

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 27, 2017

D. Waltermire
NIST
J. Fitzgerald-McKay
Department of Defense
June 25, 2017

Posture Assessment Through Posture Information Collection Discussion
Scope
draft-waltermire-panic-scope-02

Abstract

This document defines an intended discussion scope for the non-working group posture assessment through network information collection (PANIC) non-WG discussion list.

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 27, 2017.

Copyright Notice

Copyright (c) 2017 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.

Internet-Draft

PANIC Scope

June 2017

Table of Contents

1.	Introduction	2
2.	Terminology	2
3.	Components	2
4.	PANIC Solution Requirements	3
5.	IANA Considerations	4
6.	Security Considerations	4
7.	References	5
7.1.	Normative References	5
7.2.	Informative References	5
	Authors' Addresses	5

[1.](#) Introduction

Network operators need to know what is connected to their organization's networks so that they can properly manage those network elements. Managing these network elements, consisting of physical and virtual network infrastructure devices, requires access to information pertaining to these endpoint devices, including endpoint identity, the identity of software installed on the endpoint, and the configuration settings for the installed software. This information can be collected from different classes of endpoints over different protocols and using different data models. PANIC will identify a standardized solution to collect posture information for network devices, and allow that information to be shared with authorized users and devices on the network supporting security automation. PANIC aims to reuse available standards for posture assessment where possible. In particular, PANIC will leverage NETCONF [[RFC6241](#)], extending the YANG [[RFC6020](#)] data model as necessary to meet PANIC requirements. The PANIC effort will avoid redefining information exchange technologies for use cases that have already been defined.

[2.](#) Terminology

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](#)].

[3.](#) Components

The solution will consist of the following components:

Network Device: Endpoints such as routers, switches, firewalls.
Virtualized network functions are currently considered in scope.

Posture Server: Collects information from the network device.
Receives information via pushes, and requests information via pulls.

Data Repository: Stores the information collected by the posture server from the network device.

PANIC components

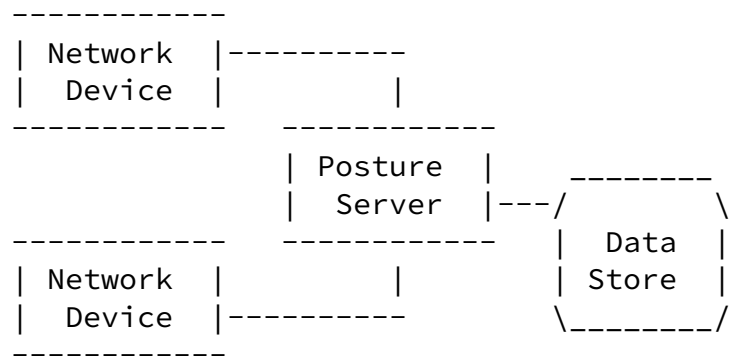


Figure 1

4. PANIC Solution Requirements

The solution will meet the following requirements:

Information Requirements for Network Device Management: PANIC will identify a minimal set of information necessary to manage network devices and to support network security functions including configuration and vulnerability management. Additional information may also be used through extension mechanisms identified by PANIC.

Authorized Posture Server Discovery: Network devices will be able to identify the posture servers with which they are authorized to communicate. PANIC will identify requirements in support of a

Posture Server discovery capability.

Data Push Functionality: Network devices will push information to an authorized Posture Server. Data pushes will be event driven. PANIC will identify what data should be pushed from the network device, and what events will trigger a push. Data pushes from Posture Server to Network Device (for example, pushing new configurations to a network device) are out of scope for PANIC.

Data Pull Functionality: A Posture Server will pull information from a network device. Data pulls will be driven by requests to the server. PANIC will identify what data should be pulled from the

network device, and how requests for the server to pull will be made.

Secure Transport of Data: Data between the network device and the Posture Server will be protected in transit by a protocol that provides authorization and authentication. PANIC will identify the protocols that can be used for transport of posture information.

Secure Storage of Data: Network device data reported to a posture server will be stored in a data repository. This data can be used to support numerous security functions on the network; therefore, this repository should be accessible by (and only by) authorized users and devices. PANIC will identify requirements for a centralized data repository, including requirements for a secure interface between a Posture Server and a Data Repository.

Standardized Data Model: Network device data will be expressed in a standardized data model that enables use and reuse of the data. PANIC will identify available data models for the expression of required information and the models used for a given exchange of posture.

Note: Use of [\[RFC2119\]](#) text is omitted at this point. More discussion is needed around these requirements.

[5.](#) IANA Considerations

This memo includes no request to IANA.

6. Security Considerations

The solution described by this document provides a mechanism to gather network device posture into a centralized datastore. Discussion is needed here about:

The need to protect such an information collection from unauthorized access or disclosure

Privacy considerations around how the endpoint devices is identified when posture is gathered

The threat introduced to the network elements by the posture information collection. There should be protections implemented to prevent the element from being vulnerable to DoS attacks by frequent polling or pushing of posture data.

7. References

7.1. 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>>.

7.2. Informative References

- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#), DOI 10.17487/RFC6020, October 2010, <<http://www.rfc-editor.org/info/rfc6020>>.
- [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>>.

David Waltermire
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20877
USA

Email: david.waltermire@nist.gov

Jessica Fitzgerald-McKay
Department of Defense
9800 Savage Road
Ft. Meade, Maryland
USA

Email: jmfitz2@nsa.gov