”A Rule Recommender using Unified Policy-Flow-Virtual Machine Analyzer (UPFVA) for Workload Management”

Tech Con 2025 Abstract 611

HPE Edge;

A Rule Recommender using Unified Policy-Flow-Virtual Machine Analyzer (UPFVA) for Workload Management

Abstract

With the rapid growth of Generative AI and high cloud solution demand, a secure, consistent, and performant data center becomes a high priority. Data center virtualization or software defined data center (SDCC) uses hypervisors to manage virtual machines (VM) that have software or applications on the operating systems. To better manage the east-west traffic for VM-to-VM communication, our cloud-based event-driven UPFVA solution utilizes IP Flow Information Export (IPFIX) data from Aruba AOS-CX switches and virtual machine client information from vSphere integrating to GreenLake Aruba Central Next Generation (CNX) [1] for application visibility and dependency pattern analysis. If an anomaly is detected, UPFVA, based on the flow information, triggers IP-to-IP rule recommendations. The rules can be auto-provisioned from cloud to an Aruba distributed services switch (DSS) through AMD Pensando Policy and Services Manager (PSM) for east-west firewall policy management. DSS then sends back the flow blocked reason to UPFVA, providing a threat mitigation closed loop workflow for an autonomous data center workload management system.

Problem statement

A traditional firewall setup blocks the external traffic to internal traffic. However, in a private cloud or data center the traffic can flow internally from one VM to another. One of the most common internal cyber-attacks is lateral movement. This type of threat starts with the attacker gaining access to a VM or a laptop. It goes through the internal network to exploit enterprise sensitive customer data. A careless employee or malicious insider can provide internal access to the attacker. One example is Anthem breach [2], which resulted in a 16 million dollars loss for the company. The common approach to protect the internal network is to use private VLAN with micro segmentation. But this is not enough to secure any large enterprise internal network. For example, a common use case is direct access between a web server and a database server. This is undesired but the flow is permitted in the same private VLAN. Understanding the traffic pattern for each IT system and accurate detection of anomalies can prevent internal advanced persistent threat type of attacks. However, a major challenge that data center administrators face is unprecedented IT complexity. The high demand for AI (Artificial Intelligence), cloud based microservices and dynamic application environment changes, lead to unmanageable datacenter IT operations. Manual tracking and constant auditing are no longer able to preserve a highly secure data center.

To help maintain operational SLAs of a data center, UPFVA provides an automated secure data center workload management system. It uses IPFIX and virtual machine information to generate an application dependency mapping (ADM) pattern to detect anomalous application behavior that differs from the traffic pattern baseline. The automated mitigation action utilizes the distributed firewall capability on Aruba's 10000 series targeting top of rack (ToR) switch profile in data centers to block the unexpected east-west flow traffic.

Our solution

UPFVA uses security as a service cloud-based design to manage the east-west traffic in a customer's network. Furthermore, it provides more granular control to direct the application traffic flow in an internal network. The solution provides a holistic view of the customer's traffic flow to ensure a secure data center. In Figure 1, the framework includes three modules, Flow and VM Visualizer, Pattern Analyzer, and Mitigator.

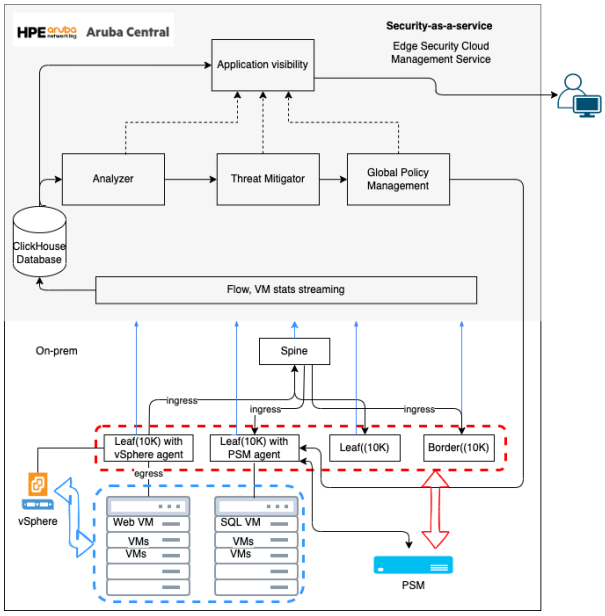

Figure 1.UPFVA architecture design

Flow and VM Visualizer Aruba Central acts as a flow collector in the cloud to stream IPFIX data from Aruba AOS-CX switches. The data includes source and destination IPs, protocol, port used, bytes and packets sent and received and collect timestamp. It also contains the name of the application that the flow belongs to. By deploying a containerized agent on CX switches to access on-prem vSphere data, UPFVA in Aruba Central collects VM IPs, operating systems, labels, and tags. This allows UPFVA to aggregate the traffic flow for IPFIX and VM data. VM labels are key-value pairs that are often used by admins to categorize and manage VMs based on the functionalities. For example, app: {webserver, database-server, frontend-server}, env: {customer relation, internal, production}. With the source and destination applications information, the traffic can be predefined into classes. As a result, the visualizer builds an application dependency mapping. For example, from Figure 2, the bottom purple flow indicates that the core service is communicating with the mysql-3 and mysql-4 databases.

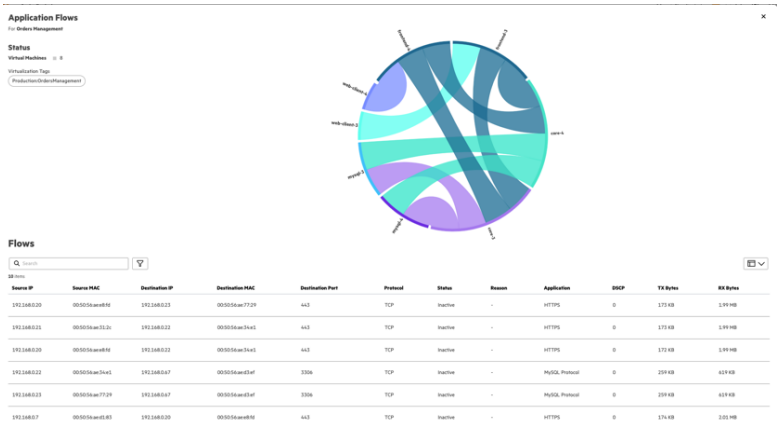

Figure 2. Application Visualizer

Baseline Pattern Analyzer UPFVA uses event driven design to depict the network traffic and to detect anti-pattern traffic flows in a customer's network environment. The visualizer provides a snapshot of flows at any point of time in the network. CNX as a cloud management system gathers customer's network data over time. The historical flow and VM data enable UPFVA to perform application dependency pattern analysis with supervised classification. To ensure the uniqueness of each application in a large datacenter, UPFVA utilizes VM-Tag in the dataset for better classification results. VM-tag is a common practice in a datacenter or a cloud provider to categorize resources for business purposes {business-unit: R&D, marketing, cost-center:123}. Once the pattern-based application dependency mapping model is built, it can be used to flag anomalies when an anti-pattern communication between two applications occurs. Figure 3 provides an example of a violation of the application communication pattern where a frontend server accesses inventory database server directly. Overall, UPFVA can be used effectively to prevent lateral movement from attackers with the traffic pattern baseline model.

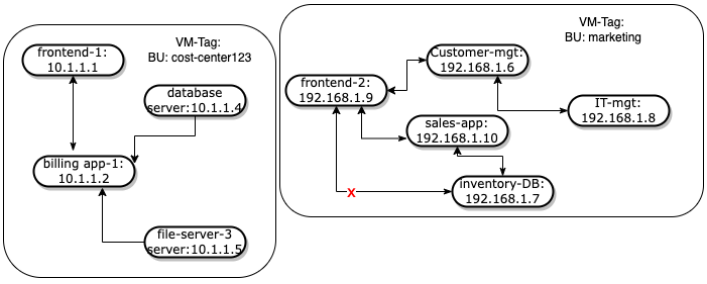

Figure 3. Anomaly pattern detection

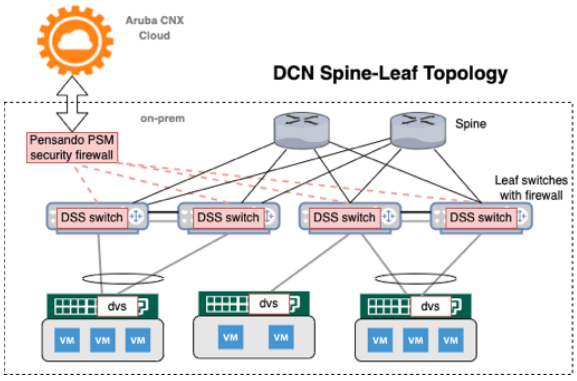

Figure 4. Mitigator Policy Management

Threat Mitigator and Closed Loop Feedback This module utilizes Aruba Central Global Policy Manager to deploy firewall policies on DSS switch through Pensando Policy and Services Manager (PSM) to block the unexpected flow. PSM is designed to establish and manage stateful firewall policies for Distributed Services Switches (DSS, Aruba CX 10000). The PSM uses gRPC to communicate with the DSS and sets the rules to the DPUs of the DSS switches. UPFVA utilizes the PSM integration in Aruba Central to set the policy rules on PSM. The rules will propagate to the DSS DPUs and enable VRF or VLAN network level policy management. In Figure 4, a DSS acts as a firewall device on top of each rack to redirect and manage east-west traffic flow. Unlike traditional centralized firewall management, it provides distributed firewall policies to secure the packet in the access layer allowing admins to manage application traffic efficiently. In Figure 3, the traffic policy rule will be set to deny any traffic from 192.168.1.9 to 192.168.1.7 with a rule name of "database server access violation".

After the flow is blocked, the IPFIX data that is streamed from DSS to cloud contains the policy action to specify that the flow is denied due to enforcing the recommended rule. The rule from CX IPFIX data will be mapped back to the cloud rule that is suggested by UPFVA from the previous module. The blocked reason feedback is visible to the user to confirm the completion of threat mitigation. Figure 6, the table indicates the reason for the flow being blocked.

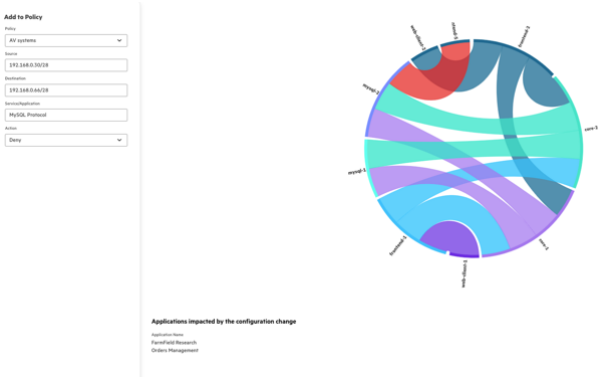

Figure 5. POC policy configuration user interface

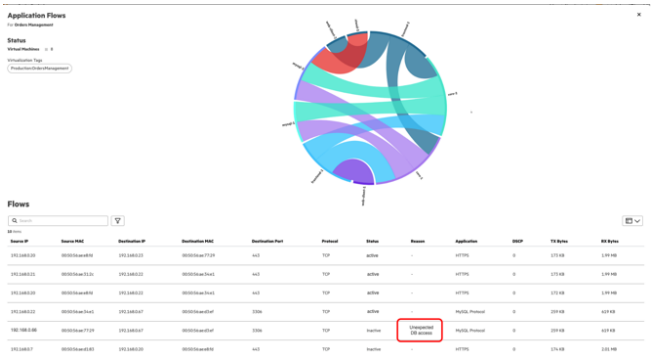

Figure 6. Expected mitigator completeness feedback

Evidence the solution works

UPFVA has been demonstrated at Discover/Atmosphere 2024. The POC (Proof of Concept) showed an unexpected flow between a frontend-5 VM accessing a database VM mysql-2. Refer to Figure 5. After the threat was flagged, UPFVA stopped the traffic between 192.168.0.30/28 and 192.168.0.66/28 by setting the rules on the Distributed Services Switches. And a blocked reason is listed in the reason column in Figure 6. The closed loop block reason provides the mitigation result to the customer. There is high demand from customers for supporting this solution in production soon.

Competitive approaches

The Cisco Nexus Dashboard [4] solution requires an on-prem management system to monitor virtual networks. UPFVA utilizes the GreenLake Aruba Central Next Generation cloud solution to create 3rd party application plugins which does not need on-prem resources for extra management and hence is cost effective. A generic event driven automatic mitigation action achieves a zero-trust network security architecture.

Current status

The data collection pipeline for CNX has been productized. It includes application visibility with IPFIX data, and vSphere virtualization pipeline. The policy configuration for CX 10K model in CNX, including a PSM cloud integration, is planned to be released in late 2024.

Next steps

The full closed loop workflow, from ML based behavior baselining to automated remediation is on the roadmap to be delivered in 2025.

References

[1] Aruba CNX-Next Generation HPE Aruba Networking Central, https://www.arubanetworks.com/products/network-management-operations/central/next-generation/

[2] Anthem breach, https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach

[3] ClickHouse database, https://clickhouse.com/

[4] Cisco Nexus Dashboard, https://www.cisco.com/site/us/en/products/networking/cloud-networking/nexus-platform/index.html