nvo3
Internet-Draft
Intended status: Informational
Expires: December 22, 2012

Y. Wei, Ed.
S. Zhang
ZTE Corporation

June 20, 2012

NVO3 Security Framework
draft-wei-nvo3-security-framework-00

Abstract

This document provides a security framework for overlay based network virtualization. It describes the security reference model, the security threats and security requirements.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 22, 2012.

Copyright Notice

Table of Contents

1. Introduction

Security is one of important factors in the envrionment of cloud computing. This issue should be addressed for the overlay based network virtualization, which supports multi-tenancy in data center.

Security considerations have already been provided in each of the individual document on framework, control plane and data plane requirements of data center network virtualization over Layer 3(NVO3). [I-D.lasserre-nvo3-framework] describes that the tenant to overlay mapping function can introduce significant security risks if appropriate security mechanisms are not used for protocol. [I-D.kreeger-nvo3-overlay-cp] describes that the protocol should protect the integrity of the mapping, and overlay exposes virtual networks to attacks on the underlying network such as traffic injection. [I-D.bitar-lasserre-nvo3-dp-reqs] also describes the security risks of the tenant to overlay mapping function.

The motivation of this document is to provide a general and consistent security description for NVO3, and to complement with security considerations in the current documents. This document is organized as follows. Section 3 describes the security reference model for NVO3. Section 4 describes the security threats under the security model. Section 5 addresses the security requirements corresponding to the security issues.

2. Terminology

This document introduces no new terminology. For reader's convenience, this document repeats some of them defined in [I-D.lasserre-nvo3-framework] [I-D.kreeger-nvo3-overlay-cp] [I-D.bitar-lasserre-nvo3-dp-reqs].

Tenant End System(TES): An end system of a tenant, which can be for instance a virtual machine(VM), a non-virtualized server, or a

physical appliance. A TES attaches to Network Virtualization Edge(NVE) node.

Network Virtualization Edge(NVE): An NVE implements network virtualization functions that allow for L2/L3 tenant separation, tenant-related control plane activity. An NVE contains one or more tenant service instances whereby a TES interfaces with its associated instance. The NVE also provides tunneling overlay functions.

Virtual Network(VN): This is one of a virtual overlay network. Two Virtual Networks are isolated from one another.

Overlay Boundary Point(OBP): This is a network entity that is on the edge boundary of the overlay. It performs encapsulation to send packets to other OBPs across Underling Network for decapsulation.

Underlying Network(UN): This is the network that provides the connectivity between the OBPs.

3. Security Reference Model

This section defines security reference model for Overlay based Network Virtualization.

The L3 overlay network provides virtual network to multi-tenants, which is deployed on the underlying network. The tenant end system attaches to the L3 overlay network.

L3 overlay network provides isolation to each tenant, which provides security to its tenant. L3 overlay network can be regarded secure zone from the view of ONV3 operator. Other components outside of the ONV3 are considered as untrusted, which may impose some attacks on the ONV3. On the other hand, each virtual network may not trust other virtual network. This model is the basis to analyze the security of ONV3.

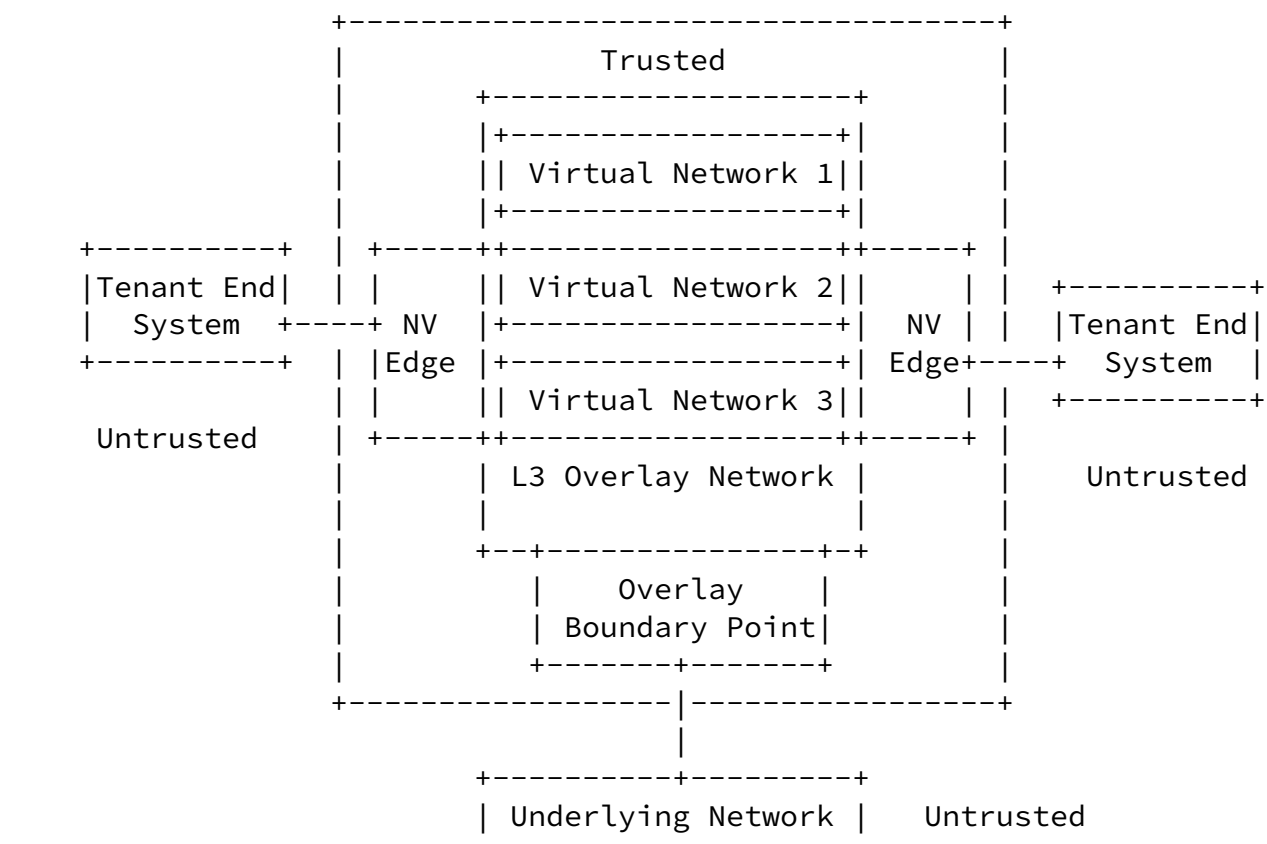
Trusted
Virtual Network 1
Virtual Network 2
Virtual Network 3
L3 Overlay Network
Overlay
Boundary Point
Tenant End
System
NV
Edge
Tenant End
System
Untrusted
Untrusted
Underlying Network
Untrusted

Figure 1: Security Reference Model for Overlay based Network Virtualization

4. Security Threats

This section describes the various security threats that may endanger overlay based network virtualization. For example, an attack on ONV3 may result in some unexpected effects:

- o Interrupt the connectivity of tenant's virtual network.
- o Inject some unwanted traffic into virtual network.
- o Eavesdrop sensitive information from tenant.
- o Degrade provider's service level.

Security threats may be malicious or casual. For example, some of them may come from the following sources:

- o A tenant who rents one or more virtual networks may want to acquire some information from other tenants co-existed in the same data center.
- o Some persons who manipulate the activation, migration or deactivation of tenant's virtual machine.

- o Some persons who phyically access to underlying network.

4.1. Attacks on Control Plane

1. Attack association between VM and VN: one of the functionalities of ONV3 is to provide virtual network to multi-tenants. ONV3 associates a virtual machine's NIC with corresponding virtual network, and maintain that association as the VM is activated, migrated or deactivated. The signalling information between endpoint and access switch may be spoofed or altered. Thus the association between VM and VN may be invalid if the signaling is not properly protected.
2. Attack the mapping of a virtual network: The mapping between the inter and outer addresses may be affected through altering the mapping table.

3. Inject traffic: The comprised underlying network may inject traffic into virtual network.
4. Attack live migration: An attacker may cause guest VMs to be live migrated to the attacker's machine and gain full control over guest VMs[VM-Migration].
5. Denial of Service attacks against endpoint by false resource advertising: for live migration are initiated automatically to distribute load across a number of servers, an attacker may falsely advertise available resources via the control plane. By pretending to have a large number of spare CPU cycles, that attacker may be able to influence the control plane to migrate a VM to a compromised endpoint.

4.2. Attacks on Data Plane

1. Unauthorized snooping of data traffic: This is attack results in leakage of sensitive information, an attacker can sniffer information from the user packets and extract their content.
2. Modification of data traffic: An attacker may modify, insert or delete data packets and impersonate them as legitimate ones.
3. Man-in-the-Middle attack on live migration of VM: When a virtual machine is migrated from one endpoint to another, the VM may be intercepted and modified in the middle of the migration.

5. Security Requirements

This section describes security requirements for control plane and data plane of NVO3.

5.1. Control Plane Security Requirements

1. The network infrastructure shall support mechanisms for authentication and integrity protection of the control plane. (1)When a protocol is used for the service auto-provisioning/ discovery, the information from endpoint shall not be spoofed or altered. (2)When a protocol is used to distribute address advertisement and tunneling information, the protocol shall

provide integrity protection. (3)The protocol for tunnel management shall provide integrity and authentication protection.

2. NVEs shall assure the information in the mapping table is coming from a trusted source.
3. The virtual network should prevent malformed traffic injection from underlying network, other virtual network, or endpoint.

5.2. Data Plane Security Requirements

1. The mapping function from the tenant to overlay shall be protected. NVEs should verify VNID is not spoofed.
2. The data plane should protect VM's state against snooping and tampering.
3. IPsec can provide authentication, integrity and confidentiality protection. IPsec can be used to protect the data plane.

6. Acknowledgements

We invite more feedbacks and contributors.

7. IANA Considerations

IANA does not need to take any action for this draft.

8. Security Considerations

TODO

9. References

9.1. Normative References

[I-D.lasserre-nvo3-framework]
Lasserre, M., Balus, F., Morin, T., Bitar, N., and Y. Rekhter, "Framework for DC Network Virtualization", draft-lasserre-nvo3-framework-02 (work in progress),

June 2012.

[I-D.kreeger-nvo3-overlay-cp]
Black, D., Dutt, D., Kreeger, L., Sridhavan, M., and T. Narten, "Network Virtualization Overlay Control Protocol Requirements", draft-kreeger-nvo3-overlay-cp-00 (work in progress), January 2012.

[I-D.bitar-lasserre-nvo3-dp-reqs]
Bitar, N., Lasserre, M., and F. Balus, "NVO3 Data Plane Requirements", draft-bitar-lasserre-nvo3-dp-reqs-00 (work in progress), May 2012.

9.2. Informative References

[VM-Migration]
Oberheide, Jon., Cooke, Evan., and Farnam. Jahanian, "Empirical Exploitation of Live Virtual Machine Migration", Feb 2011.

Authors' Addresses

Yinxing Wei (editor)
ZTE Corporation
No 68, Zijinghua Road
Nanjing, Jiangsu 210012
China

Phone: +86 25 52872328
Email: wei.yinxing@zte.com.cn

Shiwei Zhang
ZTE Corporation
No 68, Zijinghua Road
Nanjing, Jiangsu 210012
China

Phone: +86 25 52870100
Email: zhang.shiwei@zte.com.cn