



Cisco Umbrella Connector for iWAN DCA on ASR 1000

Cisco Umbrella Connector for iWAN DCA features allows direct cloud access to applications and provides sufficient bandwidth for the best application performance. It directs only specified cloud applications out to local internet and sends the remaining traffic to central site for further security inspection for malware detection.

- [Direct Cloud Access Overview, on page 1](#)
- [Direct Cloud Access Architecture, on page 1](#)
- [Direct Cloud Access Components, on page 2](#)
- [Restrictions for Direct Cloud Access, on page 3](#)
- [How to Configure Direct Cloud Access, on page 3](#)
- [Feature Information for Cisco Umbrella Connector for iWAN DCA on ASR 1000 , on page 5](#)

Direct Cloud Access Overview

iWAN Direct Cloud Access (DCA) allows local breakout direct internet access for trusted domains. For security inspection, DCA directs specified cloud applications to the internet and the remaining traffic is sent to headquarters over VPN tunnel for malware detection, Data Loss Protection (DLP), application level accesses and so on.

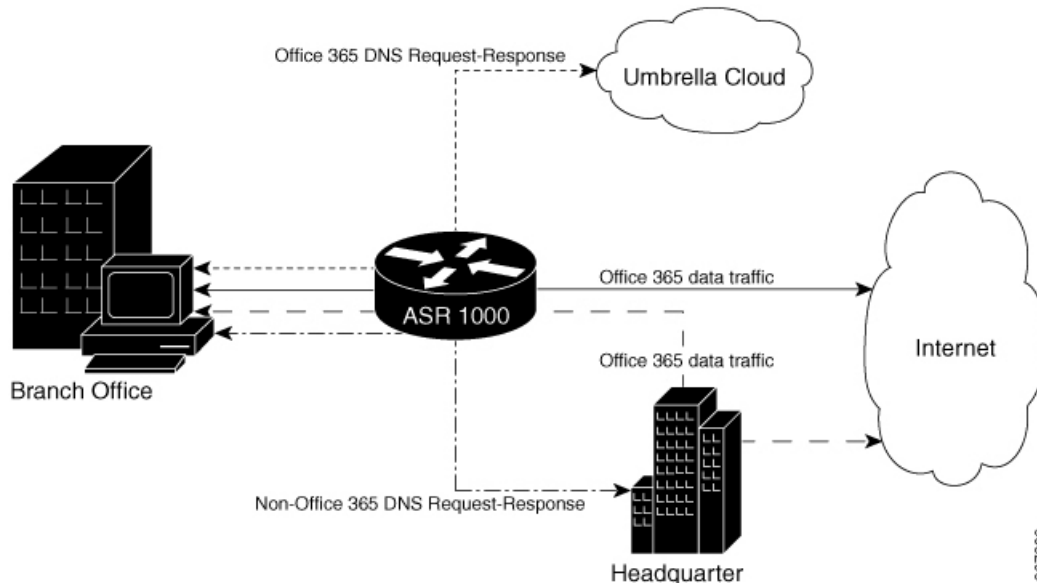
Umbrella Connector is a feature on ASR 1000 fixed platforms that intercepts DNS traffic and redirects it to Umbrella cloud for security inspection and policy application.

Direct Cloud Access Architecture

The Direct Cloud Access feature allows you to address any security concerns as the local break-out DNS traffic is first sent to Umbrella Cloud for inspection to block any malicious cloud application. You can gain more security with DCA when you connect to your cloud services through secure and private connections. Business processes run faster through direct network access to the major cloud providers. A traffic classification mechanism is required in order to achieve direct internet access for selected cloud applications. DNS method is used to classify the Cloud SaaS applications.

The following figure explains the functionality of DCA for Office 365 Cloud Application:

Figure 1: DCA for Office 365



To achieve DCA functionality:

- Classify all the cloud applications based on the DNS.
- Intercept DNS traffic and make decisions based on the classification.
 - If the traffic is from the interested cloud application then provide direct internet access. Ensure that security concerns are addressed for the breakout traffic.
 - If the traffic is not from the interesting cloud application then pass it to the Headquarter for further security inspection and processing.
- Route HTTP, HTTPS data traffic to internet or Headquarter depending on the above decision.

Direct Cloud Access Components

Direct Cloud Access feature has the following components:

- NBAR Classification
- Umbrella Connector
- Performance Routing

NBAR Classification

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications. NBAR uses several classification information metadata such as application name, ID, traffic class, business relevance, and so on.

For Direct Cloud Access feature, when NBAR recognizes the DNS traffic as belonging to cloud application, it attaches the traffic information to DNS packet so that the Umbrella Connector feature can extract and use the information.

Umbrella Connector

The Umbrella Connector is a component on ASR 1000 fixed platforms that intercepts DNS traffic and redirects it to Umbrella cloud for security inspection and policy application.

If an Umbrella connector is configured to allow local breakout for cloud applications, it redirects DNS traffic from selected cloud applications. To configure an Umbrella Connector, intercept DNS packet and look for NBAR classification result attached to the packet. If a match is found, the packet is sent to the Umbrella cloud else the packet is forwarded to the enterprise DNS resolver.

Performance Routing (PfR)

Performance Routing (PfR) component delivers intelligent path control for application-aware routing across the WAN. Once a DNS response is received, the data traffic (HTTP, HTTPS etc.) originating from the cloud application is provided direct internet access (local break-out) or is hauled back to the headquarter for further security inspection by the PfR component.

Restrictions for Direct Cloud Access

This section describes the limitations and restrictions for this feature:

- DCA is not supported for IPv6 addresses.
- DCA is not supported if the DNS traffic do not go through ASR 1000 (Umbrella interface where DCA is enabled).
- The Umbrella Connector does not provide local break-out support if applications directly access content, instead of using DNS resolution.
- DCA is not supported for DNS requests that do not have associated Network-Based Application Recognition result.
- From Umbrella Connector, local break out happens only at DNS level. Connector can not redirect non-DNS traffic.
- If an interface of the Umbrella Connector is configured to be in DCA mode, any local-domain bypass rules configured in the Umbrella global parameter-map will have no effect on DNS traffic through the interface.

How to Configure Direct Cloud Access

Configuring DCA involves two steps - defining a class map and a policy map.

Defining class-map

To define a match-all class map use the following command:

```
Router(config)# class-map match-all
```

The following is an example of defining a class map:

```
Router(config)# class-map match-all umbrella-direct-access
Router(config-cmap)# match protocol dns in-app-hierarchy
Router(config-cmap)# match protocol attribute application-set saas-apps office365
```

Defining policy-map

To define an Umbrella policy-map use the following command:

```
Router(config)# policy-map type umbrella
```

The following is an example of defining a umbrella policy map:

```
Router(config)# policy-map type umbrella umbrella-direct-access
Router(config-pmap)# class umbrella-direct-access
Router(config-pmap-c)# direct-cloud-access
```

Configuring the Cisco Umbrella Connector

To configure Cisco Umbrella Connector on the Cisco ASR 1000 fixed platforms:

- Configure a dummy token

The following configuration options are disabled and error message appears:

- DNSCrypt
- Local-domain
- Public-Key

Sample configuration:

```
enable
configure terminal
parameter-map type umbrella global
token AABBA59A0BDE1485C912AFE472952641001EEEC
exit
```

Configuring Umbrella Connector on Interface

To configure Umbrella Connector on an interface, use the following commands:

```
Device(config-if)# umbrella in
WORD Umbrella interface tag
direct-cloud-access Enable Direct Cloud Access
```

```
Router(config-if)# umbrella in direct-cloud-access
WORD Umbrella Direct Cloud Policy-map Name
```

```
Router(config-if)# umbrella
  in Umbrella In direction
  out Umbrella Out direction
```

The following is an example of interface command for Umbrella Connector with Direct Cloud Access but no policy enforcement at cloud.

```
Router(config)#int g0/0/0
Router(config-if)#umbrella in direct-cloud-access umbrella-direct-access
Router(config-if)#
```



Note For Cisco IOS XE Fuji Release 16.8.1, the policy enforcement at cloud is not supported.



Note `ip nbar protocol-discovery` interface command needs to be configured on the interfaces where umbrella in direct-cloud-access is configured for NBAR to classify DNS traffic.

Feature Information for Cisco Umbrella Connector for iWAN DCA on ASR 1000

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco Umbrella Connector for iWAN DCA on ASR 1000

Feature Name	Releases	Feature Information
Cisco Umbrella Connector for iWAN DCA on ASR 1000	Cisco IOS XE Fuji Release 16.8.1	Umbrella Connector Infra Enablement for DCA is supported for ASR 1000 fixed platforms.

