INTERNET-DRAFT
Intended Status: Informational
Expires: January 16, 2014

R. Housley
Vigil Securiy
S. Turner
IECA

July 15, 2013

sacm: Alternate Architecture
draft-handt-sacm-alternate-architecture-01

Abstract

This document proposes and alternate architecture for sacm (a proposed working group at the time this draft was submitted).

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."

Copyright and License Notice

1. Introduction

[ID.waltermire-sacm-architecture] proposed an architecture for sacm. This draft proposes an alternate architecture.

2. Initial Architecture

The initial proposed architecture is copied here for convenience:

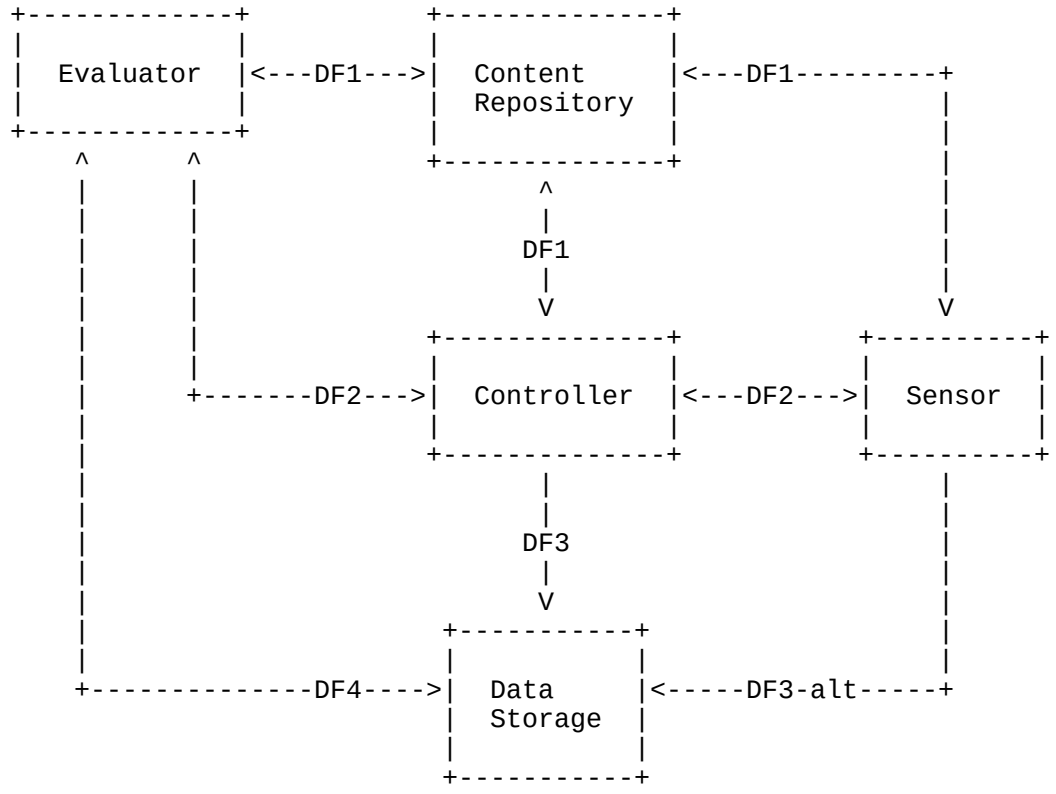

Figure 1 - Proposed sacm Architecture

The primary issue with the proposed architecture is its abstraction. For those not in the know, it makes more sense to propose an architecture in terms of actual boxes and protocols that flow as opposed to a functional architecture.

3. Alternate Architecture

In the following figure:

- BPD is a Border Protection Device (BPD), which is a firewall and IDS (Intrusion Detection System) all rolled in to one.
- Asset is either a host or a client.
- Evaluator determines whether the asset is allowed access to the network.

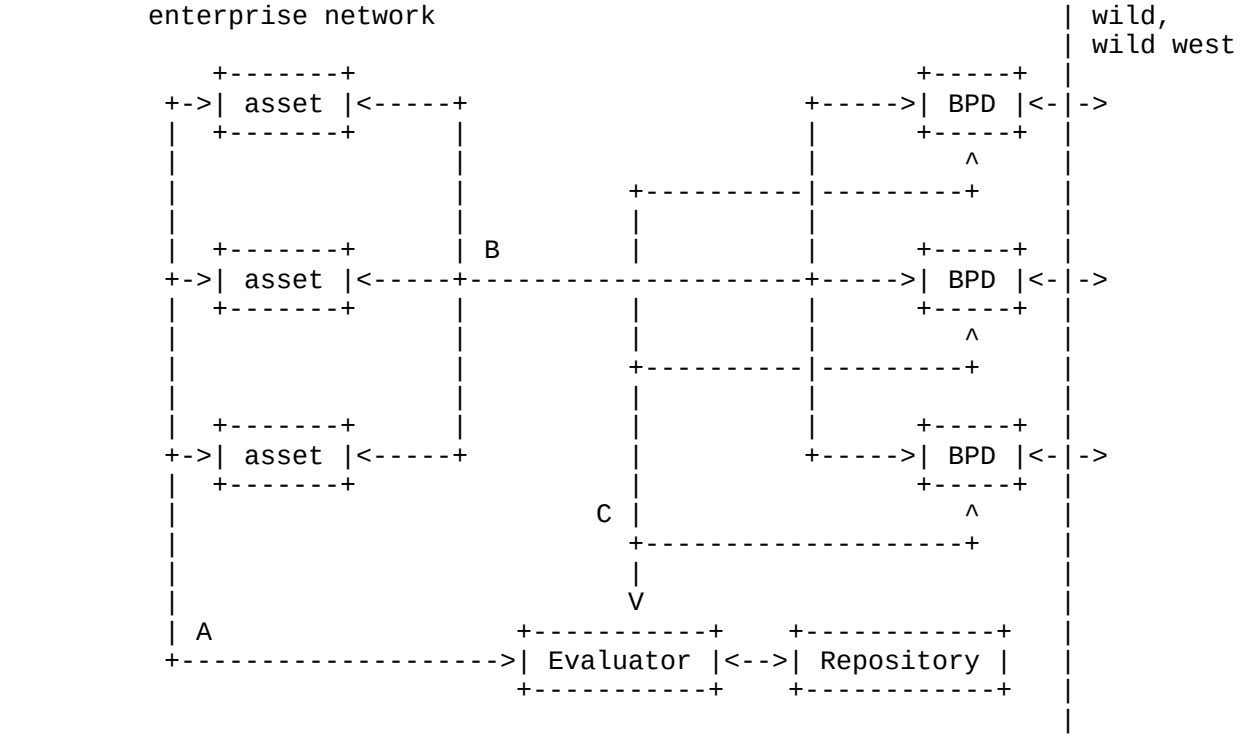

Figure 2 - Alternate sacm Architecture

Lines marked A, flowing from the asset to the Evaluator, are NEA-based protocols. The asset has a NEA client that performs posture collection, posture brokering, and posture exchange with the Evaluator. The evaluator has a NEA server that evaluates the posture, posture brokering, and posture exchange with the asset. It must be noted that the NEA client can have more than one collector (e.g., one to collect OS information, one to collect IP information, one to collect application information) and the NEA server can have

more than one evaluator.

The initial posture assessment is best done before the asset has access to the network. [ID.draft-ietf-nea-pt-eap] provides one such solution. After network access has been granted, posture should continue to be maintained [RFC6876] provides on such solution to convey updated posture attributes.

Lines marked B, flowing from the client to the BPD are network traffic that occur after initial network access has been granted. The BPDs provide a backstop to ensure that assets are acting appropriately (e.g., a client is acting as a client and not a host). These protocols are not in sacm's scope.

Lines marked C, flowing from the BPD to the (Evaluator or Repository?) ensure that the BPDs know how the asset are supposed to be acting.

[Question: Do BPDs interact with the database or the evaluator?]

[Question: Do BPDs need to talk to each other so that clients cannot choose multiple egress points to hide their activity.]

[Question: How do external enterprises interact with this enterprise]

4. Security Considerations

By identifying the components and where those functions reside this alternative architecture makes it easier to understand the required protocol flows.

5. IANA Considerations

There are no IANA considerations present in this document.

6. References

6.1 Normative References

Nada

6.2 Informative References

[RFC6876] Sangster, P., Cam-Winget, N., and J. Salowey, "A Posture Transport Protocol over TLS (PT-TLS)", RFC 6876, February 2013.

[ID.waltermire-sacm-architecture] D. Waltermire, "Security Automation and Continuous Monitoring (SACM) Architecture", draft-waltermire-sacm-architecture, work-in-progress.

[ID.draft-ietf-nea-pt-eap] Cam-Winget, N. and P. Sangster, "PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods", draft-ietf-nea-pt-eap, work-in-progress.

Authors' Addresses

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

Email: : housley@vigilsec.com

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

Email: turners@ieca.com