Cisco Domain Name System-Authoritative Source (DNS-AS)

At-A-Glance

The Role of DNS-AS

An increasing number of applications are being encrypted, which limits the effectiveness of deep-packet inspection technologies. Additionally, many applications are multiplexing their media streams, making these increasingly difficult to distinguish and treat differently.

Providing application metadata can address both of these challenges and enhance the utility of network QoS, security, performance routing and other policies.

The challenge thus becomes how to distribute such application metadata. For instance, if applications running on devices were to communicate such metadata to the network, this would require a phenomenal amount of cross-platform software development and maintenance.

However, DNS is not only a trusted source of information (as it is centrally administered, either by an enterprise or by a service provider), but is also flexible and extensible. As such, it may be used as an "authoritative source" of application metadata.

Thus, DNS-AS can provide the following value to enterprise networks:

- accurately classify encrypted applications
- identify thousands of applications (e.g. by leveraging OpenAppID)
- provide layer 7 visibility to network devices that have no deep-packet inspection capabilities
- reduce configuration complexity on network devices for classification
- require no software updates to endpoint devices, applications or operating systems

Consider two main DNS-AS use-cases:

- identifying ***internal*** applications
- identifying ***external*** applications

Identifying Internal Applications

As internal DNS servers are centrally administered by the enterprise IT department, these may be modified to include custom DNS TXT records that reflect application metadata, such as:

- application name
- application ID
- RFC 4594 traffic classification
- Business relevance, etc.

With this application metadata in place in the local DNS server database, then - for example - a network access switch with no deep-packet inspection capabilities can leverage DNS-AS to correctly classify and apply QoS (and other types of policies) to any internal application.

The DNS-AS operational steps to identify ***internal*** applications are:

1) A client requests a DNS Lookup, as shown in Figure 1.
2) The access switch examines the DNS request
3) The internal DNS Server returns a DNS response (A-Record).
4) The access switch makes ***its own*** DNS query and requests application metadata information, as shown in Figure 2.
5) The internal DNS Server returns a TXT Record with application metadata information.
6) The access switch maintains a Binding Table of application metadata.

At this point, the access switch can apply QoS policies or security or routing or other types policies to the flow.

Figure 1 DNS-AS Identification of Internal Applications-Steps 1 to 3

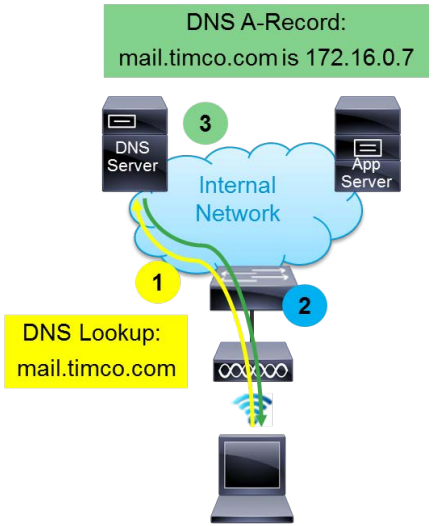
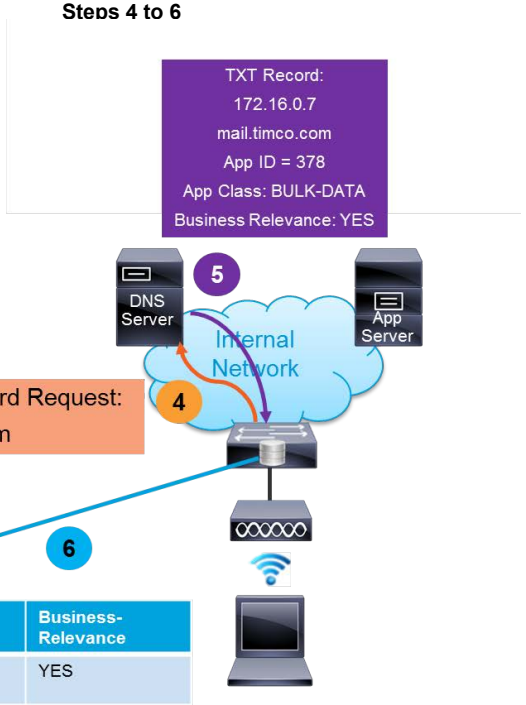


Figure 2 DNS-AS Identification of Internal Applications-Steps 4 to 6



IP Address	PTR	App-ID	App-Class	Business-Relevance
172.16.0.7	mail.timco.com	378	Bulk Data	YES

Identifying External Applications

A few additional steps are required when identifying external applications that have no application metadata in their DNS records. In this model, the internet edge router plays a key role as a DNS-AS Proxy.

The DNS-AS operational steps to identify ***external*** applications are:

1) A client requests a DNS Lookup, as shown in Figure 3.
2) The access switch examines the DNS request.
3) The external DNS Server returns a DNS response (A-Record).
4) The access switch makes ***its own*** DNS query and requests application metadata information (via a TXT record).
5) The external DNS Server has no TXT Record with application metadata.
6) The internet edge router notices the request for a TXT Record without response and:

A) On the first flow:

The internet edge router uses NBAR2 to perform deep-packet inspection to identify the flow and makes an entry in its local Binding Table.

B) On subsequent flows:

The internet edge router responds (as a DNS-Proxy) to the request for application metadata (by inserting a TXT Record into the DNS response from the external DNS server).

7) The access switch maintains a Binding Table of application metadata.

Figure 3 DNS-AS Identification of External Applications- Steps 1 to 5

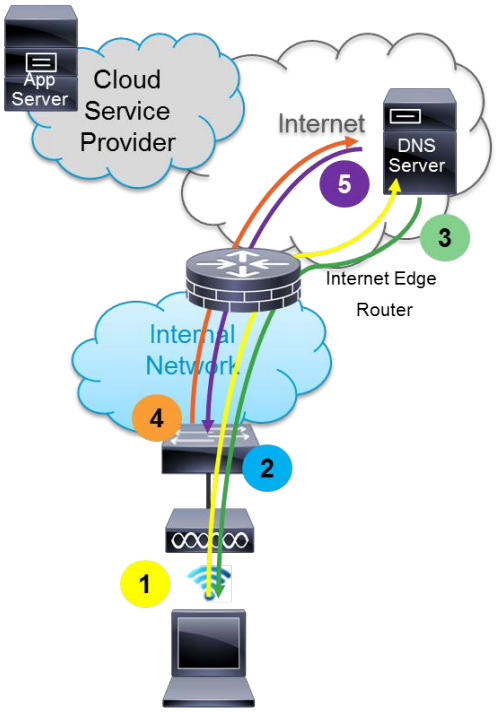


Figure 4 DNS-AS Identification of External Applications- Steps 6 and 7

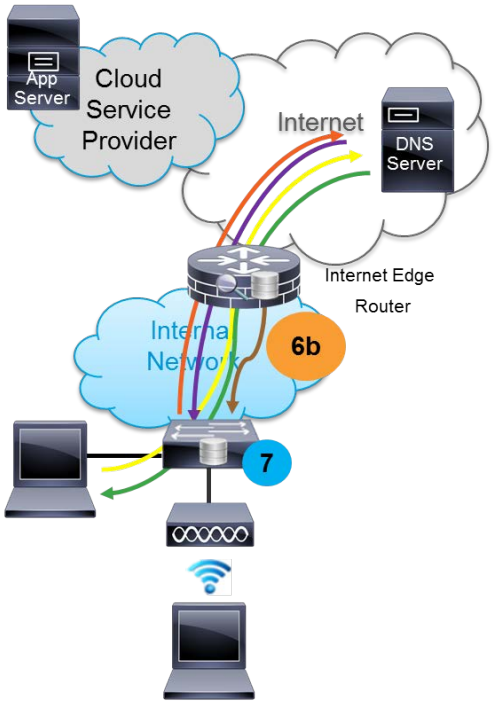
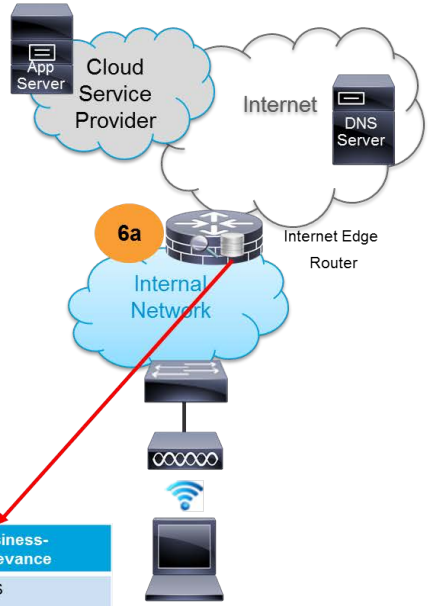


Figure 4 DNS-AS Identification of External Applications- Step 6a



IP Address	PTR	App-ID	App-Class	Business-Relevance
172.99.120.37	app.cloudco.com	3789	Transactional Data	YES

Copyright © 2015 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.