Chapter 8
Dynamic Firewall Policy Management Framework for Private Cloud

Mahesh Nath Maddumala and Vijay Kumar

Abstract In traditional networking environment, perimeter firewalls restrict the access to resources inside organizations' private network. In cloud computing, every virtual instance has to be accessed by the external parties. Due to its unique computing environment, cloud computing requires tailor-made firewall systems. To provide the desired high-availability and low-latency system, cloud services are replicated and made available in multiple geolocations or availability zones. This often leads to violation of various compliance policies and policy conflicts. The other complex issue is to manage security policies across the distributed data centers. We address these issues and present a dynamic firewall policy management scheme that uses a centralized controller to manage all firewalls in distributed data centers of a private cloud.

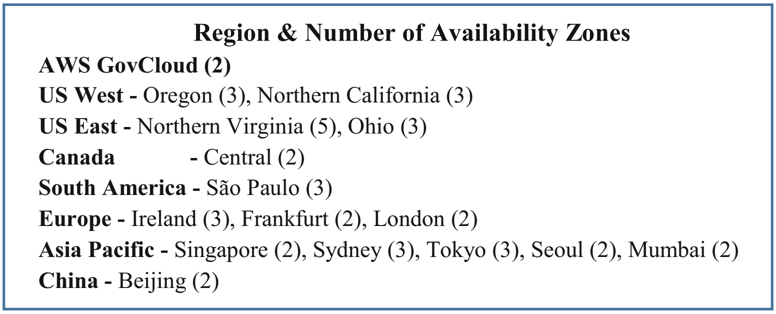
Keywords Distributed firewall policies · Cloud policies · Compliance policies

8.1 Introduction to Cloud Data Centers and Their Security Issues

In traditional networking environment, perimeter firewalls restrict the access to the resources inside the private network. In cloud computing, every virtual instance has to be accessed by the external parties. Due to its unique computing environment, cloud computing requires tailor-made firewall systems. NIST [1] defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." It is no doubt that the cloud computing has transformed the computing discipline into more profitable

M. N. Maddumala (✉) · V. Kumar
University of Missouri–Kansas City, Kansas City, MO, USA
e-mail: mahesh.maddumala@mail.umkc.edu

N. S. V. Rao et al. (eds.), *Proceedings of International Symposium on Sensor Networks, Systems and Security*, https://doi.org/10.1007/978-3-319-75683-7_8



Region & Number of Availability Zones

AWS GovCloud (2)
US West - Oregon (3), Northern California (3)
US East - Northern Virginia (5), Ohio (3)
Canada - Central (2)
South America - São Paulo (3)
Europe - Ireland (3), Frankfurt (2), London (2)
Asia Pacific - Singapore (2), Sydney (3), Tokyo (3), Seoul (2), Mumbai (2)
China - Beijing (2)

Fig. 8.1 Amazon Web Services Global Infrastructure

and efficient platform, but not without the challenges. One of the major challenges is security and privacy. According to the cloud security 2016 spotlight report by CloudPassage [2], *verifying security policies*, *visibility into infrastructure security*, and *compliance* were named as the top three cloud security challenges that cause the biggest headaches for IT security professionals.

One of the main features of the cloud computing is its high availability and performance. In order to provide low-latency and fault-tolerant services across the globe, customers prefer to replicate the data and applications and make them available at various zones across the globe. The AWS cloud [3] operates data centers in 42 availability zones within 16 geographic regions around the world as shown in Fig. 8.1. Microsoft Azure [4] is available in 34 regions around the world. Although the expansion of the cloud infrastructure to multiple regions significantly improves its availability and performance, it presents unwanted location-based compliance issues, and one such issue is internet censorship. Many countries block certain websites and services due to political and religious reasons, which poses a great challenge to the data centers to offer the services in more stringent countries. For example, Iran [5] has blocked almost 50% of the top 500 visited websites worldwide including YouTube, Facebook, Twitter, and Google Plus. China [6] governmental authorities not only block websites but also monitor the internet access of individuals. Unfortunately such restrictions present compliance challenges.

NIST [1] defines four deployment models of cloud computing—public cloud, private cloud, community cloud, and hybrid cloud. In private cloud, customers are completely responsible for securing their data, applications, platform, and infrastructure. As the cloud data centers are distributed across the globe, managing security policies and ensuring compliance and consistency across the data centers is highly challenging. There are two types of location-based compliance challenges—one is the enforcement of data residency regulations (certain sensitive information must not leave the country) and the other is the enforcement of internet censorship (certain censored information must not enter the country). The first case has been addressed by various governmental compliance policies such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security

Standard (PCI DSS), etc. The second case is enforced by the individual countries such as China, Iran, Saudi Arabia, etc. using firewalls and other filtering mechanisms. In this chapter, we deal with second case of location-based compliance issues.

In our framework, we address various security issues such as compliance policies, policy anomaly detection, and distribution of policies. We present our policy automation model with a centralized global policy manager which verifies security policies for consistency, compliance, and conflict resolution across all the firewalls.

8.2 Dynamic Firewall Policy Management for Private Cloud

The main objective of our framework is to automate the policy management of distributed firewalls of a private cloud using a centralized controller with a defined set of procedures and policy structure. The policy management includes dynamically updating the policies, ensuring the compliance and consistency of policies, resolving the policy conflicts, and providing the strong security with cooperative firewalls.

In our scheme, we choose the centralized approach over the distributed approach to manage the firewall policies across the data centers. In a distributed topology, firewalls are connected to each other forming a fully connected network so that any firewall can inform its policy changes to all other firewalls in the network. This has two disadvantages: (a) a compromised firewall could compromise all other firewalls leading to a serious security violations and (b) the overhead of information exchange among these firewalls. In a centralized topology, all the firewalls are connected to a central node (a controller). In this setup, unlike distributed topology, only the controller can propagate the policy changes to all firewalls in the network.

Every data center deploys two types of firewalls: one is a perimeter firewall which secures the entire network of the data center and another one is an internal firewall which secures individual virtual machines as shown in Fig. 8.2. The security policies

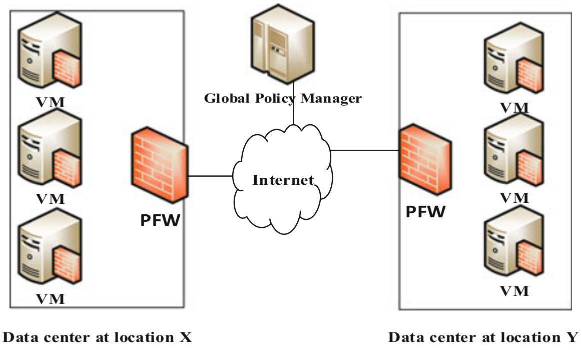


Fig. 8.2 Firewall setup in distributed data centers

configured at the perimeter firewall are common security policies which apply to all virtual machines within the data center whereas virtual machine firewall policies are specific to the individual virtual machines. For example, a virtual machine running webserver may configure webserver-based security policies in its firewall, whereas a virtual machine running email servers may configure only email-related security policies in its firewall.

8.2.1 Policies

We classify the firewall policies of a private cloud into three categories: (a) location-based compliance policies, (b) perimeter policies, and (c) group policies.

8.2.1.1 Location-Based Compliance Policies

During the process of the replicating data and applications to another data center, security policies of virtual machine firewall and data center perimeter firewall also have to be replicated. If the replicated data center is in an internet-restricted country, then that data center has to adhere to the country-specific internet policies. These policies would be configured at the perimeter firewall.

8.2.1.2 Perimeter Policies

These are the general policies configured at the perimeter firewalls to prevent common attacks and unwanted traffic, for example, blocking the access to unused ports, denying unsupported protocols, and rejecting the traffic from prohibited IP addresses.

8.2.1.3 Group Policies

The service-based security policies can be grouped as group policies. For example, VM hosting web services should have web-based security policies in its firewall, and these policies can be applied to all the VMs that are running web services. Also multiple services such as web, email, and databases can be hosted on the same virtual machine. In this case, VM hosting multiple services should have respective service based group in its firewall. These policies are configured at virtual machine firewall.

8.2.2 Dynamic Policies

The predefined security policies can only help to prevent the known attacks. To prevent the emerging advanced attacks, firewalls should be capable of creating dynamic policies by analyzing the network packets, by creating dynamic IP blacklists, etc. Similar work has been addressed in [7, 8].

8.2.2.1 Dynamic IP Address Blacklist

IP blacklist is a list of blocked IP addresses that are suspected of sending malicious packets. Security administrators maintain a static IP blacklist to block the traffic from certain IP addresses, and the list would be updated by importing latest blacklists from various security sources, often vendors. However there is a problem with the static blacklists. Firewalls could not prevent the attacks coming from the IP addresses which are not listed in the blacklists. We developed an algorithm to generate IP blacklists dynamically by identifying the frequency of the attacks originated by an IP address.

Figure 8.3 illustrates the entire process of generating dynamic IP blacklist. Initially when packet arrives, source IP address will be read and verified in the

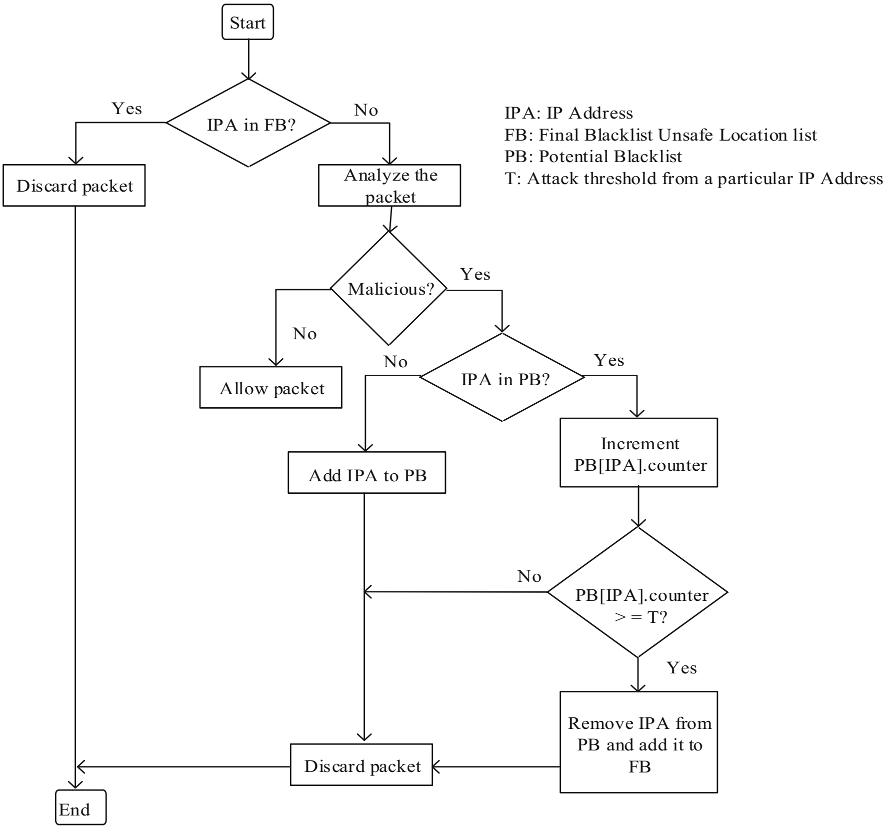


Fig. 8.3 Flowchart of dynamic creation of IP blacklist

final blacklist. If there is a match, then the packet will be discarded; otherwise, the packet will be analyzed by the firewall for any malicious content apart from the firewall policies. If any malicious content is found, then source IP address of the packet is added to the potential blacklist. A separate counter is maintained for each entry of source IP address in potential blacklist and will be incremented whenever a new attack is detected from the same IP address. When the counter value reaches the threshold limit T, IPA will be removed from potential blacklist and moved to final blacklist. Thereafter packets from the IP addresses of final blacklist are completely blocked.

8.3 Anomalies in Policy Configuration

The main and critical task of a security administrator is to configure the firewall policies. Due to the complex nature of policy specifications, it often leads to misconfiguration of policies which results in inconsistent and inaccurate policies. There are mainly two types of anomalies that can occur in policy configuration—redundant and conflict anomalies.

Redundant Anomaly When two policies represent the same set of packets with the same action, then they are said to be in redundant anomaly.

Conflict Anomaly When two policies represent the same set of packets with different actions, then they are said to be in conflict anomaly.

In our framework, we deal with three categories of firewall policies as discussed in Sect. 8.2.1: location-based compliance policies, perimeter policies, and group policies. In this section, we address the anomalies associated with these policies. As the policies in different categories may overlap with each other, they could result in redundant and conflict anomalies. We identified three possible cases that anomalies can occur in the multi-category policies—inter-category anomalies, intra-category anomalies, and intergroup anomalies.

Intra-category Anomalies In this case, the anomalies occur within the same category. For example, policies of perimeter policy category may overlap with each other. This may happen due to the security administrator's inadequate knowledge of policy configuration. The algorithm for the detection of intra-category anomalies is given in Algorithm 1.

```
ALGORITHM 1. Intra-Category_Policy_Anomaly_Detection
Input: Policy list P.
Output: TRUE or FALSE, and List of conflict and redundant policies.
RedundantPolicies = []; ConflictPolicies = []; status = FALSE
for i in 1 to n-1 do
for j in i+1 to n do
    if pi.service = pj.service and pi.value R pj.value
    then
```

```
            if pi.action = pj.action then
            RedundantPolicies.append(pi,pj);
            else
            ConflictPolicies.append(pi,pj);
            end
            status = TRUE
        end
end
end
return status
```

Intergroup Anomalies In this case, the anomalies occur between the policies of two or more groups. For example, if a virtual machine firewall requires policies of two or more groups, then GPM has to check for the anomalies that could occur between the policies of two or more groups. The detection of intergroup anomalies is given in Algorithm 2.

```
ALGORITHM 2. Inter-group_Policy_Anomaly_Detection
Input: Policy list G1, G2,..Gn.
Output: TRUE or FALSE, and List of anomaly groups.
anomaly_policies = [ ], status = FALSE
for i in 1 to n-1 do
for j in i+1 to n do
    if Intra-Category_Policy_Anomaly_Detection(Gi+Gj) == TRUE
    then
            anomaly_groups.append(Gi,Gj)
            status = TRUE
    end
end
end
return status
```

Inter-category Anomalies In this case, the anomalies occur between the policies of two or more categories. For example, policies of compliance policy category may overlap with policies of perimeter policies and vice versa. These anomalies are resolved by using precedence of the categories. For example, if there are conflicts between local and group policies, then the conflicts are resolved by retaining group policy and removing local policies.

8.4 Global Policy Manager

The core part of our framework is the centralized controller called Global Policy Manager (GPM). It would be located at the headquarters of a multinational organization.

8.4.1 Dual Mode

GPM operates in two modes simultaneously—manual and automatic. In manual mode, security administrator can update the firewall policies of any firewall or group of firewalls in the global policy base. In automatic mode, GPM receives statistics or/and policy updates from the individual firewalls and updates the global policy base accordingly. In the above two cases, GPM applies the policy changes to the relevant firewalls if necessary.

8.4.2 Global Policy Manager Architecture

The global policy manager consists of four modules: *policy injection interface*, *FW interface*, *policy manager*, and *global policy base* as shown in Fig. 8.4.

8.4.2.1 Policy Injection Interface

In manual mode, security administrators inject the compliance and group policies into the global policy base. This injection occurs during initial configuration of the framework and also whenever there are changes in compliance and group policies. This interface should be made available only to the security administrator who is accountable for security policies of all the branches of an organization.

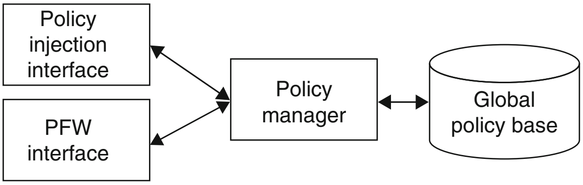


Fig. 8.4 Global policy manager architecture

8.4.2.2 FW Interface

The firewall interface communicates with the perimeter firewall and firewalls of all virtual machines of a data center. This interface is used to collect the statistics and policy changes from the perimeter firewalls.

8.4.2.3 Policy Manager

This is the key module which manages all other modules of the GPM. The activities of the policy manager include (a) analyzing the policies received from the policy injection interface and FW interface; (b) storing the policies in global policy base; (c) fetching the policies from the global policy base; (d) ensuring compliance, consistency, and correctness of the policies; and (e) communicating the policy updates to the applicable perimeter firewalls.

8.4.2.4 Global Policy Base

The policies of all the virtual machine firewalls and perimeter firewall of a data center are stored in global policy base along with the compliance and group policies.

8.4.3 Policy Configuration Procedures

Policy configuration is required to be performed in two scenarios: policies configured during initial setup of firewall and when there is any policy update due to change in existing policies.

8.4.3.1 Initial Policy Configuration

When a perimeter firewall is set up for the first time, policies should be configured as per the security requirements. The procedure of initial policy configuration is illustrated in seven steps (Fig. 8.5). Every PFW has to share location details to the GPM to apply relevant location-based compliance polices.

Virtual machine firewall has to specify the group IDs in order to acquire the group policies. GPM combines the group policies, resolves the conflicts if exists, and sends the final list of policies to the requested virtual machine firewall.

8.4.3.2 Policy Update

This framework supports dynamic policy updates. In other words, policies can be dynamically created, modified, or removed. This will be done in three ways: (a) local update, (b) GPM-initiated update, and (c) peer-initiated update.

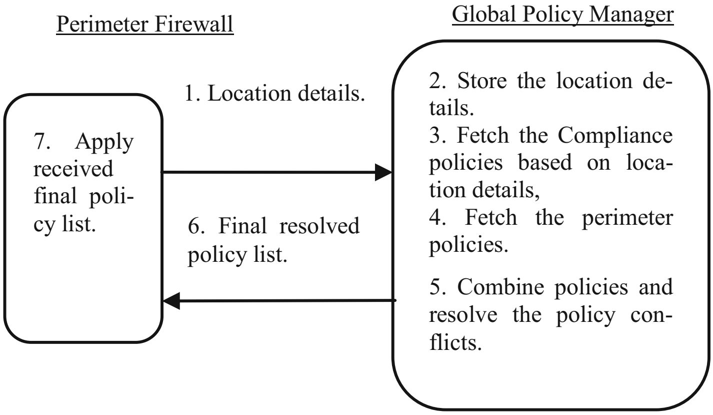

Perimeter Firewall
Global Policy Manager
1. Location details.
7. Apply received final policy list.
6. Final resolved policy list.
2. Store the location details.
3. Fetch the Compliance policies based on location details,
4. Fetch the perimeter policies.
5. Combine policies and resolve the policy conflicts.

Fig. 8.5 Initial policy configuration

Local Update Whenever a firewall detects malicious content in the packets, it can block that kind of packets with introducing or modifying a policy. This policy is updated locally and will be informed to the GPM.

GPM-Initiated Update This policy update happens when a policy-change decision is made at the organization level and initiated by GPM itself.

Peer-Initiated Update GPM may propagate updated policies to a set of firewalls. These policies are derived from the statistics or other polices received from firewalls.

8.5 Conclusion and Future Work

We have presented dynamic firewall policy management framework which automates the policy management of distributed data center firewalls using a central controller called global policy manager. We have also introduced the location-based compliance policies and dynamic creation of IP blacklists to prevent the attacks from highly unsafe locations. We would like to extend our framework to include the other deployment models of the cloud computing (public and hybrid cloud).

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing. National Institute of Standards and Technology special publication 800-145, 1–3 (2011)
2. CloudPassage: Cloud Security 2016 Spotlight report. https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf (2017). Accessed 28 Feb 2017

3. Amazon web services: AWS Global Infrastructure. https://aws.amazon.com/about-aws/global-infrastructure/ (2017). Accessed 28 Feb 2017
4. Microsoft Azure: Azure regions. https://azure.microsoft.com/en-us/regions/ (2017). Accessed 28 Feb 2017
5. Wikipedia: Internet Censorship in Iran. https://en.wikipedia.org/wiki/Internet_censorship_in_Iran (2017). Accessed 28 Feb 2017
6. Wikipedia: Internet Censorship in China. https://en.wikipedia.org/wiki/Internet_censorship_in_China (2017). Accessed 28 Feb 2017
7. Maddumala, M.N., Kumar, V.: A logic-based security framework for mobile perimeter. In: 16th IEEE international conference on mobile data management (MDM), pp. 30–33 (2015)
8. Jaiswal, C., Maddumala, M.N., Kumar, V.: Location-based security framework for cloud perimeters. IEEE Cloud Comput. **1**(3), 56–64 (2014)