Application Control

Background

In the past five years, the modern computing landscape has changed so extensively that IT Network Administrators find themselves struggling to ensure their network infrastructures can accommodate. Trends and shifts in this new computing paradigm include:

- Wide-scale adoption of mobile smartphone/tablet BYOD (Bring Your Own Device) devices stressing WiFi networks.
- The rise of cloud/web based applications that share both business and personal information between the cloud and the enterprises.
- The reliance on streaming media/VoIP (Voice over IP) applications to conduct essential business tasks such as remote conferencing and telephone calls.
- The explosive growth of social media as a means of connecting people and businesses, as well as a means of playing games.
- Broad adoption of application that use dynamic ports or port hop, otherwise making these applications difficult to manage.

For the IT Network Administrator, these trends have manifested themselves in two unique sets of challenges:

1. Quality of Experience – Preserving network bandwidth for mission critical applications such as video conferencing applications (WebEx™, GotoMeeting™, etc.) and telephony applications (VoIP phones) is essential to ensuring that these technologies deliver on their promise of a better-connected workforce. Conversely, ensuring that applications that stream media for more entertainment related purposes (Netflix™, YouTube™, Youku™, etc.) are not overly consuming network bandwidth is critical in maintaining business continuity.

2. Security – Web file storage and collaboration applications such as Dropbox™, Box™, and others make connecting employees and sharing ideas across multiple geographic regions a facile experience, but organizations typically standardize on one such service. If the organization's internal assets are vulnerable to security risks, then how does the IT Network Administrator ensure that multiple such services are not used to exchange personal data with the organization, which may not be secure?

Peer-to-Peer file sharing methods such as BitTorrent also present themselves as a security risk – not only through the possibility of infected files but also through liability risk. Organizations often ask themselves if they should facilitate potentially illegal file-sharing of copyrighted materials such as music and videos. Such activities can expose the organization to reputational and liability damage.

Further, social media applications such as Facebook™, Twitter™, Weibo, Instagram™ and others all facilitate ease of social connectivity, but it is often desirable to ensure that these are used for productive purposes. For instance, social media can be used by the organization as a way to connect with its customers and constituency, but it can also be used as a platform to play games such as Zynga™ games and the like.

Description

The ability to have visibility into the applications being run on the network as well as control of these applications gives Network IT administrators the tools to manage the quality of experience and security issues that come with modern computing.

However, it is useful to ask—how can network equipment classify and control application traffic?

Traditional attempts at classifying applications have done so using the at the lower layers of the network stack, relying on packet identification using the 5-tuple concept, i.e. source IP, destination IP, source port, destination port, and protocol. However, this traditional 5-tuple technique dates back to the late 1980s when firewalls were first conceived, as firewalls were the first types of networking equipment to use the 5-tuple technique.
However, modern network traffic has evolved to the point where it is nearly impossible for this technique to work. Factors such as ease of development, reliability, and performance have caused a significant number of network applications to migrate to common ports and protocols, specifically, HTTP (on port 80) and HTTPS (on port 443). For example, both Facebook™ traffic and YouTube™ traffic are commonly run over port 80 (HTTP), and so the conventional 5-tuple technique would not differentiate between the two.

To overcome these network management and security issues, visibility is needed at the application layer to determine what the application is and who is using it. Since it is no longer possible to classify application traffic simply based on the TCP or UDP port number, one must look deeper into the packet, at the application, presentation, and session layers of the OSI Data Model. The terms DPI (Deep Packet Inspection) and L7 (Layer 7) Classification refer to these three top layers of the OSI Data Model – the Application Layer.

Application attributes specific to certain applications can be extracted data stream using L7 DPI Application Classification. For instance, a VoIP data stream will include caller information as well as codec information. An email data stream includes attributes such as source/destination email address, as well as mail servers and mail protocols (IMAP, POP3, etc.)

The Xirrus Application Control platform uses specific L7 DPI techniques including:

• Surgical Pattern Matching
• Deep Protocol Dissection
• Semantic and Conversational Awareness
• Behavioral Analysis
• Flow Registration and Association

These techniques allow to recognize up 900+ individual applications and thousands more sub applications that utilize the same application core. Applications are classified into 15 different subcategories: Collaboration, Games, Remote Access, VPN, Database, Mail, Networking, Monitoring, Social, Web, File Transfer, Messaging, Proxy, Streaming and Xirrus.

Further, SSL traffic is accurately classified by the Xirrus Application Control Platform as TLS/SSL handshakes and certificate exchanges are first validated to ensure the traffic is not masquerading as SSL traffic—a common trait of anonymizing proxies and applications such as Skype™. Such traffic is then analyzed to identify the underlying service/site which allows for detection of popular, secure networked applications such as Salesforce, Gmail, Linkedin, etc.

Theory of Operation

Traditionally, gateway security appliances located at the Internet edge and various other demarcation points in the network infrastructure have been employed to classify and control application traffic. The challenges with this approach are several fold:

• Excessive consumption of internal network resources and bandwidth from applications running at the network edge by hosts, as application classification and control only occurs at the network demarcation point.
• The potential for security risks to spread from hosts on the same network/VLAN to another, again because application classification and control occur at the network demarcation point.
• The requirement of high performance, high cost hardware to keep up with the high data rates at the network demarcation point which results from the aggregation of the network traffic from many hosts.

As a result, organizations are realizing it is most beneficial to enforce security and traffic policies at the network edge – the ingress point where traffic enters the network from hosts. After appropriate classification of networking traffic, the ideal manners in which to control this application traffic include:

• Traffic shaping techniques
• Quality of Service differentiation
• Outright allow/deny

Using Xirrus Array OS 6.3, the IT Network Administrator can use the Xirrus Application Control platform to provide visibility and control against applications at the Wireless LAN access layer. By leveraging the distributed Array architecture that Xirrus provides with processing power and intelligence in each Array, IT Network Administrators can do so in a cost effective yet highly scalable manner.
Configuration

Application Control monitoring is enabled by default. To turn it on or off, go into the Array Web Management Interface (WMI) and select configuration, filters, filter lists and Application Control enabled or disabled, highlighted with the arrow below.

Once this is done it should be immediately apparent what kind of application traffic is on the network. To view Application Control statistics, through the Array WMI, select Application Control. This will display the screen shown below, which has pie charts for application traffic and application category, for both stations connected to the Array and also the Array traffic.

The color coding reflects the risk rating assigned for the applications and categories. In the above screen shot the Station Traffic views have been sorted by the Risk column, where 5 is higher risk from a security perspective than 1. The productivity index reflects whether the application is business related, such as a database application, or more typically a personal use application, such as Facebook. To view Application information for a specific station, select the station from the pulldown, as shown below.
Once Application Control is enabled, it is possible to select applications and application categories when creating filters, along with the other filter criteria. Below is the configuration screen for filters.
Application Examples

There are many ways that application control may be used by a network administrator. In many organizations it is useful to understand how much network traffic fits in which category to help prioritize expenditures and also to determine policies on network use.

Example 1 – Deprioritizing Benign Non-Critical Traffic

For some organizations, their concern is ensuring that the network is prioritized for business purposes, and so they may leverage Application Control to prioritize which application categories receive ample wireless bandwidth.

In the following scenario, it is evident that there is an excessive amount of YouTube traffic on this Array, which could be seriously impacting the performance of other business applications.

In this scenario, it may be desired to change the QoS for YouTube to ensure it is a lower priority than for example database access. In the screenshot below one can see that the QoS for YouTube traffic has been set to priority 1, allowing YouTube traffic to pass, but at a lower priority than other traffic.
Example 2 – Prioritizing Mission Critical Traffic

Other organizations may find themselves needing to prioritize applications for which the business is highly dependent. Conferencing applications require significant bandwidth as such applications include elements of real time audio, video, application sharing, and screen scraping. In the scenario below, WebEx represents nearly 20% of the network traffic of the organization:

As WebEx is typically used for business conferencing and sales purposes, it is desirable in this scenario to ensure a positive user experience. To set the QoS policy for WebEx, one must create a WebEx filter and set the QoS policy appropriately as below:

In the filter list, one can see that in order to maintain a positive user experience for WebEx, bandwidth hungry peer-to-peer file sharing applications such as Bittorent have been blocked. Further, YouTube traffic, which is largely consumptive in nature and may be used for business or entertainment purposes alike, has been assigned a QoS value 1, reflective of its less important nature. WebEx traffic has been assigned the highest QoS value of 2, reflective of its important business function.
Example 3 – Blocking Insecure Traffic

As all organizations are different, productivity and security concerns may often be driving the need to utilize Application Control to mitigate such concerns. For instance, Internet gaming applications can pose significant risks to both workforce productivity as well as to the integrity of the computing environment through malware and spyware infections, as such games often require the installation of non-business approved software. Businesses that are acutely sensitized to malware and spyware risks are also often again sensitized to BitTorrent use, as peer-to-peer file and software sharing are often the source of such infections. In the following example, one can see the gaming platform y8 is being used extensively.

Consequently, it is desired in this scenario to block Internet gaming as well as BitTorrent. To do so requires one to add the appropriate filters to the filter list being applied to the SSID. In this example, the SSID used is PM-Lab and the filter list is App-Filters as shown below:
In order to add/modify the filters in the filter list, one selects filter management and the filter list to be managed. A new filter is then created, and an application or application category is then selected. In the example below, the application selected is Bittorrent.

This results in a filter entry as shown below.

In this example, logging has been enabled so that dropped traffic can be seen in the Array log file.

The final filter list then results in the example below:

wherein Bittorent and the games application category is explicitly blocked (type=deny). The traffic that is dropped is logged. The Collaboration and Database Application categories are treated with a higher QoS priority of 2, while Streaming media is treated with a lower QoS of 1. Social Networking and other File Transfer Applications are treated with a QoS of 0, which is essentially best effort, lowest priority.
Tips and Recommendations

Before enforcing application policies, it is important to clearly define and educate users on the organization’s policy on network usage. Further, it is also helpful to gain a working knowledge of the use cases of different organizational functions so as not to misconstrue normal business activity as personal activity or vice versa.

For example, one must be careful not to conflate business oriented social media use with personal social media use. YouTube, Facebook, Instagram, and Pinterest all have legitimate business uses as well as personal uses! One recommended approach is to first use Application Control to monitor what applications are being used and by whom. With this information, the network administrator is in a position to verify if the use is personal or business based, and to then work with an organization’s management to determine what policies they want to apply to those applications being used.

Special consideration should be given to guest access and the guest access policies. In addition, it may be necessary to increase the level of security for wireless guest access. For example, if the current guest access is open or just based on a pre-shared key, employees could bypass policies by connecting their personal devices to the guest network. Restricting what applications guests use may not be acceptable depending on guest policy, especially as they may have legitimate reasons to access certain applications.

About Xirrus

Xirrus is the leader in high performance wireless networking. The enterprise-grade Xirrus Wi-Fi Array enables wireless connectivity for small businesses to the Fortune 500. Headquartered in Thousand Oaks, CA, Xirrus is a privately held company that designs and manufactures its family of wireless products in the USA.