WHITE PAPER – **FEBRUARY 2017**

BUILDING SECURE DATA CENTERS IN VMWARE vCLOUD AIR WITH HYBRID DMZ

vmware®

Table of Contents

Overview

This white paper describes a reference design for implementing a secure and cost-effective data center within VMware vCloud® Air™ using a Hybrid DMZ. This design provides a way for customers to build and maintain familiar security and networking architectures in vCloud Air that are 100% consistent with their on-premises environments. This practice improves redundancy and provides enhanced security and isolation for off-premises workloads.

With a Hybrid DMZ, customers can confidently integrate vCloud Air into their organization's IT processes and best practices, making it easier to harness cloud resources and drive business improvements.

The Cloud Dilemma for IT

With the advent of the digital age, companies are being pushed to embrace technology as a core part of their business across every industry. Disruptive business models like Uber and Netflix challenge incumbents, forcing companies to consider how they can respond quickly to the next big idea. IT organizations that must ensure that they are set up to help empower these business objectives.

Drivers for Adopting Cloud

Public clouds offer many benefits that help companies innovate and compete.

- Flexible Capacity: Because resources are available when needed, companies can quickly start new projects without having to purchase, procure, install, and configure infrastructure hardware.
- Global Footprint: Leading cloud providers have data centers around the world, making it simple for organizations to expand into new markets and geographies without having to set foot in the region. Applications can also get closer to end users for improved user experience.
- Infrastructure Management: Using public clouds, IT teams no longer have to maintain and patch the hardware infrastructure. They can focus on supporting business objectives instead of "keeping the lights on."

The most frequently adopted cloud strategies involve commodity storage, Disaster Recovery, and hosted or managed Infrastructure-as-a-service (IaaS) solutions for development and testing environments. Not surprisingly, IDC reports that 60% of large enterprises already run VMs in the public cloud . IDC also reports 65% of organizations have a hybrid cloud strategy today.

What Are the Attributes of a Hybrid Cloud?

Sometimes the term "hybrid cloud" cloud is used to refer to a multi-cloud strategy, where an organization is using a combination of clouds for various purposes. At VMware, we define true hybrid cloud functionality as follows:

- Virtual machine migration is bidirectional from on-premises to the cloud
- Application portability is also bidirectional
- Security is the same or better for workloads in motion or in the cloud
- IT retains control of security for workloads migrated or extended to the cloud

Barriers to Public Cloud Adoption

Even though public cloud and hybrid cloud adoption is prevalent, most workloads are still contained within traditional data centers. While the benefits for public clouds are clear, many organizations still struggle to adopt public cloud en masse. New projects and new applications are using public clouds, but existing applications, or even new applications built on traditional application methodologies, remain on-premises.

The following factors influence this practice:

- Application designs: Traditional applications, applications built on traditional stacks (for example, LAMP) tend to be based on monolithic architectures. These architectures do not work well in public clouds, which are designed for stateless, distributed applications that require scale out. Cloud-native applications are highly distributed for resiliency and availability, while monolithic architectures rely on the overall infrastructure availability. Moving from a monolithic to a distributed model requires significant rearchitecture.
- Skills and talent gap: Designing new cloud-native applications requires new skill sets from application developers, cloud administrators, and the operations team. As the architecture of public cloud services differs from traditional data center design, the expertise to manage and operate these environments is often scarce.
- Security and compliance: Because the public cloud is inherently outside the corporate firewall, some organizations worry about placing sensitive data or mission critical workloads in the public cloud.
- Network connectivity: As companies transition to cloud, they still want to ensure that these workloads are connected back to the primary data center. Many organizations want to connect a private circuit (MPLS, for example) to their cloud-based environment to ensure secure, high-speed connections. However, WAN architecture can be complex and challenging, especially when dealing with multiple environments.
- Licensing models: While public clouds have been available for years, licensing software in public cloud environments is still a challenge. Not all companies have adapted traditional per processor or per core license models for cloud usage.

Early forays into the public cloud were often initiated without IT influence. Application developers went straight to the public cloud of their choice and began building new applications on those platforms. However, the adoption challenges become more pronounced when companies consider large-scale cloud adoption. When adoption becomes part of an overall IT strategy, organizations realize they must include their security, networking, operations, and risk management teams, and often even legal and finance teams. All these teams historically have a part in running traditional data centers.

Traditional Data Center Designs

Many organizations have implemented data center designs that are oriented around a multi-tier architecture prescribed by industry leaders like Cisco. These designs share two main characteristics:

1. It promotes a “hub and spoke”, layered approach for traffic management, where traffic flows through a hub and is distributed downstream to different spokes.
2. It advocates separation between management traffic and data traffic.

VMware also recommends this approach for vSphere environments. We typically recommend that large VMware vSphere® environments have separate management clusters from vSphere compute clusters. The management cluster includes management solutions such as VMware vCenter Server®, the vSphere Replication™ Appliance, the database server, and other infrastructure components, such as Active Directory, anti-virus solutions, and other shared services.

This design methodology also allows networking and security teams to introduce a DMZ – an isolation zone between internal and external-facing services. In traditional data centers, the DMZ has access to the external network and often hosts external facing applications like web servers and mail servers. Other servers, like the database or mailbox, would be on a separate network which has access to the DMZ, but are not directly connected to the outside world.

As organizations consider public clouds for increased agility, scale, and reach, most IT, networking, and security teams have architected data centers around this design methodology for many years

vCloud Air = Your Data Center in the Cloud

Understanding the barriers to public cloud adoption, VMware designed vCloud Air to deliver a public cloud that can operate and perform like traditional data centers. vCloud Air provides flexible and scalable resources, a global footprint, and it is still an Infrastructure-as-a-Service offering that frees IT from patching and maintaining a hardware infrastructure. The underlying architecture of the service closely aligns with traditional data center best practices, permitting vCloud Air to extend, and ultimately replace, the data center.

Data Center Extension Use Cases

There are a few common IT use cases for taking advantage of vCloud Air as an extension to the corporate data center:

- Running out of data center capacity.
- Supporting test and development environments.
- Applications that are intermittent or “bursty.”
- Applications that require more geographic reach.
- Backup and disaster recovery.

In each of these use cases, the primary data center is still where most applications exist, but vCloud Air is a supplement to those resources. In these situations, vCloud Air is an ideal solution because of the underlying compatibility of the platform.

Data Center Replacement Use Cases

In certain situations, vCloud Air actually replaces a vSphere data center. Some scenarios include:

- Corporate mandate to close data center locations.
- Contract renewal approaches, and the corporate decision is to move away from managed hosting.
- Aging equipment and service contracts, or untenable software license renewal costs.
- Merger, acquisition, or spin-off that requires vacating a data center in short time.

In each of these use cases, vCloud Air is replacing investments in data centers. Before moving to this model, however, IT administrators want to ensure that vCloud Air meets or exceeds their own data center requirements.

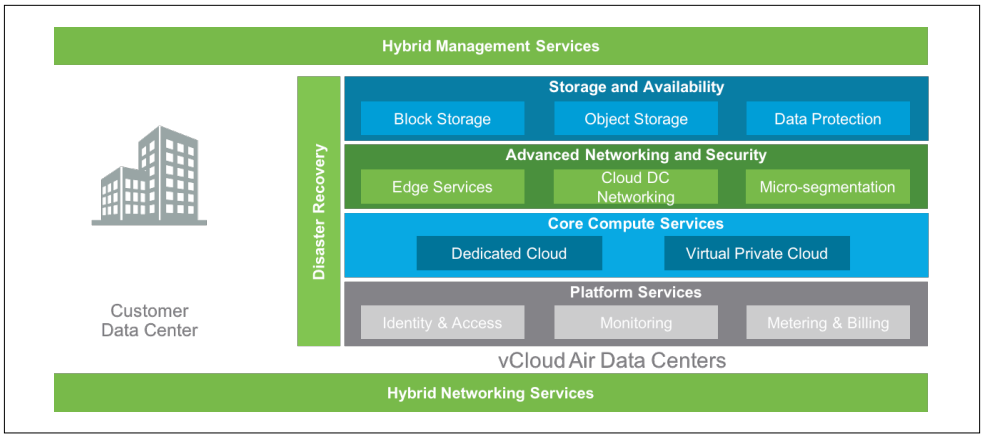

Figure 1: vCloud Air services framework for extending, replacing, and protecting customer data centers

Key vCloud Air Services

To support the various IT use cases, vCloud Air provides a broad portfolio of services which customers can enable:

- vCloud Air Dedicated Cloud is a single-tenant private cloud with dedicated computing servers, layer-2 network isolation for workload traffic, dedicated storage volumes, and a dedicated cloud management instance.
- vCloud Air Virtual Private Cloud is a multi-tenant cloud service with logically isolated compute and shared management.
- vCloud Air Disaster Recovery is a disaster recovery-as-a-service offering which enables self-service protection of vSphere virtual machines, leveraging vSphere Replication.
- Hybrid Cloud Manager™ creates an optimized, software-defined WAN to increase stretched network performance, enabling performance approaching LAN speed. Hybrid Cloud Manager also enables bidirectional workload and VMware NSX® security policy migration to vCloud Air Advanced Networking services. Hybrid Cloud Manager integrates with vCenter and is managed from the vSphere Web Client.
- Advanced Networking Services is an add-on to Dedicated Cloud and Virtual Private Cloud that provides distributed firewall capabilities, and delivers close to line rate throughput for higher workload consolidation on physical servers. It maintains a high capacity site-to-site VPN. This offering has Standard and Premium packages differentiated by the number connections and user supported per edge gateway.
- Direct Connect is a dedicated networking link that helps connect remote customer data centers to customer instances in vCloud Air. The dedicated connection circuit comprises vCloud Air Direct Connect service (from VMware) and the network connection and service from your site into the vCloud Air data center. The network connection is supplied by a network service provider who has a point of presence in the relevant vCloud Air data center.

Hybrid DMZ Reference Designs for vCloud Air

The Hybrid DMZ reference designs are a set of supported architectures that use multiple vCloud Air services to deliver a secure data center in the cloud. The designs support both data center extension and data center replacement use cases with many benefits to the organization employing them. These designs support best practices that originated in traditional data centers – namely the use of the layered DMZ as a way to both segment network traffic as well as separate management servers from compute servers.

The core of the design is the DMZ layer, which aggregates network connectivity (MPLS or IPsec) to and from different vCloud Air services. With the aggregated network, IT can consolidate the number of network connections to an individual vCloud Air virtual data center in favor of a single Hybrid DMZ connection.

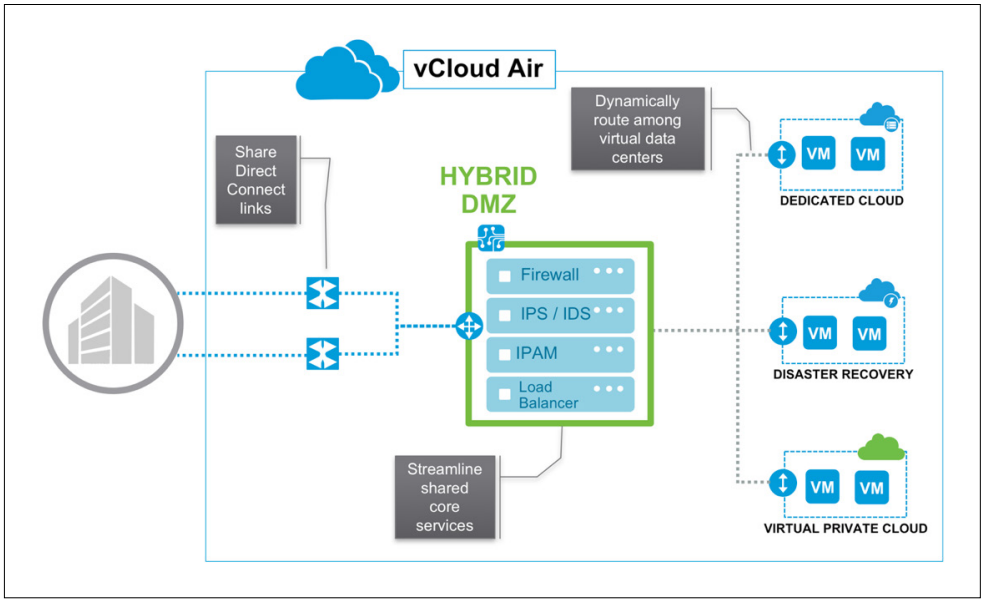

Figure 2: Example of a Hybrid DMZ design that uses the DMZ layer for networking appliances which manage three different vCloud Air services – a Dedicated Cloud, Disaster Recovery, and a Virtual Private Cloud

All Hybrid DMZ designs have at minimum:

- A DMZ layer, which is a Dedicated Cloud, sized based on customer needs.
- Advanced Networking Services for the DMZ layer act as the router for traffic to the connected services downstream.
- One or more other vCloud Air services: either a mix of services, multiple instances of the same service, or a combination of the two. For example, it can connect to two or more Dedicated Clouds or a mix of services, as shown in Figure 2. All are sized based on customer needs.
- (Optional, but recommended) Direct Connect
- (Optional) Hybrid Cloud Manager

When Do I Need a Hybrid DMZ?

You are likely to benefit from a hybrid DMZ when:

- You have multiple clouds in your configuration and want to have Direct Connect connections into all of them.
- You want to isolate traffic to endpoints in the standard DMZ model or have security appliances you plan to implement for all endpoint traffic.
- You require a singular security control point with separation of duties for end users.
- You have one or more shared services that are used by multiple clouds.
- You have licensing requirements which benefit from separate Dedicated Clouds.

In each of these scenarios, the Hybrid DMZ design can result in simplified management and networking and cost savings.

Hybrid DMZ Benefits

One of the key benefits of the Hybrid DMZ design is that it is modeled after traditional data center designs. For many organizations, it is simpler to replicate their mature architectures directly into vCloud Air without having to make significant changes. It is easier for IT decision makers to get support for vCloud Air from the networking and security teams, who find the service familiar.

Other key benefits from Hybrid Cloud Manager include:

- Centralizing shared services: Isolating shared services in the DMZ from workloads in the virtual data centers makes it easier and more cost-effective to ensure proper provisioning while also reducing costs
- Better SLA on network connectivity: Up to 10Gbps bandwidth for MPLS connectivity in an active/active state using BGP
- Use Edge as Router: No need to supply your own router for multi-segment design
- Redundancy: The Dedicated Cloud includes a built-in HA infrastructure and Active/Standby MPLS

Reference Design #1: Multi-Cloud Consolidation

Figure 3 shows a situation where a customer has multiple vCloud Air services, including a Dedicated Cloud, Disaster Recovery, and a Virtual Private Cloud. In vCloud Air, each cloud has a separate service ID (SID) and is treated as its own independent cloud service. That means they do not share any wires, as shown in the Before drawing. Even though the services are independent, the customer still requires common management servers for things like Active Directory and DNS, and each service has its own IPS/IDS solutions and well as logging service. The customer also wants to connect to each service through Direct Connect. The After drawing shows how the Hybrid DMZ aggregates the services, simplifying both the direct connect architecture and reducing the resources used for the management servers. In addition, two 10 Gbps Direct Connect Cross Connect lines are removed, saving $13,000 monthly (MSRP). These combined savings more than offset the cost of the Dedicated Cloud used for the Hybrid DMZ.

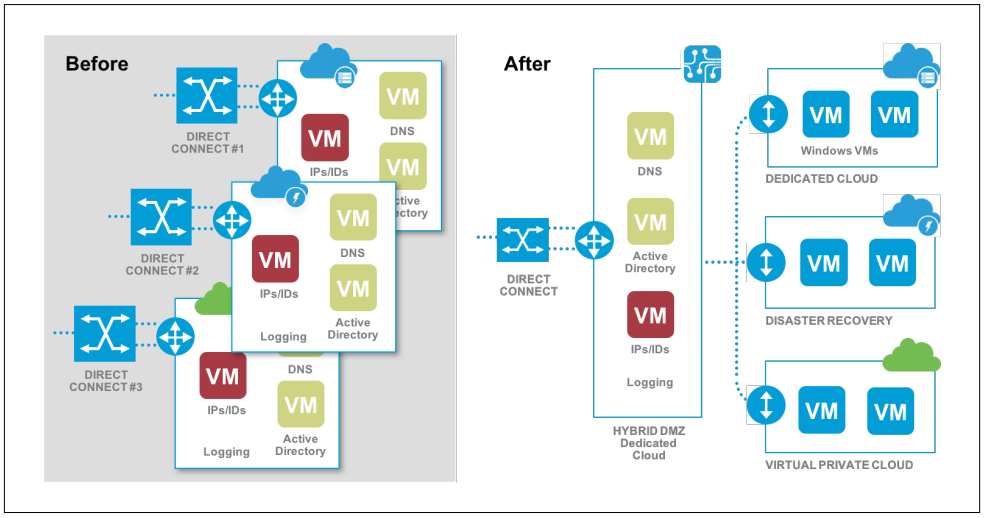

Figure 3: A multi-service vCloud Air deployment with and without Hybrid DMZ.

Reference Design #2: High Availability

Figure 4 shows an architecture where the customer plans to implement highly available Direct Connect circuits from two different vendors. In this case, there is only one Dedicated Cloud endpoint. However, the Hybrid DMZ is using the Advanced Networking Services capabilities of the DMZ layer to configure an active/standby configuration. More specifically, private routes are being advertised externally via eBGP, and internally via iBGP or OSPF. Using AS-Path Prepending, we can give route preference to one of the private lines, marking it as the active path. Then, if that line were to fail for any reason, the second Direct Connect circuit would quickly take over as the preferred path for all traffic, preventing any noticeable disruption to hybrid cloud communications.

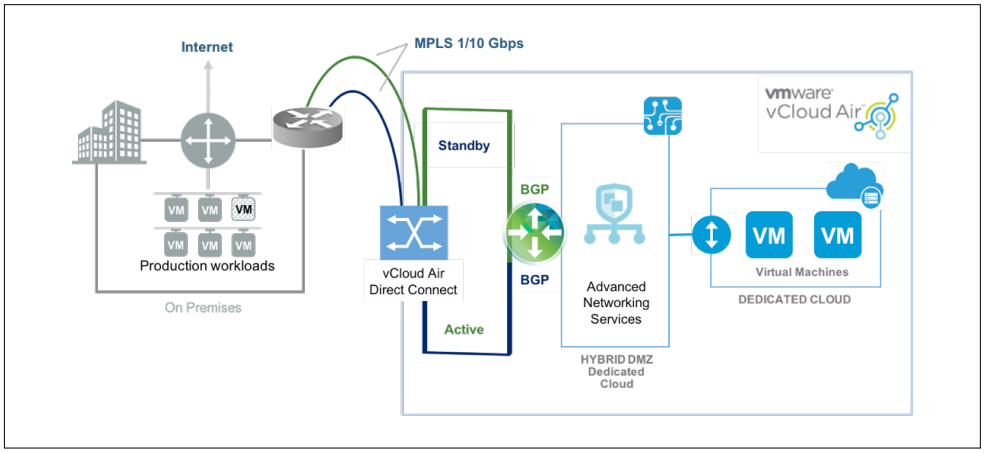

Figure 4: Example of using Hybrid DMZ to provide active/standby support into a single vCloud Air Dedicated Cloud.

Reference Design #3: North/South and East/West Isolation

This use case shows a secure configuration featuring micro-segmentation from Advanced Networking Services. It also demonstrates how the Hybrid DMZ can also host security software in a shared environment.

- The DMZ creates a centralized gate for all traffic to pass through, allowing you to efficiently place network security, optimization, or load-balancing appliances in a front-facing layer. In this way, not only does North/South (Ingress/Egress) traffic have to pass through your Advanced Networking Services Gateway, but it can also be forced through other essential management devices.
- East/West traffic can be further isolated through the use of micro-segmentation in each Advanced Networking Services-enabled cloud. This distributed firewall is deployed at the kernel level on selected VM vNics to silently allow or drop traffic between VMs based on object-driven policies.
- Each transit network is manually defined from the Hybrid DMZ to a selected backline cloud, which allows you to control the overall membership and connectivity of your individual instances. This is especially useful if you plan on having multiple separate sites connect to your cloud, since you can segregate access on a site-by-site basis.
- Internet access can be enabled in a controlled manner, so you can choose whether each Virtual Data Center can reach public addresses directly, or if they have to pass through your DMZ or On-Prem environments to do so.
- Even though a 1Gb or 10Gb Direct Connect line, or multiple lines, would be recommended, we can offer an eBGP IPSec tunnel across a public connection, giving you both a secure connection on a trusted protocol, and the management simplicity of a dynamic routing protocol.
- Backline clouds can be mixed and matched to provide you with the unique combination of services and capacity that you require.

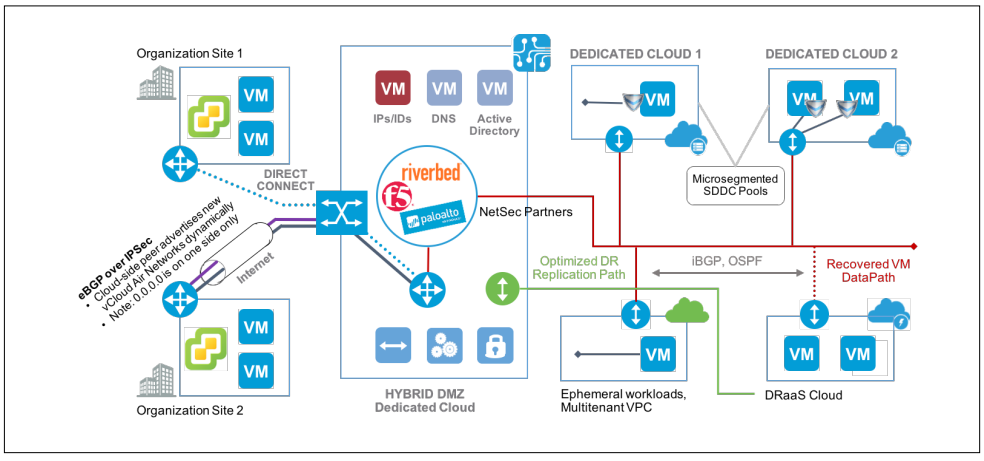

Figure 5: Security in the DMZ, with micro-segmentation and security devices

FIND OUT HOW TO BUY

The Cloud Computing Pricing Guide is an estimating tool that allows you to select the capacity and other features. http://vcloud.vmware.com/service-offering/pricing-guide

To purchase VMware products in North America, call 1-877-4VMWARE. Outside of North America, dial +1-650-427-5000.

Visit http://www.vmware.com/products or search online for an authorized reseller.

We offer several ways to purchase services according to your budget and business needs. You can pay for and consume specific services immediately through a purchase order, or separate your purchase and consumption decisions with the VMware Subscription Purchasing Program (SPP) or Hybrid Purchasing Program (HPP). You can learn about these and other programs at: https://my.vmware.com/web/vmware/spp-landing

You can pre-buy credits, then decide later which services you want to consume. These purchasing programs work similar to a gift card: SPP credits can be purchased either all at once or via a monthly commitment plan.

REFERENCES

[i] IDC Infographic Video: "Public Cloud for Data Extension and Replacement". Gary Chen. July 2016. https://youtu.be/G2JnWE_vwS0

[ii] IDC Infographic Video: "Public Cloud for Data Extension and Replacement". Gary Chen. July 2016. https://youtu.be/G2JnWE_vwS0

Summary

VMware vCloud Air is a true hybrid cloud designed to integrate seamlessly with traditional data centers. Organizations adopting vCloud Air add agility, flexibility, and scale to their existing data centers. Implementing Hybrid DMZ designs can help their cloud meet or exceed their security and performance expectations.

Next Steps

Try it Yourself

VMware Hands-on Labs are working hybrid cloud implementations available for free to registered users. These self-paced labs are running within minutes with full technical capabilities, allowing you to try vCloud Air's powerful networking and advanced features. To try it yourself, visit:
http://vcloud.vmware.com/explore-vcloud-air/try-cloud-computing-hol

Additional Resources

For more information about vCloud Air, visit the following sites:

- VMware vCloud Air Documentation Center
- vCloud Air Dedicated Cloud
- vCloud Air Virtual Private Cloud
- vCloud Air Disaster Recovery
- vCloud Air Advanced Networking Services
- vCloud Air Hybrid Cloud Manager
- vCloud Air Direct Connect

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

2/17