Microsoft Hyper-V Network Virtualization Gateways - Fundamental Building Blocks of the Private Cloud

Windows Server 2012

Iron Networks White Paper
July2012

Introduction

There are a number of challenges that enterprise customers are facing nowadays as they move more of their resources to private and public clouds. Moving services to the cloud can often be a costly administrative exercise with lots of room for error, as well as risky in the eyes of the CISO with the concern of wanting to protect data and not risk a breach of isolation in a multi-tenant environment. Fortunately Microsoft has spent a lot of time addressing some of the challenges of moving to the cloud with their new private cloud solution which consists of Windows Server 2012, and Microsoft Systems Center 2012 Service Pack 1 which enables customers to rapidly deploy scalable and flexible cloud services in their private, public, or hybrid cloud scenarios. This paper addresses Hyper-V network virtualization, a critical component of this private cloud solution, and how rapid enablement is possible with the deployment of a turn-key Hyper-V Network Virtualization Gateway.

NVGRE Protocol and the Translation Gateway

Virtual Machines isolate server environments from the physical hardware, providing an enormous advantage in managing server performance, hardware utilization and reliability. Network Virtualization provides a similar capability, allowing multiple network segments to exist on a common physical network. Each virtual network is isolated, allowing overlapping IP address subnets. Virtual network segments can also be extended across WANs, where a single IP subnet may span across multiple sites including private data centers, private clouds and public cloud provider networks. VM instances can be moved from site to site without the need to update the IP address.

Virtual Networking allows multiple customer network segments to co-exist on the same physical network and hardware. This allows cloud providers to host any number of customer networks, and allows customers to maintain their own isolated IP address subnets and manage their own network addresses. Many IT services do not run on VM servers and remain attached to the physical networks or reside on remote networks. These services include desktops and printers, storage servers, desktop access from remote locations, services accessed across the Internet, and many more. To enable nodes Virtual Networks to communicate outside of the Virtual Network requires a gateway technology. This gateway service is provided by a Network Virtualization Gateway. Without this gateway, nodes inside a virtual network are isolated and cannot communicate to the outside world.

Network gateways reside between two or more networks. These networks have different technologies or protocols and a gateway allows the networks to interact and communicate. The Microsoft Network Virtualization is implemented inside the Microsoft Hyper-V technology platform. Hyper-V had the ability to encapsulate IP networks with the NVGRE protocol. Encapsulated IP networks are isolated and abstracted from physical networks, and thereby have additional capabilities and reduced constraints imposed by physical networks.

The Network Virtualization Gateway translates network packets encapsulated with NVGRE to non-encapsulated packets, and vice versa.

- Networks encapsulated with NVGRE are isolated from other networks
- Encapsulated packets are encoded with a unique ID

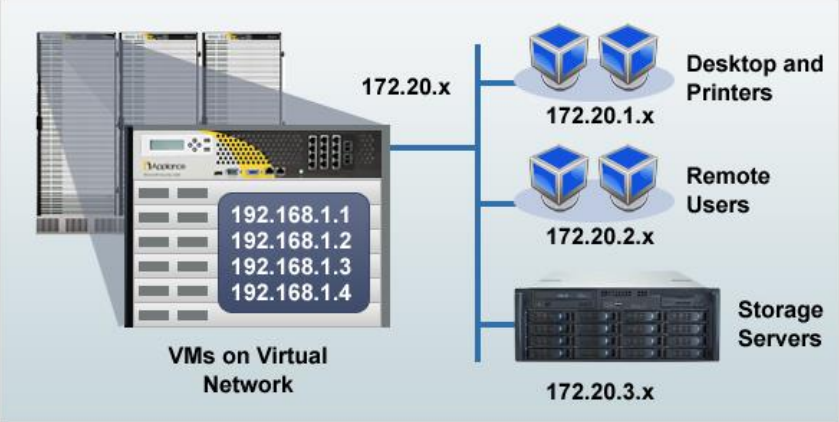
- The encapsulated packets are isolated from other encapsulated networks
- For multi-site cloud hosting facilities, customer networks are isolated from other customer networks
- The primary job of the gateway is to translate traffic between physical and virtual networks
- And route traffic to other virtual networks or resources on the physical network

Top of Rack Appliance –On-Premise gateway routes traffic within the data center

Virtual Machines inside a Virtual Network require access to resources residing on other virtual networks or residing on physical networks. One role of the gateway is to provide connectivity to resources outside of the virtual network segment.

Examples include:

- Desktops, printers or any device residing in the office environment
- Remote access for mobile users and devices – access to nodes inside a virtual network
- Virtual network nodes access to local resources such as storage servers, printers, and network equipment
- Provide access to the Internet for machines inside the virtual network segments



The Truly Green Datacenter – Power only the necessary equipment

By leveraging Hyper-V live migration and System Center Virtual Machine Manager policies, Virtual Networking enables virtual machines to move freely throughout your data center without re-addressing servers. This allows you to consolidate services and servers, and thereby powering down unused parts of the data center.

- Virtual Machines can be moved without shutting down the server
- Administrators do not have to change the address of running servers when migrating
- Virtual Network traffic between customer nodes within their own virtual network is routed automatically by the Gateway Appliance, allowing any customer node to be moved anywhere within the data center to any Hyper-V host
- Data centers can take advantage of off-peak hours to reduce operating costs and reduce wear on server hardware

Network Virtualization provides the technology to help make data centers more “green” and thereby reduce costs drastically.

Microsoft Systems Center –Virtual Networking Managed by VMM

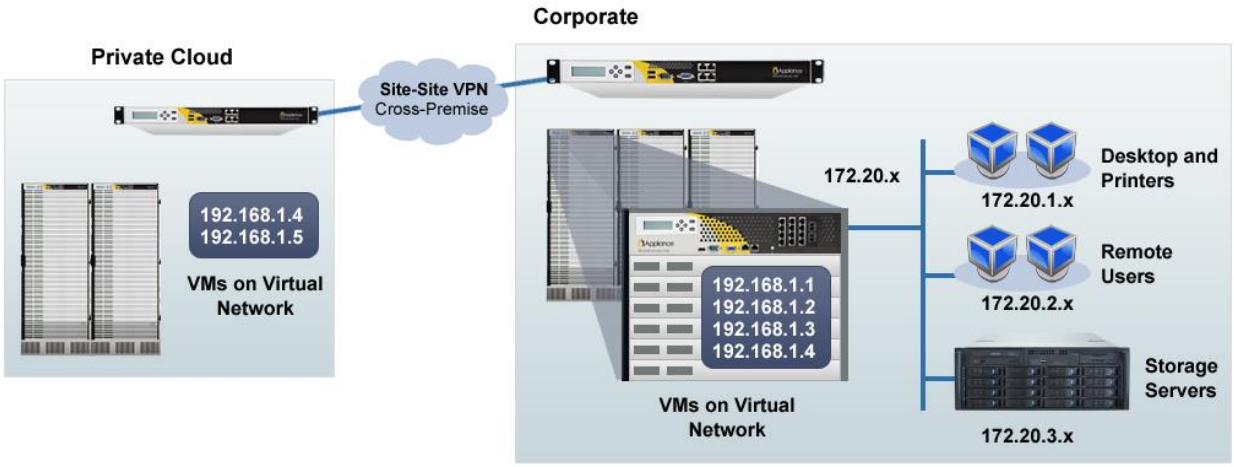
The Hyper-V infrastructure is managed by the Microsoft System Center Virtual Machine Manager. VMM is a unified management interface to create and manage virtual machines across multiple hosts. VMM has management access and visibility to every Hyper-V host and virtual machine, and is responsible for managing every aspect of the Hyper-V environment.
Since network virtualization is a component of Hyper-V, it is natural that VMM would also manage network virtualization. When you configure a virtual machine with VMM, that virtual machine can be assigned to a specific virtual network.

The Network Virtualization Gateway is integral to this infrastructure, and is managed by VMM as well. The gateway is responsible for routing traffic between virtual networks and between the virtual networks and the physical networks, so the gateway must maintain information about each virtual network and manage routing between networks. When a virtual machine is created or updated, VMM updates the routing and network topology contained within each of the gateway devices.

Multi-Site Private Clouds – Span multiple sites with a single IP subnet

The Iron Networks Virtual Networking Gateway combines encrypted VPN technologies with Virtual Networking technologies to provide a complete multi-site private cloud networking solution.

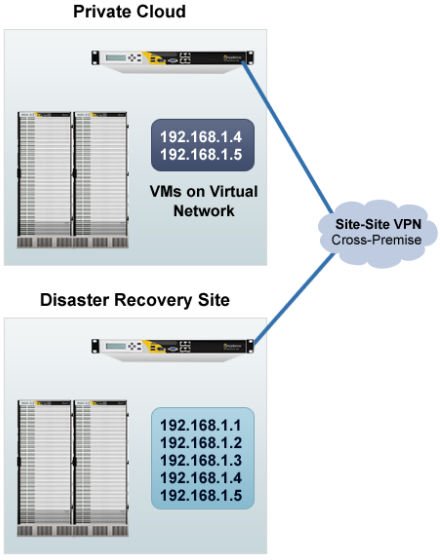
- With the built-in site-to-site cross-premise VPN, virtual networks communicate directly and seamlessly remote virtual networks
- VM nodes can move from site to site without changing IP addresses, network policies, security policies, Active Directory, DNS or network administration changes
- Expand to additional data centers or migrate to new data center facilities without the extensive planning, testing and risks associated with this operation.
    - Move and test a single node at a time
    - As if all nodes resides on a single network segment



Disaster Recovery –Enabling a “fail-over datacenter”

One of the difficulties of designing a disaster recovery data center and testing a disaster recovery plan is managing the duplicate and disparate network segments. With the multi-site capabilities of the Iron Networks Network Virtualization Gateway, services can be swung over to a recovery site and back again with no network disruption or reconfigurations.

- Some or all services can be enabled or disabled at either the primary or the recovery location almost instantly
- A single node can be lighted up at the recovery center, or the entire data center can be in stand-by mode and enabled
    - No network address updates are required
    - End users are unaffected from a network standpoint
- Disaster Recovery tests can be performed simply and without the much of the risk associated with doing network reconfigurations and backing these updates out at the end of the tests

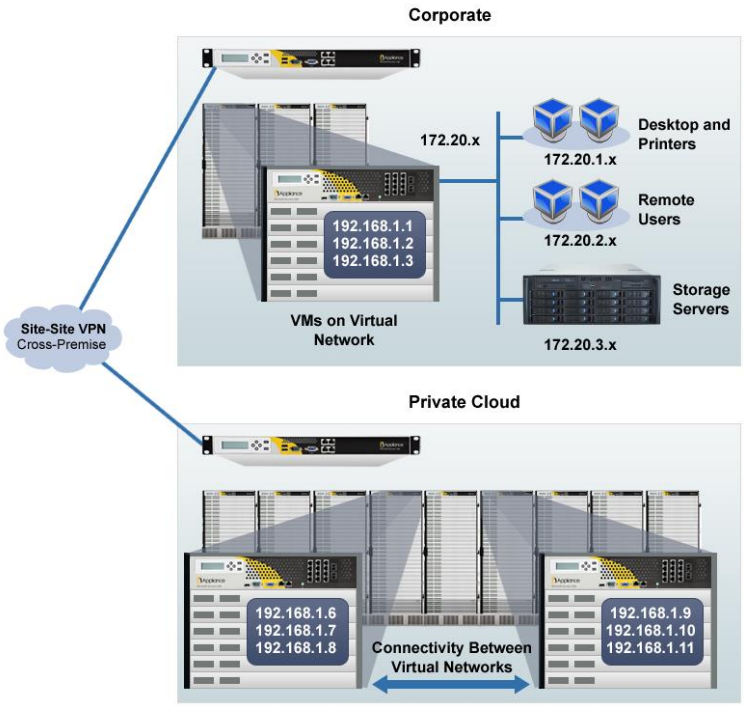


- The complexities of WAN Load Balancers and other network fail-over technologies are no longer required

Hybrid Cloud – Migrating services to the Public Cloud made simple

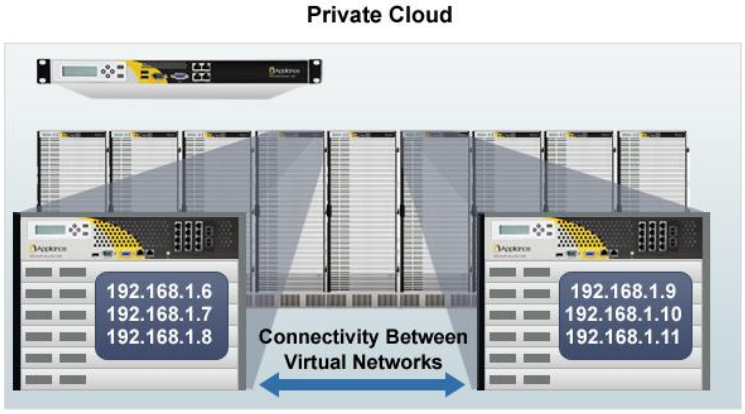
Virtual Networking allows Cloud Providers to provide customers with their own network spaces. IP address overlapping with other customer networks are not an issue

- IP network subnets can be shared between customer networks and with cloud providers
- Virtual Machines can be migrated to a cloud provider, one at a time without readdressing nodes, updating security policies or updating network management systems.
- Customers can utilize multiple public providers
- Customers can migrate to new providers as desired without a massive and disruptive migration
- Resources can spread across remote locations or kept local as is required for performance or security concerns



Public Cloud – Multi-Tenant solutions for Cloud Provider

The Iron Networks Network Virtualization appliance solutions are designed ground up for the performance, high availability and reliability requirements of Cloud Providers.

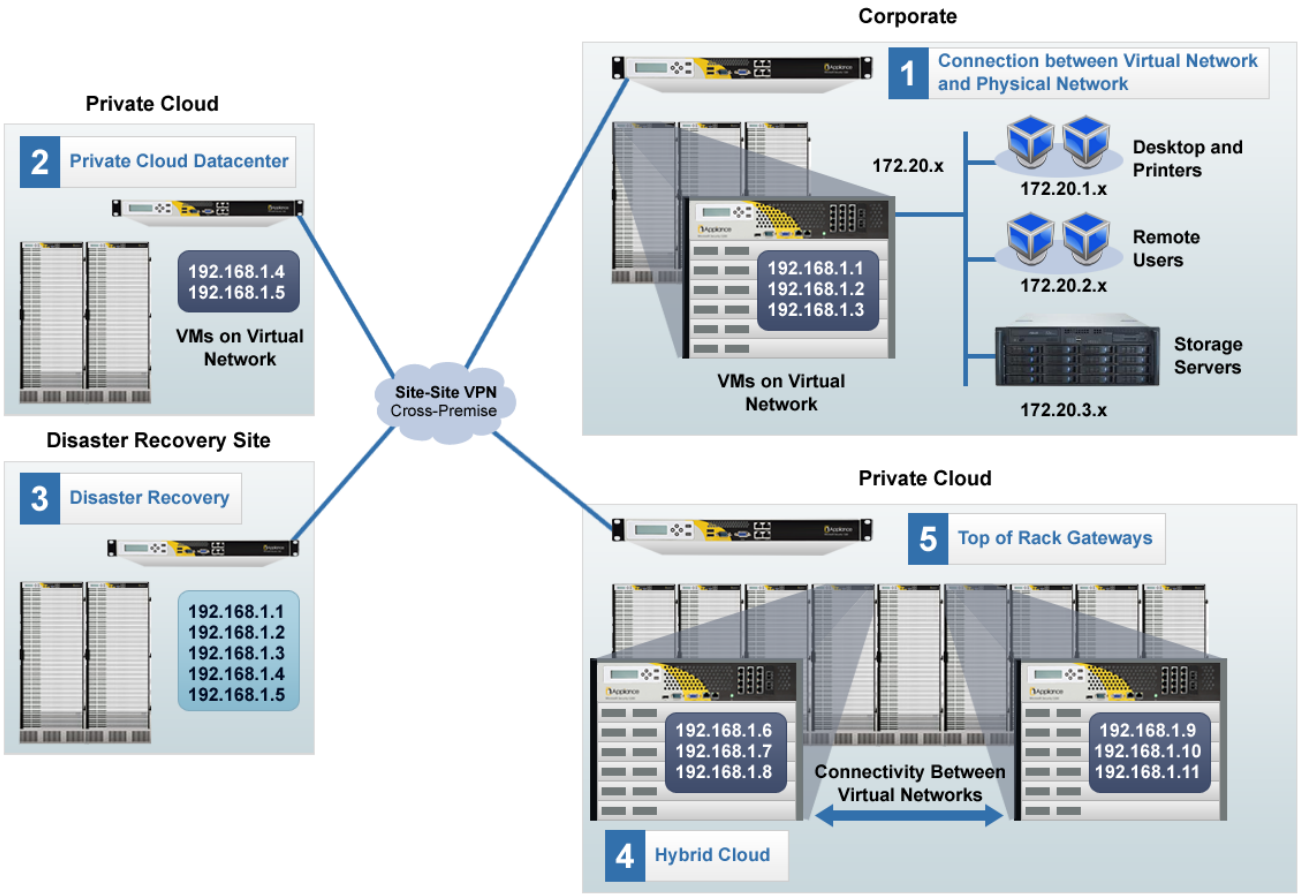


- There are no limit on the number of customer networks supported
- Cloud customers can be provided with their own virtual network space to manage as they desire
- Customer VM servers can be hosted on any hardware server in the data center
- Top of Rack appliances provide the high performance requirements for unlimited number of hosted servers and virtual machines.
    - The Top-of-Rack appliance provides communications between customer nodes
    - and a gateway for local services provided by the cloud provider, such as storage
    - and a network solution to route virtual network traffic to the Internet

Summary

Network Virtualization is an evolutionary step in network technology, providing ease of management and advanced capabilities. The Network Virtualization Gateway plays an integral role in deploying this technology as it is critical entry point between the physical network and virtual network. This document describes five major technology advancements:

1. Gateway bridging virtual networks and physical networks
2. Multi-site Private Clouds
3. Disaster Recovery site connectivity
4. Hybrid Cloud
5. Public Cloud provider network solution



Iron Networks, Inc.
980 Mission Court, Fremont, CA 94539, USA
Phone: +(1) 408-895-5000 (Local), +(1) 877-895-6277 (US-Toll Free), +(1) 408-895-5000 (International)
Fax: +(1) 408-943-8222/8101 Email: info@ironnetworks.com Website: www.ironnetworks.com