GTI
Orchestration Framework for Secure Access Service Edge (SASE) White Paper

Version:	V1.0.0
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Working Group	**5G ENS**
Task	**Research on Orchestration frame technology for SASE**
Source members	CMCC
Support members	
Editor	Jia Chen(CMCC), Kai Yang(CMCC), Peng Ran(CMCC), Haiyan Zhao(CMCC), Cancan Chen(CMCC), Yuhang Zhao(CMCC), Haiyang Su(CMCC), Xinmiao Yang(CMCC), Dongjie Lu(CMCC), Yi Jiang(CMCC), Li Su(CMCC), Bangling Li(CMCC)
Last Edit Date	（05-10-2024）
Approval Date	

Confidentiality: This document may contain information that is confidential and access to this document is restricted to the persons listed in the Confidential Level. This document may not be used, disclosed or reproduced, in whole or in part, without the prior written authorization of GTI, and those so authorized may only use this document for the purpose consistent with the authorization. GTI disclaims any liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

机密性:本文件可能包含机密信息，而对该文件的访问权限仅限于机密级别的人员。在未经GTI事先书面授权的情况下，本文件不得使用、披露或复制，或全部或部分复制，而授权人仅可将本文件用于与授权一致的目的。GTI对本文件所载资料的准确性、完整性或及时性不承担任何责任。本文件所载资料如有更改，恕不另行通知。

Document History

Date	Meeting #	Version #	Revision Contents

Table of Contents

1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

［1］GTI, GTI Operator Secure Access Service Edge White Paper(Paper_v1.0.4)

［2］Gartner, Hype Cycle for Enterprise Networking 2019

2 Abbreviations

Abbreviation	Explanation
SASE	Secure Access Service Edge
SD-WAN	Software Defined Wide Area Network
SWG	Secure Web Gateway
CASB	Cloud Access Security Broker
FWaaS	Firewall as a Service
ZTNA	Zero-Trust Network Access

3 Overview

3.1 Background

The shift to mobile and cloud has accelerated enterprise digital transformation, moving core business and data to the cloud and changing work styles. The traditional network security architecture is no longer fit for the digitalisation and cloudisation of business. For example, traditional security strategies are primarily based on boundary protection, which deploys security devices at the perimeter of the enterprise network to protect its network and data. However, business digitisation and cloudisation have blurred traditional network boundaries, making it impossible to address all security issues at a single boundary; security capabilities can only be added in multiple locations based on security requirements; and stacking multiple security technologies can increase the complexity of enterprise security systems, leading to operational difficulties and reduced efficiency[1].

With the digitisation and cloudisation of business, enterprises need to flexibly configure their network and security services to accommodate different network access scenarios. In its Hype Cycle for Enterprise Networking 2019 report[2], Gartner proposed the Secure Access Service Edge (SASE) as a solution to this problem, offering simplicity, efficiency, security and flexibility.[2].

The secure access service edge is an emerging service architecture that combines SD-WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of enterprises.

SASE needs to coordinate and orchestrate network and security functions to embed security functions into the network flow and to flexibly deploy security functions as required by the network flow, which requires a comprehensive orchestration framework.

3.2 Challenges for building Orchestration framework for SASE

SASE services differ significantly from traditional enterprise networking and present the following challenges that make it difficult to directly apply the traditional security and network function orchestration management architecture:

1. Difficulty in aligning network and security orchestration

SASE services require the integration of network and security orchestration, whereas in traditional security and network function orchestration management frameworks, networking and security are separate systems with different management interfaces and controllers. It is difficult to reconcile the different management methods of network and security orchestration,and to achieve unified orchestration, which causes big troubles in collaborative orchestration and management. As a result, the forwarding paths obtained from traditional network orchestration only solve network forwarding from the origin to the destination, while not including security functions. It is impossible to integrate security functions into the network forwarding paths and collaborative network and security orchestration cannot be achieved.

2. Distributed business requires distributed security

In the new enterprise networking model, physically widely distributed branches increase network and security costs. SASE services aims to satisfy security requirement of the distributed of enterprises branches with low cost, which requires the distributed deployment but unified and automated management of network and security functions.

3. Network and security policies can conflict

In SASE services, network and security policies often impact each other and need to be managed together. Traditional security and network function orchestration management frameworks do not have a unified controller and it is difficult to collaboratively formulate, manage and enforce security and network policies.

4. Too many vendors, difficult to be compatible

SASE services require a variety of network and security functions, it is a big challenge for a single vendor to meet all the security requirements.

In summary, to address the new challenges of network and security function orchestration in SASE services, it is necessary to build an new orchestration framework for SASE.

4 Requirements of SASE Orchestration Framework

To address the challenges mentioned above for the SASE Orchestration Framework , the following requirements need to be satisfied:

1. Orchestration of network and security in an integrated manner

The security and network measures in Orchestration framework for SASE must be connected, integrated. Business orchestration is required to be located above the network and security function management, compatible with the different management methods of both, to carry out coordinated orchestration. Thus, the network and security operations can be coordinated within an integrated architecture, ensuring consistent and synchronized function.

2. Centralized management of network and security functions with distributed deployment

The network and security infrastructure in Orchestration framework for SASE should be deployed across multiple geographical locations, as well as different nodes, with centralized management from a single centre.

3. Consistent management of network policies and security policies

The network and security operations should be managed, configured, and distributed centrally.

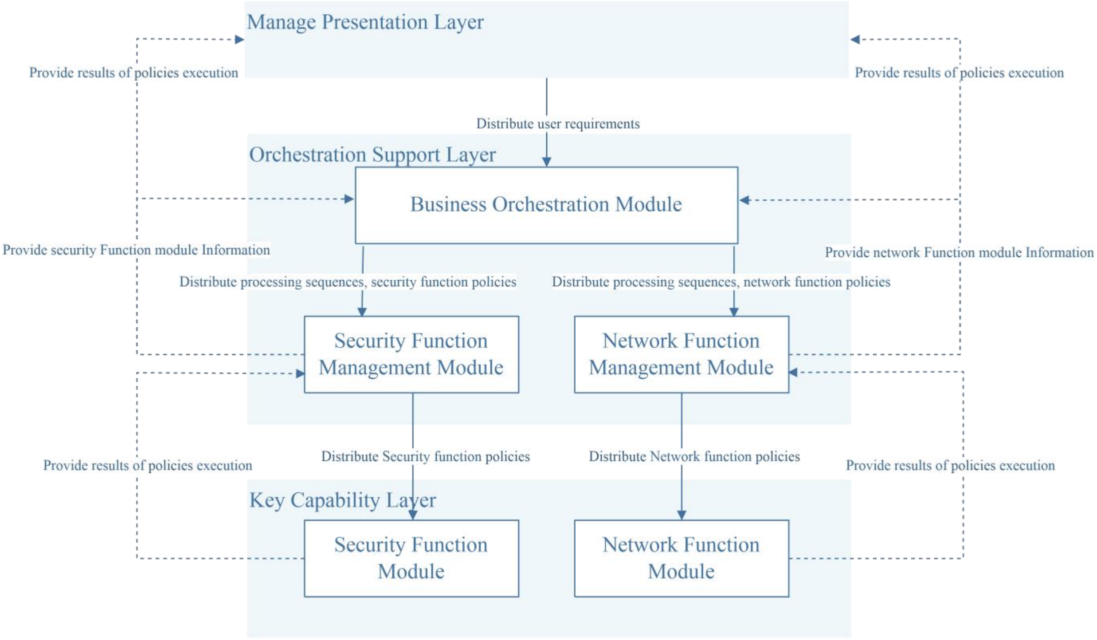
4. Interoperate with networking and security functions from multiple vendors

Compatibility between multi-vendor network devices, security devices and solutions should be achieved.

5 Reference SASE Orchestration Framework

5.1 Overview of Reference Orchestration Framework for SASE

Orchestration Framework for SASE is used to orchestrate security and network capabilities to secure the service access process. The framework is illustrated in Figure 5-1.



Manage Presentation Layer
Provide results of policies execution
Provide results of policies execution
Distribute user requirements
Orchestration Support Layer
Business Orchestration Module
Provide security Function module Information
Provide network Function module Information
Distribute processing sequences, security function policies
Distribute processing sequences, network function policies
Security Function Management Module
Network Function Management Module
Provide results of policies execution
Distribute Security function policies
Distribute Network function policies
Provide results of policies execution
Key Capability Layer
Security Function Module
Network Function Module

Figure 5-1 Reference Orchestration Framework for SASE

The framework consists of three layers: a management presentation layer, an orchestration support layer, and a capability layer. The orchestration support layer includes business orchestration modules, security, and network function management modules. The capability layer includes security and network function modules.The following is an overview of each layer and the modules it contains:

Management Presentation Layer: collect and issue user policies to the orchestration support layer.

Orchestration Support Layer: integrate security and network functions, analyze and transforms user policies, and selects applicable network and security function modules to construct network and security processing sequences. It includes three modules:

Business Orchestration Module: analyze user policies, and formulate security and network function processing sequences, security function policies, and network function policies.

Security Function Management module: manage security function modules, negotiate resources, transform and issue security function policies, and provide feedback on module status and policy execution results.

Network Function Management module: manage network function modules, negotiate resources, implement security and network function processing sequences, transform and issue network function policies, and provide feedback on module status and policy execution results.

Capability Layer: Provide network and security functions. It includes two different types of modules:

Security Function modules: execute security function policies and can be deployed physically, virtually, or in the cloud at PoPs, CPE, gateways, user terminals, and the cloud.

Network function modules: execute network function policies and can be deployed physically, virtually, or in the cloud at PoP points, CPE, gateways, user terminals, and the cloud.

5.2 Components capabilities

5.2.1 Management Presentation Layer

The Management Presentation Layer is responsible for gathering user policies through interfaces or configuration files, and then sending them to the Orchestration Support Layer. User policies describe the network and security requirements that users expect to achieve and contain both traffic-based and non-traffic-based policies.

Traffic-based user policies: contain information such as source and destination addresses, business types, resource negotiation interfaces, network and security service quality requirements, and access control conditions. The policy's objective is traffic, and its processing behavior includes traffic content awareness, filtering, access control, forwarding, and acceleration, such as filtering traffic for a specified five-tuple.

Non-traffic-based user policies: contain information such as target asset addresses, resource negotiation interfaces, security service quality requirements, execution cycle, and time. The policy's objective is non-traffic objects such as resources, and its processing behavior includes scanning, monitoring, and authentication recognition of the target asset address device, such as vulnerability scanning for devices in a specific IP range.

5.2.2 Orchestration Support Layer

5.2.2.1 Business Orchestration Module

The Business Orchestration Module analyzes user policies to select suitable network function modules and security function modules, develops network and security processing sequences, security function policies, and network function policies, and sends them to the Security Function Management Module and Network Function Management Module.

Processing sequence development: analyze user policies, select and arrange network and security function modules based on the functional descriptions, running states, network information such as network topology, network latency, and network traffic load balancing, and functional characteristics (such as proximity to user-side and resource-side and requirements for computing power) and functional sequence requirements, construct an ordered sequence of security and network functions processing.

Security policy development: accord to user policies, develop security policies for security functions in the processing sequence.

Network policy development: accord to user policies, develop network policies for network functions in the processing sequence.

5.2.2.2 Security Function Management Module

The security function management module manages security function modules, provides information on security function modules, convert and issues security function policies, and reports on the running status of security function modules.

Registration module: receive and aggregate registration information from security function modules.

Monitoring status: monitor the operational status of security function modules.

Resource negotiation: send resource negotiation requests to security function modules or their management systems, including but not limited to resource application and release.

Policy issuance: convert security function policies into specific security function module policies recognizable by selected security function modules, and issues policies.

Information provision: analyze registration information, logs, alarms, and running status of security function modules to provide all managed security function module information to both business orchestration modules and management presentation layers. Security function module information can be retrieved by functional description, unique identifier, and name.

Status reporting: collect information on security function running status, policy execution results, logs, and alarms, and report them to the management presentation layer.

5.2.2.3 Network Function Management Module

The network function management module is responsible for managing network function modules, providing information on network function modules, converting and issuing network function policies, implementing security and network function processing sequences, accessing orchestration, and reporting on the operational status of network function modules.

Registration module: receive and aggregate registration information from network function modules.

Monitoring status: monitor the operational status of network function modules.

Policy issuance: convert network function policies into specific network function module policies recognizable by selected network function modules, and issue policies.

Resource negotiation: send resource negotiation requests to network function modules or their management systems, including but not limited to resource application and release.

Information provision: analyze registration information, logs, alarms, and running status of network function modules to provide all managed network function module information to both business orchestration modules and management presentation layers. Network function module information can be retrieved by functional description, unique identifier, and name.

Execution of processing sequence: issue the corresponding network forwarding policy to the network function modules, when the execution of the security and network function processing sequence requires network forwarding cooperation.

Status reporting: collect information on network function running status, policy execution results, logs, and alarms, and report them to the management presentation layer.

5.2.3 Capability Layer

5.2.3.1 Security Function Modules

The security function module registers with the security function management module, executes security function module policies, provides feedback on policy execution results, logs, and alarms, and reports operational status information. The security function modules are divided into traffic-based security function modules(to process user traffic) and non-traffic-based security function modules(to process non-traffic objects such as assets) based on their processing objects.

Registration: register descriptive information about its function, unique identifier, name, address, calling interface, resource negotiation interface, deployment type, etc. to the security function management module.

Execution of policies: receive and execute security function module policies.

Feedback on results, logs, and alarms: provide feedback on the execution results, logs, and alarms of security function module policies in a unified format.

Status reporting: report operational status to the security function management module through a unified interface.

5.2.3.2 Network Function Modules

The network function module implements the network function module policy, provides feedback on execution results, logs, and alarms, registers modules, and regularly reports operational status.

Registration: register descriptive information about its function, unique identifier, name, address, calling interface, resource negotiation interface, deployment type, etc. to the network function management module.

Execution policy: receive and execute network function module policies.

Feedback on results, logs, and alarms: provide feedback on the execution results, logs, and alarms of the network function module policy in a unified format.

Status reporting: report operational status to the network function management module through a unified interface.

6 Procedures for SASE Orchestration Framework

6.1 Process for functional modules registration and operational status monitoring

The registration and operational status monitoring process for network and security function modules is shown in Figure 6-1.

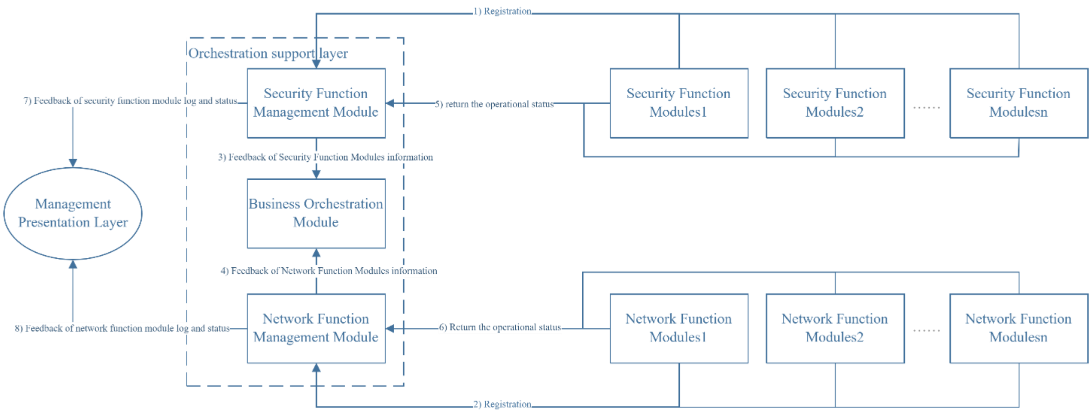

1) Registration
Orchestration support layer
7) Feedback of security function module log and status
Security Function Management Module
5) return the operational status
Security Function Modules1
Security Function Modules2
……
Security Function Modulesn
3) Feedback of Security Function Modules information
Management Presentation Layer
Business Orchestration Module
4) Feedback of Network Function Modules information
8) Feedback of network function module log and status
Network Function Management Module
6) Return the operational status
Network Function Modules1
Network Function Modules2
……
Network Function Modulesn
2) Registration

Figure 6-1 Registration and Operational Status Monitoring Process for Network and Security Function Modules

The registration and operational status monitoring process for network and security function modules is as follows:

1)The security function modules submit registration information and register with the security function management module.

2)The network function modules submit registration information and register with the network function management module.

3)The security function management module processes and stores the registration information from the security function module and provides security function module information to the business orchestration module.

4)The network function management module processes and stores the registration information of the network function module and provides network function module information to the business orchestration module.

5)The security function module returns the operational status ,logs and alarms.

6)The network function module returns the operational status ,logs and alarms.

The security function management module monitors the operational status of the security function module, aggregates logs and alarms, updates and provides the security function module information to the management presentation layer.

8)The network function management module monitors the operational status of the network function module, aggregates logs and alarms, updates and provides the security function module information to the management presentation layer.

6.2 Process for distributing network and Security Policies

The process of distributing network and security policies is shown in Figure 6-2.

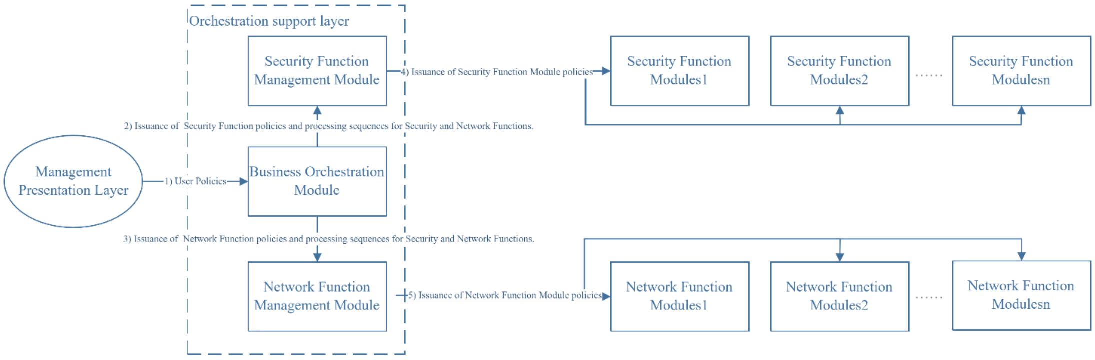

Orchestration support layer
Security Function Management Module
4) Issuance of Security Function Module policies
Security Function Modules1
Security Function Modules2
......
Security Function Modulesn
2) Issuance of Security Function policies and processing sequences for Security and Network Functions.
Management Presentation Layer
1) User Policies
Business Orchestration Module
3) Issuance of Network Function policies and processing sequences for Security and Network Functions.
Network Function Management Module
5) Issuance of Network Function Module policies
Network Function Modules1
Network Function Modules2
......
Network Function Modulesn

Figure 6-2 Network and Security Policies Distributing Process

The process of distributing network and security policies is as follows:

1)The business orchestration module receives user policies from the management presentation layer. The business orchestration module filters the appropriate security function modules and network function modules by analysing the user policies and function module information such as functional descriptions, functional characteristics, functional sequence, running states and network information such as network topology, network latency and network traffic load balancing. The business orchestration module sends resource negotiation requests to the security function modules and network function modules to be selected. Business orchestration selects security function modules and network function modules based on resource negotiation results to construct network and security processing sequences.

2)The business orchestration module distributes security and network function processing sequences and security function policies.

The business orchestration module distributes security and network function processing sequences and network function policies.

4)The security function management module receives the security and network function processing sequences and security function policies, issues policies to the corresponding security function modules, implements user traffic secure processing.

5)The network function management module receives security and network function processing sequences and network function policies, issues policies to the corresponding network function modules, implements user traffic forwarding scheduling and network optimization processing, assists in implementing the security and network function processing sequence through traffic forwarding.

6.3 Process for Policies Execution

6.3.1 Traffic-based security function module policies execution process

The execution process of the traffic-based security function module policies is shown in Figure 6-3.

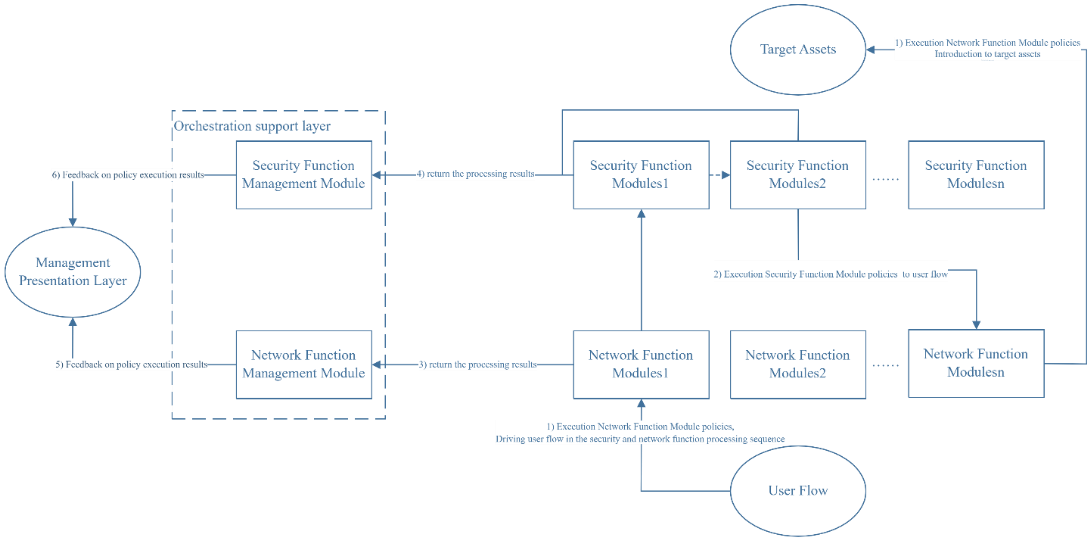

Target Assets
1) Execution Network Function Module policies
Introduction to target assets
Orchestration support layer
6) Feedback on policy execution results
Security Function
Management Module
4) return the processing results
Security Function
Modules1
Security Function
Modules2
......
Security Function
Modulesn
Management
Presentation Layer
2) Execution Security Function Module policies to user flow
5) Feedback on policy execution results
Network Function
Management Module
3) return the processing results
Network Function
Modules1
Network Function
Modules2
......
Network Function
Modulesn
1) Execution Network Function Module policies,
Driving user flow in the security and network function processing sequence
User Flow

Figure 6-3 Traffic-based security function module policies execution process

The process of the traffic-based security function module policies execution:

1)The network function modules execute the network function module policies, direct user traffic to the security and network function processing sequence, and finally direct it to the target resource.

2)The security function modules execute the security function module policies, process the user traffic, and forward the user traffic to the next function module in the security and network function processing sequence.

3)The network function modules return the processing result to the network function management module.

4)The security function modules return the processing result to the security function management module.

5)The network function management module aggregates the processing results and feeds back to the management presentation layer.

The security function management module aggregates the processing results and feeds back to the management presentation layer.

6.3.2 Non-traffic-based security function module policies execution process

The execution process of the non-traffic-based security function module policies is shown in Figure 6-4.

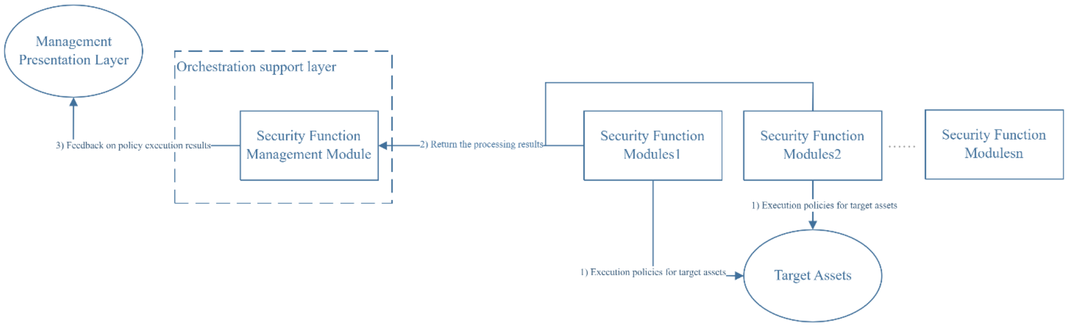

Management Presentation Layer
Orchestration support layer
Security Function Management Module
3) Feedback on policy execution results
2) Return the processing results
Security Function Modules1
Security Function Modules2
……
Security Function Modulesn
1) Execution policies for target assets
1) Execution policies for target assets
Target Assets

Figure 6-4 Non-traffic-based security function module policies execution process

When the non-traffic-based security function module is accessible from the target assets network, the process of the non-traffic-based security function module policies execution:

1)The security function modules execute the security function module policies towards the target asset.

2)The security function modules return the policy processing results to the security function management module.

3)The security function management module aggregates the policy processing results and feeds back to the management presentation layer.

When the non-traffic-based security function module is not accessible from the target assets network, a network path can be established between the non-traffic-based security function module and the target assets through the network function module. The policies execution process is shown in Figure 6-5.

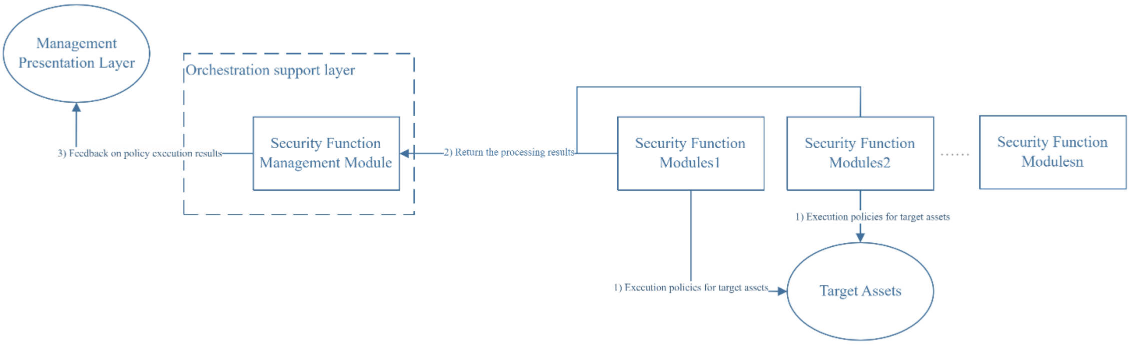

Management Presentation Layer
Orchestration support layer
Security Function Management Module
3) Feedback on policy execution results
2) Return the processing results
Security Function Modules1
Security Function Modules2
……
Security Function Modulesn
1) Execution policies for target assets
1) Execution policies for target assets
Target Assets

Figure 6-5 Non-traffic-based security function module policies execution flowchart

When the non-traffic-based security function module is not accessible from the target assets network, the process of the non-traffic-based security function module policies execution:

1)The network function modules execute the policies to establish a network path between the security function module and the target assets.

2)The security function modules execute the policies on the target asset via the network path established by the network function module.

3)The network function modules return the results back to the network function management module.

4)The security function modules return the results back to the security function management module.

5)The network function management module aggregates the policy processing results and feeds back to the management presentation layer.

6)The security function management module aggregates the policy processing results and feeds back to the management presentation layer.

6.3.3 Network function module policies execution process

The execution process of network function policies is the same as the process of the network function module described in Section 6.3.1 traffic-based security function module policies execution process.

7 Summary

In this white paper, we describe the challenges and requirements of the SASE orchestration framework, and propose a solution to achieve the integration of network and security orchestration in the building of SASE orchestration framework, which includes a reference framework diagram, an overview of the main functional modules, and a process description.