ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 9(19), DOI: 10.17485/ijst/2016/v9i19/90133, May 2016 ISSN (Online) : 0974-5645

Design a Resilient Network Infrastructure Security Policy Framework

Akashdeep Bhardwaj, G. V. B. Subrahmanyam, Vinay Avasthi and Hanumat Sastry

University of Petroleum and Energy Studies (UPES), Dehradun - 248007, Uttarakhand, India; Bhrdwh@yahoo.com, Gvbsvv@gmail.com, Vavasthi@ddn.Upes.ac.in, Hsastry@ddn.upes.ac.in

Abstract

The information security policy development life cycle tend to lack focus on use of standard terms and semantics. This results in blurred outlines for monitoring, evaluation and enforcement of the security policy for the employees causing confusion in adhering and implementing it which leads to lack of process of publishing form the security policy, end user awareness, translation of high level policy to lowest level component configuration plans and actions to take in time of crisis. This leads to the critical need for the designing an empirically tested, comprehensive security policy design. This paper proposes bridging the gap between the high level information security policy descriptions with the low level network infrastructure security implementation. **Background Objectives:** With new and innovative technologies such as Cloud, Remote computing, Enterprise Mobility, e-commerce on the rise, network security has remained an ever increasing challenge. This paper presents a security framework to bridge the gap between high level specification requirements and the low level implementation phase for network infrastructure security using the network architecture model with the security policies associated with the network components required to be enforced. **Methods/Statistical Analysis:** To achieve the framework design, architectural model and a set of design-level security policies are taken into consideration. Also discussed are the advantages and desired characteristics of the model, relating to existing process worked in the design area; and future research directions are pointed. **Findings:** The current information security policy development life cycle tends to have few disadvantages with the most critical being the overall lack of view of the policy. Typically a narrow view can be found when focusing only on development of the security policy documents and not including the actual practices for implementation or even maintenance of the security policies. This process does not address how the security policy would be development and enforced or even evaluated. The life cycle designs usually focus on policy for development instead of focusing on development process of the information security policy. **Application:** Utilizing Hybrid cloud architecture design so that internet facing tiers tend to be public clouds and internal secure applications and database tend to be private clouds. This change in network architecture helps take on the volumetric network and application layer DDoS attacks to ensure the traffic reaching the internal network tiers is free from such attackers. Using Rate controls, built-in intelligent WAFs, Client Reputation monitoring, be used in combination as part of a comprehensive defense against all types and sizes of cyber threats.

Keywords: Information Security Policy, Network Architecture, Network Firewall, Network Infrastructure, Network Security Policy, WAF

1. Introduction

With the ever growing increase in the use of computer systems, applications on cloud with internet for data exchange and communication, the need for secure computing and a well-designed network security architecture is essential for all types of organizations ranging from corporates, academic or government entities or geographically spread end users, different roles and profiles as well as use of different computing devices, communication channels[1]. This varied range introduces many new challenges to the standard traditional approaches for designing network infrastructure architectures. This manuscript focuses on new and advanced network infrastructure security systems defined as setup network devices, software and integration technologies that help collaborate and

*Author for correspondence

implement the organization's network security. In order to understand the security landscape and grasp the areas affecting network security architecture, the Figure 1 provides a general representation on the various attack types and their mitigation approaches followed.

As the security risk levels increase, the security needs of an organizations become complex. Network Security system architecture with legacy traditional approaches like single tier design and firewalls are required to undergo several design changes before acceptance[2]. Some of the changes essential to move from the traditional levels (like firewalls, IPsec, VPN) to enhanced levels include turning data centers into auto scaling clouds, virtualization based software defined networks, open stack network architecture, multi-tenant-aware provisioning networks.

Usually the design of network security systems follows three standard phases with the security policy (high level) being documented with some controls (like ISO, PCI) and guideline manual, followed by formulation of security requirement specifications and finally implementation phase (low level) that integrates and combines the security design. The problem with this approach is the gap between the high level security specification requirements and the low level implementation phase, where in the IT Security team receives the high level description and goes directly to implement the security design, however complex and multiple network components and mechanisms involved. These network devices and components are at times having completely different configuration setup [3]and features with little or no integration mechanisms.

This causes errors and improper enforcement of the actual security design leaving security holes and vulnerabilities with a false sense of security. The purpose of the Information Security Policy is to provide a framework for the information security management across the enterprise. This applies to everyone with access to the enterprise information systems (including employees, contractors, third party consultants and visitors) and to devices and systems attached to the enterprise computer and telecom network. The policy addresses processing of information by the enterprise for its operational business purpose regardless of being on paper or in electronic form. The policy also covers services provided by external parties as consultants to the enterprise as described in Figure 2.

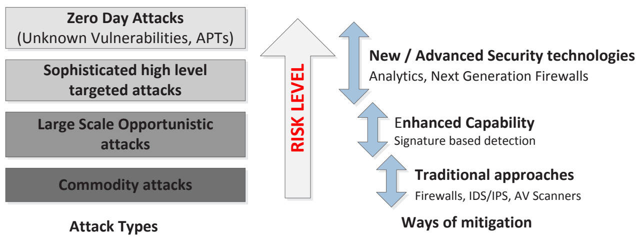
Zero Day Attacks
(Unknown Vulnerabilities, APTs)
Sophisticated high level targeted attacks
Large Scale Opportunistic attacks
Commodity attacks
Attack Types
RISK LEVEL
New / Advanced Security technologies
Analytics, Next Generation Firewalls
Enhanced Capability
Signature based detection
Traditional approaches
Firewalls, IDS/IPS, AV Scanners
Ways of mitigation

Figure 1. Attack types and Mitigation Approaches.

The Network Security Policy is a critical part of the Information Security policy that includes sub policies for various network infrastructure components but not limited to Routers, Switches, Firewalls, Load Balancers, RAS, Modems and Wireless Access Points.

2. Information Security Policy

The information security policy design needs to include information security governance, asset and data protection, and information security assurance to the senior corporate executives at the same time ensuring business objective of the organization are served. Information Security Design steps are show in the Figure 3 starting with the high level policy description, high level security analysis to the proposed network security design and network implementation steps.

As an example, Table 1 presents a revision history of the information security policy creation flow.

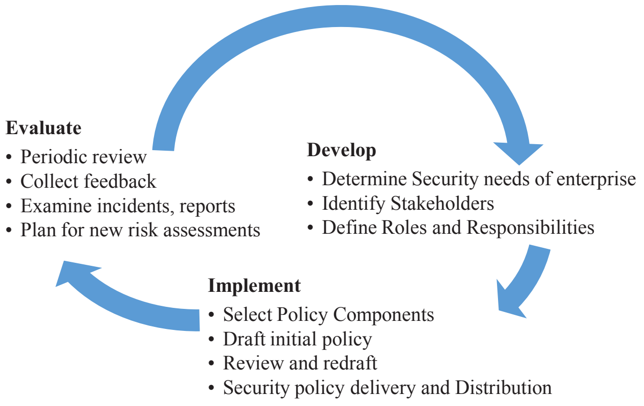
Evaluate
• Periodic review
• Collect feedback
• Examine incidents, reports
• Plan for new risk assessments
Develop
• Determine Security needs of enterprise
• Identify Stakeholders
• Define Roles and Responsibilities
Implement
• Select Policy Components
• Draft initial policy
• Review and redraft
• Security policy delivery and Distribution

Figure 2. Standard Information Security Model.

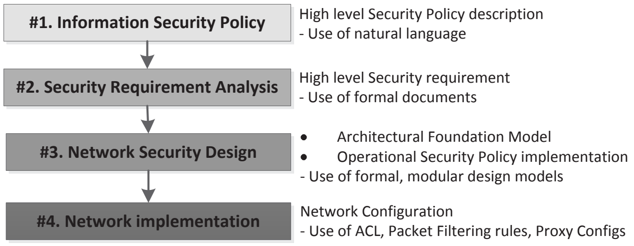
#1. Information Security Policy
High level Security Policy description
- Use of natural language
#2. Security Requirement Analysis
High level Security requirement
- Use of formal documents
#3. Network Security Design
• Architectural Foundation Model
• Operational Security Policy implementation
- Use of formal, modular design models
#4. Network implementation
Network Configuration
- Use of ACL, Packet Filtering rules, Proxy Configs

Figure 3. Information Security Design.

Table 1. Information Security Policy Revision History

Revised on	Version	Description	Approved by
01-Oct-2015	0.1	Initial Document Creation	IT Manager
10-Jan-2016	1.0	Publish Document	IT Manager
15-Jan-2016	1.1	Review document, modify policy section reflecting organizational legal-contractual service level agreements for the protection of information, including ISO, PCI DSS	IT Head
20-Jan-2016	1.2	Formal Editorial work	PMO
27-Jan-2016	1.3	Formal review and minor edits	PMO
15-Feb-2016	1.3a	Include missing protection of information assets policy clause as per Network Security Policy Design stage	PMO
22-Feb-2016	1.3b	Update mandatory requirements of the Information Security Policy with respect to Policy requirement and Network Design	PMO
10-Mar-2016	1.4	Formal review and change to use new policy template	PMO
17-Mar-2016	1.5	Formal review to reflect jobs descriptions of IT Security roles defined by HR for the organization	HR Head
25-Mar-2016	2.0	Formal approval for Senior Management	Senior executives

2.1 Security Policy Design Stage #1

The policy design starts with Information Security Policy definition stage, this typically consists of with the higher management direction and support and the organization's information security policy document to be implemented. The network security architecture [4]is only a part of the corporate information security plan and taken on board with other security components like physical, operational, data, access control, employee, communication and social among others. An example of few high level information security objectives would be –

- Ensure information is accessible only to those intended
- Provide a secure computing environment to the staff at the organization sites
- Ensure only authorized employees have access to the information and assets when required
- Ensure that information is secured against breaches of confidentiality, interruptions, integrity
- Address security of cloud hosted services and applications to ensure that risks are identified and required controls are implemented and documented

2.2 Security Policy Design Stage #2

The next stage is the Information Security Requirement analysis for risk mitigation which is actually a formal representation of the management defined high level security policy. Within the requirement analysis the focus is solely on technical security policy with regards to network infrastructure. This includes the having in place guidelines for Confidentiality in transmission, SSL for applications, [5]User authentication and authorization, determining the right to view and modify data, determining where the data can be hosted securely, Integration with LDAP or its equivalent, Limit access to production systems and devices, perform Vulnerability Scanning and Penetration testing, analyze logs for user access, implement an audit trail, ensure up to date security patches and updates, [6]send logs to a central SIEM log system, ensure antivirus/malware software, ensure data communication is encrypted, restrict transmission of sensitive information by email or other insecure vectors, deploy proven, standard encryption with strong encrypted keys to make sure the connections are secure among others. The risk mitigation takes into account the entity level controls answering queries like the ones described below.

- Describing how the vulnerable protocols are being used – type of environment, type of data (payment card, account) or even the types of devices supporting the protocols.
- Evaluate and document the risk to environment until the vulnerable protocols are removed
- Implementing process to monitor new and zero day vulnerabilities and apply controls which include upgrading all web browsers.

- Use of SSL/TLS with strong cryptographic encryption, using two factor authentication and initiate strong-encrypted sessions like IPsec Tunnels before performing any data transmission over SSL inside that tunnel.

3. Proposed Network Security Policy Framework

This paper proposes adding a Network Security Design stage to bridge the high level and low level gaps for the security design architecture. This involves the high level architecture model along with security policies that are associated with those network component devices involved in the security enforcement. This stage represents each technology being used, the integration between those technologies and the link between the each of high level security policy aims with the corresponding security components that would enforce and actually implement the policy which involves security policy management, change and release management, assessing vulnerabilities and application connectivity management as described in the Figure 4 below.

The Network Security Policy design involves a two-stage process as described below.

3.1 Architectural Foundation model

Network security designs some 10 to 15 years ago, had what can best be described as component with a hard cover outside while being soft inside – similar to chocolate gems candy. This means there was typically a secure edge perimeter in form of a firewall but had little or no security control systems on the internal network. For an architecture design to be secure and effective, it is essential to have the use of strategically placed security controls and techniques that are capable to block cyber-attacks and intrusion at each stage of the process. This encompasses all the network security components along with their data flow process required for secure communication. This model provides the way critical components are established in the network, the impact and faults generated for each and every component. The network security components include enforcement of Authentication and Integrity, Confidentiality, [7]Access Control and Audits is performed by network security components consisting of Network Management elements in form of Proxy agents (for SNMP, DHCP or DNS), Packet Filtering firewalls to create a set of rules to either accept or reject network traffic performing IP routing or be the destination for the traffic, Cryptography and SIEM log management for analysis. These components are typically off-the-shelf and the model is associated with network quality attributes such as device integration, maintainability, reliability, performance, modifiability. The network security architecture is dependent on different types of off-the-shelf components; hence the architectural model becomes a highly critical aspect of the network security policy design process.

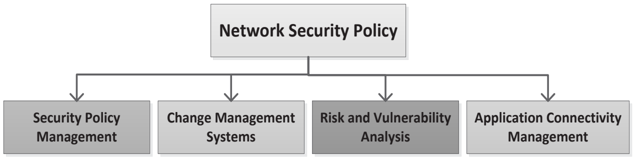
Network Security Policy
Security Policy Management
Change Management Systems
Risk and Vulnerability Analysis
Application Connectivity Management

Figure 4. Network Security Policy components.

The security architecture should be implemented to work on the premise that in case the first level attack is successful and able to breach the initial defenses, the internal network components should be able to block any subsequent stages of that attack. This is a clear requirement for an intrusion which is a zero day or near zero day attack[8]. Another feature of the model is being formal. This allows the model to be analyzed logically in an auto computational process, instead of being manually reviewed which is prone to human errors. Another feature is being hierarchical and allowing the configuration to be synthesized directly from the model and be scalable. This provides the ability to have yet-to-be developed low-level components in the form of black box sub components in high-level design model. These low-level systems can be commissioned independently in a top-down design development approach[9]. A bottom-up approach can also be taken up, which begins with process at low-level to high-level functionalities using pre-commissioned low-level black boxes. For example a network firewall can be modeled by utilizing proxy agent black boxes and packet-filtering black boxes. Then a firewall black-box could be used as the high-level component of the security design integrating with other high level components and elements like trust management, certificate management or even IOS version control. The module design[10] breaks the high level main design objective into smaller repeatable blocks. For example when design a huge network setup having several smaller sites, having the same design and similar deployment process for each site which includes common set of security controls like ACL or firewall rules. Then any change across all the sites can be applied smoothly without any major rollout changes. Thus the Architectural Foundation model consists of the following two areas as

- Network Components security configurations for
  - Security devices such as Network Firewalls, Web Application Firewall, VPN Gateways, Packet Filters and Caching devices
  - Perimeter devices Routers, Load Balancers
  - Network devices like Switches
- Data Flow which represents communication and traffic flow between the different components in the model and captured using tools like Netflow analyzer or Wireshark

3.2 Operational Security Design

This defines a set of low abstraction level security policies which are close to the actual technical implementations yet have device and vendor independence with traffic analysis as show in the Figure 5 below. The network security policy design plans using IETG RFC3060 Policy Core Information Model (PICM). This model proposes use of extensible class hierarchal policy[11] component objects representing different high-level network policies including network QoS parameters and Security configurations in order to manage, implement and control network infrastructure access as per the illustration above. The policy rule associates set of action or actions to be performed with conditions to be implemented and if the rule is defined to be active or passive for a specific duration or scheduled as per conditions.

This further helps in enforcing security mechanisms like IPsec, Dual Sign-on, Logging network related activities or keynote credentials. This converts the network component policy entities into the configurational architectural level model[12] for device level network infrastructure security system. The Network Security Design provides a standard, uniform and concise representation of the overall network security systems to be implemented, taking the high-level policies to actual implementations for each component using PCIM's abstraction which hides the lowest level of complex configuration codes from the higher view. This helps improving the design efficiency and understanding of the security system. If automated, the model can be developed in form of a system with input being the final design level policies, architectural model[13] required along with device dependent specific information and the output turns out to be the low level configurations to be implemented for each network device component. Use of Netflow and packet capture provide a fool proof and excellent process of determining the traffic flows in the network that help identify network devices and paths that would get impacted during a cyber-attack. This also provides network speed, storage, optimum location of network monitoring points and actual computing power requirement with a logical flow visibility for the network infrastructure.

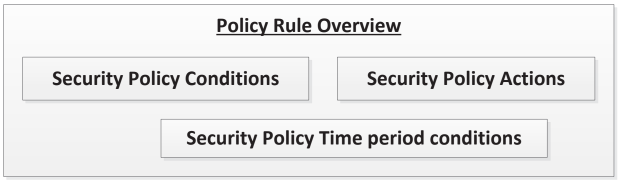
Policy Rule Overview
Security Policy Conditions
Security Policy Actions
Security Policy Time period conditions

Figure 5. Security Policy Rule Overview.

4. Related Work

As an example the authors tested the proposed model on an ongoing network infrastructure setup being designed for a commercial data center. The data center is proposed to host secure web applications for customer globally and provide them the application access in form of cloud based SaaS. The authors pointed out the use of SSL and use of Secure Shell in the design, which by current attack vectors is an ineffective and insecure protocol. The regular SSL traffic from internet went through the edge router to a network firewall which blindly allowed as show in Figure 6.

Network Policy is further comprised of network component level policies as

- VPN Policy – provides guidelines for working from home or outside office network via VPN Client using IPSec or L2TP connections.
- Wireless Policy – covers all forms of wireless data communication systems like laptops, blackberries, smart phones and PDAs capable of transmitting data packets without physical transmission media.
- Risk assessment Policy – takes into account the network device risk assessments conducted within the enterprise, their frequency and teams to perform (internal It or external consultants)

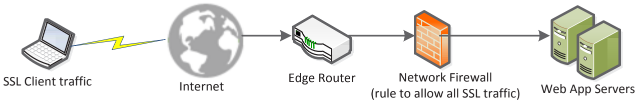

Figure 6. Traffic flow with simple SSL.

- Audit Policy – provides authority of enterprise information security team conducting an information security audit to investigate any possible security incidents ensure conformance to the enterprise security policy, monitoring end use activity.
- Encryption Policy – provides guideline on use of proven encryption algorithms like 3DES, RSA, Blowfish, RC5 to ensure effective security for the enterprise, ensues legal regulations are followed.
- Password Policy – establishes a secure standard defining password creation (alphanumeric, length, special characters), way of protecting passwords and the frequency of changing them.

Defining standards to be followed for wireless is part of the scope for the policy which includes using Advanced Encryption System (AES), Extensible Authentication protocols (EAP), Temporal Key Integrity protocol (TKIP), Protected Extensible Authentication protocol (PEAP). Similarly for Network devices use of TACACS+ for user authentication, disabling services and features (like IP directed broadcasts, TCP/UDP Small devices, drop incoming packets with invalid or spoofed IP Addresses (like RFC1918), Cisco Discovery Protocol, Telnet/FTP/HTTP services, Dynamic Trunking, enabling QoS, NTP, Netflow and SNMP with secure standard strings and disabling auto configuration.

By applying the proposed Network Security Policy design framework, the authors have taken into account the information security policy to be implemented and the low level configuration to be setup. It is recommended by PCI DSS 3.1 that SSL be replaced by TLS (currently version 2.0) which leads the infrastructure security design consideration to have the capability to decrypt SSL/TLS. The network security design phase also came up with secure shell (SSH) with no other VPN/IPsec into the data center network as depicted below in the Figure 7.

For secure inbound traffic, SSL/TLS decryption is taken as a high level policy design, then having low level configuration like forward proxies as an option to decrypt the SSL/TLS client traffic coming to the data center network. The design model recommended use of Big IP with LTM performing the decryption at perimeter Next Generation Firewall Proxy with corresponding cert assigned to each client. So for the high level plan by executive management of ensuring secure customer access to the organization applications as per the enterprise Information security Policy, this transform into SSL/TLS Client Server authentication in the Information Security requirement stage. Then as per the proposed framework in this paper, the low level configuration setup procedure work needs to be implemented that transform into the ability of the devices (BigIP LTM here) to maintain secure sessions between the application server and clients. For this the IT Security engineering team decided to control SSL Network Traffic coming towards the application server by configuring Server SSL Profile.

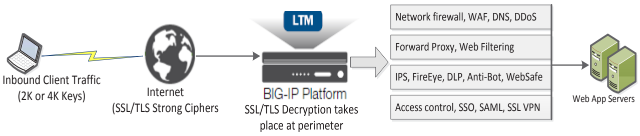

Figure 7. Traffic flow with SSL/TLS

- Configure BigIP for various client browsers from internet ranging from Internet Explorer, Mozilla, Firefox and Opera
- Creating SSL profile
  - ○ Key/Certificate pair installation on the BigIP LTM
  - ○ Terminate client-server sesure sessions on the BigIP
  - ○ Associate the SSL profile with a virtual server address (VIP)
- Creating SSL ciphers like SSL v2/v3, TSL v1 for per-session authentication
- Use of compatible BigIP LTM version of 11.20.0 or later, since the existing 9.0.0-9.4.8 and 10.0.0-10.2.2 are not compatible for TLS 1.1 or 1.2.
- Unique BiGIP LTM configuration strings as follows

SSL profile to use only TLS 1.1-compatible and TLS 1.2-compatible ciphers DEFAULT:!MYSSLv3:!MYTLSv1 tmsh create /myltm profile my client-ssl mycipher DEFAULT:!MYSSLv3:!MYTLSv1
SSL profile to support TLS 1.0 and SSL 3.0 clients DEFAULT:-SSLv3:-TLSv1:RC4-SHA tmsh create /myltm profile myclient-sslmycipher DEFAULT:-MYSSLv3:-MYTLSv1:RC4-SHA
SSL profile to support TLS 1.0, but not SSL 3.0 clients DEFAULT:!SSLv3:-TLSv1:RC4-SHA tmsh create /myltm profile myclient-sslmyciphers DEFAULT:!MYSSLv3:-MYTLSv1:RC4-SHA

For inbound decryption of traffic to specific network devices, requires use of digital certificates on the SSL/TLS interception device which allows deep level visibility to the secure SSL/TLS traffic. This lead the design team to decide on use of an embedded hardware based crypto card. This further provided enhancement in the decryption performance for the network. Other forms of cyber-attacks like ARP spoofing, CAM table overflows, DHCP response spoofing can also be understood using the network security policy model and the optimized deployment be implemented.

5. Conclusion

The design framework proposed in this research paper introduces conceptual models in form of an Architectural Design model and low design level security policies integrated with the security development configurations over various levels of abstraction with the high level policies. This gives the network security design a clear and concise understanding. By having a clear understanding of which network devices are involved in what conditions, volumes, the proposed design can immensely benefit the design architecture.

6. References

1. Saikeerthana R, Umamakeswari A. Secure data storage and data retrieval in cloud storage using cipher policy attribute based encryption. Indian Journal of Science and Technology. 2015 May; 8(S9). Doi: 10.17485/ijst/2015/v8iS9/65600.
2. Manjusha R, Ramachandran R. Secure authentication and access system for cloud computing auditing services using associated digital certificate. Indian Journal of Science and Technology. 2015 Apr; 8(S7). Doi: 10.17485/ijst/2015/v8iS7/71223.
3. Thiyagarajan M, Raveendra C, Thiagarasu V. Web Service Authentication and Multilevel Security. Indian Journal of Science and Technology. 2015 Jul; 8(15). Doi: 10.17485/ijst/2015/v8i15/73850.
4. Khan AS, Fisal N, Bakar ZA, Salawu N, Maqbool W, Ullah R, Safdar H. Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. Indian Journal of Science and Technology. 2014 Jan; 7(3). Doi: 10.17485/ijst/2014/v7i3/47646.
5. Lakshmipriya B, Leena Sri R, Balaji N. A novel approach for performance and security enhancement during live migration. Indian Journal of Science and Technology. 2016 Jan; 9(4). Doi: 10.17485/ijst/2016/v9i4/87031.
6. Kim K, Lee S, Yun Y, Choi J, Mun H. Security evaluation metric of windows-based information security products. Indian Journal of Science and Technology. 2015 Apr; 8(S8). Doi: 10.17485/ijst/2015/v8iS8/71501.
7. Chang AJT, Wu CY, Liu W. Information Security Governance Control through comprehensive Policy Architectures. Management of Innovation and Technology (ICMIT), IEEE International Conference. 2012; 9(49). p. 442–46.
8. Hwang J, Syamsuddin I. Information Security Policy Decision Making - an analytic hirarchy process approach. 3rd Asia International Conference on Modeling and Simulation. 2009; 5(22):158–63.
9. Hadjina N, Klaic A. Methods and Tools for development of information security policy - a comparative literature review. MIPRO Proceedings of 34 International Convention. 2011; 4(21):1532–37.
10. Golub M, Klaic A. Conceptual information modeling within the contemporary information security policies. Information and Communication Technology Electronics and Microelectronics (MIPRO). 2013; 2(10):1105–10.
11. Mahmood MA, Siponen M, Pahnila S. Compliance with Information Security Policies - an empirical investigation. IEEE. 2010; 43(2):64–71.
12. Mueller C, Kritzinger E, Vuuran I. Identifying gaps in IT retail Information Security Policy implementation processes. 2nd International Conference in Information Security and Cyber Forensics (InfoSec). 2015; 5(17):126–33.
13. Harnesk D, Laaksonen A, Niemimaa M. Inerpreting Information Security Policy Outcomes - a Frames of reference perspective. System Sciences (HICSS). 2013; 2(82):4541–50.
14. Wei N, Ma Y, Lu B. Research on Information Security Policy's Deployment for Smart Grid. Multimedia Information Networking and Security (MINES). 2012; 10(73):52–4.
15. Ming Z, He H, Shuzhen Y, Jingjun L. Information Security Policy in converged Network Environment. Information Theory and Information Security (ICTIS). 2010; 6(40):335–9.
16. Riekstin A, Januario G, Rodrigues B, Nascimento V, Carvalho B, Meirosu C. A Survey of Policy Refinement Methods as a Support for Sustainable Networks. IEEE Communications Surveys and Tutorials. 2016; 18(1):222–35.
17. Agbariah S. Policy exchange and management for Policy Compliance and Change Detection System in managed service in data networks. The 2014 International Symposium on Networks, Computers and Communications. 2014; 1–5.
18. Odagiri K, Shimizu S, Ishii N, Takizawa M. Establishment of Virtual Policy Based Network Management Scheme by Load Experiments in Virtual Environment. 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA). 2015. p. 769–76.

19. Arapoglou R, Rodis I, Magdalinos P, Alonistioti N. Adapting policy-based management of Future Networks using collaborative filtering techniques. 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). 2014; 224–8.
20. Agbariah S. Common policy language for Policy Compliance and Change Detection System in managed service in data networks. The 2014 International Symposium on Networks, Computers and Communications. 2014; 1–6.
21. Odagiri K, Shimizu S, Ishii N, Takizawa M. Suggestion of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations. 2015 18th International Conference on Network-Based Information Systems (NBiS). 2015. p. 180–6.
22. Basile C, Lioy A, Pitscheider C, Valenza F, Vallini M. A novel approach for integrating security policy enforcement with dynamic network virtualization. 2015 1st IEEE Conference on Network Softwarization (NetSoft). 2015; 1–5.