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

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

September 25, 2014

Interface to Network Security Functions Problem Statement
draft-dunbar-i2nsf-problem-statement-01.txt

Status of this Memo

Copyright Notice

Abstract

This draft describes the motivation, use cases, and the problem statement for Interface to Network Security Functions.

Table of Contents

1. Introduction

This draft describes the motivation, use cases, and the problem statement for Interface to Network Security Functions.

In the context of I2NSF, the term "Virtual Network Security Function" is used frequently to emphasize the point that the entities that consume the Network Security functions don't own or host them. Those network security functions can be achieved by physical appliances, or by VMs instantiated on servers.

1.1. Motivation

Enterprises are increasingly consuming network functions, especially the network security related functions that are hosted off their promises. Some of the reasons driving up this demand are the desire (and the necessity) to:

- Implement stringent security functions at branch offices where minimal security infrastructures/capabilities exist;
- Provide virtual network security services for clients, and/or applications operating over virtual networks in third party managed (or cloud) data centers;
- Maintain consistent security policies across a large number of sites, users, or 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.

To efficiently meet the dynamic demand of security functions requests from clients, it is desirable to have mechanisms to:

- Create/delete/manage virtual security functions over physical appliances, (e.g. Dynamically provision and update firewall policies for a virtual FW instance),
- Have standardized concrete rules (or attributes) for instantiating VMs for virtual security functions, and
- Have standardized mechanisms for clients, users, or applications to request/negotiate/validate security functions that are not physically located on the local premises.

Despite their increasing popularity, most common cloud security services do not yet have industry standards by which users/clients can request their desired services. (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.

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)

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 Network Security as a Service.

1.3. The scope of the proposed work

The Interface to Network Security Functions (I2NSF) initiative aims at improving the dynamic allocation and operation of network security functions by documenting a global framework that would include protocol-based control and management interfaces, along with adequate data models. The information required for the provisioning, the configuration and the operation of network security functions will be exchanged through the said interfaces and protocols. The I2NSF initiative will also take into account the need for co-existing with legacy configuration and management systems used to allocate and operate network security functions, whether they are embedded in network devices or virtualized in data center environments, for example. The standard Interface to request/negotiate/allocate/operate (Virtual) Network Security Functions (I2NSF) is one of the necessary tools for operators and service providers to offer network security functions as a service to their corporate clients.

It is envisioned that clients of the I2NSF interfaces include management applications, service orchestration systems, network controllers, or user applications that may solicit network security resources.

Various aspects to I2NSF include:

- The mechanism for clients (applications) to request/negotiate/validate security functions that are not physically located on the local premises,

- The mechanism for creating virtual security functions on physical appliances, and

- Application/user oriented rules/policies to instantiate virtual security functions as VMs on common compute servers (NFV initiative).

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 third party need Bi-directional periodic communications among multiple entities for policies negotiation, validation, potentially re-directing traffic to higher level security functions, etc. Therefore, the service requires programmatic interfaces or protocol exchange, whereas API is conventionally associated with functional calls on one system.

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: In the context of I2NSF, the term

"Virtual Network Function" is used frequently to emphasize the point that the entities that consume the Network functions, mostly L4-L7 functions, don't own or host them. Those network functions can be achieved by physical appliances, or by VMs instantiated on common compute servers (i.e. the ETSI NFV defined Virtualized network functions).

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.

NBI: Northbound Interface. "Northbound" can be ambiguous because "northbound" to entity A can be southbound to entity B. So we try to avoid using "northbound" in I2NSF.

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

Clients of a third party (or 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. Some of the functions might be hosted in data centers geographically far away from the clients that need the functions, therefore requiring traffic to be hair-pinned to the remote data centers. 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) 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. Related IETF WGs

IETF SFC is about mechanism of chaining together service functions; VNFpool is about the reliability and availability of the virtualized network functions. But none of them address how service functions are requested, or how service functions are fulfilled.

Both SFC and VNFpool don't cover in-depth specification (e.g. rules for the requested FW) for clients to request its needed functions. In SFC & VNFpool, FW function is a black box, that is treated in same way as Video Optimization function. SFC/VNFpool don't cover the negotiation part, e.g. Client needs Rule x/y/z for FW, but the Provider can only offer x/z.

IETF SACM (Security Assessment and Continuous Monitoring) specifies the mechanisms to assess end point security. The end points can be routers, switches, clustered DB, installed piece of software. SACM is about "How to encode that policy in a manner where assessment can be automated". For examples:

- a Solaris 10 SPARC or Window 7 system used in a environment that requires adherence to a policy of Mission Critical Classified.
- rules like "The maximum password age must be 30 days" and "The minimum password age must be 1 day"

IETF midcom, nsis, pcp, (arguably) SOCKS have done some work that have some aspects related to or can be used by I2NSF.

6.2. Relationship with ETSI NFV

We believe that the I2NSF is one of the enabling tools for Network Security as a Service (NSaaS), which is a subset of VNF as a Service (VNFaaS) specified by ETSI NFV Group Specification Use Cases [gs_NFV]. The main benefits of virtualized network functions are increased flexibility to efficiently share the resources, and decreased setup and management costs. NFV defines the architecture to pool together many virtual network functions to be managed and consumed collectively.

NFV, with its heavy representation from service provider side, can define more detailed service model for VNFaaS and setting requirement for IETF's narrowly scoped I2NSF interface/protocols.

6.3. OpenStack Firewall/Security as a Service

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.

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 are very primitive, even though they can be the basis of the information model for the I2NSF IETF initiative.

6.4. 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.

6.5. Productive Eco-system with Open Source Communities

Open-source initiatives are not to be considered as an alternative to formal standardization processes. On the contrary, they are complementary, with the former acting as an enabler and accelerator of the latter. Open-source provides an ideal mechanism to quick prototyping and validating contending proposals, and demonstrating the feasibility of disruptive ideas that could otherwise not be considered. In this respect, open-source facilitates the engagement in the standardization process of small (and typically more dynamic) players such as start-ups and research groups, that would see better opportunities of being heard and a clearer rewards to their efforts. An open-source approach is extremely useful as well for the production of open reference implementations of the standards at the same (or even faster) pace they are defined. The availability of such reference implementations translate into much simpler interoperability and conformance assessments for both providers and users, and can become the basis for incremental differentiation of a common solution, thus allowing a cooperative competition ("coopetition") model.

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

The I2NSF aims at documenting a high-level architecture that will describe the functional building blocks for the dynamic negotiation of security service parameters, the dynamic and subsequent allocation of network security resources and the operation of such resources, including means to assess that what has been allocated complies with what has been negotiated. The work to be conducted by the I2NSF WG also includes the documentation of use cases as well as the specification of information and data models that will provide the adequate level of abstraction. In addition, the I2NSF WG will analyze candidate protocols that may carry the information to be exchanged through the various interfaces (e.g., between a customer and a service provider, between the control plane and the data plane, etc.) for the purpose of network security resource negotiation, allocation and operation.

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

[gs_NFV] ETSI NFV Group Specification, Network Functions Virtualizsation (NFV) Use Cases. ETSI GS NFV 001v1.1.1, 2013.

[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. Giacomonni, "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.

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