Effect of dynamic ACL (access control list) loading on performance of Cisco routers

A.Bobyshev, P.DeMar, D.Lamore, Fermilab, Batavia, IL 60510, U.S.A.

Abstract.

An ACL (access control list) is one of a few tools that network administrators often use to restrict access to various network objects. ACLs can also be used to control forwarding of traffic, facilitating so-called “policy based routing”. There is a current need to update ACLs dynamically by programmable tools with as low latency as possible.

At Fermilab we have approximately four years of experience in the area of dynamic reconfiguration of network infrastructure. However, dynamic updates also introduce significant challenges for performance of networking devices. This paper introduces the results of our research, as well as practical experience in dynamic configuration of network infrastructure by using various types of ACLs. The questions that we seek to answer include what is the maximum size of the ACL, how frequently it can be downloaded without significant impact on router CPU utilization and forwarding capabilities, updating of active versus passive ACL, and updates of multiple ACLs.

Overview.

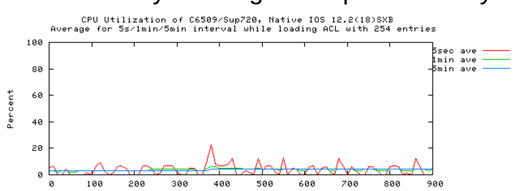
Access Control Lists (ACLs) can be used for many different network protocols, including IP, AppleTalk, IPX and others. In our tests we focus on IP protocol with so-called extended type of access lists supported in Cisco Systems' IOS software. In this paper, we do not cover the relatively new sequencing type of ACL, supported in IOS starting IOS 12.2(14)S and later.

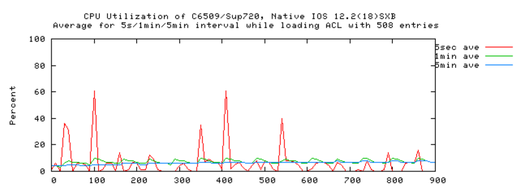
At Fermilab, ACLs are used for protection of the network perimeter, and for the implementation of policy based routing. ACLs can be modified either in the static mode, in which the network administrator make changes manually, or via automated scripts. Static changes are typically infrequent and minimally disruptive. There exists a need to understand the limits in which automated scripts can modify ACLs in order to protect network equipment from overloading its resources. Modification of ACLs can be done in two different ways. New ACL commands can completely overwrite the active ACL that is already applied on the router interface. The second way is to upload a new ACL with a different identifier, and then replace the active ACL on the router interface with the new one. Again, in this paper we do not cover the sequencing type of ACL that allows one to add, remove, or modify specific ACL entries. We seek to answer the following questions:

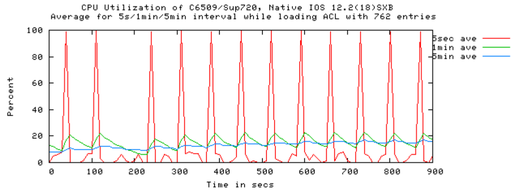
- What size ACL that can be uploaded to the routers without significantly affecting CPU utilization?
- What is the impact of loading an active ACL versus a passive ACL?
- What is the effect of uploading multiple ACLs?
- What is the maximum size of ACL that can be uploaded occasionally without significantly affecting CPU utilization?

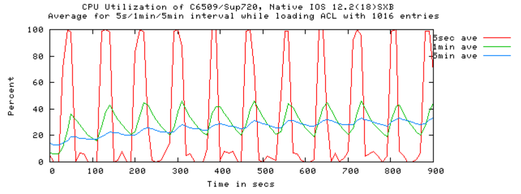
Methodology.

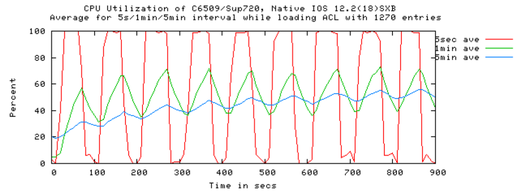
In our tests we used a Cisco Catalyst 6509 with a Supervisor 720 and 512MB of memory. The software was native IOS 12.2(18) SXB. To upload configuration updates we used the CiscoConfigCopyMIB to initiate a TFTP transfer from the router by sending it an SNMP set request with information about location of the files with ACL changes. We measured CPU utilization by polling at 5 second intervals the router's statistics for the previous 5 seconds, 1 minute and 5 minute periods. ACLs were composed from randomly generated entries of a specified number of entries. We tried to upload a new ACL every 1 minute. We were concurrently testing connectivity through the router by sending ICMP probes every 10 secs.

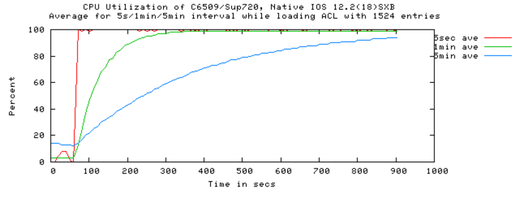








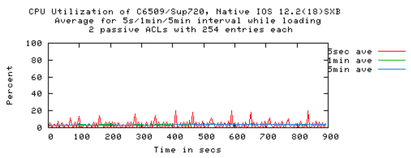


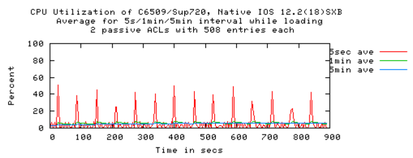


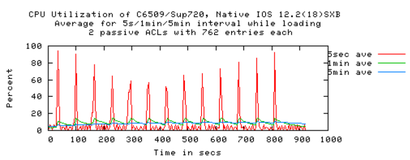
The graphs above show the effect of uploading an active ACL. 70%- 80% CPU utilization is considered high. As can be seen from the measurements, an ACL with about 1000 entries can be frequently loaded and CPU utilization will stabilize at the 30-40% level. Short spikes up to 100% are acceptable as long as their duration remains within a 5-15 second interval. At this point we did not notice other negative effects, such as problems connecting to the router or dropped ICMP packets. When the size of the ACL approached 1500 entries, the 1 minute and 5 minute average CPU utilization reached 100%. The 5 second average sustained a steady 100% level. We also noticed problems connecting to router management interface, although no dropped packets were observed. Uploading of two active ACLs gave approximately the same results. In other words, we did not observe two active ACLs increasing a negative effect on CPU utilization compared to uploading of one ACL.

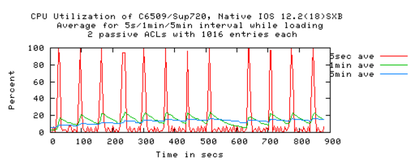
Loading of passive ACL.

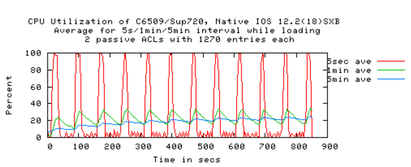
In this test a new ACL was first upload in the router under a different name. Then the old ACL was removed from the interface's configuration and the new one was applied. All the changes were made by our automated tool. The SNMP “set” request to router for uploading of new configuration was sent every minute.

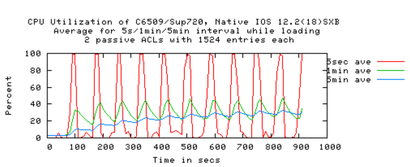


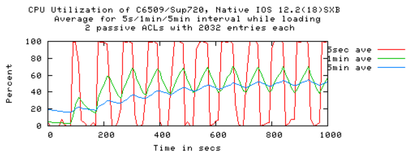


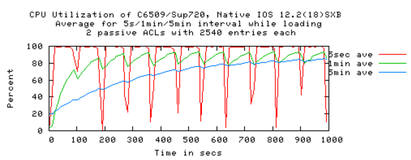








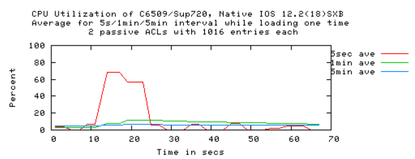


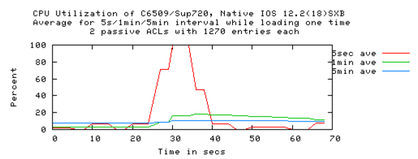


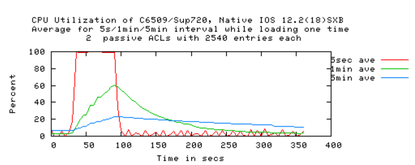
As shown by these graphs a passive method of reconfiguring an ACL is the least disruptive for the router. Using passive updates allows to raise the limit of maximum entries in the ACL to 2000 entries. We were able to upload up to three ACLs with about 2500 entries every minute without significant increase of CPU utilization compared to uploading of a single ACL of the same size. However, the 1 minute and 5 minute average CPU utilization reached 80% level which is unacceptably high. It is safer to keep the ACL size under 2000 entries.

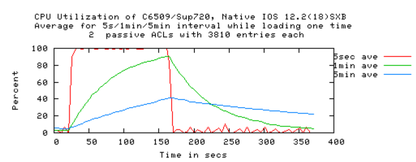
A one-time uploading of a large ACL.

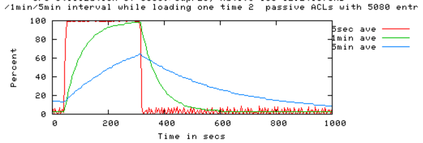
The most serious negative impact on a router's performance comes not from an ACL's size but from the process used to update it. In subsequent tests, we periodically tried to upload a large ACL, but executed the request only after CPU utilization returned to the normal levels observed before the previous request.

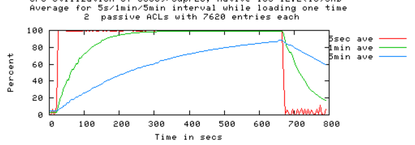












Conclusion.

- A limit of 1000 entries for ACLs is a reasonable choice when reconfigurations need to be done dynamically and frequently.
- In the case of passive updating of ACLs with about 1000 entries a router performs slightly better compared to updating of active ACLs but still may be significantly overloaded if the size of ACL grows to 2500 entries.
- A router's CPU utilization does not depend greatly on the number of active ACLs. In other words, it is less disruptive to use two ACLs with 1000 entries each rather than it is to use one ACL with 2000 entries.
- One-time loading of an ACL with 5000 entries is feasible, but it will take approximately 3-4 minutes for the router CPU utilization to return to normal levels.