Policy Engine)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>MSP's Cloud Security (SASE) through Service-Chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN Portal</td>
<td>VSD (Policy Engine)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>SASE Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>SASE POP</td>
<td>Mobile User</td>
</tr>
</tbody>
</table>

© 2021 SCTE®, CableLabs & NCTA. All rights reserved. | expo.scte.org
Considerations and Conclusions
Caveats on SASE @Peak of Inflated Expectation on Gartner’s hype cycle

SASE is at the Peak of Inflated Expectation on Gartner’s hype cycle
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
Thank You!

Charuhas Ghatge
Product and Solutions Marketing
Nuage Networks by Nokia
Charuhas.Ghatge@nokia.com