nuagenetworks
From Nokia

Secure SD-WAN 2.0

Contents

What is SD-WAN?

Gartner says SD-WAN has four characteristics

1. **Must support multiple WAN or underlay types**
   MPLS, Internet, LTE, etc

2. **Can do dynamic path selection**
   Allows for load sharing across WAN connections

3. **Provides a simple interface for managing WAN**
   Must support zero-touch provisioning at a branch, should be as easy to setup as home Wi-Fi

4. **Must support VPNs**
   As well as other third-party services, such as WAN optimization controllers, firewalls, web gateways, etc

A software-defined approach to managing wide-area networks, SD-WAN offers improved connectivity to branch offices and the cloud. End users are excited about SD-WAN because it enables them to manage and add network functionality using a cloud-based software model, which eases deployment, enables central manageability and reduces costs.

As compute resources and associated cloud services have exploded, the traditional enterprise network boundaries have expanded into the public cloud, branch locations and intelligent edges. Service providers, are increasingly providing managed SD-WAN services to enterprises and the number of enterprise SD-WAN deployments is growing rapidly.

So what does this all mean to enterprise branch security?

Security needs to evolve with SD-WAN

Existing security models cannot effectively address the evolving threat landscape and new security requirements driven by the move to virtualization (e.g. virtual machines, containers) and cloud-based architectures.

First, the current protection model in the enterprise branch is basic and can’t secure local internet breakout to the cloud, as traffic is steered over MPLS to datacenter (DC) sites where security is applied. Also, there is not much end-to-end micro-segmentation between branch and DC/cloud applications across the enterprise.

Second, with the increasing sophistication of attacks and evolving threat landscape, we cannot assume that all attacks can be prevented by protective controls. Currently there is not much visibility of branch user traffic. Visibility and security analytics are crucial for detecting attacks.

Last, but not least, the current security provisioning model for applications is largely manual and device-centric.

Direct connection to the internet increases security risk

Difficult to keep consistent network policies for both the WAN and cloud

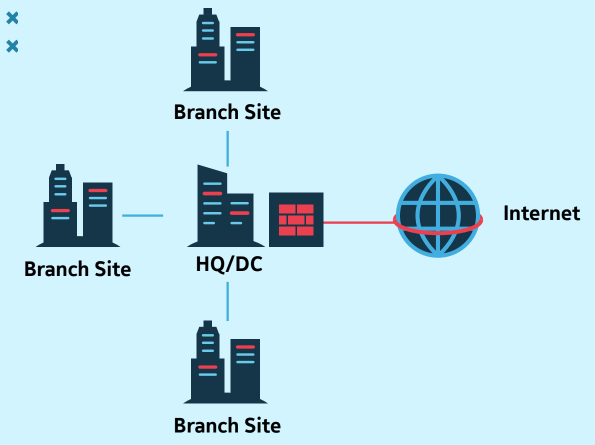
Inefficient provisioning model

Broadband internet access needs to be secured

The internet is not very secure for enterprise WAN requirements. Hence cloud-based application traffic is often backhauled from the branch to HQ before being handed off to the internet. WAN bandwidth constraints at the branch and added latency from backhauling connections introduce delay and jitter, which affect application performance.

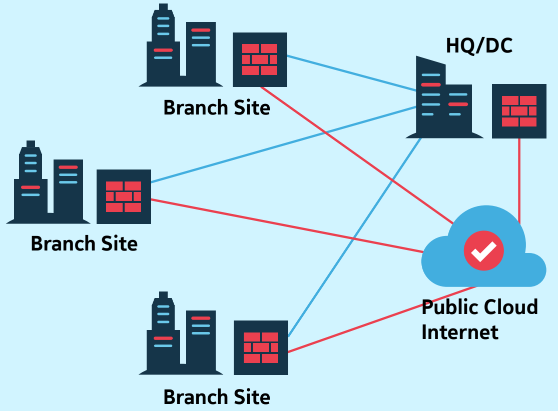
The solution is to use internet connectivity to the cloud and web applications directly from the branch. Thus, the SD-WAN solution needs to make these internet connections secure and reliable by creating encrypted tunnels between every site in the enterprise SD-WAN. It can take advantage of SSL security provided by the SaaS application for traffic going from the branch to the application directly over the internet. This makes the internet access more secure. With these encrypted links and a stateful firewall, an SD-WAN solution can prevent unauthorized outside traffic from entering the branch.

Traditional WAN — no direct internet access from branch (centralized security at HQ)



Backhauling creates delay, jitter and degrades application performance

SD-WAN – Local Internet Breakout



Direct internet access improves performance.
Secure links and encryption improves security

The SD-WAN components need to be secure and the solution must meet compliance mandates

The components that make up the Nuage Networks SD-WAN 2.0 solution (VNS – Virtualized Network Services) end points, control plane and data plane are secure, including their internal control traffic. End-point security is achieved by multi-factor authentication (MFA) and security key management.

Control plane – PKI certificates and security keys are generated and used in various communications between the VNS components.

Data plane - Encryption of the end-user data is achieved using IPSec with multiple cypher options.

These infrastructure security techniques make it feasible for the Nuage Networks SD-WAN solution to offer secure zero-touch provisioning (ZTP) using:

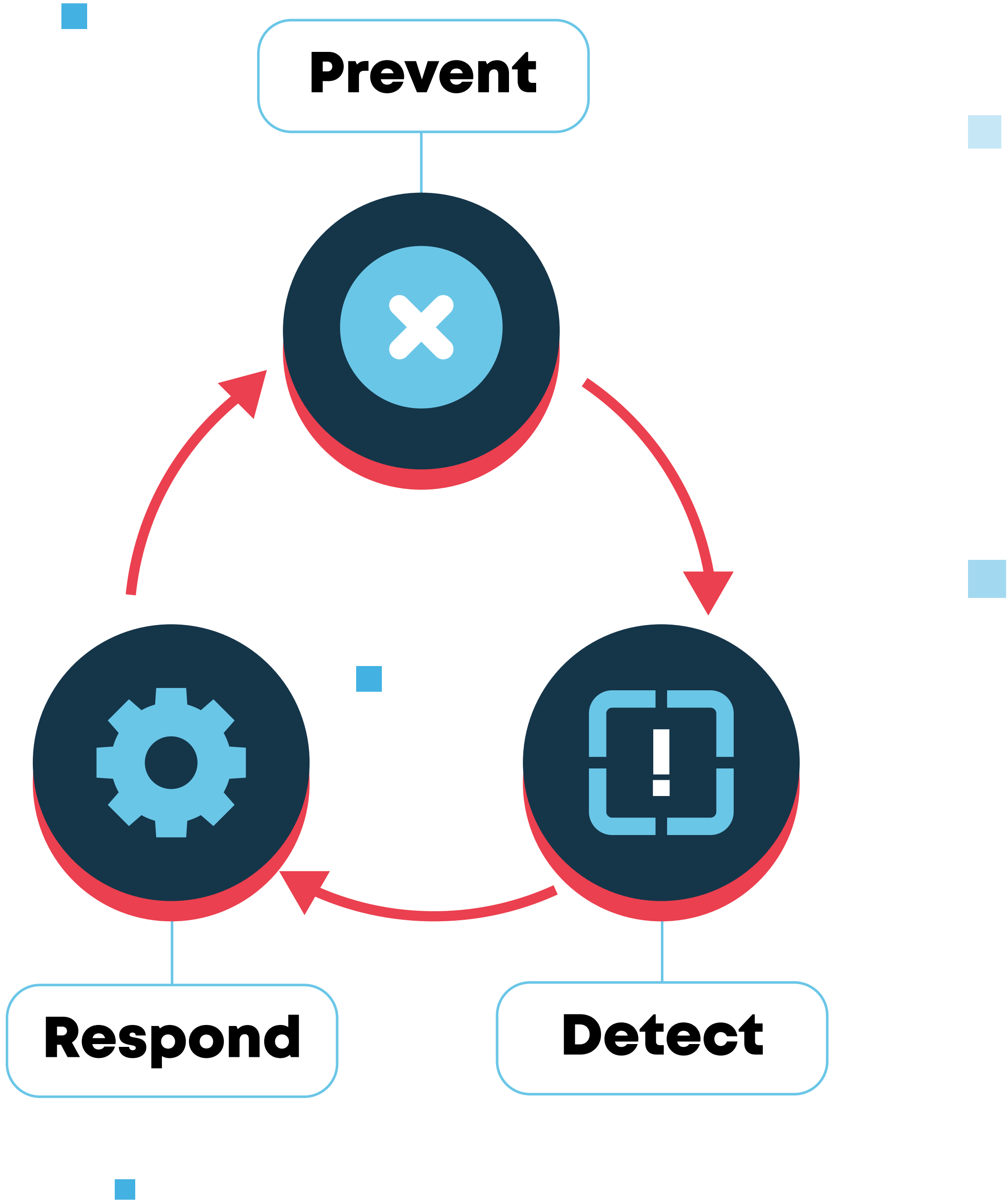
- A trusted chain through the end points, controller and the certificate authority
- Strong encryption that creates secure channels among the end points or between the end points and the controller

Compliance, such as PCI DSS, is achieved by employing user authentication, passwords, password controls, roles, and audit logs for change management.

Need to embrace Adaptive Security Architecture

Beyond prevention and detection

Gartner has defined a new security approach called **Adaptive Security Architecture ***, which goes beyond traditional prevention and detection **and includes responses based on continuous monitoring and analytics.** This adaptive security model suggests organizations move from the mindset of “incident response” to “continuous response” to defend against the new wave of security threats.

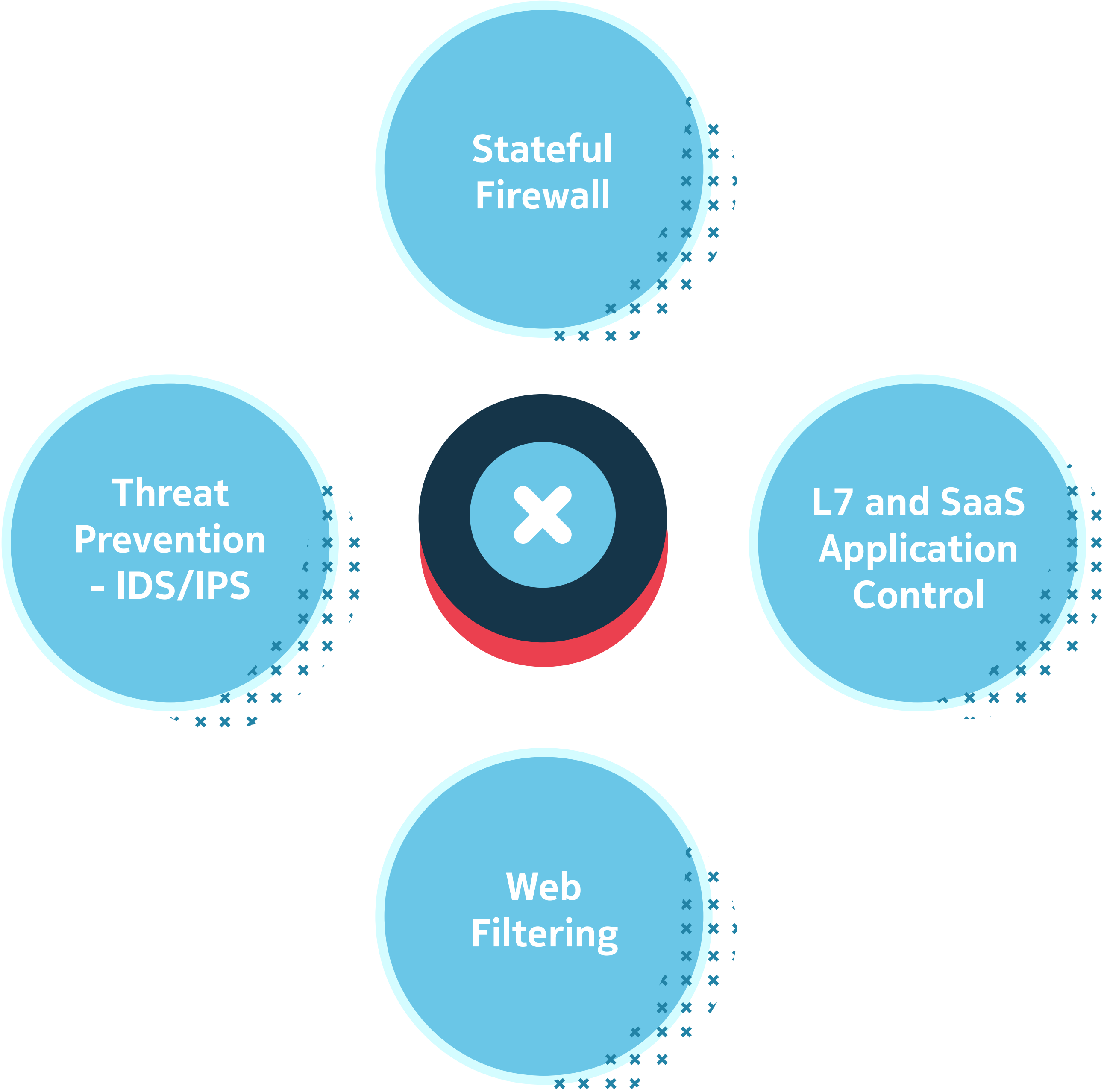


Prevent

Prevent or deter attacks so no loss is experienced

The **Benjamin Franklin** axiom that “an ounce of prevention is worth a pound of cure” is as true today as it was when **Franklin** made the quote, especially in the security paradigm.

In the next few pages we will explain how the Nuage Networks SD-WAN security solution helps you to prevent attacks, as well as detect and respond.



Prevent

L3–L4 stateful firewall

A stateful firewall filters packets based on the state and context of network connections and provides protocol inspection, such as TCP, UDP or ICMP, considering the STATE and CONTEXT of the flow, thereby eliminating additional attack surfaces. The Nuage Networks SD-WAN L3–L4 stateful firewall has been validated by a trusted third party and meets PCI-DSS v3.2 network firewall requirements.

Threat Prevention (IDS/IPS)

The embedded security capability in the SD-WAN CPE network service gateway (NSG) uses signatures of known attacks to match traffic that passes through the NSG. IDS/IPS policies are defined and managed centrally or through API. Statistics and reports on intrusion event details and rule hit count are logged and signatures are updated dynamically from the cloud and applied to the NSG.

Web Filtering

Web/URL filtering restricts branch user access to inappropriate or malicious internet content. It restricts local internet access to cloud services and whitelisted websites. Web filtering also helps mitigate malware and phishing attacks by blocking malicious webpages. Web filtering policies use a database that classifies URLs by category. The Nuage Networks URL/Web filtering function supports 1,800+ web categories and millions of websites.

L7 and SaaS application control

One of the prime benefits of SD-WAN is its ability to allow direct access for a branch user to the cloud and SaaS applications. A secure SD-WAN must have the ability to restrict user access to a specific application, set application-based policies and monitor and log application usage. For this, it needs to have a layer-7 DPI engine. Nuage Networks SD-WAN security supports a powerful Layer-7 DPI that recognizes thousands of applications. It also supports pre-defined SaaS services, such as Office365, Webex, Salesforce, Github, JIRA, Azure, AWS and Google, for easy access as well as monitoring.

Detect

Real-time security analytics and automation

With end-to-end visibility and control for each application, the operator is in a position to detect and protect resources at a very granular level using automation to respond in real time to threats.

The Nuage Networks SD-WAN security monitoring allows for contextual flow visibility of each flow, which helps in:

- Network forensics and troubleshooting
- Compliance and security audits

Identify attacks to prepare for rapid response

With SD-WAN security the admin or auditor can select a particular virtual network to collect rich contextual visibility into the flows. This helps in:

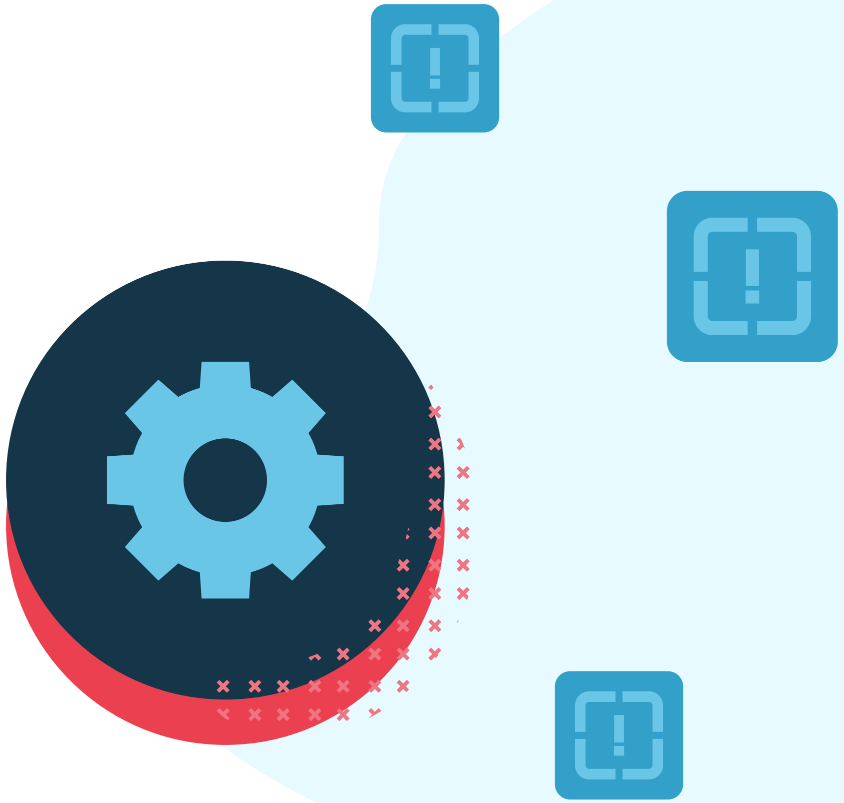
- Threat hunting and identifying attacks
- Real-time network security monitoring allowing you to generate alerts based on security events including port scan detection, portsweep detection, security policy violations and volumetric DDoS attacks.

Respond

Address incidents to minimize impact and return to secure state

A rapid and efficient incident response continues to be the biggest challenge facing security teams today. The sheer volume of these signals means that a lot of critical alerts miss getting appropriate attention. Security teams need help to scale better, be more efficient, focus on the right issues, and deal with incidents in a timely manner. This includes:

- Preventing malware on an infected branch device from entering the corporate network
- Leveraging network security analytics to identify suspect end-points based on threshold alerts.
- Use service chaining to dynamically insert security services (e.g., NGFW, IPS) for suspect traffic.



What is SASE?

SASE stands for “secure access service edge” a cloud-native architecture integrating WAN networking and security

Delivered as a managed cloud service to the enterprise

Shift from traditional box-heavy branch (NGFW, branch routers) to a thin branch (with SD-WAN) and heavy cloud model

Foundation of SASE is SD-WAN

- Cloud delivered, 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 and enforced in the WAN edge based on logical constructs and not using box-centric approach

Nuage Networks SD-WAN 2.0

Comprehensive security that is SASE-ready

Nuage Networks SD-WAN 2.0 provides:

- Stateful firewall, web/URL filtering, layer 7 and SaaS application recognition
- Visibility and policy control and extensive IP Filtering IPS/IDS provides threat prevention mechanisms.
- Real-time security analytics and automation provide powerful tools for threat hunting, network forensics and troubleshooting as well as identifying suspect end-points based on threshold alerts and using service chaining to dynamically insert security services (e.g., NGFW, IPS) for suspect traffic.

Nuage Networks SD-WAN 2.0 has the most flexible architecture for communication service providers (CSPs) to deliver SASE services such as embedded, third-party cloud security services (e.g., zScaler) or third-party partner VNFs hosted in the SD-WAN CSP cloud or our white-label service.

It also has SASE features such as:

- Zero-trust network access supported via our end-to-end micro-segmentation DNS filtering
- SWG as part of web filtering
- VM hosted in the cloud
- FWaaS offered via our white-label service

Nuage Networks SD-WAN 2.0 provides comprehensive security functions that protect your investment and comply with industry standards such as SASE.

Document Code: SR2006045076EN (June) CID207630