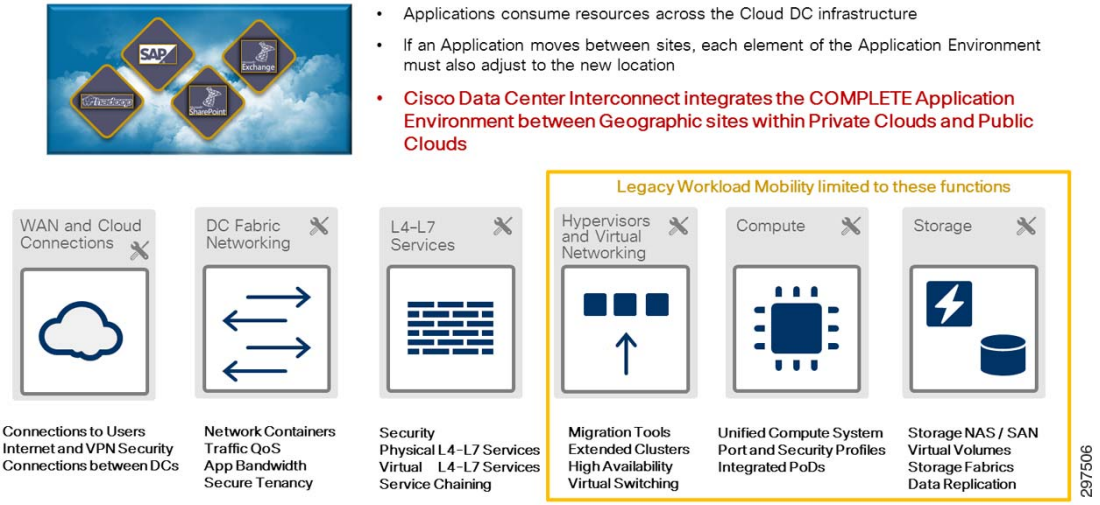
APPENDIX A

# Sample Test Results: Stateful Live Migration of Microsoft SharePoint

Most of today's business continuity and workload mobility solutions offer only basic VM mobility or recovery services between geographic sites aided by hypervisor tools and storage replication. These legacy solutions are limited to simple VM mobility or workload recovery of *completely virtual environments* hosted on the standard compute and storage stacks, as described in the Figure A-1. Unfortunately, most of today's business continuity and workload mobility solutions do not address the rest of the application environment including security, stateful L4-L7 services, network containers, tenancy, WAN connections to users, and most importantly both physical and virtual environments. What good does it do to move a VM to a new site if the rest of the application environment is left behind causing a potential security hole? If an application moves to a different data center in different city, each element of the application environment must react to that move, to preserve a secure application environment, services, and connections to external users. This section of the design guide provides an example of the next generation of Business Continuity and Workload Mobility and directly addresses multi-site Workload Mobility for the complete application environment. This section provides compelling test results to demonstrate the power of Cisco's Business Continuity and Workload Mobility Solution using a Microsoft SharePoint application.

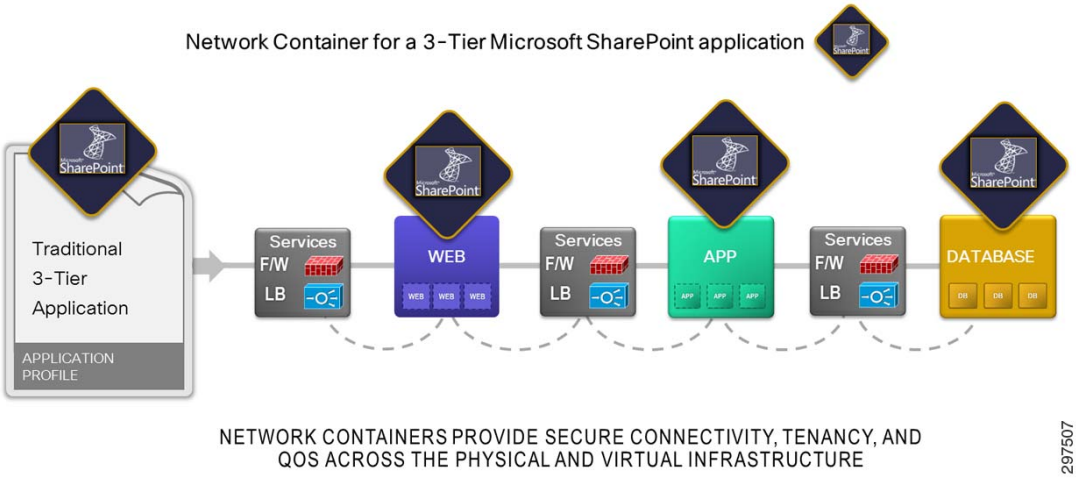
***Figure A-1 Legacy Business Continuity Solutions are Limited***



# Microsoft SharePoint Requires Stateful Services for each Application Tier

Business critical applications require a robust service environment to operate securely across the cloud. In the SharePoint example below, the application environment provides firewall and load balancing services for each tier of the SharePoint application; web, app, and database tiers. These services are stitched together using secure Network Containers that carve out a slice of resources across the data center for SharePoint, as described in Figure A-2. Network containers also provide SharePoint with secure connectivity to users, tenancy protection across the data center network, QoS for application packets, and reserved network capacity. Most Enterprises and SPs use a mix of physical and virtual resources including firewalls, load balancers, VPN termination, IDS, and network switching.

***Figure A-2 Microsoft SharePoint Application with Network Services***




Many of these services create stateful connections to users, therefore:

- If you perform a live migration of SharePoint to a new site, active stateful connections to firewalls and load balancers need to be preserved to maintain security and TCP connections to active users.

**Note** Broken user connections result in a service disruption for users which should be avoided.

- If the SharePoint application is moved to a new site, new user connections must be supported with identical security and services even though the application has relocated.

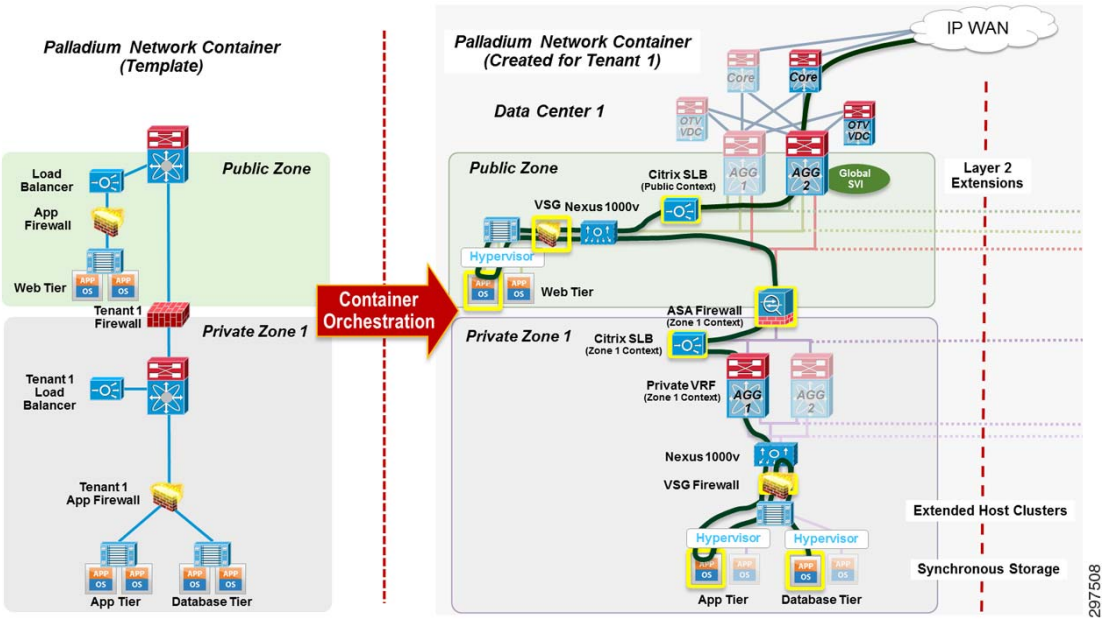
**Note** Network Services must be maintained across sites to avoid a potential security hole and a compromised data center.

# How Does Next-Gen Workload Mobility Actually Work?

We will illustrate how we performed live SharePoint migrations to a new site (75 km away) while maintaining security, stateful services, and user connections, automatically with minimal manual intervention.

Microsoft SharePoint was on-boarded onto our Private Cloud Data Center using one of the Cisco standard network containers, specifically a Palladium network container. The SharePoint Web, App, and Database tiers were deployed simply with service orchestration on the physical infrastructure of Data Center 1. Refer to Figure A-3 baseline topology.

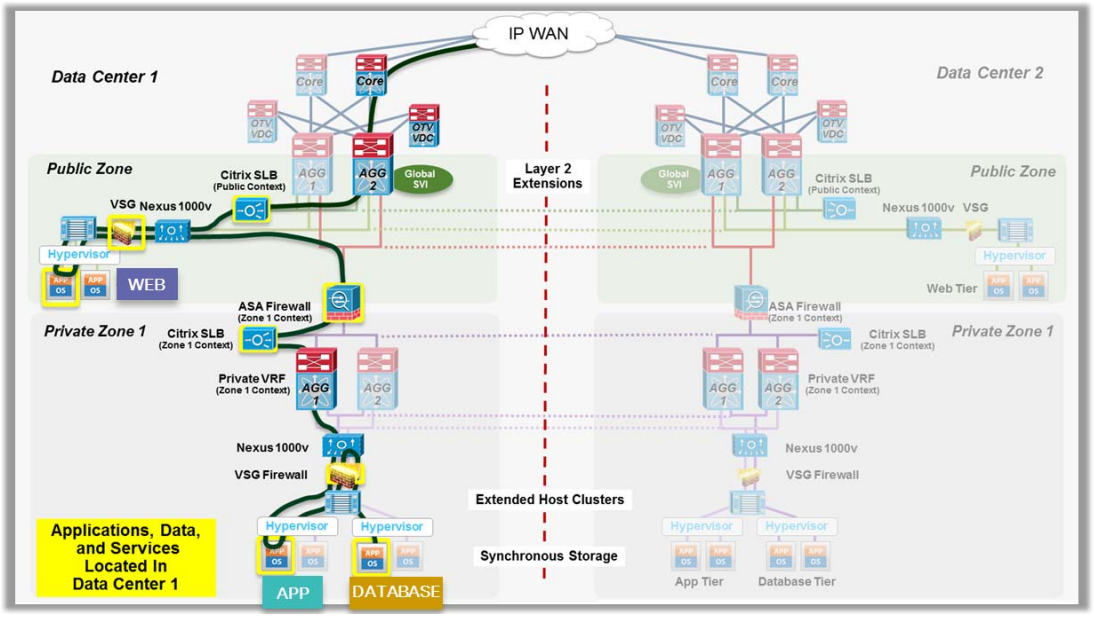
***Figure A-3 Creating a Secure Tenant for a 3-Tier Application***




- SharePoint Web Tier is in a Public Zone, and uses a virtual tenant firewall (VSG) and Citrix load balancer.
- SharePoint App Tier and Database Tier (SQL) are in a Protected Zone and use an ASA Firewall and Citrix SDX load balancer.
- Our validated design provides LAN extensions, extended clusters, secure network containers, virtual switching, and storage replication between Metro sites.

SharePoint is up and running in Data Center 1 as described in Figure A-4, supporting hundreds of users with secure connections. Now let's move SharePoint to a new site 75 km away while maintaining stateful services and without the users knowing it.

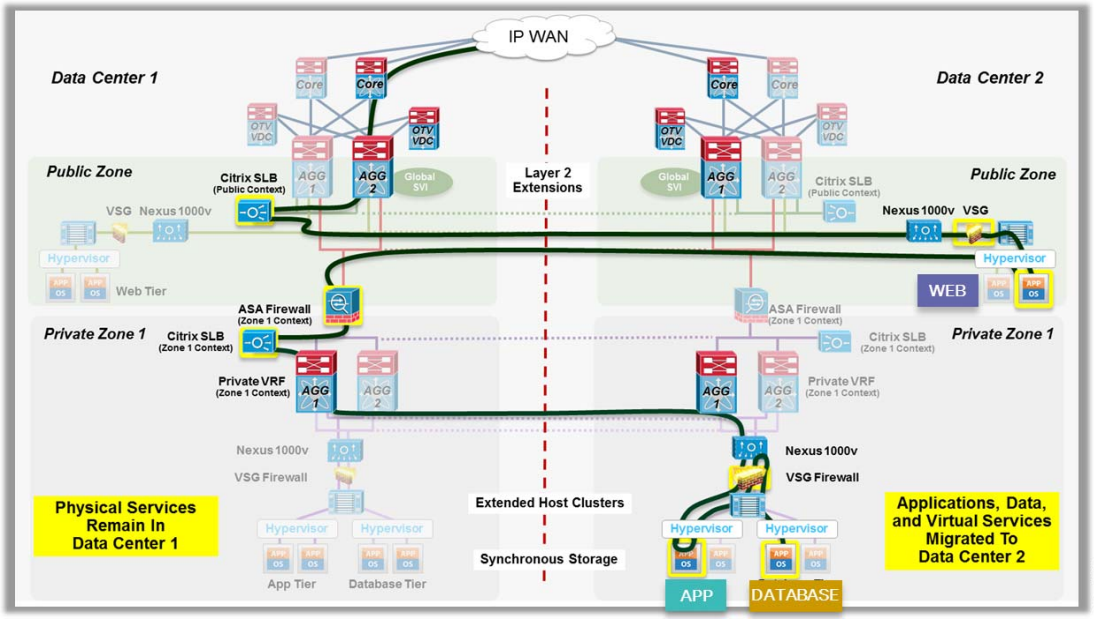
*Figure A-4 SharePoint Running Securely in Data Center 1*




**SharePoint Live Migration to Data Center 2, while maintaining secure user connections**

We performed a VMware Live vMotion of SharePoint (Web, App, Database) to new hosts in Data Center 2, described in Figure A-5. Data Center 2 is 75 km away. Our SharePoint migration had minimal disruption (2 seconds or less) and preserved all stateful services and all user connections across our validated multi-site Cloud.

*Figure A-5 SharePoint Applications Migrated Securely to Data Center 2*




A few highlights from our validated design are provided below.

- The virtual switch (Nexus 1000v), virtual firewall (VSG), and UCS automatically updated Port and Security Profiles at the new site, so our virtual switching and application firewalls were preserved without manual intervention.
- Layer 2 Extensions permit tromboning back to Data Center 1 to maintain stateful services for physical appliances (stateful firewall, load balancer), also without manual intervention.
- Our Network Container was automatically extended between Metro sites, maintaining security, tenancy, QoS, IP addressing, and user connections. SharePoint was discovered on the new host in Data Center 2 within seconds, using this extended Network Container.
- Microsoft Hyper-V hypervisors are also supported

Now let's move the rest of the network container to Data Center 2 in less than one second!

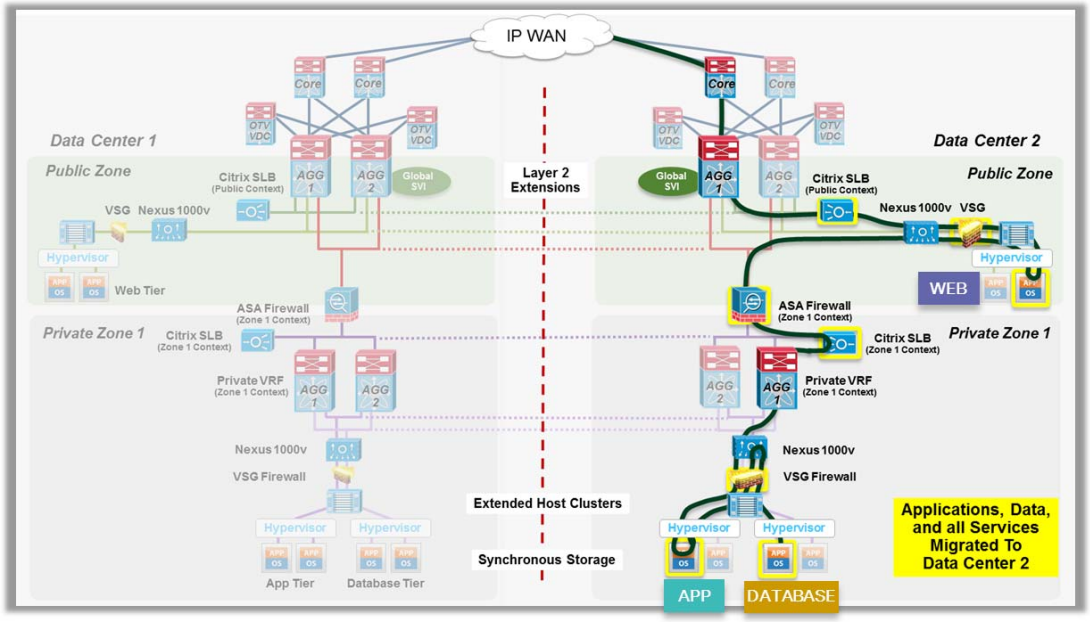
**Redirect users to a new Network Container in Data Center 2, in less than 1 second.**

With the aid of service orchestration, we simply created a new network container in Data Center 2. This new container included the same configuration, connections, and services (firewalls, load balancers) as the original container in Data Center 1. Once created, we simply redirected external users to the SharePoint application already running in Data Center 2, as described in Figure A-6.

**Note** The redirection of users happened in less than one second.

A simple routing update delivered through service orchestration performed the redirection. In this step, user connections were broken and new connections were re-established to the already running SharePoint application in less than one second.

***Figure A-6 SharePoint Applications and Network Services Migrated Securely to Data Center 2***




A few highlights from our validated design are provided below.

- Layer 2 Extensions allowed the preservation of IP Addressing for SharePoint applications and Services during migration. There is no need to "re-IP" your applications just because they've moved to a different city.

- The complete Network Container including physical and virtual resources was moved with minimal disruption to users (sub-second).
- Our Multi-site Cloud solution supports a typical Enterprise application environment, including both physical and virtual resources, with scaling for large and small private clouds.
- We also support Cold workload moves of less critical workloads that don't require these stringent stateful requirements.