Building a private network for digital transformation and enterprise cloud

As enterprises embrace social, mobility, analytics, the Internet of Things (IoT) and move to cloud-based IT models, they need more flexible and agile networks. Many are re-evaluating their networking needs, particularly for wide area networks (WANs) that connect their main sites, data centers, as well as remote locations.

Enterprises also need more efficient and cost-effective solutions to connect smaller branch sites, in addition to securing internet and mobile connectivity to enable access for employees, partners, customers and IoT devices.

This white paper outlines how large enterprises can build a private WAN to support their digital transformation and cloud IT strategies. It shows how new networking technologies can help enterprises to implement more agile, flexible, and cost-efficient networking solutions in the cloud era.
Introduction

Enterprises are evolving to leverage the latest cloud and digital technologies, such as social, mobile, analytics and the Internet of Things (IoT). This is to support new operational models so that employees, partners, and customers can connect, communicate, and collaborate more effectively.

Delivering better operational models requires real-time information and communications for a more collaborative, proactive business. It also requires an adaptive IT infrastructure capable of responding quickly to changing user needs. Key success factors for delivering this change are innovative network and cloud technologies that accelerate innovation and streamline workflows while facilitating anywhere, anytime access to data and knowledge that is critical to business success.

Many enterprises use wide area network (WAN) services to connect their headquarters, data centers, offices, factories, warehouses and branch sites. Most are attracted by the benefits of virtualized IT and cloud services, including scalability, agility, and cost efficiency. Traditional network services are costly, slow to provision, and lack both the scalability and bandwidth required to support new enterprise applications. On top of that, virtualized IT and cloud services may not offer the data security, control, and sovereignty needed to ensure the confidentiality of sensitive business data.

With the advent of the cloud, enterprises are being challenged to determine the best approach for their networking needs. Many are turning to private networks and private clouds. This will let them leverage the latest technologies in order to transform their IT infrastructure, as well as support new enterprise applications and services. Enterprises also need to prepare their IT infrastructure to support new data security and compliance requirements, such as the EU’s General Data Protection Regulation (GDPR).

As illustrated in Figure 1, a scalable, secure, and reliable private network that connects major enterprise sites and data centers, can be augmented with new and flexible solutions to connect smaller enterprise sites. Secure internet and mobile applications can also be used to connect employees, partners, customers and IoT devices, enabling greater communication and interaction.

Figure 1. Private network supporting enterprise digital transformation and the cloud
A private network enables enterprises to implement a secure private cloud that runs critical business applications in house, protects confidential data, and helps meet regulatory and compliance requirements. Moreover, a private cloud can be augmented with virtual private and hybrid clouds to run non-critical workloads and applications. That’s important because this combination improves workload distribution, enhances IT responsiveness, and increases efficiency while securing enterprise applications and data.

Private networks for digital technologies and the enterprise cloud

Many enterprises use traditional network services, such as leased lines and virtual private networks (VPNs), to connect their sites. The challenge, though, is that, while managed network services are appropriate for providing connectivity to remote sites, they are too static. They also lack the ability to easily adapt to digital technologies and the cloud, which require scalability, flexibility, and agility. Indeed, scaling bandwidth, provisioning services, managing multiple network connections, as well as ensuring optimal application performance, are all costing more. As a result, many organizations are reconsidering their network needs, particularly for digital technologies and the cloud.

Moreover, traditional network services are also expensive, inflexible, and notoriously slow to provision for smaller enterprise sites. This is particularly the case where network changes are frequent and staff have little or no networking expertise. Connecting new sites, launching new services, or making changes can take weeks or even months. What’s more, once a request is made, the process is often opaque, making problem resolution difficult. For enterprises using traditional network services to connect hundreds of small sites, the process can be complex and frustrating.

Building a private network can be a strategic investment. The network needs to combine a WAN backbone in order to connect main sites and data centers with more agile, flexible, cost-efficient, and software-defined WAN (SD-WAN) solutions in order to connect smaller enterprise sites. The good news is that the cost of building the backbone WAN to connect main sites can be offset by the lower cost of SD-WAN solutions to connect smaller sites. This can dramatically reduce overall networking costs.

By enabling the enterprise to consolidate multiple data centers and move to a more efficient cloud IT model, a private network can also support the enterprise’s IT and cloud strategy. For example, a private network can support a private cloud that provides scalability, control, and security for critical business applications. It can also support access to virtual private and hybrid cloud services that deliver the capacity, agility, and flexibility needed for less critical and on-demand applications. The savings achieved through consolidating and virtualizing multiple data centers and moving to a more agile, flexible cloud IT model enables the enterprise to further offset the cost of building the private network.

Network requirements to support digital technologies and enterprise cloud

Although many enterprises are implementing digital transformation and building a private cloud, most underestimate the impact on the network, particularly the WAN. For similar reasons, most are not yet ready to leverage hybrid clouds.
To achieve the benefits of the cloud, enterprise network infrastructure needs to be re-architected and upgraded to implement the necessary management and orchestration layers. Some of the key network requirements for digital technologies and the integration of private and hybrid cloud infrastructure include the following:

• Scalable, flexible, reliable bandwidth: Different enterprise applications require different bandwidths. A private WAN must be able to scale bandwidth up or down across multiple network domains, depending on individual application requirements. The network must also have the resilience and reliability to avoid service outages and interruptions with automatic failover mechanisms and real-time backup and recovery of critical business data without disrupting normal operational traffic.

• Agile, dynamic provisioning: There must be effective ways to ramp network resources up or down, as required. That includes the quick and dynamic orchestration of network resources across multiple enterprise sites — and potentially across multiple clouds and cloud providers.

• Flexible service level agreements (SLAs): SLAs should cover both planned and unplanned bandwidth increases and decreases. This is equally important when providing planned backups of business data or on-demand bandwidth for enterprise applications. It is also critical when reacting to unplanned events, such as link failures and network outages. SLAs should also cover enterprise application requirements, such as availability and QoS, as well as normal network metrics, such as uptime and latency.

• Multi-layer security: Security practices must ensure the confidentiality, sovereignty, integrity and availability of sensitive business data flowing across the network between different enterprise sites and cloud types. Methods should include network-based encryption and, in some instances, encryption at multiple network layers. Encryption should be controlled through centralized security management and strong user authentication that provides role-specific access to configuration and monitoring capabilities.

• Traffic engineering: Specific enterprise applications, services, and data need access to network resources, such as bandwidth and QoS. This ensures the right priority, as well as resiliency and failover mechanisms in the event of link or network failure.

• Advanced network services: A private WAN must support advanced network services to enable convergence of new network services, (such as flexible bandwidth), in addition to legacy network services, (such as leased lines), on a common IP infrastructure. Advanced network services can include network address translation (NAT), deep packet inspection (DPI), network encryption, as well as service-aware management to monitor, report, and troubleshoot at the service level.

• Application-aware networking: Enterprise and cloud-based applications use the network in different ways depending on the type of service, data, and user interface. As a result, the private WAN needs to be application-aware, adjusting automatically to application type and new cloud usage patterns with no compromise on application scale or performance.

• Real-time analytics and reporting: Enterprises must be able to analyze network, service, and application performance easily and quickly, in depth and in real time. Real-time analytics and reporting shows how the network is performing so that resources can be adjusted to changing user demands. It also helps identify potential network and security issues before they become critical and impact operational continuity and efficiency.
• Mobility and BYOD: In response to the challenges of “bring your own device” (BYOD) policies, enterprises should consider “sandboxing” (isolating and testing) mobile cloud applications. This is to prevent malware from infiltrating the enterprise environment. Real-time network analytics and reporting and network behavioural analysis can also help to identify potential security issues.

• Finally, enterprises need to consider network operations and support. They need personnel with both IT and network expertise, whether they are enterprise personnel or third-party support personnel from a service provider or specialist support organization.

Re-architecting the enterprise network for digital technologies and the cloud

When building a private network to support digital transformation and take advantage of the cloud, it’s important to start with a high-performance WAN backbone between the main enterprise and data center sites. As illustrated in Figure 2, a backbone that combines optical networking and IP/MPLS provides the core elements of scalability, reliability, quality of service and security — in addition to including the intelligence to separate multiple services and applications with differing requirements.

Existing managed VPN services can be used to connect regional and international sites where continued use of these services makes sense. Innovative solutions, such as software-defined WAN (SD-WAN) and software-defined networking (SDN), can be introduced. SD-WAN enables the connection of smaller remote enterprise sites to the private cloud more easily and at lower cost. SDN enables data center virtualization, hybrid cloud connectivity, and network optimization and automation. Furthermore, secure internet connections and mobile applications can enable employees, partners, customers and IoT devices to connect to the private WAN using secure gateways. However, the introduction of these new technologies requires the re-architecting of existing enterprise WANs. This will enable support of digital technologies, better integration with the cloud, as well as more agile and flexible connectivity models.

Figure 2. Re-architecting the enterprise network to support digital technologies and the cloud
The role of SDN and network virtualization in enterprise networks

SDN helps to automatically allocate network resources and balance workloads in and across multiple data centers and the cloud. SDN is a more dynamic, manageable, cost-effective and adaptable network architecture that is better suited to today's virtualized data centers. SDN decouples the network control and forwarding functions, and abstracts the underlying network infrastructure from the applications and services that use it. It makes networks programmable and simplifies network control, making it more agile and responsive. With additional automation, SDN also creates opportunities for policy-driven supervision.

SDN also has a role in the WAN, which is becoming more virtualized. Consequently, it will also need to be managed through an abstraction layer. This means that, unlike today, WANs in the future may not be managed as widely distributed physical network devices. Instead, higher-level network functions will be virtualized to run on standard servers, in much the same way that applications, servers, and storage are currently virtualized in the data center. These virtualized network functions will be managed as logical groupings of network resources.

Virtualization in the WAN will evolve to hide much of the cloud's complexity by managing the applications, data, servers, storage and supporting network resources as single logical representations. Using this approach, enterprises will be able to meet the needs of employees, partners, and customers more quickly, more efficiently, and at lower cost.

The role of SD-WAN in enterprise networks

SD-WAN gives enterprises more control of their network, particularly when connecting smaller sites. By mapping the virtual to the physical network and hiding its physical aspects, SD-WANs build a virtual network on top of a physical network or service. For example, SD-WAN allows sites to be connected, using a secure internet connection or an existing IP/MPLS VPN service. Both approaches can use any mix of last-mile technologies, such as xDSL, carrier Ethernet, or mobile broadband — instead of costly leased lines. Sites can have multiple physical connections for backup in order to provide additional capacity and resiliency, or for different types of traffic.

Network edge functions, such as DNS, DHCP, switching, routing, firewall, encryption, antivirus, intrusion detection, WAN optimization and load balancing, are implemented in software as virtualized network functions (VNFs). A central policy manager defines, deploys, and enforces overall network functions and advanced services, including network security. A central network controller downloads the VNFs as software that runs on standard commercial off-the-shelf (COTS) servers acting as virtual customer premises equipment (CPE) at each enterprise site.

Compared to traditional WAN services, SD-WAN is a more agile, flexible, and virtualized way to connect small enterprise sites to the private WAN. With zero-touch installation and centralized policy-based configuration, management, and control, SD-WAN ensures fast adds, moves, and changes while eliminating the need for site visits. Furthermore, enterprises can connect small sites without incurring the costs and complexities of traditional WAN services.
Building a private network for digital technologies and the cloud

For most enterprises, re-architecting their existing WAN to include a mix of private WAN infrastructure, managed WAN services, and SD-WAN is likely the best approach to support digital technologies and the cloud. At the same time, though, they need to consider the best mix to suit their individual requirements, as well as the best network management and support strategies for such a hybrid WAN environment. The following sequence outlines the options an enterprise could take to implement a hybrid WAN that supports not only its digital transformation and cloud strategies but also its business objectives:

• Build a private optical network to provide very high-speed, secure transport among major sites and data centers to create a private cloud.

• Implement a private IP/MPLS core to provide reliable connectivity among major sites and data centers, separate enterprise applications running in the private cloud, and in order to connect to hybrid cloud resources and services.

• Use managed IP/MPLS VPN or cloud connect services to connect larger remote enterprise sites to the cloud where cost/performance is justified or where changes are less frequent and more predictable.

• Implement SD-WAN access to provide more flexible connectivity to the cloud for smaller remote enterprise sites, or where changes are more frequent and unpredictable.

• Implement integrated, end-to-end configuration, monitoring and troubleshooting of the WAN infrastructure and, over time, adopt and migrate to SDN-based orchestration and automation of network and IT resources for a more dynamic, flexible, and agile cloud.

• Implement a WAN support strategy for the cloud that embraces both network and IT support, either in-house by investing in personnel with the necessary skills, or by outsourcing to an appropriate network and cloud IT support specialist, such as a systems integrator.

An enterprise could implement one or more of these options depending on its technical and business requirements. The following section describes these options in more detail.

Building a secure private optical transport network

As illustrated in Figure 3, building a secure private optical transport network, using leased or owned dark fiber and self-managed optical equipment, provides an enterprise with secure, very high-speed, point-to-point transport among large sites and data centers in a private cloud. Using diverse fiber paths and redundant optical equipment provides a high level of resilience. This approach makes sense for enterprises where bandwidth needs are increasing, can change rapidly or unpredictably, or where there is a requirement to manage the evolution of technology for business or competitive reasons.
The benefits of building a secure private optical network include the ability to:

- Provide scalability, security, and control to support business-critical cloud applications.
- Optimize latency for synchronous and time-sensitive enterprise applications.
- Support consolidation of multiple data centers to help reduce cost and complexity.
- Deliver bandwidth and capacity on demand for data center and cloud interconnect.
- Manage soaring data growth and improve server utilization across data centers.
- Control and manage business continuity and a disaster recovery strategy.
- Implement an optical layer with strong encryption and centralized key management.

The wider availability of dark fiber, more fiber-connected buildings, and the closer proximity of colocation data centers makes it attractive for enterprises to consider building a private network to support a private/hybrid cloud. However, it is important to compare the monthly recurring costs (MRCs) of a traditional network service with the up-front costs, the MRCs, and the break-even point of leasing dark fiber, as well as the purchase and maintenance costs of the optical DWDM equipment. When compared to traditional network services, the business case for an organization that is consolidating data centers and implementing a private cloud often shows that dark fiber achieves a payback period of less than two years.

Alternatively, enterprises can build a private optical network using managed wavelength or carrier Ethernet services. This approach can be cost-effective initially; however, over time, it can become costly for the private cloud. This is especially true if an enterprise has high and growing traffic. Moreover, managed services may not provide the level of control and security required by some enterprises to meet regulatory or compliance standards. Even so, these managed services can be useful for connecting to additional IT capacity and resources when needed in a virtual private cloud, or, as part of a hybrid cloud, to run less critical or on-demand applications.
Implementing a private IP/MPLS core and augmenting with VPN services

Managed IP/MPLS VPN services provide resilient, reliable, any-to-any connectivity among multiple sites. While ideal for small-to-medium enterprises, many enterprises are finding that these VPN services no longer provide the right cost/performance to support digital technologies and a private cloud. This is particularly the case for the backbone WAN. That is because VPN services are difficult to scale and costly at higher bandwidths required for backbone WANs and private/hybrid clouds.

For large enterprises, a private IP/MPLS core provides an alternative solution to support a private/hybrid cloud. The private IP/MPLS core:

- Provides resilient, reliable, any-to-any connections among main sites and data centers.
- Assures scalability, control, and predictability in the core — where it is needed most.
- Enables voice, video, and data to be delivered across a single infrastructure.
- Supports multiple services on a common platform across a common infrastructure.
- Enables traffic engineering and QoS for both legacy and cloud applications.
- Secures data with IPSec or network group encryption.
- Delivers more predictable application performance with more stringent SLAs.
- Extends virtualization among multiple SDN-enabled data centers in the cloud
- Provides connectivity from smaller sites to SDN-enabled data centers and the cloud.
- Integrates and interoperates with existing managed IP/MPLS VPN services.

![Figure 4. Implementing a private IP/MPLS core and augmenting with IP/MPLS VPN services](image-url)
A private IP/MPLS core provides an overlay to an optical network, and enables the separation and control of data from different departments and groups. One example is the separation of inter- and intra-data center traffic or the separation of sensitive business data from general data for regulatory or compliance reasons. A private IP/MPLS core also enables the enterprise to leverage the lower costs and higher performance of a private optical network or managed optical transport. The enterprise also benefits from the control, resiliency, reliability and QoS that self-managed, carrier-grade IP/MPLS routers provide. In addition to more control over bandwidth among main sites, the IP/MPLS core can be easily integrated with existing managed IP/MPLS VPN services in order to connect to smaller or remote enterprise sites. This is illustrated in Figure 4.

Using IP/MPLS VPN services to connect remote enterprise sites

Many enterprises use IP/MPLS VPN services to provide secure, resilient, reliable, and any-to-any connectivity among multiple sites. IP/MPLS VPN services are widely available from many different service providers and are ideal where the cost/performance is justified. They are also appropriate where changes are less frequent and more predictable — in the case, for example, of connecting remote enterprise sites. Among other benefits, IP/MPLS VPN services support a mix of voice, video, and data and allow applications and traffic to be prioritized, according to requirements and level of importance. Most service providers also offer a variety of SLAs, QoS guarantees, WAN-bandwidth optimization and application performance monitoring tools.

The benefits of IP/MPLS VPN services include the ability to:

- Connect multiple types of users, including partners and suppliers.
- Support Layer 2 carrier Ethernet VPNs and Layer 3 IP VPNs.
- Maximize bandwidth utilization with no restrictions on traffic mix.
- Simplify operations with WAN routing provided by the service provider.
- Support in-depth network and application monitoring.
- Support custom management levels, including full and split CPE management.
- Support other services, such as internet access, security, SIP trunking and hosted PBX.

Despite these many benefits, IP/MPLS VPN services have some disadvantages. Compared to carrier Ethernet services, bandwidth can be expensive and inflexible, particularly at data rates beyond 1 Gb/s. Often, there are separate charges for access circuits and the VPN service itself. Few offer on-demand bandwidth changes and the time to effect charges can be notoriously slow and the process opaque. Adding to the cost, most charge for bandwidth or configuration changes, as well as for traffic prioritization. And, some only support a few traffic priority levels.

For many enterprises, IP/MPLS VPN services have served them well, and they can continue to do so. One approach is to use them according to the criteria above — that is, only where they make sense for remote or international enterprise sites. To ensure that cloud-based applications have adequate performance and responsiveness, enterprises may need to upgrade their IP/MPLS VPN services. For example, some sites may need to increase bandwidth whereas other sites may need to tighten their SLAs. For many small enterprise sites, the migration to an SD-WAN solution — one that better matches the cloud's characteristics — makes more sense.
Connecting small enterprise sites using SD-WAN

When moving to the cloud, enterprises need more dynamic, agile, and flexible ways to connect small enterprise sites. Reducing the cost of connecting small enterprise sites to the private cloud is also a driving factor, particularly if staff at these sites have little or no networking expertise.

SD-WAN has precisely the right characteristics. It uses easily deployed, centrally managed, policy-based and software-defined solutions that employ standard, server-based appliances. Some benefits of SD-WAN are that it:

- Reduces the complexity and cost of connecting small enterprise sites.
- Ensures a more standard approach for small enterprise sites.
- Implements network functions in software, such as firewall, encryption, DNS and DHCP.
- Uses a central policy manager to define, deploy, and enforce network functions.
- Automates CPE configuration by downloading network topology and functions.
- Supports any mix of last-mile technologies, such as Ethernet, xDSL, or mobile broadband.
- Supports multiple connections for backup, additional capacity, and resiliency.
- Provides a more consistent quality of experience for users accessing cloud applications.

One of the challenges when evaluating SD-WAN solutions is the business case and ROI. The SD-WAN solution’s upfront CapEx and ongoing OpEx must be compared to the overall cost of traditional solutions. Because SD-WAN can use lower cost, higher bandwidth broadband links, the business case for a greenfield WAN can be very compelling. Table 1 illustrates the case.
Table 1. Typical three-year costs for IP/MPLS VPN versus SD-WAN for a 250-site enterprise

<table>
<thead>
<tr>
<th>Cost components</th>
<th>IP/MPLS VPN</th>
<th>SD-WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router CapEx</td>
<td>$750,000</td>
<td>$250,000</td>
</tr>
<tr>
<td>Router OpEx</td>
<td>$120,000</td>
<td>$150,000</td>
</tr>
<tr>
<td>Staffing OpEx</td>
<td>$240,000</td>
<td>$120,000</td>
</tr>
<tr>
<td>WAN communications</td>
<td>$6,750,000</td>
<td>$2,250,000</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$7,860,000</strong></td>
<td><strong>$2,770,000</strong></td>
</tr>
</tbody>
</table>

When compared to IP/MPLS VPN services, an analysis conducted by Nokia Nuage Networks indicates that SD-WAN solutions can improve site turn up by up to 10 times while reducing operating costs by more than 50 percent per site. However, the business case may not be as compelling if penalties for early service termination are factored into the case, even though enterprises may be willing to accept these penalties given that SD-WAN is more agile, dynamic, and flexible.

Providing secure internet and mobile access to the enterprise cloud

As social, mobile and cloud applications and services become more common, enterprises need to consider how to connect employees, partners, and customers. This introduces additional network- and data-related challenges, including scalability, capacity, and security. Increasingly, these concerns extend to IoT devices that need to communicate and send information directly to the enterprise cloud using secure fixed or mobile broadband connections. Enterprises will only be able to meet these needs by providing selective access to specific devices, applications, and services through approved and controlled mechanisms, such as secure gateways that separate and secure the private enterprise network from the public internet.

Implementing integrated management for digital technologies and the cloud

An integrated management strategy that manages multiple network layers, end-to-end services, as well as applications provides multiple benefits, including:

- Converged management across multiple network domains
- Node, network, service and application layer management
- Rapid provisioning of new cloud connections, services, and applications
- Network SLA monitoring with service and application assurance
- Correlated multi-layer, multi-technology analytics, and troubleshooting
- Simplified operational and business systems integration.

Automation helps to ensure fast, easy device configuration, reduces the risk of errors, and speeds deployment time. Multi-domain, multi-layer management improves operations by unifying workflows to maximize efficiency. It also simplifies and accelerates troubleshooting across multiple network elements, domains, and layers. For its part, advanced end-to-end network-, service- and application-aware
management helps to maintain end-to-end QoS and ensure SLAs. Equally important, network analytics, pro-active tracing, diagnostics, and fault isolation help to prevent service degradation before it impacts users.

The issues of how to address performance and track usage for applications in the cloud are two common challenges facing enterprises. To meet these challenges, distributed network-based Layer 4 to 7 application assurance provides real-time analytics and reporting. The ability to identify, classify, and analyze applications and usage trends improves performance and optimizes QoS. It provides capabilities such as:

- Performance monitoring and reporting for hosted or cloud applications with granularity across multiple network layers and segments.
- Bandwidth utilization between any two sites on a per-application, application group, or user group basis.
- Application statistics, including top bandwidth applications and top users per application.
- Centralized repositories for application data collection that provide visibility over time into use of enterprise and cloud applications.

IP network analytics identify enterprise and cloud applications and services in real-time as they transit the network. The analytics also show how applications and services are performing against their SLAs. Furthermore, multi-dimensional software analytics help to secure the network from today’s highly complex distributed denial of service (DDoS) attacks — without the cost of dedicated security appliances.

To give the network the agility and flexibility of cloud IT, network management will become more dynamic over time with wider deployment of SDN and SD-WAN. Service automation and network optimization across multiple domains will deliver network services faster, lower operational costs, and increase network resource utilization.

Implementing a network support strategy for digital technologies and the cloud

The implementation of a support strategy for digital technologies and the cloud must embrace both network and IT support. Enterprises can provide in-house support by investing in personnel with the necessary skills or they can outsource support to an appropriate network or cloud specialist, such as a service provider or systems integrator. Alternatively, an enterprise can outsource some aspects of support, such as network management, while controlling others, such as maintenance of network security, as part of its overall IT security strategy.

By purchasing a range of services to suit its needs, an enterprise can achieve the right balance between risk reduction and cost. These services could include:

- Professional services such as consultancy, design, installation and integration.
- Support services, including product support, maintenance, and repair.
- Managed services, including 24/7 management using network operations centers (NOCs)
- Build, operate, and transfer services that remove most of the risk.

Whichever approach an enterprise chooses, it must implement an end-to-end approach that combines essential services across both network and IT domains.
Conclusion

With the move to digital technologies and the cloud, and with the increasing availability of more agile and flexible SD-WAN solutions, enterprises need to re-evaluate and determine the best approach to their WAN needs. A private WAN can be a strategic investment that supports an enterprise’s digital transformation and cloud strategy. A private cloud for critical business applications can be augmented with virtual private or hybrid cloud services for less critical and on-demand applications. Enterprises can build or upgrade a private WAN backbone to connect their main sites and consolidate data centers, offsetting the cost with more flexible, efficient, and lower cost SD-WAN solutions for smaller sites. For enterprises undergoing digital transformation, this approach provides the scalability, security, and control required to enable a private cloud while reducing costs, providing flexibility, and increasing agility to support virtual private and hybrid cloud models.

Acronyms

BYOD  Bring your own device
COTS  Commercial off-the-shelf
CPE  Customer premises equipment
DDoS  Distributed denial of service
DWDM  Dense Wave Division Multiplexing
DPI  Deep packet inspection
GDPR  General Data Protection Regulation
IoT  Internet of Things
MPLS  Multi-protocol label switching
MRC  Monthly recurring charge
NAT  Network address translation
NOC  Network operations center
PBX  Private branch exchange
SDN  Software-defined network
SD-WAN  Software-defined wide area networking
SIP  Session initiation protocol
SLA  Service-level agreement
VNF  Virtualized network function
VPN  Virtual private network
WAN  Wide area networking