Stairway to the cloud

9-step blueprint to a best practices private-hybrid cloud for your enterprise

Application note

Executive summary

Nokia's success with telephone companies and mobile operators globally can overshadow its success with large enterprises. In fact, Nokia enjoys the privilege of working with half of the Forbes global top 50 enterprises.

These large enterprises are not only market leaders but also thought leaders in their respective industries and geographies. As a result, Nokia has compiled several successes in private-hybrid clouds — from the initial planning through the complete private-hybrid cloud architecture design, build and implementation.

To transform their findings into a form that can be easily consumed and more readily replicated, Nokia created this application note to highlight a best practices cloud architecture that has proven successful across companies, industries and geographies.

Contents

9-step blueprint to private-hybrid cloud

Overview

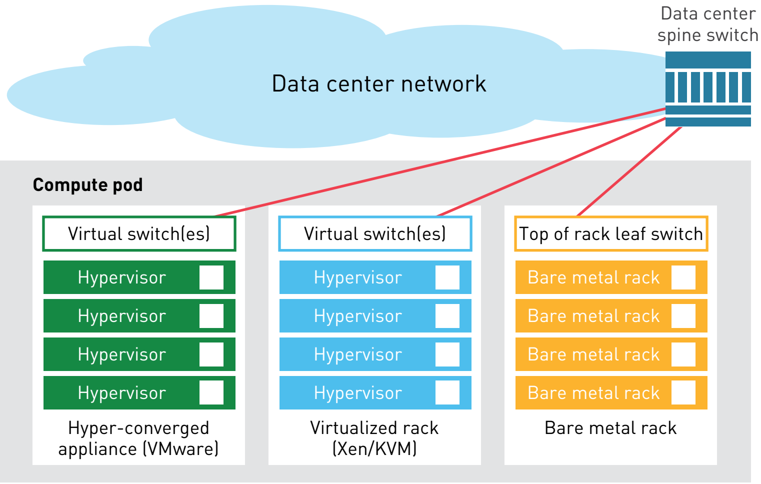
This section outlines not only a practical blueprint for a private-hybrid cloud but also the discrete, manageable steps needed for the final result. In addition to Nokia products, this blueprint leverages open source software, commodity hardware and best-of-breed vendor products. This environment provides not only robust core capabilities but also unmatched flexibility for adaptation to each enterprise's unique needs.

1. Transform your core data center architecture

As evidenced by the growth in alternate compute architectures, such as hyper-converged appliances, the data center is far from static. Today's best practice configuration for power and flexibility relies on compute pods that may be composed of hyper-converged appliances typically running on commercial hypervisor, virtualized racks that can leverage open source hypervisors such as KVM and Xen and bare metal racks for non-virtualized applications.

In parallel, a networking approach typically called "leaf-spine" has evolved. Unlike legacy network architectures that are hierarchical in design, this architecture typically includes "leaf" switches on the top of each rack or a hyper-converged appliance that are interconnected among data center "spine" switches.

Figure 1. Transform your core data center architecture



Leverage flexible compute pods with leaf-spine data center networking.

This architecture provides significant advantages in cloud environments:

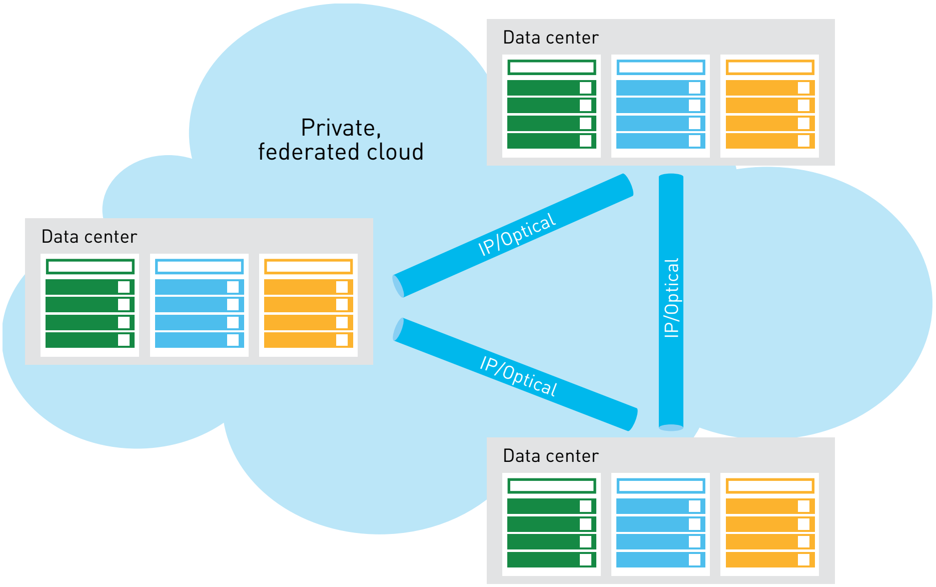
- **High elasticity:** It provides high elasticity within the pod by simplifying the addition/removal of appliances and/or racks as workloads change.
- **Very high scalability:** It also enables very high scalability in terms of the number of pods that can be installed.
- **Optimized performance:** As leaf-spine networking eliminates a tier of switches in legacy networking configurations, traffic flow within the data center is also optimized for performance.

2. Unify (“federate”) data centers into a cloud

This step leverages optical networking technologies to provide a very high speed, high capacity network backbone, ideally over dark fiber. Leveraging this backbone, IP routing products can blend specialized routing hardware with virtualized products to provide the performance, versatility and reliability needed for this cloud. Specifically, Nokia IP products work either standalone or combined with routers from other large network vendors and cover the full range of IP needs — from IP access and aggregation to IP edge, and of course, core routing.

By leveraging this infrastructure, the remote data centers can interoperate with a minimum to no performance penalty. Moreover, by implementing a DCI network approach, these remote data centers can be unified (federated) into a single cloud.

Figure 2. Unify (federate) data centers into a cloud



Unify even remote data centers into a single physical cloud with Data Center Interconnect (DCI).

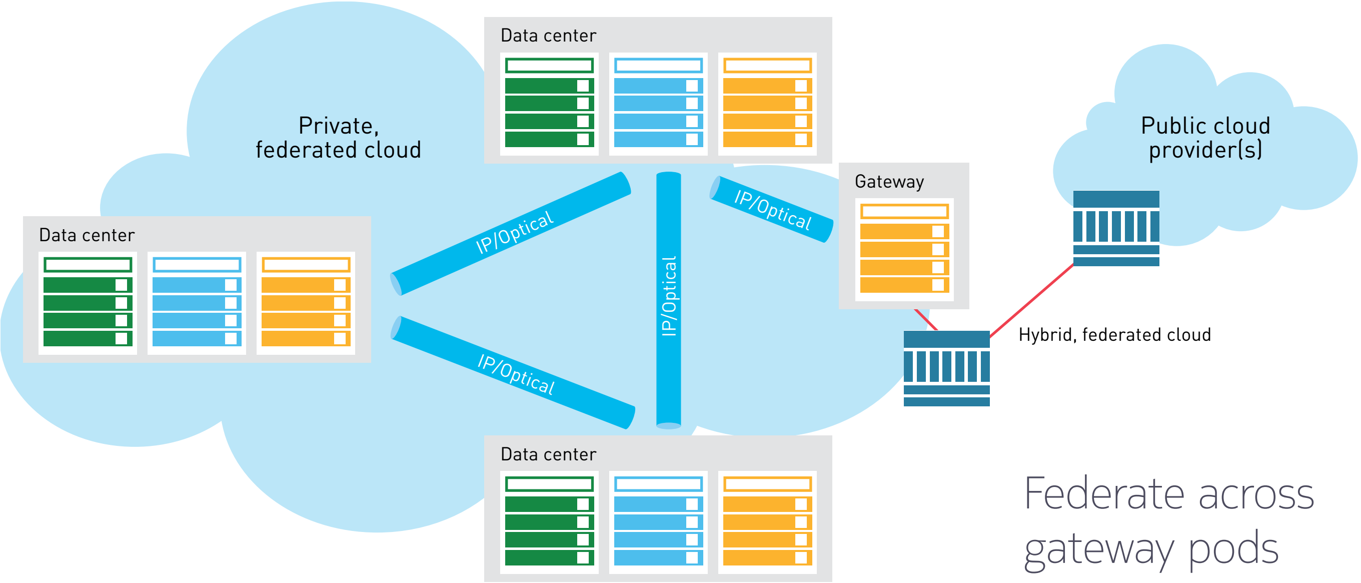
In short, federation enables a number of new capabilities:

- **Application topologies:** Rather than be limited to a single data center, applications can now tier across physical data centers.
- **Workload mobility:** As all applications and data can be accessed from any data center, workload mobility is maximized.
- **Business continuity/disaster recovery:** By eliminating the need to copy data to a remote data center for disaster recovery, both disaster recovery and business continuity limitations of legacy networking are overcome.

3. Extend your capabilities to a public cloud

While each data center can certainly have its own gateway to a public cloud provider, at high volumes having a dedicated gateway pod located as close as possible to the provider's data center can make sense from performance and cost perspectives. By leveraging the network's federation capabilities, the public cloud can be an extension of the private cloud to a true hybrid cloud architecture.

Figure 3. Extend your capabilities to a public cloud



Federate across gateway pods to public cloud provider(s) for hybrid cloud.

Adding to the federated cloud benefits discussed in the previous section:

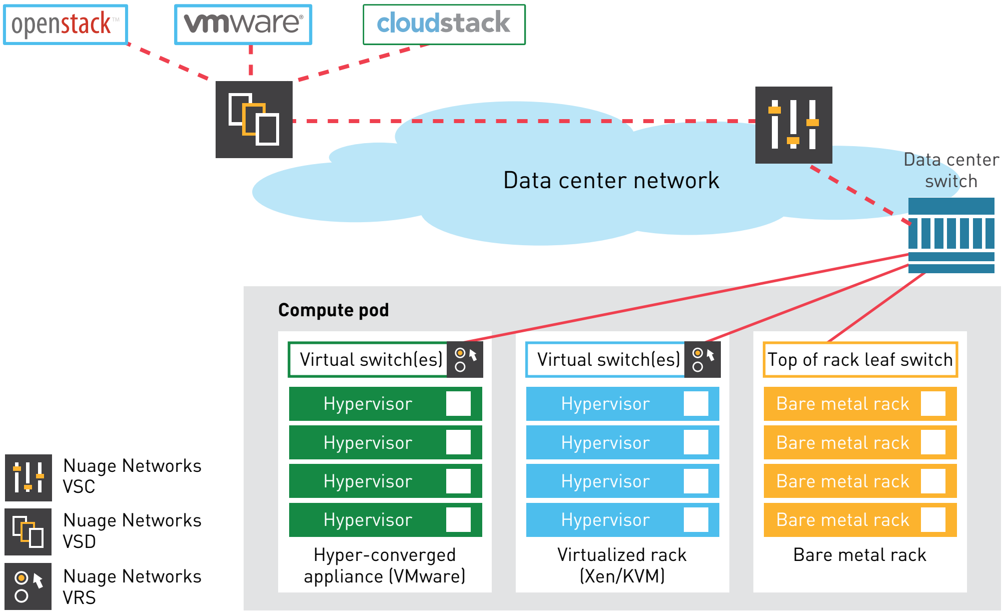
- **Scalability:** The enterprise can now leverage the public cloud for day-to-day department-level needs and burst scalability (for workloads such as big data analysis).
- **Cost:** The cost advantages of the public cloud can be realized where appropriate.
- **Flexibility:** The public cloud's flexibility in terms of supporting a wide range of environments can be leveraged for tasks such as quality assurance.

4. Overlay for full end-to-end programmability

Being able to physically communicate through federation is a necessary prerequisite but is not the complete solution for full end-to-end programmability for the private-hybrid cloud. To provide software controls that encompass both spinning up new virtualized and bare metal resources, enable workload mobility, provide full automation, and ensure high security, two key technologies are needed — one or more cloud platforms and a software-defined networking (SDN) platform. To transform existing legacy architecture without creating a separate cloud or upgrading a good percentage of the infrastructure, an overlay SDN is ideal.

For this step, any cloud platform (OpenStack, CloudStack, and/or proprietary releases from commercial vendors) can provide automated orchestration across server, networking and storage layers. Nuage Networks Virtualized Services Platform (VSP) overlays even the most complex multi-data center environment with multiple virtualization hypervisors and a multivendor network hardware environment without requiring forklift upgrades. Composed of three major components — Nuage Networks Virtualized Services Directory (VSD), Nuage Networks Virtualized Services Controller (VSC), and Nuage Networks Virtual Routing and Switching (VRS), Nuage Networks VSP virtualizes even bare metal resources such as database application servers and hyper-converged appliances. With consistent virtualization across the environment, Nuage Networks VSP can deliver end-to-end programmability from the cloud platform throughout the network and everywhere within the data center.

Figure 4. Overlay for full end-to-end programmability



Implement cloud and SDN platforms.

This approach adds and streamlines important fundamental cloud operations:

- **Full programmability:** With this approach, all operations of the private-hybrid cloud can be programmed — from provisioning to mobilizing to de-provisioning workloads and assets.
- **Full automation:** By leveraging application programming interfaces (APIs) and portals provided by the cloud platform, both self-service and internal operations can be fully automated.
- **Workload mobility, both virtualized and bare metal:** By leveraging programmability and automation, workloads are fully mobile anywhere within the cloud.

5. Provide services from any branch or location

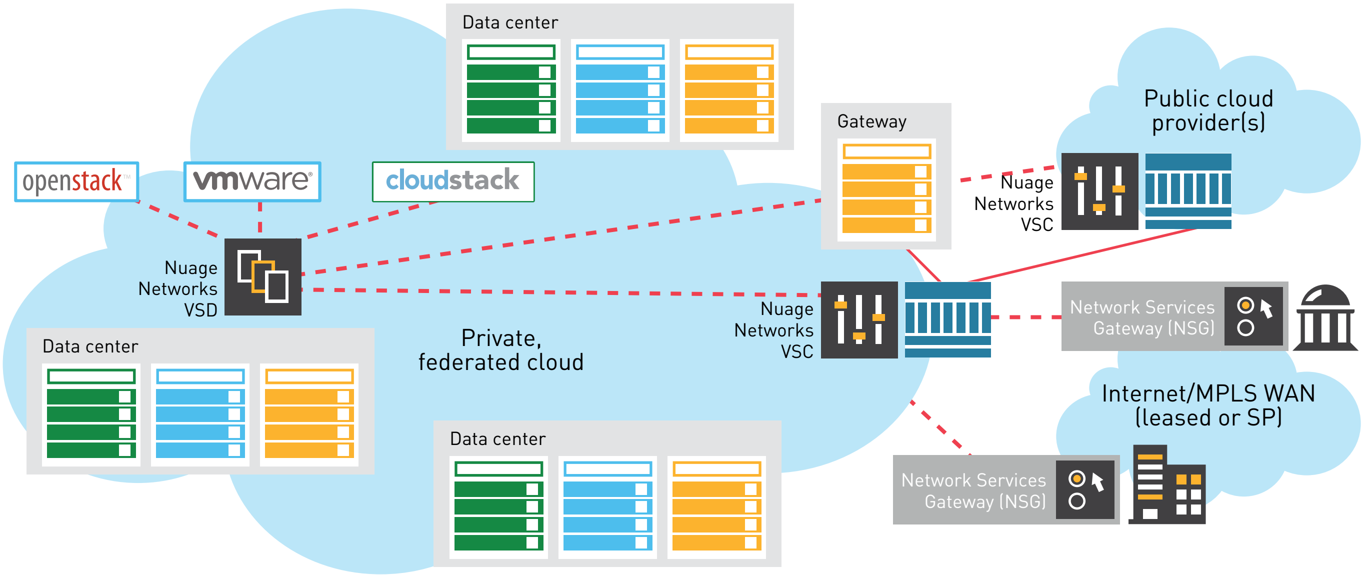
While cloud architectures are typically Internet Protocol (IP) based, the networks that connect most remote branches and warehouses are typically based on a wide area network (WAN) that runs on a different protocol, most commonly multiprotocol label switching (MPLS) with a completely separate hardware and management infrastructure. Another complication usually arises in that the “last mile” connecting the branch can be any mix of older copper telephone lines, fiber and dark fiber.

Nokia’s Fixed Access portfolio provides branch connectivity over a range of IP, WAN and last-mile technologies. Further, older WAN technologies can be converted to IP with the addition of a converter for seamless integration into the cloud network.

By taking advantage of this unified connectivity, Nuage Networks Virtualized Network Services (VNS) ensure that networking to the branch using an internet or an MPLS connection is managed consistently with the rest of the cloud. And by leveraging an on-premise physical or virtual appliance, the network services gateway (NSG), endpoint provisioning is not only efficient but also extremely cost effective.

Provide access from every branch — around the block or around the globe — across any network.

Figure 5. Provide services from any branch or location



New enabled capabilities have features such as:

- **Every network point is now cloud-ready:** Every remote point — whether in a remote office, branch, warehouse or even a parking lot — can now become part of the private-hybrid cloud.
- **End-to-end programmability and automation:** All the capabilities described above in terms of programmability and automation are available all the way out to the office, branch or warehouse.
- **Independence of the physical network:** This approach widens connectivity options beyond just MPLS to include IP, to operate consistently whether the line is leased or service provider-provided, and to also work across several last-mile connection types.

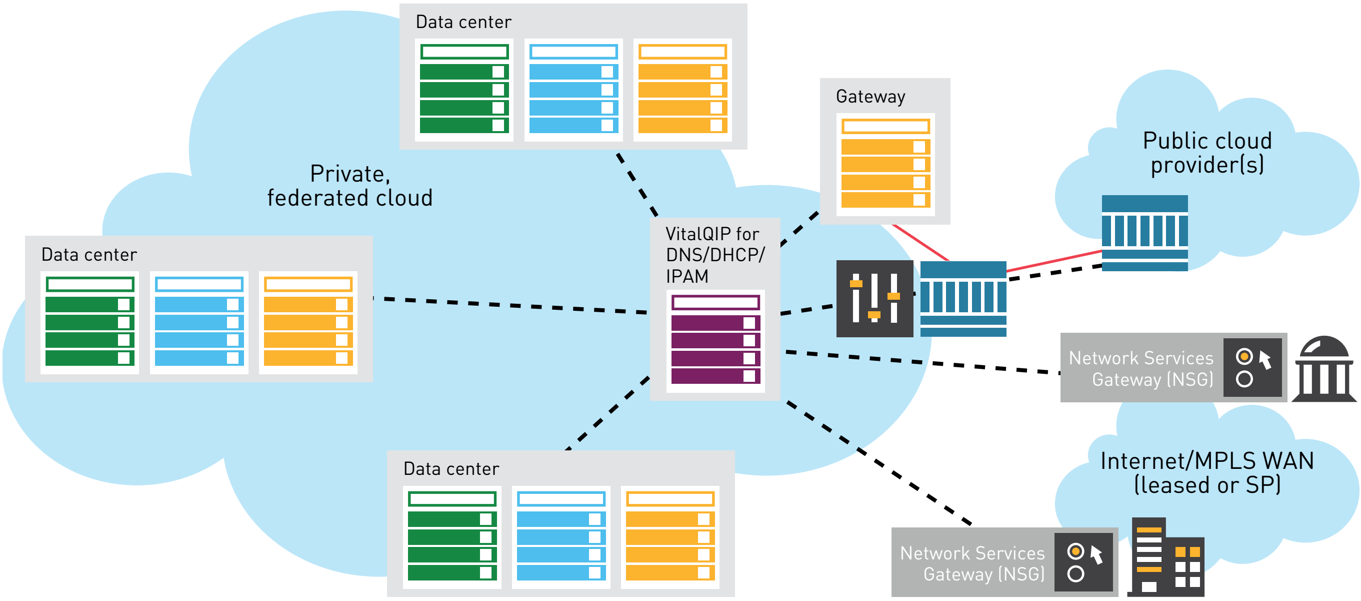
6. Enable fast and reliable connections everywhere

Network services – Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM) — commonly abbreviated as DDI — are the unsung heroes of a private cloud. As literally every request from each web server page to an application call typically invokes DNS, performance and reliability issues are both pervasive throughout the cloud and difficult to detect. In a similar manner, workload mobility involves getting a new IP address assigned dynamically upon request through DHCP as assigned by the IPAM system.

Nokia VitalQIP provides highly reliable and scalable DDI network services that are trusted by some of the largest enterprises, including financial institutions and government agencies in the world. VitalQIP also enables performance and reliability monitoring and alerting from a variety of vendor-supplied and open source tools.

Provide the right resources to data centers, application tiers, services and devices.

Figure 6. Enable fast and reliable connections everywhere


Data center
Gateway
Private, federated cloud
Public cloud provider(s)
Data center
VitalQIP for DNS/DHCP/IPAM
Network Services Gateway (NSG)
Internet/MPLS WAN (leased or SP)
Data center
Network Services Gateway (NSG)

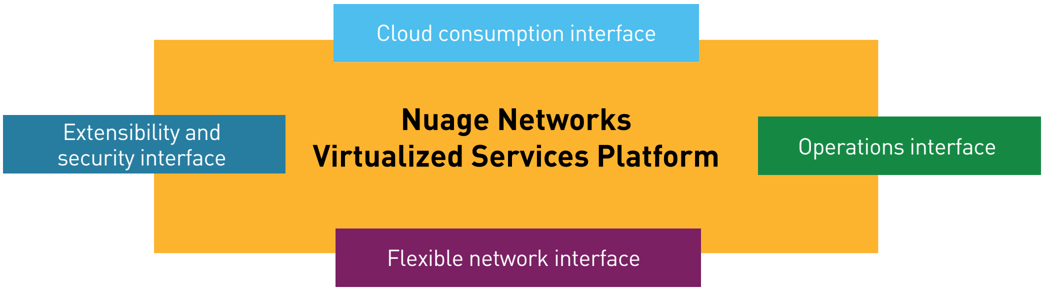
While siloed DDI network services can be found in servers, network hardware and other platforms, a unified DDI platform that operates throughout the private-hybrid cloud has strong advantages:

- **Resource optimization:** A centralized DDI platform helps optimize both physical resources (IP ports) and operational resources (via enabling self-service approaches).
- **Security:** Because many hacker, malware and denial of service attacks leverage DNS, having a unified DDI platform is vital to protecting the enterprise.
- **Performance:** Many network performance issues arise from poorly configured DNS settings, yet are very difficult to detect.

7. Provide best-of-breed options to your developers

Most enterprises have found that migrating complex legacy environments to a leading-edge cloud environment is much easier and provides more powerful capabilities when vendor lock-in is broken in favor of best-of-breed flexibility. Leveraging the Nuage Networks VSP rich interfaces, developers can not only ensure that all current environments but also exciting, leading-edge development environments, such as Kubernetes and Mesos, are supported in the private cloud.

Figure 7. Provide best-of-breed options to your developers


Cloud consumption interface
Extensibility and security interface
Nuage Networks Virtualized Services Platform
Operations interface
Flexible network interface

Provide your developers with leading-edge development environments and flexibility in vendor offerings.

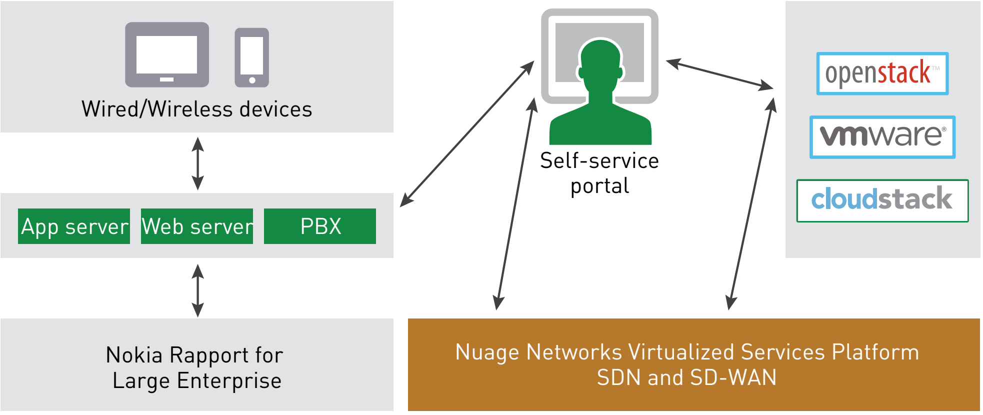
Leveraging these rich interfaces in the private-hybrid cloud provides new capabilities:

- **Best-of-breed tools in every category:** With Nuage Networks VSP, best-of-breed tools, including industry-leading vendor appliances and platforms, DevOps tools and open source, can be fully leveraged. For example, the platform supports hypervisors, docker containers and bare metal side-by-side in the same data center.
- **Full range of vendor solutions:** Best-of-breed solutions for every network task, a full range of networking hardware, performance accelerators and more can be implemented in the cloud.
- **Security extensions:** As desired, literally every packet can be inspected by one or more external security offerings.

8. Expand customer communications and services options

Having a separate communications silo for mobile, voice, video and messaging hinders the ability of enterprise to communicate consistently with its customers across all channels while also increasing costs. By enabling a private cloud-based communications and collaboration framework, applications can have communications functions quickly embedded, which means enterprises can dramatically expand both customer communications and services options, such as providing self-service portals.

Figure 8. Expand customer communications and services options


Wired/Wireless devices
App server
Web server
PBX
Nokia Rapport for Large Enterprise
Self-service portal
openstack
vmware
cloudstack
Nuage Networks Virtualized Services Platform SDN and SD-WAN

Enable mobile and telephony-based applications along with self-service capabilities.

By integrating a communications and collaboration framework into the private cloud, new capabilities arise:

- **Customer satisfaction:** Can leverage multichannel communications capabilities to serve customers independently from the platform that they utilize (for example, laptop, pad, mobile or landline), as well as enable customers to self-serve for even complex requests.
- **Globalization:** By adding the flexibility of connecting customers to the right support team for their needs, including preferred language, globalization initiatives move from possible to feasible.
- **Adaptability:** Because mobile applications can be quickly updated to handle, for example, a response to a natural disaster, an urgent product recall and more, adaptability is maximized.

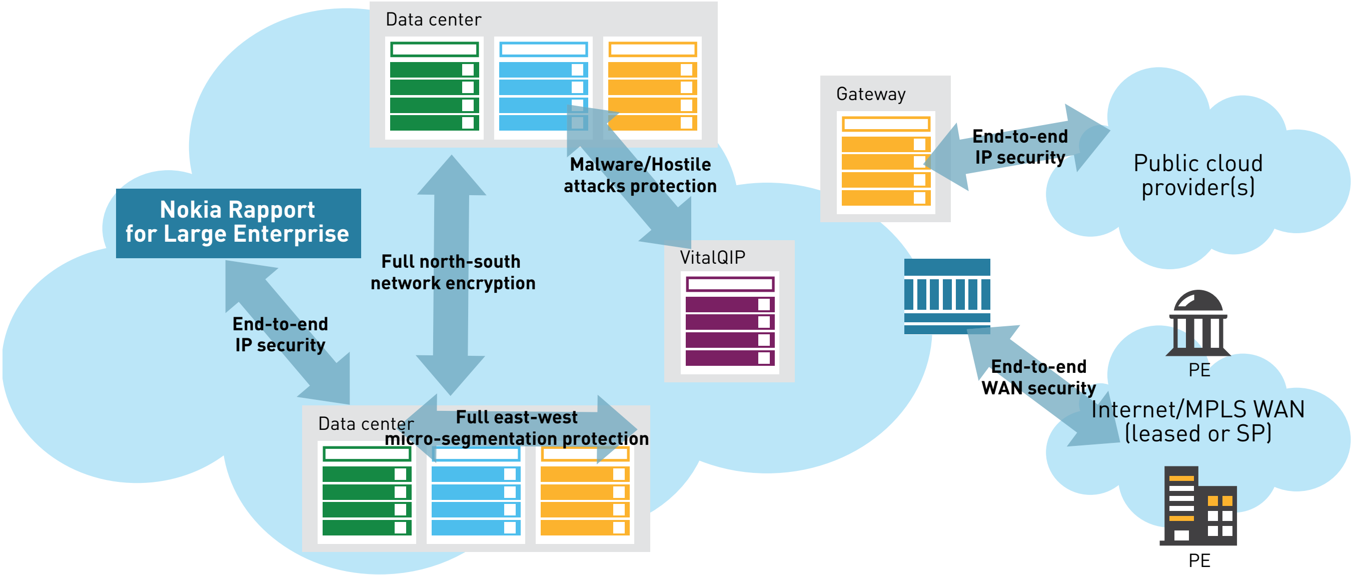
9. Audit security built into previous steps and supplement

All of the infrastructure elements discussed earlier include a range of security protection measures ranging from physical encryption of data in transit to protect against a variety of internal and external threats, protection of virtualized communications within a hypervisor via a micro-segmentation approach to protect against internal threats, and protection against malware and other largely external threats. Perhaps most importantly, the Nuage Networks VSP policy-based security also prevents a real-world security issue — inadvertent security exposures due to manual error.

However, it's likely that application-level security will need to be designed or adapted for each enterprise's private cloud environment. Using a wide range of APIs including REST and other interfaces, this application layer security can be easily integrated into the cloud.

Evaluate and address your unique application layer protection needs.

Figure 9. Audit security built into previous steps and supplement


Data center
Malware/Hostile attacks protection
Gateway
End-to-end IP security
Public cloud provider(s)
Nokia Rapport for Large Enterprise
Full north-south network encryption
VitalQIP
End-to-end IP security
End-to-end WAN security
PE
Internet/MPLS WAN (leased or SP)
Data center
Full east-west micro-segmentation protection
PE

By integrating application layer security with that of the infrastructure, several advantages can be realized:

- **Security gaps are minimized:** Not only are gaps between the infrastructure and application layers minimized, but timing gaps due to manual processes are also minimized or eliminated.
- **Best of breed at application layer:** With integration capabilities, the best-of-breed approach at the application layer can be selected.
- **End-to-end automation:** With this approach, an end-to-end automation of security can be created.

Summary

Key points

Building any new and complex architecture, such as a private-hybrid cloud, can be a daunting task. However, if the task is broken down into specific, realizable steps, then the construction process can be methodically executed yet minimize risk overall as each step is relatively self-contained.

While each enterprise environment has unique considerations, Nokia believes that this private cloud architecture provides a solid baseline foundation that can be tailored as needed. Now it is hoped that enterprises utilize this application note to smooth their path to the cloud and that they will also contribute their knowledge to this architecture over time.

Learning more

Nokia provides cloud solutions to large enterprises overall as well as targeted approaches for specific verticals. To learn more, please point your browser to: https://networks.nokia.com/large-enterprises.

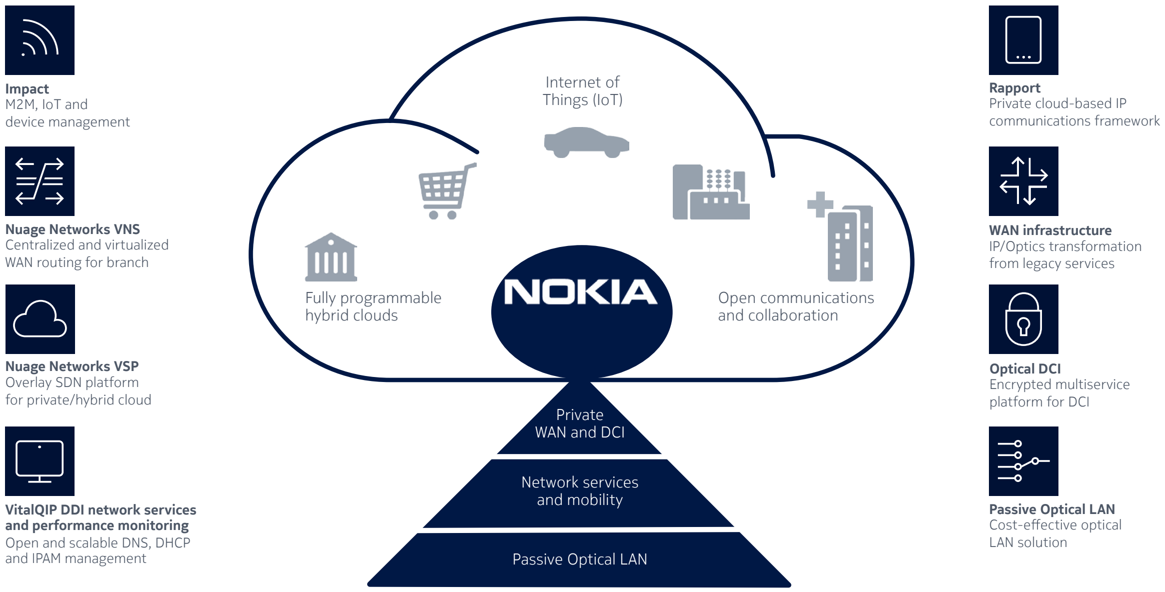
Nokia in the enterprise

What we bring to the enterprise

Nokia’s success with telephone companies and mobile operators globally can overshadow its success with large enterprises. In fact, Nokia enjoys the privilege of working with half of the Forbes global top 50 enterprises.

As shown below, Nokia provides the fundamental infrastructure components needed to build a variety of robust cloud architectures that support a diverse set of enterprise applications and platforms. Building on a foundation of Passive Optical LAN (POL) components and a broad array of network services and IP routing and optical transport hardware, a scalable, reliable and secure private-hybrid cloud can be constructed.

Figure 10. Private-hydrid clouds for the global enterprise



Impact
M2M, IoT and device management
Nuage Networks VNS
Centralized and virtualized WAN routing for branch
Nuage Networks VSP
Overlay SDN platform for private/hybrid cloud
VitalQIP DDI network services and performance monitoring
Open and scalable DNS, DHCP and IPAM management
Internet of Things (IoT)
Fully programmable hybrid clouds
NOKIA
Open communications and collaboration
Private WAN and DCI
Network services and mobility
Passive Optical LAN
Rapport
Private cloud-based IP communications framework
WAN infrastructure
IP/Optics transformation from legacy services
Optical DCI
Encrypted multiservice platform for DCI
Passive Optical LAN
Cost-effective optical LAN solution

Layering in the capabilities of SDN and software-defined WAN (SD-WAN) and DDI network services yields the ability to create fully programmable hybrid clouds. Adding in an IP communications framework removes silos and vendor lock-in for open communications and collaboration across the organization. Finally, with an Internet of Things and device management platform, true IoT clouds can be built.

While these capabilities apply to all large enterprises, Nokia is focusing on a few key verticals to accelerate its success. Currently, financial services, healthcare, automotive and retail are verticals that are widely benefiting from Nokia’s products.

Acronyms

API	application programming interface
DCI	Data Center Interconnect
DDI	DNS/DHCP/IPAM
DevOps	development and operations
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
IP	Internet Protocol
IPAM	Internet Protocol Address Management
KVM	kernel-based virtual machine
LAN	local area network
MPLS	multiprotocol label switching
NSG	network services gateway
PE	premise equipment
POL	Passive Optical LAN
REST	representational state transfer
SDN	software-defined networking
SD-WAN	software-defined WAN
VNS	Virtualized Network Services
VRS	Virtual Routing and Switching
VSC	Virtualized Services Controller
VSD	Virtualized Services Directory
VSP	Virtualized Services Platform
WAN	wide area network

NOKIA

About Nokia

Nokia is a global leader innovating the technologies at the heart of our connected world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience.

For more information on our solutions for large enterprises, visit https://networks.nokia.com/large-enterprises.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1704010120EN (May)