



Facing Network Policy Complexity

Cyber Operations Inc.
<http://www.CyberOperations.com>
153 Cahaba Valley Parkway
Pelham, AL 35124
Ph: 866-404-2923
Fax: 205-503-5732

Access Policy Complexity

With the growth of the internet the amount of malicious activity as well as the size of the networking resources that have to be managed by a typical organization have grown and continue to grow. Changes in the size and nature of the internet environment have caused an increase in size and complexity of network filtering policy and implementation. These issues are compounded when different personnel, hardware brands, and physical locations come into play. The end result is a need for a new type of tool for managing network access control.

Network access policies are frequently updated by different personnel in the same organization. Personnel turnover, number of policy rules, and the fallibility of human memory lead to mysterious access control lists entries for which no one knows the reason for creation, but everyone fears the possible adverse effects of deleting them.

The very linear and simplistic nature of access list syntax in most network devices which is intended to allow straightforward configuration causes problems when scaling to large lists and large organizations.

Access list policies must coincide when some are overall policies that change infrequently while others are known offender lists that are constantly updated. Organizations with multiple locations and multiple network gateways need a way to control compliance to their access policies on all these devices at different locations.

Differences between router and firewall devices from different vendors cause an increase in the time network administrators must devote to learning to operate these devices as well as in increase in the likelihood of costly errors. Often, it is not feasible for organizations to adopt new technologies offered by new network security devices because they cannot afford the time required for their IT professionals to become familiar with a new platform.

The time required to manually configure access list changes in all the devices used by an organization to filter network traffic limits the ability of security professionals to react to new threats effectively.

Networking professionals are increasingly realizing that a better way is needed to handle the complexities of network access policy. They are seeking out tools to help them address these issues in several ways.

Automation: Organizations managing multiple devices do not want to manually enter new rules or manually upload new versions of access lists to each router and firewall whenever there is a change to policy or a need to respond to a threat.

Compliance: Managers who are responsible for networking infrastructure need a way to verify that the policies that are developed for the network are actually being implemented correctly and applied as directed.

Portability: Configuring access control lists is an area that has basically all of the concepts in common between vendors, and no standard for the syntax or format. The disparity between devices is not only a drain on manpower in organizations, but it also a hindrance to adopting better solutions when they become available.

Tracking: Organizations also need a way to track what changes have been made to their access lists both globally and on a per device basis for troubleshooting and for ensuring compliance to policy. When a policy related problem occurs, anyone responsible for finding the solution needs the ability to see what has changed.

Several helpful data artifacts that are not easily or not sufficiently tracked by most network filtering devices are:

1. Why was a rule put in place?
2. Who put the rule in place?
3. When should the rule cease to be in effect, if ever?

Troubleshooting: Network administrators and their managers need tools to help them create correct access rules before deployment and track down the source of problems when they do occur.

The solution to all these problems hinges on two concepts: centralization and indirection. If your rules are not maintained in a centralized location, you will inevitably duplicate work and introduce opportunities for human error during deployment. If you place a level of indirection between the administrator and the devices then you remove the need to constantly learn new platform specific configuration syntax, and you have a point where you can introduce management tools to help you ensure compliance and troubleshoot problems.

“Any problem in computer science can be solved with another layer of indirection.”
- David Wheeler

Cyber Operations’ *Cyber ACL* offers a total solution to these problems. The system is based around a central server and database that provides the same web interface to all users, automates deployments to devices, provides platform independence by handling translation to each device’s native syntax, gives users advanced editing and troubleshooting tools, and allows managers to track all list modifications and deployments.