Documentation

Enforcing Zero Trust with Distributed Cloud Firewall and the Default Action Rule

Aviatrix Distributed Cloud Firewall (DCF) provides a foundational framework for implementing zero trust principles across multi-cloud environments. A key component of this framework is the Default Action Rule, which establishes a baseline security posture by controlling how traffic is handled in the absence of explicit rules.

Default Action Rule Behavior

NOTE

The Default Action Rule is only created if using Controller 8.1.

When Distributed Cloud Firewall is enabled in Aviatrix CoPilot, a Default Action Rule is automatically created in the Post Rules Policy List. This global rule governs the default behavior for traffic that does not match any user-defined rules. Administrators can configure the Default Action Rule to either **Permit** or **Deny** traffic. To align with zero trust best practices, you must set this rule to **Deny**. The rule then becomes an "implicit deny" rule that remains at the bottom of the ruleset and is enforced globally.

IMPORTANT

Before setting the Default Action Rule to Deny, or deleting the legacy DefaultDenyAll Rule if it exists, you should define Permit rules for trusted SmartGroups that specify allowed traffic flows. This ensures that critical services remain accessible and avoids unintended disruptions.

(Only applicable if you used DCF prior to Controller 8.1) Once traffic patterns have been reviewed and appropriate rules are in place, the optional Greenfield Rule—used to allow all traffic during initial setup—can be removed.

SmartGroups and Policy Enforcement

SmartGroups enable dynamic, tag-based policy enforcement. These groups are defined using cloud-native metadata such as instance tags or labels. Rules can refer to these dynamic cloud-based SmartGroups instead of groups of static IP addresses, allowing for scalable and context-aware access control.

For example, a rule might permit HTTP and HTTPS traffic from a SmartGroup representing frontend web servers to another SmartGroup representing backend APIs. This approach supports micro-segmentation and limits lateral movement within the network—key objectives of a zero trust architecture.

Additional Distributed Cloud Firewall Features Supporting Zero Trust

Distributed Cloud Firewall includes several features that enhance zero trust enforcement:

- Geolocation Filtering: Administrators can restrict traffic based on country or region, reducing exposure to high-risk geographies.
- Threat Intelligence Feeds: Integration with threat feeds allows for automatic blocking of known malicious IP addresses and domains.
- SaaS services can be protected by defining policies that restrict access to specific applications or services, ensuring that only authorized users and devices can interact with certain resources.
- TLS Decryption and URL Filtering: These capabilities provide visibility into encrypted traffic and enable fine-grained control over web access.
- Logging and Monitoring: Selective logging of Permit and Deny actions supports auditing and incident response without overwhelming storage resources.

Operational Considerations

The Default Action Rule cannot be deleted and serves as a persistent enforcement mechanism. It is important to regularly audit policy rules and SmartGroup definitions to ensure they reflect current organizational requirements and security posture.

By combining the Default Action Rule with SmartGroups and other DCF capabilities, Aviatrix enables organizations to implement a zero trust model that is both comprehensive and adaptable to evolving cloud environments.

Implementation Methodology

A structured approach to zero trust implementation with Aviatrix includes:

- Traffic Analysis: Use CoPilot's monitoring capabilities to document legitimate traffic patterns between application components.
- Policy Development: Create SmartGroups to accurately represent application components, then establish explicit DCF Permit rules for required communications.
- Validation Testing: Create and validate your policy with the Default Action set to Permit before changing the Default Action to Deny. This ensures that all necessary traffic is allowed before enforcing the deny-by-default posture.

- Production Deployment: Transition production environments to the deny-by-default configuration while monitoring for any unexpected issues.
- Continuous Refinement: Review and optimize policies regularly.

Related Topics

- Distributed Cloud Firewall Setup and Default Action Rule