Four Key Elements of a Secure, High-Performance Hybrid Cloud Networking Strategy

Delivering an optimized bridge to the cloud with Citrix CloudBridge
As Infrastructure as a Service (IaaS) grows, many IT organizations see valuable opportunities to move workloads to third-party clouds on a temporary basis. But this agility can come at a cost; the simple Internet connectivity typically used for this migration places significant limitations on security and performance.

To avoid these compromises, enterprises need to make sure their hybrid cloud connectivity strategy addresses the following key elements:

- End-to-end security
- On-demand provisioning
- Deep app visibility
- Optimized app delivery

Citrix® CloudBridge™ enables enterprises to meet all four of these requirements through a single solution. Extending the security and performance of datacenter networks to any public cloud, CloudBridge unlocks the full agility of IaaS—without compromises.

**The rapid rise of IaaS—and the challenges it presents**

Cloud computing has become a mainstream element of IT infrastructure. Gartner predicts that the markets for Infrastructure as a Service (IaaS), cloud management and security devices, and Platform as a Service (PaaS) will grow from $7.6 billion in 2011 to $35.5 billion in 2016—a compound annual growth rate (CAGR) of 36 percent.¹ More and more companies now rely on cloud services to spin up virtual machine environments and the associated storage and backup for uses such as:

- **Test and development projects.** Cloud services accelerate time-to-market by allowing IT to access development resources on-demand without the need to provision physical servers and other hardware.

- **Seasonal or peak computing capacity.** Companies can scale up quickly to meet surge demand, then scale down just as easily, with pay-as-you-go pricing instead of the high capital costs of fixed infrastructure.

- **Business continuity.** Cloud services can be used to provide rapid access to virtualized applications when a site’s primary datacenter has become unavailable, without the high cost of creating and maintaining a secondary disaster recovery site.

• **Storage replication.** By mirroring stored data to the cloud, companies can support disaster recovery and ensure that data will be available whenever and wherever it is needed.

• **Linking staging environments.** As web and cloud projects proliferate, many companies are creating multiple pre-production environments, some on-premise, some in the cloud. It’s important to maintain version control and integrity while moving data between these environments.

In cases like these, the cloud service is being used to augment existing datacenter capacity, and the respective workloads will typically be moved to the third-party cloud for a defined period of time, then moved back to the corporate datacenter.

**CloudBridge – Use cases**

- Cloud Bursting
- Development
- QA/Testing
- Storage Replication
- Staging Environments
- Disaster Recovery
- Business Continuity

The ability to move workloads between the organization’s own private cloud and a public cloud offers tremendous agility to respond to new needs quickly and cost-effectively. However, this strategy can involve an often-overlooked drawback: the use of basic IPSec VPNs and simple Internet connectivity for the migration. While the growth of cloud services has been synonymous with the use of the public Internet, its limited ability to provide secure and performance-based connectivity can put the organization’s assets and productivity at risk.

**Four critical elements for hybrid cloud connectivity**

Most enterprises seeking to leverage off-premise cloud services must currently make a compromise between agility on one hand, and security and performance on the other. Developers and business units with tactical projects or temporary requirements often forgo security and connect to public cloud services with unproven security. While this provides on-demand access to virtual resources, it also exposes enterprise content and data to most Internet-centric vulnerabilities by opening new, often unprotected entry points.
Enterprise IT typically takes the opposite approach, employing more secure cloud access through an IPSec VPN or through carrier-based MPLS circuits to a cloud connection point. This provides adequate performance and security—but lacks the flexibility to create and tear down connections based on dynamic project needs, especially given the yearly contracts required by carriers.

The tradeoff between the agility business demands, and the security and performance IT requires, makes it impossible for enterprises to realize the full business value of a hybrid cloud strategy. To meet both sets of requirements, IT needs a cloud connectivity solution that can support all four essential elements of a complete hybrid cloud network strategy:

- **End-to-end security.** IT faces a critical need to ensure complete security for data in motion between the corporate datacenter and the third-party cloud. This will ensure that enterprise assets are not compromised in transit, as well as preventing threats from entering the enterprise network through vulnerabilities inherent in public Internet connectivity. End-to-end security can also be essential for meeting IT governance policies and mandates.

- **Optimized application delivery.** The agility of cloud computing can’t come at the cost of performance. IT has to be able to enable the delivery and enforcement of service level agreements (SLAs) to ensure consistent productivity for users and the business.

- **On-demand provisioning.** Much of the value of cloud computing lies in the ability to tap into scalable resources quickly and easily. Developers, business units and other groups must be able to connect to the specific cloud services they need, when they need them, to address time-sensitive or temporary capacity requirements.

- **Deep application visibility.** To keep the business running at peak performance, IT needs the visibility to monitor, capture and analyze information on the way enterprise applications are being used, and to quickly find and fix application problems as they emerge.

Four key elements needed in a hybrid cloud network strategy

End to End Security

On-demand provisioning

Deep Application Visibility

Optimized Application Delivery
Most cloud connectivity solutions on the market today fail to address the entire stack of capabilities needed to meet these requirements, focusing instead on a single specific tier. Only a complete, secure, optimized bridge between on-premise and third-party clouds can allow enterprises to fully realize their strategy to use cloud services for both production and non-production workloads.

**Delivering secure and optimized bridging with CloudBridge**

Citrix CloudBridge enables enterprises to extend the security and performance of their datacenter networks to the cloud of their choice. The solution incorporates proven Citrix Netscaler® and Citrix Branch Repeater® technology into a virtual or physical device that builds a bridge in an on-demand manner to a target environment.

Offered in both virtual and physical appliances, CloudBridge is simple to deploy for almost any role in the enterprise. An intuitive configuration GUI extends a bridge from the corporate datacenter or private cloud to a termination point at another datacenter or cloud provider. Security is delivered through built-in IPSec, and optimization is provided through compression, caching and deduplication. Integrated NetScaler functionality includes global server load balancing (GLSB) for layers 4 – 7, which is applied worldwide across geographically distributed server farms in both cloud locations. This greatly increases the resiliency of the connection and provides seamless sessions even in the event of traffic issues. Once the bridge is built, workloads can move between locations until the user decides to terminate the session, at which point a single click deactivates the tunnel.

CloudBridge enables IT to address all four critical elements of a complete hybrid cloud networking strategy through a single solution:

- **End-to-end security.** CloudBridge protects data with IPSec security—supporting higher speeds and advanced encryption beyond the basic VPNs offered by most cloud providers—to keep it secure as it traverses the network links between the enterprise and the cloud. CloudBridge is also the only solution to enable both VPN tunneling and WAN optimization. Enterprises can move or burst processing to the cloud while keeping databases and corporate directories safely in corporate datacenters, so they can deliver the service levels they need without compromising on security.

- **Optimized application delivery.** Integrated TCP optimizations, compression and data deduplication minimize the performance degradation that can be introduced by WAN connections between enterprise datacenters and the cloud.

- **On-demand provisioning.** L2 network bridging makes the cloud network a natural extension of the enterprise’s L2 network, making it easy to shift compute resources to the cloud without having to re-architect applications.

- **Deep application visibility.** CloudBridge provides the application-level visibility and monitoring IT needs to guarantee delivery and capture essential business intelligence.
Conclusion
Leveraging the agility of cloud services shouldn’t require enterprises to sacrifice security or performance. A complete strategy for hybrid cloud connectivity must encompass both of these elements, in addition to the on-demand provisioning users need and the deep application visibility IT requires. Unlike single-tier cloud connectivity solutions, CloudBridge addresses the full scope of capabilities IT needs to migrate workloads to and from third-party clouds easily, securely, transparently and with high performance. In this way, companies can meet their business needs more quickly and cost-effectively, realizing the full potential of their IaaS strategy.

Resources
• Citrix CloudBridge website
• Citrix CloudBridge overview (pdf)
• Citrix CloudBridge on Amazon Web Services