Barracuda®

Application Usage & Risk Report

on Barracuda CloudGen Firewall

White Paper

What is the Application Usage and Risk Report?

The Application Usage and Risk Report is a predefined report type in the Barracuda Report Creator tool and provides automated reports and risk analysis based on the network traffic that is traversing the network. It provides an overview how effective the currently deployed technologies are in detecting and enforcing the corporate application usage policies and gives recommendations what should be taken into account when redefining these policies.

In a nutshell, the Application Usage and Risk Report is a great sales enablement tool to let customers see what is really happening on their corporate networks, what they have been missing so far and how they can reclaim their networks.

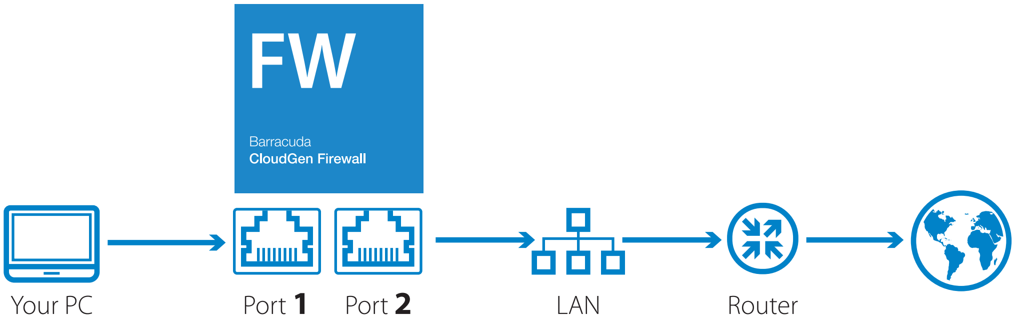
How does it work?

Generating an Application Usage and Risk Report requires deploying either a Barracuda CloudGen Firewall (via SPAN port or L2 Bridge) within the network where the network traffic that is passing the Internet perimeter shall be monitored.

Barracuda CloudGen Firewall F-Series Deployment

Transparent Bridge setup

The easiest ways to setup a Transparent Bridge is to use the Setup Wizard that will automatically start when you initially connect either to a freshly installed or a newly ordered Barracuda CloudGen Firewall F unit. Simply follow the steps in the wizard. The default firewall rule "EVAL-MODE-BRIDGE" will be automatically deployed.



For further details on the wizard and on how to manually configure a L2 bridge, please visit the Barracuda Campus (campus.barracuda.com).

Port Mirroring via SPAN Port (Switched Port Analyzer)

Barracuda CloudGen Firewall F-Series also provides the possibility to process traffic that is mirrored from a switch. Enabling the port mirror function of the F-Series unit has to be done via the Command Line Interface:

Step1 Log on via SSH

Step2 Configure a port on which the mirrored packets from the switch will arrive. Port mirroring needs to be enabled on the specific port which will receive the mirrored traffic. The port also needs to be set into promiscuous mode. As an example, to receive mirrored packets on Port 2 of the Barracuda CloudGen Firewall you would type the following commands:

```
acpfctrl monitor set dev port2
ip link set port2 promisc on
```

Step3 In order to switch of the mirroring and to set the port back to “normal”, please type the following commands:

```
acpfctrl monitor flush
ip link set port2 promisc off
```

On how to enable port mirroring on a switch and how to configure the destination port, please refer to the support documentation of the affected vendor. Here is an example on how to configure SPAN Port capabilities of the Cisco Catalyst 6500 Switch series: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-seriesswitches/10570-41.html

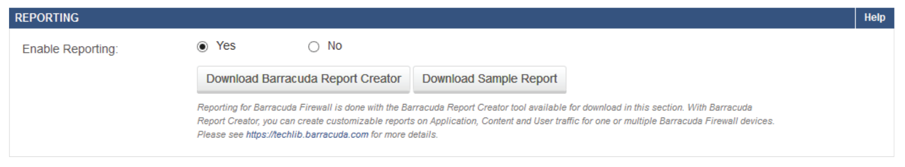
Configuring the Barracuda Firewall Report Creator:

Step1 Get the Barracuda Firewall Report Creator

Download the Barracuda Firewall Report Creator from the Barracuda Customer Portal by using your Barracuda Networks Account. Install it by double-clicking either the EXE or MSI archive. Follow the on-screen instructions to complete the installation.

> **Operating System**: Microsoft Windows Vista, or later
>
> **Additional Requirements**: Microsoft .NET Framework 4.0 Client Profile
>
> **Note**: Microsoft .NET Framework 4.0 Client Profile is not contained in the installation archive for the Barracuda Report Creator.

On the Barracuda NextGen Firewall X-Series you can also download the Barracuda Report Creator from within the UI under **Basic** > **Administration** > **Reporting**.

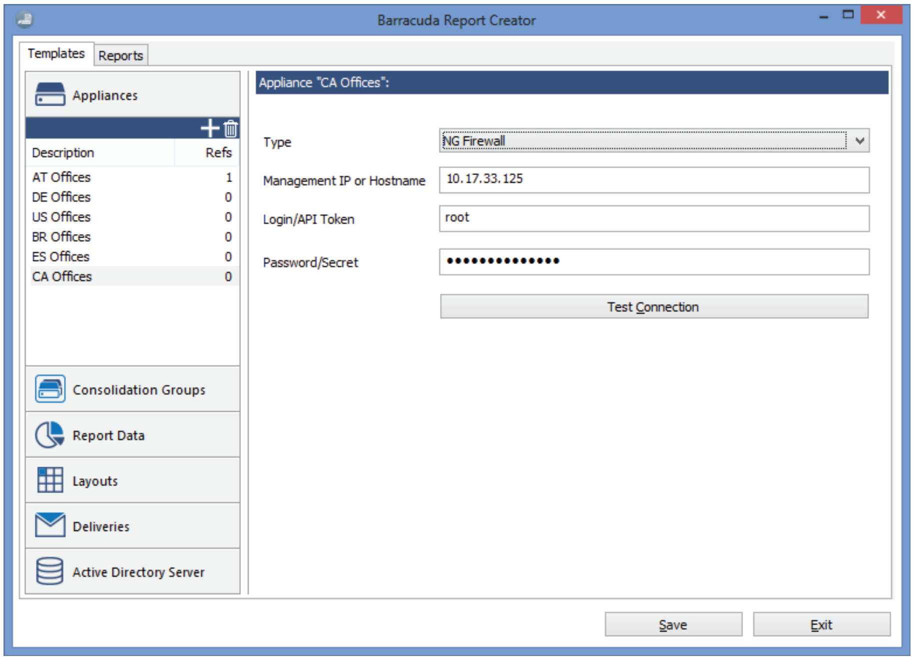


Enable Reporting: ● Yes ○ No

Reporting for Barracuda Firewall is done with the Barracuda Report Creator tool available for download in this section. With Barracuda Report Creator, you can create customizable reports on Application, Content and User traffic for one or multiple Barracuda Firewall devices. Please see https://techlib.barracuda.com for more details.

Step2 Configuring the Barracuda Firewall Report Creator

In the Appliances section of the Barracuda Firewall Report Creator, create an entry for every firewall unit that you want to generate a report for. For each entry, specify the settings for connecting to the appliance.



Description	Refs
AT Offices	1
DE Offices	0
US Offices	0
BR Offices	0
ES Offices	0
CA Offices	0

Appliance "CA Offices":

Type: NG Firewall

Management IP or Hostname: 10.17.33.125

Login/API Token: root

Password/Secret: ••••••••••••••

(a) Click the **Templates** tab. In the **Appliances** section in the left pane, click the "plus" icon.

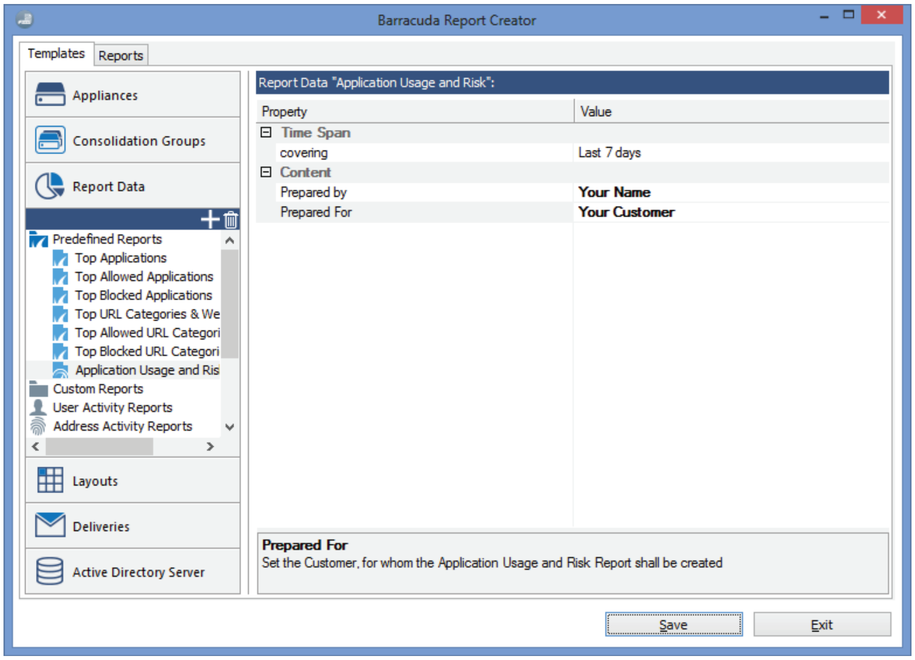
(b) Choose a product **Type** – either **Barracuda CloudGen Firewall F-Series** or **Barracuda NextGen Firewall X-Series**.

(c) Enter the **Management IP** or **Hostname**, **Login**, and **Password** for the appliance.

(d) Click **Test Connection** to verify that the Barracuda Firewall Report Creator can connect to the appliance.

(e) Click **Save**.

In the **Report Data** section of the Barracuda Firewall Report Creator, choose the Predefined Report type Application Usage and Risk.



Report Data "Application Usage and Risk":

Property	Value
⊟ Time Span	
covering	Last 7 days
⊟ Content	
Prepared by	**Your Name**
Prepared For	**Your Customer**

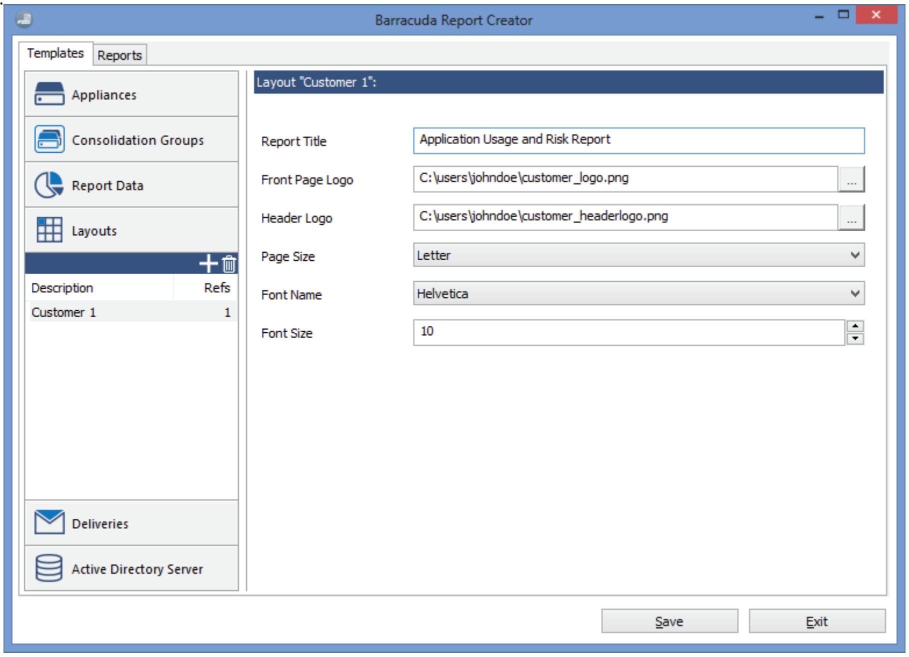
Prepared For
Set the Customer, for whom the Application Usage and Risk Report shall be created

(a) Configure the **Time Span** for which the report is generated.

(b) Fill out the **Prepared by** and **Prepared for** fields. This information will be displayed on the front page of the generated reports.

Step3 Create a report layout template (**Layouts**) to configure the look and feel of the report.

(a) Click **Layouts** and create a new template by clicking the "plus" icon



Layout "Customer 1":

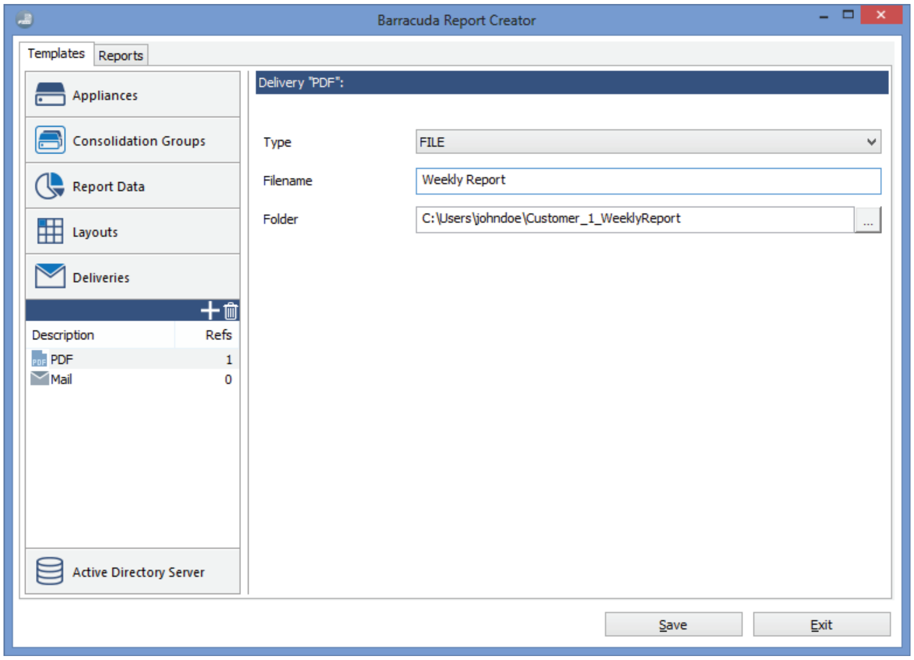
Description	Refs
Customer 1	1

Report Title: Application Usage and Risk Report
Front Page Logo: C:\users\johndoe\customer_logo.png
Header Logo: C:\users\johndoe\customer_headerlogo.png
Page Size: Letter
Font Name: Helvetica
Font Size: 10

(b) Configure Report Title, Front Page and Header logo, Page Size (paper format), Font Name and Size.

(c) Don't forget to Save the configuration changes.

Step4 **Configure a delivery template** (**Deliveries**), whether the report will be saved as a PDF file or it will be automatically sent via email.



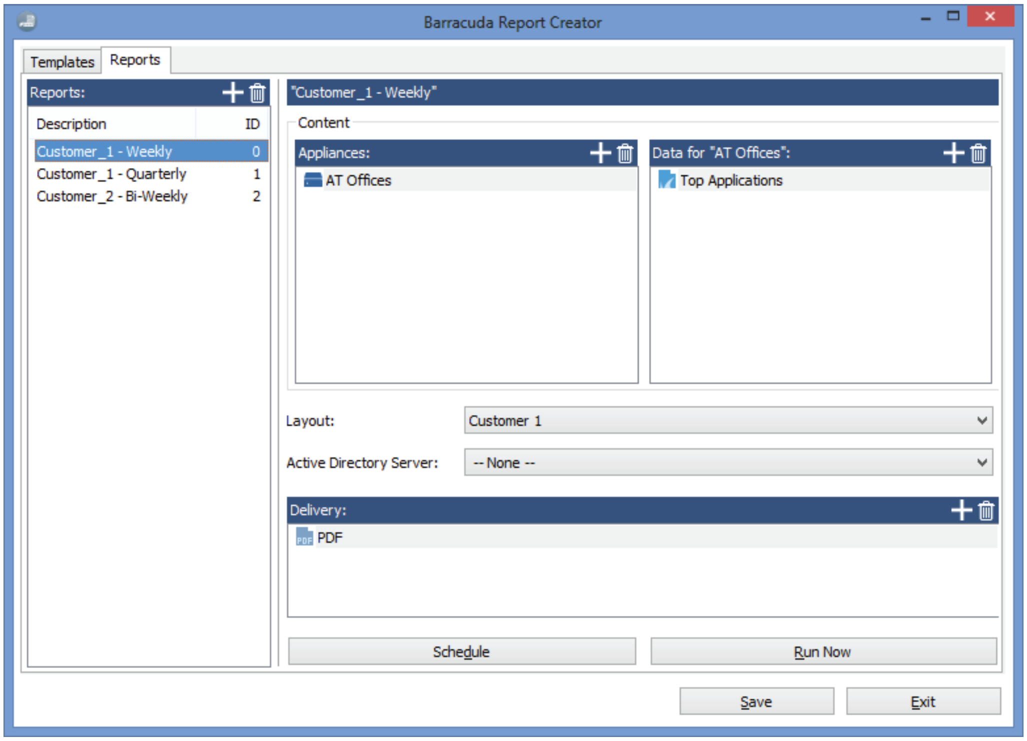
Delivery "PDF":

Description	Refs
PDF	1
Mail	0

Type: FILE
Filename: Weekly Report
Folder: C:\Users\johndoe\Customer_1_WeeklyReport

Generating Reports

After setting up the Barracuda Firewall Report Creator, you can generate the desired reports.



Description	ID
Customer_1 - Weekly	0
Customer_1 - Quarterly	1
Customer_2 - Bi-Weekly	2

Layout: Customer 1

Active Directory Server: -- None --

Step1 Click the **Reports** tab.

Step2 In the **Reports** section in the left pane, click the "plus" icon.

Step3 Enter the desired name for the report.

Step4 In the **Appliances** section, click the "plus" icon and select the appliance.

Step5 In the **Data for "your appliance name"** section, click the "plus" icon and then select the desired pre-defined report.

Step6 Select the desired **Layout** from the list.

Step7 In the **Delivery** section, click the "plus" icon and then select a delivery method.

Step8 Click **Save Configuration**.

Step9 Click **Run Now** to generate the report.

For further details on the wizard and on how to manually configure a L2 bridge, please visit the Barracuda Campus (campus.barracuda.com).

About Barracuda CloudGen Firewall

As your organization relies on more cloud-based applications like Office 365, Salesforce, and Dropbox, internet connectivity becomes even more important. Our Barracuda CloudGen Firewalls combine powerful application awareness and network routing capabilities to provide the highest levels of internet availability for users and critical applications.
Unlike other firewalls in the industry, Barracuda CloudGen Firewalls were designed with the modern network in mind. As organizations grew in the number of remote offices and employees, secure remote access (both site-to-site and client-to-site) became critical. Our proprietary TINA protocol allows us to provide powerful capabilities such as traffic shaping within VPN tunnels, tunnel encapsulation, traffic compression, NAT reversal, and much more. Barracuda's CloudGen Firewall family allows customers to leverage the latest in virtualization, cloud applications and mobile technologies while accommodating for rapid growth. They are more than just security devices, they make the network smarter, ensure access to critical network resources and improve productivity across the organization.

For questions about Barracuda CloudGen Firewall or for a free 30-day evaluation, visit
http://www.barracuda.com/products/cloudgenfirewall_f or
call Barracuda Networks at +1 408-342-5400.

About Barracuda Networks, Inc.

Barracuda provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud, and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com