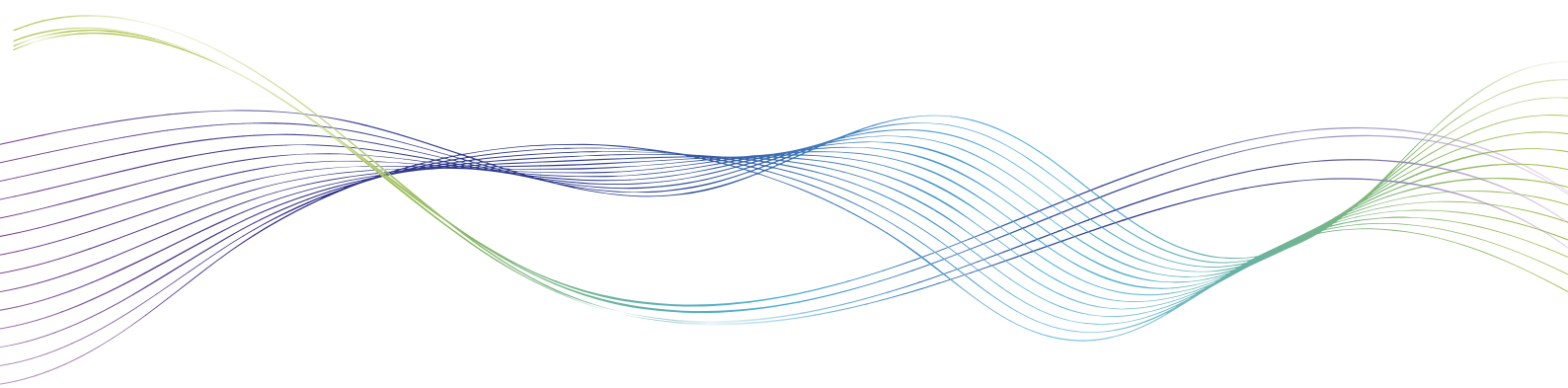
CISCO ACI & ALGOSEC

Holistic policy management for ACI and the hybrid network

An AlgoSec Whitepaper / Version 15 - 17.10.23

Table of contents



Abstract: AlgoSec and Cisco ACI integration

The solution described in this document provides an application-centric approach that delivers unified visibility across the entire network estate, on-premises and in the cloud, and utilizes intelligent automation to manage security changes, assess risk, and maintain compliance.

The integration of the AlgoSec solution with Cisco ACI enables Cisco customers to:

1. **Monitor security policy changes** across your Cisco ACI infrastructure.
2. **Get risk and compliance reports** for Cisco ACI configurations and network security devices connected to the ACI fabric.
3. **Extend Application-driven policy change automation across your entire hybrid cloud estate.**

Key features of the integrated solution

AlgoSec's solution supports Cisco ACI in the following ways:

Proactively assesses risk in Cisco ACI contracts and recommends the necessary changes to eliminate misconfigurations and compliance violations.

Provides data for each device, including detailed change history, current risk status, and device topology.

Provides a network topology map of the entire network, simulating traffic routes and security policies for ACI and other network and security devices.

Automatically generates audit-ready regulatory compliance reports for the entire ACI fabric.

Manages traffic change requests in a holistic manner, including:

1. Automatically pushing security policy changes to Cisco ACI, creating contracts and filters to enforce data center whitelist policies.
2. Identifying and provisioning changes to firewalls, both within the ACI fabric, as well as for other network security controls on-premises and in the cloud.

Introduction

Goals of this document

This document provides guidance on the integrated solution for AlgoSec Security Management Suite and Cisco ACI with aspects relating to customer value, architecture and design, and high-level setup. It describes key use-cases and options to automate and simplify data network security management in general, and Cisco ACI policy specifically.

Prerequisites

This document assumes that the reader is familiar with Cisco ACI and has a basic understanding of how service graphs work.

Terminology

This document uses the following terms and acronyms:

AFA
AlgoSec Firewall Analyzer

AFF
AlgoSec FireFlow

ASMS
AlgoSec Security Management Suite

BD
Bridge domain

EPG/ ESG
Endpoints

Problem statement

In today's fast-paced world, the growing demand to support a variety of applications across the data center and to ensure the compliance and security of these applications poses significant challenges to data center administrators. Managing network security policies across physical, virtual, and public cloud networks and multi-vendor security devices requires a delicate balance between reducing risk and provisioning connectivity for critical business applications to drive productivity.

With thousands of network security rules across many different security devices, numerous and frequent changes, and a lack of holistic visibility, managing security policies manually is nearly impossible today. It's too complex, too time-consuming, and it's riddled with errors – causing outages, security risks, and compliance violations.

Background

AlgoSec security policy management

AlgoSec's platform delivers a unified way to visualize and manage application connectivity and security policies across all public clouds, private clouds, containers, and on-premises networks. Its unique solution visualizes connectivity flows and security posture by collecting information across the network and associating security policy with specific applications.

Using its unique vendor-agnostic deep algorithm for change management automation, AlgoSec enforces application connectivity and security policy, thus preventing human errors, reducing exposure to security risk and expediting time-to-market.

Cisco Application Centric Infrastructure (ACI)

Cisco ACI, an industry-leading software-defined networking solution, facilitates application agility and data center automation. ACI enables scalable multi-cloud networks with a consistent policy model and provides the flexibility to move applications seamlessly to any location or any cloud while maintaining security and high availability.

AlgoSec Firewall Analyzer (AFA) - Network abstraction and policy analysis

AlgoSec Firewall Analyzer delivers visibility and analysis of complex network security policies across on-premises and cloud networks. It automates and simplifies security operations, such as understanding network path, auditing policy cleanup, risk and compliance analysis, and audit preparations. Using Firewall Analyzer, security and operations teams can optimize the configuration of firewalls, routers, web proxies, and related network infrastructure to ensure security and compliance.

Risk mitigation and compliance reporting

AFA automatically generates pre-populated, audit-ready compliance reports for leading industry regulations, including PCI DSS, HIPAA, SOX, GDPR, NERC, FISMA, and ISO, in addition to custom corporate policies. These reports provide a complete audit trail of all changes and approval processes, reducing audit preparation efforts and costs by as much as 80%. AFA can report on individual devices or aggregate groups of devices, including Cisco ACI contracts, into a single report (See figure 1 for example).

Gain visibility into heterogeneous networks

AFA automatically pulls policy information from a wide range of devices, including Cisco ACI. It analyzes tenants, contracts, and EPG /ESG values to understand network flows and their associated risks (See figure 2).

Figure 1: For example

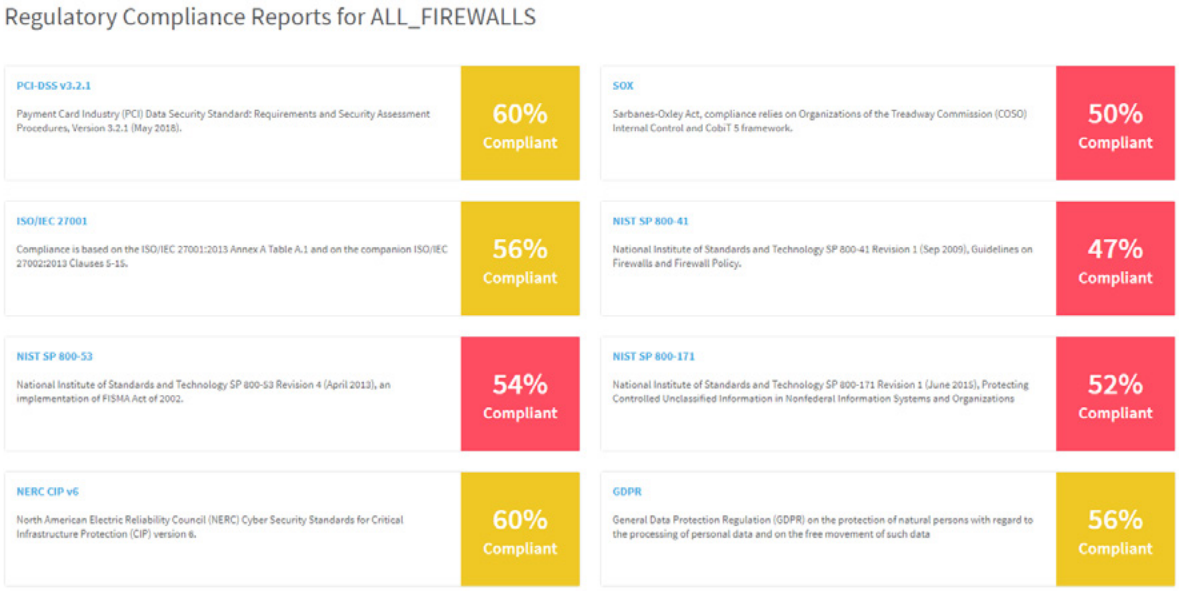
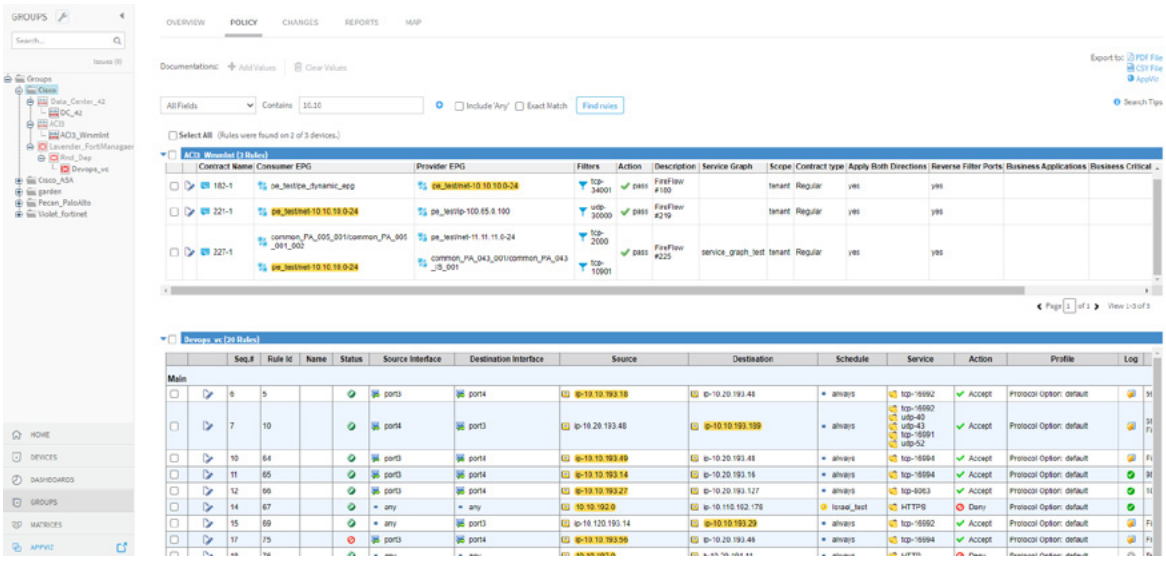


Figure 2: Policy search



Network map

AFA also supports Cisco ASA, Cisco Firepower, Cisco routers, and other firewalls in an interactive network topology map of the entire heterogeneous network. The network map is based on routing configuration analysis read from the many devices AlgoSec integrates with.

Use this map to understand the path of a specific flow in the network including network security elements in the path and their impact on network security policies.

This is used to troubleshoot policy configuration issues across a complex network path, plan changes and view detailed change histories, see current risk status, and perform "what-if" traffic queries (See figure 3).

Contract scopes

ASMS supports the following scopes of contracts: Tenant, VRF, Application Profile and Global. The AlgoSec default scope is Tenant.

ASMS also supports connectivity between EPGs defined by Contract Preferred Groups (CPGs). For every VRF that has the Preferred Group option enabled, an artificial rule is constructed (See figure 4).

As far as ACI is involved, AlgoSec refers to the overlay network. AlgoSec presents VRFs as network elements. Bridge domains and L3Out elements are considered interfaces with their respective routing policy.

Figure 3: Network map

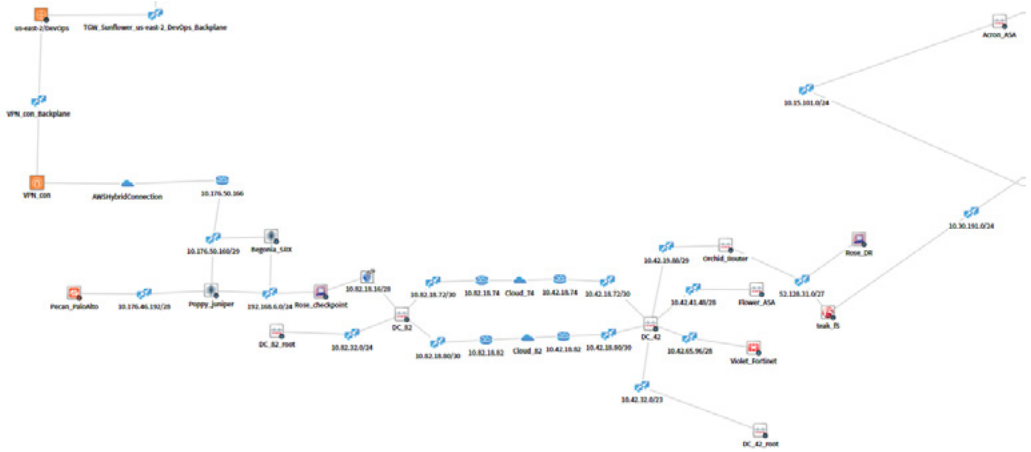


Figure 4:

Source (Consumer EPGs)	Destination (Provider EPGs)	Services (Filters)	Rule number
All EPGs of the VRF (regular and external) that have "prefGrMemb" attribute equal to "include"	All EPGs of the VRF (regular and external) that have "prefGrMemb" attribute equal to "include"	Any	Last*

* Generated CPG rules are placed at the end of the relevant section in parsed_config.json (after vzAny rules) in alphabetical order (of VRF name).

AlgoSec FireFlow (AFF) - Security policy change automation

AlgoSec FireFlow helps you process security policy changes in a fraction of the time, enabling you to respond to business requirements with the agility they demand. FireFlow automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation, and auditing, including automated provisioning on multi-vendor firewalls, routers, cloud security groups, and Cisco ACI.

A traffic change request workflow includes multiple phases, each described below. The workflow can be customized to include a manual approval or an automatic, zero-touch implementation. Complex conditional workflows can also be customized. We recommend consulting with AlgoSec professional services for more information about custom workflows.

Initial plan: Design change requests intelligently

AlgoSec's Traffic Simulation engine works across on-premises and cloud security controls to automatically analyze change requests and discover all devices and rules that need to be changed. Unnecessary changes for traffic that already works are instantly identified and closed and requestors are notified. This helps to prevent up to 30% of change requests from being processed unnecessarily.

In this stage, AlgoSec FireFlow can also provision devices used in ACI service graph redirect policies if they are relevant for the contract. For details, see Service Graph redirects.

Risk check: Analyze change requests to ensure compliance and mitigate risk

FireFlow automatically analyzes every proposed change – before it is implemented – to ensure compliance with regulatory and corporate standards and identify any changes in risk levels. This proactive Risk Check can be tailored to suit individual customer-specific compliance and enterprise security standards.

Rule design and provisioning: Save time and avoid manual errors

FireFlow automatically designs the technical implementation steps for all requests, ensuring that they are designed in the most efficient method possible and avoiding future policy cleanup efforts and optimization challenges. AlgoSec's ActiveChange technology can then automatically implement recommended policy changes directly on the device or firewall management platform, saving time and preventing human error.

Automated peer review (SmartValidation)

After ActiveChange pushes changes to devices, SmartValidation automates the peer-review process. This peer-review ensures that the Network Analyst who is responsible for the request implementation can be confident that the request was implemented accurately. SmartValidation is critical in preventing tickets from being closed prematurely.

Prevent unauthorized changes (Auto-matching)

FireFlow's unique Auto-Matching capability correlates change requests with actual policy changes that are detected on devices across the estate, detecting unauthorized and out-of-band changes, and ensuring that changes are implemented exactly as they were requested and approved.

AlgoSec AppViz - Application discovery and connectivity management

AlgoSec AppViz makes it easy to discover, provision, and maintain network connectivity for your critical business applications. By automatically discovering and mapping application connectivity requirements to the underlying network infrastructure, AppViz accelerates business application delivery, minimizes outages, and enforces security and compliance across virtual, cloud, and physical networks.

AppViz bridges the gap between application owners and network/security operators by providing application owners with an easy-to-use GUI for defining applications' abstract connectivity requirements without needing to refer to the underlying network elements.

AlgoSec AppViz extends the application-centric approach of Cisco ACI to the entire hybrid network. Integrating AppViz with AFF enables application owners to translate traffic flow "intent" to network-wide security policy changes, which are implemented on various network devices in path.

Application owners can use the AppViz GUI to create a database of application flows, which are imported from various repositories, such as CMDB, or are discovered directly from the network. An example of such discovery – especially useful for greenfield or migration use-cases – is the integration of Cisco Secure Workload with AlgoSec AppViz. For details, see Integration with Cisco Secure Workload Analytics.

Integrated solution overview

AlgoSec Security Management Suite for ACI is delivered via a software license, and hardware appliances can be provided, if needed. ASMS supports enterprise-scale deployments and uses APIC northbound REST APIs to learn APIC policy configuration, and automatically push changes to it.

In addition to Cisco ACI and Cisco network security devices, AlgoSec integrates with all leading brands of traditional and next-generation firewalls and cloud security controls (such as AWS security groups and Network Access Lists), as well as routers and load balancers, to deliver a unified security policy management across your enterprise hybrid network (See figure 6).

AlgoSec connects to the network security elements listed above, either through REST API when available, or sometimes through SSH/CLI.

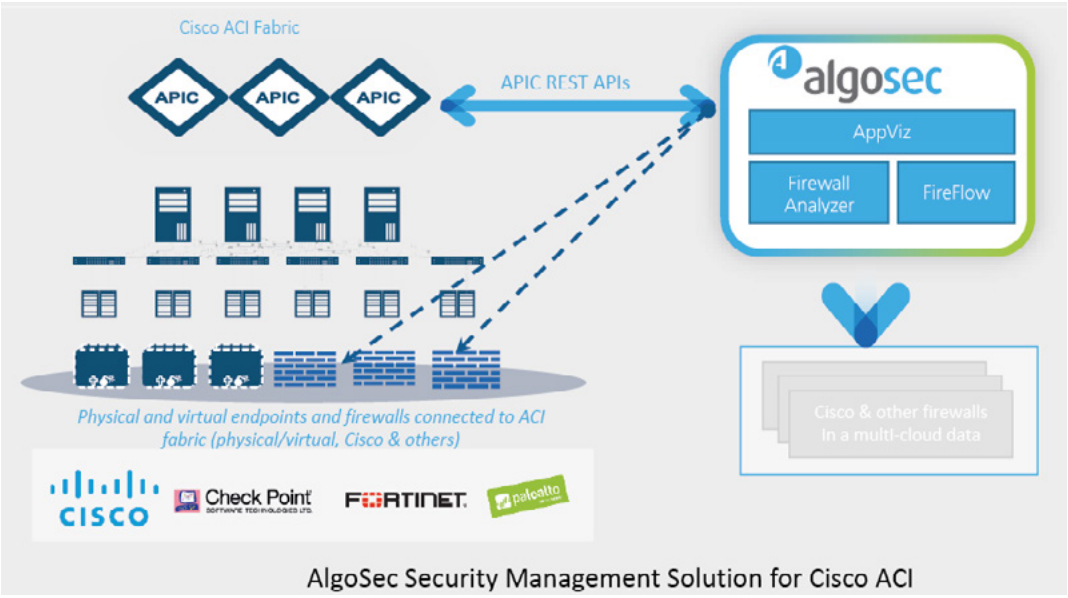
In cases where a vendor has a management system, that system usually takes precedence. Such examples include FMC (for Cisco Firepower), Panorama (for Palo Alto), Provider 1 (for Checkpoint), and FortiManager (for FortiGate gateways).

AlgoSec uses routing tables, tunnels, NAT definitions, and more[1] to create an integrated network model that is as accurate as possible to consider flows that are external to the ACI fabric and cross network domains. AlgoSec can read and write access lists and security policies to analyze risks, perform traffic simulation queries, and automate changes.

AlgoSec also integrates with a variety of enterprise IT tools to align with the organization's work processes. AlgoSec integrations span a variety of areas, such as ITSM tools for change request processes, identity managers, and communication tools like Skype for Business, which integrates with AlgoSec's chatbot AlgoBot (See figure 7 on the next page).

For the full list of supported devices, see Supported Devices & Solutions.

Figure 6:



AlgoSec Security Management Solution for Cisco ACI

[1] Each vendor may have multiple features related to routing. For details about the features supported for each vendor, see AlgoSec documentation.

Deploying AlgoSec

ASMS deployment options include using AlgoSec's pre-installed hardware, VM appliances, or cloud instances. In these cases, customers can get started right away without manually installing ASMS.

Alternately, you can install ASMS on your own Linux servers (RedHat Linux and CentOS Linux versions 6.10).

For more details, see Advanced AlgoSec Deployment Modes and the ASMS Installation and Setup Guide.

Once deployed, access ASMS via your browser to add devices to your environment and analyze reports, as well as manage workflows, change requests, and business flows. ASMS feature availability is dependent on your license type and scope (See figure 8).

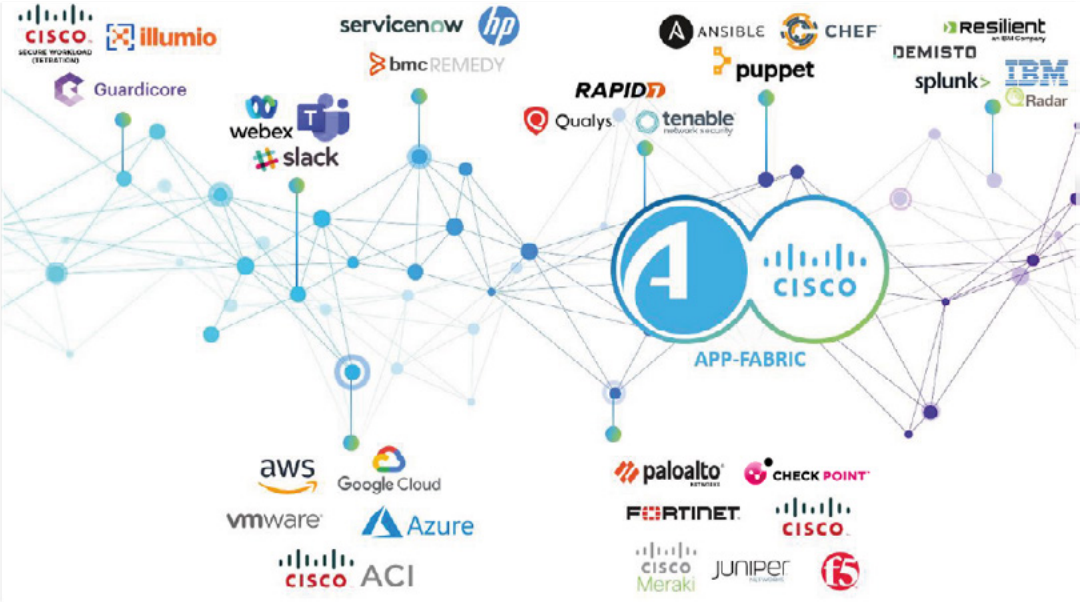


Figure 7: AlgoSec 3rd party integration

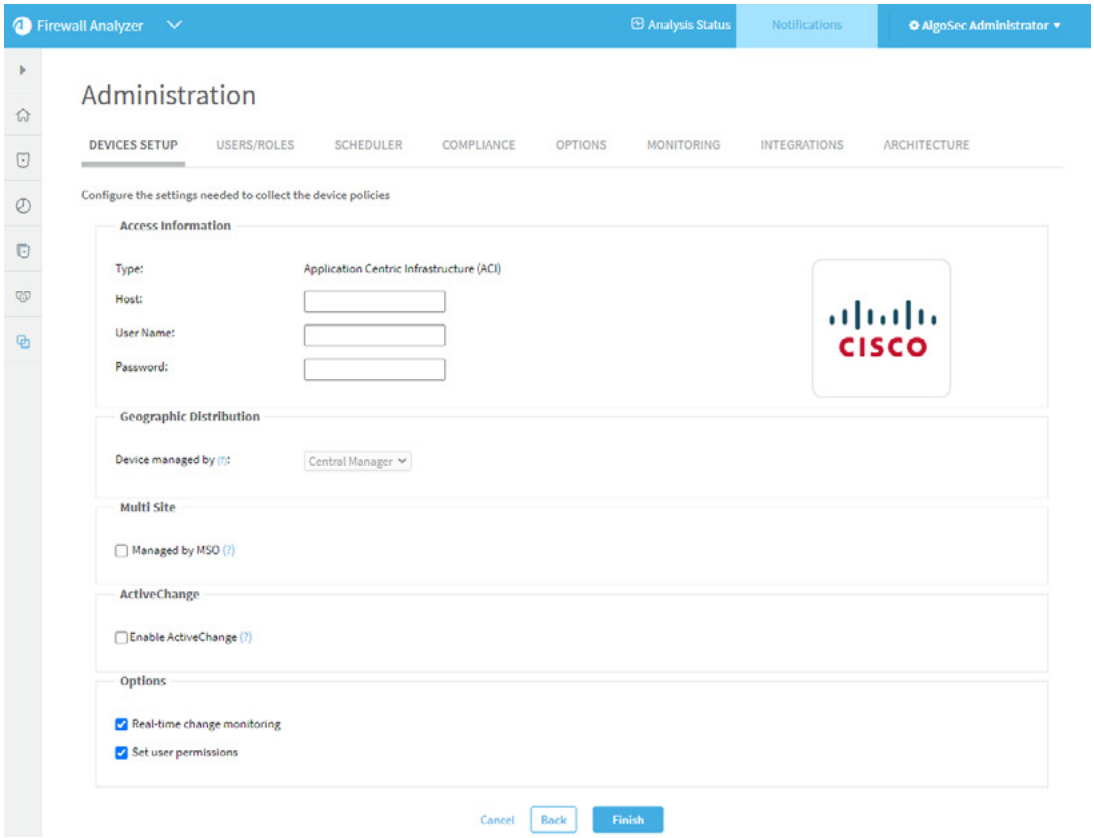


Figure 8: AFA GUI for adding a new Cisco ACI device

Change automation – Deep dive

The following image shows the major intelligent automation steps in the FireFlow workflow:

Request a network change | Identify devices in the flow path | Check for risk involved | Plan the rules | Implement the change on the devices | Validate the change

FireFlow organizes these steps as follows:

- Initial plan, where you request a network change and FireFlow identifies the relevant devices
- Risk check, where FireFlow checks for risks involved
- Rule planning, where the actual work order is planned and approved
- Smart validation, where FireFlow's Auto-Matching feature verifies that the change made matches the request.

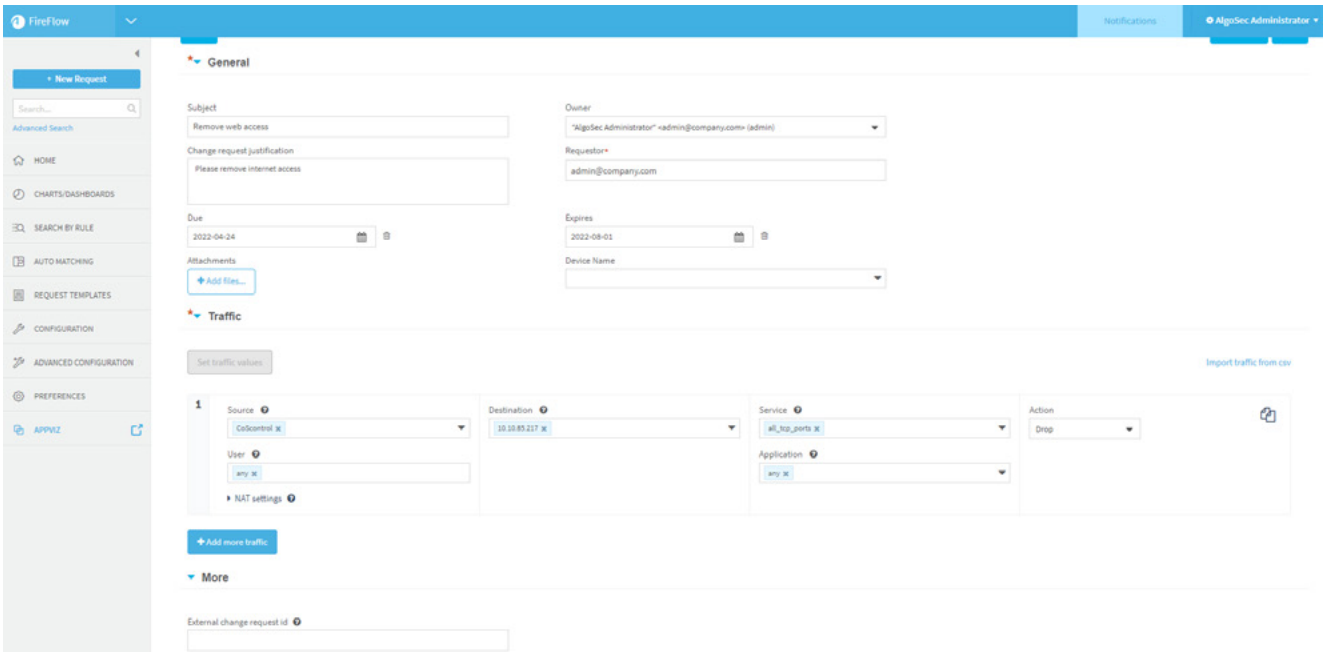
AlgoSec's unique ActiveChange technology complements FireFlow's workflow, with automated change implementation across a wide range of devices.

**FireFlow change automation flow

Step 1: Request a network change

A FireFlow traffic workflow change request can be initiated from the FireFlow or AppViz UI, or using an API, often integrated with a ticketing system like Service Now (See figure 9).

Figure 9: AFF GUI for multi-approval request template



Each change request enables you to provide traffic flow details as well as request meta-data, such as the fields listed in the following table (See figure 10). For more details, see the AlgoSec FireFlow Requestor's Guide.

Figure 10: Change request fields

Field name	Description
Subject	Subject of the change request
Owner	An initial owner of the change request, if relevant
Change request justification	Describes the need behind the new change request
Requestor	Your email address
Due / Expires	A date by which the change request must be completed, as well as a date by which, if uncompleted, the request expires
Attachments	Enables you to add supporting data or the request as initially provided by the request initiator, such as design documents
Device Name	Relevant for requests for specific devices. If left blank, the system calculates this automatically
Source / Destination	The traffic source and destination, including an IP address, subnet, range, or EPG/ESG name
Service	The traffic service
Action	Indicates whether the request is related to allowing or blocking connections, either **Allow** or **Drop**[2].
External change request ID	The ID number of the same request opened in a different external system that integrates with FireFlow.

Step 2: Identify devices in the flow path (initial plan)

FireFlow uses the network map modeling to identify the devices in the requests traffic path. You must onboard devices in AFA before performing this step.

If FireFlow identifies that either the source or destination are in the ACI fabric, in one of the identified bridge domains, the appropriate ACI tenant is added to the initial plan results. Additional network devices, such as next-generation firewalls, routers, and more, may also be added.

Note: in the case of overlapping IP addresses between ACI tenants; AFF can be customized with conditional logic for tenant selection[3], or alternatively user can select manually the relevant tenant.

At this point, FireFlow also updates the devices list in the initial plan with any network devices that are included in a service graph redirect associated with that flow (See figure 11 on the next page). For more details, see Service Graph Redirects.

[2] Drop action is not supported on all device types, and specifically on ACI at this time. Expected as roadmap item.

[3] AFF customization is recommended to be done by AlgoSec PS or personnel certified to perform such customizations.

To explore the traffic path and the reasons for the recommended changes, AlgoSec displays a subset of the network map with traffic simulation results and mark the devices that permits, blocks or partially allow the requested traffic.

Figure 11:
FireFlow initial plan

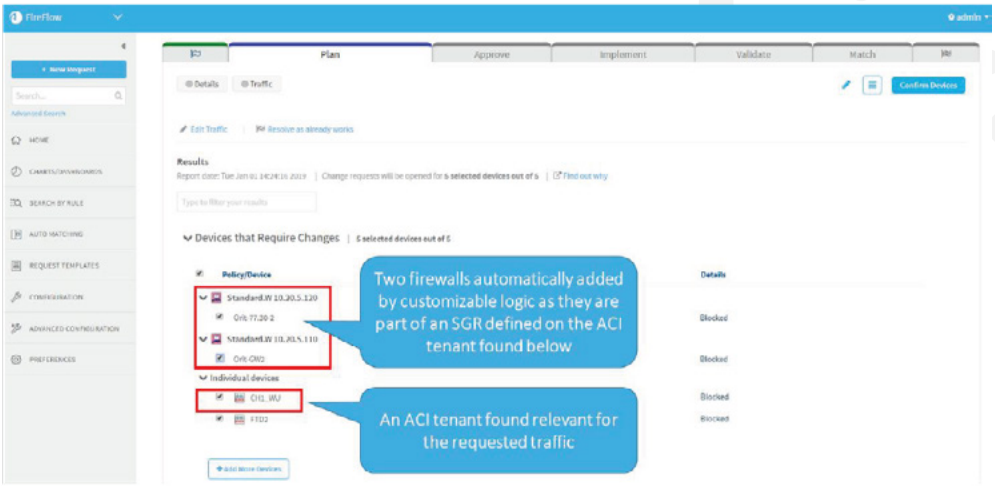
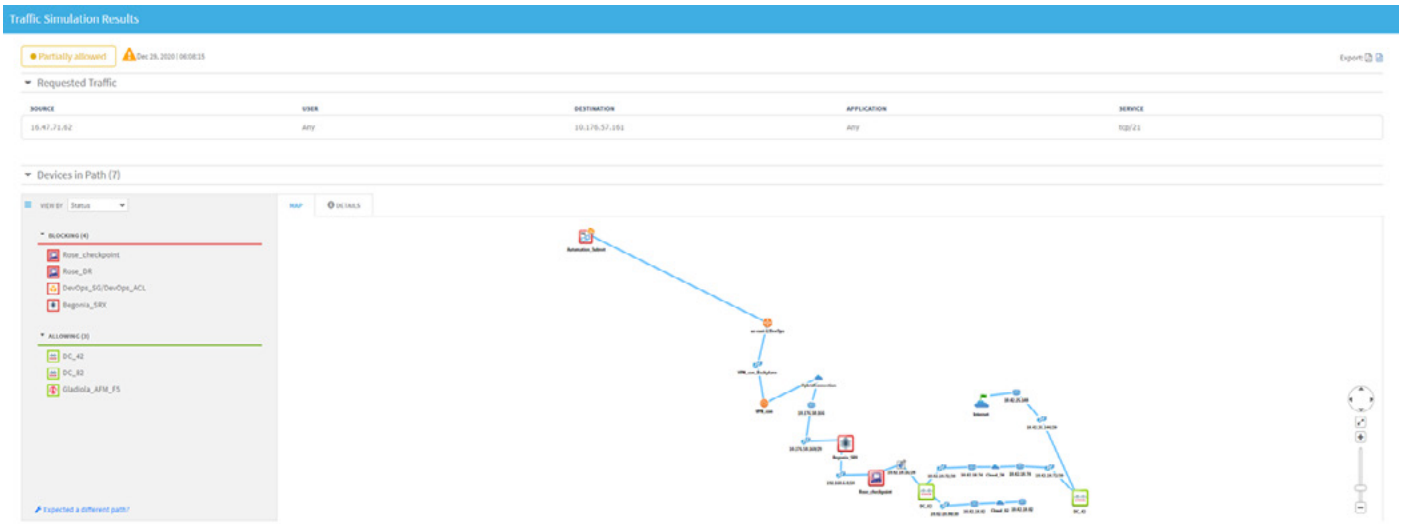


Figure 12: Traffic simulation results



Step 3: Check for risks

At this phase of the workflow, FireFlow provides an indication of risks associated with the flow (See figure 13 for example).

Users can look carefully through the risks listed, and then define whether the request is approved, denied, or must be revised. Customized logic can be applied to automatically approve the request based on the risk level identified.

For more details, see Risk Profiles.

Figure 13: Risks flagged during a change automation process

Risk Check Result

Recalculate

Risk profile: Perimeter.xml
Based on device: ACI3_WmmInt
Risk Check Result is from: Tue Apr 26 11:23:05 2022.

Risks Found: 1 medium risk.

		Code	Risk Description
1.	!	R08	"Allow Any service" rules (×1)

Step 4: Rule planning (work order)

In this stage, FireFlow calculates the network security rule that needs to be created or modified for each device[4]. Rule structure and logic may be different per device type and are device specific (See figure 14 and 15 for example).

When working with ACI, new contracts include the following:

- Consumer EPG/ESG
- Provider EPG/ESG
- Service Graph
- Filter, based on the requested "service" value in the change request

For more details, see EPG Selection or Creation Logic and Service Graph Redirects.

Figure 14:
Change request that results in new filter creation as well as new contract creation

During the work order stage, users can also modify the calculated fields.

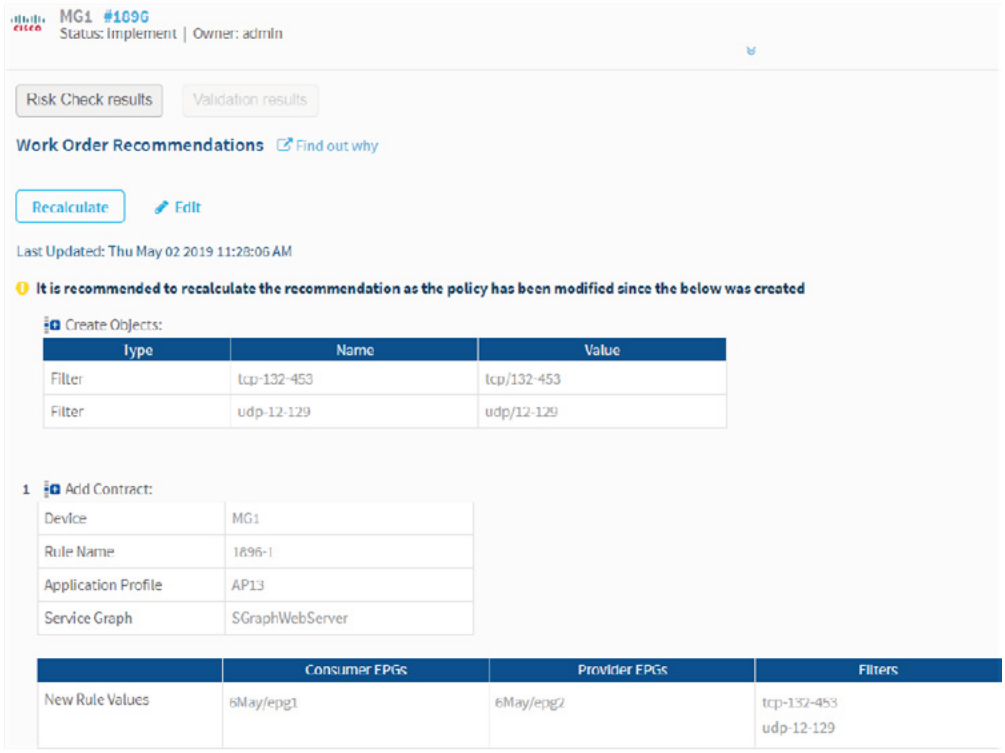


Figure 15:

[4] Rule modification is not supported for ACI at this time. Expected as roadmap item.

Analyzing existing EPGs/ESGs

During analysis, AFA reads all configuration data from ACI and saves EPG values according to the following logic:

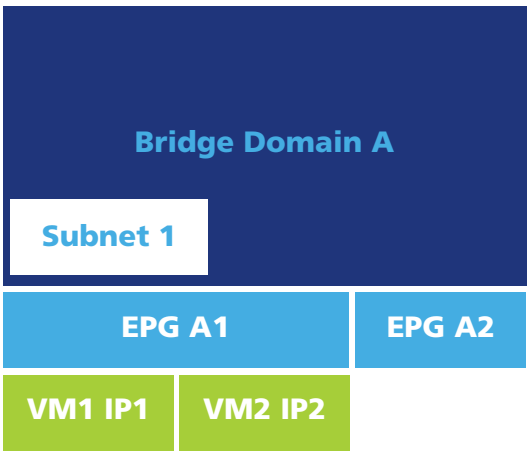
- If an EPG is associated to specific VMs, their IP addresses are saved as the EPG value.
- Otherwise, AFA reads the subnets defined for the EPG and subnets of the associated Bridge Domain (BD) and considers these subnets for the EPG(s).

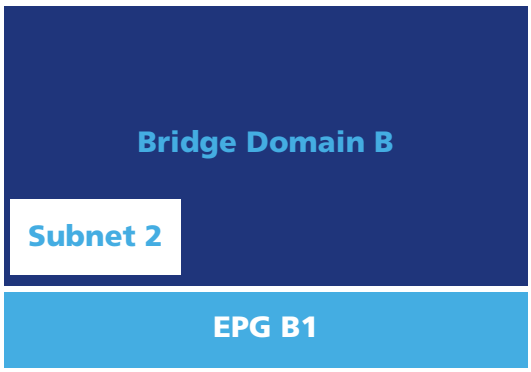
EPG/ESG selection or creation Logic

While creating Cisco contracts, ASMS handles EPGs in provider or consumer fields as follows:

- Analyzing Existing EPGs
- Assigning EPG to a new contract

Figure 16: example EPG analysis





EPG	Value
A1	IP1, IP2, Subnet1
A2	Subnet 1
B1	Subnet 2

Assigning an EPG to a new contract

Requests can be generated from FireFlow, AppViz, or the FireFlow API, and the behavior described below is the same for all cases. For the sake of simplicity, the steps below describe the process as performed from the FireFlow GUI.

Users can submit change requests using the following data as source or destination values:

Existing EPG name	Change requests can be submitted with an existing EPG as the source or destination value using dropdown options in the FireFlow UI. FireFlow uses the selected EPG in the contract provisioning.
IP or subnet address	Change requests can be submitted with an IP or subnet address as the source or destination. In such cases, the following occurs: • Matching EPG. If FireFlow finds an existing EPG that matches this defined address exactly, this EPG is selected. FireFlow can also identify an EPG that is a superset of the defined address (contains the defined address) and assign that to the contract instead. This is known as automatic wider selection. • No matching EPG. If no EPG is found, FireFlow Recommends creating a new EPG and attaches it to the relevant BD. In such cases, a new BD is not created, and the user can either keep the default EPG name or assign a custom name.

Note: In all cases, users can edit the work order to select a different EPG, equal to or wider than the submitted source or destination. This is especially relevant when you are working with multiple EPGs that have the same content.

Step 5: Implement change on the device

During this stage, the change designed in the previous stages is implemented on the device. FireFlow can push the change using existing APIs, including REST APIs for Cisco ACI and most modern devices, or SSH for other devices.

Any EPGs created by ActiveChange are empty.

After implementing the FireFlow work order, users must configure any newly created EGPs in the APIC to allow the required traffic.

EPG configuration may include VMM domains, VLAN to EPG mapping, or other supported mapping mechanisms (See figure 17 for example).

Step 6: Validation

To validate that the changes were implemented as requested, FireFlow relies on the latest configuration read from the device. FireFlow also alerts users if any new rules are wider than originally requested. Monitoring cycles are performed every 5 minutes.

ACI rule (contract) removal workflow

ASMS enables a privileged user to submit a request to remove one or more ACI contracts, which initiates the FireFlow change request lifecycle. When removing a contract, ASMS deletes the contract and all relations (consuming or providing) of this contract from EPGs that were using it. ASMS does not delete the EPG when removing a contract.

Supported ACI constructs

ASMS reads various ACI constructs including tenants, EPGs, Bridge domains, subnets, VRF's and more. For a full list see Appendix: ACI constructs read by AlgoSec.

Risk profiles

Risks are identified based on preconfigured risk profiles in AFA, which enable security analysts to define network segmentation. For more details, see the AlgoSec Firewall Analyzer Administration Guide (See figure 18 for example).

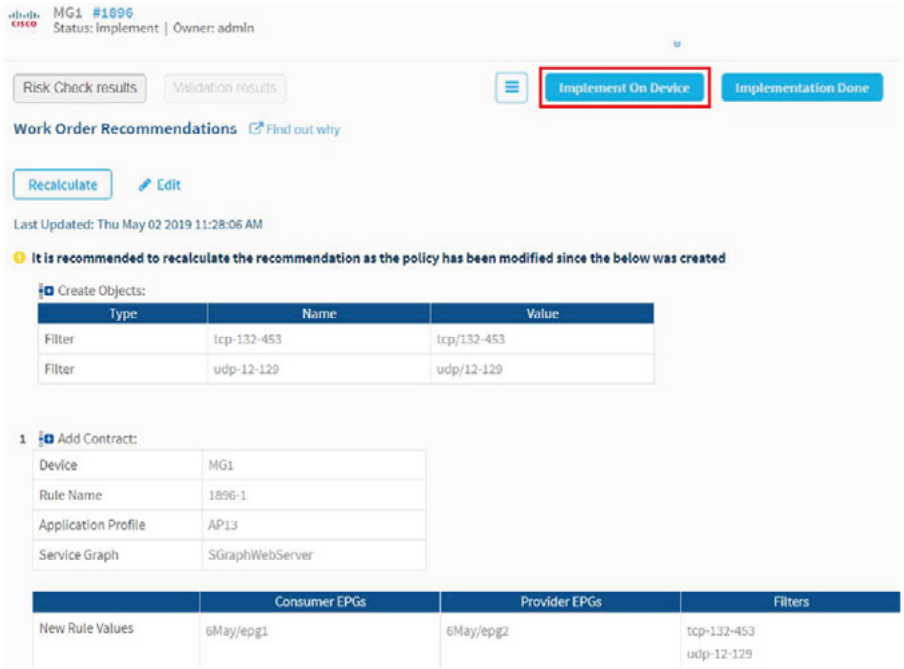


Figure 17: Implement changes from FireFlow

Figure 18: Sample pre-configured risk profile

To / From	Net1	Net2	Net3	PartnerNet	PCIzone;S	Other
Net1	-	not(forbiddenSvc)	SecureSrvs ; C2	Any	SecureSrvs	Any
Net2	Any	-	Any	Any	SecureSrvs	Any
Net3	OnlySrvX	not(OnlySrvX)	-	Any	SecureSrvs	Any
PartnerNet	PartnerSrv	PartnerSrv ; C1	PartnerSrv ; C1	Any	SecureSrvs	Any
PCIzone;S	SecureSrvs	SecureSrvs	SecureSrvs ; C2	SecureSrvs ; C3	-	None;H
Other	-	-	http_Services	-	None;H	Any

Service graph

One of the useful features in Cisco ACI is the ability to define a service graph redirect that results in traffic flows being routed to additional network elements for security, such as next-generation firewalls, and other purposes.

A common deployment of connecting the next-generation firewall is with a single interface (AKA one-armed mode); this configuration is now supported by AlgoSec for the following brands: Cisco Firepower, Check Point, Palo Alto and Fortinet Firewall (other brands may work but were not certified). (See figure 19).

Note: Service graph support is provided since version A30.0 as a highly customizable feature. Until version A32.50, it required significant configuration to achieve its designed goal.

In A32.50, AFA enhancements to Service Graph support for Cisco ACI devices include automated collection of service graph data and identification and presentation of additional paths from service graph. Configuration is now automatic.

The AlgoSec automation process enables the following:

- Provisioning next-generation firewalls included in the contract's service graph
- Provisioning the service graph field in the contract when creating a new contract

AlgoSec's core capability is in provisioning new traffic in existing devices and provides unique functionality for identifying the relevant devices for the flow.

Provisioning logic

This following describes the logic for provisioning firewalls included in the contract's service graph:

- Prerequisite 1: Match a service graph name to network devices
- Prerequisite 2: Logic for matching service graph to requested traffic flow

This process is performed as part of FireFlow's Initial Plan phase. For details, see Step 2: Identify devices in the flow path (initial plan).

Prerequisite 1: Match a service graph name to network devices (done automatically in A32.50 and above):

Before ASMS can identify service graph redirects, administrators must define any security devices included in those service graphs. This is done using an auxiliary configuration file with the following format:

Tenant Name	Service Graph Redirect Name	Devices
Jasmine_ACI	SG_HTTP_S	CKP1, F51
Jasmine_ACI	SG_HTTP3	PAN1
Flower_ACI	SG_eCommerce	PAN1, PAN2
Begal_ACI	SG_2	FP1, F52
Begal_ACI	SG_SQL	FP1, F52

In this file, the device names must exactly match the names used to identify the devices in ASMS. These are the device names that are shown in the AFA device tree. For more details, see the AlgoSec Firewall Analyzer Administrator Guide.

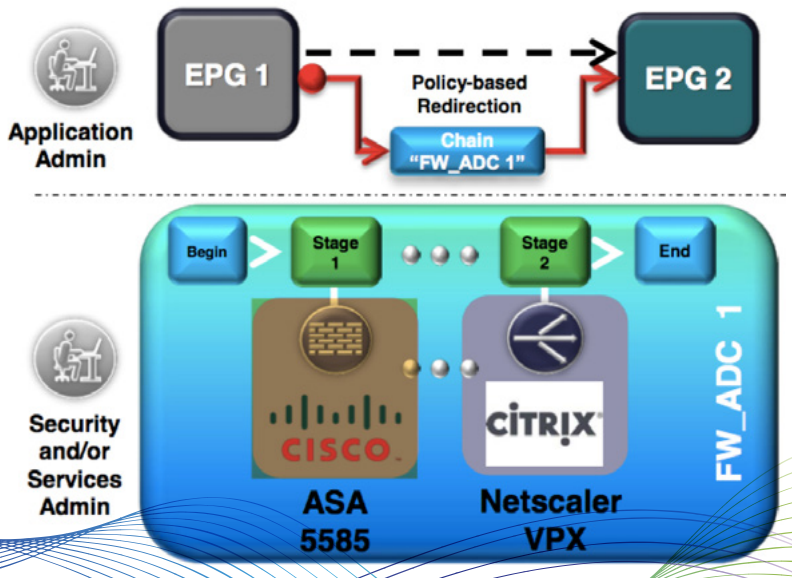


Figure 19:
Cisco ACI service graphs

Prerequisite 2: Logic for matching service graph to requested traffic flow (done automatically in A32.50 and above)

Administrators must also define the network logic used to define the service graph redirect. This can be done using system-default logic, or custom logic:

- **System-default logic:** Enables the system to resolve a service graph redirect based on straightforward rules for source and destination ranges for a specific traffic flow. This is provisioned, for example, as follows:

Source	Destination	Tenant Name	Service Graph Redirect Name
10.1.0.0-10.1.0.255.255	10.2.1.6	Jasmine_ACI	SG_HTTP_S
10.1.0.0-10.1.0.255.255	10.2.1.6	Jasmine_ACI	SG_HTTP_S
10.1.1.3	10.2.1.6	Jasmine_ACI	SG_HTTP3
10.5.7.3-10.5.7.8	10.9.1.5	Flower_ACI	SG_eCommerce
192.1.1.3	192.2.1.6	Begal_ACI	SG_2
0.0.0.0-255.255.255.255	10.3.1.1	Begal_ACI	SG_SQL

- **Custom logic:** Enables the system to resolve service graph redirects based on any custom logic, using the available values in the change request parameters. For details, see Table 1: Change request fields.

Note: This method uses a FireFlow hook. We recommend consulting with AlgoSec professional services to create custom logic hooks.

Sizing and capacity planning

AlgoSec system sizing is based on the number and the complexity of the devices monitored and analyzed by the system. Storage requirements are also impacted by the retention policy, including resolution and retention period.

ASMS can be scaled by adding replica units to assist with the complex analysis and monitoring tasks, and NAS may be added to scale storage.

Detailed sizing data can be calculated with the ASMS Sizing Guide. For more details, see the ASMS Installation and Setup Guide.

Advanced AlgoSec deployment modes

AlgoSec provides flexibility to deploy the AlgoSec Security Management Suite in HA and/or DR configurations. In High-Availability (HA), AlgoSec appliances can be clustered for fault tolerance, ensuring availability if system components fail. In Disaster Recovery (DR) AlgoSec appliances can automatically synchronize data with offsite appliances to provide redundancy and ensure data preservation in the event of a failure at the primary site. AlgoSec can also deploy a flexible architecture that provides both HA and DR. AlgoSec provides enterprise-grade distributed architectures to support both single locations and geographically distributed environments:

- **Load distribution** architectures are comprised of a primary appliance and one or more replica appliances, all in one geographical location. Replica appliances provide additional processing power to manage the analysis of large numbers of devices.
- **Geographical distribution** architectures are comprised of a central manager appliance, which collects data from remote agent appliances at other locations. Remote agents collect data from and deliver data to devices in their own geographic locations.

Multi-site ACI

AlgoSec does not integrate directly with the ACI multi-site orchestration (MSO)*, and can partially support multi-site deployments as follows (See figure 20):

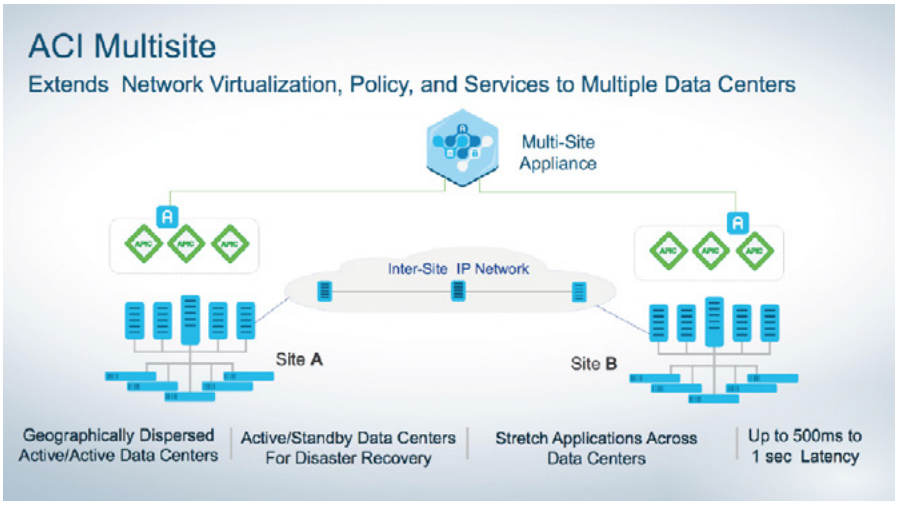
- Administrators must set up each APIC cluster individually in ASMS.
- ASMS can read policies by connecting to each APIC cluster individually.
- ASMS can write policies locally to any APIC cluster managed by an MSO for tenants managed locally. Their policies will not be visible in the MSO.
- Creating multi-site contracts in AFF via Active Change is an Early Availability feature.
- **Note: In case you are using an MSO, it is recommended to consult with an AlgoSec ACI expert on design considerations.**

Integration with Cisco Secure Workload

Through seamless integration, AlgoSec extends Cisco Secure Workload's application segmentation capabilities to all network security devices across the enterprise network – physical or virtual, on-premises or in the cloud. Additionally, AlgoSec complements Cisco Secure Workload by extending its application connectivity visualization to the underlying network security infrastructure, providing the network and security teams with business context for their firewall rules and policies, as well as for security risks and vulnerabilities.

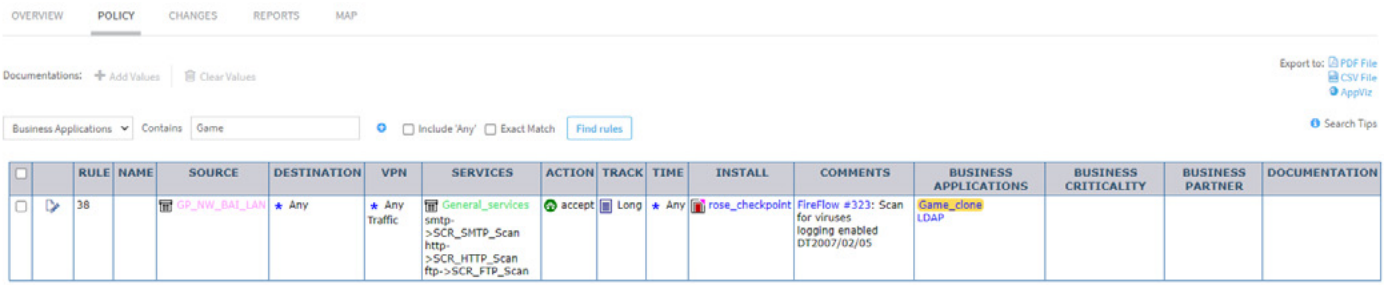
*Network Dashboard orchestrator (NDO) support is scheduled for Q1 2024

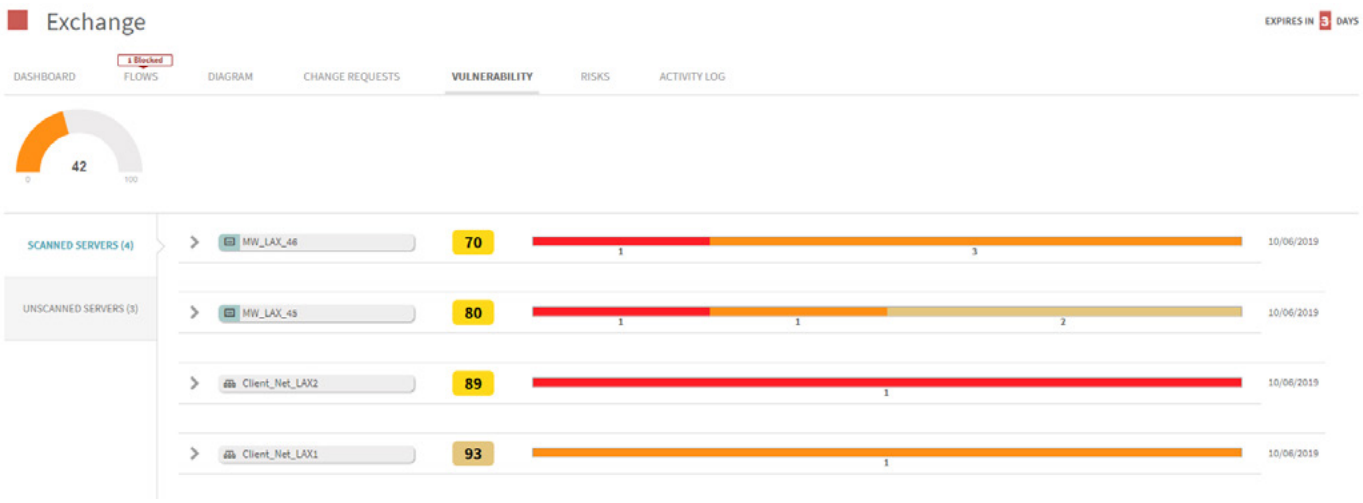
Figure 20:



Key features of the integrated solution:

- Automatically discovers business application connectivity, dependencies, and behavior.
- Automatically generates whitelist policies based on actual application behavior and pushes the policies to the relevant network security devices.
- Ensures consistent end-to-end implementation of micro-segmentation policy across both endpoint and network enforcement points, continuously.
- Reports on all network security risks and vulnerabilities impacting each application.
- Allows users to easily search through all security rules across in the entire network, and filter by business applications.
- Monitors critical application connectivity status and verifies that supporting network security policies are intact.
- Automatically tags security policy rules across multiple security devices, platforms, and technologies, with the business applications they support.





Additional details

AlgoSec licenses

This section describes the license types supported by AlgoSec. You can choose a software license type, a support level, and a support duration period (See figure 22).

1. **AlgoSec Firewall Analyzer (AFA) and AlgoSec FireFlow (AFF)** are licensed according to the number of firewalls and spine/leaf switches. AFF includes two types of licenses:

- **AFF** Prepares and recommends changes for firewall policies for ACI contracts, with or without approvals, as per each customer's configuration.
- **AFF + Active Change** Prepares, recommends, and automatically enforces security policy changes and ACI contract changes, with or without approvals, as per each customer's configuration.

2. **AlgoSec AppViz** is licensed according to the number of applications in use.

The following tables list features included in each software license package and bundle type:

- Visibility features by license type
- Compliance features by license type
- Policy automation features by license type
- Application-connectivity-based intent

Table 1: Visibility features by license type

	AFA	AFF	AFF+ Active-Change	AFA + AFF	AFA+AFF+ Active-Change	AppViz
Clean up and optimize firewall rulesets	✓			✓	✓	
Discover and mitigate risky firewall rules	✓			✓	✓	
Unify security policy management across on-premises and cloud environments	✓	✓	✓	✓	✓	✓
Monitor and audit all security policy changes	✓			✓	✓	
Visualize application connectivity						✓

Table 2: Compliance features by license type

	AFA	AFF	AFF+ Active-Change	AFA + AFF	AFA+AFF+ Active-Change	AppViz
Track and audit the entire change lifecycle		✓	✓	✓	✓	
Proactively analyze change requests to ensure compliance and mitigate risk		✓	✓	✓	✓	
Mitigate risk with baseline configuration compliance	✓			✓	✓	
Continuous regulatory compliance preparation	✓			✓	✓	

Table 3: Policy automation features by license type

	AFA	AFF	AFF+ Active-Change	AFA + AFF	AFA+AFF+ Active-Change	AppViz
Automate the security policy change workflow		✓	✓	✓	✓	
Design change requests intelligently		✓	✓	✓	✓	
Save time and avoid manual errors with automatic policy push		✓	✓		✓	
Prevent unauthorized changes		✓	✓	✓	✓	
Integrate with existing IT service management (ITSM) solutions		✓	✓	✓	✓	

Table 4: Application-connectivity-based intent

	AFA	AFF	AFF+ Active-Change	AFA + AFF	AFA+AFF+ Active-Change	AppViz
Automatically translate connectivity requirements into firewall rules						✓
Discover and map underlying rules and access control lists (ACLs) to applications						✓
Assess the impact of network changes on application availability						✓
Simplify large-scale server migration projects						✓
Ensure secure decommissioning of applications						✓

Platform integration support & compatibility

The following table lists supported ACI versions and firewall devices for each ASMS component.

AlgoSec component	Product version	ACI supported version	Supported Firewall devices
AlgoSec Firewall Analyzer (AFA)	v6.11 and higher	v2.2,v3.2, V4.0 and V5.0	Cisco ASA, FTD, Palo Alto Networks, Fortinet, Check Point Firewalls as well as native cloud security devices. For more details, see Supported Devices & Solutions.
AlgoSec FireFlow (AFF)			
AlgoSec AppViz			
ActiveChange (for AFF)	v2018.1 and higher		

Appendix: ACI constructs read by ASMS

This section lists the ACI constructs read by ASMS as follows:

ACI constructs understood by ASMS

Object class	Parent class	Description
aaaUser	-	A locally authenticated user account
aaaLogin	-	Response from APIC REST API for aaaLogin request
fvAEPg	fvAp	Application EPG (End Point Group)
fvAp	fvTenant	Application Profile
fvCtx	fvTenant	VRF
fvBd	fvTenant	Bridge Domain
fvCEp	fvAEPg	A client endpoint attaching to the EPG
FvESg		EndPoint Security Group objects
FvEPSelector		Endpoint Security Group Selector, to decide which endpoints belong to the ESG based on selector matching
fvIp	fvCEp	The IP address of an endpoint
fvStCEp	fvAEPg	The static endpoint represents a silent client attached to the fabric which will not produce traffic of its own
fvStIp	fvStCEp	The static client endpoint IP address
fvVip	fvAEPg	Virtual IP address
fvnsUcastAddrBlk	vnsAddrInst	The first and last unicast IP addresses in the namespace block
vnsAddrInst	fvAEPg	The IP address namespace/IP address range
fvSubnet	fvBd	A subnet defines the IP address range that can be used within the bridge domain
fvTenant	-	Tenant
l2extInstP	l2extOut	The external network instance profile represents a group of external subnets that have the same security behavior
l2extOut	fvTenant	The L2 outside policy controls connectivity to the outside
l3extInstP	l3extOut	The external network instance profile represents a group of external subnets that have the same security behavior

Object class	Parent class	Description
l3extOut	fvTenant	The L3 outside policy controls connectivity to the outside
l3extSubnet	l3extInstP	The network visibility of the domain
l3extIp	l3extMember	A secondary IP address policy
l3extLIfP	l3extLNodeP	The logical interface profile, which defines a common configuration that can be applied to one or more interfaces
l3extLNodeP	l3extOut	The logical node profile defines a common configuration that can be applied to one or more leaf nodes
l3extMember	l3extRsPathL3OutAtt	The member is used for providing per node IP address configuration
l3extRsEctx	l3extOut	The private layer 3 network context that belongs to a specific tenant or is shared
l3extRsPathL3OutAtt	l3extLIfP	The path endpoints (ports and port channels) used to reach the external layer 3 network
l3extVirtualLIfP	l3extLIfP	
vzAny	fvCtx	vzAny associates all endpoint groups (EPGs) in a context (fvCtx) to one or more contracts (vzBrCP), rather than creating a separate contract relation for each EPG
vzBrCp	fvTenant	Contract
vzEntry	vzFilter	A filter entry is a combination of network traffic classification properties
vzFilter	fvTenant	Filter
vzSubj	vzBrCp	Contract subject
uribv4Nexthop	uribv4Route	A URIB next hop database record
uribv4Route	-	A route

ACI object relationships understood by ASMS

Relation object	Relation source	Relation target	Note
fvRsBd	fvAEPg	fvBd	Relation from EPG to Bridge Domain
fvRsCons	fvAEPg	vzBrCp	Consumer relation from EPG to Contract
fvRsCtx	fvBd	fvCtx	Relation from Bridge Domain to VRF (Context)
fvRtCtx			
fvRsProv	fvAEPg	vzBrCp	Provider relation from EPG to Contract
l2extRsEBd	l2extOut	fvBd	Relation from L2 outside policy to the private layer 2 bridge domain
vzRsSubjFiltAtt	vzSubj	vzFilter	Relation from Contract subject to Filter
vzRsSubjGraphAtt	vzSubj	vnsAbsGraph	Relation from Contract subject to Service Graph
vzRtAnyToCons	vzBrCp	vzAny	Consumer relation from Contract to vzAny of a VRF
vzRtAnyToProv	vzBrCp	vzAny	Provider relation from Contract to vzAny of a VRF
vzRsAnyToCons	vzAny	vzBrCp	Consumer relation from vzAny of a VRF to Contract
vzRsAnyToProv	vzAny	vzBrCp	Provider relation from vzAny of a VRF to Contract
vzRtCons	vzBrCp	fvAEPg	Consumer relation from Contract to EPG
vzRtProv	vzBrCp	fvAEPg	Provider relation from Contract to EPG
fvRsDomAtt	fvAEPg	infraDomP	An EPG can be linked to a domain profile via the Associated Domain Profiles

ACI constructs configurable by ASMS

Object class	Support level
vzBrCp	Create new Contracts with existing EPGs or vzAny as consumer and provider, with existing or new Filters, manually provided Service Graph
vzFilter	Create new Filters while creating new Contracts
fvAEPg	Application EPG (End Point Group)

ACI API calls by ASMS

- /api/class/fvTenant.json
- /api/class/configJobCont.json
- /api/class/uribv4Route.json
- /api/mo/<qualifiedTenantDomainName>.json
- /api/mo/uni/tn-<tenantName>/brc-<contractName>.json
- /api/mo/uni/tn-<tenantName>/flt-<filterName>.json
- /api/mo/<epgDn>/rsprov-<contractName>.json
- /api/mo/<epgDn>/rscons-<contractName>.json
- /api/mo/<vrfDn>/rsanyToProv-<contractName>.json
- /api/mo/<vrfDn>/rsanyToCons-<contractName>.json
- /api/mo/uni/tn-<tenantName>/ap-<appProfileName>/epg-<epgName>.json
- /api/mo/uni/tn-<tenantName>/ctx-<vrfName>/any.json
- /api/mo/uni/tn-<tenantName>/out-<l3outName>/instP-<externalEpgName>.json
- /api/mo/uni/tn-<tenantName>/brc-<contractName>/subj-<subjectName>.json
- /api/mo/uni/tn-<tenantName>/ap-<appProfileName>.json
- /api/mo/uni/tn-<tenantName>/cif-<importedContractName>.json
- /api/mo/<epgDn>/rsconsIf-<importedContractName>.json
- /api/mo/<vrfDn>/rsanyToConsIf -<importedContractName>.json
- /api/aaaLogin.json
- /api/aaaLogout.json
- /api/aaaRefresh.json

ACI MSO related API calls by ASMS

- /api/v1/auth/login
- /api/v1/auth/refresh-token
- /api/v1/auth/logout
- /api/v1/sites
- /api/v1/schemas
- /api/v1/backups/backupRecords
- /api/v1/backups
- /api/v1/backups/backupRecords/{backupRecordId}
- /api/v1/execute/schema/{shemaName}/template/{templateName}

Summary

Integrating Cisco ACI with AlgoSec enables you to:

- **Automatically design and push security policy changes** to Cisco ACI by creating contracts and filters to enforce data center whitelist policy. AlgoSec also provisions firewalls connected to the ACI fabric or otherwise part of the network security controls in an enterprise multi-cloud environment.
- **Proactively assess risk** in Cisco ACI contracts and recommend changes needed to eliminate misconfigurations and compliance violations, both while making policy changes as well as periodically for the entire multi-cloud environment.
- **Reflect underlying security policies** in application policy, as implemented on firewalls and other security devices.

Product availability

The AlgoSec platform is available as part of the Cisco SolutionsPlus Program and is listed on the Global Price List (GPL).

For more details, see:

- Cisco Application Centric Infrastructure
- AlgoSec & Cisco integration

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

AlgoSec lives at the intersection of the infrastructure, security policy and the applications that run your business, enabling greater visibility, reduced risk and zero-touch change automation across the entire hybrid network.

See what securely accelerating your digital transformation, move-to-cloud, infrastructure modernization, or micro-segmentation initiatives looks like at www.algosec.com

www.AlgoSec.com