Protecting VMs in a Multi-Tenancy Environment

Prepared by:

XenServer Engineering

CITRIX®

www.citrix.com

Table of Contents

1. Executive Summary

Segregation of network data is a basic business requirement when deploying applications, desktops or virtual machines in an environment where you cannot trust all users of the network. This is an inherent issue in public and private clouds because of the lack of physical segregation of systems. XenServer, and cloud infrastructures built on XenServer, provide the high level of protection needed by organisations and regulatory authorities. The choice of technologies which are tried and trusted in global organizations, have been improved and extended in XenServer 6.1.0. This White Paper highlights the VLAN improvements, VM aware multi-tenancy extensions, and the updated Open vSwitch. XenServer is a key enabler for Software Defined Networks: the virtualised network infrastructure that many cloud service providers and large enterprises are now deploying.

1.1. Audience

This white paper is aimed at those who are interested in using a public cloud to host their applications, desktops or multi-purpose virtual machines (VMs), and are looking for a greater understanding of the protections available to ensure their network traffic can't get intercepted or confused with that of other users of that cloud.

Businesses using a private cloud to host VMs from distinct functional groups or sub-organizations are subject to the same concerns, and this white paper is equally applicable to them.

The target reader will have an understanding of the technical issues around networking and VM segregation in a hosted environment.

2. Introduction

Security is often the primary concern voiced by organisations and business units when considering a move to using a cloud hosted solution. All organisations need to be sure that their resources and data are secure, and that other organisations cannot access them without authorisation. Of particular concern is network data: it must be possible to secure data pathways when sharing any networking resource (e.g. physical switches or network interface cards) to prevent malicious or accidental unauthorized access or denials of service to ensure that whilst also you need to be certain that there is no chance that network data that was destined for your VMs does not end up being visible to them, and that there is no opportunity for them to snoop on data either entering or exiting your VMs.

Segregation of data is paramount, and this white paper addresses a number of ways in which Citrix XenServer 6.1.0 has provided even greater protection in the network sphere.

2.1. Specific concerns

There are many examples of situations in which network data from one organisation or department needs to be segregated. These might include:

- Large enterprises needing to isolate HR records, finance, customer credit card details and Intellectual Property assets;
- Organisations ensuring separation of business unit applications and data;
- Outsourced development requiring separate areas for each development activity;
- Healthcare organisations with statutory responsibilities to ensure patient record confidentiality;
- Universities needing to partition examinations, enrolment details and commercial research from their other teaching and research activities;
- Telcos and network service providers having to separate billing, CRM, payment systems, resellers portals and application hosting environments;
- Financial organisations needing to isolate client details and partition trading, wholesale and retail banking for regulatory reasons;
- Governments having the requirement to partition records for taxation, welfare, healthcare, education and other departments.
- Production environments need to be logically separated from Development and Test infrastructures.
- Publically facing web services must be separated from systems containing confidential data.

In all of the cases noted above, the physical or virtual system performing the different activities must be isolated: XenServer uses hypervisor and memory separation techniques to ensure virtual machine isolation even when sharing the same physical host. However, as soon as these systems send data over a shared network the security of that data is vulnerable. Administrators and auditors need to be confident that network traffic can only be accessed by the intended recipient. There are two general approaches by which rogue, or malicious, actors can attempt to disrupt network traffic for which they are not authorised: interception and impersonation.

Interception is when a third party reads data intended for some other recipient, whether it is incoming or outgoing: it is sometimes referred to as *sniffing*, and can take place either on a machine which is hosting a set of VMs, or any of the switches in the network between the parties communicating.

Impersonation or *spoofing* is when a third party masquerades as another, with the intention of receiving data intended for another party, fraudulently accessing another system, or disrupting the transmission of data. Impersonation can occur at either the Ethernet layer (*ARP spoofing*) or at the IP layer (*IP spoofing*); both can cause network traffic to be misrouted or lost.

- ARP spoofing: the aim is to associate the attacker's MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly sent to the attacker instead.
- IP spoofing: the attacker creates IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

Both types of spoofing can occur due to incorrect configuration by system administrators, causing unintentional, but often equally disastrous, consequences.

3. Preventing Vulnerabilities with XenServer

XenServer 6.1.0 contains enhanced controls which simplify and improve protection against both types of attacks – interception and impersonation. These features are explained in more detail below. There are also further measures which can be applied using advanced techniques which are briefly described in the final part of this section.

3.1. VLAN Improvements

Virtual Large Area Networks (VLANs) are the industry standard technique to segregate network traffic, thus preventing interception by unauthorised parties. Almost all physical switch vendors support the technology, with a maximum of 4,096 separate VLANs on a single Layer 2 (L2) network. All packets from each system on the VLAN are tagged so that all switches on the network know that they should be kept distinct. This tagging can also be performed by XenServer, allowing network segregation of VMs on the same host. The operation of the VLAN is therefore transparent to the 'bare metal' machines and VMs on the VLAN.

XenServer 6.1.0 does not introduce VLANs; XenServer can be configured to tag traffic from any VM with any legal VLAN assignment, traffic from external sources tagged with the correct VMs VLAN will have the tag stripped transparently, before the traffic passes to the VM.

Two major improvements in XenServer 6.1.0:

1. **Scalability**: In XenServer 6.1.0, significant improvement has been made in performance when using many VLANs in the same pool. Although previously supported, it is now practical to route thousands of VLANs.

2. **Trunking**: XenServer 6.1.0 can be configured to pass tagged traffic to VMs. This allows advanced networking capabilities to be provided by virtual appliances, for example software VPNs and software routers.

3.2. Multi-Tenancy Extensions

Security extensions in the XenServer networking stack enable administrators to protect against impersonation and interception as discussed above. In the XenServer 6.1.0 release, these extensions are enabled and configured by additional persistent VM configuration options. This means that VMs remain protected during migration, power events and other pool administrative tasks.

The new multi-tenancy extensions allow XenServer administrators to lock a virtual switch port to a MAC address and a list of IPv4 or IPv6 addresses. This means that when these extensions are deployed, VMs cannot:

1. **Impersonate** any other VM;

2. **Intercept** traffic intended for any other VM.

XenServer will ensure that traffic from a VM on a locked port will be dropped if does not come from the MAC address and IPv4/IPv6 that are associated with that port, thereby protecting all other VMs on that host from malicious attacks from that VM.

3.3. Open vSwitch

XenServer 6.1.0 also includes an improved version of the Open vSwitch (OVS)[1] – an *OpenFlow*[2]-compliant virtual switch. This component provides Switch functionality to XenServer, including:

- the ability to create and maintain fine-grained routing rules on a host-per-host level;
- manage access control lists on a MAC or IPv4/IPv6 basis;
- create GRE tunnels between XenServer hosts and other enabled switches;

This functionality allows XenServer hosts to be used as part of a larger, software-defined network (SDN).

Although administrators do not need to interact with the OVS directly in order to take advantage of the capabilities list above, an increasing number of cloud services providers and large enterprises are beginning to leverage the advantages offered by SDNs.

4. Conclusion

XenServer 6.1.0 provides additional protection for organisations who wish to ensure high levels of segregation for their network data, whether between departments in a private cloud, or between different customers in a public cloud. Use of VLANs – now better supported in XenServer 6.1.0 – and multi-tenancy extensions allows organisations to enjoy the levels of protection that they require across multiple use cases. Further advanced techniques using the Open vSwitch which is part of XenServer 6.1.0, allow even greater control and integration of XenServer into the virtualised network infrastructure that many cloud service providers and large enterprises are now deploying.

[1] To learn more about the Open vSwitch see, http://openvswitch.org/

[2] To learn more about OpenFlow see, http://www.openflow.org/wp/learnmore/

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com

The copyright in this report and all other works of authorship and all developments made, conceived, created, discovered, invented or reduced to practice in the performance of work during this engagement are and shall remain the sole and absolute property of Citrix, subject to a worldwide, non-exclusive license to you for your internal distribution and use as intended hereunder. No license to Citrix products is granted herein. Citrix products must be licensed separately. Citrix warrants that the services have been performed in a professional and workman-like manner using generally accepted industry standards and practices. Your exclusive remedy for breach of this warranty shall be timely re-performance of the work by Citrix such that the warranty is met. THE WARRANTY ABOVE IS EXCLUSIVE AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICES OR PRODUCTS PROVIDED UNDER THIS AGREEMENT, THE PERFORMANCE OF MATERIALS OR PROCESSES DEVELOPED OR PROVIDED UNDER THIS AGREEMENT, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM, AND ALL IMPLIED WARRANTIES OF MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, OR AGAINST INFRINGEMENT. Citrix' liability to you with respect to any services rendered shall be limited to the amount actually paid by you. IN NO EVENT SHALL EITHER PARTY BY LIABLE TO THE OTHER PARTY HEREUNDER FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT OR PUNITIVE DAMAGES (INCLUDING BUT NOT LIMITED TO LOST PROFITS) REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, OR STRICT LIABILITY. Disputes regarding this engagement shall be governed by the internal laws of the State of Florida.

851 West Cypress Creek Road   Fort Lauderdale, FL 33309   954-267-3000   http://www.citrix.com