

SPECIFICATION

METHOD AND DEVICE FOR CLOUD HOST TOTAL TRAFFIC NETWORK ACCESS

PROTECTION

TECHNICAL FIELD

The present invention relates to the technical field of cloud computing and information security, in particular to a cloud-host-oriented full-traffic network access protection method and apparatus.

BACKGROUND

Firewall is a system composed of computer hardware and software and deployed at a network boundary. The firewall serves as a connection bridge between an internal network and an external network, and protects data entering and leaving the network boundary to prevent malicious intrusion, spread of malicious codes, etc., so as to ensure the security of internal network data. A firewall technology is an applied security technology based on network technologies and information security technologies. Almost all enterprises install firewalls on connection borders of internal networks and external networks (such as the Internet). The firewall can safely filter and isolate harmful network security information and behaviors such as external network attacks and intrusions, etc. However, in the face of cloud hosts, traditional network firewall technologies have no longer met the requirements of network security.

The cloud hosts are important parts of cloud computing in infrastructure applications, and locate at the bottom of a pyramid of a cloud computing industry chain, which are products derived from a cloud computing platform. This platform integrates three core elements of Internet applications: computing, storage, and network, and provides users with public Internet infrastructure services. The cloud hosts are a virtualization technology similar to a VPS host. The VPS uses virtual software of VZ or VM to virtualize multiple parts similar to independent hosts on one host, which can realize a single-machine multi-user application, where each part may be a separate operating system which can be managed with the same method as the hosts. However, the cloud hosts are to virtualize multiple parts similar to independent hosts on a group of cluster hosts. Each host in the cluster has a mirror image of the cloud hosts, which greatly improves the security and stability of the virtual hosts. With the application and development of cloud hosts, the problems of network security cannot be ignored, especially the network security problems among multiple cloud hosts.

At present, a firewall protection strategy can be configured on a host machine where the

cloud hosts reside, which can meet the requirements of micro-isolation of some cloud hosts, but cannot complete the requirements of subdividing strategy and overlaying strategy. The south-north protection of traditional cloud hosts is completed through a local firewall, which has higher technical requirements for cloud tenants in ordinary non-specialized technical fields. Moreover, the protection strategies for east-west and south-north traffic of the cloud hosts are prone to conflict. The east-west protection and the south-north protection will have conflicts on the actual network paths if the same configuration is made for the same type or network segment area during the configuration process. For example, if the cloud host protection is configured to permit an access request from a 10.18.*.* network segment to a port 80, but only an access of a 10.19.*.* network segment to the port 80 is permitted in the east-west traffic, the problem of inaccessibility for all would occur. The strategy query, creation, modification, and troubleshooting related to the east-west and south-north traffic protection among multiple cloud hosts are cumbersome to operate and lack coordination, which require higher professional technical requirements for cloud tenants.

SUMMARY

In order to solve the problems that the traditional firewall technology cannot meet the security protection of existing cloud hosts, the south-north protection using the local firewall of traditional cloud hosts has higher professional technical requirements, the protection methods of east-west and south-north traffic of cloud hosts are prone to conflicts in protection strategy configuration, the protection strategy configurations of relevant east-west and south-north traffic among multiple cloud hosts lack coordination and have cumbersome operation steps, etc. The present invention develops a cloud-host-oriented full-traffic network access protection method and apparatus.

The present invention seeks for the protection of the following technical schemes:

Using a cloud computing service orchestration technology, a cloud computing platform can seamlessly interact with a cloud host operating system host firewall and a distributed firewall of a cloud computing virtualization platform through "self-service interaction", complete the micro-isolation among cloud hosts, achieve automatic network protection strategy configuration, and support automatic division of regions, automatic configuration of default rules, self-defined addition of rules and their types, and other operations.

A firewall of the cloud host operating system is responsible for south-north traffic management. Under the traditional three-layer protection at the traditional data center level, through the strategy delivery and configuration application of a self-service cloud host firewall, with effectively control in the east-west traffic by cloud host resources a layer of south-north traffic protection superimposed is achieved meanwhile. The positioning of each firewall function is

clarified, and also the problem that protection strategies are prone to conflicts can be effectively solved.

The query, creation, and modification of relevant strategies are uniformly managed by a cloud platform. Cloud tenants can carry out independently query, filing application, automatically delivery and other operations of relevant strategies according to established processes, which greatly simplify the operation steps of cloud tenants and provide an intuitive query interface to facilitate the collaborative configuration of strategies among multiple devices. 。

Specifically:

The present invention provides a cloud-host-oriented full-traffic network access protection method, wherein said full-traffic network access protection refers to network security protection in full traffic and comprises: south-north traffic access protection of a cloud host firewall and a traditional data center firewall, and east-west traffic access protection of a distributed firewall of a cloud computing platform.

Said south-north traffic access protection refers to: a south-north traffic access protection which is implemented for respective configuration for the traditional data center firewall and the cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, said respective configuration refers to configuration, automatic scheduling, and delivery of south-north traffic access protection strategies for an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall.

Said east-west traffic access protection refers to: an east-west traffic access protection which is implemented by establishing an enhanced adaptation module that supports the distributed firewall on a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and achieving uniform configuration of the east-west traffic access protection strategy on a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform.

Through said uniform configuration on entrances of the east-west traffic access protection and south-north traffic access protection on the cloud computing platform and combining with cloud tenants, cloud host service grouping and a preset rule strategy in the cloud computing platform, said south-north traffic access protection and said east-west traffic access protection would achieve seamless interaction and above operations further implement automatic configuration on the full-traffic network access protection strategy, accordingly full-traffic network access protection for a single cloud resource and multiple cloud resources would achieve. Further,

the method comprises the following steps:

S1: establishing a response rule for the distributed firewall, i.e., establishing a response rule for the distributed firewall on the cloud hosts of the cloud computing platform according to the network protocol of the heterogeneous cloud basic environment at the cloud resource level, and automatically implementing said east-west traffic access protection through acquiring commands for configuration, automatic shielding and delivery of the acquired east-west traffic access protection strategy; wherein said distributed firewall supports heterogeneous networks deployed by an enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

S2: establishing a response rule for a full-traffic firewall, i.e., establishing said response rule for the south-north traffic access by performing configurations on the api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall using the cloud service orchestration and automation technology; and performing the uniform configuration on the entrances of the east-west protection and the south-north protection in combination with the cloud tenants, the cloud host service grouping and the preset rule strategy in the cloud computing platform, to achieve said east-west traffic access protection and said south-north traffic access protection of bidirectional traffic protection strategies by implementing fused optimization, automatic division and automatic configuration , and further establishing the response rule for the full-traffic firewall;

S3: configuring a full-traffic protection strategy in which the cloud tenants configure said relevant south-north traffic access protection strategy or said east-west traffic access protection strategy on a terminal display interface respectively according to demands, and automatically generating a full-traffic network access protection strategy demand order after the configuration is completed; and S4: acquiring full-traffic protection strategy requirements and making a response, the cloud hosts automatically read the full-traffic network access protection strategy based on the full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and automatically responds to the rules in steps S1 and S2 according to the read strategy and performs adaptive configuration, automatic scheduling and issuing commands through continuously acquiring the configured full-traffic protection strategy in step S3, to realize real-time automatic execution of the full-traffic network access protection.

Further, in the step S4 of acquiring the full-traffic protection strategy demands and making the response, said automatic execution comprises automatically starting the firewall if the firewall is stopped.

Further, in said step S4 of acquiring the full-traffic protection strategy demands and making the response, an automatic response is made finally through the cloud service orchestration and automation technology for the delivery and effectiveness of the full-traffic network access protection strategy according to the acquired application and review uniformly performed by the cloud tenants on the cloud platform, thereby achieving an automatic protection capability; and all of the above operations have logging and query traceback, providing positioning use for future troubleshooting in operation and maintenance.

The present invention further provides a cloud-host-oriented south-north traffic access protection method, wherein the south-north traffic access protection is implemented for a configuration for a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, said configuration referring to a configuration for inbound and outbound strategies of the cloud host firewall, thereby achieving the configuration, automatic scheduling and delivery of the south-north traffic access protection strategy; and said configuration objects of the inbound and outbound strategies of the cloud host firewall comprise: a port level, a protocol level, a source IP and a target IP level.

The present invention further provides another cloud-host-oriented south-north traffic access protection method, wherein the south-north traffic access protection is implemented for respective configuration for a traditional data center firewall and a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, wherein said respective configuration refers to configurations for an api interface opened to the traditional data center firewall and for inbound and outbound strategies of the cloud host firewall, thereby achieving configuration, automatic scheduling, and delivery of a south-north traffic access protection strategy; and said configuration objects of the inbound and outbound strategies of the cloud hosts firewall comprise: a port level, a protocol level, a source IP and a target IP level.

The present invention further provides a cloud-host-oriented east-west traffic access protection method, wherein the east-west traffic access protection refers to: establishing an enhanced adaptation module that supports the distributed firewall on a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and achieving uniform configuration of the east-west traffic access protection strategy of a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform, and the

east-west traffic access protection is further achieved.

Further, in the protection method, said protection strategies all support cloud tenants to perform self-defining.

Further, wherein that said protection strategies all support the cloud tenants to perform self-defining comprises: the cloud tenants configure the relevant access protection strategies on a terminal display interface according to their requirements, and after the configuration is completed, corresponding said access protection strategies requirements orders are generated automatically; and the cloud computing platform acquires the protection strategies requirements orders, and adaptively configures the protection strategies in order to implement the corresponding protection strategies.

The present invention further provides a cloud-host-oriented full-traffic network access protection apparatus, which comprises :

a response rule module for a distributed firewall, used to establish a response rule for the distributed firewall on the cloud hosts of a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and automatically implement an east-west traffic access protection through acquired commands for configuration, automatic scheduling and delivery of the east-west traffic access protection strategies, wherein said distributed firewall supports heterogeneous networks deployed by the enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

a response rule module for a full-traffic firewall, used to establish a response rule of the south-north traffic access by performing configurations on an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall using the cloud service orchestration and automation technology; and at the same time, through performing the uniform configuration on the entrances of the east-west protection and the south-north protection in combination with service grouping on cloud tenants, cloud host and preset of rules and strategies in the cloud computing platform, implement fused optimization, automatic division and automatic configuration of bidirectional traffic protection strategies for the east-west traffic access protection and the south-north traffic access protection, and further establish the response rule for the full-traffic firewall.

a full-traffic protection strategy configuration module, used for the cloud tenants to respectively configure the relevant south-north traffic access protection strategy or the east-west traffic access protection strategy on a terminal display interface according to demands, and automatically generate a full-traffic network access protection strategy demand order; and

a full-traffic protection strategy demand acquisition and response module, used to allow the cloud hosts to automatically read said full-traffic network access protection strategy based on said full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and realize an automatic response through said response rule module for the distributed firewall and said response rule module for the full-traffic firewall according to the read strategy, and by continuously acquiring the configured full-traffic protection strategy in the full-traffic protection strategy configuration module to perform commands for automatic scheduling and delivery, automatically implement the full-traffic network access protection in real time.

Further, the full-traffic protection strategy configuration module further comprises:

a display submodule used to display an interactive order process of the platform on a user terminal interface; and

a self-service configuration submodule used to support user-defined configurations, including a configuration made through said interactive order process of the platform, to achieve automatic delivery, autonomous query, history query and other configurations and operations.

The present invention further provides an electronic apparatus, wherein, the electronic apparatus comprises a memory and a processor, said memory is configured to store a configuration program system that can operate said apparatus on the processor, the configuration program being configured to implement said protection method on being executed by the processor.

The present invention further provides a computer-readable storage medium, wherein, said computer-readable storage medium is configured to store a configuration program of the apparatus, said configuration program being executed by one or more processors to implement said protection method.

Compared with the prior art, the present invention has the following advantages.

The interactive network protection strategy configuration is implemented by means of the uniform management performed by the cloud platform to support automatic division of regions, automatic configuration of default rules, self-defined addition of rules and their types, and other operations.

A user can perform more precise and targeted restrictions on the south-north traffic through operating the firewall of above system.

The distributed firewall provides network communication efficiency for the east-west traffic, makes management more efficient, and realizes rapid network security strategy configuration and delivery.

The cloud tenants can implement configuration automatic delivery, autonomous query,

history record query and other configurations operations by using an interactive order process of the platform. The operation experience for the cloud tenants is optimized, and the protection strategies can be configured without complex operations for the cloud tenants.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates steps of a cloud-host-oriented full-traffic network access protection method provided by the present invention.

FIG. 2 is a configuration program module diagram of a cloud-host-oriented full-traffic network access protection apparatus provided by the present invention.

FIG. 3 is a configuration program submodule diagram of a configuration full-traffic protection strategy in another cloud-host-oriented full-traffic network access protection apparatus provided by the present invention.

FIG. 4 is a detailed flowchart of another cloud-host-oriented full-traffic network access protection provided by the present invention.

FIG. 5 is a configuration program diagram of a first cloud-host-oriented south-north traffic network access protection apparatus provided by the present invention.

FIG. 6 is a configuration program diagram of a second cloud-host-oriented south-north traffic network access protection apparatus provided by the present invention.

FIG. 7 is a configuration program diagram of a cloud-host-oriented east-west traffic access protection apparatus provided by the present invention.

DETAILED DESCRIPTION

In order for those skilled in the art to understand the schemes of the present invention better, the technical schemes in the embodiments of the present invention will be described clearly and completely in conjunction with the accompanying drawings in the embodiments of the present invention. Apparently, the described embodiments are merely some embodiments, rather than all embodiments, of the present invention. Based on the embodiments of the present invention, all other embodiments derived by a person of ordinary skill in the art without creative efforts shall fall within the protection scope of the present invention.

It should be noted that the terms "first", "second" and the like in the description and claims, as well as the above-mentioned drawings, of the present invention are used to distinguish similar objects, but not necessarily used to describe a specific order or precedence order. It should be understood that data used in this way may be interchanged where appropriate so that the embodiments of the present invention described herein can be implemented in a sequence other

than those illustrated or described herein. Furthermore, the terms "including" and "having" and any variants thereof are intended to cover non-exclusive inclusions. For example, a process, method, system, product, or device that comprises a series of steps or units is not necessarily limited to those steps or units that are clearly listed, but may comprise other steps or units that are not clearly listed or are inherent to such processes, methods, products, or devices.

First, some nouns or terms appearing in the process of describing the embodiments of the present application are applicable to the following interpretations.

A cloud service orchestration technology means end-to-end automation of a process of deploying services in a cloud environment. More specifically, it refers to automated scheduling, coordination, and management of complex computer systems, middleware, and services-all of which facilitate accelerating the delivery of IT services while reducing the cost. It is configured to manage cloud infrastructure, which provides and allocates needed cloud resources to customers, such as creating virtual machines, allocating storage capacity, managing network resources, and granting access to cloud software. By using an appropriate orchestration mechanism, users can deploy and start using services on servers or on any cloud platform.

The south-north protection of traditional cloud hosts is completed through a local firewall, which has higher technical requirements for cloud tenants in ordinary non-specialized technical fields. Moreover, the protection strategies for east-west and south-north traffic of the cloud hosts are prone to conflict. The east-west protection and the south-north protection will have conflicts on the actual network path if the same configuration is made for the same type or network segment area during the configuration process. For example, if the cloud host protection is configured to permit an access request of a 10.18.*.* network segment to a port 80, but only an access of a 10.19.*.* network segment to the port 80 is permitted in east-west traffic, the problem of inaccessibility for all would occur. The present invention implements the protection of full-traffic network access through a cloud computing service orchestration technology and an automation technology, thereby effectively avoiding the above problems.

In order to make the advantages of the technical solutions of the present invention clearer, detailed description to the present invention in conjunction with drawings and embodiments is made as follows.

The present invention provides a cloud-host-oriented full-traffic network access protection method, wherein the full-traffic network access protection refers to network security protection in full traffic, comprising: south-north traffic access protection of a cloud host firewall and a

traditional data center firewall, and east-west traffic access protection of a distributed firewall of a cloud computing platform.

In the present embodiment, the cloud host firewall here refers to a cloud host operating system firewall in the prior art. A firewall of the cloud host operating system is responsible for south-north traffic management. Under the traditional three-layer protection at the traditional data center level, through the strategy delivery and configuration application of the self-service cloud host firewall, cloud host resources effectively controlled can be realized in the east-west traffic, and at the same time, a layer of north-south traffic protection is superimposed. The positioning of each firewall function is clarified, and also the problem that protection strategies are prone to conflicts can be effectively solved.

Said south-north traffic access protection refers to: a south-north traffic access protection which is implemented for respective configuration for the traditional data center firewall and the cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, said respective configuration refers to configuration, automatic scheduling, and delivery of south-north traffic access protection strategies for an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall, and supports cloud tenants to perform self-defining.

In the present embodiment, said respective configuration also refers to the configuration, automatic scheduling and delivery of inbound and outbound strategies for the traditional data center firewall, and supports cloud tenants to perform self-defining. The cloud tenants here are not limited to enterprises and individual users. The self-defining here refers to a configuration self-defined by the cloud tenants on a terminal display interface provided by the system according to his/her own needs.

Said east-west traffic access protection refers to: an east-west traffic access protection which is implemented by establishing an enhanced adaptation module that supports the distributed firewall on a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and performs uniform configuration of the east-west traffic access protection strategy on a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform.

In the present embodiment, said configuration of the east-west traffic access protection

strategies comprises: performing unified east-west traffic protection strategy configuration for cloud hosts in the multi-cloud heterogeneous environment on the cloud computing platform; and through deep integration with cloud tenants and cloud host service grouping in the cloud computing platform, implementing automatic strategy configuration and delivery effectiveness based on a whole life cycle of cloud resource provisioning and delivery, service group changes, and resource reclamation and extinction, etc.

Through uniform configuration on entrances of the east-west traffic access protection and south-north traffic access protection on the cloud computing platform and combining with cloud tenants, cloud host service groups and a preset rule strategy in the cloud computing platform, said south-north traffic access protection and said east-west traffic access protection would achieve seamless interaction and above operations further implement automatic configuration on the full-traffic network access protection strategy, accordingly full-traffic network access protection for a single cloud resource and multiple cloud resources would achieve.

In the present embodiment, the east-west traffic is mainly responsible for the external strategy configuration of a cloud host service system layer, and the south-north traffic is mainly responsible for the external strategy protection of a cloud host monomer.

FIG. 1 illustrates steps of a cloud-host-oriented full-traffic network access protection method provided by the present invention.

As shown in FIG. 1, the present embodiment shows a cloud-host-oriented full-traffic network access protection method. The method comprises the following steps:

S1: establishing a response rule for the distributed firewall, i.e., establishing a response rule for the distributed firewall on the cloud hosts of the cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and automatically implementing said east-west traffic access protection through commands for automatic scheduling and delivery of the acquired east-west traffic access protection strategy; wherein said distributed firewall supports heterogeneous networks deployed by the enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

S2: establishing a response rule for a full-traffic firewall, i.e., establishing said response rule for the south-north traffic access by performing configurations on an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall using a cloud service orchestration and automation

technology; and performing the uniform configuration on the entrances of the east-west protection and the south-north protection in combination with the cloud tenants, the cloud host service grouping and the preset rule strategy in the cloud computing platform, to achieve said east-west traffic access protection and said south-north traffic access protection of bidirectional traffic protection strategies by implementing fused optimization, automatic division and automatic configuration , and further establishing the response rule for the full-traffic firewall;

S3: configuring a full-traffic protection strategy in which the cloud tenants configure said relevant south-north traffic access protection strategy or said east-west traffic access protection strategy on a terminal display interface respectively according to demands, and automatically generating a full-traffic network access protection strategy demand order after the configuration is completed;

in the present embodiment, specifically, a preset protection strategy generation form corresponding to the cloud hosts is displayed on a cloud tenant terminal interface, so that the cloud tenant can fill in the relevant south-north traffic access protection strategy as needed; generating corresponding entries for preset protection strategies in a workspace corresponding to the cloud hosts, so that the cloud tenants can fill in the relevant east-west traffic access protection strategy as needed; and the full-traffic network access protection strategy demand order is automatically generated; and

S4: acquiring full-traffic protection strategy demands and making a response, the cloud hosts automatically read the full-traffic network access protection strategy based on the full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and automatically responds to the rules in steps S1 and S2 according to the read strategy and performs adaptive configuration, automatic scheduling and issuing commands through continuously acquiring the configured full-traffic protection strategy in step S3, to realize real-time automatic execution of the full-traffic network access protection.

In the present embodiment, in the step S4 of acquiring the full-traffic protection strategy demands and making the response, said automatic execution comprises automatically turning on the firewall if the firewall is not turned on.

In the present embodiment, in said step S4 of acquiring the full-traffic protection strategy demands and making the response, an automatic response is made finally through the cloud service orchestration and automation technology for the delivery and effectiveness of the full-traffic network access protection strategy according to the acquired application and review

uniformly performed by the cloud tenants on the cloud platform, thereby achieving an automatic protection capability; and all of the above operations have logging and query traceback, providing positioning use for future troubleshooting in operation and maintenance.

In the present embodiment, the full-traffic network access protection adopts rule access control, which is not only limited to protection for access, but actually also comprises an interaction with a threat intelligence library of the cloud computing platform in the strategy configuration, taking some malicious blacklist ip intercept as strategy protection.

FIG. 2 is a configuration program module diagram of a first cloud-host-oriented full-traffic network access protection apparatus provided by the present invention.

As shown in FIG. 2, a cloud-host-oriented full-traffic network access protection apparatus comprises:

a response rule module 101 for a distributed firewall, establishes a response rule for the distributed firewall on the cloud hosts of a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and automatically implements the east-west traffic access protection through acquired commands for configuration, automatic scheduling and delivery of the east-west traffic access protection strategy; wherein, said distributed firewall supports heterogeneous networks deployed by the enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

a response rule module 102 for a full-traffic firewall, used to establish a response rule for the south-north traffic access by performing configurations on an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall using a cloud service orchestration and automation technology; and at the same time, through performing the uniform configuration on entrances of the east-west protection and the south-north protection in combination with service grouping on cloud tenants, cloud host and preset of rules and strategies in the cloud computing platform, implement fused optimization, automatic division and automatic configuration of bidirectional traffic protection strategies for the east-west traffic access protection and the south-north traffic access protection , and further establish the response rule for the full-traffic firewall;

a full-traffic protection strategy configuration module 103, used for a cloud tenant to respectively configure the south-north traffic access protection strategy or the east-west traffic access protection strategy on a terminal display interface according to demands, and automatically

generate a full-traffic network access protection strategy demand order; and

a full-traffic protection strategy demand acquisition and response module 104, configured to allow the cloud hosts to automatically read said full-traffic network access protection strategy based on said full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and realize an automatic response through said response rule module for the distributed firewall and said response rule module for the full-traffic firewall according to the read strategy, and by continuously acquiring the configured full-traffic protection strategy in the full-traffic protection strategy configuration module to perform commands for automatic scheduling and delivery, automatically execute the full-traffic network access protection in real time.

FIG. 3 is a configuration program submodule diagram of a configured full-traffic protection strategy in another cloud-host-oriented full-traffic network access protection apparatus provided by the present invention.

Further, as shown in FIG. 3, the full-traffic protection strategy configuration module 103 in another cloud-host-oriented full-traffic network access protection apparatus provided by the present invention further comprises:

a display submodule 1031 , used to display an interactive order process of a platform on a user terminal interface; and

a self-service configuration submodule 1032, configured to support user-defined configurations, including a configuration made through said interactive order process of the platform, where the cloud tenant can implement operations such as automatic delivery, autonomous query, and history query and others through the interactive order process of the platform; the cloud tenants determine the south-north traffic access protection of the cloud hosts, then determine a target cloud host, and fills in relevant strategies according to a preset form; or/and the cloud tenants determine the east-west traffic access protection of the cloud hosts, then determine a target workspace, and fill in relevant strategies according to a preset form.

In the present embodiment, the cloud tenants determine the south-north traffic access protection of the cloud hosts, then determine the target cloud host, and fill in relevant strategies according to the preset form; or/and, the cloud tenants determine the east-west traffic access protection of the cloud hosts, then determine the target workspace, and fill in relevant strategies according to the preset form.

Specifically, a preset protection strategy generation form corresponding to the cloud hosts is

displayed on a cloud tenant terminal interface, so that the cloud tenants can fill in the relevant south-north traffic access protection strategy as needed; corresponding entries are generated for preset protection strategies in the workspace corresponding to the cloud hosts, so that the cloud tenants can fill in the relevant east-west traffic access protection strategy as needed; and a full-traffic network access protection strategy demand order is automatically generated.

Further, said self-service configuration sub-module 1032 also supports logging and query traceback for all operations, and provides positioning use for future troubleshooting in operation and maintenance. A query entrance is set in the interactive order process.

FIG. 4 is a detailed flowchart of another cloud-host-oriented full-traffic network access protection provided by the present invention.

As shown in FIG. 4, the full-traffic protection is implemented by the following process steps: through the full-traffic protection strategy configuration module 103, the cloud tenants can initiate an application on a client side, and independently select and determine full-traffic access protection order demands of the cloud hosts on a display interface. Specifically, in the case of determining the south-north traffic protection of the cloud hosts, the cloud tenants select a target cloud host and fill in the relevant strategies according to the preset form; and in the case of determining the east-west traffic protection of the cloud hosts, the cloud tenants select the target workspace and fill in the relevant strategy demands according to preset entries.

After the full-traffic access protection order demands of the cloud hosts are determined, a cloud tenant order demand is directly submitted to the cloud computing platform, and the cloud computing platform will automatically perform full-traffic demand adaption according to the order submitted by the user.

Further, in the full-traffic demand adaptation process, the system first confirms a traffic protection type in the full-traffic demands. If it is the south-north traffic protection, the cloud host firewall or/and the traditional data center firewall are continuously invoked, and the cloud computing platform acquires the protection strategy based on the demands of the cloud tenants, and adaptively configures the corresponding security protection strategy; if it is the east-west traffic protection, the configured distributed firewall is invoked, and the cloud computing platform acquires the protection strategy based on the demands of the cloud tenants, and adaptively configures the corresponding security protection strategy; then, the bidirectional traffic protection (east-west and south-north) strategies subjected to the adaptive configuration achieve automatic response by establishing a response rule module 101 for the distributed firewall and establishing a

response rule module 102 for the full-traffic firewall, and the full-traffic protection strategy demand acquisition and response module 104 delivers and executes the strategies, so as to realize the full-traffic network access protection of the cloud hosts.

In addition to the above method for implementing the full-traffic network access protection, the present invention also provides two other methods for implementing south-north traffic access protection by using a cloud computing automation technology or using a cloud computing service orchestration technology.

The first method is a cloud-host-oriented south-north traffic access protection method, wherein south-north traffic access protection is implemented for a configuration for a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system and using a cloud computing service orchestration technology for cloud resources of a group of service systems, the configuration referring to a configuration for inbound and outbound strategies of the cloud host firewall, thereby achieving the configuration, automatic scheduling and delivery of the south-north traffic access protection strategy; and configuration objects of the inbound and outbound strategies of the cloud host firewall comprise: a port level, a protocol level, a source IP and a target IP level.

FIG. 5 is a configuration program diagram of a first cloud-host-oriented south-north traffic access protection apparatus provided by the present invention. In FIG. 5:

a cloud host firewall configuration module 201: configured to configure inbound and outbound strategies of the cloud host firewall by using a cloud computer automation technology for cloud resources of a single service system and using a cloud computing service orchestration technology for cloud resources of a group of service systems;

a self-adaptive response module 202: configured to establish a self-adaptive response rule for the cloud host firewall on the cloud computing platform to implement automatic adaptation, automatic scheduling and delivery of the south-north traffic access protection strategy;

a protection strategy configuration module 203: configured for a cloud tenant to configure the relevant south-north traffic access protection strategy on a terminal display interface according to demands, and automatically generate a south-north protection strategy demand order after the configuration is completed; and

a protection strategy acquisition and response module 204 : configured for the cloud hosts to automatically read the access protection strategy based on the access protection strategy demand order submitted by the cloud tenant on the cloud computing platform, automatically respond to

the self-adaptive rules according to the read strategy, and automatically execute the south-north traffic access protection in real time by continuously acquiring the strategy in the protection strategy configuration module to perform commands for adaptive configuration, automatic scheduling and delivery.

The second method is a cloud-host-oriented south-north traffic access protection method, wherein south-north traffic access protection is implemented for respective configuration for a traditional data center firewall and a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system and by using a cloud computing service orchestration technology for cloud resources of a group of service systems, wherein the respective configuration refers to configurations for an api interface opened to the traditional data center firewall and for inbound and outbound strategies of the cloud host firewall, thereby implementing the configuration, automatic scheduling, and delivery of a south-north traffic access protection strategy; and the configuration objects of the inbound and outbound strategies of the cloud host firewall comprise: a port level, a protocol level, a source IP and a target IP level.

FIG. 6 is a configuration program module diagram of a second cloud-host-oriented south-north traffic network access protection apparatus provided by the present invention. In FIG. 6:

a cloud host firewall configuration module 301: configured to respectively configure the traditional data center firewall and the cloud host firewall by using a cloud computer automation technology for cloud resources of a single service system and using a cloud computing service orchestration technology for cloud resources of a group of service systems;

a self-adaptive response module 302: configured to establish a self-adaptive response rule for the cloud host firewall on the cloud computing platform to implement automatic adaptation, automatic scheduling and delivery of the south-north traffic access protection strategy;

a protection strategy configuration module 303: configured for a cloud tenant to configure relevant said south-north traffic access protection strategy on a terminal display interface according to demands, and automatically generate a south-north protection strategy demand order after the configuration is completed; and

a protection strategy acquisition and response module 304: configured for the cloud hosts to automatically read the access protection strategy based on said access protection strategy demand order submitted by the cloud tenant on the cloud computing platform, automatically respond to the self-adaptive rules according to the read strategy, and automatically execute said south-north

traffic access protection in real time by continuously acquiring the strategy in the protection strategy configuration module to perform commands for adaptive configuration, automatic scheduling and delivery.

In addition to the full-traffic network access protection method, the present invention also provides a cloud-host-oriented east-west traffic access protection method by using the cloud computer automation technology and the cloud computing service orchestration technology, wherein the east-west traffic access protection refers to: establishing an enhanced adaptation module that supports the distributed firewall on a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and achieving uniform configuration of the east-west traffic access protection strategy of a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform, and the east-west traffic access protection is further achieved.

FIG. 7 is a configuration program diagram of a cloud-host-oriented east-west traffic access protection apparatus provided by the present invention. In FIG. 7:

a response rule module 401 for a distributed firewall, configured to establish a response rule for the distributed firewall on the cloud hosts of the cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and automatically implement the east-west traffic access protection through commands for automatic scheduling and delivery of the acquired east-west traffic access protection strategy, wherein, said distributed firewall supports heterogeneous networks deployed by the enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

a self-adaptive response module 402: configured to establish a self-adaptive response rule for the cloud host firewall on the cloud computing platform to implement automatic adaptation, automatic scheduling and delivery of the east-west traffic access protection strategy;

a protection strategy configuration module 403: configured for a cloud tenant to configure the relevant east-west traffic access protection strategy on a terminal display interface according to demands, and automatically generate an east-west protection strategy demand order after the configuration is completed; and

a protection strategy acquisition and response module 404: configured for the cloud hosts to automatically read the access protection strategy based on the access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, automatically respond to

the self-adaptive rule according to the read strategy, and automatically execute the east-west traffic access protection in real time by continuously acquiring the strategy in the protection strategy configuration module to perform commands for adaptive configuration, automatic scheduling and delivery.

Further, in the two methods for implementing south-north traffic access protection and one method for implementing east-west traffic access protection, the protection strategies all support the cloud tenants to perform self-defining, including: the user performs self-defined configuration on the protection strategies, and then the cloud computing platform acquires the protection strategies and adaptively configure the protection strategies in order to implement the corresponding protection strategies.

Further, the automatic execution comprises automatically starting the firewall if the firewall is stopped.

Further, in the step of acquiring the strategy demands and making the response, an automatic response is made for the delivery and effectiveness of the access protection strategy according to the acquired application and review uniformly performed by the cloud tenants on the cloud platform, and finally through the cloud service orchestration and automation technology, thereby achieving an automatic protection capability; and all of the above operations have logging and query traceback, providing positioning use for future troubleshooting in operation and maintenance.

In the present embodiment, an electronic apparatus is further comprised. The electronic apparatus comprises a memory and a processor, wherein the memory is configured to store a configuration program system of the cloud-host-oriented full-traffic network access protection apparatus provided by the present embodiment that can be operated on the processor, the configuration program being configured to implement the cloud-host-oriented full-traffic network access protection method provided by the present embodiment. when being executed by the processor.

In the present embodiment, a computer-readable storage medium is further comprised. The computer-readable storage medium is configured to store a configuration program of the cloud-host-oriented full-traffic network access protection apparatus provided by the present embodiment, the configuration program being executed by one or more processors to implement the cloud-host-oriented full-traffic network access protection method provided by the present embodiment.

The above description is only preferred embodiments of the present invention, and it should be noted that those of ordinary skill in the art may also make several improvements and modifications without departing from the principles of the present invention, which should be considered as the protection scope of the present invention.

CLAIMS

What is claimed is:

1. A cloud-host-oriented full-traffic network access protection method, wherein said full-traffic network access protection refers to network security protection in full traffic and comprises: south-north traffic access protection of a cloud host firewall and a traditional data center firewall, and east-west traffic access protection of a distributed firewall of a cloud computing platform;

said south-north traffic access protection refers to: a south-north traffic access protection which is implemented for respective configuration for the traditional data center firewall and the cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, said respective configuration refers to configuration, automatic scheduling, and delivery of south-north traffic access protection strategies for an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall; and

the east-west traffic access protection refers to: an east-west traffic access protection which is implemented by establishing an enhanced adaptation module that supports the distributed firewall on the cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and performing uniform configuration of the east-west traffic access protection strategy on a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform; and

through uniform configuration on entrances of the east-west traffic access protection and south-north traffic access protection on the cloud computing platform and combining with cloud tenants, cloud host service grouping and a preset rule strategy in the cloud computing platform, said south-north traffic access protection and said east-west traffic access protection would achieve seamless interaction and above operations further implement automatic configuration on the full-traffic network access protection strategy, accordingly full-traffic network access protection for a single cloud resource and multiple cloud resources would achieve.

2. The full-traffic network access protection method of claim 1, further comprising the following steps:

CLAIMS

S1: establishing a response rule for the distributed firewall, i.e., establishing a response rule for the distributed firewall on the cloud hosts of the cloud computing platform according to the network protocol of the heterogeneous cloud basic environment at the cloud resource level, and automatically implementing said east-west traffic access protection through commands for configuration, automatic scheduling and delivery of the acquired east-west traffic access protection strategy; wherein said distributed firewall supports heterogeneous networks deployed by an enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

S2: establishing a response rule for a full-traffic firewall, i.e., establishing said response rule for the south-north traffic access by performing configurations on the api interface opened to the traditional data center firewall, as well as the port level, the protocol level, the source IP, the target IP level and other forms of the cloud host firewall using the cloud service orchestration and automation technology; and performing the uniform configuration on the entrances of the east-west protection and the south-north protection in combination with the cloud tenants, the cloud host service grouping and the preset rule strategy in the cloud computing platform, to achieve said east-west traffic access protection and said south-north traffic access protection of bidirectional traffic protection strategies by implementing fused optimization, automatic division and automatic configuration , and further establishing the response rule for the full-traffic firewall;

S3: configuring a full-traffic protection strategy in which the cloud tenants respectively configure said relevant south-north traffic access protection strategy or said east-west traffic access protection strategy on a terminal display interface according to demands, and automatically generating a full-traffic network access protection strategy demand order after the configuration is completed; and

S4: acquiring full-traffic protection strategy demands and making a response, the cloud hosts automatically read the full-traffic network access protection strategy based on the full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and automatically responds to the rules in steps S1 and S2 according to the read strategy and performs adaptive configuration, automatic scheduling and issuing commands through continuously acquiring the

CLAIMS

configured full-traffic protection strategy in step S3, to realize real-time automatic execution of the full-traffic network access protection.

3. The full-traffic network access protection method of claim 1 or 2, wherein in the step S4 of acquiring the full-traffic protection strategy demands and making the response, said automatic execution comprises automatically starting the firewall if the firewall is stopped.

4. The full-traffic network access protection method of claim 1 or 2 or 3, wherein in said step S4 of acquiring the full-traffic protection strategy demands and making the response, an automatic response is made finally through the cloud service orchestration and automation technology for the delivery and effectiveness of the full-traffic network access protection strategy according to the acquired application and review uniformly performed by the cloud tenants on the cloud platform, thereby achieving an automatic protection capability; and all of the above operations have logging and query traceback, providing positioning use for future troubleshooting in operation and maintenance.

5. A cloud-host-oriented south-north traffic access protection method, wherein the south-north traffic access protection is implemented for a configuration for a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, said configuration referring to a configuration for inbound and outbound strategies of the cloud host firewall, thereby achieving the configuration, automatic scheduling and delivery of the south-north traffic access protection strategy; and said configuration objects of the inbound and outbound strategies of the cloud host firewall comprise: a port level, a protocol level, a source IP and a target IP level.

6. Another cloud-host-oriented south-north traffic access protection method, wherein the south-north traffic access protection is implemented for respective configuration for a traditional data center firewall and a cloud host firewall by using a cloud computing automation technology for cloud resources of a single service system or by using a cloud computing service orchestration technology for cloud resources of a group of service systems, wherein said respective configuration refers to configurations for an api interface opened to the traditional data center firewall and for inbound and outbound strategies of the cloud host firewall, thereby achieving configuration, automatic

CLAIMS

scheduling, and delivery of a south-north traffic access protection strategy; and said configuration objects of the inbound and outbound strategies of the cloud host firewall comprise: a port level, a protocol level, a source IP and a target IP level.

7. A cloud-host-oriented east-west traffic access protection method, wherein said east-west traffic access protection refers to: establishing an enhanced adaptation module that supports the distributed firewall on a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and achieving uniform configuration of the east-west traffic access protection strategy of a cloud host in a multi-cloud heterogeneous environment on the cloud computing platform, and the east-west traffic access protection is further achieved .

8. The protection method of any one of claims 1 to 7, wherein said protection strategies all support cloud tenants to perform self-defining.

9. The protection method of claim 8, wherein that said protection strategies all support the cloud tenants to perform self-defining comprises: the cloud tenants configure the relevant access protection strategies on a terminal display interface according to their requirements, and after the configuration is completed, corresponding said access protection strategies requirements orders are generated automatically ; and the cloud computing platform acquires the protection strategies requirements orders, and adaptively configures the protection strategies in order to implement the corresponding protection strategies.

10. A cloud-host-oriented full-traffic network access protection apparatus, wherein comprises:

a response rule module for a distributed firewall, configured to establish a response rule for the distributed firewall on the cloud hosts of a cloud computing platform according to a network protocol of a heterogeneous cloud basic environment at a cloud resource level, and automatically implement an east-west traffic access protection through acquired commands for configuration, automatic scheduling and delivery of the east-west traffic access protection strategies; wherein, said distributed firewall supports heterogeneous networks deployed by the enhanced adaptation module in advance at the cloud resource level on the cloud computing platform, according to the network protocol of the heterogeneous cloud basic environment;

a response rule module for a full-traffic firewall, configured to establish a response

CLAIMS

rule of the south-north traffic access by performing configurations on an api interface opened to the traditional data center firewall, as well as a port level, a protocol level, a source IP, a target IP level and other forms of the cloud host firewall using a cloud service orchestration and automation technology; and at the same time, through performing the uniform configuration on the entrances of the east-west protection and the south-north protection in combination with service grouping on cloud tenants, cloud host and preset of rules and strategies in the cloud computing platform, implement fused optimization, automatic division and automatic configuration of bidirectional traffic protection strategies for the east-west traffic access protection and the south-north traffic access protection, and further establish the response rule for the full-traffic firewall;

a full-traffic protection strategy configuration module, configured for the cloud tenants to respectively configure the relevant south-north traffic access protection strategy or the east-west traffic access protection strategy on a terminal display interface according to demands, and automatically generate a full-traffic network access protection strategy demand order; and

a full-traffic protection strategy demand acquisition and response module, configured to allow the cloud hosts to automatically read said full-traffic network access protection strategy based on said full-traffic network access protection strategy demand order submitted by the cloud tenants on the cloud computing platform, and realize an automatic response through said response rule module for the distributed firewall and said response rule module for the full-traffic firewall according to the read strategy, and by continuously acquiring the configured full-traffic protection strategy in the full-traffic protection strategy configuration module to perform commands for automatic scheduling and delivery, automatically execute the full-traffic network access protection in real time.

11. The full-traffic network access protection apparatus of claim 10, wherein the full-traffic protection strategy configuration module further comprises:

a display submodule, configured to display an interactive order process of the platform on a user terminal interface; and

a self-service configuration submodule, configured to support user-defined configurations, including a configuration made through said interactive order process of the platform, to achieve automatic delivery, autonomous query, history query and other configurations and operations.

CLAIMS

12. An electronic apparatus, wherein, the electronic apparatus comprises a memory and a processor, said memory is configured to store a configuration program system that can operate said apparatus of claims 10 to 11 on the processor, the configuration program being configured to implement said protection method of one of claims 1 to 9 on being executed by said processor.

13. A computer-readable storage medium, wherein said computer-readable storage medium is configured to store a configuration program of the apparatus of one of claims 10 to 11, said configuration program being executed by one or more processors to implement said protection method of one of claims 1 to 9.