The bridge to possible

Cisco Tetration and AlgoSec

A Defense-In-Depth Approach to Application Segmentation and Security

Through the integration between AlgoSec Security Management Suite and the Cisco Tetration™ platform, customers can realize the benefits of defense-in-depth security through consistent application segmentation policy delivered as both macrosegmentation policies through infrastructure elements and white list-based microsegmentation policies enforced on the workloads.

The need

Today's business applications are the life blood for an organization, and they are struggling to secure those effectively. There are three primary challenges they face

1. Applications run in a multicloud environment and workload types vary from bare-metal to virtual, containers, and serverless.
2. These applications are highly dynamic and constantly changing, either because of built-in scale-out capabilities or through continuous delivery with new versions of the application being rolled out.
3. Application behaviors are also unique to each environment, depending on how they are deployed and consumed.

These factors contribute to an increase in the organization's attack surface and create gaps in the security infrastructure that application and security teams are challenged to fix.

About AlgoSec

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec, 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-premises networks. Over 1800 enterprises, including 20 of the Fortune 50, use 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.

A traditional perimeter-based security approach alone is ineffective in meeting these new demands. To address these security challenges effectively, a new defense-in-depth approach is needed. While defense-in-depth is not a new approach, the challenge has been how to define and discover a consistent policy to implement at different layers while enforcing these policies in a scalable fashion. When dealing with modern distributed and dynamic applications, this approach requires insight into applications and their dependencies. It also requires the capability to apply business context and automation to core security policy management processes, such as change management, risk and compliance assessment, and auditing.

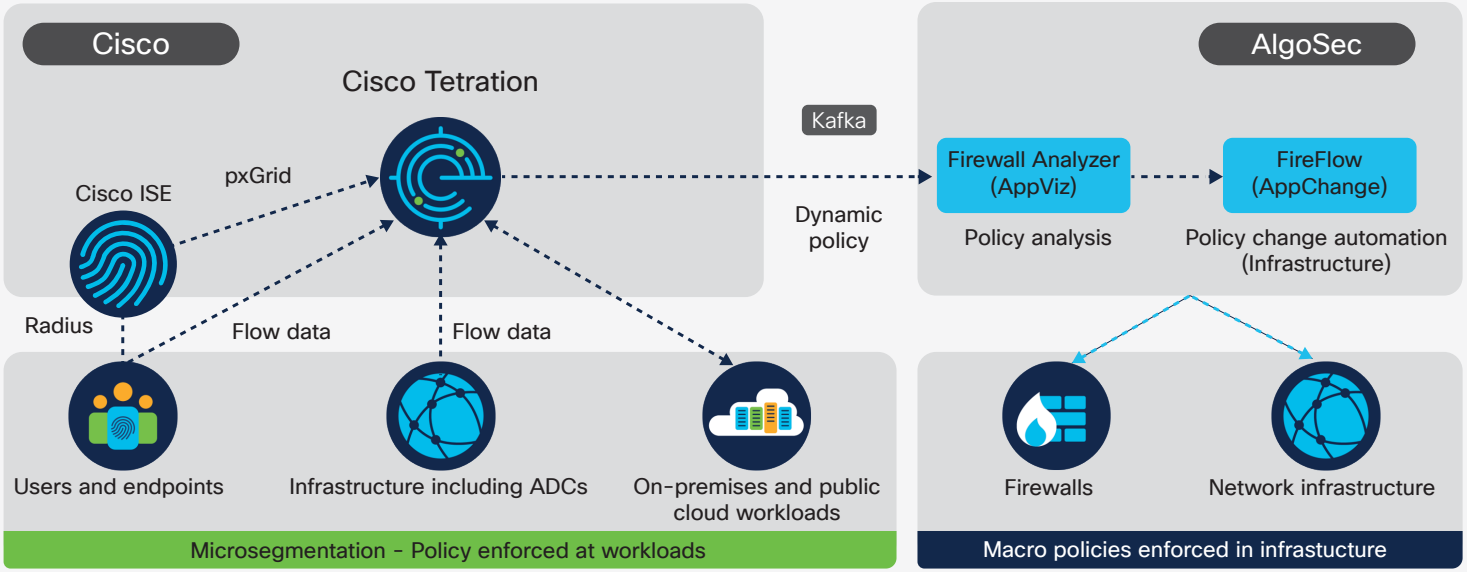
By combining the strengths of the Cisco Tetration platform for application policy discovery and workload-based enforcement with the AlgoSec Security Management Suite for the optimization and control of infrastructure-based segmentation, you can apply defense-in-depth security for applications running in any infrastructure and any cloud.

Cisco Tetration dynamically enforces granular microsegmentation policies on the workloads, while providing a consistent, real-time policy stream via Kafka for consumption by AlgoSec AppViz. This policy is further optimized and orchestrated for enforcement across infrastructure-based elements such as firewalls and network.

This allows customers to realize the benefits of defense-in-depth across a diverse multicloud environment, with the demands of any application from static, legacy operating systems to dynamic container-based microservices.

The figure below (Figure-1) is a high-level architecture diagram of how Cisco Tetration and AlgoSec can be used to implement defense-in-depth security for any data center or multicloud application environment.

Figure 1. Cisco Tetration – Algosec integration architecture



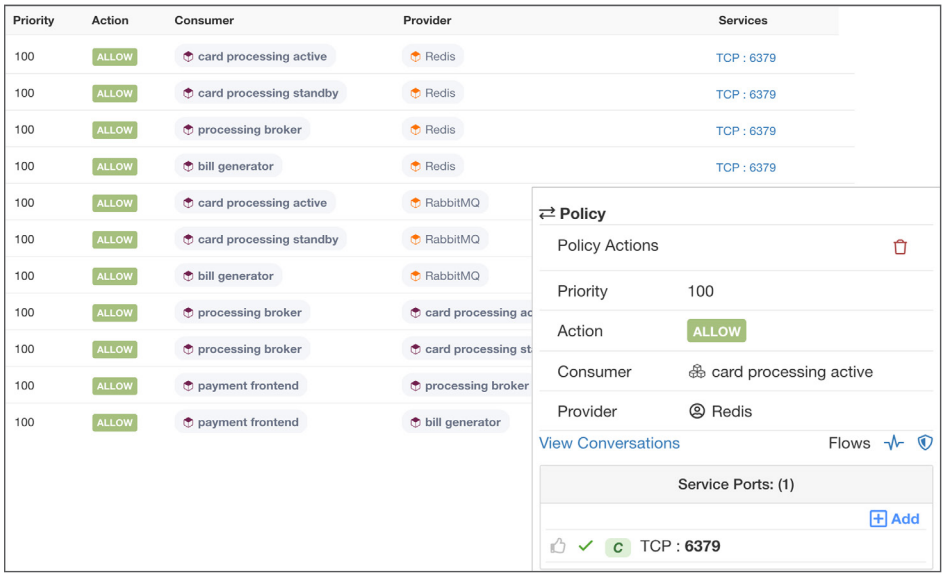
The bridge to possible

Cisco Tetration platform

Cisco Tetration is an application workload security platform designed to secure your compute instances across any infrastructure and any cloud. To achieve this, it uses behavior and attribute-driven microsegmentation policy generation and enforcement. It enables trusted access through automated, exhaustive context from various systems to automatically adapt security policies.

To generate accurate microsegmentation policy, Cisco Tetration performs application dependency mapping to discover the relationships between different application tiers and infrastructure services. In addition, the platform supports "what-if" policy analysis using real-time data or historical data to assist in the validation and risk assessment of policy application pre-enforcement to ensure ongoing application availability. The normalized microsegmentation policy can be enforced through the application workload itself for a consistent approach to workload microsegmentation across any environment, including virtualized, bare-metal, and container workloads running in any public cloud or any data center. Once the microsegmentation policy is enforced, Cisco Tetration continues to monitor for compliance deviations, ensuring the segmentation policy is up to date as the application behavior changes.

Figure 2. Example segmentation policy generated by Cisco Tetration



AlgoSec Security Management

The AlgoSec Security Management solution provides holistic, business-level visibility across the entire network security infrastructure, including business applications and their connectivity flows in the cloud and across software-defined networking (SDN) and on-premises networks. With AlgoSec, users can manage application connectivity, proactively analyze risk from the business perspective, tie cyber attacks to business processes, and intelligently automate time-consuming security changes—all at zero touch and seamlessly orchestrated across any heterogeneous environment.

Through the AppViz interface (Figure 3) you can import applications from Cisco Tetration. Once the applications are onboarded onto AppViz (Figure 4), users can automate security changes on multiple firewalls across the entire security estate.

Figure 3. AlgoSec user interface with Cisco Tetration integration

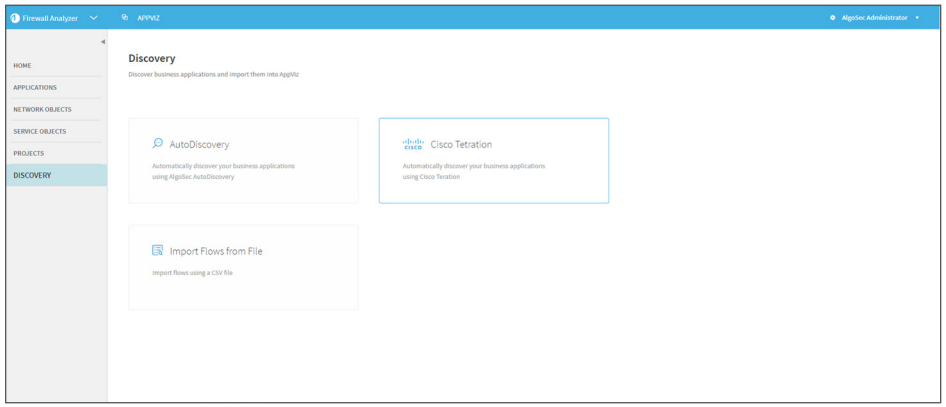
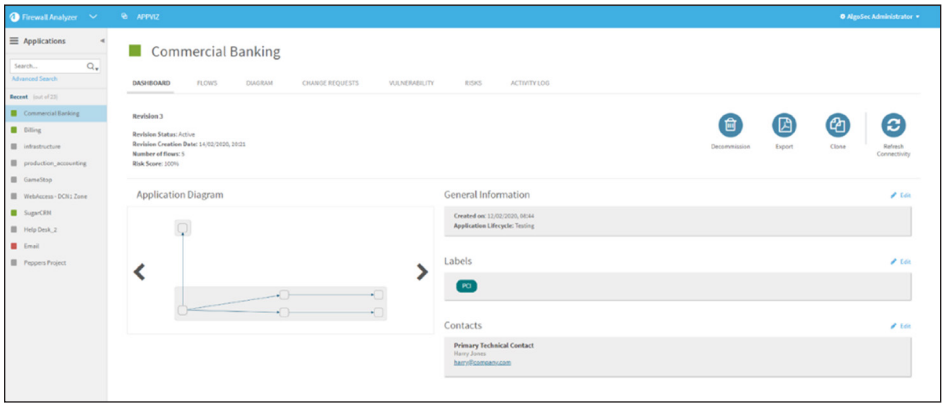


Figure 4. Imported application in AppViz



The integrated solution offers these main features:

- Sharing of the normalized segmentation policy in real time (Figure 2)
- Automatic tagging of security policy rules across multiple security devices, platforms, and technologies with the business applications they support (Figure 4)
- Enforcement of granular microsegmentation policies on the workloads
- Generation of a summarized or aggregated policy to be enforced in the infrastructure
- Using the same policy governance and change model that is already in place
- Enforcement of macro (coarse-grained) policy at the infrastructure layer

Figure 5 AlgoSec automatically tags security policy rules with the applications they support

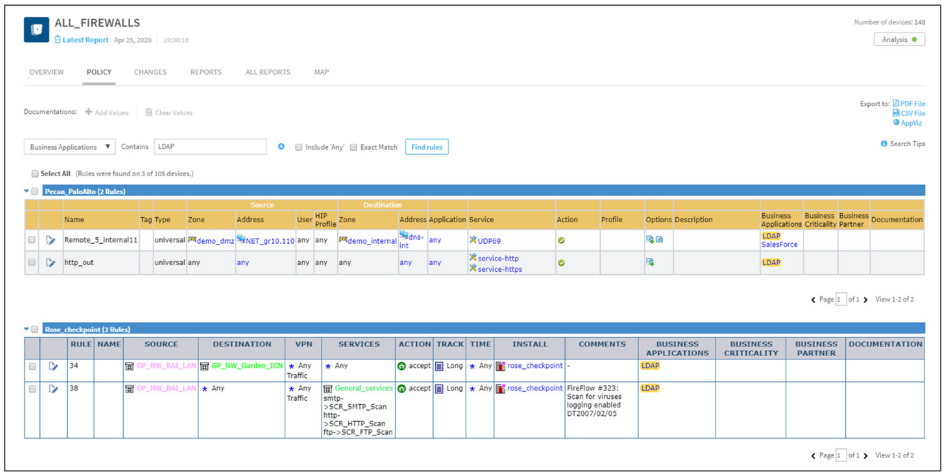
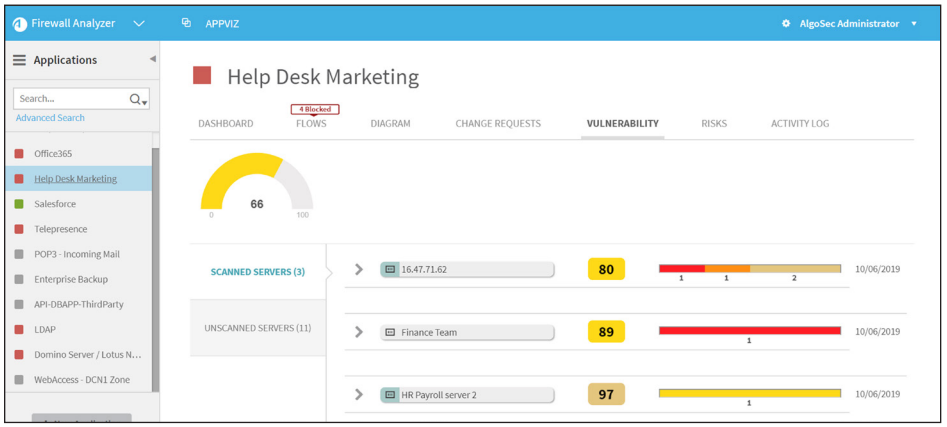


Figure 6. The Cisco and AlgoSec solution shows risks and vulnerabilities affecting each application



The bridge to possible

For more information

See www.cisco.com/go/tetration.

Main benefits of the integrated solution

- Enables you to implement defense-in-depth in your data center and cloud environments
- Extends implementation of microsegmentation to legacy and other appliance-based environments
- Realizes consistent security across any infrastructure, any cloud
- Leverages existing change control processes that are in place
- Allows you to make changes and secure your environment within minutes rather than days or weeks

Main use cases for the integrated solution

Table 1 presents the main use cases for the Cisco Tetration Analytics and AlgoSec solution.

Use case	Benefits
Consistent segmentation policies across application workloads and infrastructure such as firewalls	• Publish the segmentation policies over Kafka in real time • AlgoSec updates firewall rules or other infrastructure elements to enforce relevant policy elements
Enforce microsegmentation policies where workload-based enforcement is not possible	• There are instances where microsegmentation policies cannot be enforced on workloads • For such applications or application components, microsegmentation policies can be orchestrated as firewall rules by AlgoSec
Manage risk, vulnerabilities, and compliance in the context of affected business applications	• Manage network security risks in the context of affected business applications • Prioritize vulnerability and patch management based on affected business applications • View aggregated information about network security risks and vulnerabilities relevant to a specific business application

C22-739268-01 05/20