DEPLOYMENT GUIDE

PENSANDO

Pensando Enterprise Deployment From Start to Finish

The explosion of data generated by applications inside and outside of the data center has businesses of all sizes facing stark choices: scale up capacity with a traditional IT architecture, or move more workloads to public clouds. Either approach means IT staff often end up spending more time managing complexity and infrastructure than they do innovating for their enterprise.

Pensando has created a third option: the Pensando Distributed Services Platform, the first secure, programmable, edge-accelerated solution that directly addresses the generational shift occurring as data pushes to the edge of the cloud.

The Pensando platform delivers a powerful, scalable combination of networking, security, and analytics capabilities. This guide describes how these features can be introduced in an enterprise data center without disrupting existing operations.

The Pensando Distributed Services Platform

The foundation of a Pensando platform deployment is a set of *Distributed Services Cards* (DSCs)—custom, fully-programmable processors optimized to execute a software stack, and delivering cloud, compute, networking, storage and security services wherever data is located. The DSCs are centrally managed and monitored by the *Policy and Service Manager* (PSM), which runs as a fault-tolerant cluster of virtual appliances.

The comprehensive set of services delivered by the Pensando platform can be deployed across any environment in a phased approach, and these capabilities can be implemented gradually to minimize disruption. In addition, the Pensando platform's REST APIs and automation features enable integration with a customer's existing management environment. At each deployment stage, administrators can measure and evaluate the impact of each new service. Incremental deployment of services enables familiarization and feature qualification with minimal service impact and then the new services can be refined and customized.

The remainder of this document describes a typical path that can be followed for gradually introducing the Pensando platform into an enterprise data center without requiring a large upfront financial investment, and without steep learning and qualification curves.

Introducing DSCs as NICs

DSCs are shipped as pre-installed components within servers from top hardware vendors, or can be installed in existing systems in place of a traditional NIC. The first step in leveraging the capabilities of the Pensando platform is to enable DSCs as regular NICs within the existing enterprise network, using the drivers delivered or supported on all major operating systems. (Linux drivers are in-box and upstreamed as of the 5.4 kernel release, and are also available for older Linux versions, VMware ESXi, and Microsoft Windows Server.)

As each host is deployed and its DSC is enabled, it can be managed like any other server. Even in this most basic mode of operation, the DSC is a state-of-the-art device with advanced CPU offload and visibility capabilities that extend far beyond a traditional network adapter. The DSC supports Link Aggregation Group (LAG) with the Link Aggregation Control Protocol (LACP) over its interfaces for high availability—just like any other NIC.

Introducing the PSM and Gaining Visibility

The next step in the journey is to reap more benefit from the Pensando platform by subscribing to a Policy and Services Manager (PSM) license together with a **Silver** Services Package to control the DSCs and gain more operational visibility.

The PSM is a highly scalable management platform that runs centrally on industry standard servers. For fault tolerance and scalability, the PSM is implemented as a cluster that executes on a minimum of three VMs that should run on different physical hosts.

DSCs can be associated with the PSM in one of two ways. Using the `penctl` utility on the host, the administrator can specify the IP address of the PSM. Alternatively, a network administrator can configure a DHCP server to provide the address of the PSM to the DSCs, based on a DHCP Option 60 request and an Option 43 response, allowing for PSM address configuration with minimal effort.

Once a DSC has the address of the PSM, the DSC requests "admission" by the PSM. The administrator can specify whether DSCs are admitted automatically, or whether explicit consent must be given for admitting each DSC.

Once a DSC is admitted, the PSM offers valuable visibility features. The administrator can use the PSM to access telemetry data collected by the DSCs ("Fields" options in Figure 1) organized by various categories ("Measurement" options in Figure 1).

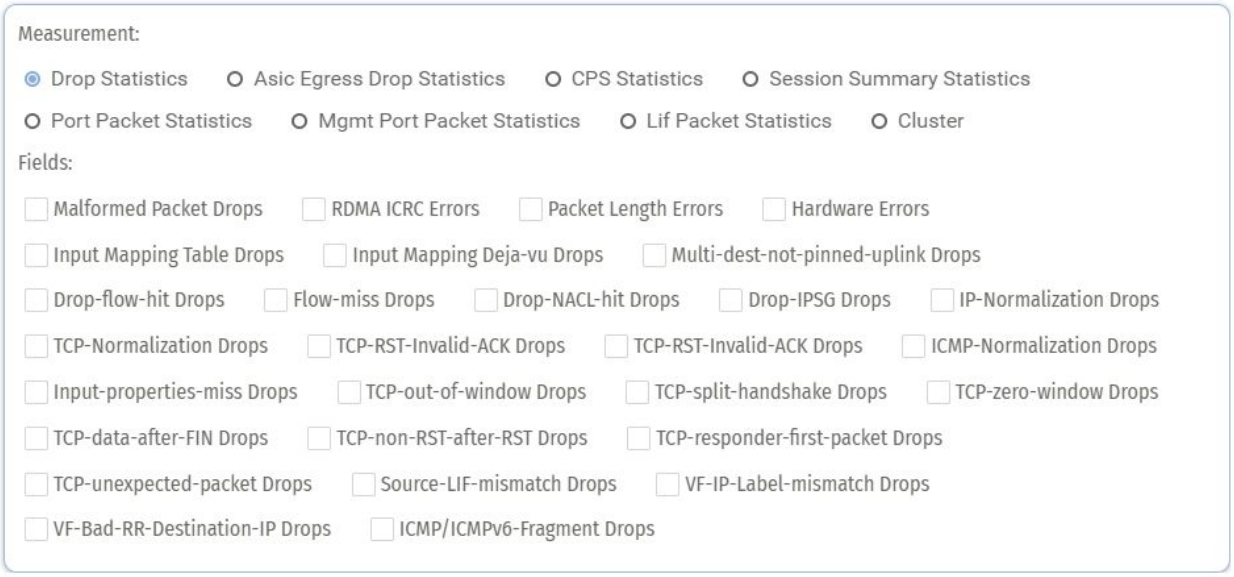

Figure 1. PSM telemetry data-gathering options

A subset of these metrics can be selected to create custom graphs such as the one shown in Figure 2 below. Graphs can be saved by name, showing the latest metrics values. The result is a comprehensive dashboard of the health and performance of the hosts, applications, and the platform itself.

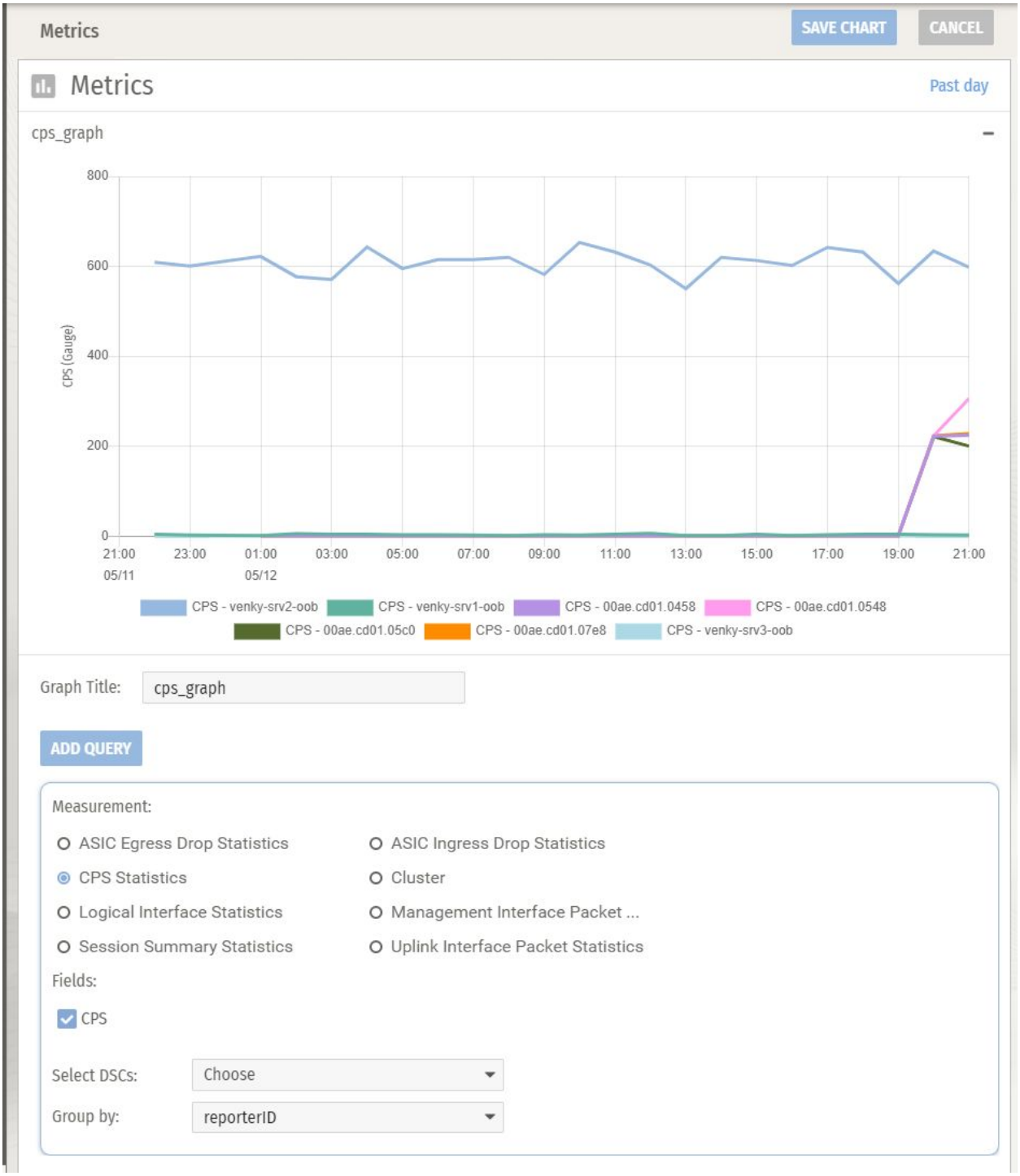

Figure 2. Creating a custom graph on the PSM

The administrator may also activate bi-directional interface-based mirror sessions, which create a copy of each packet entering and exiting a selected physical interface of the card, and sends the packet to a collector using standard ERSPAN (Encapsulated Remote Switch Port Analyzer) encapsulation. Mirror session configuration allows the administrator to instantly have full visibility of the interface's traffic to troubleshoot networking or security issues, without having to deploy a dedicated infrastructure with tap points and a separate collection

network. Note that existing Top-of-Rack ERPSAN implementations are only unidirectional, whereas Pensando DSCs are unique in having full bi-drectional visibility.

Flow Level Visibility

By using the PSM and a Silver Services Package license subscription, the administrator can activate the **Flow aware** Feature Set on its DSCs and unlock a number of features that allow further visibility of network traffic.

Mirror sessions can be activated with flow-based granularity rather than a coarse-grained interface level. As shown in Figure 3, the administrator can configure mirror sessions to a level as fine as a flow identified by a 5-tuple: source and destination IP address, transport protocol, source and destination transport port. Only packets that match the defined policy are mirrored and sent to a specified collector, which significantly reduces any tap network bandwidth requirements, compared with interface-based mirroring.

The DSCs can be configured with multiple collectors to receive mirrored traffic, based on different policies[1].

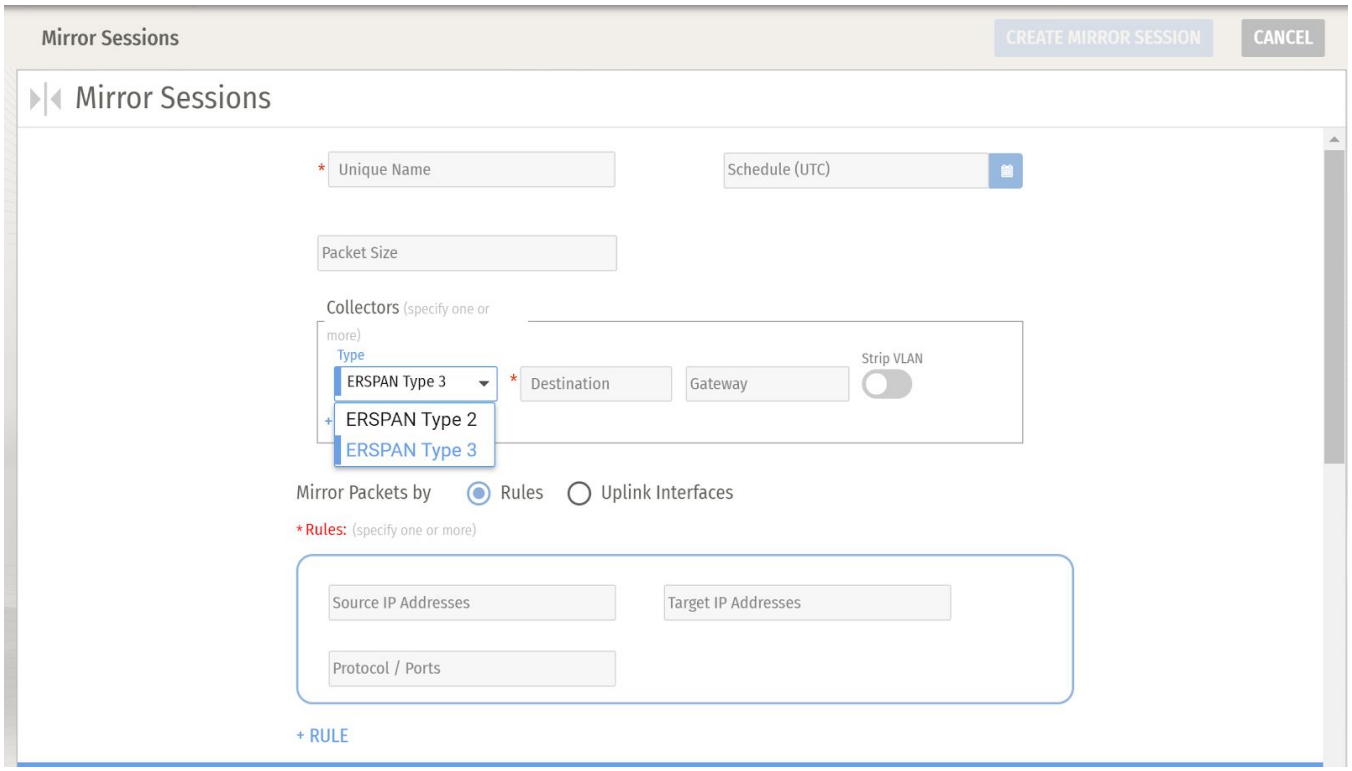

Figure 3. Configuring mirror sessions

DSCs also have the ability to collect a broad range of statistics on all flows. The administrator can use the PSM to configure policies specifying which flows should be monitored. As shown in Figure 4, each monitored flow is identified through the 5-tuple: source and destination IP address, transport protocol, source and destination transport port.

[1] Please see Release Notes for actual scale limits.

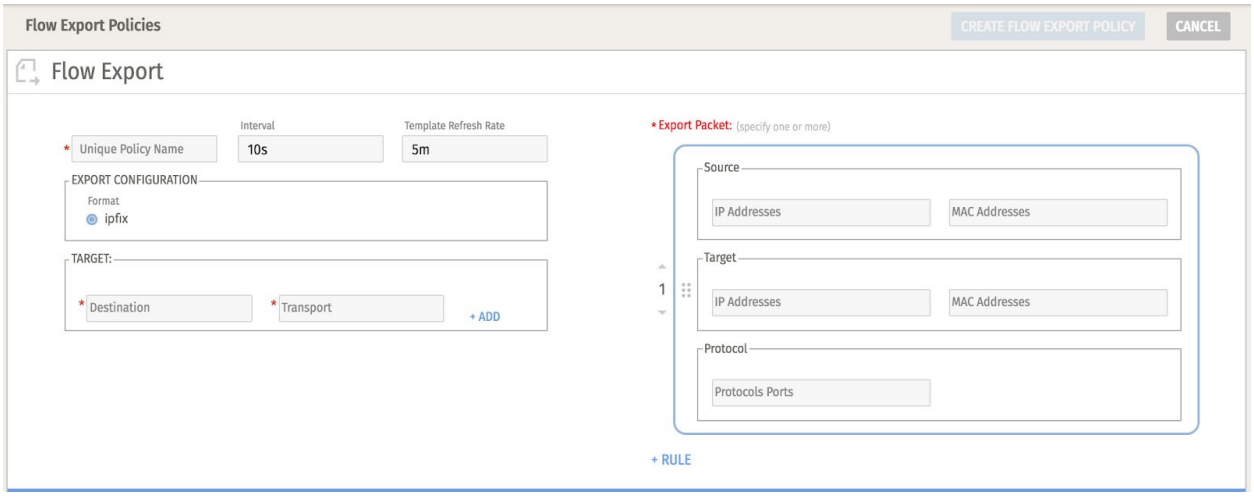

Figure 4. Flow export configuration

The PSM administrator specifies the collector (or target) that should receive the flow information in IPFIX format and the transport (protocol and port) that should be used.

Unlike typical enterprise network environments, the PSM administrator does not have to specify which exact DSC should be configured for flow monitoring and exporting. In a fully integrated manner, the PSM and DSCs work together to ensure that flow collection and the export destination is available to all DSCs, and any DSCs involved in the flow will collect and export the relevant information. As a result of this fully integrated approach, if the workload generating a flow moves through the network (e.g. a VM is moved through vMotion to a different server), the platform keeps seamlessly monitoring and collecting flow information without any required intervention by any administrator.

Through these visibility functions, administrators can gain insight into the traffic patterns in their enterprise data centers, to troubleshoot performance issues, or to identify performance bottlenecks even before they become an issue. Moreover, administrators might use the information collected as a baseline of what legitimate traffic should look like and use such a baseline to drive enforcement policies, as described in the journey's next step.

Security Enforcement

The Platinum Services Package takes the PSM administrator on the next step in the journey by entitling them to associate the **Flow aware with firewall** Feature Set to their DSCs, thereby creating a distributed stateful firewall. The Pensando platform provides a particularly efficient solution for the protection of data center East-West traffic, which traditional firewall appliances are not well positioned to enforce. In fact, using a firewall appliance to police East-West traffic causes the well-known "traffic tromboning" effect: in order to be inspected by the firewall, traffic between data center hosts must traverse the spine-leaf data center network fabric twice, as shown in Figure 5.

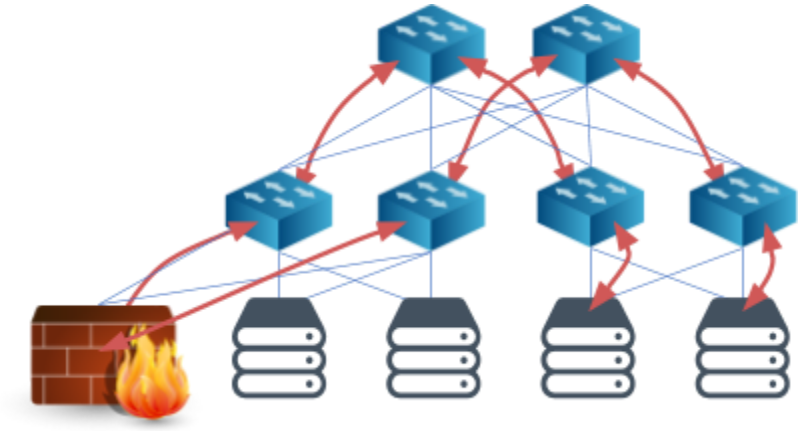

Figure 5. Tromboning

With Pensando, DSCs are already in the data path, and can inspect traffic directly. No additional load is placed on the network; no additional appliances need to be purchased and managed, as shown in the figure below.

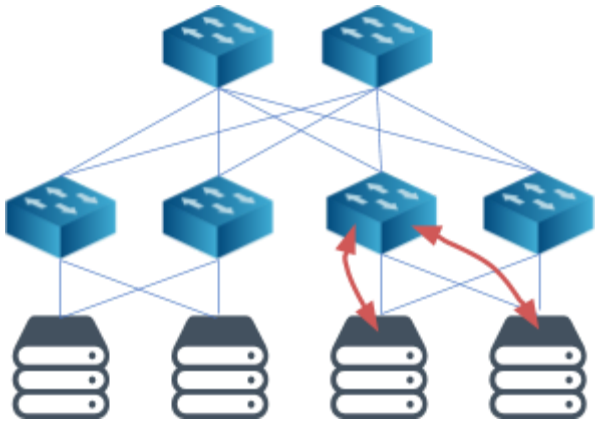

Figure 6. Simplified firewall traffic

The PSM administrator determines which packets should be forwarded and which should be dropped, depending on security policies defined with a granularity as fine as a 5-tuple: source and destination IP address, transport protocol, source and destination transport port, as shown in the figure below.

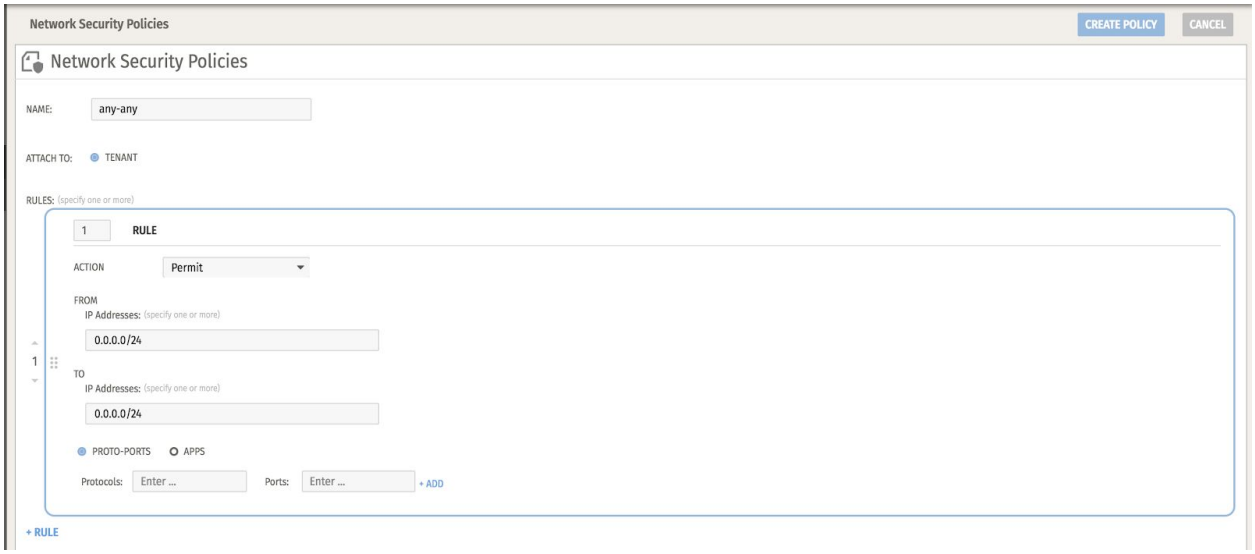

Figure 7. Setting security policies

The network administrator can have full visibility on the firewall operation by exporting the firewall logs from the DSCs enforcing the firewall policies directly to "syslog" collectors. The PSM administrator can specify a single collector for all logs, or distribute the logs to different collectors based on the action that is being logged (e.g., allow, deny, reject, etc.).

The **Flow Aware with Firewall** Feature Set supports all features presented in previous sections in addition to security enforcement. Hence, the PSM administrator can define policies for mirroring packets belonging to specific flows to ERSPAN collectors, export information about selected flows to IPFIX collectors, and specify which workloads can communicate, thereby realizing the goal of microsegmentation.

Custom Orchestrators and Controllers

In addition to the graphical user interface (GUI) used in the previous examples, the PSM offers a REST (REpresentational State Transfer) API (Application Programming Interface) for the programmatic configuration of all features offered by the Pensando platform. The programmatic API enables the integration of the network, security, and visibility services offered by the Pensando platform to an existing orchestrator used by an enterprise for enabling cloud-like automation of their data center.

Conclusion

The Pensando platform offers distributed network, security, and visibility services that are executed on Distributed Services Cards installed in enterprise data center hosts with central management and monitoring by a Policy and Services Manager. This Deployment Guide illustrates how the journey towards platform adoption can be taken incrementally in enterprise data centers so that users can gradually become familiar, while minimizing the risks associated with introducing a new technology and new solutions in the data center.

About Pensando

Founded in 2017, Pensando Systems is the company pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage and security services to transform existing architectures into the secure, ultra-fast environments demanded by next generation applications. The Pensando platform, a first of its kind, was developed in collaboration with the world's largest cloud, enterprise, storage, and telecommunications leaders and is supported by partnerships with HPE, NetApp, Oracle, IBM, Equinix, and multiple Fortune 500 customers. Pensando is led by Silicon Valley's legendary "MPLS" team – Mario Mazzola, Prem Jain, Luca Cafiero, Soni Jiandani and Randy Pond – holding an unmatched track record of disruptive innovation having already built $8Bn/year businesses across storage, switching, routing, wireless, voice/video/data, & software-defined networking. The company is backed by investors that include Goldman Sachs and JC2 Ventures. For more information, please visit www.pensando.io

DOCUMENT REVISIONS

Pub Date	Exp/Review Date	Description
3-Aug-2020		Initial release.
18-Jan-2021	19-Jan-2022	Non-technical revisions.