Network Working Group   Z. Qiang
Internet Draft   A. Kavanagh
Intended status: Informational   Ericsson
Expires: March 26, 2014   September 26, 2013

Security Requirements of NVO3
draft-zu-nov3-security-requirements-00.txt

Status of this Memo

Copyright Notice

Abstract

This draft discusses the security requirements and several issues which need to be considered in securing a NVO3 network architecture based virtualized data center network for multiple tenants. In addition, the draft also discusses issues that could be addressed or mitigated.

Table of Contents

1. Introduction

Security is the key issue which needs to be considered in the design of a data center network. This document first highlights the security risks that a NVO3 network may encounter, and documents the lists the security requirements that a NVO3 network should fulfill.

Note, it is not the intention to replace the Security Considerations section in each NVO3 draft by this document. This document provides the high level views of the security requirements when NVO3 network is developed. It only lists the architecture level security requirements which can be used as inputs at the design phase of the NVO3 network architecture, control plane and data plane. Each NVO3 drafts must have its security considerations which shall define the detail security solutions of a specific architecture and / or protocol. This document is only the input document when the Security Considerations section in each NVO3 draft is discussed.

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. Terminology

This document uses the same terminology as found in the NVO3 Framework document [I-D.ietf-nvo3-framework] and [I-D.kreeger-nvo3-hypervisor-nve-cp].

4. Security Risk

Overlay infrastructure increases security risks and introduces new threats. In a NVO3 network, there are security risks that the attack made on the underlying network, including the NVO3 control protocols, may be initiated from an exposed overlay virtual network; or the attack made on the encapsulated virtual networks may be initiated from the underlying network or a compromised overlay virtual network.

In a perfect world, virtualization is considered secure with no level of privilege within the virtualized guest environment that permits interference with the host system. There are really not any security issues if a tenant network is isolated as it is designed.

In practice, there are occasional misconfigurations and/or security vulnerabilities that allow an attacker to circumvent these protections and gain access to other virtual machines, or even worse the underlay network. While the misconfigurations or vulnerabilities are pretty rare, they do exist.

5. Security Control

5.1. Control Plane Protection

The DC service provider has the responsibility to protect the NVO3 control plane signaling against any attacking.

R1. The NVO3 network design must provide high availability, especially where DoS/DDoS attacks may be possible. Any NVAs or NVEs shall not become the bottleneck of the control plane traffic.

R2. The control plane design shall minimize the amplification effects which have the potential to be used by attackers to carry out reflection attacks.

R3. At the NVA-NVE control plane, authentication and authorization of the NVA MUST be supported to prevent a compromised network component for impersonating as a NVA when communicate with NVEs.

R4. At the NVA-NVE control plane, authentication of the NVE SHOULD be supported to prevent a compromised network component for impersonating as a NVE when communicate with the NVA.

R5. At the NVE-NVE control plane, authentication of the NVE MUST be supported to prevent a compromised network component for impersonating as a NVE when communicate with other NVEs.

R6. The NVE MUST apply ingress controls at the NVE-NVE interface to filter the incoming signaling traffic and discard any traffic received from non-participating NVEs.

R7. The NVA-NVE control plane protocol MUST be protected with integrity and confidentiality against any off-path or on-path attacks.

R8. The NVE-NVE control plane protocol MUST be protected with integrity and confidentiality against any off-path or on-path attacks.

R9. At the Hypervisor-to-NVE control plane protocol, integrity and authentication of the hypervisor SHOULD be provided to prevent a compromised hypervisor for impersonating as another hypervisor when communicate with the NVE.

R10. If the Inter-DC control plane traffic is crossing Public Internet, it MUST be protected by one or more security solutions to provide confidentiality, integrity and availability.

R11. The NVE MUST have separated address space for data plane tunnel end point and control plane traffic in order to minimize security exposure of the control plane addresses, as recommended in [RFC6169].

5.2. Data Plane Protection

Data plane protection is the primary concern for a NVO3 network.

R12. All data plane packets SHOULD be protected in transit with confidentiality and integrity, including the un-tunneled traffic between the End devices and the NVEs, and the tunneled traffic between the NVEs.

R13. The NVO3 infrastructure SHOULD support VN based security policy management, i.e. security policy defined with a granularity down to VN ID.

R14. When the security policy management is enabled for the data packets of a VN, the security policies MUST be applied on the un-tunneled data packets.

R15. When the security policy management is enabled for the data packets of a VN, the same security policies MUST be applied on the VN data traffic during and after VM mobility.

R16. When the security policy management is enabled for the data packets of a VN, the security policies MUST be applied on the inter-VN traffic.

R17. When Public Internet connectivity is allowed for a VN, the security policies MUST be applied on the VN Public Internet traffic before forwarding between the VN and Internet.

R18. The NVE SHOULD apply security policies on the data packets received from the End Devices before encapsulation. Any disallowed traffic shall be discarded.

R19. The NVE SHOULD apply security policies on the data packets received from the remote NVEs after de-capsulation, and discard any disallowed data packets before forwarding to the End Devices.

R20. The NVE SHOULD filter on the outer address of the tunneled data packets received from the remote NVEs, and discard any data packets received from any non-participating NVEs.

R21. The NVE SHOULD filter on the inner address of the tunneled data packets received from a remote participating NVE, and discard any data packets which the participating NVE is not authorized to send.

R22. When Layer 3 service is supported, the NVE SHOULD discard tunneled IP packets that specify additional routing, as recommended in [RFC6169], though it may be allowed for the End Device to configure what source-routing types are allowed.

R23. If the inter-DC data plane traffic is crossing Public Internet, it MUST be protected by one or more security solutions to provide confidentiality, integrity and availability.

R24. Additional security mechanisms MAY be supported on the interworking function when supporting multiple encapsulation formats in a NVO3 network.

R25. During VM mobility, the NOV3 network MUST avoid forwarding the data packets to the incorrect NVE.

5.3. Operation and Management

R26. The NVO3 Operation and Management traffic MUST be isolated from any other underlay traffic in order to minimize security exposure of the Operation and Management traffic, as recommended in [RFC6169].

R27. The NVO3 Operation and Management data MUST be protected with confidentiality, integrity and availability while in transit.

5.4. Logging

R28. All NVO3 network components, e.g. NVA and NVE, SHOULD support collection of security logs and sending them to a centralized logging service.

R29. A centralized security logging and audit handling mechanism SHOULD be supported. Any access to the NVO3 resources SHOULD be recorded and stored in the centralized logging and audit storage.

5.5. Scalability

R30. The NVO3 network security solutions SHOULD minimize the impact on scalability and allow for simple configuration, e.g. simple security credential management.

5.6. Extensibility

R31. The NVO3 network security solution SHOULD be extensible to allow new security functionality to be introduced in the future.

R32. The NVO3 network security solution SHOULD be defined such that End Devices existing security solution can be supported without implementation impacts.

6. Security Considerations

This is a requirement document for the NVO3 network security and in itself does not introduce any new security concerns.

7. IANA Considerations

No actions are required from IANA for this informational document.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

[RFC6169] S. Krishnan, D. Thaler, J. Hoagland, "Security Concerns with IP Tunneling", RFC 6169, April 2011.

8.2. Informative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[I-D.ietf-nvo3-overlay-problem-statement] Narten, T., Gray, E., Black, D., Fang, L., Kreeger, L., and M. Napierala, "Problem Statement: Overlays for Network Virtualization", draft-ietf-nvo3-overlay-problem-statement-03 (work in progress), May 2013.

[I-D.kreeger-nvo3-hypervisor-nve-cp] Kreeger, L., Narten, T., and D. Black, "Network Virtualization Hypervisor-to-NVE Overlay Control Protocol Requirements", draft-kreeger-nvo3-hypervisor-nve-cp-01 (work in progress), February 2013.

[I-D.ietf-nvo3-framework] Lasserre, M., Balus, F., Morin, T., Bitar, N., and Y. Rekhter, "Framework for DC Network Virtualization", draft-ietf-nvo3-framework-03 (work in progress), July 2013.

9. Acknowledgments

Many people have contributed to the development of this document and many more will probably do so before we are done with it. While we cannot thank all contributors, some have played an especially prominent role. The following have provided essential input: Suresh Krishnan, David Allan I, Makan Pourzandi.

Authors' Addresses

Zu Qiang
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x47370
Email: Zu.Qiang@ericsson.com

Alan Kavanagh
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: alan.kavanagh@ericsson.com