SXP Proposal

Name

Source-Group Tag eXchange Protocol (SXP)

Repo Name

sxp

Description

SXP is a control protocol to propagate the binding between an IP address and a Source Group Tag (SGT) which is supported in the majority of Cisco devices. This project is to implement SXP in ODL so that ODL will have the binding information from the large installed base of Cisco devices. ODL can process this information and provide it to applications and network elements.

SXP is a protocol published in the IETF https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/ which propagates information about the binding of an IP address to a Source-Group Tag (SGT) between network devices.

Within SXP, source groups are endpoints connecting to the network which have common network policies. Each source group is identified by a unique SGT value, 2-octet number. The SGT to which an endpoint belongs can be assigned statically or dynamically. And the SGT can be used as a classifier for network policies (like ACLs, QOS, etc.) which change in real-time based upon contextual information at the time of attachment.

For example, a dynamic assignment of an IP to a group may be made via a RADIUS authentication server that assigns user1 to a marketing group and user2 to a finance group. The two users may be in the same subnet (user1 – 1.1.1.1, user2 1.1.1.2). When ODL gets the IP to SGT bindings, it is in a position to apply policies based on the policy group membership. ODL will be applying policies based on real-time contextual information from the Radius authentication.

Today SGTs can be used by firewalls (FW) to create topology independent Access Control List (ACL) decisions - since source and destination IP/SGT information can be sent to the firewall. This also provides FW ACL automation since at the time of new endpoint attachment to the network, SXP can update the FW of the new IP/SGT for the endpoint. By extending this type of topology independent policy definition and automation through the SDN controller, it becomes possible to apply it to other services and networking devices.

Within ODL, manipulation of policy groups will often use Group Based Policy (GBP) infrastructure. Source groups in SXP have the same meaning as endpoint groups in ODL GBP. Thus the GBP infrastructure in ODL can be used with SXP SGTs.

This implementation will follow the [1] to the extent possible.

Motivation

Cisco has a wide installed base of network devices supporting SXP. By including SXP in ODL, the binding of policy groups to IP addresses can be made available for possible further processing to a wide range of devices, and applications running on ODL. The range of applications that would be enabled is extensive. Here are just a few of them:

1. ODL based applications can take advantage of the IP-SGT binding information. For example, access control can be defined by an operator in terms of policy groups, while ODL can configure access control lists on network elements using IP addresses, i. e., existing technology.
2. Interoperability between different vendors. Vendors have different policy systems. Knowing the IP-SGT binding for Cisco makes it possible to maintain policy groups between Cisco and other vendors.
3. ODL can aggregate the binding information from many devices and communicate it to a network element. For example, a firewall can use the IP-SGT binding information to know how to handle IPs based on the group-based ACLs it has set. But to do this with SXP alone, the firewall has to maintain a large number of network connections to get the binding information. This incurs heavy overhead costs to maintain all of the SXP peering and protocol information. ODL can aggregate the IP-group information so that the firewall need only connect to ODL. By moving the information flow outside of the network elements to a centralized position, we reduce the overhead of the CPU consumption on the enforcement element. This is a huge savings - it allows the enforcement point to only have to make one connection rather than thousands, so it can concentrate on its primary job of forwarding and enforcing.
4. ODL can relay the binding information from one network element to others. Changes in group membership can be propagated more readily through a centralized model. For example, in a security application a particular host (e. g., user or IP Address) may be found to be acting suspiciously or violating established security policies. The defined response is to put the host into a different source group for remediation actions such as a lower Quality of Service, restricted access to critical servers, or special routing conditions to ensure deeper security enforcement (e. g.,

redirecting the host's traffic through an IPS with very restrictive policies). Updated group membership for this host needs to be communicated to multiple network elements as soon as possible; a very efficient and effective method of propagation can be performed using ODL as a centralized point for relaying the information.

Although the IP-SGT binding is only one specific piece of information, and although SXP is implemented widely in a single vendor's equipment, bringing the ability of ODL to process and distribute the bindings, is a very specific immediate useful implementation of policy groups. It would go a long way to develop both the usefulness of ODL and of policy groups.

Scope

The scope of this work includes enhancing Opendaylight platform with IP-SGT bindings that can be learned from connected SXP-aware network nodes. Implementation will support SXP protocol version 4 according to the IETF I-D [1]. All protocol legacy versions 1-3 are supported as well. Additionally, version 4 adds bidirectional connection type as an extension of a unidirectional one.

The project proposes Yang models that describe SXP protocol messaging and architecture. Finally, learned bindings can be used for a supervised SXP network topology analyses. We can dynamically provide for the end user SXP network topology construction (nodes tree or a whole nodes graph) from a learned data, or detect potential sources for such a IP-SGT binding within a supervised network. Please refer to the previous Section 4 Motivation for additional details on the scope.

Resources Committed (developers committed to working)

Martin Mihálek (mamihale@cisco.com)

Matthew Robertson (mrobertson@lancope.com)

Initial Committers

Miloslav Radakovic (mradakov@cisco.com) IRC: mradakov

William Deigaard (soren@rice.edu)

Matthew Robertson (mrobertson@lancope.com)

Vendor Neutral

There is existing code.

No vendor package names in code.

No vendor branding / trademark present in code or output of build.

No vendor branding / trademark present in documentation.

Meets Board Policy (including IPR)

Inbound Code Review has been performed with no issues found (Phil Robb - 10/22/2014).

References

[1] M. Smith, R. Kandula - Source-Group Tag eXchange Protocol (SXP)