Firewalls Aren't Just About Security

Cloud Applications Force Firewalls to Enable Productivity

Cyberoam®

www.cyberoam.com

Executive Summary

The advent of cloud computing brings in competition for bandwidth with internal applications moving to the cloud. Organizations cannot deploy new solutions for each new challenge thrown up by the cloud. The solution lies in what firewalls *do vs* what firewalls *can do*.

If we stopped looking at firewalls or UTMs as just security solutions that block bad traffic, we would be in a position to turn them into productivity solutions that function as business enablers. Making them operate at the Application Layer 7 and the User Layer 8 enables them to view application traffic not with an outdated port-protocol combination but as a dynamic function which they can then enable effectively.

Using the 4 Elements of who (user), which (application), when (time) and what (bandwidth), firewalls can introduce layer 7 and 8 visibility and control based on time and bandwidth requirements to lower the peaks and troughs in the bandwidth demand, give priority to white applications, block black applications, yet allow intelligent access to grey applications. With this, they enhance productivity, yet create an attractive work place.

Contents

While current industry focus rests on potential security challenges that Cloud introduces, productivity challenges are bound to hit organizations sooner. Barring bandwidth critical applications like VoIP and video conferencing, organizations are not geared to delivering assured application access to users.

Introduction

With the advent of the cloud, tradition doesn't hold much good anymore. Applications *traditionally* residing "inside" the network would be "outside" on the cloud, competing for the first time with external applications for bandwidth. *Traditional* ways of looking at firewalls limit organizations' ability to meet the fight for bandwidth brought on by the movement of applications to the cloud.

Managing access to applications is a complex affair already given the vast multitude of applications, their availability over the Web and the acceptance of SaaS (Software as a Service) as mainstream applications.

Cloud computing adds to this complexity in application access and control. By blurring the hitherto clear distinction between internal applications hosted within organizations' data centers and external applications available over the World Wide Web, the challenge of managing application access and control becomes far more complex than is garnering attention.

While current industry focus rests on potential security challenges that Cloud introduces, productivity challenges are bound to hit organizations sooner. Barring bandwidth critical applications like VoIP and video conferencing, organizations are not geared to delivering assured application access to users.

Yet, organizations cannot afford to increase the number of solutions indiscriminately to handle cloud challenges. The solution to the task of assured Application-QoS (Quality of Service) lies in firewalls and UTMs (Unified Threat Management)[1]. They need to move out of their traditional siloed thinking that fit the era of perimetered networks which are fast disappearing as far as applications are concerned. Firewalls need to open themselves to solve emerging requirements by going beyond straight forward *allow-disallow application* rules to provide granular controls that apply QoS by applications and users, which they had not considered before.

The current approach of ignoring the Application Layer 7 and the User Layer 8 by most firewalls or the decoupling of these 2 layers with a few firewalls handling Layer 7 and IAM (Identity and Access Management) solutions handling Layer 8 is bound to make organizations buckle under bandwidth and the resultant productivity pressures.

A new approach within the firewall that comprehensively covers the 4 elements - Application, User, Time and Bandwidth - which can easily be handled through Layer 7-Layer 8 visibility and controls delivers the required productivity by moving firewalls beyond their traditional security-focused approach.

[1] For the purpose of this white paper, the term 'firewall' would be used to refer to both firewalls and unified threat management solutions since firewalls are an integral feature of UTMs.

Applications while making business life simpler and personal life seemingly more meaningful, bring with them a significant threat to security and productivity.

The Cloud Age Challenge of Applications

The history of application usage is the history of communication, knowledge expansion, entertainment and collaboration over the World Wide Web.

Communication & Knowledge Expansion

What started off as a means of instant communication via email, moved into knowledge expansion with the quantum rise in sites that added data and more data on a daily basis. So far so good, even though an increasing number of people in the organization were being given Internet access. To make matters fairly simple, applications followed a predictable pattern of port-protocol usage.

Entertainment

With millions of people finding themselves online, entertainment followed quickly with bandwidth-hungry gaming, chat, audio and video downloads. Productivity losses mounted in two ways. While some employees indulged in non-business application usage with gaming, audio-video downloads through peer-to-peer networks like Kazaa and more, business-critical applications suffered for want of sufficient bandwidth.

At this point, organizations woke up to the fact that access to applications must be controlled not just for the vast number of vulnerabilities they opened the network to, but also for the terabytes of bandwidth they consumed and the quantum of productivity loss this entailed. Port blurring now began in earnest, adding to the complexity of application control.

Collaboration

Collaboration followed close on the heels of what began quietly as file sharing mechanisms to overcome the limitation of email in transferring heavy files. While Microsoft Sharepoint, Google Docs are a couple of examples for collaboration tools, WebEx, Adobe Connect, GoToMeeting solutions were already bringing people together, carrying sales and marketing pitches to internal collaborative working and communications.

Collaboration is on a high year-on-year rise in adoption, riding on the wave of ease-of-transfer, speed in work, collaboration across globally distributed resources and reduced costs of travel and transportation.

Today, it's a mixed bag of personal, professional, audio, video, collaborative, entertainment, instant communication applications that are taking the web and hence organizations by storm. Driven Top-down in case of SaaS applications like SalesForce, NetSuite's ERP, Birst with its Business Intelligence as well as Bottom-up with Facebook, Twitter, You Tube, Instant Messengers, these applications while making business life simpler and personal life seemingly more meaningful, bring with them a significant threat to security and productivity.

A change in the way firewalls handle organizational requirements, shifting from their traditional goal of *Block the Bad Stuff*, to a new goal of *Enable the Good Stuff* can meet the current challenge.

Cloud Computing

Enter cloud computing - today we stand at a point where significant change is happening in the way we compute, collaborate, store and retrieve data. What was once within the network, is now moving rapidly outside the perimeter.

SaaS has gained increasing mainstream acceptance. Cloud increases this outward application mobility multi-fold with most or all internal applications set to move outside the perimeter. This phenomenon critically impacts bandwidth consumption in organizations.

The ready adoption, smooth transition to cloud computing and its success also depends to a large extent on the ease and ready access to hosted applications and data which will now begin to compete with existing 'external' applications.

Organizations will struggle to balance the need for the 3 categories of applications: Business or White Applications; Non-Business or Black Applications and; Socio-Business or Grey Applications.

In the absence of clear guidelines, critical, white applications will end up competing for bandwidth with non-critical black or grey applications at all times of the day. Work suffers and the very productivity which cloud is meant to enhance declines. Costs rise as bandwidth consumption hits the roof.

A change in the way firewalls handle organizational requirements, shifting from their traditional goal of *Block the Bad Stuff* to a new goal of *Enable the Good Stuff* can meet this challenge.

With applications multiplying, 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.

Firewalls Aren't Just About Security

Traditional firewalls paid attention to the source and destination address, the ports and protocols. It didn't seem to matter which packet was entering or leaving the network, as long as it met the rules created for these parameters, because applications themselves followed the port-protocol combination.

Further, 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 applications rose exponentially in number and variety this required controlling which applications entered the organization. Things changed further when Internet access became ubiquitous across the organization - not everyone required access to every application. Hence the user became important to firewalls.

Of critical importance is the fact that firewalls could no longer expect applications to follow a standard port-protocol combination. Earlier, all HTTP applications had followed port 80. All SSL applications followed port 443.

With applications multiplying, 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.

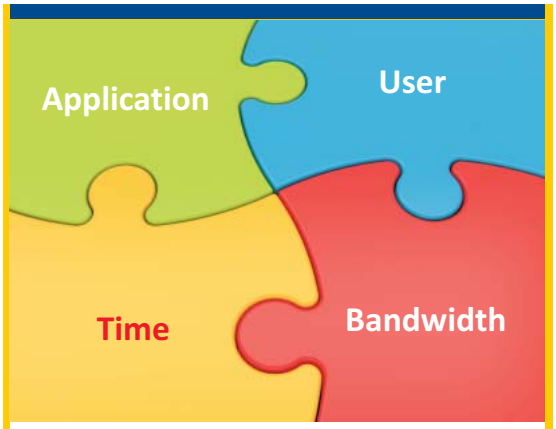
Not to mention proxy avoidance sites and software like ByPassU, YouMask, UltraSurf that bypass traditional firewalls, allowing users to surf unfettered on the World Wide Web.

But with critical applications residing within the network, simple rules that blocked black and even grey applications seemed to do the job with a fair degree of efficiency and focus continued to remain on the security aspects of application rise. The need to manage bandwidth by applications was not felt.

With SaaS, collaboration and Cloud taking the traditionally internal applications outside the network, the bitter fight for bandwidth is already here. These applications would be up there in the cloud jostling for users' time, space and bandwidth with external applications.

With potentially every data moving to the cloud in the future, bandwidth would fall short from time to time. Of critical importance is the fact that 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.

The question isn't just of ensuring application availability, but also of optimizing bandwidth if costs are to stay within control. Hence, managing the 4 Elements of who (user), which (application), when (time) and what (bandwidth) which introduce layer 7 and 8 visibility and control based on time and bandwidth requirements become necessary to enhance productivity and control costs at the same time.



Integrating firewalls with the 4-Element: Application-User-Time-Bandwidth matrix ensures the creation of the most efficient, straightforward set of firewall rules that meet the QoS requirements of application access.

Managing the 4 Elements: Application - User - Time - Bandwidth

Integrating firewalls with the 4-Element Application-User-Time-Bandwidth matrix ensures the creation of the most efficient, straightforward set of firewall rules that meet the QoS requirements of application access. In making bandwidth available for critical applications and staggering non-critical application usage, firewalls can now even out the peaks and troughs of bandwidth consumption and ensure Application-QoS availability, delivering an enhanced user experience.

While all 4 elements are critical, bandwidth is the common element that forms the foundation for effective management of the other 3.

Application

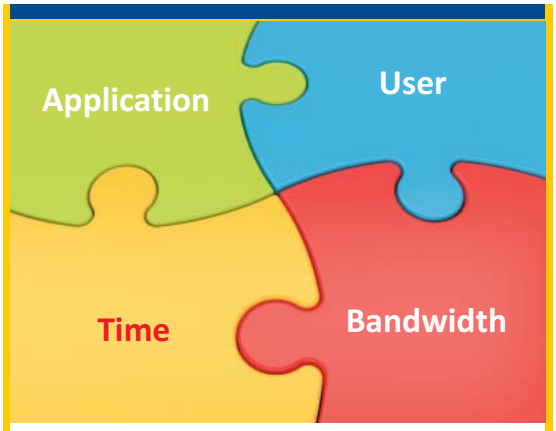
Firewalls will need to distinguish between applications. Let's take the 3 categories of applications across the Black, White and Grey areas.

- **Business (White)** - Fully business applications like VoIP, Salesforce would require primacy in the organizational bandwidth hierarchy. Hence, they take priority in bandwidth assignment at all hours of the day.
- **Non-Business (Black)** - Fully recreational applications like iTunes and P2P are more likely to be placed lowest in bandwidth priority. Organizations may want to block them totally as in the case of P2P. Or given the bottom-up demand for some social media applications and the need to build an attractive work place, they may resort to limiting the time of availability and to certain groups of users.
- **Socio-Business (Grey)** - The real question lies with these grey in-betweens - applications that began as personal in usage - instant messengers, social media tools like Facebook and You Tube - but evolved into a mix of business and recreation. Users today, are likely to use a variety of these applications to conduct a combination of official and personal business - Facebook which began as a social media application, is finding an increasing number of users for its chat and mail facility. Creating communities of partners or customers over Facebook has become an integral part of marketing and communication too.

User

While Salesforce, Microsoft Sharepoint or Google Docs would always require priority in access, and iTunes would be a straight forward decision of limited or no availability, things aren't too clear when one comes to social media applications like You Tube, LinkedIn and file transfers over Instant Messengers. This is where recognition of the User becomes significant.

Let's say You Tube is required within the organization for the sales and marketing departments. One would tend to think that a simple rule allowing You Tube for these departments and disallowing it for all others would do the job. What happens when as a result, a VoIP call by the CEO or a WebEx conference or Sharepoint collaboration suffers.



Before placing any controls where a complex matrix of application, user, time and bandwidth are involved, the right place to begin with is to observe the traffic and a deeper look into the pattern of usage

In addition to the Layer 7 Applications, organizations would now need to bring in the Layer 8 User too within the firewall rules. Armed with this, the organization can now define the minimum bandwidth needed for the application and apply the firewall rule accordingly, setting the highest priority to these bandwidth critical applications.

Time

The third important element for firewall rules would be time of the day. For applications that are bandwidth-critical but not time-critical, limiting their access to certain times of the day smoothens the bandwidth graph.

The organization would be better off setting a rule for say, You Tube access with maximum bandwidth availability beyond which it would be unable to use the organization's bandwidth. In addition, it can pre-define non-working hours for higher bandwidth availability to this grey application. This eliminates the strain on bandwidth.

Thus, incorporating the 4 Elements within the firewall is the way to manage applications in a cloud era.

Observing the 4 Elements

But before placing any controls, particularly in this case where a complex matrix of application, user, time of the day and bandwidth are involved, the right place to begin with is to observe the traffic.

At first look, all that organizations have is a bandwidth chart with its peaks and troughs showing the pattern of bandwidth consumption within the organization. To impose any rule that promotes business productivity without restricting it requires a deeper look into the pattern of usage

focusing on the following factors:

1. Distinguish among Applications
    a. White - Business applications
    b. Black - Non-Business applications
    c. Grey - Overlapping applications
2. Distinguish among Users
    a. Critical users by hierarchy or role
    b. Bandwidth-consuming users - with the distinction between Business and recreational users
    c. Specific requirements of users and departments - Eg. Social media applications for sales and marketing departments
3. Study the Criticality of Time - Note the times of the day when business critical applications and non-business applications are Used
4. Identify Bandwidth Requirement - List the bandwidth required for key business applications individually

Answers to the above tell the organization, who (element of user) is using which application (element of application), when (element of time) and what total and individual bandwidth (element of bandwidth) is likely to be needed.

Armed with this 4-element data, IT departments can begin the task of taking the individual departmental heads into the discussion and negotiate checks and limitations to even out the peaks and troughs.

Cyberoam is the only UTM that functions from Layer 2 to Layer 8, offering visibility and control into the Application Layer 7 and the User Layer 8 irrespective of the application origin.

Cyberoam makes you Cloud-Ready

Cyberoam is the identity-based Unified Threat Management (UTM) solution that has consistently maintained a balance between security and productivity within the organization.

It is the only UTM solution that functions from Layer 2 to Layer 8, offering visibility and control into the Application Layer 7 and the User Layer 8 irrespective of the application origin. At the same time, it offers unified security, allowing organizations to create rules for all UTM features, including bandwidth management from the firewall page itself.

Hence, it is in a position to handle the complex matrix of applications, users and time requirements within organizations to defuse the fight for bandwidth by applications even before it begins.

Cyberoam Features & Benefits: Application QoS

- Identifies applications and users
- Offers application-user-time-bandwidth control
- Delivers assured access to applications
- Delivers productivity gains
- Controls bandwidth costs
- Delivers network and data security

Cyberoam helps organizations control who is accessing which application, when and using what amount of bandwidth leading to high levels of productivity as well as cost containment by optimizing bandwidth consumed within the organization.

By taking both security and productivity into the equation, Cyberoam provides organizations with an effective solution that meets the business requirements and not just the security requirements, keeping them Cloud Ready.

Cyberoam Security Portfolio

Unified Threat Management (UTM)

Cyberoam Central Console (CCC)

SSL VPN

Cyberoam iView
Intelligent Logging & Reporting

Data Protection & Encryption
Device Management
Application Control
Asset Management

Cyberoam Endpoint Data Protection

Cyberoam Awards & Certifications

2008 - Emerging Vendor of the Year

Toll Free Numbers
USA : +1-877-777-0368 | **India :** 1-800-301-00013
APAC/MEA : +1-877-777-0368 | **Europe :** +44-808-120-3958

Cyberoam