illumio

TECHNICAL BRIEF

Illumio for Microsoft Azure Firewall

Firewall policy for the cloud

Product Overview

Microsoft and Illumio have partnered to bring together the security benefits of the cloud-native Microsoft Azure Firewall and Zero Trust Segmentation. This combination supports Azure customers to better protect their Azure deployments, accelerate the move to the cloud, and provide consistent end-to-end security across their hybrid and multi-cloud deployments.

Firewall policy setting can be complex. Setting granular policy and moving towards a Zero Trust, least-privilege posture is the goal, but firewall policy commonly defaults to highly permissive access to avoid application downtime and reduce the effort required for rule development.

Illumio for Azure Firewall delivers:

Enhanced Azure Firewall experience

Simple cross-platform security policy

Segmentation that adapts policy based on insights

Key Benefits

- Enable Zero Trust for the cloud
- Reduce risk of application downtime
- Understand application dependencies

Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.

Illumio for Azure Firewall provides a simple solution:

- Visually identify least-privilege policy
- Use natural language labels rather than IP addresses to create policy
- Automate policy testing and enforcement
- Simplify the process of firewall rule attestation

With Illumio for Microsoft Azure Firewall, every Azure Firewall becomes a true Zero Trust enforcement point.

Features and Benefits

Whether you are looking to secure a new application freshly deployed into Azure or support the migration of an application from a data center into the cloud, Illumio for Azure Firewall enables you to build the right protection safely.

Total visibility

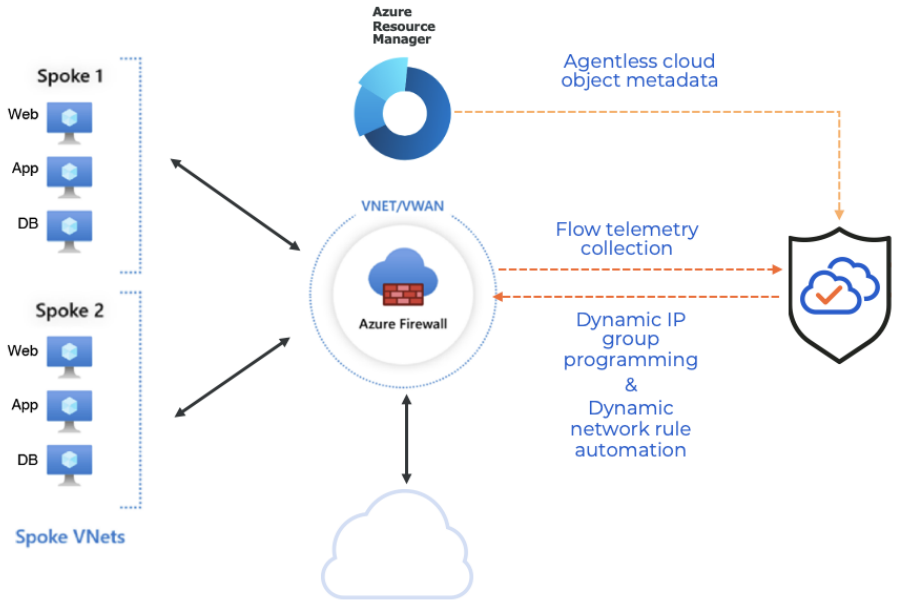
- Visualize data flows through the Azure Firewall for perspective on connectivity at the cloud boundary.
- Visualize Network Security Group data flows for perspective on east-west communications between workloads within a cloud.
- Visualize multicloud data flows for a holistic perspective on application data flows.
- Monitor changes in data flow over time to identify potential anomalies and malicious activity.

Consistent security

- Program Azure Firewalls with label-based policy so that the correct policy based on context is applied at the perimeter and the workload across cloud environments.
- Define policy based on application properties instead of unrelated properties such as IP addresses — policy is tied to the application and not the network.
- Decentralize policy setting to teams closest to the applications with centralized review and management for compliance — supporting "shift left" security.

Validated policy

- Deploy changes directly to the Azure Firewall Manager safely with continuous validation.
- Understand the impact of policy on the environment before moving to enforcement — ensuring applications do not break.
- Reduce time to policy attestation by visualizing policy and its use to deny or allow traffic.



Illumio for Azure Firewall

- **Firewall context & label to IP group mapping**
- **Visibility of Firewall objects and traffic flows**
- **Label based programming of Firewall policy with simulation mode**

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.