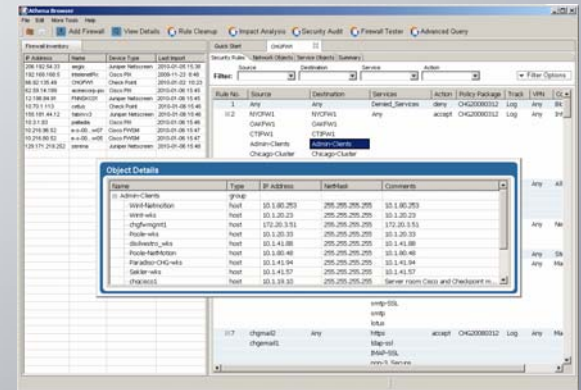


Athena's Firewall Browser

Quick Start How-To Guide

Use this How-To Guide to take advantage of flexible features available in the Firewall Browser. Once you have imported your configurations, you can use the powerful search capabilities to:



Verify if a change request is already handled by the security rules

In the Security Rules tab, specify Source and Destination IP addresses and service, select the option Filter by IP address/Port and hit enter. For Cisco, select the entering interface or exiting interfaces for the IP packet represented in the change request to pinpoint the access-list that needs to be modified. For Netscreen, select entering and exiting zones for the IP packet in the change request to pinpoint the zone to zone policy that needs to be modified. The rule results will show all the rules that match any part of the packet. If the IP addresses in the change request are too broad (because of a netmask), then the rules have to be queried (with object groups expanded if present) to see if the change request is completely handled or partially handled by the matched rules.

Find the best objects that can be reused for making a change

In the Network objects tab, specify the IP address and netmask you are interested in, and in the Service objects tab, specify the port you are interested in, to find all objects that match the given input. Use the Type drop down to further filter results to the required address or service object type. You can also specify search on the object hierarchy to locate additional objects that contain your input specification.

Find the best rules that can be reused for making a change

In the Security Rules tab, specify any 2 or 3 of the Source, Destination IP addresses and/or service values from the change request, select the option Filter by IP address/Port and hit enter. This will give you all rules that match the given input. You can select the rules from the results that best match your request for modification. You may have to try multiple combinations before you select the rule that is a best match.



Figure out the impact of a change to an object group

In the Security Rules tab, specify the object name in Source or Destination or Service and select Search Object hierarchy. This will show all rules that refer to the given object name including parent/ancestor object groups as Source or as Destination or as Service.

Find out if the change being contemplated (src, dst, service, action) can have an adverse impact

In the Security Rules tab, specify Source, Destination IP addresses and service, select the option Filter by IP address/Port and hit enter. Look for rules that have the opposite action (accept, deny) of the change request and make sure that you take into account the effect of these rules before making a change. For example, if the change is allowing a new service for very specific source or destination, the rule needs to be added before a deny rule that blocks the service. Similarly if the change is closing a security hole, then the new rule needs to be added before all rules that allow the service.

Find out if the rule being added makes redundant any existing rules

In the Security Rules tab, specify Source and Destination IP addresses and service being used for the rule, select the option Filter by IP address/Port and hit enter. Look at the returned results to see if any rules are completely covered by the new rule.

