Documentation

Security

Dynamic Trust Enforcement with Distributed Cloud Firewall

Aviatrix Distributed Cloud Firewall (DCF) is a policy-driven security solution embedded in the cloud fabric itself. It dynamically enforces trust across the entirety of your organization's cloud workloads, ensuring comprehensive protection and compliance.

Key Features of Distributed Cloud Firewall

DCF provides advanced security capabilities, including:

- Dynamic trust enforcement across cloud workloads
- Policy-driven inspection and security
- Layer 4 visibility and policy enforcement
- URL/FQDN Filtering with WebGroups (not supported for DCF on Edge)
- ExternalGroups for reputation-based threat detection/prevention and geographical IP blocking/filtering (replaces ThreatIQ and Geoblocking functionality)
- Transparent MITM decryption and Advanced Threat Detection with Suricata
- Aviatrix SmartGroups for dynamic policy application based on tags and attributes
- Transit FireNet integration with partner firewalls (Check Point, F5, Fortinet, Palo Alto Networks)

Embedded Security in the Cloud Fabric

DCF is seamlessly integrated into the cloud fabric, enabling organizations to enforce zero trust principles dynamically. By inspecting and securing workloads, DCF ensures that security policies are applied consistently across all cloud environments.

High-Performance Encryption and Transit Security

Aviatrix encrypts all data in-transit using high-performance encryption (HPE), eliminating standard IPSec speed limits. This ensures secure transit connections between cloud service providers (CSPs) and CSP regions without sacrificing performance.

The Aviatrix Distributed Cloud Firewall provides centralized security policy management and enforcement across multi-cloud environments, enabling consistent workload protection and trust verification throughout ud network infrastructure..

Network Security covers the following features:

- Distributed Cloud Firewall Overview
- Enforcing Zero Trust with Distributed Cloud Firewall and the Default Action Rule
- Groups
- Configuring Distributed Cloud Firewall
    - Distributed Cloud Firewall Rulesets
    - Distributed Cloud Firewall Setup and Default Action Rule
    - Creating Groups for Distributed Cloud Firewall
    - Distributed Cloud Firewall Rulesets
        - Creating a Distributed Cloud Firewall Ruleset
        - Editing a Distributed Cloud Firewall Ruleset
        - Managing Distributed Cloud Firewall Rulesets
    - Creating Distributed Cloud Firewall Rules
    - Distributed Cloud Firewall Actions
    - Distributed Cloud Firewall Settings
    - Viewing Distributed Cloud Firewall Rule Details
    - Enabling Security Group Orchestration
- Monitoring Distributed Cloud Firewall
    - Distributed Cloud Firewall Monitoring
    - Retaining Distributed Cloud Firewall Log Files
    - Resetting Distributed Cloud Firewall Traffic Count
- Advanced Security Features
    - Detected Intrusions for Distributed Cloud Firewall Rules
    - Blocking Known Threat IP Traffic using ThreatIQ
    - Blocking Traffic from Countries using Geoblocking
    - Detecting Network Anomalies using Network Behavior Analytics
- Legacy to Distributed Cloud Firewall Migration
    - General Guidelines for Migrating from Legacy ThreatIQ and Geoblocking to Distributed Cloud Firewall
    - Migrating from Legacy Egress to Distributed Cloud Firewall
- Aviatrix Kubernetes Firewall
