I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: September 19, 2016

S. Hares
Huawei

March 18, 2016

I2NSF Data Flow Requirements
draft-hares-i2nsf-mgtflow-reqs-00.txt

Abstract

This document discuss the stresses on I2NSF management traffic during periods DDoS and network attacks, and how application layer tuning of I2NSF management traffic can improve the managementtraffic flow.

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 September 19, 2016.

Table of Contents

1. Introduction

The Interface to the Network Security Function (I2NSF) Working Group is chartered with providing architecture and mechanisms to inject into and retrieve information from network security devices. The I2NSF problem statement ([I-D.ietf-i2nsf-problem-and-use-cases] indicates that service providers lack a standard management interface which preserves:

- o critical communications during DDoS attacks (DOTS),
- o allows hosts to continue even during the DDoS attacks,
- o aids reporting of these attacks the CERT (MILE),
- o and manages network connnectivity of devices out of compliance (SACM).

This document describes the stress on I2NSF management traffic during DDoS and network attacks/incidents, and some mechanisms that help traffic flow during these periods. I2NSF considers two directions: I2NSF controller to NSF/vNSF, and I2NSF user to I2NSF controller.

2. Stresses on traffic between I2NSF and vNSF/NSF

During periods of DDoS attacks, I2NSF management traffic may encounter high error rates, congestion, restricted bandwidth caused by DDoS related traffic (ICMP spams, transport protocol SYN attacks, port spams, and others.), or attacks on specific network machines. Message integrity may be compromised by attacks on the transport

protocols, or by replay attacks on message sequence. However, during this same time period the I2NSF controller needs to send to NSFs/ vNSFs new filter policies or other configuration changes. IDS/IPS NSF functions may need to send I2NSF controller information to help detect the attack source or stop the attack.

During DDOS attacks or network security incidents, the client programs may want to receive status information from the I2NSF controller. This communication will also be impacted by the high error rates, congestion, and restricted bandwidth caused by DDoS related traffic or network security attacks.

This stress can be illustrated by examining two types of management traffic which need to be exchanged with the I2NSF controller: DDoS Open Threat Signaling (DOTS) traffic, and security incident (CERT) traffic reports.

2.1. DOTS (DDoS Open Threat Signaling) Management Traffic

Sending information about DDoS threats occurs during periods where the DDoS is congesting the network or causing large packet losses. I2NSF controllers may receive requests from DOTS controllers to configure new network security functions (NSFs) or reconfigure existing security functions on vNSF or NSF devices. I2NSF controllers may need to receive specific events from vNSF/NSF devices, and receive traffic monitoring data and logs regarding network security incidents.

The DOTS requirements for messages from devices with security functions (such as firewalls in routing devices) are specified in: [I-D.ietf-dots-requirements]. The following are DOTS descriptions of the resiliency needed by the management data:

- Resilence (DOTS-G-003) in the face of severally constrained severely constrained network conditions imposed by the attack traffic. The protocol SHOULD be resilient, that is, continue operating despite message loss and out-of-order or redundant signal delivery,

- Small message sizes (DOTS-G-005) to prevent fragmentation so that all of the message goes through in attack,

- Message integrity (G-006) and Message level replay protection (G-007) must exist for data streams even during periods of attack,

- Session-level Health monitoring (aka Heart beats) during attack (DOTS-OP-003), and

- o Abiilty to request/stop mitigation quickly (DOTS-OP-005)

2.2. MILE - Managed Incident Lightweight Exchange

Reporting and managing security incident traffic is being investigated by the MILE working group. The MILE related protocols ([RFC5070], [I-D.ietf-mile-rfc5070-bis]) provide data formats for reporting network security incidents during time periods of network attack. Similar to DOTS, the data passed by these protocols requires resilience, message integrity, message level replay protection, and session-level health monitoring. During these attacks, the use of small message sizes may be necessary.

3. Stresses on I2NSF controller to User traffic

The user application communicating with the network security controller uses the I2NSF protocol to:

- o give commands that direct the actions of the Network Security Controller during normal operation and during periods of security attack,

- o give commands to direct the creation of policy on the Network Security controller, or on the NSF or vNSF devices,

- o receive reports on the status of network security including DDoS attacks, outages, and devices operating outside the appropriate security software or actions, and

- o give commands to link the network security controller to additional resources (e.g. CERT for incident report or additional IDS/IPS services)/

The communication to perform security operations may encounter DDoS and network attack related outages, network congestion (bursts of congestion or time periods of congestion), and specific network attacks on messages protocols (E.g. TCP syn attacks, ICMP based attacks).

4. I2NSF Management Traffic Flow Needs

The I2NSF communication needs to support application layer services that handle the transport layer’s failure to support critical communication. These application services must provide the following to preserve the end-to-end communication between I2NSF controller to NSF/vNSF and between I2NSF controller and the user:

- o data flow resilence,

- o breaking the data traffic into appropriate sizes for pass through congestion (aka "chunking" the data) and re-assembly of data prior to handing to application,

- o message integrity and replay protection,

Each I2NSF agent and I2NSF client needs to provide this support at the application level since security attacks often attack the tranport connections. This is true whether the communication is between the I2NSF Controller to vNSF/NSF device, or between the user's client device and the I2NSF controller.

5. I2NSF Protocol with Session Layer Services

The diagram in figure 1 shows how a secure session service (SSE) at the application layer of the I2NSF protocol that could provide these

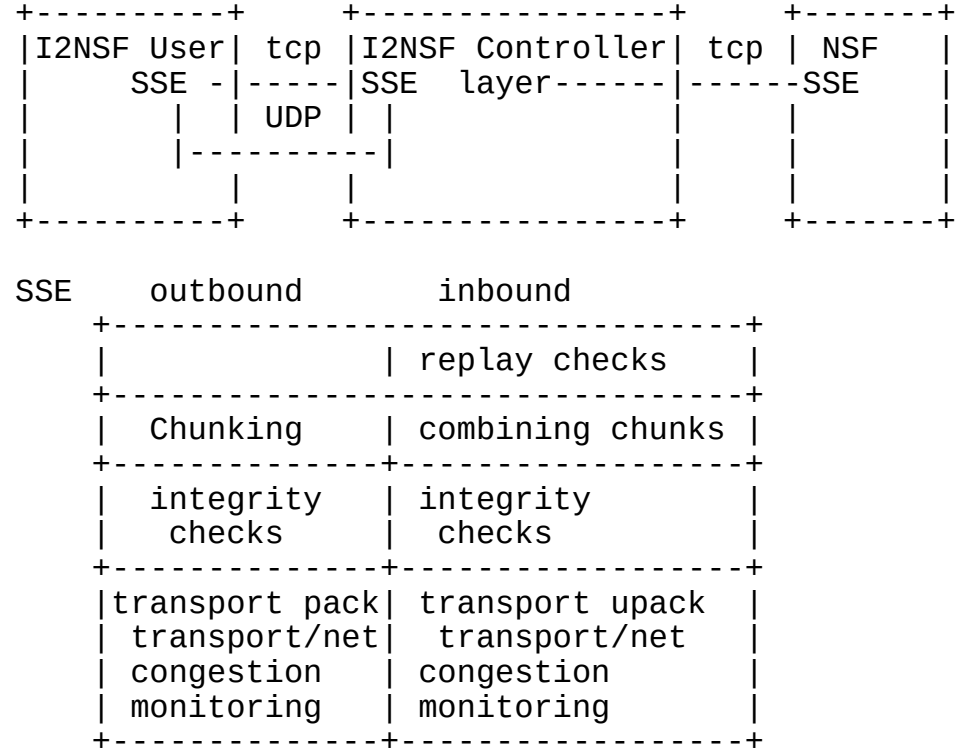

Figure 1

6. Impact of I2NSF potential use of I2RS protocol

I2NSF protocol may want to consider extending the I2RS protocol [I-D.hares-i2rs-protocol-strawman] for communication to routers/ switches that have onboard security functions. The first version of

the I2RS protocol will support communication by NETCONF [RFC6241] (with extensions), RESTCONF [I-D.ietf-netconf-restconf] (with extensions), and other protocols. The I2RS working group is seeking feedback on management traffic during network outages (security related or network connectivity related) in order to determine what protocols are needed beyond NETCONF and RESTCONF. This management traffic includes configuration, events, log information, alerts, traffic monitoring information, traffic statistics, and end-to-end performance information. I2NSF could help the I2RS working group determine the security management information needed to be passed to NSF or vNSF functions in routers.

7. IANA Considerations

There are no IANA requirements for this requirementdocument.

8. Security Considerations

TBD

9. Acknowledgements

The following people have aided in the discussion

- Russ White,and
- Robert Moskowitz.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

10.2. Informative References

[I-D.hares-i2rs-dataflow-req] Hares, S., "I2RS Data Flow Requirements", draft-hares-i2rs-dataflow-req-01 (work in progress), March 2016.

[I-D.hares-i2rs-protocol-strawman] Hares, S., "I2RS protocol strawman", draft-hares-i2rs-protocol-strawman-00 (work in progress), March 2016.

[I-D.ietf-dots-requirements]
Mortensen, A., Moskowitz, R., and T. Reddy, "DDoS Open Threat Signaling Requirements", draft-ietf-dots-requirements-00 (work in progress), October 2015.

[I-D.ietf-i2nsf-problem-and-use-cases]
Hares, S., Dunbar, L., Lopez, D., Zarny, M., and C. Jacquenet, "I2NSF Problem Statement and Use cases", draft-ietf-i2nsf-problem-and-use-cases-00 (work in progress), February 2016.

[I-D.ietf-i2rs-architecture]
Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", draft-ietf-i2rs-architecture-13 (work in progress), February 2016.

[I-D.ietf-mile-rfc5070-bis]
Danyliw, R., "The Incident Object Description Exchange Format v2", draft-ietf-mile-rfc5070-bis-16 (work in progress), February 2016.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-09 (work in progress), December 2015.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, DOI 10.17487/RFC5070, December 2007, <http://www.rfc-editor.org/info/rfc5070>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

Author’s Address

Susan Hares
Huawei
Saline
US

Email: shares@ndzh.com