Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to publish it as an RFC and to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on April 26, 2012.
Abstract

This contribution addresses the service providers’ requirements to support VPN-Oriented data center services. It describes the characteristics and the framework of VPN-oriented data center services and specifies the requirements on how to maintain and manage the virtual resources within data center resources and the supporting network infrastructures for those services.

Table of Contents

1. Introduction....................................................3
2. Conventions used in this document............................4
3. Service definition and requirements............................4
   3.1. VPN-oriented data center computing services.............4
   3.1.1. VPN-oriented data center computer service requirements...4
   3.2. VPN-oriented data center storage services...............5
   3.2.1. VPN-oriented data center storage services requirements...5
4. Requirements for data center networks in supporting VDCS......6
   4.1. Requirements for extending VPNs into data center using VPN gateways..........................................................6
   4.2. Requirements for extending VPNs into data center using intra-data center VPN......................................................8
5. Data center resource management requirements for VDCS........8
6. Security requirements...........................................9
7. Other requirements...............................................9
8. References...................................................10
1. Introduction

Layer 2 and 3 VPN services offer secure and logically dedicated reachability among multiple sites for enterprises. VPN-oriented data center service is for those VPN customers who want to offload some dedicated user data center operations such as software, compute, and storage, to the shared carrier data centers. Those customers often do not want to use public Internet as the primary network accessing and handling the traffic between the customer (user and user data centers) and the carrier data centers. Instead, they would prefer to use the carrier data center as a natural extension of the VPN they are already using, realizing the benefits of a multi-tenant data center while retaining as much control as possible. For example, they want to maintain the restrictive control on what and how the virtualized data center resources, e.g., computing power, disk space, and/or application licenses, can be shared.

VPN-Oriented Data center Services allow the VPN services to be extended into carrier data centers and to control the virtual resource sharing functions. As a carrier, a VPN-Oriented data center service product may be offered globally across multiple data centers. Some of the data centers may be owned by the cloud service provider, while others may be owned by a partner of the service provider and/or an enterprise user. In addition, multiple VPN-oriented data center Service products (e.g. SaaS and PaaS) can be offered from the same data center.

VPN-Oriented data center services differentiate it from other carrier data center services in the following aspects:

- Strictly maintaining the secure, reliable, and logical isolation characteristics of VPN for the end-to-end services provided.
- Making the traditional data center services (like computing, storage space, or application licenses) as additional attributes attached to VPNs.
- VPN is aware of how and what data center resources are associated with the VPN.
This draft describes the characteristics of those services, the service requirements, and the corresponding requirements to data center networks. It also describes a list of the problems that this service is causing to the network provider/operator, especially for the existing VPN customers. These issues must be addressed in order for service providers to facilitate the addition of virtualized services to the VPNs of existing customers.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. Service definitions and requirements

3.1. Virtual Private Computing Service (VPCS)

This refers to Virtual Machines (VMs) and/or physical servers in a virtualized carrier data center being attached to a customer VPN. It is also known as National Institute of Science and Technology (NIST)’s Infrastructure-as-a-Service (IssS) being attached to a customer VPN. The customer can choose different properties on the computing power, preference on which data center to host those servers, and etc.

3.1.1. Virtual private computing services requirements

These requirements apply to all VPN-oriented data center services defined in this draft unless specified otherwise.

   o Any virtualized carrier data center providing VPCS SHALL be able to automatically provision and/or change the resources associated with the VM/ Servers based on the signaled messages through the VPN. For example, the resources CAN be bandwidth, amount of memory, and/or CPU cycles associated with the VMs.

   o VPN customers SHALL be able to automatically instantiate or remove Virtual Machines (VMs) inside the provider’s DC using inband signaling requests sent by the user’s host (VM/server).
3. Virtual private network (VPN) service (VPN)

- VPN customers SHOULD be able to move VMs among customer private data centers and carrier data centers based on their own load balancing criteria and algorithm.
- VPN customers SHALL be able to monitor, log, and track all VM/server related usage information on per VPN basis.
- VPN customers SHALL be able to control if and how VM mobility can occur.

3.2. Virtual private storage service (VPSS)

This refers to disk space, either virtual or actual blocks of hard drives in data centers, being added to a customer’s VPN.

3.2.1. VPN-oriented data center storage service requirements

- The VPN customer SHOULD be able to choose different content replication properties. For example, the customer can control if the content has to be replicated locally or has to be replicated at a geographically different location (identifiable by the customer if needed and subject to latency constraint); if the storage has to be co-located with certain VMs/hosts; or which VMs/hosts have access to the content, and etc.
- These storage properties SHOULD be associated with the VPN. Any data center providing the storage space for a VPN SHOULD be able to automatically provision or change the required storage space based on the properties associated with the VPN.
- The VPN customer SHOULD be able to automatically add disc space or remove disc space to the VPN’s associated storage through the changing of the VPN properties.
- The VPN customer SHOULD have the ability to specify the stored content life cycle management properties. Those properties include but not limited to how long the stored content shall be stored and how it should be erased/deleted.
- Control of whether data is encrypted.
- Specify required access speed for a storage hierarchy.
4. Requirements for Data Center networks in support of VPN-Oriented Data center Services

The success of VPN services in the enterprise and the government world is largely due to its ability to virtually segregate the customer traffic at layer 2 and layer 3. The lower the layer that segregation can be maintained, the safer it is for the customers from security and privacy perspectives. Today’s Data Centers use VLANs to segregate servers and traffic from different customers. Since each customer usually needs multiple service zones to place different applications, each customer usually needs multiple VLANs. Even small data centers today can have thousands of VLANs. Therefore, pure VLAN segregation is not enough for large data centers. In addition, since carrier data center resources can be viewed as added attributes to VPNs, traffic segregation per VPN becomes an essential requirement to VPN-oriented data center services because of its ability to control the data center virtual resources’ assignments, thus ensuring end-to-end resource allocation for service level performance insurance as well as manageability.

4.1. Requirement for extending VPNs into data center networks using VPN gateways

When a data center does not use L2VPN or L3VPN as the intra-data center network, but still wants to provide the VPN-oriented data center services for external VPN customers, a VPN gateway function can be added to the data center networks to extend the external VPNs into the data center networks and to connect with the VMs and virtual storage. (Note that L2/3 data center network technology used can include TRILL, PBB, SPB, OpenFlow, STP, etc.) The VPN gateway function has to meet the following requirements:

- Each external L2/L3VPN SHALL be given a unique Identification (ID), and the traffic separation within the data center SHALL be maintained per ID.
- Each data center Service associated with a VPN SHALL be transmitted over an unique set of intra-data center network connections (logical or physical).
- The VPN gateway SHOULD maintain a record and the mapping of virtual and physical data center resources to physical/logical connections associated with each specific VPN running the VPN-oriented data center services.
- The carrier and the customer SHALL be able to monitor the resource assignment and usage per VPN per service.
The customer SHOULD be able to dynamically re-configure the data center resources assignment and allocation per services and/or per VM through the re-configuration of its VPN properties.

Beyond L2/L3 reachability, VPN gateway SHALL support multiple services per VPN.

VPN gateway SHOULD have the capability to differentiate QoS within the VPN on per service basis. For example, storage service may have higher QoS requirement than computing service.

VPN gateway SHOULD support multiple external VPN instances and SHOULD be able to map them to the associated services.

VPN gateway SHALL maintain the reportable record of how traffic separation per VPN is achieved through the data center network.

Each external VPN SHALL be given a unique Identification (ID), and the traffic separation within the data center SHALL be maintained per ID.

The VPN gateway SHOULD maintain a record and the mapping of virtual and physical data center resources to physical/logical connections associated with each specific VPN running the VPN-oriented data center services.

The VPN gateway SHOULD be able to control the traffic flow and assign the dedicated virtual resources accordingly.

The carrier and the customer SHALL be able to monitor the resource assignment and usage per VPN per service.

The customer SHOULD be able to dynamically re-configure the data center resources assignment and allocation per services and/or per VM through the re-configuration of its VPN properties.

VPN gateway SHALL support multiple services per VPN.

VPN gateway SHOULD have the capability to differentiate QoS within the VPN on per service basis. For example, storage service may have higher QoS requirement than computing service.

VPN gateway SHOULD support multiple external VPN instances and SHOULD be able to map them to the associated services.

VPN gateway SHALL maintain the reportable record of how traffic separation per VPN is achieved through the data center network. VPN Gateway SHOULD be able to allocated intra-data center network resources according to external VPN
network’s requirements dynamically for bandwidth, QoS and traffic engineering purpose.

4.2. Requirement for extending VPNs into data center networks using intra-data center VPN

When a L2/3 VPN is used as the network technology inside the data center, each external VPN SHALL be mapped to a unique internal VPN.

5. Data Center Resource Management Requirements for VPN-oriented Data center Services

Today, data center server resources are managed by data center servers’ administrators or management systems, and supported by hypervisors on the servers. This process is invisible to the underlying networks. The data center management functions include managing servers, instantiating hosts to VMs, managing disk space, and etc.

Traffic loading and balancing and QoS assignments for data center networks are not easily considered by some Data Center server administration systems. Therefore, there is an interworking gap between the networks and the Data Center’s server administration systems. This gap needs to be filled in order for the VPN-oriented data center service to operate.

o The resources in data center MUST be partitioned per VPN.

o The data center service orchestration system SHALL have the ability to dedicate a specific block of disk space per services per VPN. The dedicated block of disk space CAN be maintained permanently or temporarily per VPN requirement, controlled by the associated properties of VPN.

o The carrier and the VPN customer SHALL be able to monitor the dedicated block of disk space per VPN per services.

o If a VPN specifies its associated storage space to be accessible only by certain hosts, the VPN customer SHALL have the ability to indicate the mechanism used to prevent the unwanted data retrieval for the block of disk space after it is no longer used by the VPN, before it can be re-used by other parties.
6. Security Requirements

- The VPN-Oriented Data center Service SHOULD support a variety of security measures in securing tenancy of virtual resources such as resource locking, containment, authentication, access control, encryption, integrity measure, and etc.

- The VPN-Oriented Data center Service SHOULD allow the security to be configured end-to-end on a per-VPN/per-service/per-user basis. For example, the Data center Systems SHOULD be able to resource-lock resources such as memory, and also SHOULD be able provide a cleaning function to insure confidentiality before being reallocated.

- The VPN-Oriented Data center Service SHOULD be able to specify an authentication mechanism based for both header and payload. Encryption algorithm CAN also be specified to provide additional security.

- Security boundaries CAN be specified and created per VPN to maintain domains of TRUSTED, UNTRUSTED, and Hybrid. Within each domain access control, additional techniques MAY be specified to secure resources and administrative domains.

7. Other Requirements

- The VPN-Oriented Data center Service SHALL support host-to-host configuration exchanges via inband signaling.
The VPN-Oriented data center service solution MUST have sufficient OAM mechanisms in place to allow consistent end-to-end management of the solution in existing deployed networks. The solution SHOULD use existing protocols (e.g., IEEE 802.1ag, ITU-T Y.1731, BFD) wherever possible to facilitate interoperability with existing OAM deployments.

8. References

Thanks to Paul Unbehagen, Linda Dunbar, Bhumip Khasnabish, LiZhong Jin, Norival Figueira, and Zhengping You for review this draft and providing valuable inputs.

Authors’ Addresses

Ning So
Verizon Inc.
2400 N. Glenville Ave.,
Richardson, TX 75082
ning.so@verizon.com

Dave McDysan
Verizon Inc.
22001 Loudoun County PKWY.
Ashburn, VA 20147
Dave.mcdysan@verizon.com

Henry Yu
TW Telecom
10475 Park Meadows Dr.
Littleton, CO 80124
Henry.yu@twtelecom.com

John M. Heinz
CenturyLink
600 New Century PKWY
KSNCAA0420-4B116
New Century, KS 66031
john.m.heinz@centurylink.com

9. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.