SD-WAN

A conceptual introduction

Paresh Khatri

CTO, IP Networks Division, APAC

                                 Public

Agenda

Enterprise WANs

SD-WAN 101

Use Cases
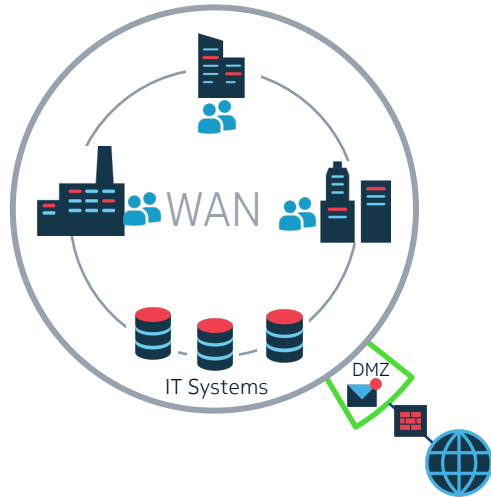
Inter-operability

Wrap-up

Public
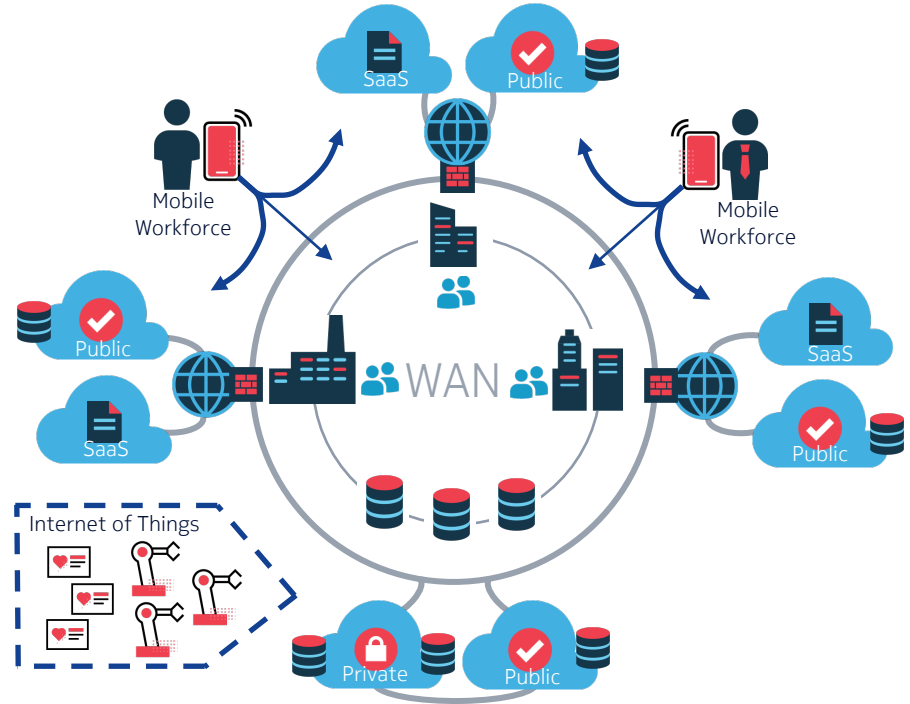
NOKIA

Enterprise WANs

- History and evolution
- Traditional approach
- Challenges
- Re-thinking the branch

Public

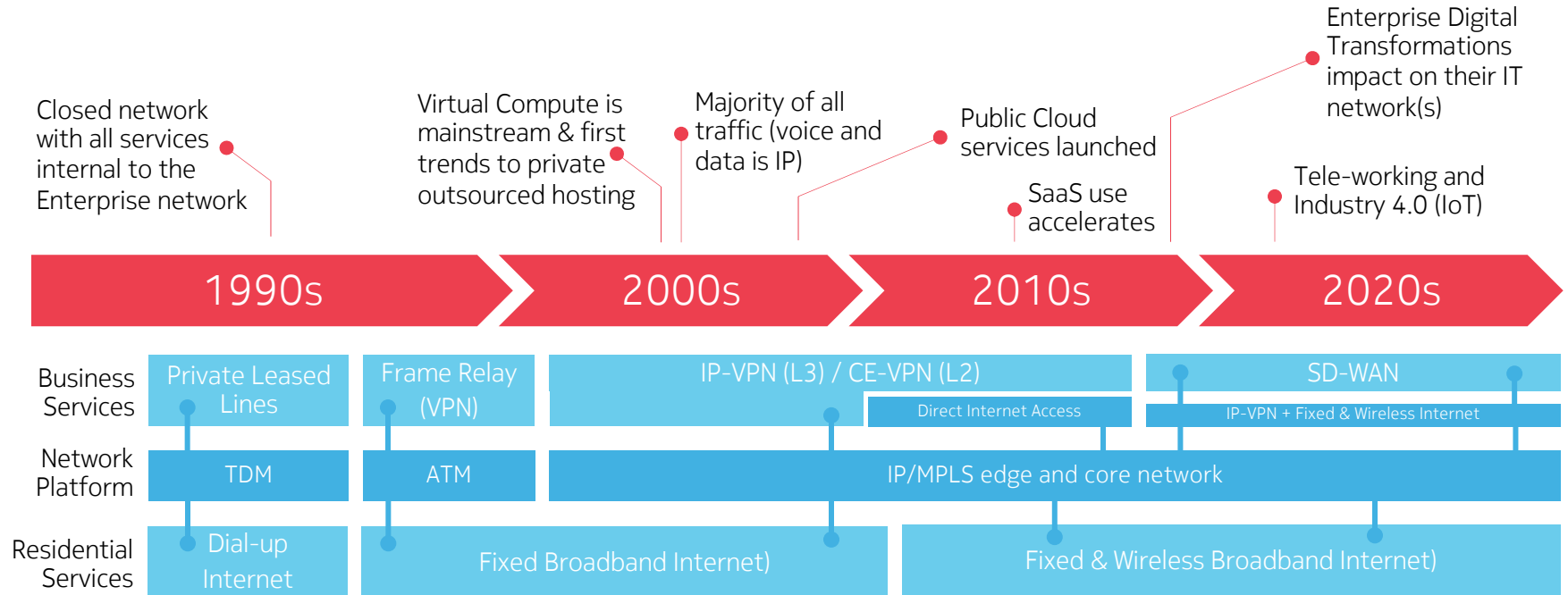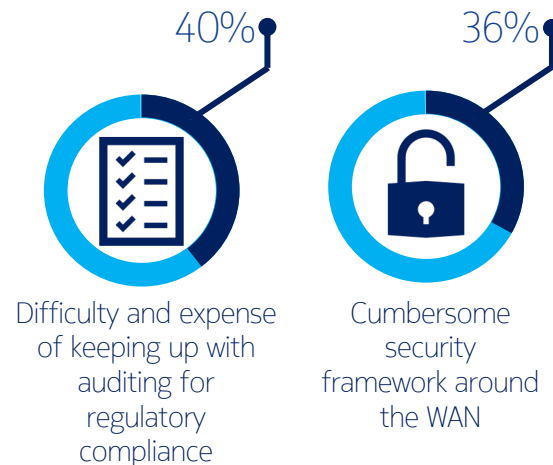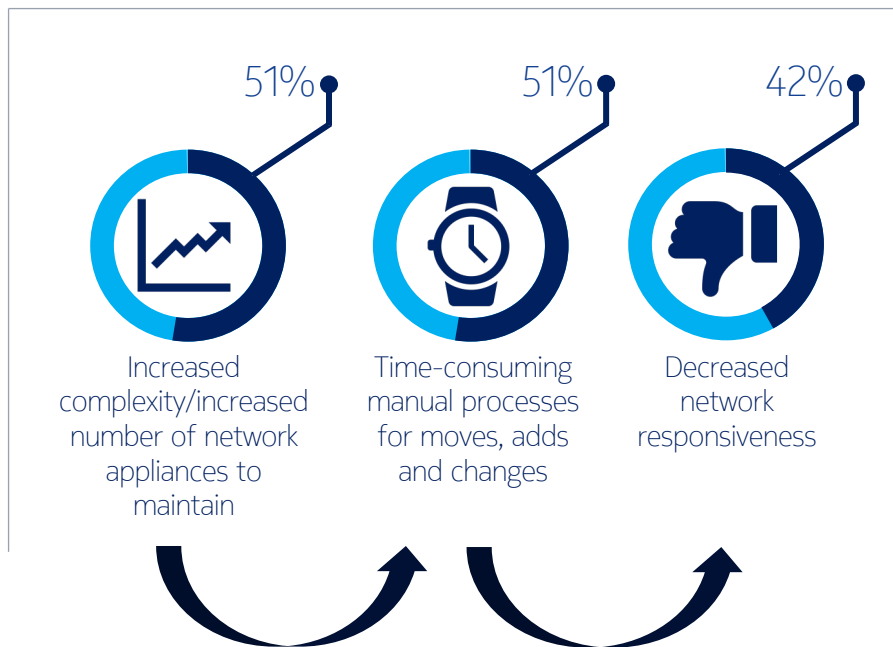**NOKIA**

Enterprise Networking Services

1990s-2000s

2010s-2020s

© Nokia 2022

Public

NOKIA

Evolution of the Enterprise WAN

Business networks and key technology shifts

Closed network with all services internal to the Enterprise network

Virtual Compute is mainstream & first trends to private outsourced hosting

Majority of all traffic (voice and data is IP)

Public Cloud services launched

SaaS use accelerates

Enterprise Digital Transformations impact on their IT network(s)

Tele-working and Industry 4.0 (IoT)

| 1990s | 2000s | 2010s | 2020s |

	1990s	2000s	2010s	2020s
Business Services	Private Leased Lines	Frame Relay (VPN)	IP-VPN (L3) / CE-VPN (L2) / Direct Internet Access	SD-WAN / IP-VPN + Fixed & Wireless Internet
Network Platform	TDM	ATM	IP/MPLS edge and core network	
Residential Services	Dial-up Internet	Fixed Broadband Internet)	Fixed & Wireless Broadband Internet)	

Public

NOKIA

The voice of the enterprise
Enterprise managers polled by IDG on today's WAN - Five biggest issues

51% — Increased complexity/increased number of network appliances to maintain

51% — Time-consuming manual processes for moves, adds and changes

42% — Decreased network responsiveness

40% — Difficulty and expense of keeping up with auditing for regulatory compliance

36% — Cumbersome security framework around the WAN

IDG Research :Enterprise Poll, Optimizing the WAN

Public

NOKIA

Rethinking of the 'Branch'

Branch (def): Any location requiring attachment to an Enterprise WAN

Fixed

Office / Building

Private Datacenter

Retail / Store Front

Kiosk / ATM

Temporary

Pop-up / Co-location

Mobile workforce

Virtual

Public Cloud (IaaS)

Cloud Applications (SaaS)

Public

NOKIA

SD-WAN 101

- Definition
- SD-WAN @ MEF
- SD-WAN versus traditional WANs/VPNs
- Implementation elements

Public

NOKIA

SD-WAN 101

- Definition
- SD-WAN @ MEF
- SD-WAN versus traditional WANs/VPNs
- Implementation elements

Public

NOKIA

What is an SD-WAN service?

SD-WAN?
–

No widely-adopted industry standard definition … the MEF has made an effort, though, and it may well become the accepted definition

What, then, is an SD-WAN service?

Public

NOKIA

Key capabilities of an SD-WAN service (1)
Fundamental capabilities

- **IP-based virtual overlay service**

  Provides connectivity between different sites/users/devices of a subscriber's network

- **Transport-agnostic**

  Can be delivered over a variety of underlays:
  - On-net MPLS
  - Off-net Internet
  - Access technologies include cable, DSL, PON, wireless/cellular etc.

- **Support of any topology**

  Full-mesh, partial-mesh, hub-and-spoke

- **Application-aware routing**

  Application traffic (e.g., Skype for Business or SAP) is forwarded over different WAN underlays based on QoS, security and business priority policies

- **Policy-based packet forwarding**

  QoS or security policy

- **High availability**

  Via multiple underlay connections e.g. combination of an MPLS and an Internet access circuit

Public

NOKIA

Key capabilities of an SD-WAN service (2)
Fundamental capabilities

● **Service automation**

Centralised control, management and orchestration typically accessed via a customer portal

● **CPE automation**

Zero-touch provisioning of CPE

● **Value-added services**

Eg. WAN optimization, security services (SASE)

● **Management**

Completely managed by the service provider or co-managed

NOKIA

SD-WAN 101

- Definition
- **SD-WAN @ MEF**
- SD-WAN versus traditional WANs/VPNs
- Implementation elements

Public

NOKIA

What is an SD-WAN service?
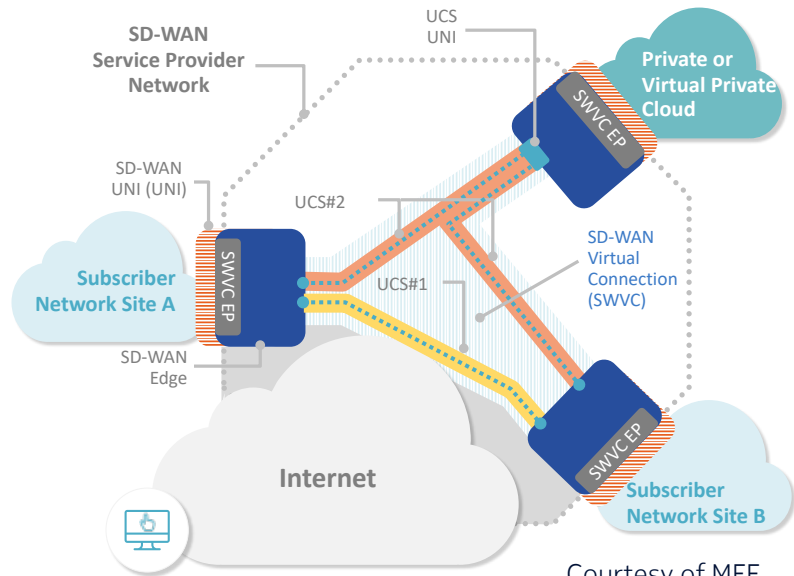
SD-WAN according to MEF

MEF defines an SD-WAN service as…

A service that provides a Subscriber with a virtual overlay network that enables application-aware, policy-driven, and orchestrated connectivity between SD-WAN User Network Interfaces (UNIs). It also provides the logical construct of a L3 Virtual Private Routed Network for the Subscriber that conveys IP Packets between Subscriber sites. MEF 3.0 SD-WAN services can take advantage of multiple Underlay Connectivity Services (UCS) to deliver differentiated service capabilities rather than connectivity services based on a single transport facility.*

*Source: https://www.mef.net/wp-content/uploads/2019/11/MEF-white-paper-MEF-3-0-SD-WAN-Services.pdf

Public

NOKIA

SD-WAN @ MEF
MEF 70.1

- SD-WAN terminology, service components and an SD-WAN service definition

SD-WAN
Service Provider
Network

UCS
UNI

**Private or
Virtual Private
Cloud**

SWVC EP

SD-WAN
UNI (UNI)

UCS#2

**Subscriber
Network Site A**

SWVC EP

UCS#1

SD-WAN
Virtual
Connection
(SWVC)

SD-WAN
Edge

Internet

SWVC EP

**Subscriber
Network Site B**

Courtesy of MEF

SD-WAN User to Network Interface (UNI)
Demarcation point between the Service Provider and the
Subscriber's responsibility

SD-WAN Virtual Connection (SWVC)
Logical multipoint connection between the SD-WAN
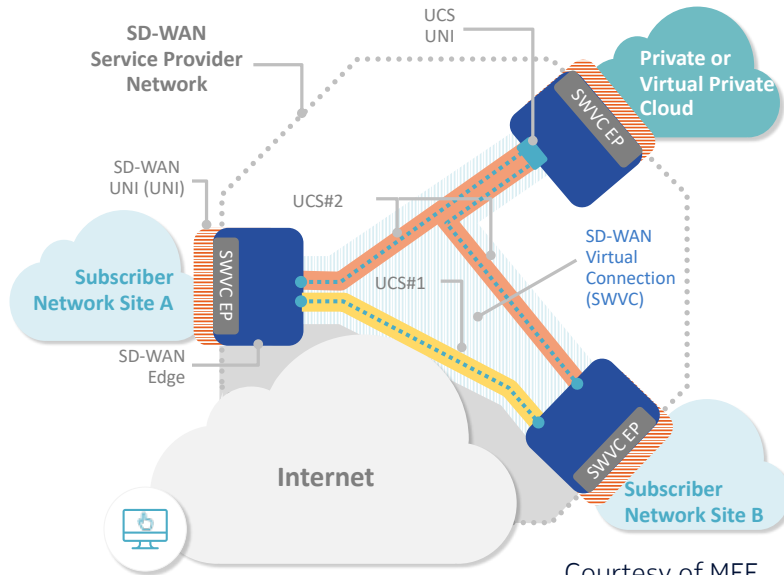UNIs that corresponds to the SD-WAN Service

SD-WAN Virtual Connection End-Point (SWVC EP)
Logical point at which policies are assigned to
application flows and applied to each IP Packet

NOKIA

SD-WAN @ MEF
MEF 70.1

- SD-WAN terminology, service components and an SD-WAN service definition

SD-WAN
Service Provider
Network

UCS
UNI

Private or
Virtual Private
Cloud

SD-WAN
UNI (UNI)

UCS#2

SWVC EP

SD-WAN
Virtual
Connection
(SWVC)

Subscriber
Network Site A

SWVC EP

UCS#1

SD-WAN
Edge

SWVC EP

Internet

Subscriber
Network Site B

Courtesy of MEF

SD-WAN Edge
Connects the SD-WAN UNI to the UCSs, including
mapping packets to application flows, applying policies,
and selecting a TVC over which to forward each flow.

Underlay Connectivity Service (UCS)
Various services including (but not limited to) Ethernet
Services (MEF 6.2), MEF IP Services (MEF 61.1)
including MPLS VPNs and public Internet Access, and
MEF Optical Transport Services (MEF 63).

Tunnel Virtual Connection (TVC)
The point-to-point paths across the UCSs that compose
an SD-WAN Service

Internet Breakout
Access to the Internet from an SD-WAN UNI for certain
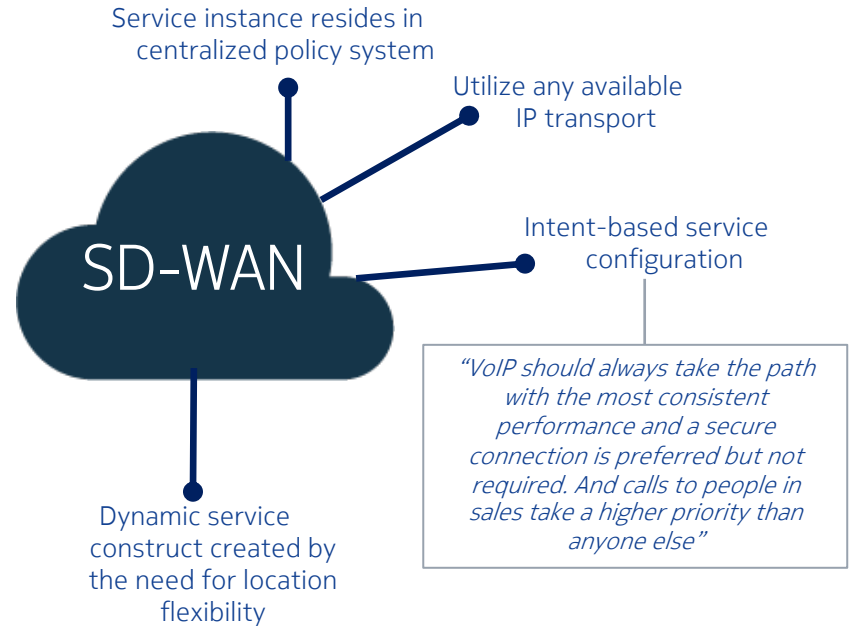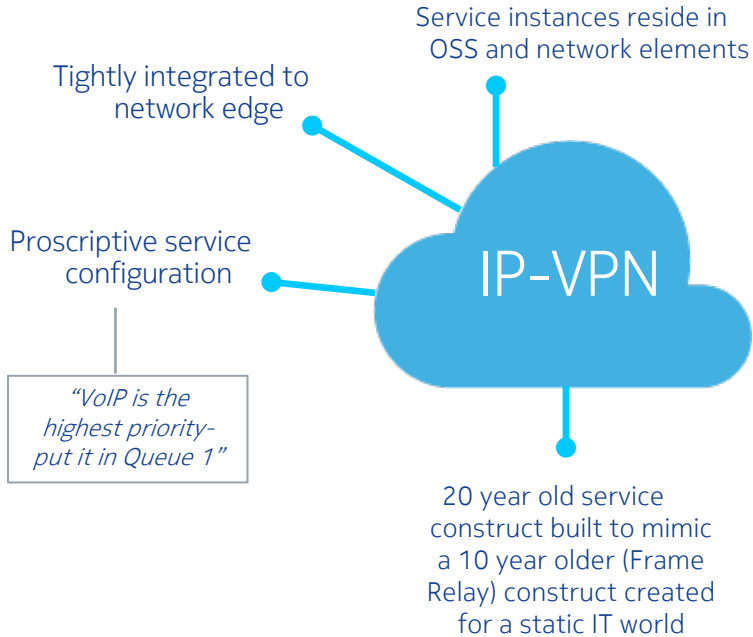application flows, via an Internet Access UCS.

Public

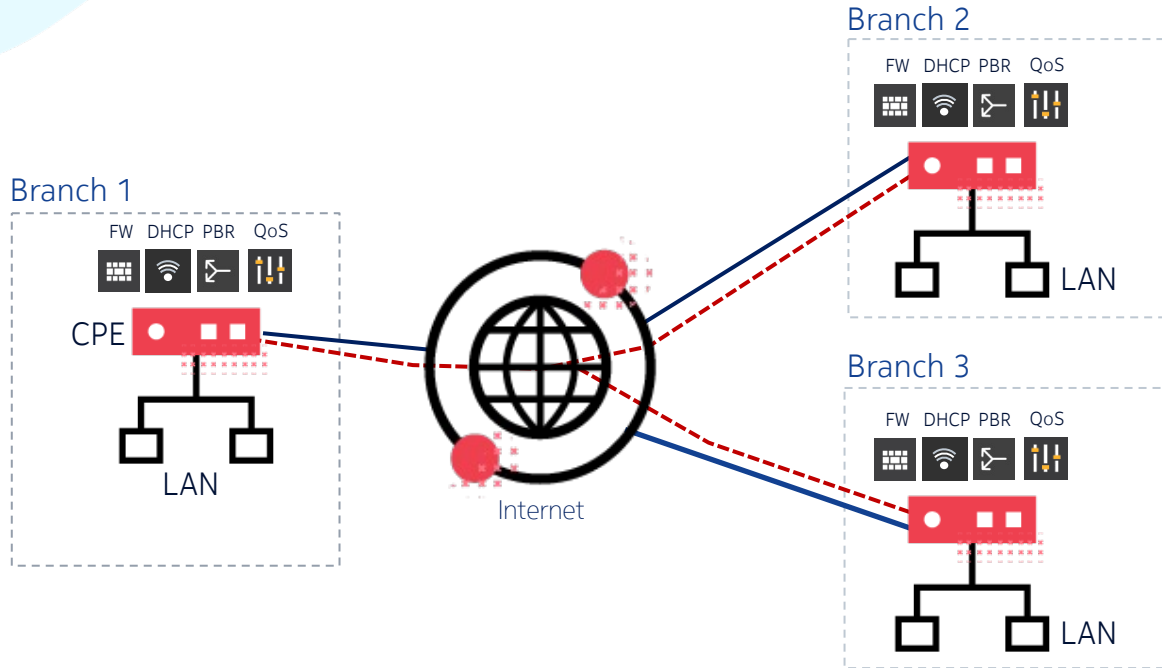**NOKIA**

SD-WAN 101

- Definition
- SD-WAN @ MEF
- **SD-WAN versus traditional WANs/VPNs**
- Implementation elements

Public

NOKIA

SD-WAN vs traditional VPNs

IP-VPN

Service instances reside in OSS and network elements

Tightly integrated to network edge

Proscriptive service configuration

"VoIP is the highest priority- put it in Queue 1"

20 year old service construct built to mimic a 10 year older (Frame Relay) construct created for a static IT world

SD-WAN

Service instance resides in centralized policy system

Utilize any available IP transport

Intent-based service configuration

"VoIP should always take the path with the most consistent performance and a secure connection is preferred but not required. And calls to people in sales take a higher priority than anyone else"

Dynamic service construct created by the need for location flexibility

Public

NOKIA

DIY IPsec VPNs

Branch 1

FW DHCP PBR QoS

CPE

LAN

Branch 2

FW DHCP PBR QoS

LAN

Branch 3

FW DHCP PBR QoS

LAN

Internet
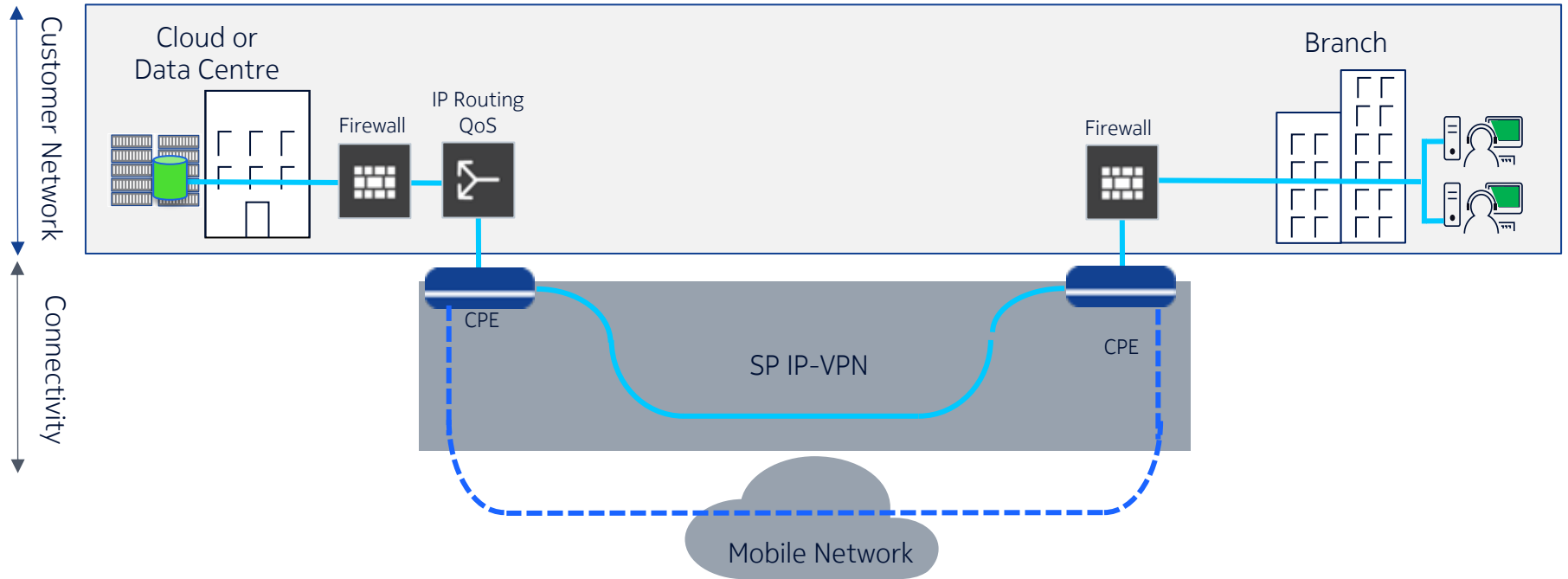
With SD-WAN, service providers become engaged in the customer overlay network, providing a managed service for SMB/SME. Value-added services are introduced from the data center.
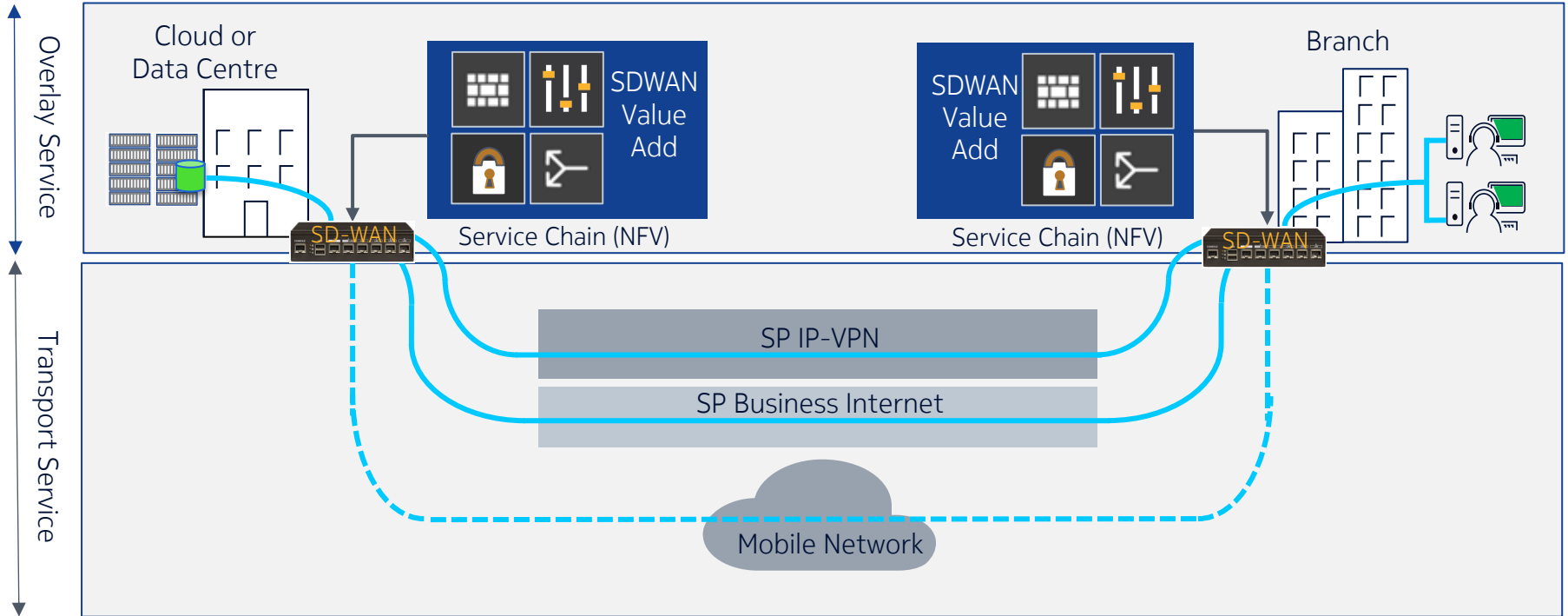
Public

NOKIA

IP-VPN based Wide Area Network (WAN)
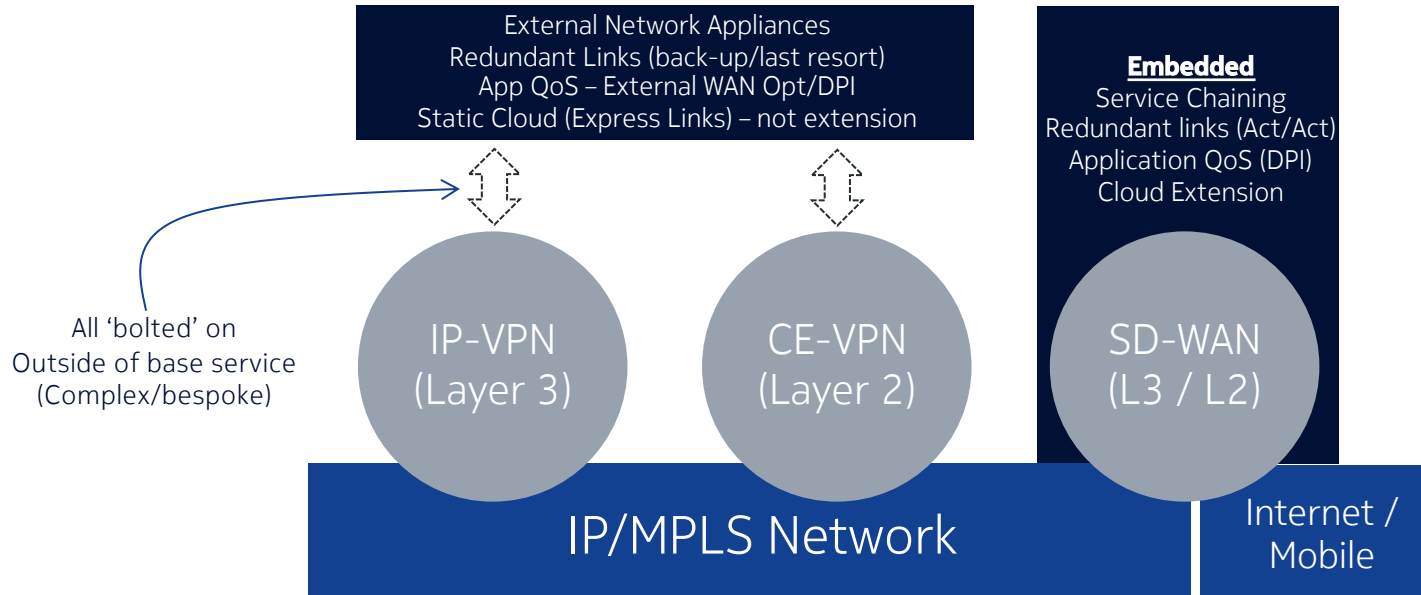
Clear separation between customer and VPN transport service

Customer Network

Connectivity

Cloud or
Data Centre

Firewall

IP Routing
QoS

Branch

Firewall

CPE

SP IP-VPN

CPE

Mobile Network

© Nokia 2022

Public

NOKIA

SD-WAN Service Overview

Value opportunity in delivering seamless IP and IT services

Public

NOKIA

Positioning SD-WAN Services

External Network Appliances
Redundant Links (back-up/last resort)
App QoS – External WAN Opt/DPI
Static Cloud (Express Links) – not extension

Embedded
Service Chaining
Redundant links (Act/Act)
Application QoS (DPI)
Cloud Extension

All 'bolted' on
Outside of base service
(Complex/bespoke)

IP-VPN
(Layer 3)

CE-VPN
(Layer 2)

SD-WAN
(L3 / L2)

IP/MPLS Network

Internet /
Mobile

The value of SD-WAN to enterprises is in the network being more adaptable to their changing business needs

© Nokia 2022   Public
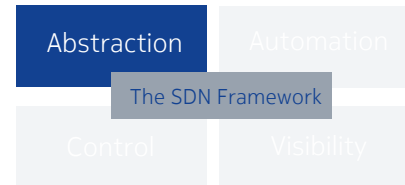
NOKIA

SD-WAN 101

- Definition
- SD-WAN @ MEF
- SD-WAN versus traditional WANs/VPNs
- **Implementation elements**

Public

NOKIA

Implementing SD-WAN
Abstract the wide area network from the underlying transport
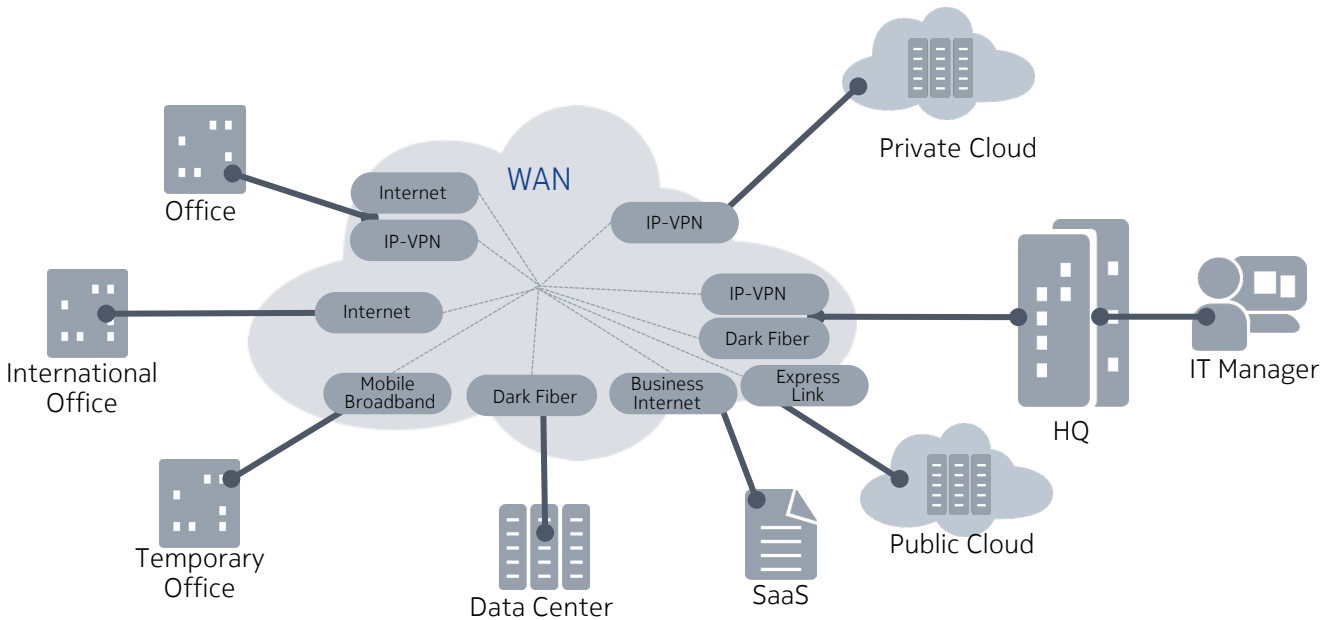
1 **Abstract** – the service from the transport

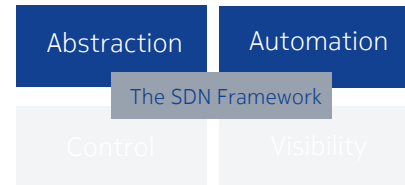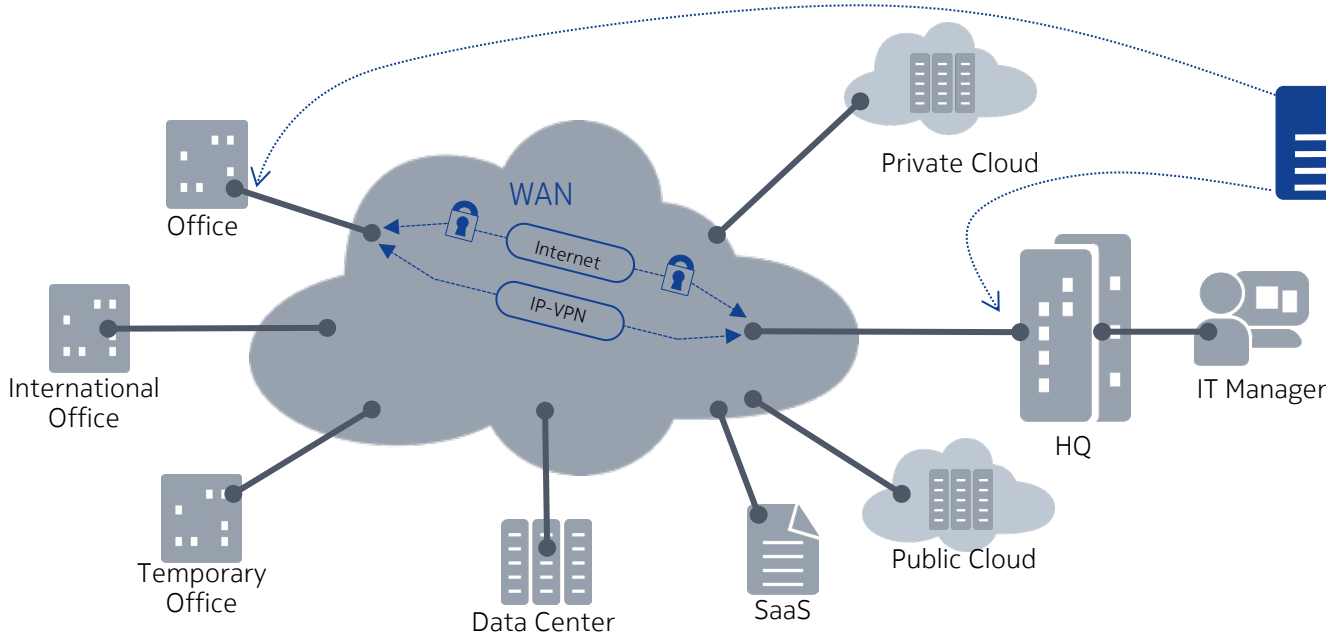|	
Abstraction	Automation
	The SDN Framework
Control	Visibility

Public

NOKIA

Implementing SD-WAN
Automate the key changes in the network via centralized policy
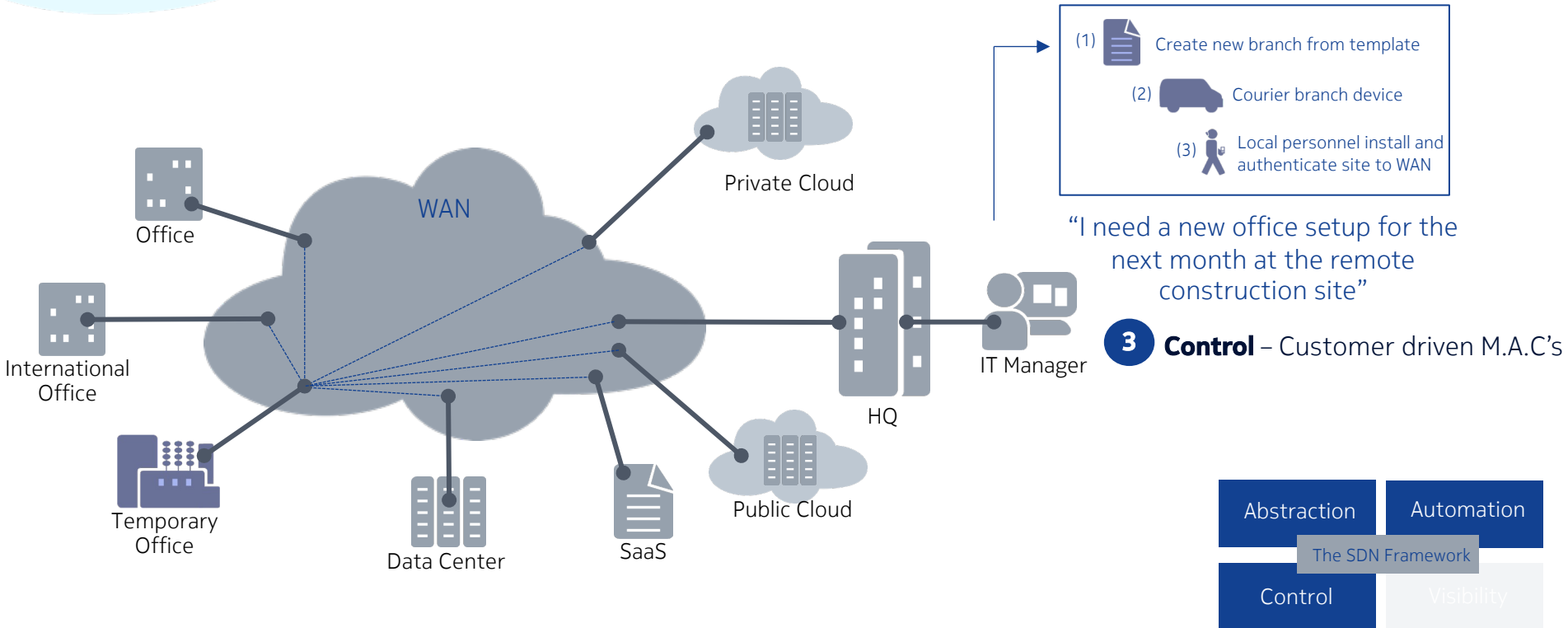

Branch Policy:
"Videoconferencing should use the encrypted Internet link with all other traffic forwarded over IP-VPN link"

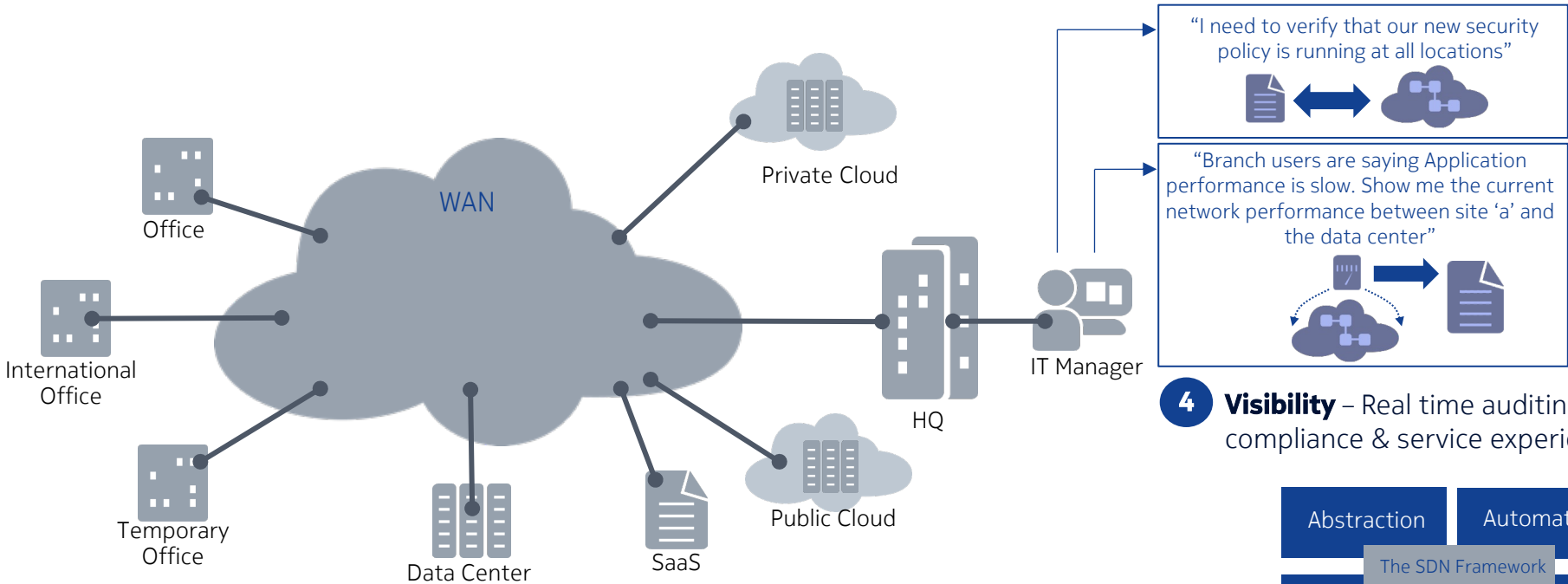**2** **Automate** – via policy based networking

Abstraction | Automation
The SDN Framework
Control | Visibility

Office

International Office

Temporary Office

Data Center

SaaS

Public Cloud

Private Cloud

WAN

Internet

IP-VPN

HQ

IT Manager

Implementing SD-WAN
Control via comprehensive self-service portal

(1) Create new branch from template

(2) Courier branch device

(3) Local personnel install and authenticate site to WAN

Private Cloud

WAN

Office

International Office

Temporary Office

Data Center

SaaS

Public Cloud

HQ

IT Manager

"I need a new office setup for the next month at the remote construction site"

3 **Control** – Customer driven M.A.C's

Abstraction	Automation
The SDN Framework	
Control	Visibility

Public

NOKIA

Implementing SD-WAN

Visibility into the state of the network and its performance

"I need to verify that our new security policy is running at all locations"

"Branch users are saying Application performance is slow. Show me the current network performance between site 'a' and the data center"

Private Cloud

WAN

Office

International Office

Temporary Office

Data Center

SaaS

Public Cloud

HQ

IT Manager

4 **Visibility** – Real time auditing / compliance & service experience

Abstraction	Automation
The SDN Framework	
Control	Visibility

Public

NOKIA
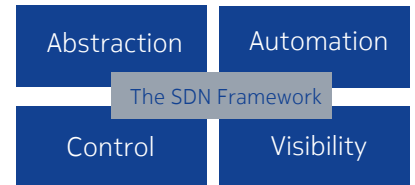
What does SD-WAN look like?

Overlay offers
transport choices

Policy-based control

Service-governance
of service functions

App

Site

Multiple
transport links

Separation of service
from transport

App

DC/cloud

Application-aware
path selection

VM
VM
VM
VM
VM
VM

Expand
to include
applications

IT approach to network
service delivery

Site
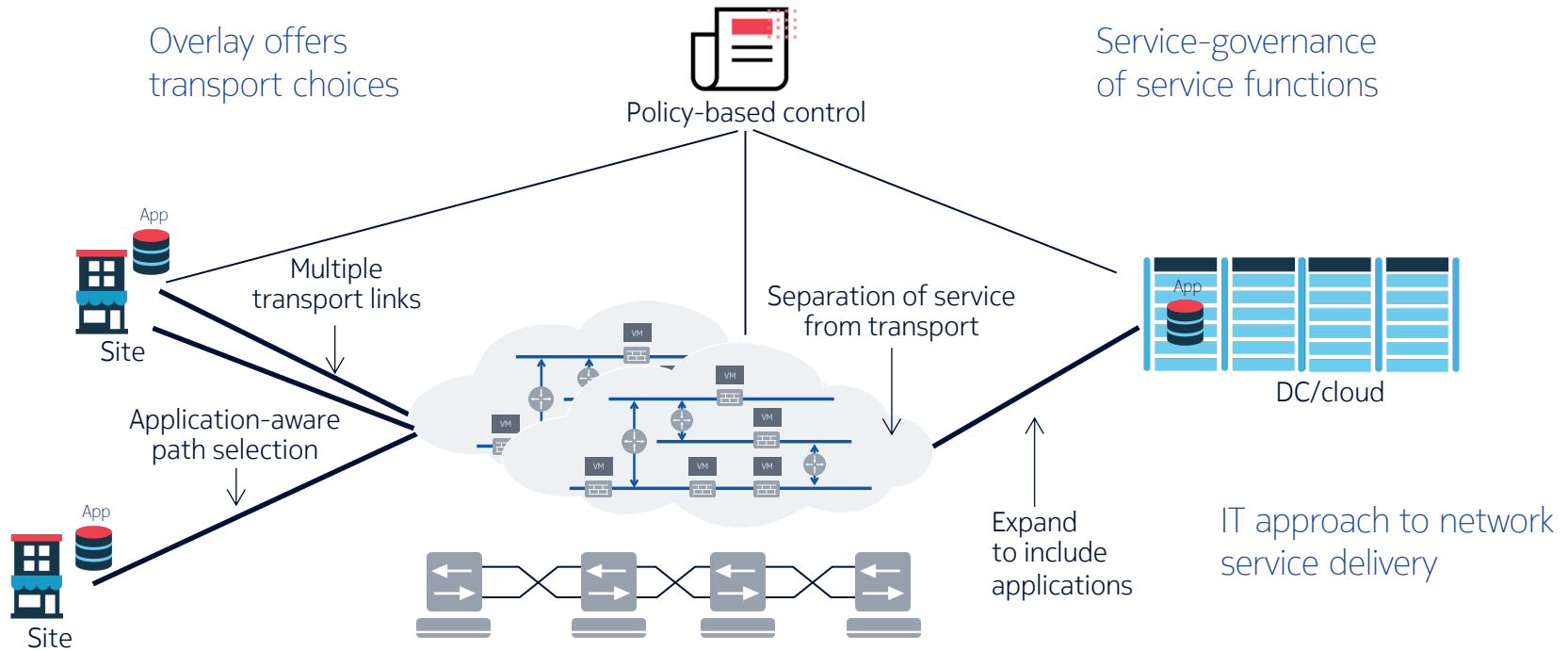
Elements of an SD-WAN implementation
Architectural view

Self-service portal

Orchestrator — Policy engine

Controller — Network control

Control protocol(s)

Control protocol(s)

Service chaining

F/W

NAT

WAN

Data Centre

uCPE

Branch Offices

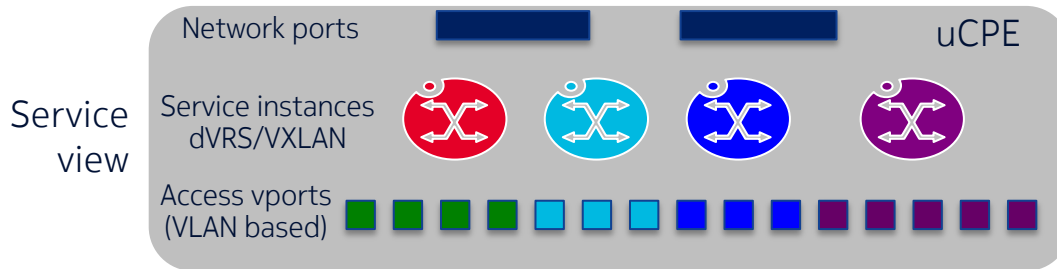uCPE

Internet

Public Cloud

uCPE

Branch Offices

Public

Use Cases

© 2020 Nokia

Public
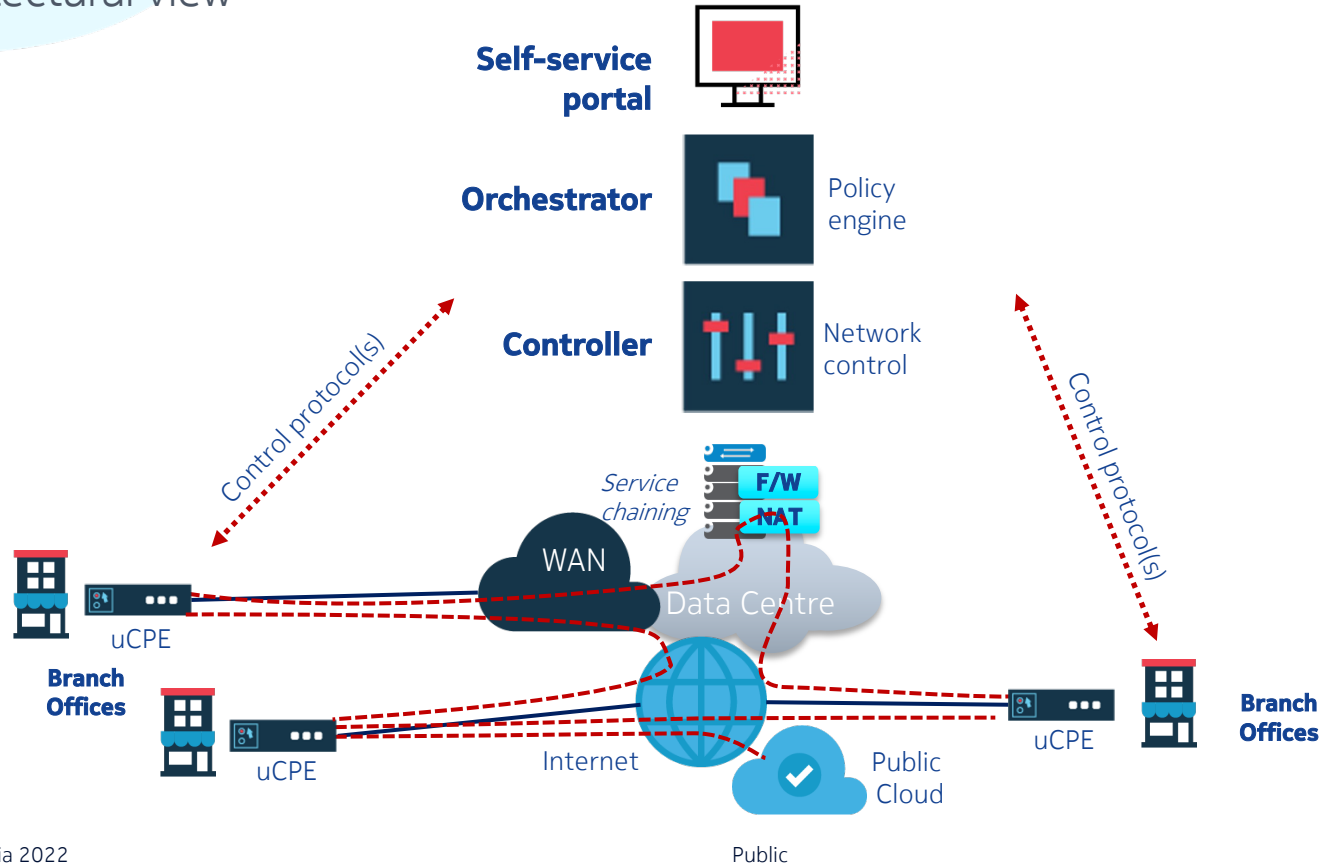
Defining services

1. Admin models the uCPE

2. Admin assigns user rights

3. Admin/users define service types

4. Admin/users define security zones (segmentation)

5. Admin/users define QoS, NAT, DHCP

6. Admin/users instantiate uCPE membership

Enterprise   Users

FW   DHCP   NAT   QoS   VPN

SDWAN Service Catalogue

Orchestrator

Service view

Network ports   uCPE

Service instances
dVRS/VXLAN

Access vports
(VLAN based)

© Nokia 2022   Public

NOKIA
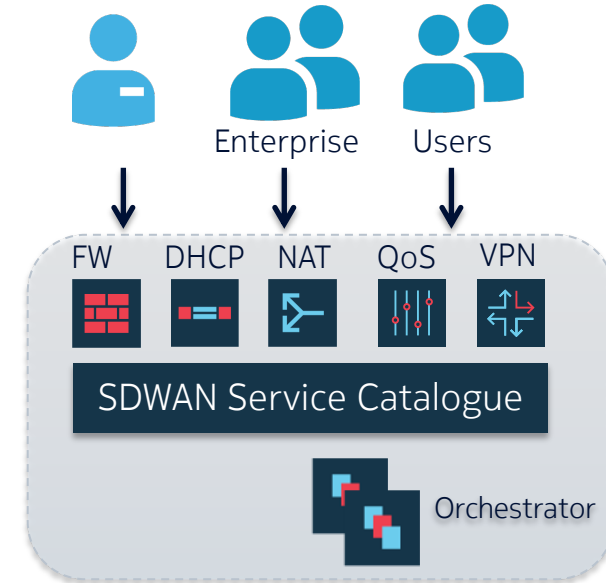
Centralized service templates
Solving the management-plane problem

SD-WAN System

Orchestrator

Controller

- Local DHCP server
- DNS cache/forwarder
- NAT/PAT services
- L4 stateful FW
- L4-QoS awareness

FW   DHCP   NAT   QoS   VPN

LAN

Compute   SD-WAN Agent

uCPE

WAN

NOKIA
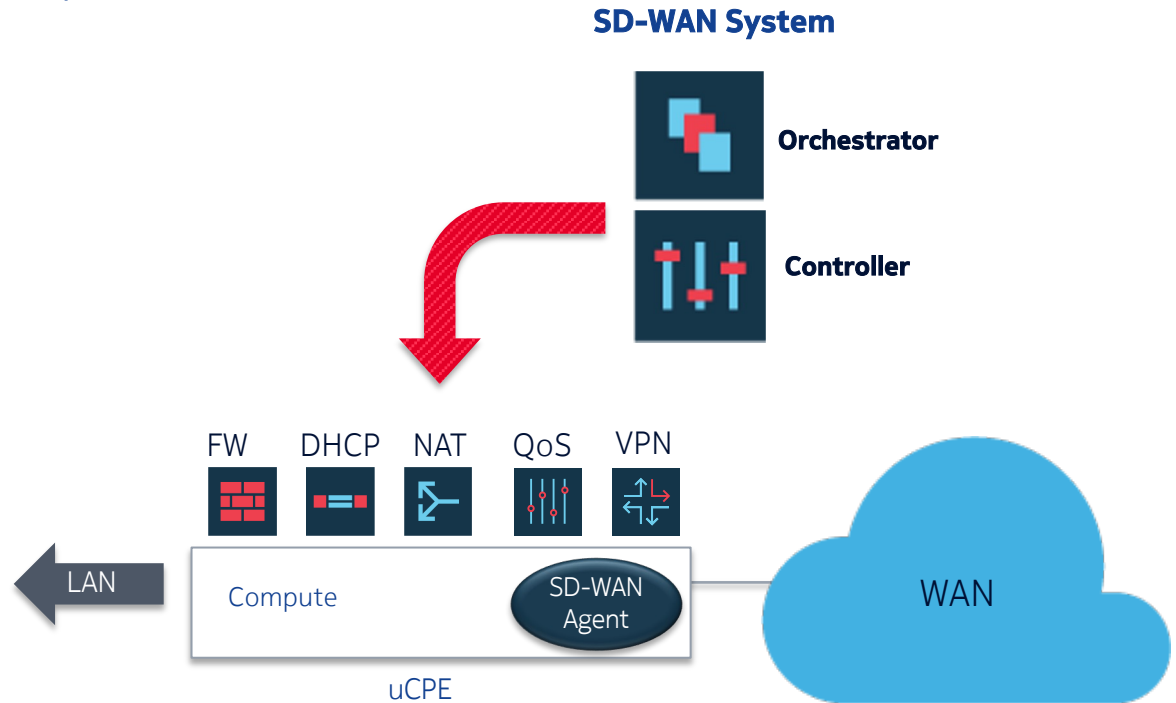
Automated branch bootstrapping

Orchestrator

Bootstrap
Process

Branch

IP
network

User
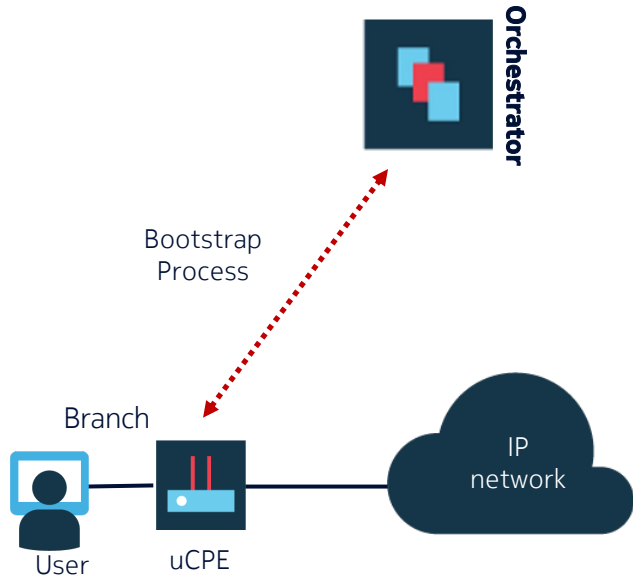
uCPE

① Onboard new uCPE in orchestrator platform

② Define SD-WAN service & policies in orchestrator platform

③ Physically install uCPE at branch & input installer authentication.

④ uCPE self-bootstraps.

⑤ Controller sets up SD-WAN connectivity

NOKIA

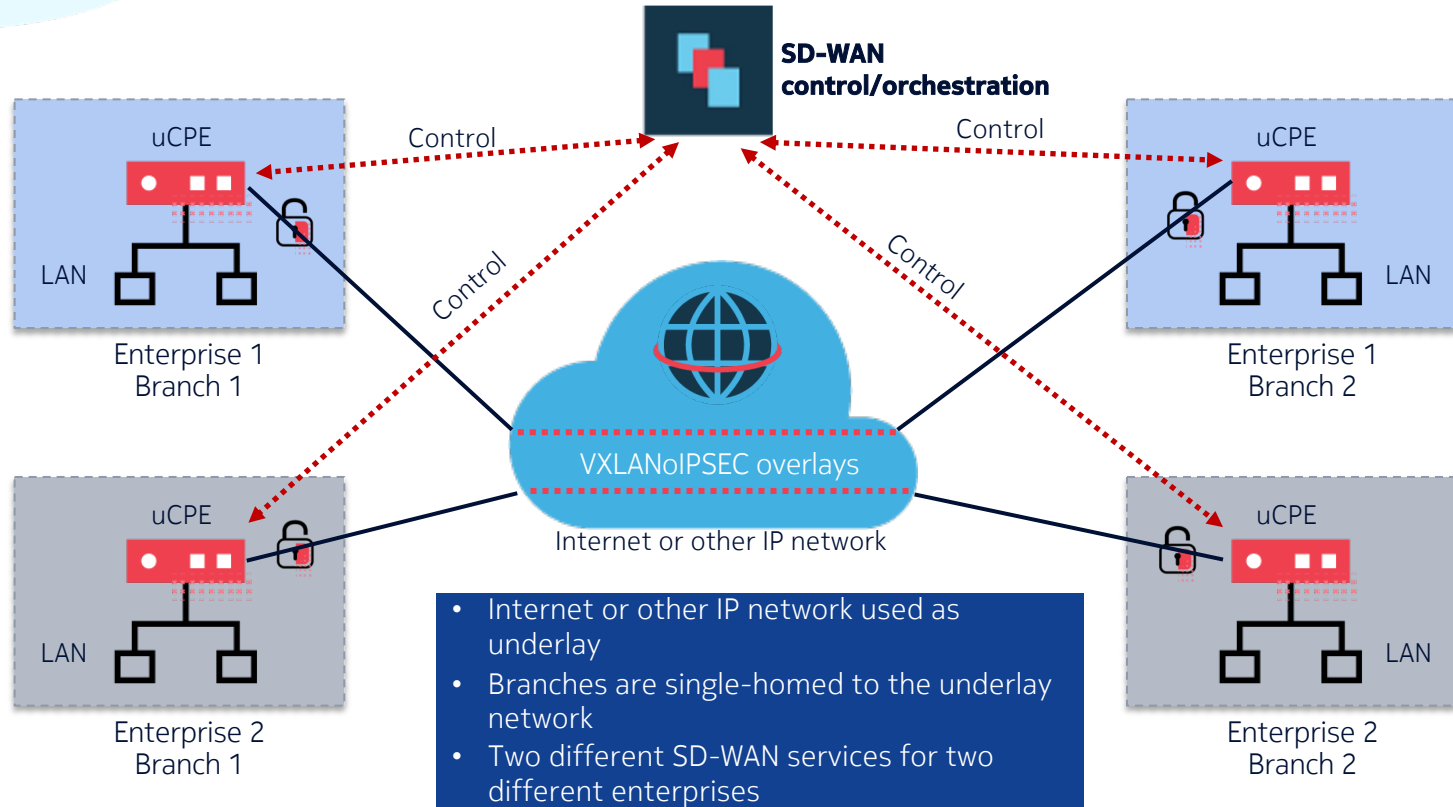# Use case: SD-WAN overlay on Internet underlay

Single enterprise shown

SD-WAN
control/orchestration

Control

Control

uCPE

uCPE

LAN

LAN

Enterprise 1
Branch 1

Enterprise 1
Branch 2

VXLANoIPSEC overlays
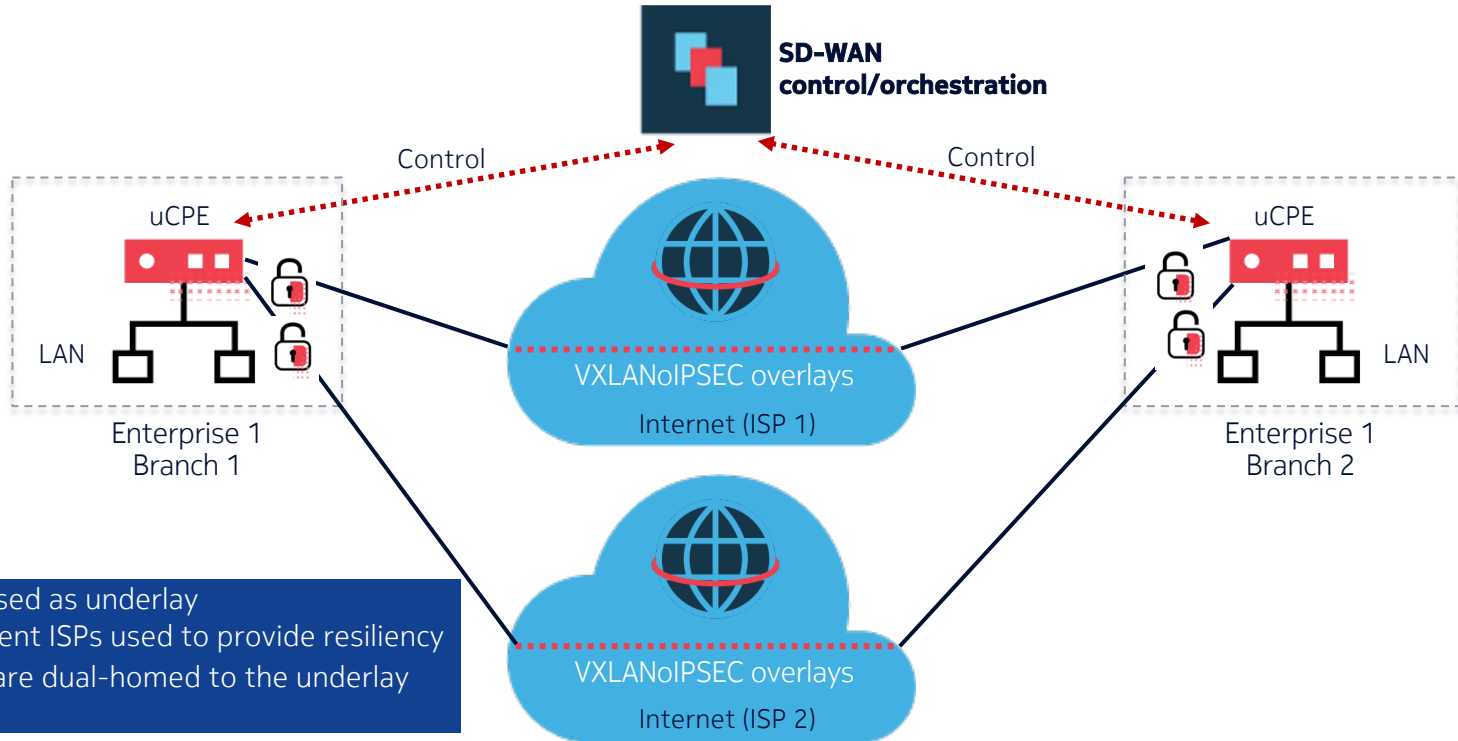
Internet or other IP network
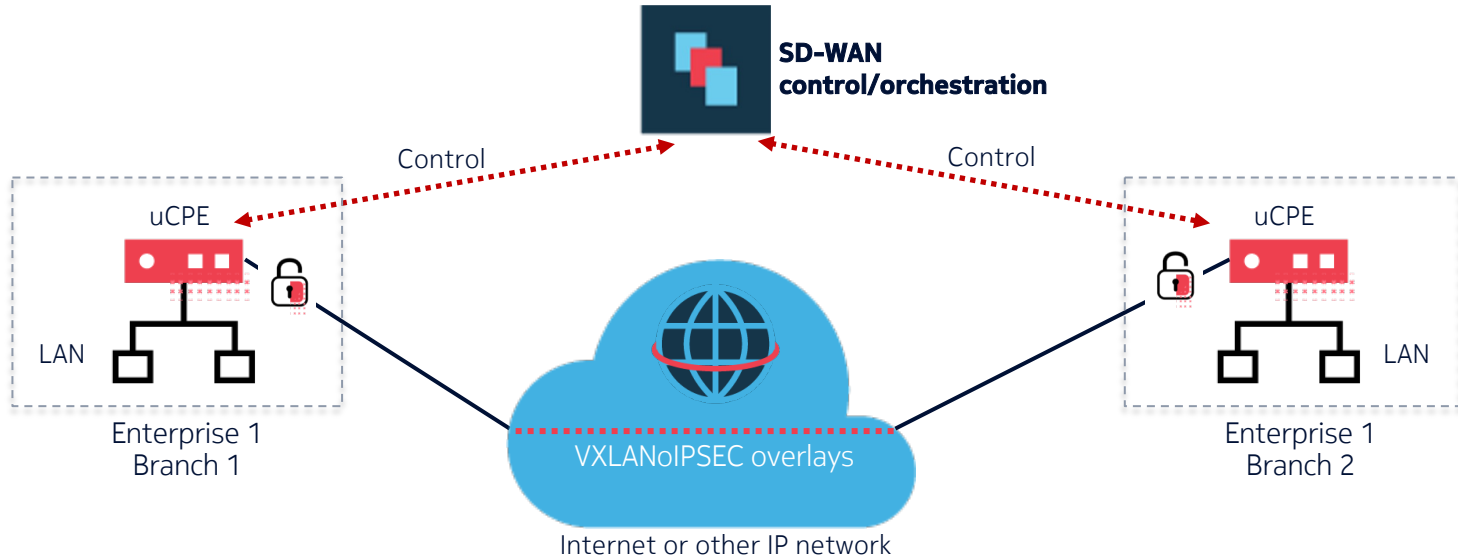
- Internet or other IP network used as underlay
- IPsec security is highly desirable when using the public Internet as an underlay
- Branches are single-homed to the underlay network
- SD-WAN provider is not necessarily the underlay service provider

Public

NOKIA

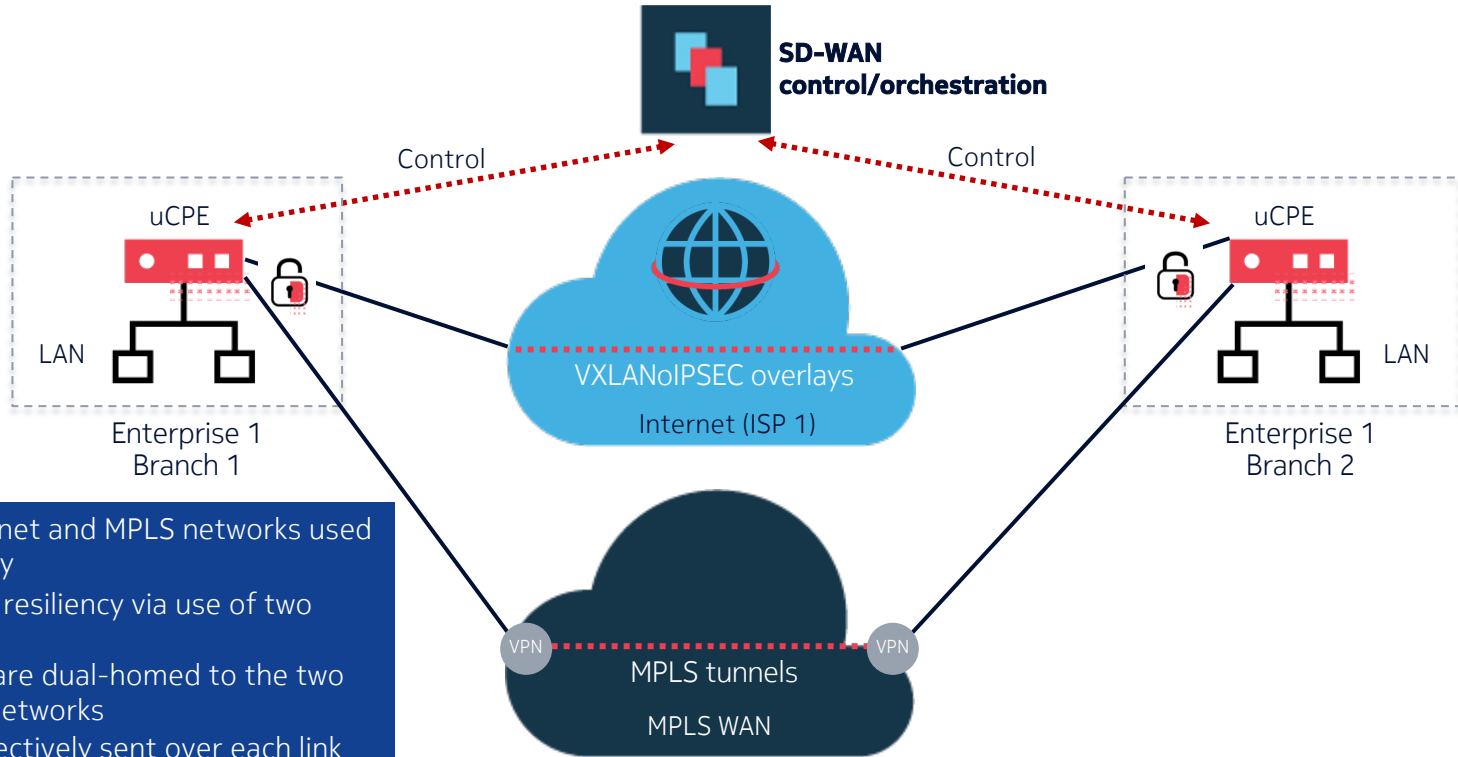# Use case: SD-WAN overlay on Internet underlay
Multiple enterprises shown

SD-WAN control/orchestration

Control

Control

Control

Control

uCPE

LAN

Enterprise 1
Branch 1

uCPE

LAN

Enterprise 1
Branch 2

VXLANoIPSEC overlays

Internet or other IP network

uCPE

LAN

Enterprise 2
Branch 1

uCPE

LAN

Enterprise 2
Branch 2

- Internet or other IP network used as underlay
- Branches are single-homed to the underlay network
- Two different SD-WAN services for two different enterprises

 Public

NOKIA

Use case: SD-WAN overlay on dual Internet underlays

SD-WAN control/orchestration

Control

Control

uCPE

uCPE

LAN

LAN

VXLANoIPSEC overlays
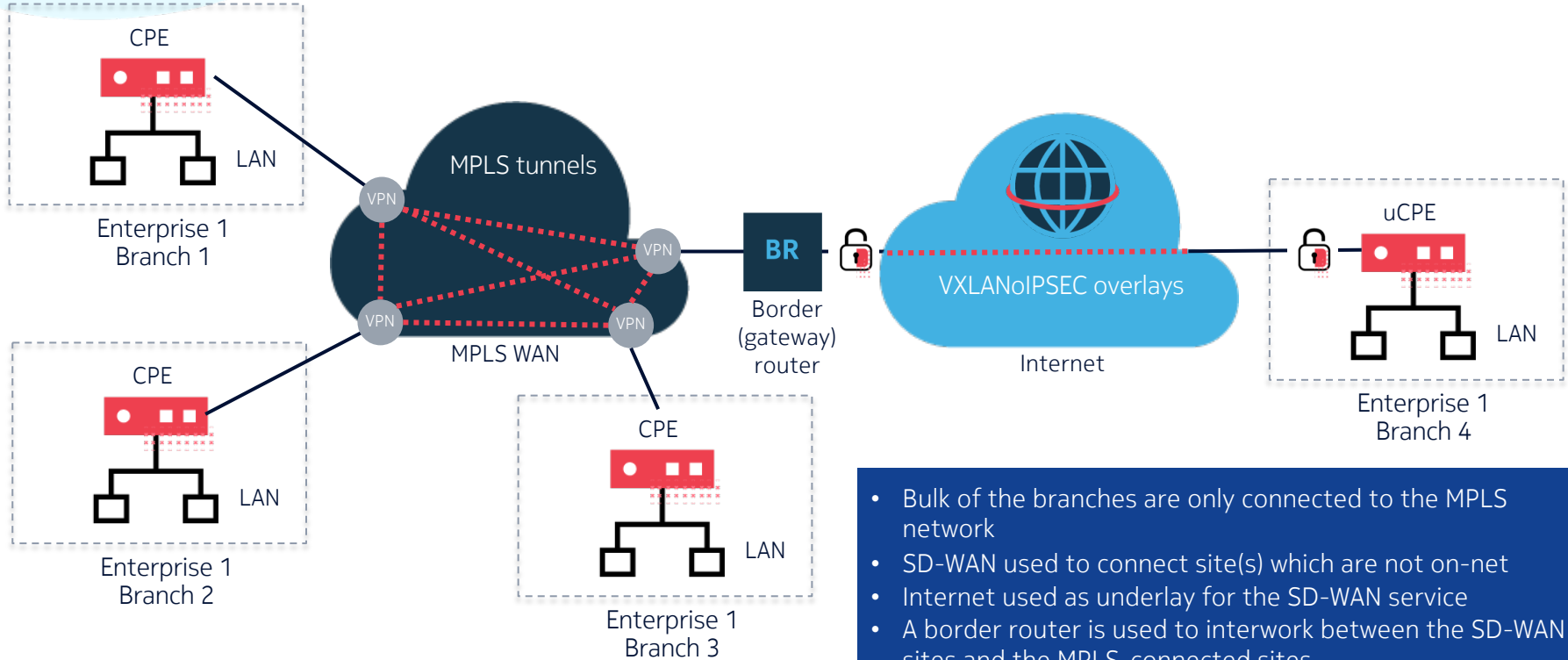
Internet (ISP 1)

Enterprise 1
Branch 1

Enterprise 1
Branch 2

- Internet used as underlay
- Two different ISPs used to provide resiliency
- Branches are dual-homed to the underlay network

VXLANoIPSEC overlays

Internet (ISP 2)

Public

NOKIA

Use case: SD-WAN overlay on Internet and MPLS underlays (hybrid WAN or Internet offload)

SD-WAN control/orchestration

Control

Control

uCPE

uCPE

LAN

LAN

VXLANoIPSEC overlays

Internet (ISP 1)

Enterprise 1
Branch 1

Enterprise 1
Branch 2

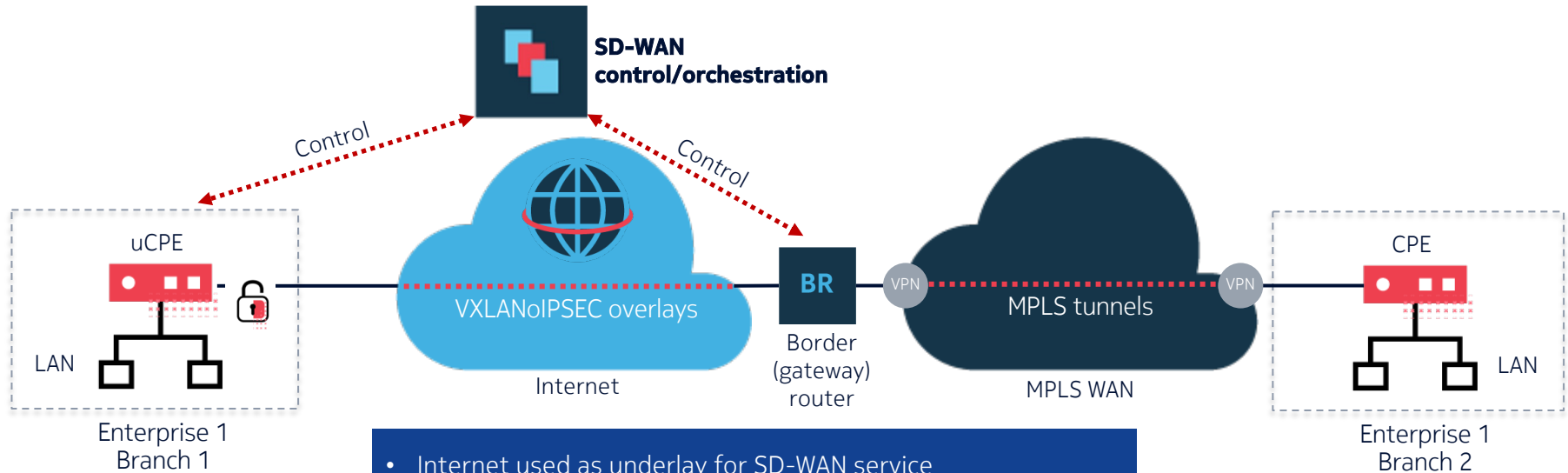VPN

VPN

MPLS tunnels

MPLS WAN

- Both Internet and MPLS networks used as underlay
- Additional resiliency via use of two underlays
- Branches are dual-homed to the two underlay networks
- Traffic selectively sent over each link

© Nokia 2022

Public
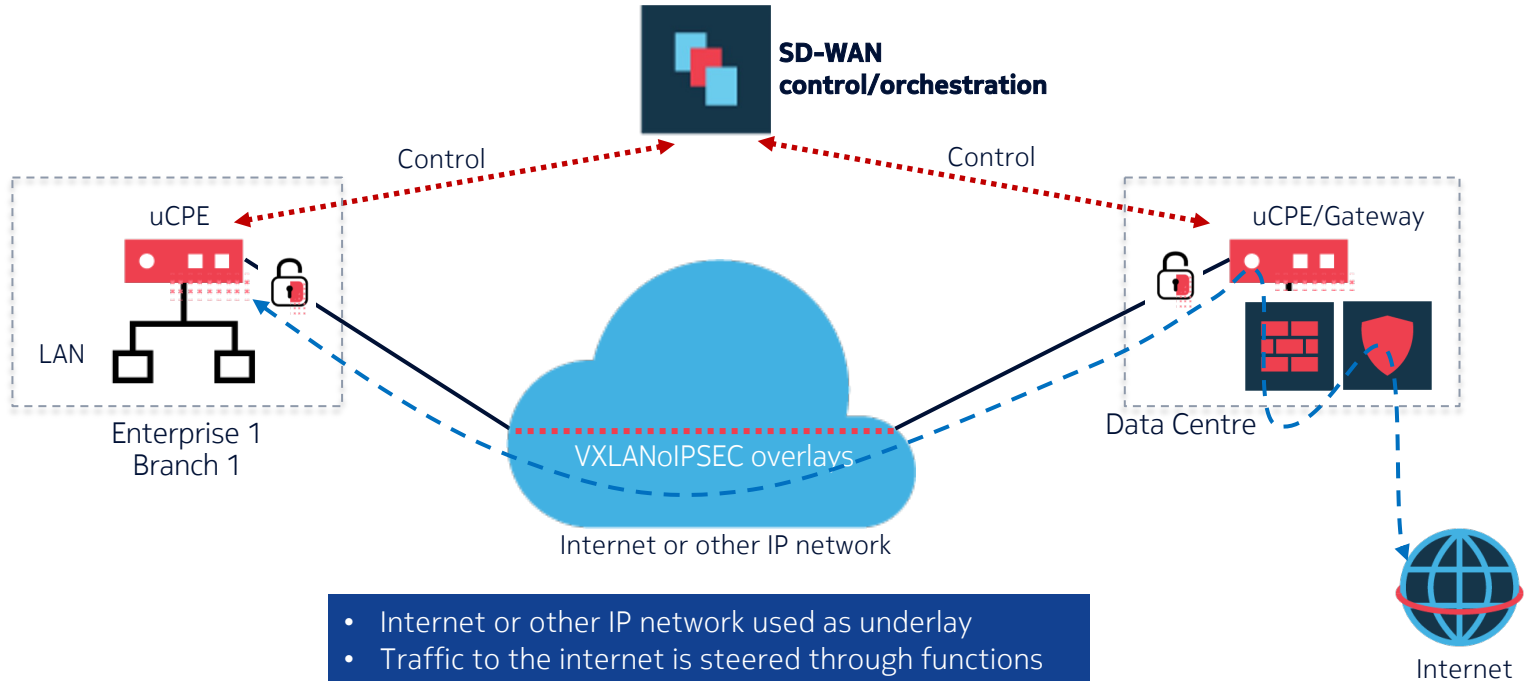
NOKIA

Use case: MPLS VPN offnet extension

- Bulk of the branches are only connected to the MPLS network
- SD-WAN used to connect site(s) which are not on-net
- Internet used as underlay for the SD-WAN service
- A border router is used to interwork between the SD-WAN sites and the MPLS-connected sites

Public

NOKIA

Use case: SD-WAN inter-operating with MPLS VPN

SD-WAN control/orchestration

Control

Control

uCPE

LAN

Enterprise 1
Branch 1

VXLANoIPSEC overlays

Internet

BR

Border
(gateway)
router

VPN

MPLS tunnels

VPN

MPLS WAN

CPE

LAN

Enterprise 1
Branch 2

- Internet used as underlay for SD-WAN service
- SD-WAN Branches are single-homed to the underlay network
- Certain branches are only connected to the MPLS network
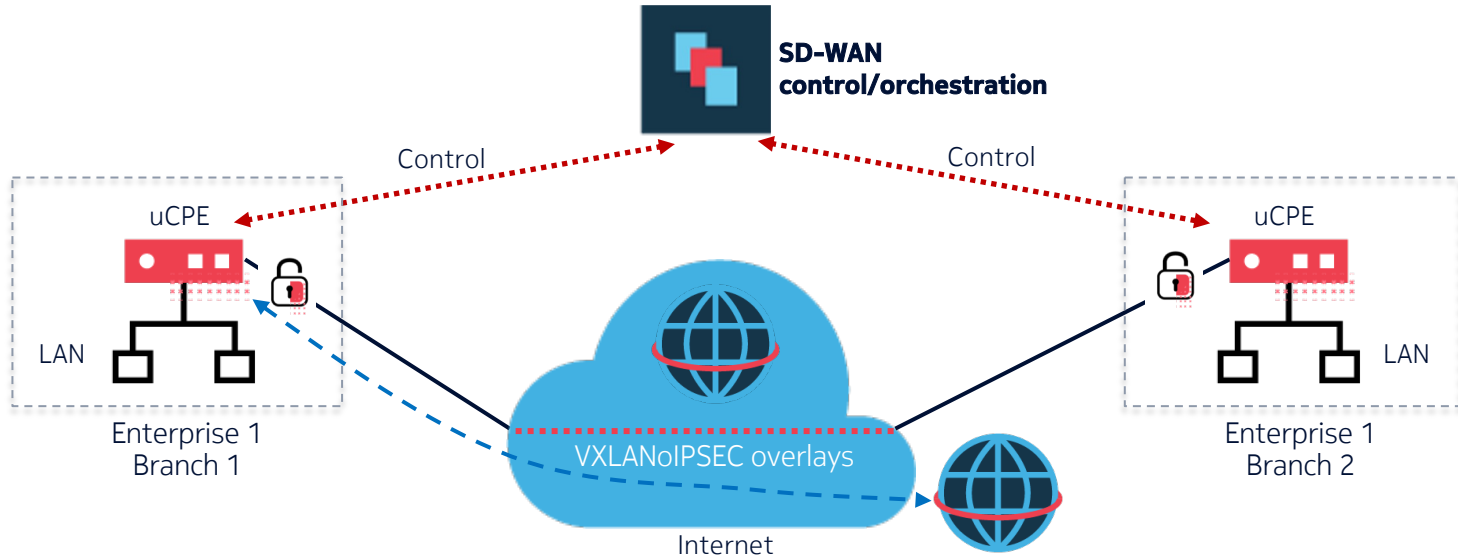- A border router is used to interwork between the SD-WAN service and the MPLS-connected sites

NOKIA

Use case: SD-WAN with service chaining

SD-WAN control/orchestration

Control

Control

uCPE

LAN

Enterprise 1
Branch 1

VXLANoIPSEC overlays

Internet or other IP network

uCPE/Gateway

Data Centre

Internet

- Internet or other IP network used as underlay
- Traffic to the internet is steered through functions offering value-added services (e.g. firewalls/anti-virus) at a central data centre
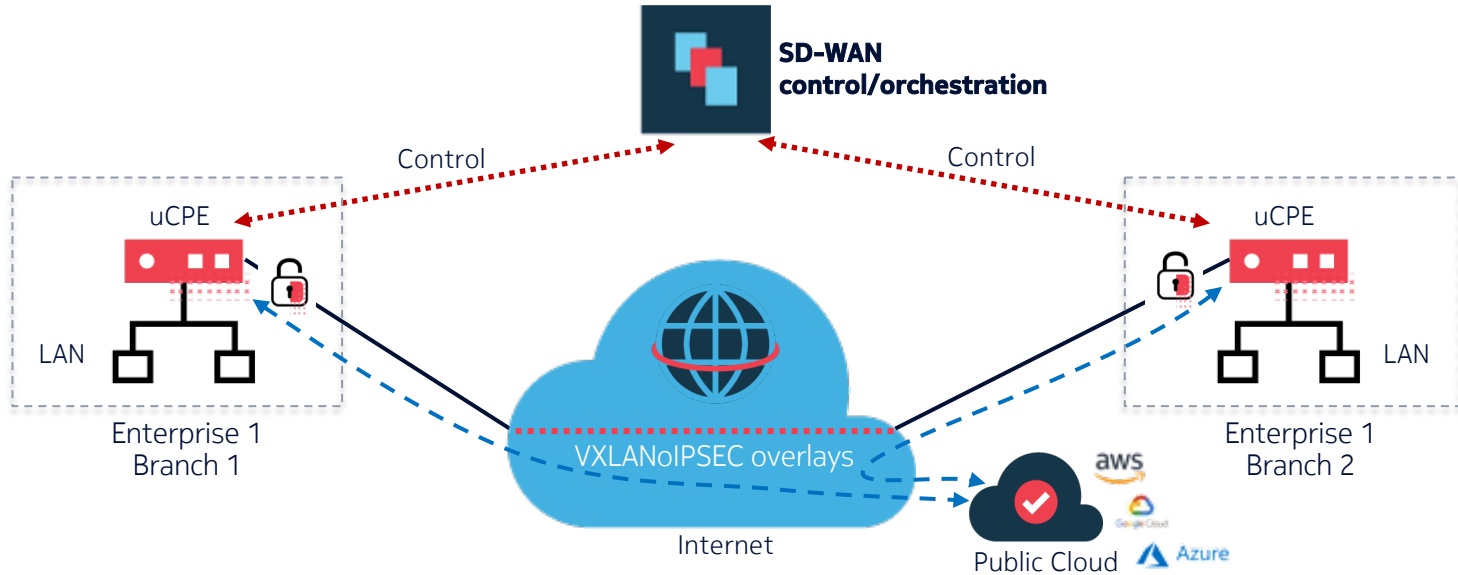
NOKIA

Use case: Local Internet breakout

SD-WAN control/orchestration

Control

Control

uCPE

uCPE

LAN

LAN

Enterprise 1
Branch 1

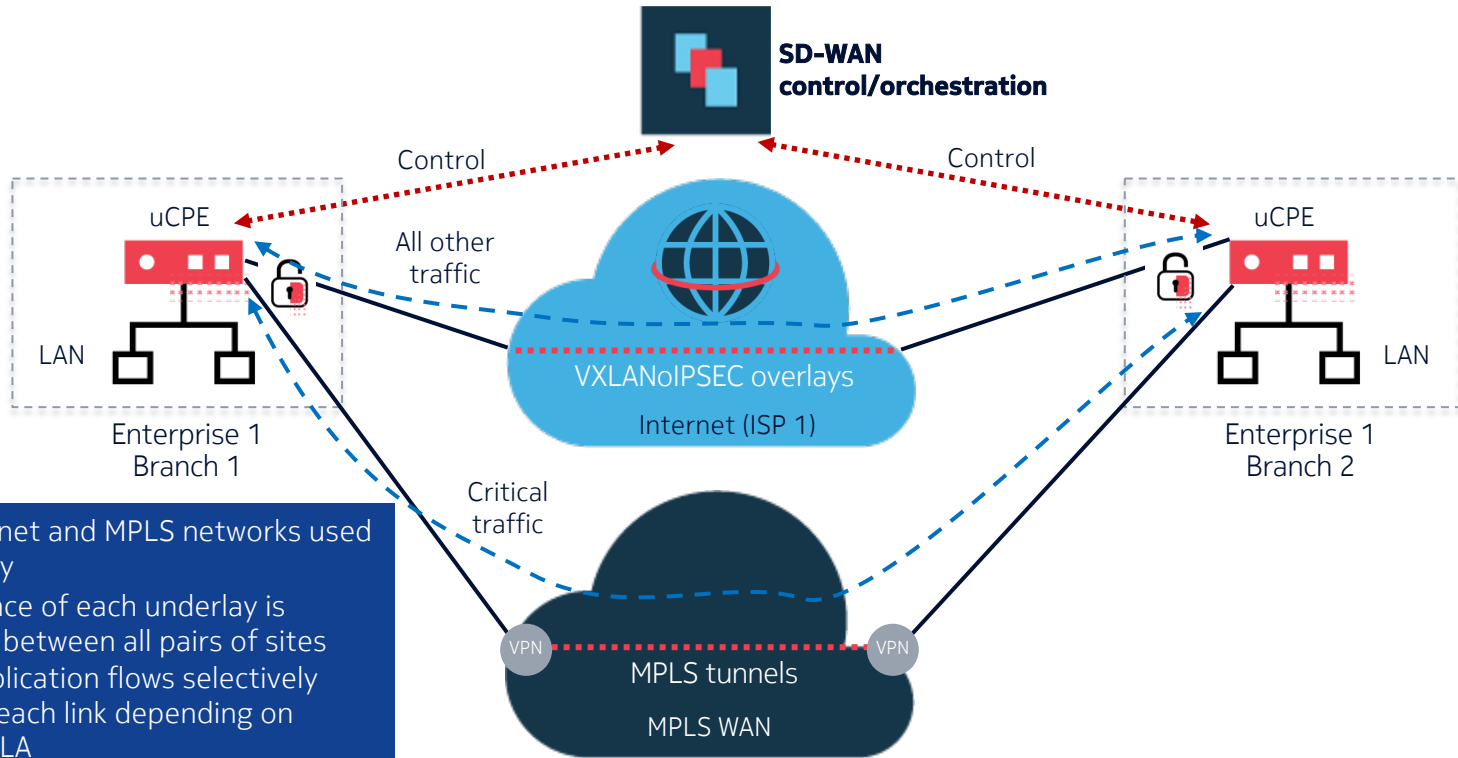VXLANoIPSEC overlays

Enterprise 1
Branch 2

Internet

- Internet used as underlay
- IPsec security is highly desirable when using the public Internet as an underlay
- Branches are single-homed to the underlay network
- Local breakout to the internet; can secure the traffic using on-premise security solution or cloud-based security

Public

NOKIA

Use case: Public cloud access

SD-WAN control/orchestration

Control

Control

uCPE

uCPE

LAN

LAN

Enterprise 1 Branch 1

Enterprise 1 Branch 2

VXLANoIPSEC overlays

Internet

aws

Google Cloud

Public Cloud   Azure

- Internet used as underlay
- IPsec security is highly desirable when using the public Internet as an underlay
- Branches are single-homed to the underlay network
- Local breakout to the internet; can secure the traffic using on-premise security solution or cloud-based security

NOKIA

Use case: Application-aware routing

SD-WAN control/orchestration

Control

Control

uCPE

uCPE

All other traffic

VXLANoIPSEC overlays

Internet (ISP 1)

LAN

LAN

Enterprise 1
Branch 1

Enterprise 1
Branch 2

Critical traffic

VPN

VPN

MPLS tunnels

MPLS WAN

- Both Internet and MPLS networks used as underlay
- Performance of each underlay is measured between all pairs of sites
- Traffic application flows selectively sent over each link depending on required SLA

Public

NOKIA

Inter-operability

© 2022 Nokia

Public

NOKIA

Inter-operability

SD-WAN systems

Most (all) SD-WAN implementations are closed. There is no ability to mix-and-match uCPE and controllers from different vendors without going through gateway devices

uCPE hardware

Most implementations will allow white-box hardware to host SD-WAN uCPE functionality

Service definition

MEF70.1-compliant implementations allow uniformity of externally-visible service behaviour

MPLS network interop

Implementations allow differing degrees of interworking with MPLS networks via border routers/gateways

Data plane

No standard data plane. Variants of VxLAN/IPsec implementations exist

Control plane

No standard control plane. Various implementations exist including OF-TLS.

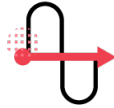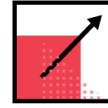NOKIA

Wrap-up

Public

NOKIA

SD-WAN
Key Benefits

Dedicated Network
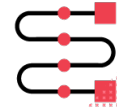A secure and managed private network slice with application aware routing

Powerful Connections
Underpinned by highly resilient access across multiple underlay connections

Highly Agile
Different transport on a per-location basis and scale up bandwidth as needed

Built-in Diversity
For critical sites requiring 100% uptime, multiple always on uplinks can be used simultaneously

Application Networking
Traffic is routed based on application type and importance to your business

Robust Security
Centrally managed, policy-based security framework that simplifies control and minimizes threats for all network end-points

Active Management
24/7 proactive monitoring of the service by SP team and always on customer access via intuitive service portal

Detailed Reporting
Rich business-oriented reporting on WAN usage by application, end-user and device

Public

NOKIA