DPtech service chain Technical White Paper

Hangzhou DPtech Technologies Co., Ltd.

May 2014

1. Overview

The enrichment of network applications has shifted users' focus from network interconnection to network identification applications in order to meet the applications' requirements for security, availability, and fast speed. Cybersecurity convergence has become the development trend of the industry. Against this backdrop, network vendors have been introducing devices, deploying services boards in switches for security protection. Although this form of device, which combines switches and boards, integrates security functions into a single chassis, it is still a stand-alone device sharing backplane and power supply in essence due to the fact that network, security, and application delivery usually run in independent operating systems and present multiple IP addresses externally on the network.

When multiple services boards are required in deployment to realize functions such as firewalls, IPS, load balancing, flow control, and behavior auditing, the traditional form of device, i.e., switch + board, is plagued by the following limitations:

• It is complicated to perform traffic management.

As the services board and switch are independent devices, it is necessary to plan and deploy specific mode for each service board during traffic management before developing a plan about how traffic enters the service board from the switch and then returns to the switch. The traffic management mode is particularly complicated when deploying multiple service boards. In addition, this management mode imposes a great number of restrictions on the type and quantity of service boards.

• It is complicated to perform maintenance and configuration.

Service boards and switches are interconnected through invisible built-in interfaces. This requires network operation and maintenance personnel to be very familiar with the product and its configuration, thus bringing great difficulty to maintenance and configuration.

• Undifferentiated security protection.

In switch + board mode, traffic can only pass through all boards in series in the same sequence. However, in actual networking, different services have different security requirements. For example, service A needs to go through FW and IPS processing, while service B only needs to go through FW processing. Traditional solutions cannot provide differentiated security protection for different services, so some service boards have to process traffic that is unnecessary to process, resulting in increased latency, compromised equipment performance, and growing costs.

2. Introduction to service chain Technology

service chain technology is an innovative traffic management technology initiated by DPtech, with an aim to realize traffic management characterized by flexible scheduling between different

service modules in a converged device. As the core technology of DP xFabric solution, the flow definition technology is based on the ConPlat operating system implementation converged in DPtech L2 ~ 7, the advantages of which, compared with the traditional traffic management method, are shown as below:

• Traffic management policy is configured through Web interface, enabling simple and simplified traffic management configuration.

• Flexible definition of the type of services flowing through the service boards is allowed and a traffic management policy based on services is realized.

• Besides, the sequence in which the business streams flow through the service boards can be defined on a flexible basis, enabling different business streams to pass through the boards in a user-defined order.

Fig.1 service chain Interface

Figure 1 shows the interface of service chain, from which we can see four modes of implementation supported by this technology:

• Online forwarding mode Service modules are deployed in the network in an online manner and packets are forwarded at layers 2 and 3. It usually applies to service types such as firewalls, load balancing, etc.

• Online transparent mode Service modules are deployed in the network in a transparent manner. It usually applies to service types such as IPS and flow control.

• Bypass mode Service modules are deployed in the network in a bypass manner. It is usually used in combination with the online forwarding service to realize multiple deployments of various service boards.

• Transparent serial mode Service modules are deployed in the network in a transparent manner.

It may be used with the online forwarding services to realize multiple deployments of various service boards.

2.1 Online forwarding mode

Fig.2 Online forwarding service

Figure 2 shows the online forwarding mode. In this mode, the type and sequence of data streaming through the service boards can be defined based on physical port, source IP address and destination IP address. Once the policy is configured in place, the main control board generates corresponding interface entries and issues the policy. When the packet reaches the inbound interface of the DPX19000/DPX8000 device, a policy query is performed. If there is no service chain policy available for the source IP address, destination IP address or inbound interface, the packet will only be forwarded through ordinary layers 2 and 3 before forwarding through the outbound interfaces. Once the service chain policy is deployed in the source IP address, destination IP address or inbound interface, the packet will be forwarded to the chip's ACL corresponding to the inbound interface in accordance with the instructions from the main control, and then to the service board corresponding to Service 1, which is shown in the figure.

When the service board of Service 1 receives the packet, it will match the table entry. Based on the results, it will discard any undesired packets for this board or send them to a service board software for further processing. At this time, the service board will initiate a query on whether this data stream has established a session on this board or not. If no session has been established, a new one will be created; if a session has already been established, please continue to apply other policies configured for this service board. When Service 1 has been processed, further query on whether a service board has been configured following this board will be made. If not, the service stream will be forwarded on this board in layers 2 and 3 before sending out of the device. If the query result shows a service is configured following this board, the packet will be sent to the next service board through the high-speed channel between the boards for further service processing.

The service board for the online forwarding service provides master/standby mode. The master/standby boards work in a prioritized manner. In other words, as long as there is a master service board, the business data stream will be preferentially forwarded to the master service board. The business data stream will be automatically switched to the standby service board only when the master service board fails, so as to ensure proper data forwarding and improve the reliability of the device.

The online forwarding service supports data streams flowing through different service boards according to the IP address object. If this option is activated, only data streams corresponding to

the address object will pass through the service board. For data stream that fails to meet the conditions, the service board will directly forward them to layers 2 and 3 before sending them out of the device.

2.2 Online transparent mode

Fig3 Online transparent service

Figure 3 shows the interface of the online transparent mode. In this mode, a pair of physical interfaces, i.e., inbound and outbound interfaces, should be assigned. Upon the configuration of service chain policy, the main control board generates corresponding interface entries and issues the policy. When the packet reaches the inbound interface of the DPX19000/DPX8000 interface, the board looks for issued ACL matches. If it matches, the packet will be forwarded to corresponding service boards for business processing. When the processing is completed, the packet will inquire for service chain policy. If there is no service followed, the packet will be sent out of the device through pre-defined outbound interface. If there is a service followed, the packet will be sent to the next service board for processing.

The transparent service supports the bypass feature, which allows the packet to skip failed service board in case of any failure found in the board. This ensures a proper forwarding of the packet and a reliable network.

2.3 Bypass Mode

Fig.4 Bypass Service

Figure 4 shows the interface of the bypass mode. The service module of bypass service is externally connected to the network and not involved in forwarding any packets. All packets are retained in the service board after entering bypass service board without sending out of the device. Once the bypass service is configured, packets reaching the inbound interface of DPX19000/DPX8000 device and matching service chain policy will be mirrored to corresponding service boards for processing.

The bypass service mode can be used in conjunction with the online forwarding mode to realize multiple board deployment. At this time, you need to check the “Yes” box of the “Any online business available?” option, and configure correspondingly in the online forwarding mode. In this mode, the packet, after reaching the bypass interface, will be mirrored to the bypass service board, and then handled as online service for service processing and forwarding.

2.4 Transparent serial mode

Fig5 Transparent serial mode

Figure 5 shows the interface of the transparent serial mode, which should work with the online forwarding mode to realize multiple deployments of service boards. Once the service chain is configured, packets reaching the inbound interface of DPX19000/DPX8000 device will be forwarded to Service 1 in the transparent serial mode in accordance with the ACL rule on the inbound interface as shown in the figure. Then the packets will be processed on service boards for Services 2 and 3 (skip this step if no Services 2 or 3 is configured). Afterwards, the packets will be sent to the online forwarding service board through the high-speed channel between the boards for further service processing before sending out of the device.

The transparent serial mode works in a prioritized manner. In other words, as long as there is a master service board, the business data stream will be preferentially forwarded to the master service board. The business data stream will be automatically switched to the standby service board only when the master service board fails so as to ensure business reliability. In addition, the transparent serial mode supports the bypass feature, which allows the packet to skip failed service board in case of any failure found in the board. This ensures a proper forwarding of the packet and a reliable network.

3. Typical applications

The four modes of service chain technology enable simplified traffic management on a single service board and among multiple boards.

- **Typical application 1**

Requirements: Deploy a firewall and a UAG board. The data flows through the firewall and the UAG board serves as an external connection and perform behavior auditing.

Service chain policy: Configure UAG on the bypass service board. Simply check the “Yes” box of the “Any online business available?” option, and configure the firewall service board on the online forwarding service.

- **Typical application 2**

Requirements: Deploy firewalls, load balancing, IPS, and UAG service board. The data flows through the firewall, IPS, UAG, and load balancing service boards in turn for forwarding.

service chain policy: Service 1, Service 2 and Service 3 are configured on firewall, IPS, UAG service boards in the transparent serial mode (the sequence of which is subject to adjustments), and configure Service 1 on the load balancing board in the online forwarding mode.

4. Summary

Service chain constitutes one of the four core technologies from the DP xFabric solution. When used alone, it is capable of achieving traffic management among various service boards upon simple configuration through Web interfaces. Compared with traditional switch + board products whose drawbacks include complicated traffic management, unchangeable sequence and limited types of boards, the steam definition technology not only supports the richest array of service boards in the industry, but also flexible in configuring various user-defined traffic management policies. In conjunction with other core technologies from the DT xFabric solution, including VSM all-in-one virtualization, OVC one-to-many virtualization and VEM vertical virtualization, the service chain technology empowers a simpler, more intelligent and reliable application definition network, helping its users build a new generation of security virtual network featuring cybersecurity convergence, comprehensive coverage, one-click configuration and multiple subnetworks.

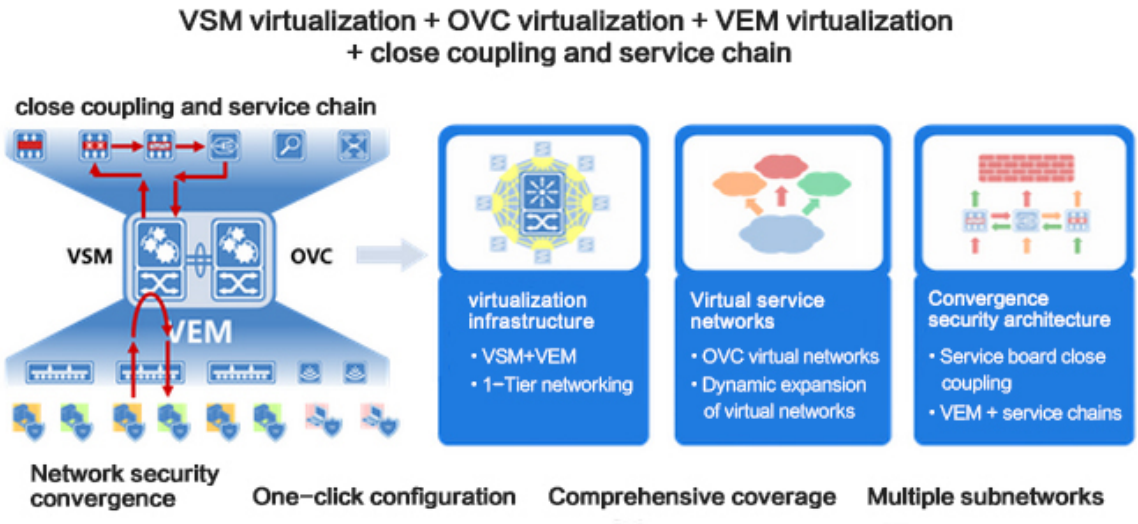

Fig.6 DP xFabric Solution Architecture