A new era in application delivery

Application Delivery Networking (ADN) tools provide integrated, cost-effective ways to improve application response time

By Robin Layland , Network World , 01/15/2009

The CIO sends out an e-mail to his IT managers saying that because of the economic downturn, networking costs must be reduced.

At the same time, cost saving projects such as consolidating branch office servers into the data center must be continued. End users are clamoring for improved response time to help increase productivity, no matter how much data the new Web applications or data center consolation creates.

The CIO also decides that there will be increased collaboration using telepresence and video conferencing in order to reduce the travel budget.

Adding to the network managers growing headache is that there is no let up when it comes to criminals and hackers attacking the network. The bad guys are now launching sophisticated and financially motivated attacks at the application layers with malware that is even harder to detect.

Related Content

But the CIO does not want to see a flood of new security devices each with their own installation and maintenance cost.

On top of all that, the corporate compliance office is calling for the network to play its part in ensuring that the enterprise is in compliance with corporate policies and regulatory mandates. If something is violating the new rules and regulations, then the network manger must either prevent it or at least report that it has happened. To top it off, operations has said that if you bring in one more new appliance, they will bar you from the data center and wiring closets.

What does it all add up to? The network is being asked to provide more services at the application layers.

There are several ways to address these issues. For example, WAN optimization and application acceleration tools provide a way to reduce response time, control bandwidth costs and support cost reduction projects, such as server consolidation.

Filtering and QoS allow network managers to control non-business traffic and plug the security holes they create.

A range of application security solutions from secure Internet gateways, Web/application firewalls, antivirus aimed at application layer threats, to data loss prevention are the way to stop hackers and criminals. Control and reporting at the application level along with many of the security solutions allow IT to meet compliance.

The problem is that implementing all these necessary but separate solutions will cause the number of appliances to grow, increasing cost and complexity.

What is needed is an integrated solution that can classify, prioritize and control traffic at the application layer while also providing most, if not all, of the needed application layers services. The banner this solution flies under is Application Delivery Networking.

Application Delivery Networking

Application delivery is an overlay on the existing packet forwarding infrastructure. Switches and routers, along with network devices such as network layer firewalls, 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 the application layers (5-7) within the network.

The services that application delivery provides fall within four groups.

1. The first is application visibility. This is monitoring at the application layers For example, application monitoring breaks Web/HTTP packets flowing over Port 80 down even further by showing which Web application and the specific transaction type.
2. The second set of functions is Service Load Balancing (SLB) and server health monitoring. 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.
3. The third grouping goes by two names, either application acceleration or WAN optimization. Its job is to improve response time and reduce bandwidth usage.
4. The last grouping is application level security. Examples of application security are Web and application firewalls, data loss prevention, secure Internet gateways, Internet filters and malware prevention.

Related Content

The key to application delivery meeting the new challenges is to integrate in a single solution the right mix of application visibility, acceleration, optimization, security and SLB. Two key features are needed to transform the current disorganized state of application delivery into Application Delivery Networking (ADN). The ADN solution needs to understand the applications as well as control the services. Only tight integration will provide this.

Classification and visibility

The first building block of an ADN solution is good application classification. The application delivery solution needs 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 the HTTP XML message for the company's product catalog is a general inquiry or a transaction to buy the product.

The purchase request may need to go to a specific XML gateway and firewall while the inquiry may not. The ability to make these types of distinctions is becoming more critical and requires that the ADN solution have good classification.

Performing the classification in the application delivery solution has the benefit of reducing the time and cycles spent performing the DPI. The old way had each device performing the DPI, adding latency each time.

An important issue for network managers to consider is how often the vendor updates their classification engine. The reason frequent updates are needed is that new applications are being invented constantly and existing applications are constantly changing. Regular updates allow the solution to keep pace with the changes and are especially important since many of the new applications can adversely impact the performance of the enterprise's network.

The flip side of classification is visibility and monitoring. If a device can classify application traffic, it is in the ideal position to perform the monitoring function, reporting to network operations what is happening across the network. Combining monitoring with the ADN solution overcomes a problem with the current approach of performing the monitoring in separate equipment.

For example, let's say a message needs to run through a Web/application firewall, data loss prevention appliance and then an application specific XML gateway. If there is a complaint about response time, it is critical to know how much latency each of these appliances added.

A traditional monitor would not know the answer because it sees the message only once. The ADN solution knows how much latency each service added, giving a clearer picture of what is happening to network operations.

Controlling the flow

The second building block of an ADN solution is the ability to control the acceleration, security or other application services that are needed, based on the application classification and policy definition. The ADN solution knows which services are needed and can vary the services based on the application and even the transaction type, orchestrating the services the application flow receives.

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 service to ensure that no sensitive data is being printed, since it is easily carried out by anyone.

Controlling the traffic flow is important to guarantee that voice traffic is treated correctly. The ADN solution needs to prioritize voice traffic at the front of the queues for application services. Additionally it needs to understand voice traffic and know not to accelerate it, since there is nothing acceleration can do for voice traffic that is already highly compressed.

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. It also allows more security to be applied to the non-business traffic.

An ADN solution may not have integrated all the application services an enterprise needs, requiring the enterprise to use an application service appliance from another vendor. For example, if the ADN solution sends an e-mail with an attachment to a data loss prevention appliance, the DLP decides whether the e-mail needs to be stopped or can be forwarded with some encryption. It then communicates what to do with the message to the ADN solution, using ICAP.

Network managers should look for an ADN vendor that certifies that the communication between the ADN solution and their application service works.

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

A good feature is to provide role based management where different application groups can provide customization for their application, while the ADN solution ensures that they don't interfere with each other.

ADN in the enterprise

ADN with application classification and control will allow enterprises to gain control of the applications flowing over the network. Application visibility and control allows enterprises to meet the regulatory requirements while allowing them to know what applications are running across the network. This will allow enterprises to provide effective security, control cost and provide better service. Non-business applications will not overrun the network and mission critical applications will be protected.

Where does the ADN solution need to be? It is needed wherever application delivery services and security are applied to the application traffic. It is needed in the data center, 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.

What application services need to be in an ADN solution? Application visibility is a must since it is needed for efficient classification and thus application monitoring should come with the package. Network managers should always consider a solution that has integrated as many application services as they need in the same box.

There are several reasons why an integrated ADN is the best approach. The first is it reduces the number of appliances that need to be deployed and maintained, reducing operation cost. An integrated solution also can reduce latency since the time it takes a specialized appliance to process the packet and perform its own deep packet inspection is eliminated.

It also eliminates the communication that has to happen between the appliance and the ADN, reducing both the time it takes and eliminating potential problems. Policy management is simplified because the technical staff only has to create the policies for the ADN and not for additional appliances.

Having an integrated ADN that performs traffic filtering can save time and processing by the other appliance services by eliminating traffic before it reaches them. Thus as a general rule the more application services that are packaged within the ADN solution the more efficient it will be.

What product name does the ADN solution point go by? Application Delivery Controller (ADC) is a good candidate, but the problem is that this name is already taken and associated with the server load balancers in the data center. ADCs can function as the ADN solution for the data center but currently they are highly optimized for the data center and are not appropriate for the network edges. Therefore we need a name for the ADN solution outside the data center and a good candidate might be the Application Services Controller (ASC). While enterprises would prefer one solution for all locations this is not realistic in the foreseeable future.

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 point products.

Layland is head of Layland Consulting. He can be reached at robin@layland.com

All contents copyright 1995-2009 Network World, Inc. http://www.networkworld.com