Deploying Smart VPN and Secure Connect for Cloud-Ready Businesses

#TimeToDoBig
#TimeToDoBig

## Deploying Smart VPN and Secure Connect for Cloud-Ready Businesses

### Table of Contents

1. Introduction
2. Security Issues with Cloud Computing
3. The Concept of Virtual Private Network
4. How does VPN help in safely accessing the cloud?
5. What makes Smart VPN a Private Network Solution of Choice?
6. Conclusion
Introduction

Cloud computing has generated considerable interest, and industries such as banking, insurance, e-commerce, hospitality, BPOs and ITES are increasingly adopting it. The service delivery model of the cloud offers data storage and versatile computing solutions for users in all these markets.

With the cloud, it is feasible to achieve multi-level virtualisation and abstraction. This element has been validated through the efficient combination of data, applications and custom software in cloud platforms. Cloud also allows for networking similar to that in grid computing or distributed processing.

While cloud services are gaining ground due to the full range of benefits they offer, the wireless networks that they have created have also raised certain security concerns. As Internet-driven solutions, these systems are prone to risks and vulnerabilities such as Distributed Denial of Service (DDoS) attacks, data thefts, and web scraping.

The security of their wireless network and cloud environment is, therefore, a critical differentiator for organisations that want to leverage the technology. This paper looks into the key security issues with cloud computing and how the same can be addressed using virtual private networks (VPN) and a secure connection to the cloud.

Security Issues with Cloud Computing

In the cloud, resources are entrusted to third parties and are accessed over the Internet. For most businesses, this implies only partial control over their data and applications. They question if external service providers can safeguard their sensitive information while also ensuring compliance with regulations on its access. According to Gartner¹, most of the Internet attacks target web apps owned by businesses.

Organisations also express concerns on building their private clouds as this can create a single point of vulnerability with the aggregation of different kinds of sensitive data onto a single platform.
Their apprehensions are not unfounded. Of the several cloud computing security issues, the primary ones can be classified as:

**Distributed-Denial-of-Service Attacks (DDoS)**

When heavy traffic (usually disguised as bots) is initiated to the cloud, genuine users can lose complete access or find it difficult to access their data/apps.

**Employee Carelessness**

BYOD culture and the freedom to work from any location may cause employees to log on to enterprise cloud solutions from unsafe devices, making the platform vulnerable to malware and other IT threats.

**Social Engineering Attacks and Phishing**

The openness of cloud computing systems has triggered frequent phishing and social engineering attacks wherein hackers manipulate authorised users to divulge sensitive information or click a malicious link/file.

**Sharing of Cloud Solutions**

With multiple entities storing and accessing their data, apps and computing systems from the same platform, there are concerns of threats originating from different users.

**Data Loss and Inadequate Backups**

Poor data backups and incorrect data syncing have caused many business cloud users to be victims of ransomware and other cyber threats.

**System Vulnerabilities**

Cloud systems may have their own vulnerabilities, particularly with networks built on multiple third-party platforms and complex infrastructures. Once the weakness of some popular third-party app becomes known, it can be easily used against businesses that use the system.
The Concept of Virtual Private Network

As cloud computing becomes indispensable for businesses, it is essential to create a secure connectivity passage and networking environment. This is where a virtual private network (VPN) comes into play.

By building a virtual private tunnel, VPN technology protects the data being transmitted over the Internet. Users can enter a secure internal network, access resources, communicate and exchange data, even though they do it via public Internet connectivity. They need not have a dedicated connection resource like a leased line for this level of security.

Before data is transmitted in a VPN, it gets encapsulated in a packet that has a header to provide routing details until the packet traverses through a public network to reach the endpoint of its tunnel. When each packet reaches the endpoint, it is “de-capsulated” and sent to its final destination.

A VPN is a business-standard connectivity solution that is not impacted by delays and risks of vanilla Internet services. It has a built-in quality of service (QoS), resiliency, flexible capability, and business continuity support.

IPSec, L2TP, PPTP and SSL have been the commonly used tunnelling protocols for VPN. A new protocol option that has now become popular is the multiprotocol label switching service (MPLS).

With MPLS VPN, once a data packet gets labelled, it can bypass the multiple hop analysis. Consequently, it travels at high speed for secure communications.
How does VPN help in safely accessing the cloud?

For organisations storing their sensitive data and running applications in the public or hybrid cloud, the best way to protect these assets is to control access to them via the Internet. With a VPN, they can securely connect to the infrastructure that houses their resources because it builds a network that is isolated from the Internet. The authorised users can connect to the cloud only through this isolated private network. They must use specific external devices (within the VPN) for the access.

The security model of a VPN can be compared to that of a castle defended by wide and deep moats and drawbridges. A moat used to isolate castles from attacks is like non-routable IP address ranges. Alongside, the use of drawbridges allowing entry/exit of authorised users is similar to the VPN’s strictly controlled access for traffic and external devices.

What makes VPN an ideal pathway to the cloud?

The top factors include:

**Lower Risk**

With millions of computers and smartphones exposed to the Internet, the risk of cyber attacks for the overall public network and systems connected to it multiplies. A VPN allows only trusted devices to reach an enterprise’s private network, reducing the number of attack vectors that a hacker can use to compromise network security.

VPN solutions also implement mutual authentication wherein both the server and the device connecting to it verify each other’s identity. When the server establishes the user and device, it may also enforce particular rules that permit access to only a part of the systems/services in the cloud. The concerned organisation can define these levels and access rights.
Data encryption is another security benefit afforded by the VPN. It is particularly crucial for mobile employees who need to access business assets in the cloud over free Wi-Fi hotspots at airports and other public places. In their attempts to steal credentials from unsuspecting users, hackers may use malicious Wi-Fi connections to mimic a legitimate hot-spot. When their device is connected via VPN, the traffic is encrypted end-to-end, and authentic users can keep their online activities private. They are immune to threats from rogue networks.

The use of SaaS applications is more secure when they are accessed via a corporate VPN. This is because SaaS apps typically have only the username & password authentication process. If there are no measures for maintaining password strength and account lockout on several unsuccessful attempts, weak password recovery mechanisms can be exploited for unauthorised access to enterprise apps. With a VPN, IT teams can restrict employee access to SaaS applications through only a specified range of the company’s IP addresses.

Businesses that use cloud solutions such as IaaS, and have employees who need to access their private network from global locations, can scale their private network connectivity through VPN. It helps in bringing the network closer to the location where the employees are based.

Users also get better speeds and low latency with their remote access if VPN servers co-exist with private network resources and have been implemented in cloud regions closest to them.

When an organisation develops and distributes its IaaS-based IT services across regions, employees can use a remote-access VPN to access the distributed cloud infrastructure services from a site nearest to them. In essence, this enables the company to build a global private network that’s isolated, cost-effective, fast and secure.

Security and Extension of Private Network Services

Many enterprises now run their applications on infrastructure offered by multiple cloud providers. In this scenario, secure inter-cloud communications are critical. A VPN securely routes private traffic between different clouds and on-premise data centres within the corporate IT network.

Builds Upon Previous Security Investments

Amidst rising incidents of cyber threats, businesses need to invest heavily in their security measures. They hire experienced IT professionals and deploy custom tools, software, hardware and processes to optimise their overall security setup.
The security of a network perimeter is primarily enhanced by the use of a private network, along with public network access secured through web proxies, firewalls and intrusion detection systems.

To deploy multiple security features for a business technology infrastructure, most IT teams now use Unified Threat Management (UTM) solutions. With UTM, they can integrate anti-virus, anti-spam, and content filtering. These are combined with network security systems such as intrusion prevention, data loss prevention and firewalls to enhance the overall IT security for the organisation. This is another deployment where a VPN server fits in.

UTM tools are applied in a few central networking locations for maximised return on investment. With VPN, the organisation can direct all traffic from different networks and devices to the primary location and maintain security without the operational complexities of protecting network infrastructure at various locations.

When combined into a UTM solution, VPN helps in reducing the attack surface for network exploitation and centralises security services for all devices on the network. The endpoint security systems, including antivirus software and operating system security patches, can be pushed to devices connected through VPN akin to the devices being connected directly to the business IT network. This linking enables the organisation to have an integrated defence against cyber threats for all networked devices irrespective of their location.

**Enhances Employee Productivity**

Employees who are out of the office and away from the secure connectivity of their corporate networks may still need to work on enterprise applications and access data stored in the cloud.

High-speed Internet access – now offered by several service providers – and the presence of Wi-Fi hotspots across regions makes it feasible to access the cloud. The VPN secures this Internet access for employees to stay productive at any location. They can use the VPN with cellular Internet connectivity to keep working with enterprise applications even when they are away from the workplace.

**What Makes Smart VPN a Private Network Solution of Choice?**

Tata Tele Business Services (TTBS) has devised the Smart VPN for businesses that aim to balance their metrics of service availability, data privacy, network security, employee mobility and cost control.
The Secure Connect component of Smart VPN enables businesses to safely offload their data and apps to a privatised segment of any public cloud. Using TTBS Secure Connect, organisations also get predictable and SLA-backed enterprise-grade network connectivity to their cloud platforms.

In addition to providing the security of a privatised network, Secure Connect enables the efficient operation of data-heavy enterprise apps. It builds better end-user experience as the business data travels between on-premise infrastructure and the cloud.
3- Internet VPN

Internet VPN – the third feature of Smart VPN – employs IP to transfer business data across Internet networks operated by third parties. These networks may be in forms of broadband, 3G/4G or leased line. The integrity, authenticity and confidentiality of the data flow are ensured by the IPSec protocol that creates secure VPNs over the Internet. It builds point-to-point connections.

IPSec is good at connecting remote offices and even temporary connections – such as exhibitions and other business events – to a VPN. And when a primary network is down, it provides a backup for connectivity. IPSec also creates an additional layer of security through authentication and encryption requirements. It allows an organisation to maintain its own IP addressing plan through tunnels between the sites.

The Internet VPN element of Smart VPN is offered with on-site and on-the-move options. While the former helps in extension of connectivity to site offices, on-the-move service is for enterprises with mobile employees and working models such as BYOD and work-from-home.

Smart VPN across Industries

By seamlessly combining the strengths of MPLS, Secure Connect and Internet VPN, Smart VPN helps businesses optimise their workflows and enable secure network access to employees, business partners, customers and suppliers.

An e-commerce company can make its services more private by using Smart VPN that hides the IP address and even the ISP from prying eyes. Furthermore, the traffic to the website gets encrypted. This feature benefits the customers whose activities will stay hidden from other websites, and they will not be bothered by intruding advertisements.

Travel & hospitality companies that are expected to have secure websites for quick online bookings also benefit from Smart VPN. The encryption protocols keep their Internet traffic and online data safe from cyber crooks. Additionally, with a privatised network, hotels can offer optimal Wi-Fi services on-site to their customers.

Enterprises in the ITES sector can efficiently maintain their cloud-based IaaS products by using and upgrading them through Smart VPN.
Deploying Smart VPN and Secure Connect for Cloud-Ready Businesses

Connecting to different subsets of IaaS such as Compute as a Service, Storage as a Service, Web Hosting as a Service, Disaster Recovery and Backup as a Service, Desktops as a Service (DaaS), and Servers as a Service is more secure through a privatised network.

Another domain that stands to gain from Smart VPN includes the BPOs that are increasingly adopting Voice over Internet Protocol (VoIP) to communicate with the customers they serve. The security risks of VoIP such as viruses, malware, Denial of Service and call hijacks are adequately addressed by Smart VPN, which secures all communications and transactions over the Internet.

For the banking, financial services & insurance (BFSI) industry, the security of data is the top priority. They are also appreciative of the potential of the cloud for their business. As an OpEx model, SaaS holds the promise of agility in supporting volatile business cycles and demand patterns. With a web-based interface, it offers better operational control. Smart VPN enables BFSI players to leverage all benefits of SaaS and other cloud solutions while maintaining high levels of security in their processes.

Conclusion

By combining security, QoS and any-to-any connectivity, as well as giving more control on networks with real-time performance reporting, Smart VPN offers the enterprise-grade connectivity that businesses need. The end-to-end SLA provided by TTBS makes this solution more reliable for organisations.

Light on the budget and rich in functionality, Smart VPN is a full-featured tool having a broad array of remote access solutions with fine-tuned access controls.

To know more about this exclusive offering of TTBS, contact the team on:

- 1800-266-1515 (Toll free)
- 1515@tatatel.co.in (Non technical)
- data.enterprise@tatatel.co.in (Technical)
- 8090001515*
- Live Chat*
  *Mon - Sat | 10:00 a.m. to 7:00 p.m.

Data Source:
Deploying Smart VPN and Secure Connect for Cloud-Ready Businesses

Get in touch

TATA TELE BUSINESS SERVICES
Market leaders with the widest range of products and solutions.
| Collaboration | Connectivity | Cloud & SaaS | IoT Solutions | Marketing Solutions | Security Solutions

Call 1800 266 1800
Email dobig@tatatel.co.in
Visit www.tatateleservices.com

Find us on

#TimeToDoBig