



New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, on page 1](#)

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 5.1(2g)

| Feature or Change | Description | Where Documented |
|---|---|--|
| <p>Allow All Traffic option is available for third-party firewalls and Azure network load balancers deployed as pass-through devices on a redirect-enabled service graph</p> | <p>Beginning with release 5.1(2g), the Allow All Traffic option is available for third-party firewalls and Azure network load balancers deployed as pass-through devices on a redirect-enabled service graph.</p> | <p>Deploying Layer 4 to Layer 7 Services</p> |
| <p>IP-based rules for inter-VRF contracts in the same VNet</p> | <p>Prior to release 5.1(2g), if two EPGs had a contract and were in the same VNet but belonged to different VRFs, ASG-based rules were used to enable communication between those hosted VRFs in that VNet.</p> <p>Beginning with release 5.1(2g), if two EPGs have a contract and are in the same VNet but belong to different VRFs, IP-based rules are now used to enable communication between those hosted VRFs in that VNet.</p> | <p>Security Groups</p> |

Table 2: New Features and Changed Behavior in Cisco APIC for Cisco APIC Release 5.1(2)

| Feature or Change | Description | Where Documented |
|---|--|---|
| Ability to map network security groups (NSGs) to subnets | Prior to release 5.1(2), NSGs were mapped to EPGs. Beginning with release 5.1(2), NSGs are now mapped to subnets instead of EPGs. | Configuring Cisco Cloud APIC Components |
| Support for express route gateway deployment | Beginning with release 5.1(2), support is now available for express route gateway deployment, where you can deploy an express route gateway in the hub VNet using redirect or without using redirect. | Express Route Gateway |
| Increase in number of CSRs supported | Beginning with release 5.1(2), the maximum number of CSRs supported per region increased from 4 to 8. | Changing the Number of CSRs |
| Cloud services support | Beginning with release 5.1(2), support is added to allow you to automate network segmentation and security policies for cloud native services and third-party services. | Configuring Cisco Cloud APIC Components |
| Support for private IP address to access a Cisco Cloud Services Router | Beginning with release 5.1(2), you can assign a private IP address to a Cisco cloud services router and Cisco Cloud APIC. | Private IP Address Support for Cisco Cloud APIC and Cisco Cloud Services Router |
| Restricting Access by Domains | Beginning with release 5.1(2), security has been enhanced for a user by restricting access using security domains and RBAC rules. | Restricting Access |
| Support for Third Party Load Balancers | Third party load balancer is a non-cloud native Layer 4 to Layer 7 load balancer. Beginning with release 5.1(2), you can use third party load balancers for Azure deployments. | Deploying Layer 4 to Layer 7 Services |
| Layer 4 to Layer 7 Service Redirect support for cloud native and third-party services | Prior to release 5.1(2), support was available for the Layer 4 to Layer 7 Service Redirect feature for Cisco Cloud APIC. Beginning with release 5.1(2), this is extended to also support cloud native and third-party services. | Deploying Layer 4 to Layer 7 Services |

| Feature or Change | Description | Where Documented |
|---|--|--|
| Support for Custom Naming for cloud resources | Beginning with release 5.1(2), during Layer 4 to Layer 7 service deployments, you can provide custom names to cloud resources, such as network load balancers, application load balancers and application security groups. | Cloud Resources Naming |

