Prioritize Access to Business Applications
With Cyberoam’s Application Visibility & Control
Contents

Executive Summary ................................................................................................................. 2
Identifying APPLICATIONS to Manage them ........................................................................ 3
Identifying USERS behind Applications ............................................................................... 3
Managing Application QoS in Organizations ...................................................................... 3
Cyberoam Unified Threat Management: ............................................................................. 4
  - Application Visibility- Application Security
  - Managing Bandwidth with Policy, User, Time-based Controls
  - Maximizing Network Security and Productivity
Conclusion ................................................................................................................................. 5
Executive Summary

The story of application evolution in organizations is the story of evolution of communication, entertainment and collaboration over the World Wide Web. What started off as a means of instant communication via email and Instant Messengers, was quickly followed with entertainment in the form of bandwidth-hungry gaming, chat, audio and video downloads. Collaboration tools like Microsoft Sharepoint and Google Docs moved to WebEx, Adobe Connect, GoToMeeting solutions, bringing people together and carrying sales and marketing pitches to internal/external audience, encouraging collaborative working.

Applications are a mix of personal and professional applications that are taking the web and hence organizations by storm. For example, applications like SaaS, SalesForce, and NetSuite’s ERP are purely business applications that are rich in business intelligence. However, socio-buisness applications like Facebook, Twitter, YouTube, and Instant Messengers, while making personal life more meaningful, are turning out to be business-enablers too. Nevertheless, uncontrolled and unmonitored use of socio-business applications can become a significant threat to security and productivity in organizations.

Organizations are quickly waking up to the fact that access to applications must be controlled not just for the vast number of vulnerabilities they introduce to the network, but also for the excessive mis-use of bandwidth they consume and the considerable loss of productivity. With employees indulging in non-business application usage with gaming, audio-video downloads through peer-to-peer networks like Kazaa, and more, business-critical applications are forced to deal with insufficient bandwidth, resulting in poor Application QoS and frustrated users. The solution is to identify and control access to specific applications so as to achieve optimal bandwidth utilization for business-critical applications.
Identifying APPLICATIONS to Manage them

Traditionally, it didn’t matter which application was going through the network, because applications followed the port-protocol combination. All HTTP applications followed port 80. All SSL applications followed port 443.

Things changed when applications rose exponentially in number and variety. There were business-critical applications like VoIP, SAP and Salesforce; socio-business applications like Facebook and Gmail; non-critical applications like YouTube and iTunes; and finally the undesirable applications like BitTorrent, gaming applications and more. Some chose not to flow through traditional ports for the sake of greater efficiency and success in packet transit, while some chose this route to bypass the limitations of the firewall. The day of port hopping arrived. Not to mention proxy avoidance sites and software like ByPassU, YouMask, UltraSurf that bypass traditional firewalls, allowing users to surf unfettered on the World Wide Web.

As a result, sophisticated application-level threats started hitting organizational networks. The already-scarce bandwidth was consumed by a small group of applications, notwithstanding their little use to the business. Business-critical applications like VoIP suffered, in other words, business suffered! The need for applications visibility became urgent and foremost!

Identifying USERS behind Applications

Back then, it didn’t seem to matter who received the traffic in the organization as long as the destination or source address was acceptable because few people had access to Internet. Things changed when Internet access became ubiquitous across the organization - not everyone required access to every application. While Salesforce, Microsoft Sharepoint or Google Docs would always require priority in access, and iTunes would be a straightforward decision of limited or no availability, things started getting vague when one thought of social media applications like You Tube, LinkedIn and file transfers over Instant Messengers. This is where recognition of the User started becoming significant.

Managing Application QoS in Organizations

As QoS takes on a more prominent role throughout a wide array of businesses, organizations require greater controls over applications, especially the socio-business applications like Facebook that challenge business-critical applications for bandwidth. Facebook began as a social media application and is finding an increasing number of users for its chat and mail facility. However, creating communities of partners or customers over Facebook has become an integral part of marketing and communication too for organizations. Organizations hence needed a shift from their traditional goal of “block the bad stuff” to a new goal of “enable the good stuff” to meet the bandwidth challenge.

Besides, as long as critical applications were residing within the network, simple rules that blocked black and even grey applications seemed to do the job with a fair degree of efficiency. But with SaaS, collaboration and Cloud taking the traditionally internal applications outside the network, the bitter fight for bandwidth has already arrived. These applications would be up there in the cloud jostling for users’ time, space and bandwidth with external applications.
Given the bandwidth-hungry nature of applications like audio, video, conferencing and certain collaboration functions, organizations would be perpetually short of bandwidth if their firewalls were unable to identify applications and users. So the real challenge isn’t just of identifying applications as they come into the organizations, but also of optimizing bandwidth as per the need for an application by users to ensure Application QoS within organizations.

Cyberoam Unified Threat Management

Application Visibility - Application Security
Cyberoam offers visibility over Layer 7 (the application layer) and Layer 8 (the user layer) to give complete information on which applications are accessed within the organization by which user, irrespective of their ports and protocols. Organizations get full transparency over applications entering their networks using standard Port 80, 443, non-standard ports, port hopping or tunneling through encrypted SSL traffic – indicating application-layer threats that can be blocked using firewall policies, right at the network perimeter to ensure Application Security.
Managing Bandwidth with Policy, User, Time-based Controls
Cyberoam implements application-based Bandwidth Management to accelerate business-critical applications, stagger non-critical applications, selectively accelerate socio-business applications and block undesirable or malware-infected applications based on network policy, user and time. Business-critical applications can be given maximum bandwidth. In the same way, undesirable applications can be assigned zero bandwidth, blocking their entry into the organization.

Organizations can group applications as per their requirements into business-critical, entertainment, communication, collaboration and control access through Firewall policies. Users can be distinguished based on hierarchy or their roles, business and recreational users, or through specific requirements of a user or department. For applications that are bandwidth-critical but not time-critical, limiting their access to certain times of the day eliminates the strain on bandwidth. YouTube access can be defined with a maximum bandwidth availability beyond which it would be unable to use the organization’s bandwidth. However, specific non-working hours can be pre-defined for higher bandwidth availability to this non-critical application.

Maximizing Network Security & Productivity
Efficiencies in managing applications mitigate internal threats like misuse of corporate resources and time by employees. With Cyberoam, organizations can provide meaningful access of applications to users. This results in balanced bandwidth usage within organizations that supports QoS of business-critical applications. Cyberoam’s user-based reports, as opposed to IP-based reports of other solutions, provide at-a-glance information to track employees’ application usage, enabling organizations to minimize the drain on productivity through Fantasy Football, gaming, and more.

Conclusion:
Cyberoam Unified Threat Management appliances offer visibility and control over applications and users, irrespective of the application origin. It helps organizations in application QoS by managing the complex matrix of applications, users and time requirements to defuse the fight for bandwidth by applications, even before it begins.

Cyberoam UTM appliances take security deep down to the user level with Cyberoam’s Layer 8 Technology. The Cyberoam Firewall can seamlessly integrate with Active Directory that ties users to Cyberoam’s security, no matter where they move within the network. This takes a deeper meaning in context of Cyberoam’s Security, Compliance and Employee reports that give user-activity information in real-time to organizations.