Feb. 28, 2013
Jeremy Li

Credit: Barracuda Networks NG Firewall Live Demo

Barracuda Networks Inc., (https://www.barracudanetworks.com) has 170,000 customers in 80 countries worldwide and received many awards: (1) Barracuda Web Filter and the Barracuda Spam & Virus Firewall winners of the 7th Annual 2012 Hot Companies and Best Products Awards by Network Products Guide, the industry's leading technology research and advisory guide; (2) Barracuda Networks Honored in 2012 SC Magazine Reader Trust Awards; (3) Barracuda Networks Finalist in three Categories - Storage Awards.

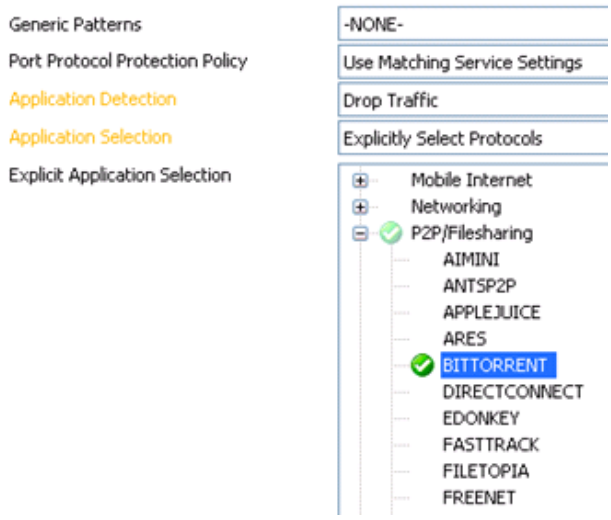
Barracuda Networks Inc., recently replaced another vendor's firewall at Southern California Gas Company by working with Juniper, Inc., to achieve the goal of reducing network complexities of configuring multiple different vendors' appliances with more flatter network and relying on its NG firewall to get rid of many additional licenses such as Traffic Shaping and Web Filtering.

There are eight hardware models of the Barracuda NG Firewall that can handle up to 21 Gbps of firewall throughput and 4 Gbps of VPN throughput. All models are centrally manageable through the Barracuda NG Control Center. Visit https://www.barracudanetworks.com/products/ngfirewall/models for details.

The demo consists of the followings:

1. Create a Rule to Control Skype Traffic

Create a rule for controlling Skype traffic via its Layer 7 Application Detection technique. It can (1) detect the Skype traffic; (2) limit its network bandwidth via QoS, also known as Traffic Shaping; (3) simply dropping its traffic. It also can block various unwanted traffic easily, as illustrated in the screenshot left.



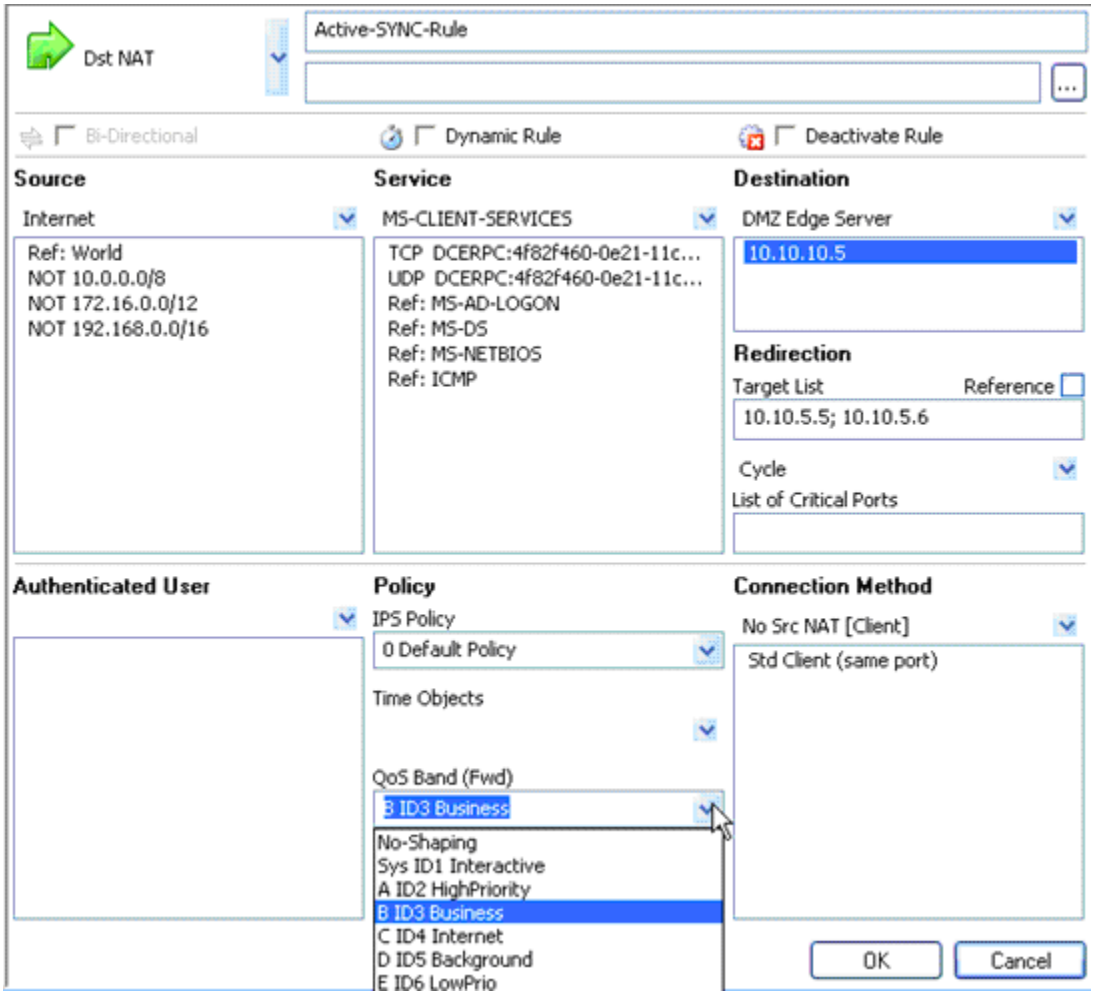
Note: Per Barracuda, neither Palo Alto NG Firewall nor Cisco Firewall ANA (Active Network Appliance) have QoS within its own box unless a third party appliance is used. Cisco ANA and Blue Coat Appliance can not block Layer 7 application traffics such as Skype. Both features referenced above are

free of charge with any model of Barracuda models.

2. Allow Microsoft ActiveSync Traffic through the NG firewall

Microsoft Exchange ActiveSync [EAS] is a synchronization protocol based on HTTP and XML that allows mobile devices access information on an Exchange Server (e.g., e-mail, calendar, contacts, tasks and Global Address List).

A rule was created to allow EAS traffic passing through the NG firewall. This can easily replace Microsoft ISA Server(s) in order to reduce the network complexity. A Forwarding Rule was created, as illustrated in a screenshot below:



Note: Target List: Two IP Addresses of Microsoft Exchange Client Access Servers (CAS) are listed as 10.10.5.5 and 10.10.5.6. One Microsoft CAS server or Edge Server is listed as 10.10.10.5 in DMZ.

Special notes:

Microsoft announced to discontinue its Threat Management Gateway 2010 (TMG), formerly known as ISA Server and its Forefront-branded solutions. Visit http://blogs.technet.com/b/server-cloud/archive/2012/09/12/important-changes-to-forefront-product-roadmaps.aspx for details.

3. Traffic Shaping / QoS

The licenses of the Traffic Shaping / QoS are included by default. It also supports BGP, OSPF, RIP and I&II. Visit http://lacaaea.com/vendors/trafficShaping.jpg and http://lacaaea.com/vendors/trafficShaping022813.jpg for details.

4. Built-in Intrusion and Prevention System (IPS):

Visit http://lacaaea.com/vendors/IPS022813JPG.JPG for details.

5. Built-in Real Time Trace Sessions and WireShark Capability

Visit http://lacaaea.com/vendors/WireShark021813.JPG for details.

6. Built-in Web Filtering (Similar to Blue Coat Web Filtering)

The presenter showed three techniques listed below:

a) **Create Transparent Proxy Rule**

That is widely being used because each client (browser) does not have to use a proxy setting in its browser configuration (Easy). With that configure, each browser can bypass the Blue Coat to visit a secured website such as https://www.facebook.com even though an enterprise policy does not allow a user to visit a social media site.

Mitigation: Create a Separate Proxy for HTTPS as listed below:

b) Create Forward Proxy Rule (Supports both HTTP & HTTPS)

This method must specify each IP address of the proxy in browser setting (client) for both HTTP and HTTPS protocols in browser. A Separate Proxy for HTTPS must be created to mitigate the issue referenced in a). Most IT units hate this method because it requires configuring each browser for each client. On the other hand, create a GPO policy should be able to address this issue.

Note: The performance might be an issue because the NG Firewall appliance must handle HTTPS traffic. Therefore, a higher performance unit must be purchased.

c) Create Integrated FLEX Cloud Web Filtering Rule

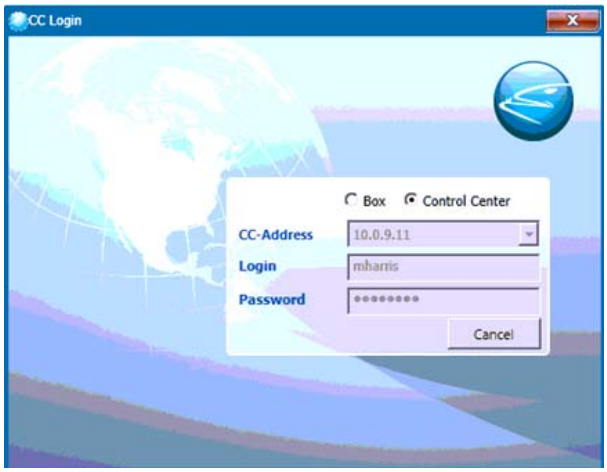
The advantage of this method is for perform that will be similar to the transparent proxy for HTTP. Now, an enterprise can manage HTTP, HTTPS, FTP and other common protocols from the cloud. However, this method adds a cost. Each user license is about $4.00 for the size of the County of Los Angeles.

Another benefit is for control. For example, all remote clients that have agent installed. For example, an iPad (BYOD) with browser installed (downloadable form Barracuda website) can not visit a site blocked by the corporate policy even though a user uses it at home. Therefore, it can prevent any virus or spyware bring into the corporate network.

7. Centralized Control & Management

Via Control Center Login console, as shown in a screenshot below, a firewall administrator can manage many tasks:

- Unlimited number of NG Firewalls from a single console
- Make any configuration change to any number of devices instantly from one place.
- Centrally control rules, traffic shaping patterns, administrative control, 90-day authentication changes, etc.



Now, an firewall administrator can view multiple firewalls from many different location in a single console, as shown in the picture via a link below http://lacaaea.com/vendors/CCLogin022813JPG.JPG .

8. SDN Platform Available Now!

Chassis w/Barracuda designed Hypervisor, I/O Virtualized, Network Virtualized, and Application programmable. In other words, the most scalable firewall available today.

Conclusion:

The true Next-Generation Firewall that focuses security on applications and users (a role based model focusing on layer 7 application traffic) is distinguished from a traditional firewall that focuses on the protocols of the network traffic (e.g., http with a layer 3 network traffic) and the network port (e.g., port 80 for web browser traffic). The NG-firewall can look at application that is coming in and who is allowed to use it. The Barracuda Networks NG Firewall live demo proved that its product is a NG Firewall that looks like a good product. However, it faces a stiff competition from other vendors.

Note: The network security companies such as Check Point have added application control capabilities on its existing traditional firewall to act like the NG firewall.

Challenge:

Although Cisco legacy firewall might be still number one in the enterprises in terms of the installed base, it has lost to the new comer such as Palo Alto Networks, who can deliver a better network security in the past few years. To date, 500 companies out of the Forbes Global 2000 are now Palo Alto Networks' new customers due to its true Next-Generation Firewalls technology and capability that can effectively deal with the ever increasingly complex and fast-growing number of applications such as Skype or Dropbox running from various clients such as BYOD. To date, Palo Alto Networks has more than 11,000 customers in over 100 countries and installed base is growing rapidly day after day.

As a result, Barracuda has three big competitors: Cisco Systems, Check Point Technologies, Inc. and Palo Alto Networks. For many enterprises who are not willing to adapt to the newer technology that will allow enterprises to secure their network and safely guard the growing number of applications running on their network fast enough, they will stay with the incumbent Cisco or Check Point, while for those who are willing to adapt to the newer technologies in order to enhance the current security, they will choose the Palo Alto NG firewall and other NG firewall vendors at the expense of Cisco Systems.

Recommended Reading:

1. State of Texas Moves More Than 100,000 State Employees to Microsoft Cloud

The State of Texas is moving more than 100,000 employees onto Office 365 at a cost of about $3.50 per user, per month, making it the largest statewide deployment of email and collaboration services in the U.S.

http://www.microsoft.com/en-us/news/Press/2013/Feb13/02-15TexasO365PR.aspx

2. How New York City is going to Consolidate 50 Data Centers from 40 City Agencies into One Location

http://www.datacenterknowledge.com/archives/2011/03/01/nyc-opens-consolidated-data-center/

3. Has the CIA Opted for Amazon Cloud? (GovTech)

http://www.govtech.com/e-government/Has-the-CIA-Opted-for-Amazon-Cloud.html

4. The Android Boom? (INFOGRAPHIC)

http://www.govtech.com/infographics/The-Android-Boom.html (GovTech)

Acknowledgement

Thank Mark Harris, Sr. Consulting Systems Engineer at Enterprise Business Unit, Barracuda Networks for his time to present a live demo of Barracuda Network NG Firewall.