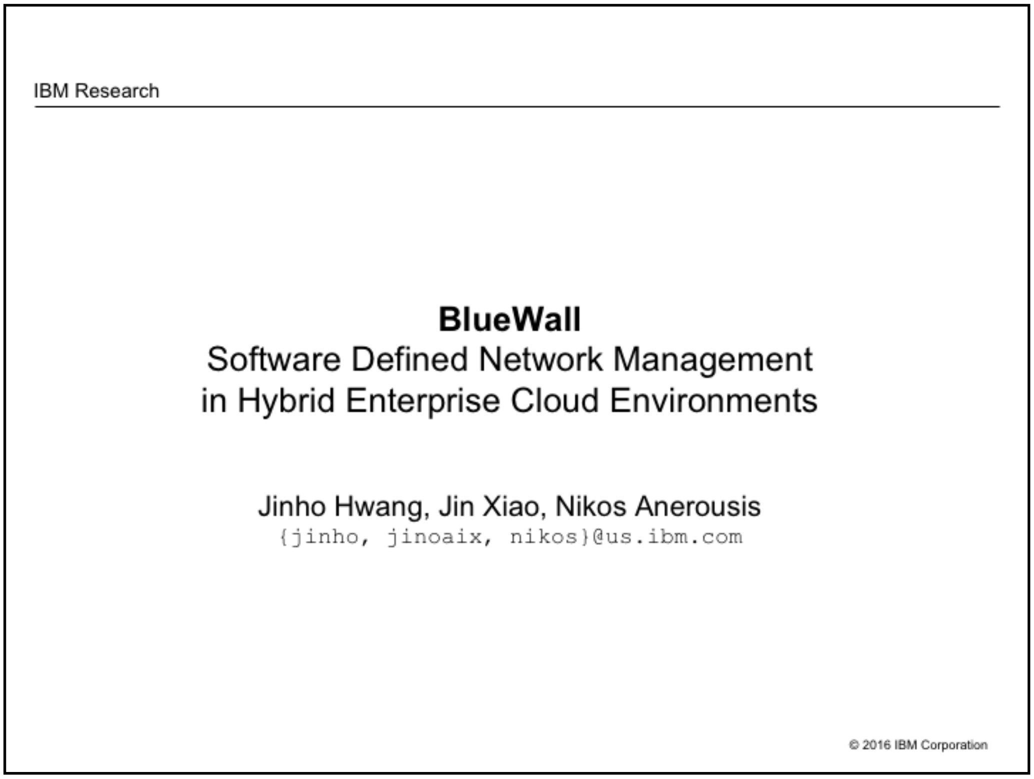
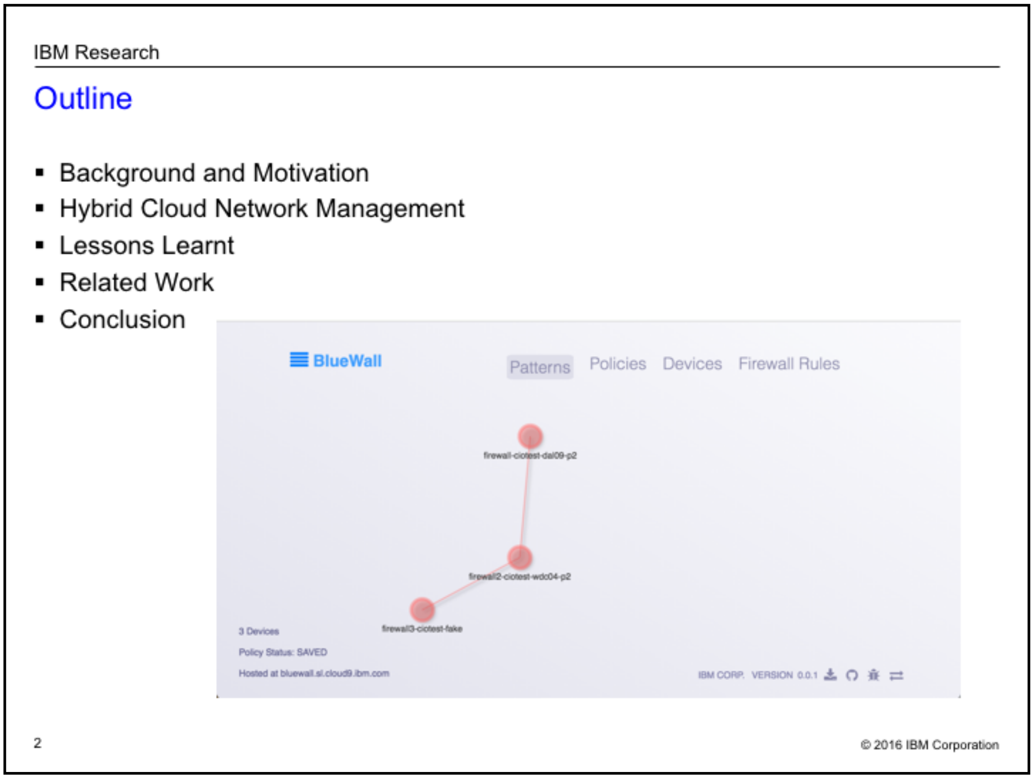
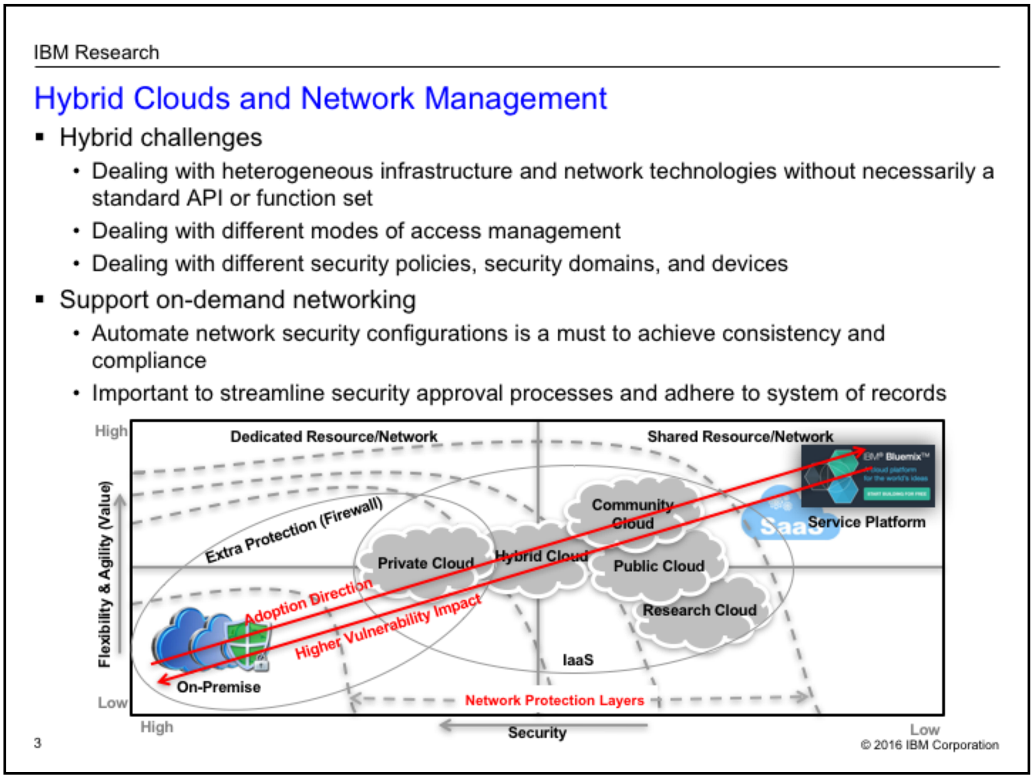


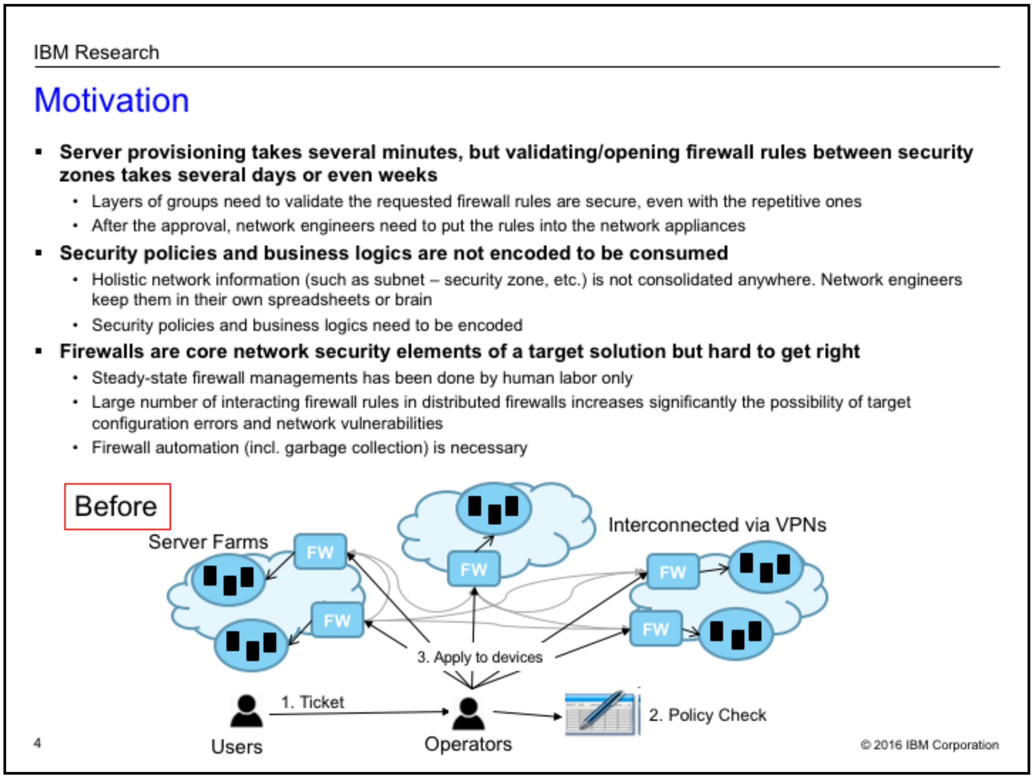
BlueWall is a service for distributed network management in hybrid cloud environments, specifically including on-premise data centers, Infrastructure as a Service (SoftLayer, AWS), and Platform as a Service (Bluemix). While the current centralized network management require exposures of the environments to the centralized management stack, the BlueWall only needs to deploy one micro-service into each environment and secure communication channel back to the orchestrator. This distributed approach allows different policies and application patterns be governed in different network environments, which enables high flexibility when deploying cloud instances in hybrid cloud platforms. We show how BlueWall orchestrates different network environments in a distributed manner, and further how different policies are applied. Finally, we discuss lessons learnt and challenges encountered during this hybrid network management.



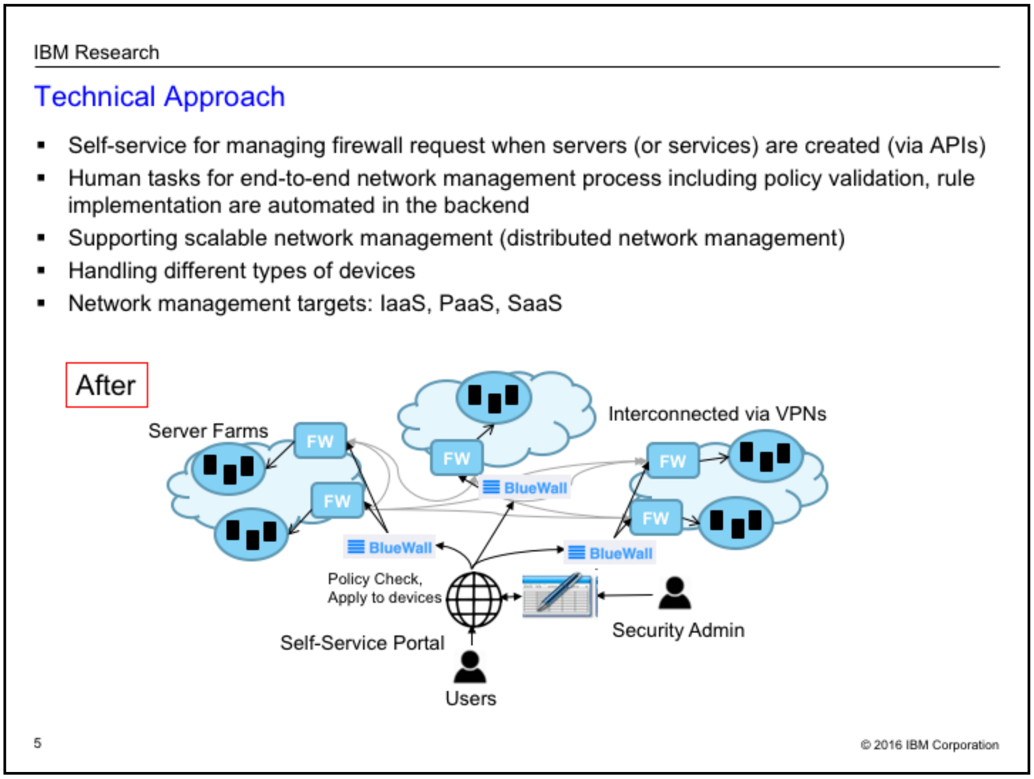
We explain background and motivation of the hybrid cloud network management, and discuss challenges, benefits of distributed network management, and our approach. We illustrate the BlueWall architecture and deployment model. Lastly, we discuss lessons learnt.



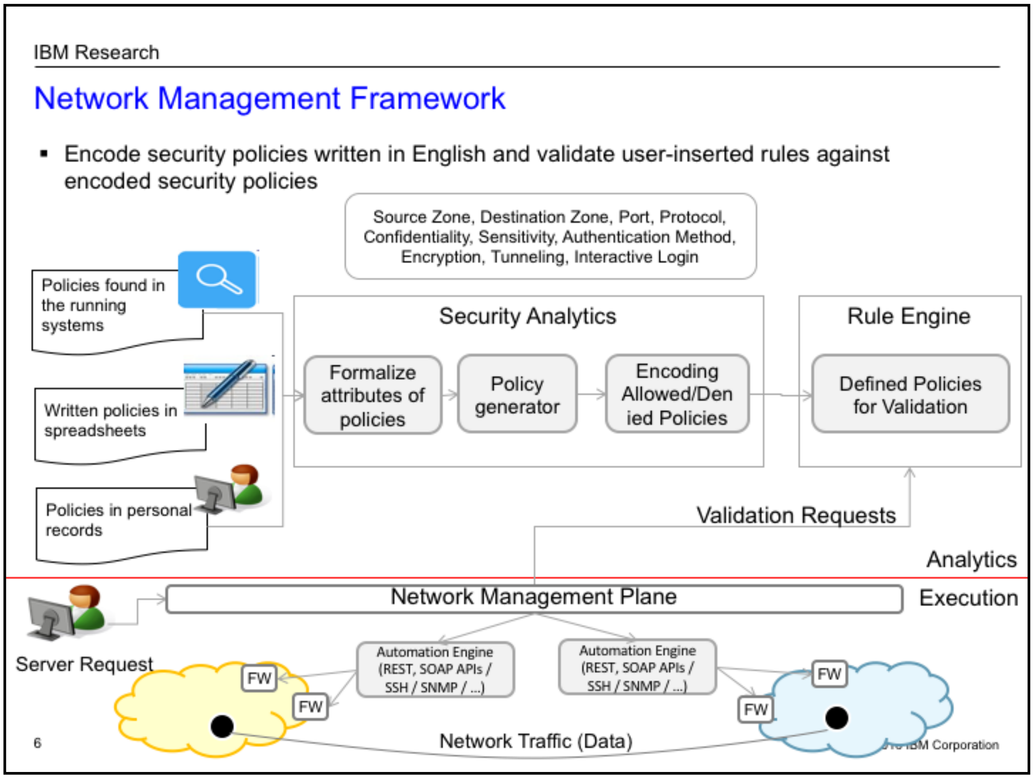
Hybrid cloud holds tremendous promise to enterprises as it allows the enterprise to flexibly deploy services and workloads among on premise, public data centers and private data centers. In many industry market sectors (e.g., banking, healthcare, etc.), hybrid cloud is the only method for enterprises to establish a cloud-centric infrastructure whereby sensitive data are only stored and processed on premise. It follows then hybrid cloud management solutions are needed to address the three listed issues. Each cloud environment today has its own infrastructure design, service mix and methods of access, deploy and operation, especially for network provisioning, configuration and security management. Security policies and the definition of security domains are also domain and infrastructure dependent, that gets further complicated and widened as workloads are spread across multiple cloud infrastructure. At the same time, with increasing automation and resource virtualization, on-demand service/application creation and deployment is a common strategy used to support agile business and development models, and network on-demand challenges us to provide solutions for rapid security configurations that are expedient, consistent and compliant across hybrid environments. Alongside this automation, is the need for streamlined security approval process that can support ease of human administration and compliance audits.



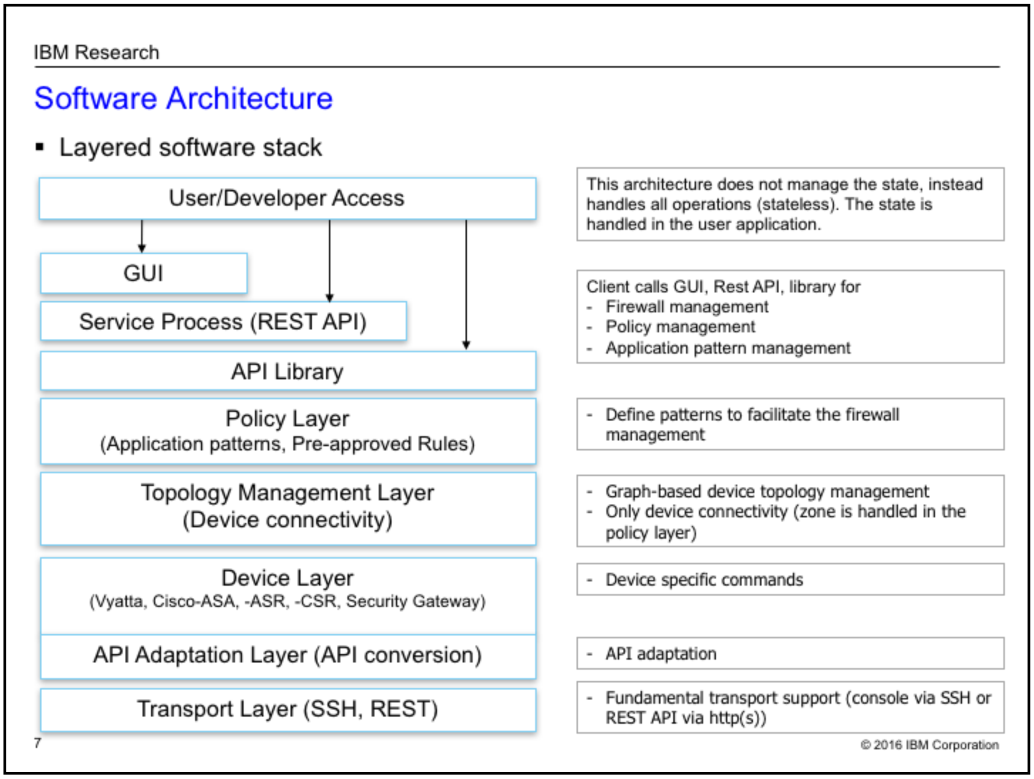
The network security is one of the most important measurement of enterprises. This becomes even more important when enterprises are moving to the cloud environments. Instead of moving everything into the cloud, many companies choose to run hybrid cloud modes with combination of on-premise data centers, public data centers, and private center centers. With the automation of clouds, server provisioning takes several minutes, but validating/opening firewall rules between security zones takes several days or even weeks with stringent security policies, often written in the documents and examined by the security administrators. The main reason for this slow process is that security policies and business logics are not usually encoded to be consumed, and holistic network information (such as subnet – security zone, etc.) is not consolidated anywhere. Also, without the right automation in place, enterprises are wary of large number of interacting firewall rules in distributed firewalls increasing significantly the possibility of target configuration errors and network vulnerabilities.



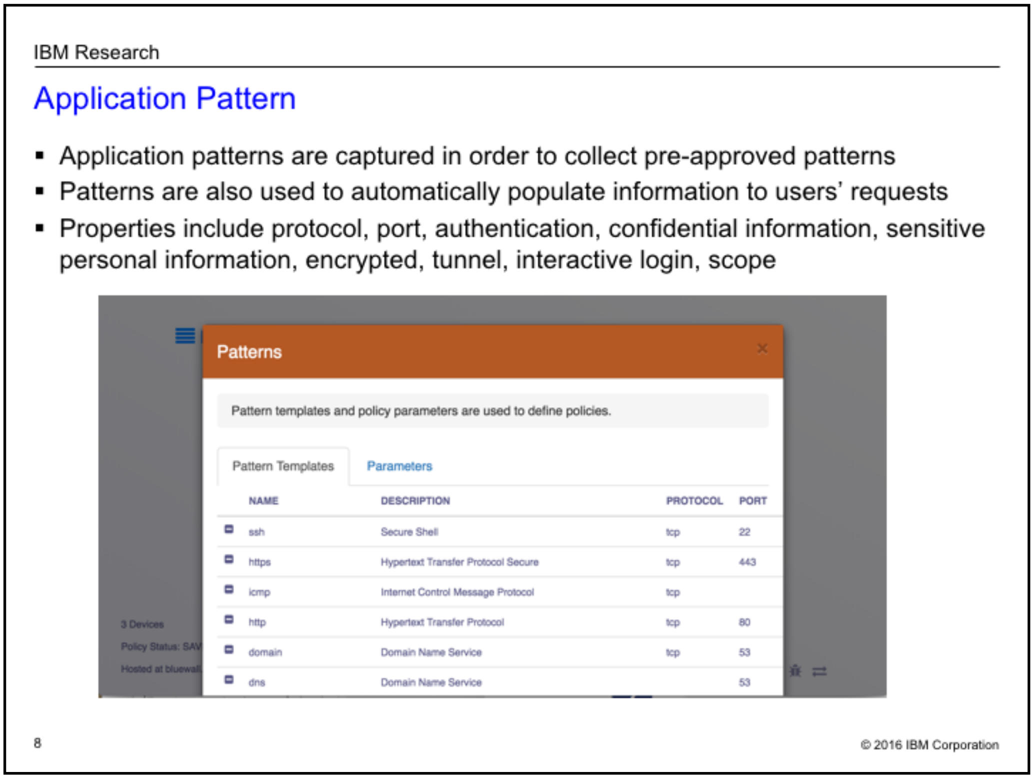
In order to provide a correct network configuration consistent and compliant to the security policies, the automation, audit, and compliance are required. The central orchestrator only keeps the default security policies and application patterns associated with them, but all the automation that manipulate the devices and environmental policies are done in each cloud environment level. To achieve this level of automation, a self-service for managing firewall request when servers (or services) are created (via APIs), and human tasks for end-to-end network management process including policy validation, rule implementation are automated in the backend. Also, this distributed network management supports scalable network management, and handles different types of devices.



The network management (orchestration) plane framework includes the migration of existing security policies into the consumable (encoded) security policies. The identified security attributes include source zone, destination zone, port, protocol, confidentiality information, sensitive personal information, authentication method, encryption, tunneling, and interactive login. Policies are mined from the written security documents, running systems, and personal records, and analyzed to draw common security policies. Then, the defined policies are used for the firewall rule validation in real time when users request new firewall rules and compliance checks are done.



Each micro-service deployed into each cloud environment has this software architecture that covers security policies, topology managements, and device access layers. The network orchestrator access each micro-service through REST APIs, and administrators can also access the service via a graphical user interface. The policy layer downloads the security properties and required rules from the network orchestrator and can append new policies based on the environment. The topology management layer keeps track of the device connectivity in order to find a flow path. The device layer allows this service to access devices via ssh, SOAP, or REST APIs.

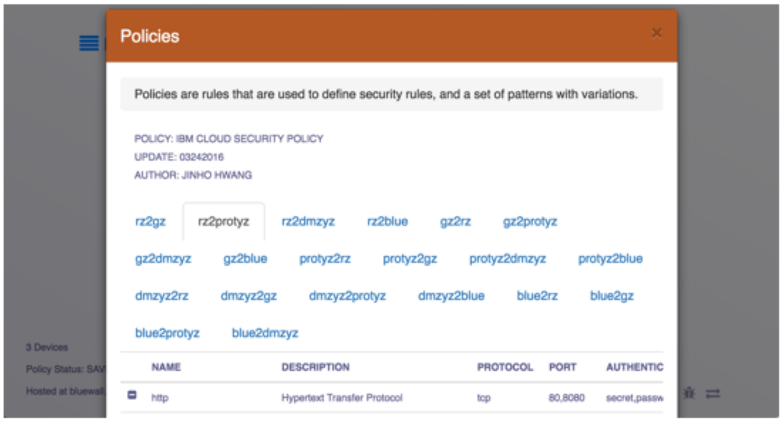


The application patterns are used to collect pre-approved application patterns that can automatically populate the corresponding properties to certain application. The application patterns allow users to specify the application name in order to find all the pertinent properties including protocol, port, authentication, confidential information, sensitive personal information, encrypted, tunnel, interactive login, scope.

IBM Research

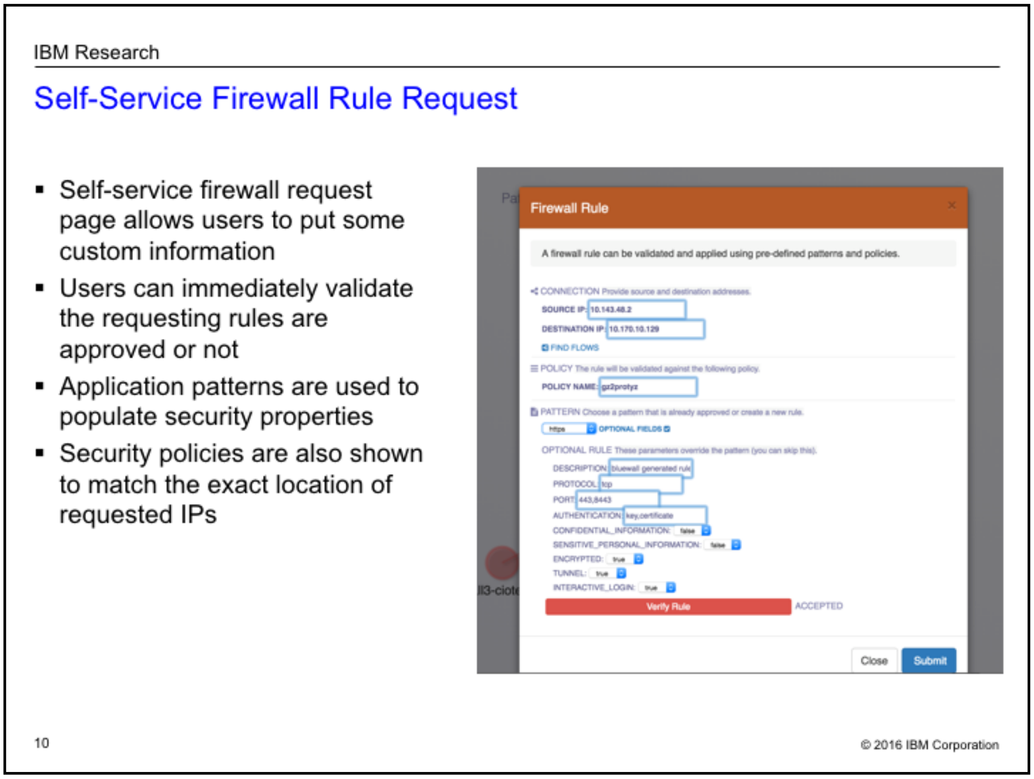
Security Policy

- Network security policies (i.e., zone policy) are captured to validate the firewall rule requests
- Network policies can be adjusted depending on how cloud environments are set up
- Each network policy includes a list of application patterns and their properties

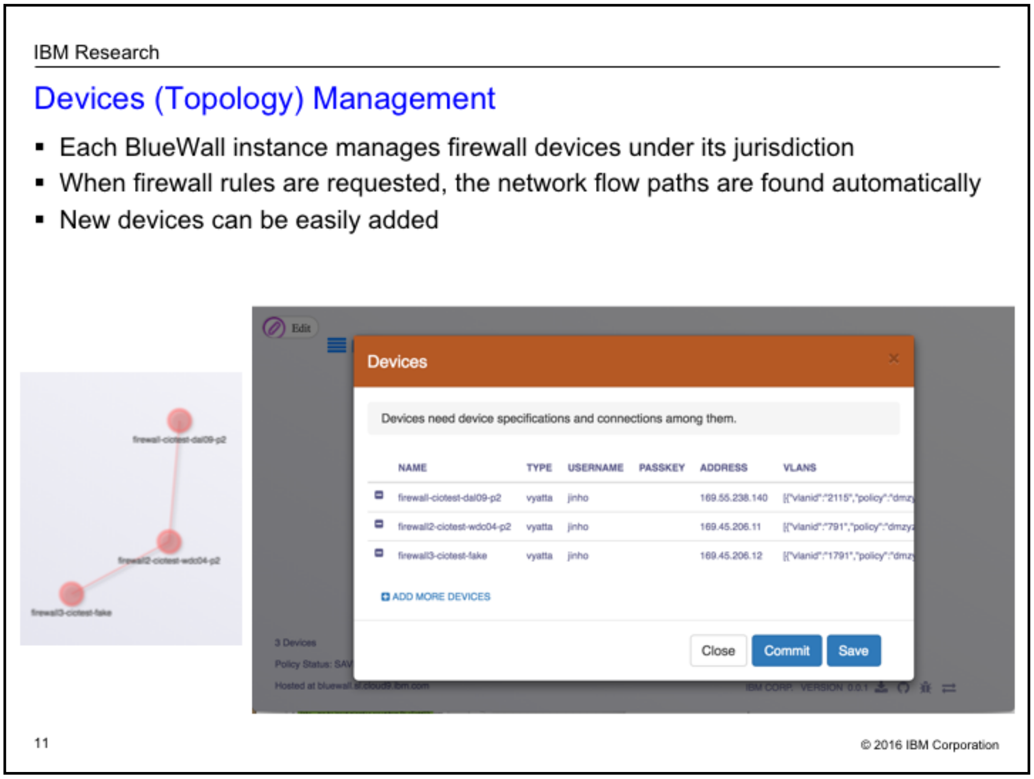


9

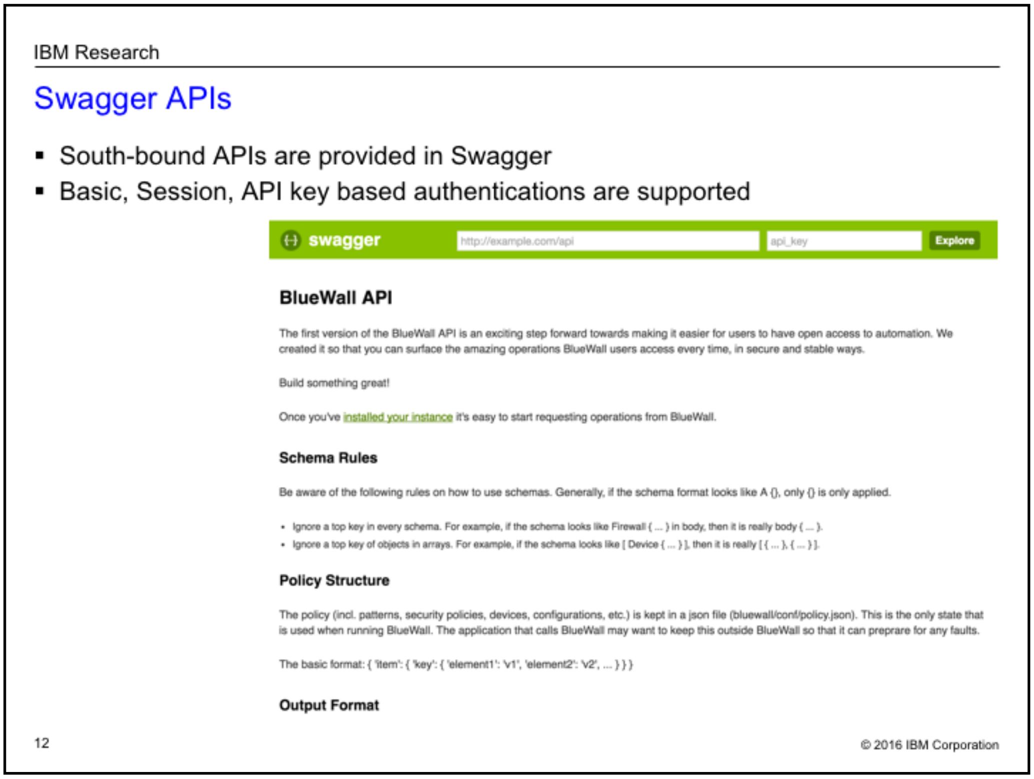
The network security policies include zones and devices that are used to validate the firewall rule requests. The minimally required security policies are downloaded from the network orchestration plane. Depending on the flow path from which device/zone to device/zone, an applied policy is determined and validated against it. Network policies can be adjusted depending on how cloud environments are set up, and Each network policy includes a list of application patterns and their properties.



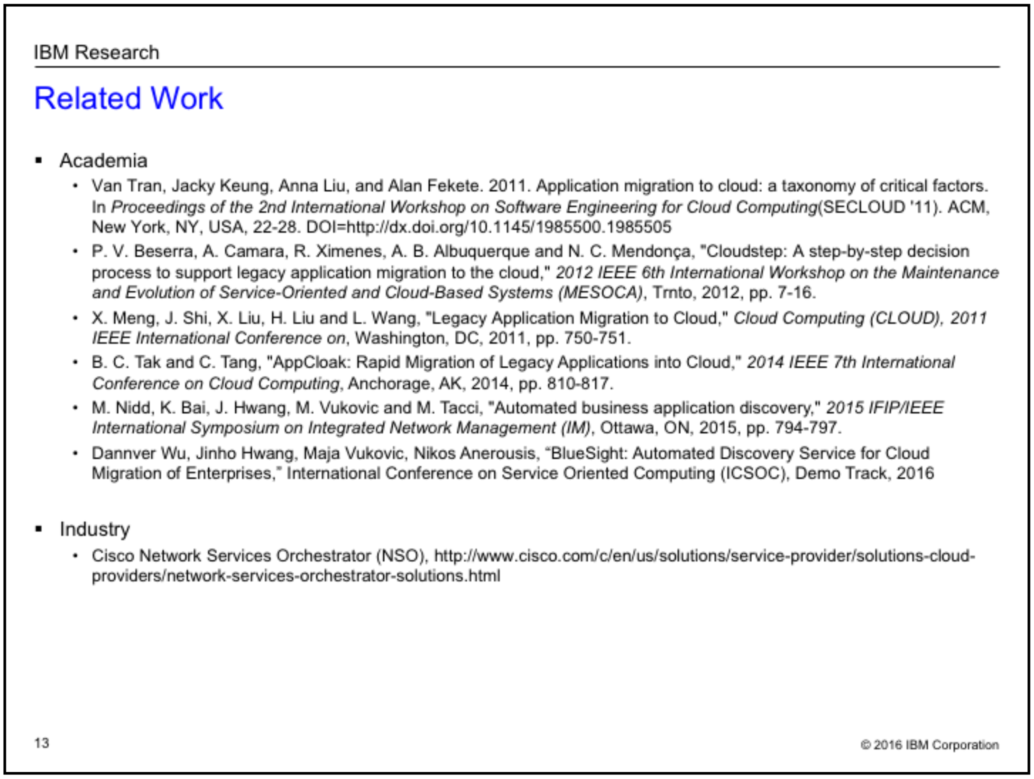
Users can submit the firewall rule requests through the self-service firewall request form. Users can immediately validate the requesting rules, which used to take a couple of days or weeks going through the human approval chains. Also, applications patterns are used to populate security properties for the sake of consistency and convenience. Security policies are also shown to match the exact location of requested IPs.



The devices are managed in each service of each environment. The device information is used to discover the flow path along the network routing path, and this helps to determine which security policy needs to be used across different devices (and zones). The network orchestration layer does not need to know anything related to the devices.



The south-bound APIs are provided in the swagger format. Currently, the BlueWall provides 5 APIs including policy, firewall, verify, flows, and patterns. The policy APIs allow administrators or orchestrators to update the security policies. The firewall APIs allow users to request firewall rules. The verify APIs enable real time rule validation. The flows discover flow paths with source and destination pair. The patterns provide pre-defined application patterns. The authentication method include basic, session, and key based approaches.



Van Tran, Jacky Keung, Anna Liu, and Alan Fekete. 2011. Application migration to cloud: a taxonomy of critical factors. In Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing(SECLOUD '11). ACM, New York, NY, USA, 22-28. DOI=http://dx.doi.org/10.1145/1985500.1985505

P. V. Beserra, A. Camara, R. Ximenes, A. B. Albuquerque and N. C. Mendonça, "Cloudstep: A step-by-step decision process to support legacy application migration to the cloud," 2012 IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), Trnto, 2012, pp. 7-16.

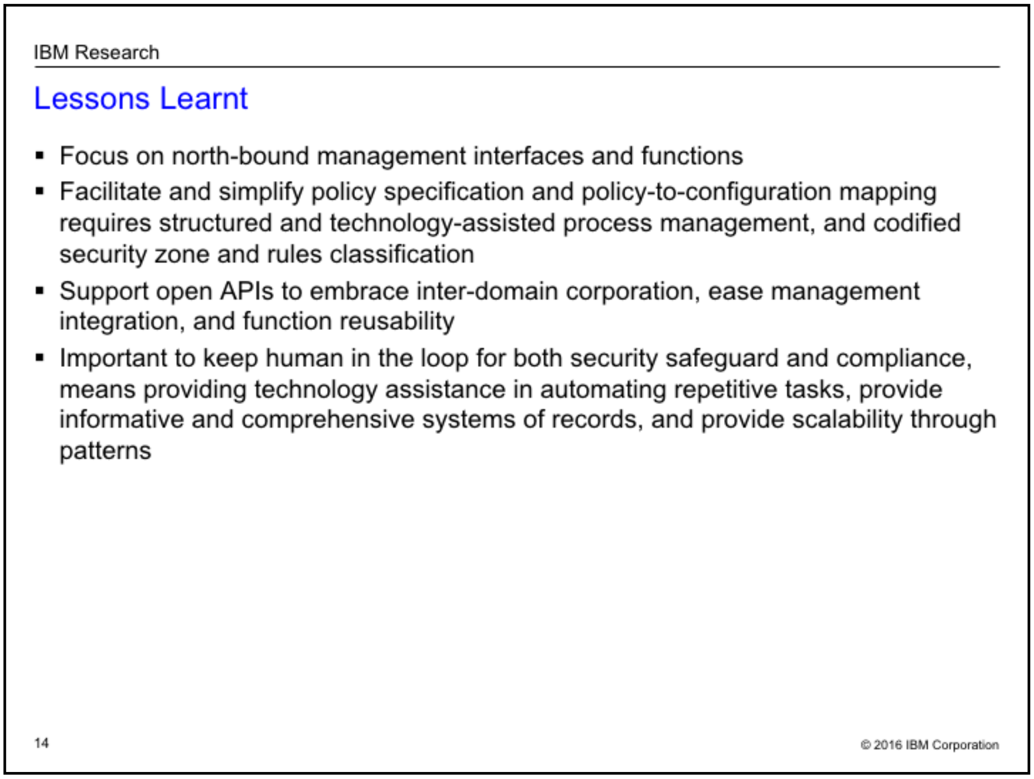
X. Meng, J. Shi, X. Liu, H. Liu and L. Wang, "Legacy Application Migration to Cloud," Cloud Computing (CLOUD), 2011 IEEE International Conference on, Washington, DC, 2011, pp. 750-751.

B. C. Tak and C. Tang, "AppCloak: Rapid Migration of Legacy Applications into Cloud," 2014 IEEE 7th International Conference on Cloud Computing, Anchorage, AK, 2014, pp. 810-817.

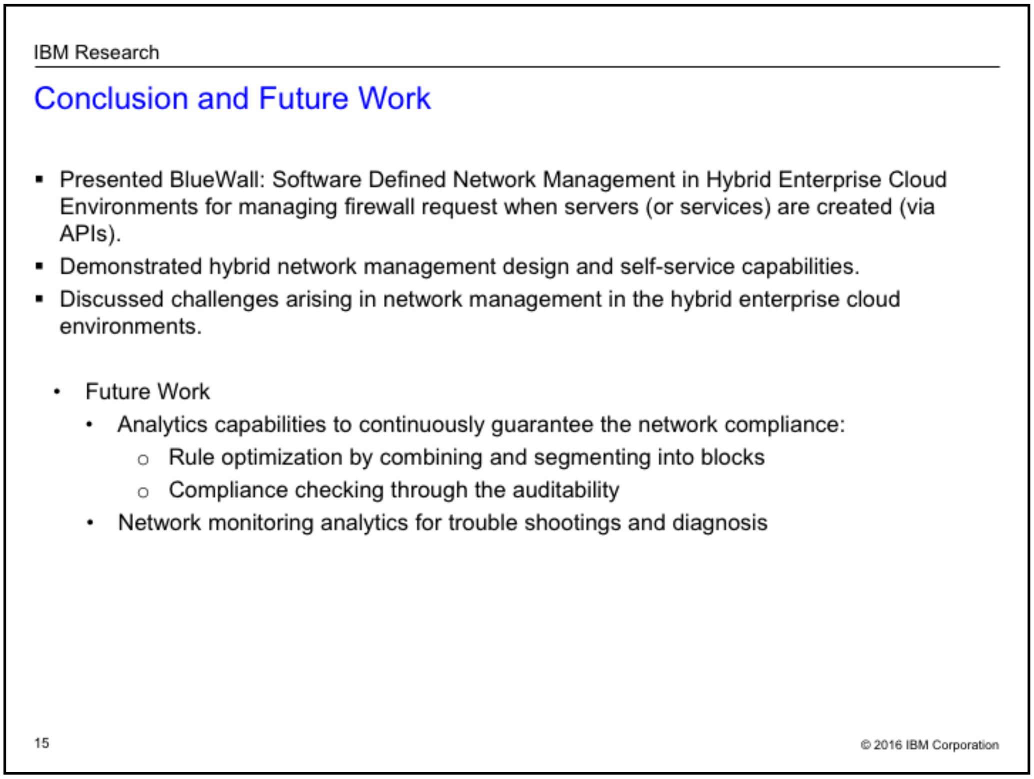
M. Nidd, K. Bai, J. Hwang, M. Vukovic and M. Tacci, "Automated business application discovery," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015, pp. 794-797.

Dannver Wu, Jinho Hwang, Maja Vukovic, Nikos Anerousis, “BlueSight: Automated Discovery Service for Cloud Migration of Enterprises,” International Conference on Service Oriented Computing (ICSOC), Demo Track, 2016

Cisco Network Services Orchestrator (NSO), http://www.cisco.com/c/en/us/solutions/service-provider/solutions-cloud-providers/network-services-orchestrator-solutions.html



Through our research and development, we've come to learn many voids need to be filled to achieve hybrid cloud management. In particular, hybrid could network security management and automation requires a comprehensive encapsulation, definition and representation of security policies, patterns, topology and domain specific administration rules. Network automation needs to be supported by a overarching orchestrator and governed by a security policy approval process. In order to facilitate and simplify policy specification to achieve management scale, process management need to provide security zone abstraction, pattern-based specification of policy rule sets, and dealing with inter-zone policy specification in broad strokes, while providing consistent mapping of policy to rules. We also adhered to open API designs which is much needed in developing hybrid cloud management solutions as it allows for easy integration of new policies and technologies in a transparent and standardized way, and promise cross-domain function reuse. Finally, it is important to keep human in the loop, as humans are ultimately accountable for both security safeguard and compliance audits. We focused on technology assistance that automate repetitive and mundane tasks at the rule creation and network configuration level, while keeping human administration at the top policy and inter-domain level by providing abstraction, domain association and end-to-end workflow view across hybrid infrastructure. We further provided detailed and consistent systems of records that enabling tracking any network configuration requests among its requesting application/service, applicable security policies across security zones, approval records, and log of network execution.



We presented BlueWall -- a service for distributed cloud network management in hybrid cloud environments. We showed how BlueWall manages security policies, application patterns, device topologies, how BlueWall orchestrates different network environments in a distributed manner. We also discussed lessons learnt and challenges encountered during this hybrid network management.

Currently our system focuses on automation of the firewall validation and automation of the rule implementation in the hybrid environments spanning different cloud data centers. Our future work is two-fold, we plan to focus on automated network audit and compliance checks of existing rules, especially when policies are changed. Secondly, we want to extend the platform to support the network analytics that can monitor the network devices and perform trouble shootings. That will require distributed analytics processing platform, and consolidated data store for the comprehensive analytics.