DEFINING AND ENFORCING A MICRO-SEGMENTATION STRATEGY

Micro-segmentation is a crucial defense-in-depth strategy for enterprises. It segregates and protects key company data to limit attackers' lateral movements across the corporate network. It is also effective in reducing the scope of audits for regulations such as PCI-DSS. But managing the firewall rules that enforce your micro-segmented network is challenging – and the more segments you have, the more firewalls you need to deploy and manage. This inherent trade-off between security and complexity often results in under-segmented networks, which are not as secure as they should be. Fortunately, AlgoSec makes it easy to define and enforce micro-segmentation throughout your network and across all leading firewall platforms.

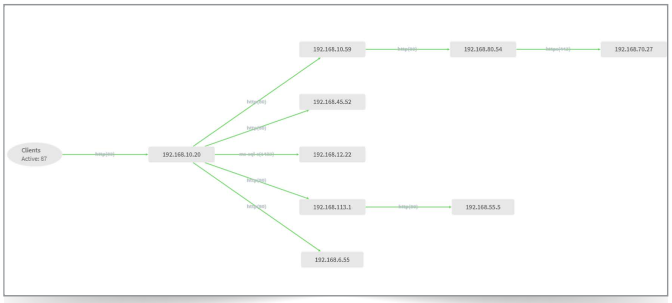
Discover Business Applications

This first step to segmentation is understanding the traffic traversing in the network and identifying the intent of the flows by mapping them to the applications they support. This can be achieved by:

IMPORTING the flows from a CSV file

INTEGRATING with a micro-segmentation tool such as Cisco Tetration, Illumio or Guardicore

UTILIZING AlgoSec AutoDiscovery to analyze your traffic flows and turn them into a clear map. AutoDiscovery receives network traffic metadata as NetFlow, SFlow, or full packets and then digests multiple streams of traffic metadata to let you clearly visualize your network traffic.



The AlgoSec Benefits

- Auto-discover applications and their connectivity flows – without requiring any prior knowledge
- Design your segmentation zones with live and always up-to-date map of connectivity requirements
- Easily define allowed traffic between your network segments
- Ensure changes adhere to your micro-segmentation strategy and compliance requirements
- Automatically implement network security changes
- Support software-defined micro-segmentation on platforms such as Cisco ACI and VMWare NSX

Business Impact

- Easily define and continuously enforce your micro-segmentation strategy across your heterogeneous environment
- Effectively limit the lateral movement of cyber attackers across your network
- Ensure continuous compliance of your micro-segmentation network security strategy
- Avoid errors, rework and application outages due to the micro-segmentation complexity
- Create a scalable and repeatable process that aligns the different teams involved in the change process
- Maintain uniform security policy across the entire cloud and on-premise hybrid environment

Defining the Segments with Application Mapping

AlgoSec AppViz provides an application-centric approach to your segmentation strategy. Leveraging the AutoDiscovery results, the AppViz advanced optimization algorithm aggregates a group of connections into thick flows. This can prevent overloading multiple rules on the firewalls, which can potentially lead to performance degradation. At the same time, business application owners get a clear view of the network flows that support their application.

This simplifies the experience of the security operation expert defining and maintaining a segmentation strategy by making the firewall rules clearer to understand and manage. The algorithm predicts the future behavior of the traffic and assures it is aligned with the segmentation policy.

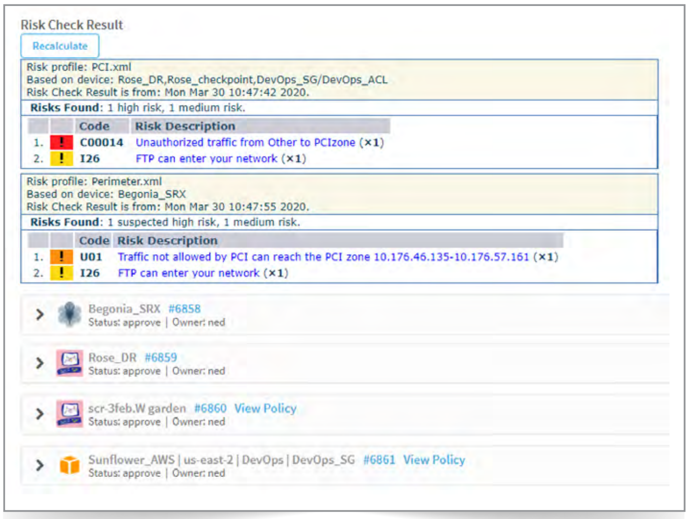
Mapping the flows associated with the business applications will give you the business intelligence you need to define the segmentation zones around your business applications, limiting outages and downtime.

Implement Segmentation Policies

AlgoSec FireFlow helps you process security policy changes that are required for segmentation strategy. FireFlow automates the entire security policy change process — from design and submission to proactive risk analysis, implementation, validation, and auditing.

AppViz leverages FireFlow's automation capabilities to allow network engineers to easily execute the many required changes related to rolling out the segmentation strategy in the network — while ensuring that changes are done quickly, in line with the segmentation strategy. All that is needed is to request to apply the discovered application flows from AppViz to the network and all the heavy lifting will be done by FireFlow.

Once the zones have been defined in the network, FireFlow will ensure the that the segmentation strategy is upheld within the network. The intelligent risk-analysis step proactively assesses each request against the defined segmented zones ensuring all changes align with the segmentation strategy without introducing new risk or breaking compliance.



Risk Check Result

Risk profile: PCI.xml
Based on device: Rose_DR,Rose_checkpoint,DevOps_SG/DevOps_ACL
Risk Check Result is from: Mon Mar 30 10:47:42 2020.

Risks Found: 1 high risk, 1 medium risk.

		Code	Risk Description
1.	!	C00014	Unauthorized traffic from Other to PCIzone (×1)
2.	!	I26	FTP can enter your network (×1)

Risk profile: Perimeter.xml
Based on device: Begonia_SRX
Risk Check Result is from: Mon Mar 30 10:47:55 2020.

Risks Found: 1 suspected high risk, 1 medium risk.

		Code	Risk Description
1.	!	U01	Traffic not allowed by PCI can reach the PCI zone 10.176.46.135-10.176.57.161 (×1)
2.	!	I26	FTP can enter your network (×1)

Begonia_SRX #6858
Status: approve | Owner: ned

Rose_DR #6859
Status: approve | Owner: ned

scr-3feb.W garden #6860 View Policy
Status: approve | Owner: ned

Sunflower_AWS | us-east-2 | DevOps | DevOps_SG #6861 View Policy
Status: approve | Owner: ned

Comprehensive Support for Heterogeneous Environments

AlgoSec supports all the leading brands of traditional and next generation firewalls and cloud security controls, as well as routers, load balancers and web proxies across any heterogeneous and multi-vendor cloud, SDN or on-premise enterprise network environments. Additionally, AlgoSec seamlessly integrates with the leading IT service management, SIEM, identity management, orchestration systems and vulnerability scanners to deliver unified security policy management. To find out more about AlgoSec's ecosystem of technology partners, visit www.algosec.com/algosec-ecosystem.