

# Comparing Athena FirePAC With Tools That Use Pattern-Based Syntactic Analysis



***Written by:***

Vijaya Raghavan  
Director  
Athena Security India Pvt. Ltd.  
+91 98452 09423

## Executive Summary

We compared the policy analysis provided by tools that use a pattern based, or syntactic analysis approach, with that of Athena FirePAC. These solutions are not comparable to FirePAC because syntactic analysis is based only on security rules or ACLs. The semantic analysis approach used by FirePAC is necessary because a firewall's response to traffic is determined by security rules combining with network address translation and routing rules. By ignoring the latter rule types, syntactic analysis tools provide policy results that are not always accurate.

Policy analysis was compared against the following parameters:

1. In the presence of Network Address Translation and Routing rules.
2. Against devices that allowed interface specific rules.
3. Quality of directional analysis.
4. Assessment of policies to or from the firewall.
5. Handling of default behavior.
6. Analysis of virtual private networks.

The following comparison will elaborate on what we determined makes Athena FirePAC's policy analysis qualitatively superior and consistently more accurate in all the above situations.

## Comparison Report

### Network Address Translation and Routing Rules

Syntactic rule analysis does not analyze network address translation (NAT) and routing rules in its policy analysis. This analysis is confined to ACLs or the security rules and results in the reporting of spurious policies as being present – a case of false positive policies. In particular, anti-spoofing rules are not taken into consideration during policy analysis with dubious results.

Athena FirePAC does a true semantic analysis of the rule base including security rules (ACLs), NAT rules and route rules. These rules are analyzed in the same manner in which they are processed by the firewall and hence the policy results are accurate and reflect the true policies that are programmed into the device. Anti-spoofing rules are understood and correspondingly modeled.

### Handling of interface specific rules

Several firewall brands allow security rules to be applied by device interface. That is, the rule base is divided into sections or rule-sets and each rule-set may be applied to one or more of the device interfaces. This means that based on the direction and path of the traffic through the device, different rules are applied to filter and translate the data packets flowing through the device. Syntactic analysis tools may not support such interface specific rule handling and consider the rule base to be universal and applied across all interfaces. This is because syntactic analysis tools do not have a behavioral model of different devices to support its analysis.

Athena FirePAC understands different firewall brands and their unique handling of data traffic. Its analysis incorporates this understanding and allows for brand specific differences of behavior. Consequently, the ability of FirePAC to produce accurate results in a heterogeneous network is superior.

## **Directional Analysis**

Syntactic analysis tools do not perform directional policy analysis. That is, policies in the security rule base are equally applied to all directions of traffic. This is wrong because routing and network address translations alter the nature of traffic that is allowed between the different firewall interfaces and networks connected to them.

Athena FirePAC performs truly bidirectional analysis taking all rules into consideration. Thus, it is able to predict accurately the traffic that is allowed between two interfaces of the firewall in either direction, and as often is the case, there is a difference to what is allowed and what is stopped in either direction.

## **Policies to/from the firewall**

All firewalls have specific policies for the traffic that is allowed to the firewall itself and what is permitted from the firewall. These are crucial policies because they determine the vulnerability of the firewall itself to attacks. Syntactic analysis tools do not highlight the policies to and from the firewall. This kind of policy analysis does not provide the complete information that is obtainable through a strict analysis of the rule base.

Athena FirePAC computes policies to, from and through the firewall in an identical way – that is, by using its powerful semantic analysis technology. So, the nature of traffic that is allowed to and from the firewall is accurately determined and vulnerabilities comprehensively reported.

## **Handling of default behavior**

Firewall device default behavior is not taken into consideration by syntactic analysis tools. This is because the policy is extracted from the security rules exclusively, ignoring device default behavior. This can lead to erroneous conclusions on policy.

Athena FirePAC uses device defaults during policy analysis and is thus able to accurately predict device behavior at runtime.

## **Virtual Private Networks**

The policy analysis from syntactic policy analysis tools does not properly address virtual private networks. It is not possible to interrogate the software about the traffic that is allowed or stopped by the virtual private networks. That is, policy queries are not supported for VPNs. Athena FirePAC models virtual private networks as virtual device interfaces and uses the information in the rule base to determine the policies that are allowed or denied to these VPNs. Thus the nature of traffic through VPNs can be queried and policy checks can be installed into the analysis in order to ensure that network security is not compromised via the VPN.