Acceleration, Optimization, Security and the Data Center: Application Delivery's Next Step

Robin Layland
Layland Consulting
April 2009

The economic downturn is putting pressure on IT to reduce costs and to support other IT groups' cost-saving projects. Cost-saving projects such as consolidating branch office servers to the data center and increased collaboration using video and TelePresence are getting the green light. At the same time a down economy means increased security risk from professional criminals.

Application delivery is one of the chief tools to meet these challenges. Application Delivery solutions such as WOC (WAN Optimization Controllers) and the data center ADC (Application Delivery Controllers) reduce WAN and server costs. They can also play a key role in security. The problem is that there are some serious short-comings with the first generation of Application Delivery solutions that keep them from meeting their full potential.

Application Delivery needs to take the next evolutionary step. Application Delivery vendors need to provide an integrated solution that can classify, control and prioritize traffic at the application layer while also providing most, if not all, of the needed application services and security. The banner this second generation set of solutions flies under is Application Delivery Networking.

Application Delivery Networking

First, a little background on what exactly falls in the Application Delivery area. Application Delivery is an overlay on the existing packet routing/switching infrastructure. Switches and routers perform an excellent job of moving data around the network and providing security based on the TCP/IP layer and below (layers 1–4). Application delivery complements this packet-forwarding infrastructure by providing services at application layers within the network.

The services that Application Delivery provides fall within four broad categories.

- Application visibility: This is monitoring at the application layers 5 - 7. For example, application monitoring breaks Web/HTTP packets down by showing which Web application and the specific transaction type or function.
- Service Load Balancing (SLB): SLBs provide a single view of the application to the user while sending the traffic to multiple servers running the application and monitoring response time. It also provides monitoring of the health of the server to determine when there are problems.

- Application services: The best known of these are application acceleration for improving response time and WAN optimization for reducing bandwidth usage. Another example is performing DNS and DHCP services that were performed Microsoft servers that have been moved to the data center.
- Application level security: Examples of application security are Web, XML and application firewalls; data loss prevention; anti-virus; Secure Internet Gateways; Internet filters and malware prevention.

Application Delivery Networking (ADN) needs to evolve by integrating into a single solution the right mix of application visibility, application services, security and SLB. ADN solutions need two key abilities to make this evolution work.

Classification and Visibility

Application Delivery Networking solutions need to have very efficient Deep Packet Inspection (DPI) that can determine the message's application and its function along with who is sending and receiving the message and where they are located. For example, the classification needs to know if an HTTP XML message is a general inquiry or a transaction to buy the product. For example, the purchase request may need to go to specific XML gateway and firewall while the inquiry may not. A message from an outsider may require more security than from an internal user. The ability to make these types of distinctions is becoming more critical and requires the ADN solution to have a good classification engine.

Since the ADN is performing the classification it makes sense to have it tell operations what is going on in the network. Thus the ADN will increasingly take over the monitoring function that is traditionally performed in separate equipment. What is needed is for the ADN vendors to either develop the complex reporting and monitoring capability that existing monitors have or to partner with monitoring companies to include their solution as part of an integrated solution.

Controlling the Flow

The second ability that ADN solutions need is the ability to orchestrate the application services and security for a flow based on the application classifications and policy definitions. For example, when the Citrix desktop virtualization application sends a screen update all that is needed is for it to be accelerated, monitored and checked for security. If the same application is sending a print job to a local printer it should be run through a Data Loss Prevention security service to ensure that no sensitive data is being printed since it is easily carried out by anyone. If it is a web application then the data need to be sent to a web firewall and if it contains XML is may also need to be sent to an XML firewall.

Control is also important since the sequence in which a flow receives application services matters. Application acceleration significantly changes the message by substituting its own indicators for blocks of data when it performs dictionary

compression. After acceleration has done this it is impossible to perform application security. Thus the ADN has to determine the correct sequence to send the messages to the application services.

Performing QoS and bandwidth management is an integral part of controlling the traffic flow. Control combined with classification lets the ADN solution understand what traffic is important. While some peer-to-peer and video traffic is business related much comes from non-business applications. Control allows the ADN solution to filter out or move it to the back of the queue while moving latency-sensitive voice and video traffic to the front of the queue.

The ability to customize the ADN solution is important because each enterprise and application is different. ADNs should be judged on their built-in customization and how easy they make it for an enterprise to develop additional customization.

Encryption Problem

The ADN needs to also deal with the problem presented by encryption. It is hard to be against encrypting all traffic. The widespread deployment of SSL makes it easy, leading to increased encrypted traffic. The problem is that the application services and security both need to see the traffic in clear text. The current solution is for each appliance built for these services to perform “man-in-the-middle” de-encryption and then re-encrypt the traffic after it has done its task. All the appliances are all involved to some degree in key management and the more appliances involved the greater the risk something will go wrong. It is also very inefficient and adds to latency when each appliance to perform its own de- and re-encryption.

The solution is for the ADN to perform the de- and re-encryption. When a message comes in the ADN de-encrypts the message and then inspects the message to understand what it is. Once it knows this it can then run it through it customization and policy rules which tells it which services and security the messages needs and allow it to set the correct priority. It then runs the message through the required services and then re-encrypts the message.

An Integrated Solution

A simple way to think of the ADN is that it performs **E**ncryption services, **C**lassifies the messages, uses **C**ustomization to determine what is needed and then **C**ontrols where and in what order the messages goes to application services and security or **EC^3**.

No enterprise should buy an ADN solution that just provides EC^3. Integrated into any ADN solution should be the application services and security that an enterprise needs. Examples of these services include application acceleration, WAN optimization, monitoring, filtering, anti-virus, web/XML/application firewalls and SLB. The way to think of the ADN solution is that it is **EC^3+services**. A good rule is that 80% or more of the application services an enterprise needs should be part of the ADN. Having the ADN

perform the classification and directing the traffic to the right services internally has an additional benefit of reducing the time and cycles spent performing the DPI and the encryption process. Without an integrated solution each device performs the DPI, adding latency each time and wasting resources.

Not every application service can be part of an ADN. There are always new services being created or specialized services that comprise only a very small percentage of the enterprise's traffic. Network managers should make sure the ADN uses a standard protocol, such as ICAP, to communicate with the application services appliance. This will allow new services to be more easily integrated into the application delivery scheme.

Placement of an ADN

Where does the ADN solution need to be? It is needed wherever application delivery services and security are applied to the application traffic. That includes in the data center, at the branch office and remote locations and at the Internet boundary. It is also needed in each mobile employee's laptop when they are outside the enterprise. One day it will be needed in all smart devices such as phones and handheld devices.

Selecting an ADN solution

You can't buy a concept so when shopping what are ADN products called? In the data center they go by the Application Delivery Controller (ADC) name. ADCs are built on an SLB base and provide the EC^3 functions along with many of the application and security services needed for the data center. They are built as high throughput solutions that are required in the data center. Their application and security services are all aimed at the servers and are not appropriate for the network edges. The leading vendors include Cisco, Foundry, Citrix and F5 but there are several other smaller vendors. While improvements are still needed, they are well on the way to being complete ADN solutions for the data center.

What about for the other locations – the WAN edge in the data center; the Internet gateway; branch office and PC? Unlike ADC in the data center, branch office and PC ADNs must be deployed as a paired solution – one in branch office or PC and its counterpart on the WAN edge in the data center and internet edge. The application delivery solution commonly installed in these locations is a WOC. The WOC comes from the acceleration/optimization arena and thus provides that functionality along with performing the encryption service and some other application services. They are generally lacking in the classification, control, security and monitoring features. A few vendors are starting to make the transformation to next generation ADN solutions by adding the classification, control and application and security services. They come in two flavors. The first is a stand alone or appliance solution with Blue Coat being the leader. Blue Coat is combining its acceleration and security solution with control, classification and monitoring technology to provide the closest stand alone solution. The second flavor is to put the ADN inside a router with Cisco with its ISR router the leader.

What other vendors should you keep your eye on? It is possible that UTM with their full range of security services could add the EC^3 functionality along with acceleration and monitoring but none have done it yet. Riverbed is moves to add the visibility component to its product. Additionally, Riverbed and possibly other WOC vendors are heading towards the next gen ADN by adding the ability to run other vendors services in their equipment but they have not yet implemented the full EC^3 ability.

Using the WOC name for the branch office and Internet gateway ADN solution is not the best name going forward. The problem is that it primarily refers to the optimization function and if there are solutions from UTM or router vendors that provide an ADN solution they will unlikely use that name. The lack of a good name means in the short term managers will have to perform their own detective work since you can't search on one name and find all the potential players. One solution would be to call them all ADC. While they are both next generation ADN solutions their focus is too different to have any synergy by combining the two and more likely a combination would be a better solution. Thus using the same name for each solution will only lead to confusion. A possible name may be an Application Service Control (ASC) or WAN Application Delivery Controller (WADC). ASC recognizes that the solution does not have to just come from the acceleration/optimization camp. WADC recognizes the relationship to the data center ADC while emphasizing its focus on the WAN.

It is clear that application delivery needs to make the step up to an architected ADN solution that brings order to the application layer. Without it, network managers will be overwhelmed with application services and security devices that will drive up their cost and lead to poor service. Given the recent dramatic changes in the economic landscape, now more than ever, network managers should start demanding an architected application delivery networking approach from vendors and not settle for a collection of appliances.

About Robin Layland

Robin Layland (http://www.Layland.Com) is the president of Layland Consulting. He has been at the forefront of networking as consultant/analyst and as a leader in the corporate world. During each stage of his career he has worked at implementing new technology. As an industry analyst and president of Layland Consulting he has covered all aspects of networking from both the business and technical side. He has published over 100 articles in leading trade journals including Network World, Business Communication Review, Network Magazine and Data Communication and speaks frequently at industry events. In the 90's he was instrumental in moving corporations to IP. He spent a combined fifteen years at American Express and Travelers Insurance in a wide range of jobs including network architect, technical support, management, programming, performance analysis and capacity planning. Robin has published over 100 articles on network strategy and technology. He is a graduate of the University of North Carolina at Chapel Hill.