

Network Working Group
Internet Draft
Intended status: Informational
Expires: January 2015

L. Dunbar
Huawei
M. Zarny
Goldman Sachs
C. Jacquenet
France Telecom
S. Chakrabarty
US Ignite

July 4, 2014

Dynamic Network Security as a Service Problem Statement
draft-dunbar-nsaas-problem-statement-00.txt

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, 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/lid-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 January 4, 2009.

Internet-Draft

Network SaaS Problem Statement

July 2014

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Abstract

This draft describes the motivation, use cases, and the problem statement for network security as a service.

Table of Contents

1.	Introduction.....	3
1.1.	Motivation.....	3
1.2.	Network Security Functions under Consideration.....	4
1.3.	The scope of the proposed work.....	5
2.	Conventions used in this document.....	6
3.	Use Case: Virtual Firewall Function On Demand in Cloud DCs.....	7
4.	Use Case: Security Functions provided to a Mobile Operator.....	7
5.	Problem Space.....	8
5.1.	Issues of the current Cloud-based Security Solutions.....	8
5.2.	Other problems.....	9
5.3.	The Benefits.....	9
6.	Related industry initiatives.....	10
6.1.	OpenStack Firewall/Security as a Service.....	10
6.2.	Security as a Service by Cloud Security Alliance.....	10
7.	Potential Solutions.....	11
8.	Conclusion and Recommendation.....	11
9.	Manageability Considerations.....	11
10.	Security Considerations.....	11
11.	IANA Considerations.....	11
12.	References.....	12

12.1. Normative References.....	12
12.2. Informative References.....	12
13. Acknowledgments.....	12

1.Introduction

This draft describes the motivation, use cases, and the problem statement for dynamic network security as a service.

1.1. Motivation

The main benefits of virtualized network functions are increased flexibility to efficiently share the resources, and decreased setup and management costs. These services can be deployed in enterprise networks or in provider networks. Many enterprises are increasing consuming these services hosted in their providers' networks. In particular, they are consuming network security services hosted off premises.

Some of the reasons driving up this demand are the need and desire to:

- . Dynamically provision and update firewall policies
- . Implement stringent security functions at branch offices where minimal security infrastructures/capabilities exist
- . Provide virtual network security services for applications operating over virtual networks such as NV03
- . Maintain consistent security policies across a large number of small low powered/low processing sensors

According to [[Gartner-2013](#)], the demand for cloud-based security services is growing. Small and medium-sized businesses (SMBs) are increasingly adopting cloud-based security services to replace on-premises security tools, while larger enterprises are deploying a mix of traditional and cloud-based security services.

Despite their increasing popularity, most common cloud security services-like most cloud services in general-do not yet have industry standards by which users can request their desired services from some vendors. (The "user-provider" relationship may exist between two different firms or between different domains of the same

firm.)

Another area ripe for standardization is how these services may be dynamically provisioned, updated, or/and verified to fulfill on-demand requests. Issues here range from the more typical ones like the scalability, availability and extensibility of the cloud-based services to more esoteric ones like a lack of intelligent policy to

configuration translation and a lack of consistent way to implement policies across multiple regions and entities.

Open source projects like OpenStack and CloudStack have begun to tackle the issues but much work remains. The objective of this draft is to describe the problem set for which future architecture and solutions can be developed.

1.2. Network Security Functions under Consideration

There are many network functions being deployed and new ones are popping up with business and application demands. In order to have a concrete context for the protocols discussion, we start with the following network security related functions:

- . Firewall
- . DDOS/Anti-DOS
- . Access control/Authorization/Authentication
- . Remote identity management
- . Secure Key management
- . Intrusion Detection System/ Intrusion Prevention System (IDS/IPS)
- . Threat detection: Eavesdropping, Trojans, viruses and worms, Malware, etc.

The reason for starting with security-related functions is due to the wide acceptance of security functions that are not running on customer/enterprise premises. Numerous security vendors are now leveraging cloud based models to deliver security solutions. This shift has occurred for a variety of reasons including greater

economies of scale, streamlined delivery mechanisms, and the demand of business and applications for more sophisticated security functions that they do not have. Consumers, enterprise clients as well as applications are embracing the business model of requesting for security functions that do not run on their own premises on demand, also known as Security as a Service.

1.3. The scope of the proposed work

Virtual Security Function is a security function that can be requested by one domain (e.g., two different domains of one service provider, enterprise clients, or applications, etc.) but may be owned or managed by another domain (e.g., service provider). Those security functions may be hosted on physical appliances or instantiated as virtual machines on common compute server (i.e. the Virtualized network functions defined by ETSI NFV).

Note: Virtual Security Function and "Cloud-based Security Functions" are used interchangeably in this draft.

The "requester <-> provider" relationship has different connotations in different scenarios:

- . Client <-> Provider relationship, i.e. client requesting some network functions from its provider;
- . Inter-domain, e.g. Domain A <-> Domain B relationship, i.e. one operator domain requesting some network functions from another operator domain, where "A" and "B" can be from same operator or different operators; or
- . Applications <-> Network relationship, i.e. an application (e.g. cluster of servers) requesting some functions from network, etc.

The security functions offered by 3rd party need Bi-directional periodic communications between the requesters and the providers for policies negotiation, validation, potentially re-directing traffic to higher level security functions, etc. Therefore, the service requires protocol exchange. Simply API is not enough.

The objective of the proposed work is to standardize the protocols (or the interface) and architecture for Requester and Provider to negotiate the functions needed as well as the associated attributes.

The proposed protocols between requester and provider can be used for the following scenarios:

- . A Client requests a certain network security function from a provider

- . The provider fulfills the request for example, by instantiating an instance of the service in question, or configures an additional rule in an already provisioned service.

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.

Cloud DC: The data centers that are not on premises of enterprises yet have the compute/storage resources that can be requested or purchased by the enterprises. What the enterprises actually get is Virtual Data Centers.

DC: Data Center

Domain: The term "Domain" in this draft has different connotations in different scenarios:
Client <-> Provider relationship, i.e. client requesting some network functions from its provider;
Domain A <-> Domain B relationship, i.e. one operator domain requesting some network functions from another operator domain; or
Applications <-> Network relationship, i.e. an

application (e.g. cluster of servers)
requesting some functions from network, etc.

Virtual Network Function: an L4-L7 network function that can be requested by one domain (e.g. two different domains of one service provider, enterprise clients, or applications, etc.) but may be owned or managed by another domain (e.g. service provider). Those network functions would be running over physical appliances or instantiated as virtual machines on common compute servers (i.e. the ETSI NFV defined Virtualized network functions). The "Network Function" here means a range of L4-L7 functions.

Dunbar, et al.

Expires January 4, 2015

[Page 6]

Internet-Draft

Network SaaS Problem Statement

July 2014

Virtual Security Function: a security function that can be requested by one domain but may be owned or managed by another domain.

Cloud-based security functions: used interchangeably with the "Virtual Security Functions" in this draft.

3. Use Case: Virtual Firewall Function On Demand in Cloud DCs

Clients of a cloud data center not only need virtual networks to interconnect their virtual compute/storage resources, but they also need virtual firewall services to enforce the proper communication policies. VPN clients, especially branch office access points, may need firewalls that are hosted by the VPN provider to be integrated with the VPN service.

Per [\[NW-2011\]](#), A cloud-based firewall is different from an on-premise one (aside from its location) in three key areas: scalability, availability and extensibility.

- . Scalability: Cloud-based firewalls are designed to serve multiple customers and their increasing demand. Unlike with an on-premise firewall, upgrading a cloud-based firewall-e.g., for greater throughput-should be transparent to enterprise users.
- . Availability: Cloud-based firewall providers tend to offer

extremely high availability through their highly redundant and resilient data centers. In contrast, most enterprises may not be able to offer "carrier-grade" high availability.

- . Extensibility: Enterprises looking for vendor diversity can subscribe to cloud-based firewalls from different providers. Furthermore, additional features can be added more seamlessly, transparently.

4. Use Case: Security Functions provided to a Mobile Operator

Maintaining security is challenging, especially in mobile environments, where all kinds of user devices (smartphones, pads, personal assistants, etc.) access applications located in the cloud. Not only are applications no longer hosted in contained data centers, (which have a higher chance of encountering various security threats), but also the mobile devices might not have the

sophisticated processing power or expertise to run up-to-date security protection functions to guard against rapidly changing threats.

Evolving threats to mobile networks can affect mobile devices, radio access networks (RANs), and applications hosted in cloud data centers.

The trend is to have security functions delivered as a service from the provider, without requiring on-premise hardware or software maintenance.

These security services often include authentication (e.g., the ability to authenticate employees to control the cloud services and data they have access to), anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

The security function offering can be between different domains of one operator or between subscribers to providers. Backhaul operators can offer the security function services to mobile operators.

Security-as-a-Service to mobile environments offers a number of benefits, including:

- . Greater security expertise than typically available to mobile users,
- . Flexibility of managing evolving threats
- . Ensuring service availability
- . Reducing deployment and operational costs
- . Effectively organizing groups of apps or users,
- . Constant virus definition updates.

5. Problem Space

5.1. Issues of the current Cloud-based Security Solutions

Many vendors already offer Security as a Service in the cloud. However, all their solutions are proprietary, with different interfaces and different modes of operation. Some offerings follow a peer-to-peer model: i.e. requiring clients to peer with vendor provided functions hosted in the cloud. A competing model requires clients to download their desired functions to local devices. In this model, it is difficult to maintain consistent software updates across all the devices. Consistency issues can exist across: (1)

Dunbar, et al.

Expires January 4, 2015

[Page 8]

Internet-Draft

Network SaaS Problem Statement

July 2014

multiple regions for a single application; (2) multiple applications; and/or (3) multiple zones (e.g., between internal and perimeter zones).

In addition, the current mode of operation for Security as a Service via a Cloud infrastructure does not have any common interfaces/mechanisms for clients or applications to verify if the required functions can fulfill the policies needed by the clients/applications. There is a lack of user-friendly service (policy) template.

5.2. Other problems

Here are some other problems associated with Security Function on Demand that might be out of the scope of this proposed WG:

- . Diverse security services:
The proposed WG might not be able to cover every possible

security service.

- . Scalability:
Not only diverse CPU/memory needed for different security functions can be difficult to manage, but the solution itself may have some limits, e.g. maximum number of firewall rules.
- . Availability:
The VNF pool is to address the availability of virtualized network functions.
- . Converting policies to vendor-specific configurations
- . Dynamic features update

5.3. The Benefits

The goal of the proposed work is to establish an architectural framework and mechanisms for clients (or one domain) to request security functions from a network provider (or another domain). The framework allows the clients to view, request, and/or verify the security functions/solution offered by different vendors. This

framework can make it easy for a cluster of devices requiring the similar security policies to have consistent policies across multiple sites.

The network service providers, with their physical access to a vast number of enterprises and consumers, are very well positioned to provide the "Security Function on Demand" platform. The providers can act as security function brokers to their directly connected domains. They can offer a service catalog and standard mechanisms by which enterprises (or applications) can query request, or/and verify the needed security functions.

With the standard protocols for clients to request the needed security functions, network operators can leverage their current VPN to enterprises and access to a vast population of end users to offer a set of consolidated Security solutions. The IETF can play an instrumental role in defining this common interface and framework for network operators.

6. Related industry initiatives

6.1. OpenStack Firewall/Security as a Service

OpenStack completed the Firewall as a Service project and specified the set of APIs for Firewall services:

http://docs.openstack.org/admin-guide-cloud/content/fwaas_api_abstractions.html

OpenStack has defined the APIs for managing Security Groups:

http://docs.openstack.org/admin-guide-cloud/content/securitygroup_api_abstractions.html

The attributes defined by OpenStack Firewall/Security as a Service will be the basis of the information model for the proposed work at the VNFOD IETF initiative.

6.2. Security as a Service by Cloud Security Alliance

https://cloudsecurityalliance.org/research/secaas/#_get-involved

SaaS by CSA is at the initial stage of defining the scope of work.

7. Potential Solutions

While it is too early to specify any solutions, some potential candidates are described just to prove that the identified problem is well bounded for the IETF to specify the needed solutions.

The protocol needed for this negotiation may be somewhat correlated to the dynamic service parameter negotiation procedure [RFC7297]. The CPP template documented in RFC7297, even though currently covering only Connectivity, could be extended as a basis for the negotiation procedure. Likewise, the companion CPNP protocol could be a candidate to proceed with the negotiation procedure.

The "security as a service" would be a typical example of the kind of (CPP-based) negotiation procedures that could take place between a corporate customer and a service provider. However, more security specific parameters have to be considered by this proposed work.

8. Conclusion and Recommendation

Although open source projects such as OpenStack have taken on the security as a service initiative, much work needs to be done. For example, OpenStack today covers only a minimal set of security functions. The IETF has a responsibility to define a comprehensive framework and necessary standards by which network security functions may be offered, requested, implemented or verified.

9. Manageability Considerations

TBD.

10. Security Considerations

TBD

11. IANA Considerations

This document requires no IANA actions. RFC Editor: Please remove this section before publication.

12. References

12.1. Normative References

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

[RFC7297] Boucadair, M., "IP Connectivity Provisioning Profile",

[RFC7297](#), April 2014.

[12.2](#). Informative References

- [Boucadair-framework] M. Boucadair, et al, "Differentiated Service Function Chaining Framework", < [draft-boucadair-service-chaining-framework-00](#)>; Aug 2013
- [Gartner-2013] E. Messmer, "Gartner: Cloud-based security as a service set to take off", Network World, 31 October 2013
- [NW-2011] J. Burke, "The Pros and Cons of a Cloud-Based Firewall", Network World, 11 November 2011
- [SC-MobileNetwork] W. Haeffner, N. Leymann, "Network Based Services in Mobile Network", IETF87 Berlin, July 29, 2013
- [Application-SDN] J. Giacomoni, "Application Layer SDN", Layer 123 ONF Presentation, Singapore, June 2013

13. Acknowledgments

Acknowledgements to Andy Malis for his review and contributions.

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

Dunbar, et al. Expires January 4, 2015 [Page 12]

Internet-Draft Network SaaS Problem Statement July 2014

Authors' Addresses

Linda Dunbar

Huawei Technologies
5340 Legacy Drive, Suite 175
Plano, TX 75024, USA
Phone: (469) 277 5840
Email: ldunbar@huawei.com

Myo Zarny
Goldman Sachs
30 Hudson Street
Jersey City, NJ 07302
Email: myo.zarny@gs.com

Christian Jacquenet
France Telecom
Rennes 35000
France
Email: Christian.jacquenet@orange.com

Shaibal Chakrabarty
US Ignite
1776 Massachusetts Ave NW, Suite 601
Washington, DC 20036
Phone: (214) 708 6163
Email: shaibalc@us-ignite.org