IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

IP Fabric

Network Security Policy Management

Your network security policy management tools help ensure that your policies are properly defined, and placement is ideal. Injecting network assurance into this can give you deeper insight into the behavior of your network. Notify your tools when changes are made, and easily measure the success of your changes.

Gartner
COOL VENDOR 2022

Your Challenge

Security teams are constantly changing firewall rules in accordance with policy.

Do you find yourself asking these questions?

- Are the security appliances themselves hardened in line with configuration standards?
- Have any new security devices been added to the network?
- Have there been any configuration changes which add new segments to the network, or bypass security appliances?
- Have any new servers been brought up in the network segments I know of?

Our Solution

IP Fabric fills these gaps in your knowledge through automated daily discovery, flexible visualization, and intent verification.
You always know exactly what is in your network, and if all devices are configured in alignment with your policies.

Our approach to visualization gives you the context to know how changes affect your network as a whole. Data is key to managing your security policy.

Benefits

- Implement a proactive approach to security management.
- Reduce MTTR when you do have to be reactive.
- Align your security and network teams

Secure your infrastructure

Have a network baseline from which to validate the hardware, software & config aren't vulnerable to attack.

A Zero-Trust Approach

Secure the network edge.

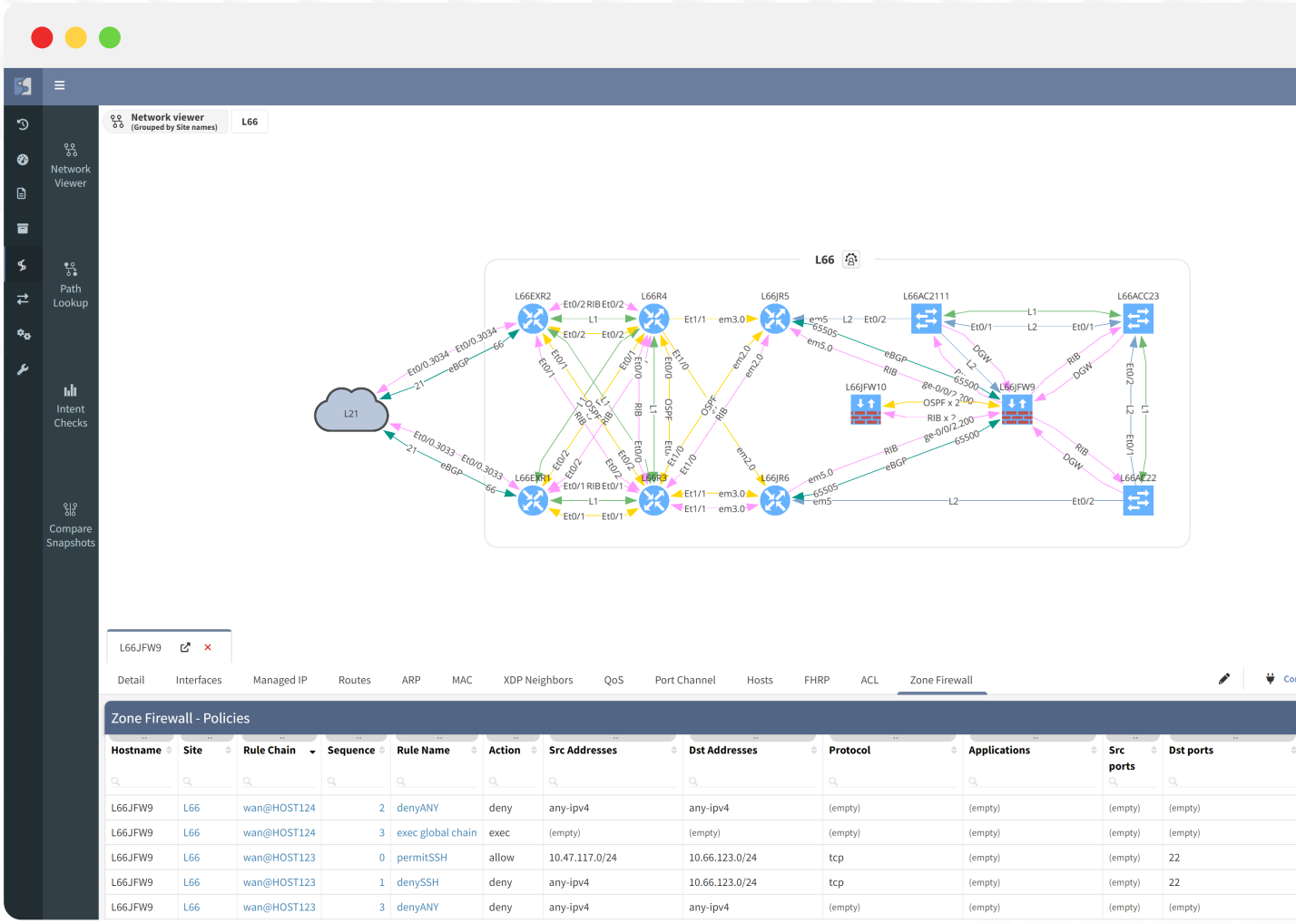
Supports Segmentation

Control how traffic flows through your network.

Policy Automation

Deploy policy from a central point.

algosec SKYBOX SECURITY tufin FIREMON



Hostname	Site	Rule Chain	Sequence	Rule Name	Action	Src Addresses	Dst Addresses	Protocol	Applications	Src ports	Dst ports
L66JFW9	L66	wan@HOST124	2	denyANY	deny	any-ipv4	any-ipv4	(empty)	(empty)	(empty)	(empty)
L66JFW9	L66	wan@HOST124	3	exec global chain	exec	(empty)	(empty)	(empty)	(empty)	(empty)	(empty)
L66JFW9	L66	wan@HOST123	0	permitSSH	allow	10.47.117.0/24	10.66.123.0/24	tcp	(empty)	(empty)	22
L66JFW9	L66	wan@HOST123	1	denySSH	deny	any-ipv4	10.66.123.0/24	tcp	(empty)	(empty)	22
L66JFW9	L66	wan@HOST123	3	denyANY	deny	any-ipv4	any-ipv4	(empty)	(empty)	(empty)	(empty)

More resources

- Solution Brief | IP Fabric & Security Assurance
- Video | IP Fabric & Skybox

ABOUT **IP FABRIC**

IP Fabric is solving Network Assurance for large enterprises by creating a digital twin of the entire network infrastructure, containing information about every technology and protocol, and capable of simulating forwarding and security scenarios. IP Fabric's network model is also used as a Network Source of Truth for network automation initiatives, serving as an API for the entire network. IP Fabric was recognized by Gartner as Cool Vendor in Network Automation for 2022.

Don't take our word for it

REQUEST A DEMO

Request a demo and discover how to increase your networks visibility & get better time efficiency.

IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

115 Broadway, 5th Floor
New York, NY, 10006
United States

info@ipfabric.io

Kateřinská 466/40
Prague - 12000
Czech Republic

sales@ipfabric.io

ipfabric.io