DEPLOYMENT GUIDE

Fortinet and AlgoSec Security Management Suite
Fortinet and AlgoSec Security Management Suite

Overview ......................................................... 3
Deployment Prerequisites ................................. 3
Architecture Overview ................................. 3
FortiManager Configuration ......................... 3
AlgoSec Configuration ................................. 5
Conclusion ......................................................... 10
Overview

Fortinet (NASDAQ: FTNT) is a global provider of high-performance network security and specialized security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape.

The Fortinet Security Fabric brings together all components in your network. It is Broad, Powerful and Automated. In addition to Fortinet products, the Security Fabric also integrates with 3rd Party partners to extend the power of the Security Fabric to other parts of an organization. For more information regarding our Security Fabric Partners, please refer to our Technology Alliances here: https://www.fortinet.com/partners/partnerships/alliancepartners.html

The leading provider of business-driven security management solutions, AlgoSec helps the world’s largest organizations align security with their business processes. With the AlgoSec Security Management Suite, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch – across their cloud, SDN and on-premise networks. Over 1,500 enterprises, including 20 of the Fortune 50, utilize AlgoSec’s solutions to make their organizations more agile, more secure and more compliant – all the time. Since its inception, AlgoSec has offered the industry’s only money-back guarantee.

Today’s business environment is characterized by continual changes, and business needs rapidly evolve across various organizational functions of companies. In this dynamic and rapidly changing business environment, IT often struggles to gain adequate visibility and control, to ensure security policies and regulatory guidelines are complied with. Effective security policy management that accommodates the dynamic nature of today’s organizations is a key challenge for many IT departments.

Fortinet and AlgoSec have partnered to deliver an industry-leading security solution to address these needs. Bringing together AlgoSec’s business-driven security policy automation with Fortinet’s industry-leading FortiGate® network security firewall platform enables customers to benefit from AlgoSec’s comprehensive security policy management capabilities, while simultaneously leveraging the best-validated security protection in the industry provided by Fortinet.

Architecture Overview

![Architecture Diagram]

FortiManager Configuration

Create and configure an administrator account for AlgoSec.

From System Settings go to Admin > Administrators > Create New.
Enter a User Name, New Password and Confirm the Password.

Set the Admin Profile to Super_User and click OK at the bottom.

The screen should look like the image below.

Enable the Web Service from the Network settings.
Remote Procedure Call (RPC) needs to be set to read-write when using FortiManager version 5.2.3 and above (see link to the Technical Note at the end for more details).

Connect to the FortiManager CLI to change the AlgoSec administrator account permissions. Enter the following CLI commands:

```
(FMG-VM64) # config system admin user
(USER)# edit algosec
(algosec)# set rpc-permit read-write
(algosec)# end
```

Configure FortiManager to send Syslog to the AlgoSec IP address. From System Settings go to Advanced > Syslog Server and click Create New.

Enter a Name. Enter the IP Address or FQDN of the AlgoSec server. Click OK.

**AlgoSec Security Management Suite Configuration**

Configure AlgoSec to monitor FortiManager. Go to Administration > Devices Setup.
Click New and select Devices.

For Device Type select Fortinet FortiManager and click Next.

For Access Information enter the FortiManager IP address, User Name and Password. Enable Active Change. Set the Syslog-ng server to Localhost and click Next.
Note: if you wish to use your own Syslog server click New and configure the following.

Under Baseline Configuration Compliance click Configure.

Enter the Host IP, User Name and Password. For Baseline Profile select Fortinet – FortiGate.
Click Test Connectivity.

Enter the Host IP, User Name and Password. For Baseline Profile select Fortinet – FortiGate.
Click Test Connectivity.
Click OK and OK. Your screen should look similar to the following. Click Finish.

Note: if you selected Set user permissions then the Edit Users dialog box appears. Set which users will have access to the reports produced by the device (see below).

When configuration is completed you will see the following screen.
Switch to the Devices page, and select ALL_FIREWALLS in the firewall tree on the left.

Then click ‘Analyze’ on the right pane to run a full risk, compliance and cleanup analysis on all the newly added Fortinet firewalls.
Conclusion

You are now ready to use the AlgoSec Security Management Solution with your Fortinet Firewalls. Refer to AlgoSec Firewall Analyzer, FireFlow and BusinessFlow user guides for more information on the various capabilities you can use.

FortiManager Administration Guide:
http://docs.fortinet.com/uploaded/files/3872/FortiManager-5.6.0-Administration-Guide.pdf

Technical Note on enabling RPC in FortiManager:

Solution Brief:
https://www.fortinet.com/content/dam/fortinet/assets/alliances/Fortinet-AlgoSec-Solution-Brief.pdf

For Manual Data Collection methods refer to the AlgoSec Firewall Analyzer Administration Guide.