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

At-A-Glance

The Role of DNS-AS for QoS

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 policies. However, the method to distribute such metadata is in itself a challenge. 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, and as such may be prohibitive.

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.

As such, 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, these may be modified to include custom DNS TXT records that include 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 operational steps are outlined below.

1) A client requests a DNS Lookup, as shown in Figure 1.
2) The access switch intercepts and clones the DNS request
3) The internal DNS Server returns a DNS response (A-Record)
4) The access switch requests application metadata information (via a TXT record), 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 and 2

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

Dynamic Application-Based QoS Policies

A unique advantage that a controller-based architecture brings to the network is the ability to deploy dynamic QoS policies in a scalable and virtually instantaneous manner.

For example, APIC-EM can integrate via APIs to collaborative multimedia applications, including Cisco Jabber and Microsoft Lync (now Skype for Business). By means of this integration, QoS policies can be dynamically applied throughout the network to prioritize voice and video flows.

Such dynamic QoS policies allow for these applications to have their flows protected with QoS, regardless of whether: