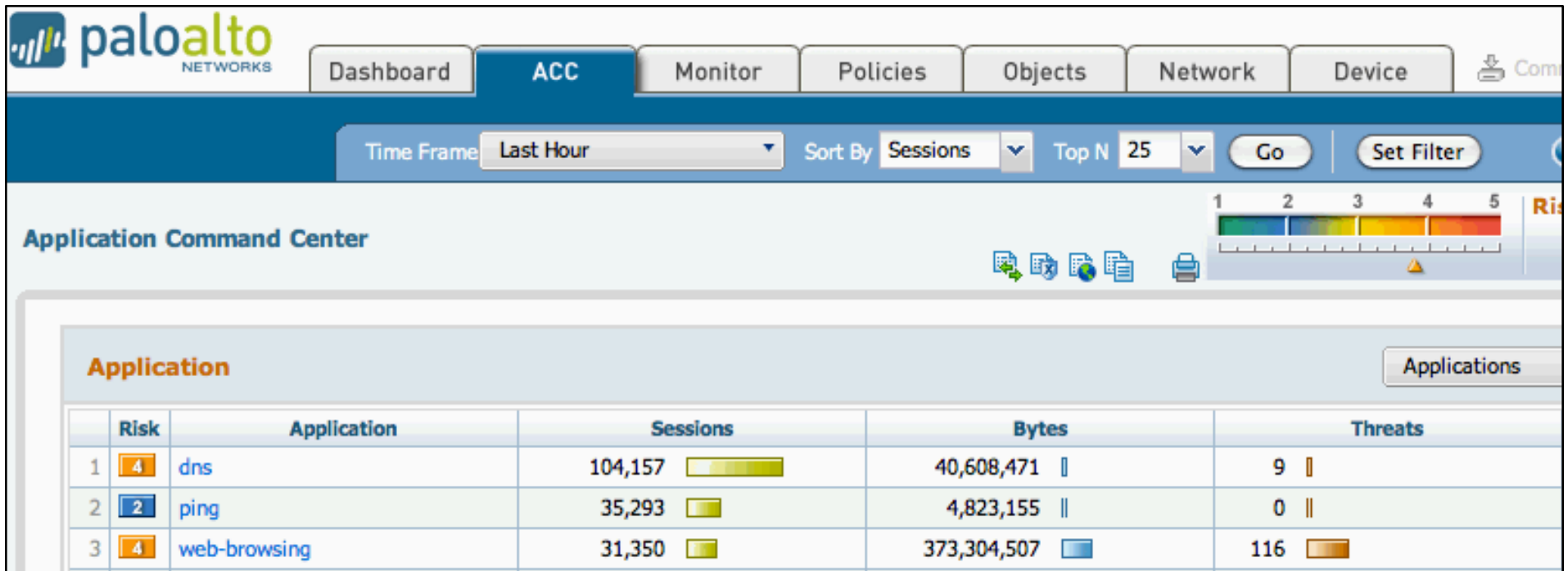


Your PaloAlto Firewall (Pan for short) can provide you visibility in your network on the fly. The visibility in the ACC (Application Command Center) can help you determine what applications, threats, and URL categories are present in a specific time frame. This lesson provides the basics.

The ACC is often used to determine events during the last hour which is the default time frame.

Login.

Login to your Pan box and click the **ACC** tab at the top of the screen. Note the default time frame of the Last Hour, Sort by Sessions, and the top 25 Applications are listed. These can be changed to suit your requirements.



The screenshot shows the PaloAlto Networks ACC interface. At the top, there are navigation tabs: Dashboard, ACC (selected), Monitor, Policies, Objects, Network, and Device. Below the tabs, there are controls for Time Frame (Last Hour), Sort By (Sessions), Top N (25), and buttons for Go and Set Filter. A risk scale is visible on the right side of the interface. The main content area displays a table titled 'Application Command Center' with the following data:

	Risk	Application	Sessions	Bytes	Threats
1	4	dns	104,157	40,608,471	9
2	2	ping	35,293	4,823,155	0
3	4	web-browsing	31,350	373,304,507	116

Applications and Bandwidth Usage.

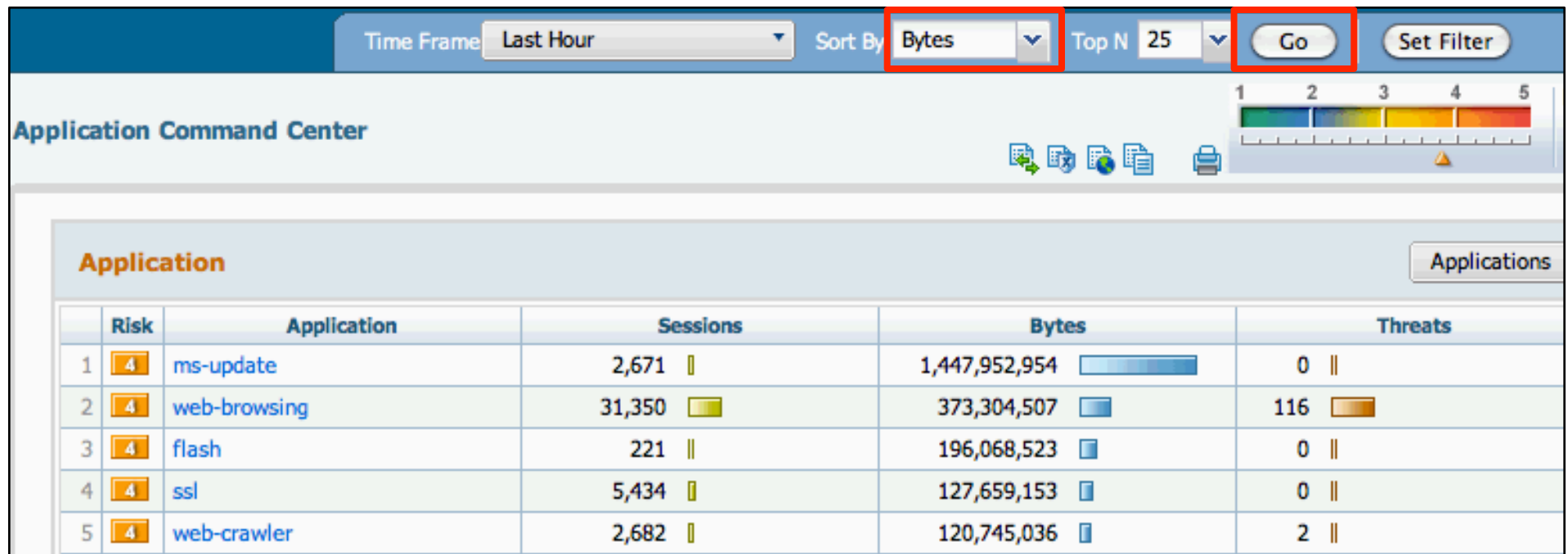
The ACC is can be used to identify applications that are hogging bandwidth when users complain that the Internet is slow. To view the applications that are bandwidth intensive change the sort by "**Sessions**" to "**Bytes**." This will sort the apps by bandwidth and tell you who the heavy hitters are.

To view by "Bytes" click the down arrow next to the **Bytes** field then click "**Go**."

Note the heavy hitters are: ms-update, web-browsing, flash, ssl, and web-crawler. Using the notation of 1024 bytes = 1 kilobyte you can do the math in your head.

If the Bytes column has 3 commas then Gigabytes.
If the Bytes column has 2 commas then Megabytes.
If the Bytes column has 1 comma then Kilobytes.

In this example ms-update did 1.4 Gigabytes in the last hour. That's your heavy hitter.





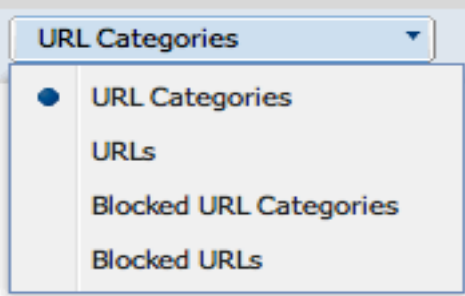












The screenshot shows the Application Command Center interface. At the top, there are controls for Time Frame (Last Hour), Sort By (Bytes), Top N (25), and a Go button. Below these controls is a table with columns for Risk, Application, Sessions, Bytes, and Threats. The table lists five applications: ms-update, web-browsing, flash, ssl, and web-crawler. The Bytes column for ms-update is highlighted with a blue bar, indicating it is the highest bandwidth user.

	Risk	Application	Sessions	Bytes	Threats
1	4	ms-update	2,671	1,447,952,954	0
2	4	web-browsing	31,350	373,304,507	116
3	4	flash	221	196,068,523	0
4	4	ssl	5,434	127,659,153	0
5	4	web-crawler	2,682	120,745,036	2

URL Content Filtering Categories.

Scroll down to the URL content filtering area. In the example below we can see traffic broken down in to URL categories. This gives you an idea of what kind of traffic traversed the network in the last hour. Number 6 for example shows that the network did 276 MB of **Streaming-Media**.

The pull down menu "**URL Categories**" can be changed to display URL information based on URLs that were blocked, etc.

URL Filtering				URL Categories
	Category	Sessions	Bytes	
1	computer-and-internet-info	13,946 	4,294,442,275 	 <ul style="list-style-type: none">● URL CategoriesURLsBlocked URL CategoriesBlocked URLs
2	internet-portals	2,492 	2,377,460,874 	
3	unknown	2,203 	573,722,762 	
4	business-and-economy	5,452 	326,585,639 	
5	content-delivery-networks	160 	303,700,169 	
6	streaming-media	835 	276,114,635 	
7	computer-and-internet-security	7,796 	213,740,451 	

Threat Prevention.

Scroll down to the Threat Prevention area. The threats listed are all threats that the Pan box either blocked or alerted on depending on how you have your Threat Prevention objects set. You can use the pull down menu to further refine what is displayed.

In this example note #1 Win32.Conficker. If you click on the name of the threat then the ACC will be changed (drill down) to reflect the last hours traffic and only the Conficker events. This enables you to find the source of the Threat.

Threat Prevention							Threats
	Severity	Threat	ID	Type	Count	Color	
1	CRITICAL	Win32.Conficker.C p2p	12544	spyware	474		
2	CRITICAL	Microsoft SQL Server Stack Overflow Vulnerability	30009	vulnerability	248		
3	CRITICAL	Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	32735	vulnerability	98		
4	INFORMATIONAL	HTTP Non RFC-Compliant Response Found	32880	vulnerability	24		
5	LOW	ISC BIND 9 Dynamic Update Request Denial of Service Vulnerability	32783	vulnerability	23		
6	HIGH	Microsoft ASN.1 Library Bit String Processing Heap Corruption	31967	vulnerability	19		
7	HIGH	Bredavi.Gen Command and Control Traffic	13043	spyware	12		
8	INFORMATIONAL	RFC2397 Data URL Scheme Usage Detected	30419	vulnerability	11		

- Threats
- Types
- Spyware
- Spyware Phone Home
- Spyware Download
- Vulnerabilities
- Viruses