# Migrating from Legacy Egress to Distributed Cloud Firewall

If you configured Egress FQDN filtering in the Aviatrix Controller, Aviatrix strongly recommends that you upgrade to Distributed Cloud Firewall (DCF) with its accompanying WebGroups functionality (available as of Controller version 7.1.1710).

If you migrate to DCF you can no longer use Legacy Egress FQDN.

DCF allows for more granular security policies and a higher level of threat protection. DCF provides significant performance improvements through distributed processing, optimized rule evaluation, and elimination of duplicate gateway-specific rules.

Reach out to your Aviatrix Sales Representative for assistance with this migration.

NOTE

Ensure that you are running Controller 7.2 or higher.

## Considerations Before Migration

- Existing High Availability setups are compatible and encouraged.
- Protocol Migration: DCF WebGroups support HTTP and TLS traffic only (ports 80, 443, 8080, 8443). For Legacy Egress filters using other protocols (SSH, SMTP, FTP, etc.), migrate using SmartGroups:
  - Use hostname SmartGroups for FQDN-based filtering of non-HTTP/TLS protocols (Controller 7.2 or greater)
  - Use CIDR-based SmartGroups when static IP addresses are known and suitable
- Wildcard Compatibility: DCF WebGroups have full wildcard support, which will accommodate legacy filters with mid-string wildcards (sub.*.domain.com).
- Gateway Requirements:
  - Spoke Gateways and Public Subnet Filtering (PSF) Gateways
  - Standalone Gateways must be redeployed as Spoke Gateways
  - Alternative Approach: FireNet Egress gateways should consider migrating to Distributed Egress per VPC.

Spoke gateways must meet the minimum size (for example, t3.small for AWS) to handle the distributed processing of DCF rules. If you have Spoke Gateways that are smaller than the minimum size, you must upgrade them to a supported size before migrating. Performance can be tuned using the About Auto Right-Sizing feature.

## Combined Comparison: Legacy Egress vs. Distributed Cloud Firewall

The following table combines the comparison of capabilities and the mapping of Legacy Egress features to Distributed Cloud Firewall (DCF) components:

| **Capability/Component** | **Legacy Egress** | **DCF** | **Benefits/Notes** |
|---|---|---|---|
| FQDN Filtering | Create tags containing domain lists, then attach gateways to tags | Create WebGroups with domain lists, reference in DCF rules | • Centralized domain management<br>• Better performance<br>• Advanced threat protection |
| Resource Definition | Assign individual Spoke Gateways to FQDN tags | Create SmartGroups with flexible match criteria (VPC/VNet, Subnets, VMs, IP/CIDR, External Connections, Hostnames) | • Dynamic resource matching<br>• Scalable policy management<br>• Reduced configuration overhead |
| Policy Actions | Select Allowlist/Denylist per tag | Configure Allow/Deny actions per DCF rule with granular control | • Rule-level action control<br>• More flexible policy combinations<br>• Support for complex scenarios |
| Policy Enforcement | Enable/Disable entire tags | Enable/Disable individual DCF rules with monitoring mode | • Granular rule control<br>• Safe testing with monitor mode<br>• Independent rule lifecycle |
| Protocol Support | All protocols and ports supported | HTTP/TLS (ports 80, 443, 8080, 8443) for WebGroups; hostname SmartGroups for non-Web traffic (Controller 7.2 or greater); all protocols for CIDR-based rules | • Optimized for Web traffic (TLS or HTTP)<br>• FQDN filtering for non-Web protocols<br>• Deep packet inspection<br>• Protocol-aware filtering |

| Capability/Component | Legacy Egress | DCF | Benefits/Notes |
|---|---|---|---|
| Rule Scope | Gateway-specific (duplicate rules needed for HA pairs) | Global rules apply across all gateways | • Simplified management<br>• Automatic HA coverage<br>• Consistent policy enforcement |
| Performance | Per-gateway processing with potential bottlenecks | Distributed processing with optimized rule evaluation | • Higher throughput<br>• Lower latency<br>• Better scalability |
| Logging & Monitoring | Gateway-specific logs in CoPilot FlowIQ | Centralized DCF Monitor with enhanced visibility | • Unified log view<br>• Advanced filtering<br>• Better troubleshooting |
| Wildcard Support | Full wildcard support (.domain.com, sub..domain.com) | Full wildcard support (*.domain.com, sub..domain.com) | • Simplified pattern matching<br>• Better performance<br>• Consistent behavior |
| Gateway Types | Spoke, Standalone, FireNet Gateways | Spoke and Public Subnet Filtering (PSF) Gateways only | • Focused on modern architectures<br>• Optimized performance<br>• Simplified deployment |
| FQDN Tag with domains | Legacy Egress Component | WebGroup(s) | May create multiple WebGroups if different port/protocol combinations exist |
| Gateway attachment to FQDN tag | Legacy Egress Component | SmartGroup (VPC/VNet-based) | Uses account, region, and VPC/VNet name as match criteria |
| Stateful Firewall Tag (CIDR list) | Legacy Egress Component | SmartGroup (CIDR-based) | Maintains original tag name |
| Individual CIDR in policies | Legacy Egress Component | SmartGroup (CIDR-based) | Named as cidr_(CIDR)-(mask) unless matches existing tag |
| Discovery mode | Legacy Egress Component | Special DCF Rules | Creates rules with "Any-Web" WebGroup and logging enabled |
| Default stateful firewall action | Legacy Egress Component | Catch-all DCF Rules | Creates appropriate default rules based on VPC security posture |

## Manual Migration Process

For manual migration, follow these steps to replicate your Legacy Egress FQDN configurations in Distributed Cloud Firewall:

### Step 1: Inventory Current Configuration

Document your existing Legacy Egress configuration:

| Element | Information to Record |
|---|---|
| Tags | All tags in Security > Egress Control > Egress FQDN Filter |
| Domain Lists | FQDNs/URLs associated with each tag |
| Gateway Attachments | Which gateways are attached to each tag (from Egress FQDN Gateway View) |
| Allow/Deny Actions | ALLOWLIST/DENYLIST setting for each tag |
| Status | Enabled/Disabled status for each tag |
| Source Configuration | Any custom source IP settings for tags with attached gateways |
| Port/Protocol | Port and protocol information for each FQDN rule |

### Step 2: Create WebGroups

For each Legacy Egress FQDN tag:

1. Navigate to Security > Distributed Cloud Firewall > WebGroups.
2. Click **+ WebGroup**.
3. Configure the WebGroup:
   - Name: Provide a descriptive name for the WebGroup
   - Domains: Add the FQDNs from the legacy tag
   - Type: Select based on content (e.g., Social Networking, Streaming Media)

Create separate WebGroups for different port/protocol combinations from the same legacy tag.

### Step 3: Create SmartGroups

Create SmartGroups to represent the resources that were attached to the legacy FQDN tags:

#### *VPC/VNet SmartGroups*

1. Navigate to Security > Distributed Cloud Firewall > SmartGroups.
2. Click **+ SmartGroup**.
3. Configure for VPC/VNet matching:
   - Name: Provide a descriptive name

- Resource Type: VPC/VNet
- Match Criteria: Account, Region, Name
- Values: Specify the VPC/VNet details

***CIDR SmartGroups (for Stateful Firewall Tags)***

For any Stateful Firewall tags being migrated:

1. Navigate to Security > Distributed Cloud Firewall > SmartGroups.
2. Click **+ SmartGroup**.
3. Create CIDR-based SmartGroups.
    - Name: Provide a descriptive name
    - Resource Type: IP/CIDR
    - CIDR: Enter the IP ranges from the legacy tag

## Step 4: Create DCF Rules

For each legacy configuration, create corresponding DCF rules:

1. Navigate to Security > Distributed Cloud Firewall > Policies.
2. Select a ruleset or create a new one.
3. Click **+ Rule**.
4. Configure the rule:
    - Name: Provide a descriptive name
    - Source SmartGroups: Select the VPC/VNet SmartGroups
    - Destination: Select "Public Internet" for egress rules
    - WebGroups: Select the appropriate WebGroup for FQDN filtering
    - Protocol: TCP (for HTTP/TLS traffic)
    - Port: Specify the ports (80, 443, 8080, 8443)
    - Action: Allow or Deny (matching legacy configuration)
    - Logging: Enable for monitoring
    - Enforcement: Start with disabled for testing

## Step 5: Handle Non-WebGroup Protocols

For Legacy Egress rules using protocols not supported by WebGroups (non-HTTP/TLS traffic), migrate using SmartGroups:

**For Protocols Requiring FQDN filtering (Controller 7.2 or greater)**

1. Navigate to Groups > Settings > DNS Server for Hostname Resolution.
2. Configure either Gateway’s Management DNS Server or custom DNS servers.
3. Create SmartGroups with Resource Type "Hostname":
    a. Navigate to Security > Distributed Cloud Firewall > SmartGroups
    b. Click **+ SmartGroup**.
    c. Select "Hostname" Resource Type.
        - Hostname: Enter the FQDN from your legacy rule
        - Name: Provide a descriptive name
4. Create DCF rules:
    a. Source SmartGroups: Select the VPC/VNet SmartGroups
    b. Destination: Select the hostname-based SmartGroup
    c. Protocol: Specify the protocol (e.g., TCP, UDP)
    d. Port: Specify the ports (e.g., 22 for SSH, 25 for SMTP)

**For Protocols with Known Static IP Destinations**

1. Research the current IP addresses for the FQDNs.
2. Create CIDR-based SmartGroups for the static IPs:
    - Resource Type: IP/CIDR
    - IP/CIDRs: Enter the IP ranges
    - Name: Provide a descriptive name

Hostname SmartGroups provide dynamic DNS resolution and are the preferred method for maintaining FQDN-based filtering. Use CIDR-based SmartGroups only when hostname SmartGroups are not suitable for your use case.

## Step 6: Create Catch-All Rules

For each VPC/VNet, create appropriate catch-all rules based on the security posture of the VPC/VNet:

- For VPCs with Stateful Firewall Default Deny: Create deny rules for those VPCs
- For VPCs with Stateful Firewall Default Allow: Create allow rules (placed below deny rules to avoid unintentionally overriding or blocking the effect of a valid lower-priority rule)
- For VPCs without Stateful Firewall Policies: Create "Catch All Unknown" rules (review manually)

- Global Catch-All: Create a final rule with source/destination "Any"; set to ALLOW initially, change to DENY after testing

## Post-Migration DCF Ruleset Example

The following example illustrates a typical DCF ruleset after migrating three VPCs with different Legacy Egress configurations:

| Rule Name | Source SmartGroup | Destination | WebGroup/Protocol | Port | Action | Purpose |
|---|---|---|---|---|---|---|
| Allow-HTTP-to-Google | sg-app-servers | 0.0.0.0/0 | wg-google-http / HTTP | 80 | Allow | Allow app servers to access Google over HTTP |
| Deny-FTP-to-External | sg-dmz | 0.0.0.0/0 | N/A / FTP | 21 | Deny | Block DMZ servers from accessing external FTP sites |
| Allow-TLS-to-Internal-API | sg-backend | 10.10.10.0/24 | wg-internal-api / TLS | 443 | Allow | Permit backend servers to reach internal API over TLS |
| Monitor-AnyWeb-to-Discovery | sg-discovery | 0.0.0.0/0 | wg-any-web / HTTP, TLS | 80, 443 | Monitor | Log all web traffic from discovery group for analysis |

This example demonstrates how Legacy Egress FQDN tags are replaced by WebGroups for Web traffic and hostname SmartGroups for non-Web protocols, with appropriate source SmartGroups representing each VPC.

## Best Practices and Recommendations

### Pre-Migration Planning

- Test Environment First: Always test the migration in a lab environment before production
- Backup Configuration: Export current Legacy Egress configuration before starting migration
- Start with PERMIT: Begin with global catch-all action set to PERMIT, then transition to DENY after validation
- Phased Approach: Consider migrating VPCs/VNets in phases rather than all at once
- Maintenance Window: Plan appropriate maintenance windows for production migration

### Configuration Optimization

- Rule Consolidation: Take advantage of DCF's ability to have multiple ports in a single rule
- SmartGroup Reuse: Create reusable SmartGroups that can be referenced across multiple rules
- WebGroup Organization: Organize WebGroups by business function or security policy purpose
- Logging Strategy: Enable logging on all rules initially, then optimize based on monitoring needs
- Rule Ordering: Ensure more specific rules appear before general catch-all rules

## Migration Validation and Testing

### Pre-Production Testing

1. Lab Environment: Deploy the configuration in a test environment first
2. Monitor Mode: Enable logging on all rules with Enforcement disabled
3. Traffic Analysis: Review DCF logs in Security > Distributed Cloud Firewall > Monitor
4. Domain Validation: Verify the Domain field is populated for WebGroup traffic

### Production Deployment

1. Maintenance Window: Schedule appropriate downtime
2. Phased Approach: Enable rules incrementally
3. Monitoring: Monitor traffic and logs continuously
4. Rollback Plan: Prepare to disable DCF rules quickly if needed

## Post-Migration Monitoring

- Traffic Validation: Monitor DCF logs to ensure all expected traffic is flowing correctly
- Performance Monitoring: Validate that network performance meets expectations
- Rule Effectiveness: Review rule hit counts to identify unused or overly broad rules
- Security Posture: Confirm that the migrated configuration maintains desired security controls

### Post-Migration Validation

1. Functional Testing: Verify applications work as expected
2. Log Analysis: Check DCF logs for proper rule matching
3. Performance Monitoring: Validate improved performance
4. Security Posture: Confirm that security policies are enforced as intended

# Troubleshooting

### WebGroup Not Matching Traffic

- Verify the Domain field is populated in DCF logs
- Check if traffic is TLS-encrypted for HTTPS domains
- Confirm port/protocol settings match actual traffic

### Performance Issues

- Review rule ordering for efficiency
- Consolidate rules where possible
- Consider SmartGroup optimization

### Non-Web Traffic

- Use hostname SmartGroups for non-TLS/non-HTTP protocols (Controller 7.2 or greater)
- Configure CIDR-based alternatives for older versions
- Leverage DCF’s comprehensive protocol support

### Translation Errors

- Check input file format and completeness
- Verify Controller version compatibility

### DCF Configuration Issues

- Check resource naming conflicts
- Verify SmartGroup and WebGroup dependencies

## Related Topics

- Egress Control Filter Workflow
- Distributed Cloud Firewall Overview
- Web Groups Overview
- Smart Groups Overview