Chapter 6
Network Security Policy Automation:
Enterprise Use Cases and Methodologies

Myo Zarny
vArmour Networks, USA

Meng Xu
vArmour Networks, USA

Yi Sun
vArmour Networks, USA

ABSTRACT

Network security policy automation enables enterprise security teams to keep pace with increasingly dynamic changes in on-premises and public/hybrid cloud environments. This chapter discusses the most common use cases for policy automation in the enterprise, and new automation methodologies to address them by taking the reader step-by-step through sample use cases. It also looks into how emerging automation solutions are using big data, artificial intelligence, and machine learning technologies to further accelerate network security policy automation and improve application and network security in the process.

BACKGROUND

Policy automation is a broad term—both policy and automation could mean many things to many people. This chapter discusses specifically about network security policy automation, looking into what network security policies mean; how they are derived and enforced in practice in larger enterprise environments; what the most common use cases driving network security policy automation are; and finally, what the emerging automation approaches are. The authors will take the reader through a few sample use cases to illustrate the most common methods.

DOI: 10.4018/978-1-6684-3694-3.ch006

The use cases are based on real-world scenarios from larger enterprises that have already begun the journey to automation. Their requirements include not only the functionality but also other key aspects such as scale, performance, resilience, and redundancy. The solutions described here should be familiar to many in the standards community, and some of them are already productized to various degrees by commercial vendors. Because many solutions and their adoption in the market are still relatively new, the goal is to give readers a better understanding of these solutions.

What Are Policies?

The term policy could have different meanings depending on the context. It could refer to broad high level Information Technology (IT) policies that support business objectives; detailed technical and procedural requirements for specific areas of IT; or anything in between. In colloquial usage, the term policy is often used interchangeably with similar terms like standards and guidelines although in more formal (academic) usage, the terms are not always interchangeable (Kim, 2016, p. 41; SANS, 2018).

The following is a simplified description of what policies could mean in different settings:

- General IT policies are a set of (codified) high level requirements, procedures and guidelines for all IT that enable the business. Such policies may cover topics like service availability, disaster recovery, business continuity planning, regulatory compliance, information security, or end-user training. Managers and senior technical architects tend to be the intended audience.
- IT security policies define what it means to be secure for IT technologies including applications, databases, systems, and networks. According to Wikipedia (Wikipedia, 2018), IT security policies codify practices that aim to prevent "unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information", "regardless of the form the data may take (e.g., electronic, physical)."
- IT security policies can be further broken down into sub-areas like network security, systems security, application security, legal liability, etc. Each sub-area can be divided further still—e.g., how strong the customer passwords ought to be; when and where customer data needs to be encrypted at what minimum strength; who from what networks can access to which systems in what networks and perform what functions; how frequently compliance audits ought to take place; etc. The main consumers of "low-level" policies are IT engineers, who will need to implement the policies.
- In theory, most specific policies support their higher level policies, which in turn ultimately support the business objectives.

Depending on the organization, the breadth and depth of IT policies differ greatly. Large firms, especially those that need to demonstrate regulatory compliance, typically maintain teams whose main responsibilities include developing/updating IT security policies and performing regular audit reviews. On the other hand, smaller firms may not have the technical and financial wherewithal to maintain such a staff; not all (or none) of the policies may be formally codified or documented as practices that should/must be adhered to.

To be sure, codified authoritative policies need to exist for policies to be automated. It is a best practice to formally document all approved IT policies, and disseminate updated policies throughout the IT organization on a regular basis. In practice, however, even large organizations with dedicated Info Sec