

AthenaFirePAC v2.1.2.1 Release Notes

Release Date: 08 April 2009

1 Summary of Release

This is the v2.1.2.1 release of the AthenaFirePAC™ product.

2 Devices Supported

Following devices are supported:

- Cisco PIX
- Cisco ASA
- Cisco FWSM
- Netscreen
- Checkpoint FW-1 NGX
- Secure Platform
- Cross beam
- Nokia IPSO

Limitations of each device adapter are presented in Section 4 Known Issues in this Release in these Release Notes.

3 Overview

FirePAC provides comprehensive firewall analysis with four essential must-have capabilities for every network engineer.

Four types of report are generated using Athena FirePAC:

- The Risky Policy Findings report includes report based on packet filtering ACLs, routing tables, and NATs. It will also evaluate the policies against industry best practices
- The Rule Conflict Report identifies rule conflicts in firewalls by identifying redundant, correlated, generalized and shadowed rules.
- The policy query report analyzes the firewall policy. It is possible to query the policy for a specific address space.
- The Culprit rules analysis report analyzes the risky policy findings to identify rules occurring most frequently in failed firewall checks.
- The policy diff report compares the firewall policy between two configurations.

4 New features

This release contains the following new features:

- An optional feature for migration has been implemented.
- Migration policy diff report generates a policy diff report with ruletrails that display the policy differences between the original device configuration and the new device configuration of a different type.

5 Known Issues in this Release

The known issues in this release follow. Where applicable, they are categorized by Device Adapter type:

- Implicit rules cannot be traced back to original configuration for devices other than checkpoint.
- Same route rules with preference are not handled in the parsing of CiscoPIX dynamic routes.
- NSM Configurations for Netscreen firewalls are not supported.
- On Windows 2000, GDI+ library must be installed for better quality graphics.
- Reports cannot be generated for very large accept policies.

Issues Common to All Devices

The known issues common to all device adapters in this AthenaFirePAC 2.1.2.1 release are:

- IPv6 is not supported.
- DHCP/DIALUP based IP addresses are not supported for network interfaces.
- Dynamic VPN connection is not supported for any device adapters.
- Policy-based routing is not supported.
- Dynamic discovery of VPN peer is not supported
- DCE RPC services is not supported
- Traffic filtering based on application layer information is not supported

The other known issues in this release follow. Where applicable, they are categorized by Device Adapter type.

PIX Devices

- Failover/Cluster configurations are not supported.
- GRE tunnel is not supported.
- ASA multiple context - Network Interface sharing between contexts is not supported.
- FWSM multiple contexts are not supported
- FWSM versions below 3.1 are not supported.

NetScreen

- NSRP failover configurations (Active/Active, Active/Standby) and interface failover are not supported.
- Transparent mode is not supported.
- Hub and Spoke VPN configurations without an explicit policy to allow traffic between the hubs are not supported.
- Virtual systems are not supported.

Checkpoint

The following global properties for Checkpoint are included in this release.

```
Accept Remote Access Connections
Accept Outgoing Packets
Accept Domain Name over UDP
Accept Domain Name over TCP
Accept ICMP Requests
Accept CPRID Connections
Accept DHCP traffic
Accept RIP
```

The following are not supported for checkpoint devices.

- Remote Access VPNs.
- Domain-based VPN routing.
- VPN domain behind internal interfaces of a gateway.
- Directional VPN, Multiple Entry Point VPN and Route-based VPN.
- IP Pool NAT.
- Authentication rules that intersect with the user database are NOT supported.
- Checkpoint security rules which authenticate users, clients and sessions are not supported by FirePAC
- Overlapping NAT using the following parameters that can be defined on an interface:

```
enable_overlapping_nat_ overlap_nat_dst_ipaddr,
overlap_nat_src_ipaddr and overlap_nat_netmask.
```

The following global properties settings are not supported:

- Accept VPN-1 Pro/Express Control Connections
- Accept VRRP packets originating from cluster members
- Enable VPN Directional Match
- Virtual systems are not supported.

6 Problems Addressed in this Release

The following salient problems were resolved in this release:

- HyperLinks in Culprit Rule Report for Checkpoint are now linked correctly.
- PCI analysis now treats PCI Zones as PCI Zones only and not as internal or DMZ
- If Checkpoint route format is wrong, FirePAC displays an ERROR message instead of WARNING
- Culprit rules summary table is now sorted in descending order
- Splash screen pops down after the application is launched.
- Services are now correctly ordered in policy summary.
- Error handling has been improved in Device Translators.
- Duplicate host with same names are no longer supported in devices repository.
- FirePAC Bounds are determined and upgrade is suggested before running analysis.
- AthenaFirePAC can no longer be uninstalled when the application is open.