

The Future of Next Generation Firewalls Requirements and Vision

David Buckwald

Director of Systems Engineering, Americas



Technology Trends

Impacts to Productivity & ROI



Drives Infrastructure Requirements



- Bandwidth
- Performance
- Availability
- Efficiency
- Manageability
- Security

Security is an Ongoing Challenge

Ripped from the Headlines



<http://www.esecurityplanet.com/headlines/article.php/3907811/Most-Large-Companies-Were-Hacked-in-2010.htm>

Security is an Ongoing Challenge

Ripped from the Headlines



<http://www.guardian.co.uk/technology/2010/jan/14/google-hacking-china-cyberwar>

Seemingly Safe Applications

Adobe PDF Reader



Home / News & Blogs / Zero Day

Another day, another Adobe PDF Reader security hole

By Ryan Naraine | November 5, 2010, 11:46am PDT

Summary

Adobe today acknowledged the public release of a demo PDF file that could be weaponized to launch denial-of-service or even remote code execution attacks.



A new day, a new security vulnerability haunting users of Adobe's PDF Reader software.

Adobe today acknowledged the public release of a demo PDF file that could be weaponized to launch denial-of-service or even remote code execution attacks.

The [proof-of-concept](#), posted to the Full Disclosure security mailing list, successfully crashes fully patched versions of Adobe Reader. The company says it is investigating the issue and [warned](#) that arbitrary code execution "may be possible."

Topics

November 5, 2010, 11:46am PDT

<http://www.zdnet.com/blog/security/another-day-another-adobe-pdf-reader-security-hole/7693>

Adobe Download Manager

The Worst Security flaw in Adobe Download Manager



Adobe issued a fix on Tuesday for a critical infirmity in its **Adobe Download Manager** program that could be used by an attacker to download malware onto a user's PC.

People who have downloaded the newest version of **Adobe Reader** for Windows or **Flash Player** for Windows from **Adobe's Official site** are affected with this suspicious malware. The issue is resolved for any new downloads of **Adobe Reader** and **Flash Player**, the company said.



Adobe Download Manager is a tool that helps users to download the files from Adobe Servers. It is used for downloading and is deleted when the computer is updated. Adobe recommends users to update the...

<http://glanceworld.com/the-worst-security-flaw-in-adobe-download-manager.html>

Malware Lurks in Social Networks

- Set-up:** Create bogus celebrity LinkedIn profiles
- Lure:** Place link to celebrity “videos” in profile
- Attack:** Download of “codec” required to view video
- Infect:** Codec is actually Malware
- Result:** System compromised



The Problem...

Vulnerabilities are in the software everyone uses everyday...

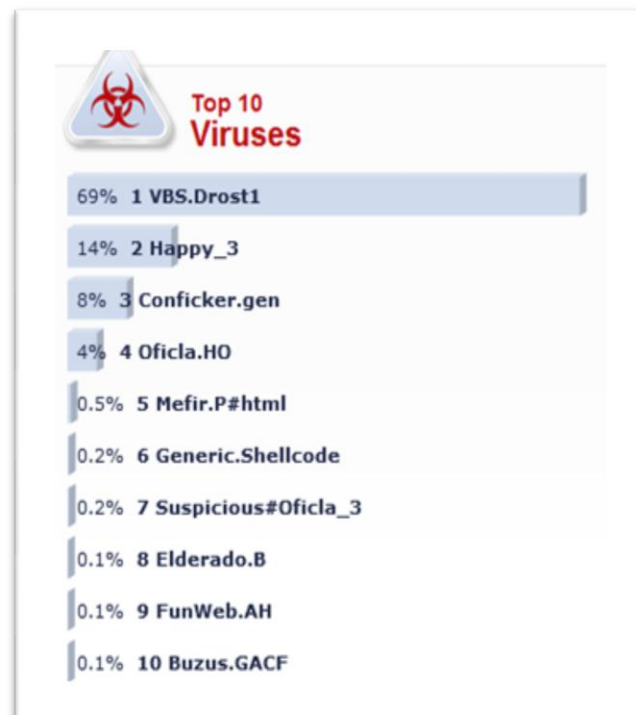
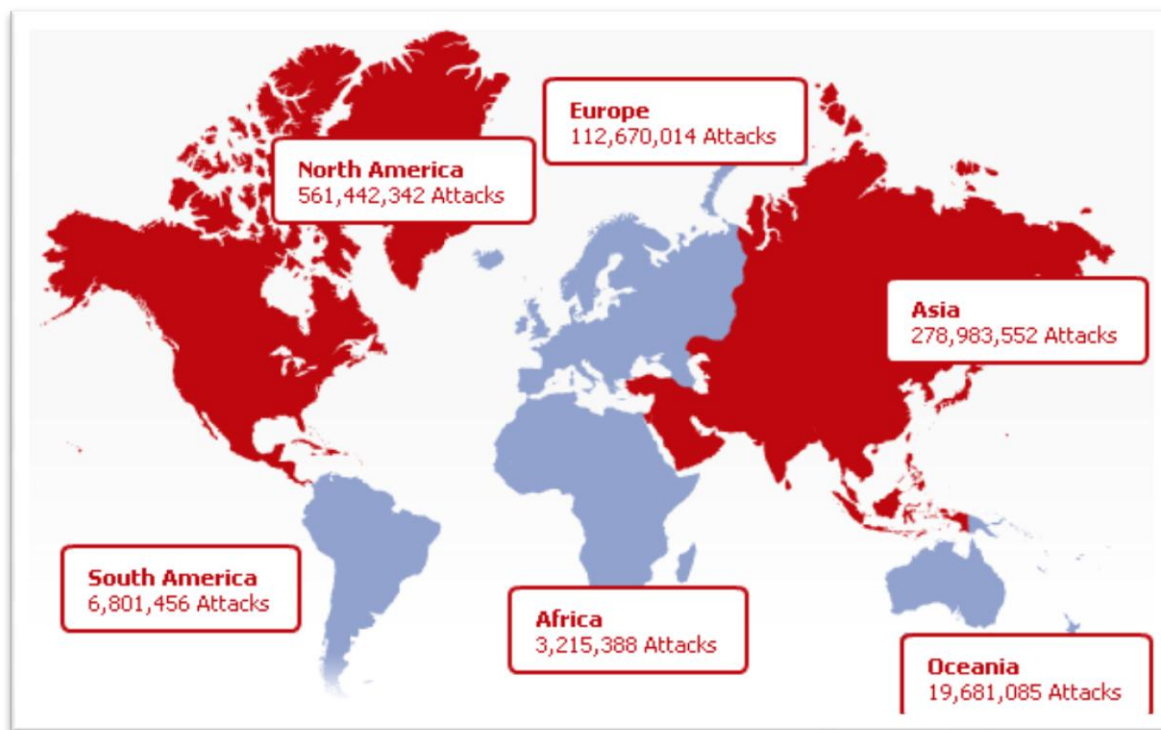
Problem

- Programmers make mistakes
- Malware exploits mistakes

[Microsoft Security Bulletins Coverage \(Nov 09, 2010\)](#)
[MS Excel PtgExtraArray Parsing Memory Corruption \(Nov 5th, 2010\)](#)
[New IE 0-day Vulnerability \(Nov 5, 2010\)](#)
[IBM Rational Products Backdoor Account Access \(Oct 29, 2010\)](#)
[New Adobe Acrobat 0-day Vuln \(Oct 28, 2010\)](#)
[HP Data Protector Media Operations DoS \(Oct 22, 2010\)](#)
[Bandok Keylogger Trojan \(Oct 21, 2010\)](#)
[Obot Infostealer Trojan \(Oct 15, 2010\)](#)
[Microsoft Security Bulletins Coverage \(Oct 12, 2010\)](#)
[Virus Murofet.A \(Oct 8, 2010\)](#)
[Apple Safari WebKit Counter Vulnerability \(Oct 7, 2010\)](#)
[Ofida Trojan Spam Campaign \(October 1, 2010\)](#)
[HP Data Protector Express Stack BO \(Oct 1st, 2010\)](#)
[FakeAV Downloader - CV spam \(Sept 24, 2010\)](#)
[New mass-mailing worm seen in the wild \(Sep 10, 2010\)](#)
[MySQL Denial of Service Vulnerabilities \(Sep 9, 2010\)](#)
[Bamital Trojan - Pay Per Install \(Sept 3, 2010\)](#)
[Apple QuickTime QTPlugin Code Execution \(Sept 2, 2010\)](#)
[Apple Safari Button Rendering Code Execution \(Aug 25, 2010\)](#)
[PS3 Jailbreak Trojan \(Aug 25, 2010\)](#)
[Microsoft Windows SMB Pool Overflow \(Aug 20, 2010\)](#)
[Ackantta Trojan spam campaign \(August 19, 2010\)](#)
[Yahos Worm Spreading in the Wild \(Aug 12, 2010\)](#)
[Microsoft Security Bulletins Coverage \(Aug 10, 2010\)](#)
[New Bredolab spam campaign \(August 6, 2010\)](#)
[Symantec AMS2 Remote Command Execution \(Aug 5, 2010\)](#)
[Rise in Zeus spam campaigns \(July 30, 2010\)](#)

Result: Relentless, Unyielding Malware

A Typical Day in 2010



SonicWALL Security Center www.sonicwall.com/securitycenter.asp

What Are Your Employees Doing?

- Blogging
- Facebook
- Twitter
- IM
- Streaming video
- Streaming audio
- Downloading files
- Playing games
- Personal Webmail

Time spent on **Facebook** was **greater** than time spent on **Google** sites for the first time in history. (comScore, August 2010)

Together Facebook.com and Google.com accounted for **14%** of all Internet visits last week. (Hitwise, March 2010)

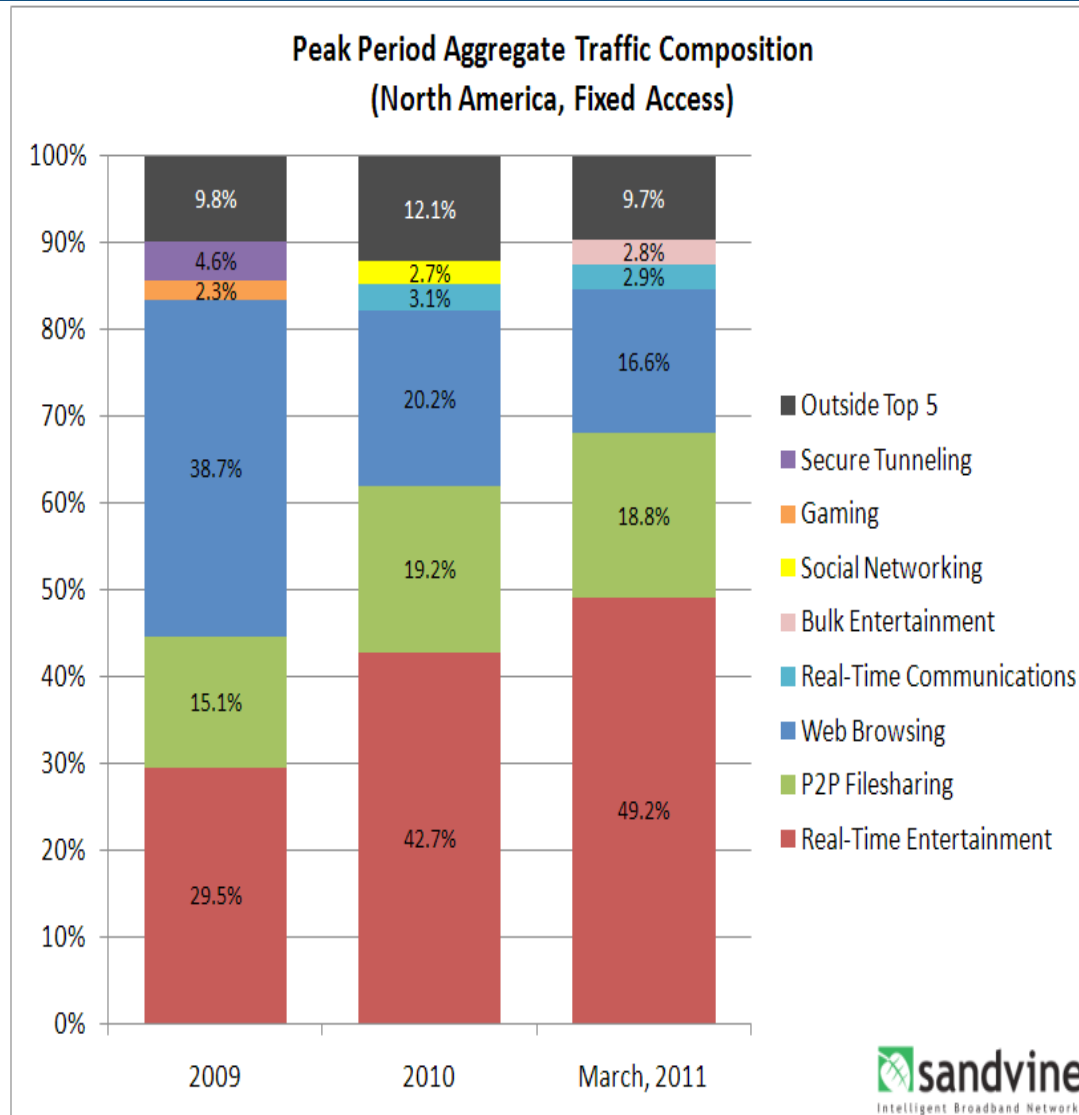
BANDWIDTH COST



PRODUCTIVITY



What Are Your Employees Doing?



The Problems Today:

Security and Productivity



What are the **THREATS**?



Where is this **TRAFFIC** coming from?



What **APPLICATIONS** are really on my net

Where is ALL my **BANDWIDTH** going?



Application Chaos

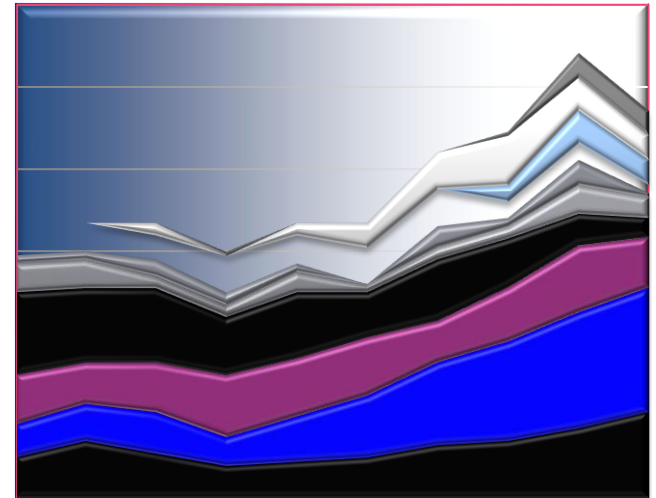
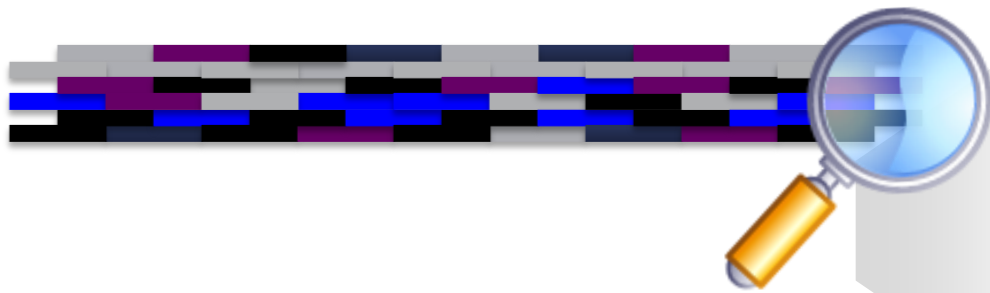
IT Controls Challenged

Who Chooses What Applications are Good or Bad?



Overcoming Application Chaos...

Requires a completely new paradigm focused on users and applications



What is a Next-Generation Firewall

Requirements

- Stateful Inspection
- Intrusion Prevention
- **Application Control**
- SSL Decryption/Inspection

Considerations

- Security
- Application Control
- Scalability

Options

- *Gateway AV*
- *Gateway Anti-Malware*

Next-Generation Firewall

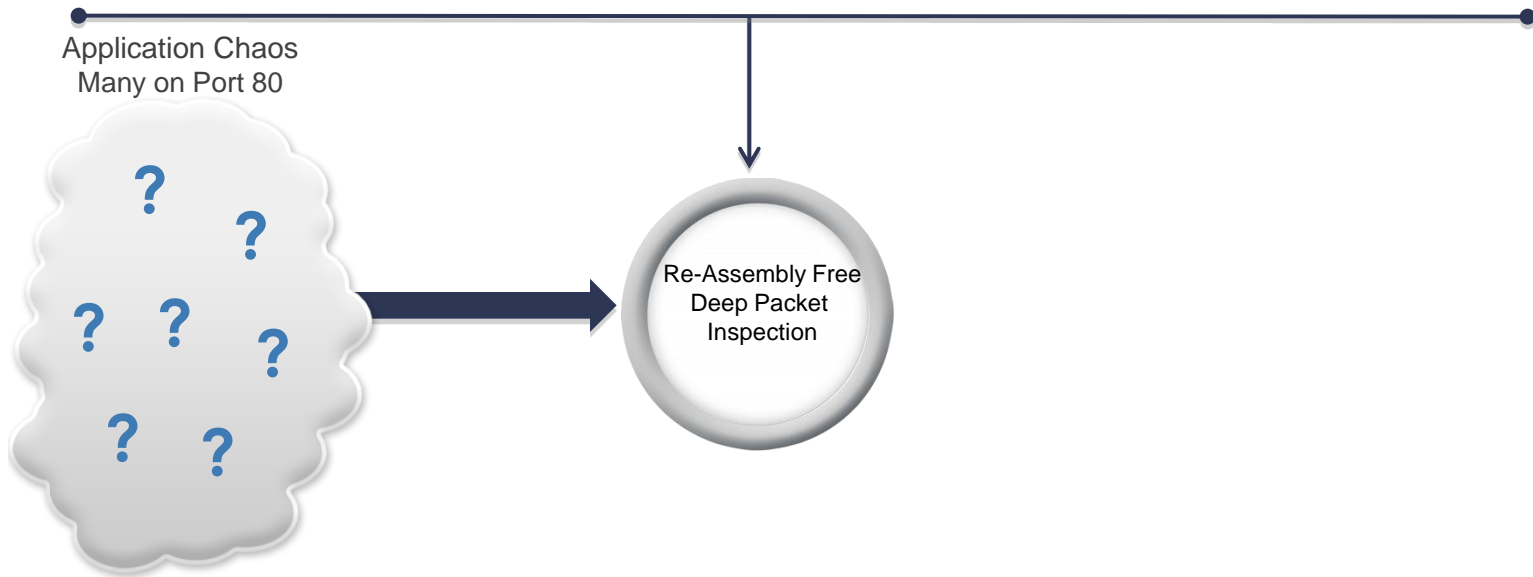
Identify



Categorize



Control



Next-Generation Firewall

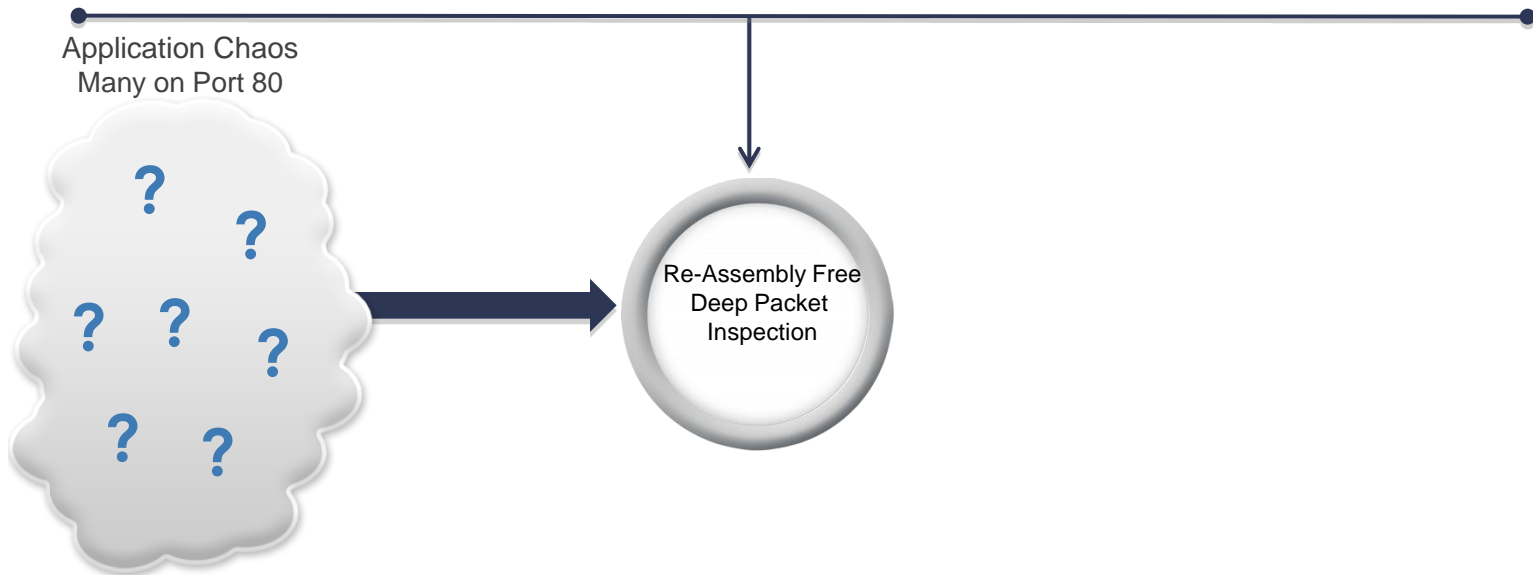
Identify



Categorize



Control



Next-Generation Firewall

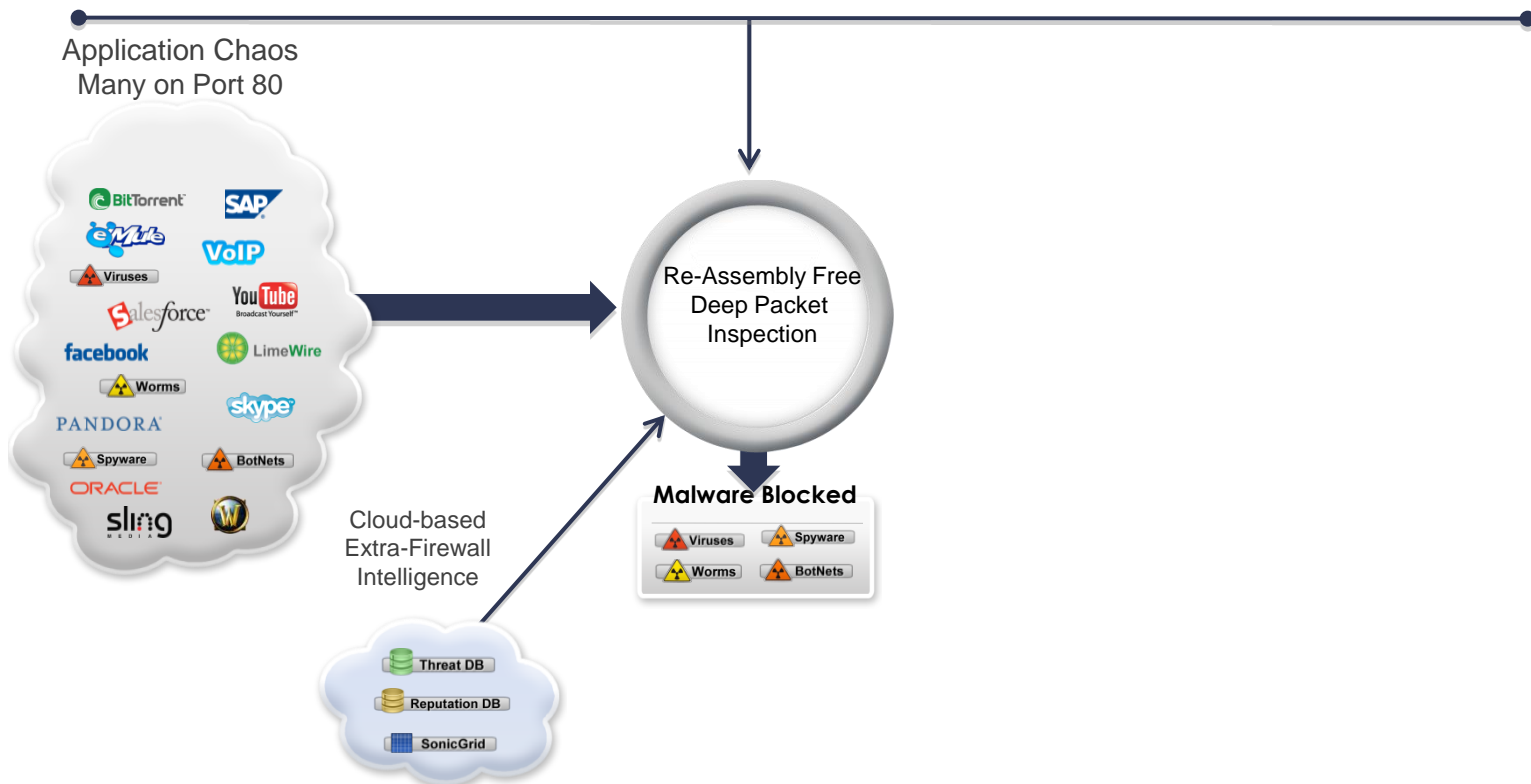
Identify



Categorize



Control



Next-Generation Firewall

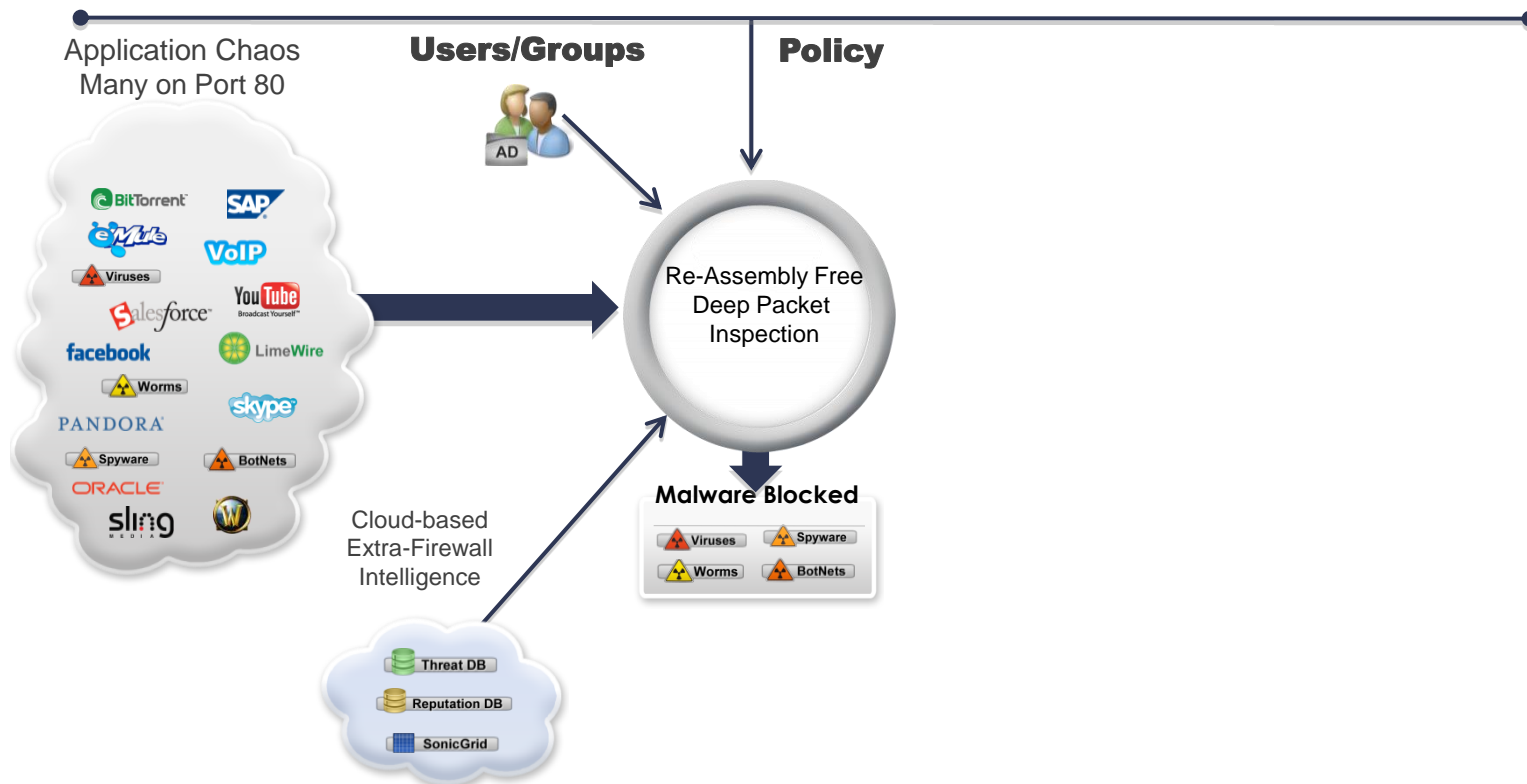
Identify



Categorize



Control



Next-Generation Firewall

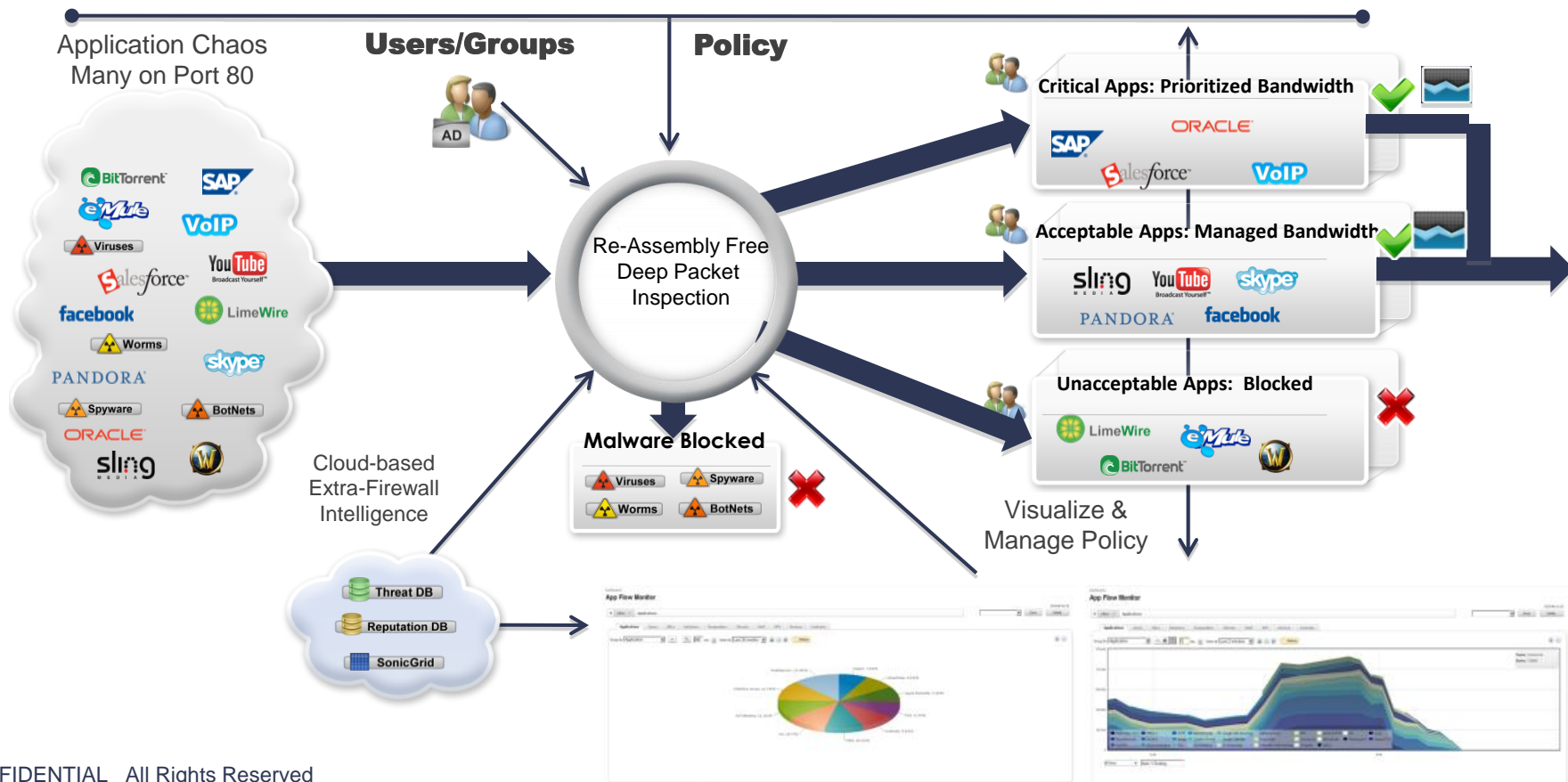
Identify



Categorize



Control



The Power of Seeing – Application Visualization

Dashboard /

App Flow Monitor

+ Filter Applications

Applications

Users

URLs

Initiators

Responders

Threats

VoIP

VPN

Devices

Contents

Group By: Application

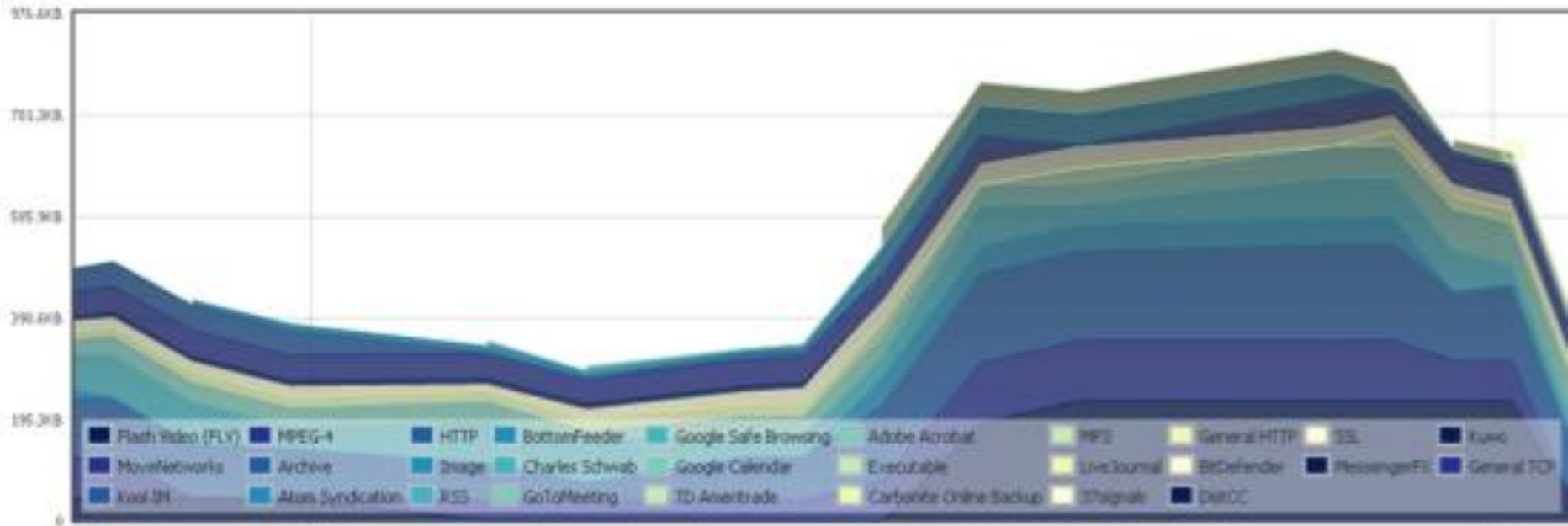


1 sec.

Interval:

Last 2 minutes


Status



All Items

Auto Y-Scaling

Application Identification

 Network Security Appliance

AlertWizardsHelpLogout

Mode: Configuration

Dashboard

App Flow Monitor

Real-Time Monitor

Top Global Malware

Log Monitor

Connection Monitor

Packet Monitor

System

Network

3G/Modem

SonicPoint

Firewall

Firewall Settings

DPI-SSL

VoIP

Anti-Spam

VPN

SSL VPN

Virtual Assist

Users

High Availability

Security Services

Log

Dashboard /

App Flow Monitor

08:28:18 Oct 08

Filter

ApplicationsUsersURLInitiatorsRespondersThreatsVoIPVPNDevicesContents

Group By: Application

600 sec. Interval: Last 5 minutes

Status

	Application	Sessions	Packets	Bytes	Rate (KBps)	Threats
	HTTP	20	1210	715012	616.601	0
	General URL	177	1868	179661	255.877	0
	Archive	1	303	169878	0.305	0
	General UDP	49	272	47497	117.772	0
	SSL	3	64	17122	9.566	0
	YouTube	10	111	11893	16.425	0
	DNS	67	140	11426	63.158	0
	RSS	2	22	10796	4.760	0
	General TCP	63	171	10123	21.147	2
	BitTorrent	12	56	8096	3.894	0
	YouSendIt	2	20	7113	3.016	0
	IMDb	5	56	6444	2.470	0
	Amazon.com	2	20	2632	1.144	0
Total:		426	4380	1204825		

Note: To manage App Flow data collection, please go to [Log > Flow Reporting](#).

Network Analysis Tools

“Who’s watching YouTube?”

SonicWall Network Security Appliance

Alert | Wizards | Help | Logout

Mode: Configuration

Dashboard / **App Flow Monitor**

10:29:08 Oct 04

+ Filter x

Applications | Users | URLs | Initiators | Responders | Threats | VoIP | VPN | Devices | Contents

Group By: Application | 600 sec. | Interval: Last 5 minutes

Application	Sessions	Packets	Bytes	Rate (KBps)	Threats
HTTP	20	905	580640	431.664	0
undclassified	657	2835	339148	917.326	6
Archive	6	523	282565	16.646	0
BitTorrent	52	163	27517	103.826	0
YouTube	12	142	15428	17.247	0
DNS	82	164	13740	80.508	0
MySpace Video	4	41	10338	8.188	0
SSL	1	43	7446	12.346	0
MySpace	1	101	6519	0.874	0
IMDb	6	56	6282	3.132	0
Image	2	14	4404	1.568	0
RSS	1	10	2054	0.835	0

User Identification

- Single Sign On (AD/LDAP Integration)
- Local Login
- Identify Top Bandwidth users

App Flow Monitor

Filter x

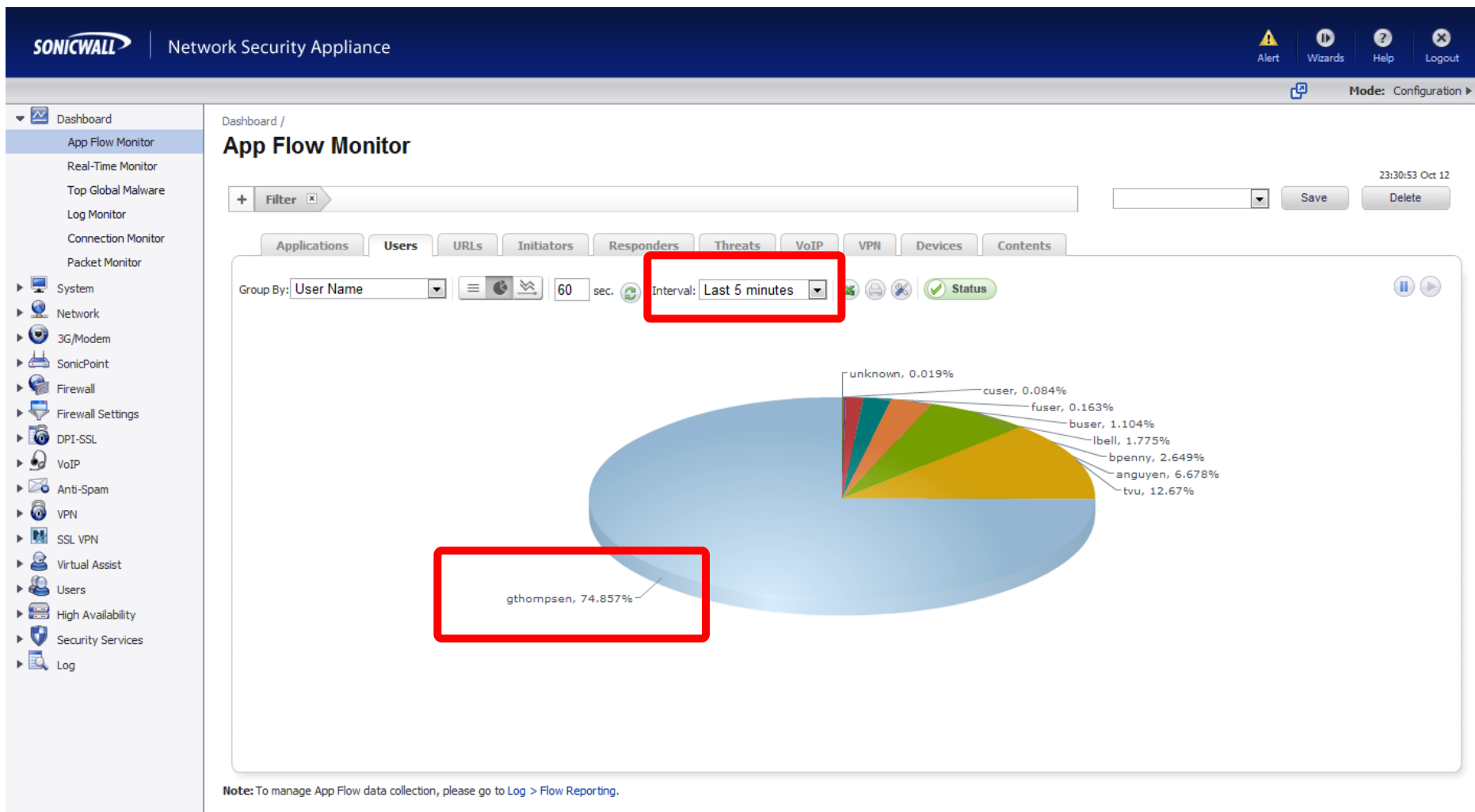
Applications Users URLs Initiators Responders Threats VoIP VPN Devices Contents

Group By: User Name 600 sec Interval: Last 5 minutes Status


User	Sessions	Packets	Bytes	Rate (KBps)	Threats
bpenny	70	976	276514	250.363	0
lbell	68	911	266337	313.884	0
gthompson	107				
unknown	2				
euser	16				
epresley	1				
buser	54				
ldevore	4				
tvu	57				
anguyen	3				
sforrest	2				
cuser	2				
hholmes	9				
Total:	400				

Note: To manage App Flow data collection, please go to Log > Flow Reporting.

Identify the Bandwidth Hogs



Or view Bandwidth Hogs in detail

 Network Security Appliance

AlertWizardsHelpLogout

Mode: Configuration

Dashboard

App Flow Monitor

Real-Time Monitor

Top Global Malware

Log Monitor

Connection Monitor

Packet Monitor

System

Network

3G/Modem

SonicPoint

Firewall

Firewall Settings

DPI-SSL

VoIP

Anti-Spam

VPN

SSL VPN

Virtual Assist

Users

High Availability

Security Services

Log

Dashboard /

App Flow Monitor

23:37:00 Oct 12

Filter

SaveDelete

ApplicationsUsersURLsInitiatorsRespondersThreatsVoIPVPNDevicesContents

Group By: User Name

60 sec.


Interval: Last 5 minutes

Status

	User	Sessions	Packets	Bytes	Rate (KBps)	Threats
<input type="checkbox"/>	bpenny	104	1357	374747	482.297	0
<input type="checkbox"/>	gthompson	82	1189	321852	370.995	0
<input type="checkbox"/>	lbell	82	1078	307629	267.653	0
<input type="checkbox"/>	buser	110	259	76856	248.175	2
<input type="checkbox"/>	anruven	135	216	32891	190.570	1
<input type="checkbox"/>	tvu	22	146	11582	16.490	0
<input type="checkbox"/>	cuser	5	49	16110	15.521	0
<input type="checkbox"/>	sforrest	3	38	6194	5.057	0
<input type="checkbox"/>	kthibodeaux	1	2	214	1.254	0
<input type="checkbox"/>	fuser	1	2	172	1.008	0
<input type="checkbox"/>	ldevore	1	9	827	0.609	0
<input type="checkbox"/>	unknown	2	2	128	0.000	0
Total:		548	4347	1149202		

Note: To manage App Flow data collection, please go to [Log > Flow Reporting](#).

Connection Tracking by Country

 Network Security Appliance

Wizards ? Logout

Mode: Configuration ▶

Dashboard /

App Flow Monitor

+ Filter x

00:05:24 Oct 04


Save Delete

Applications Users URLs Initiators Responders Threats VoIP VPN Devices Contents

Group By: Country [Chart Icon] [Table Icon] [Line Icon] 600 sec. Interval: Last 5 minutes [Refresh Icon] [Status Icon]

Responder	Sessions	Packets	Bytes	Rate (KBps)	Threats
<input type="checkbox"/> United Kingdom	14	98	11258	22.753	0
<input type="checkbox"/> Canada	10	54	6935	16.046	0
<input type="checkbox"/> Germany	4	29	2411	4.368	0
<input type="checkbox"/> Afghanistan	3	26	2151	2.888	0
<input type="checkbox"/> Denmark	3	22	2030	5.026	0
<input type="checkbox"/> Russian Federation	4	8	1765	10.342	0
<input type="checkbox"/> India	3	15	1405	3.320	0
<input type="checkbox"/> Taiwan	4	6	1125	6.592	0
<input type="checkbox"/> Austria	1	11	1052	1.438	0
<input type="checkbox"/> Slovenia	2	4	872	5.109	0
<input type="checkbox"/> Italy	2	4	863	5.057	0
<input type="checkbox"/> Sweden	1	9	799	1.264	0
<input type="checkbox"/> France	2	3	567	3.322	0
Total:	465	5758	1775002		

Track Suspicious Traffic

 Network Security Appliance

AlertWizardsHelpLogout

Mode: Configuration

Dashboard

Real-Time Monitor

App Flow Monitor

Top Global Malware

Log Monitor

Connection Monitor

Packet Monitor

System

Network

3G/Modem

SonicPoint

Firewall

Firewall Settings

DPI-SSL

VoIP

Anti-Spam

VPN

SSL VPN

Virtual Assist

Users

High Availability

Security Services

Log

Dashboard /

App Flow Monitor

Filter x Responders x

Application: Russian Federation Thailand Bahamas


Group By: Country

600 sec. Interval: Last 5 minutes

Status

Responder	Sessions	Packets	Bytes	Rate (KBps)	Threats
Russian Federation	3	5	2043	11.971	0
Thailand	5	15	827	2.802	0
Bahamas	1	2	366	2.145	0
Total:	9	22	3236		

Dig Deeper into Suspicious Traffic

 Network Security Appliance

AlertWizardsHelpLogout

Mode: Configuration ▶

DashboardReal-Time MonitorApp Flow MonitorTop Global MalwareLog MonitorConnection MonitorPacket MonitorSystemNetwork3G/ModemSonicPointFirewallFirewall SettingsDPI-SSLVoIPAnti-SpamVPNSSL VPNVirtual AssistUsersHigh AvailabilitySecurity ServicesLog

Dashboard /

App Flow Monitor

+ Filter x Responders x

00:22:36 Oct 04SaveDelete

ApplicationsUsersURLsInitiatorsRespondersThreatsVoIPVPNDevicesContents

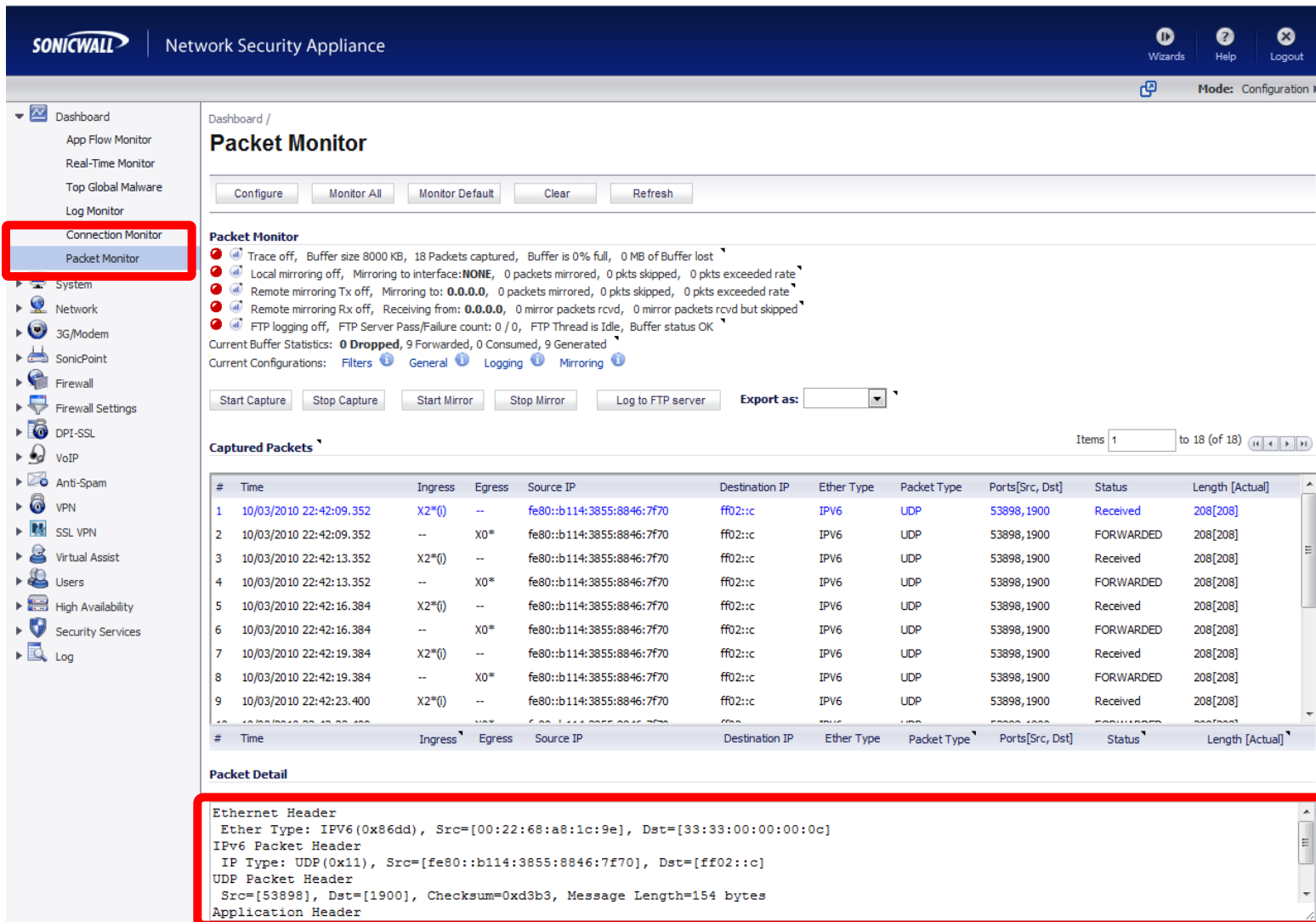
Group by: Application

600 sec. Interval: Last 5 minutes

Status

	Application	Sessions	Packets	Bytes	Rate (KBps)	Threats
<input type="checkbox"/>	HTTP	13	570	469177	851.109	0
<input type="checkbox"/>	unclassified	120	1077	111507	172.358	0
<input type="checkbox"/>	BitTorrent	2	82	48002	2.225	0
<input type="checkbox"/>	YouTube	17	200	21676	26.860	0
<input type="checkbox"/>	Facebook	3	36	4215	3.350	0
<input type="checkbox"/>	DNS	14	28	2465	14.443	0
<input type="checkbox"/>	IMDb	1	6	600	0.748	0
Total:		170	1999	657642		

Capture Packets for Further Analysis



The screenshot displays the SonicWall Network Security Appliance interface, specifically the Packet Monitor section. The left sidebar shows the navigation menu with 'Packet Monitor' highlighted. The main content area includes a status bar with buttons for 'Configure', 'Monitor All', 'Monitor Default', 'Clear', and 'Refresh'. Below this, the 'Packet Monitor' section shows a summary of capture statistics: 18 packets captured, 0 MB of buffer lost, and 0 packets mirrored. It also displays current buffer statistics: 0 dropped, 9 forwarded, 0 consumed, and 9 generated. The 'Captured Packets' table lists 18 items, showing details such as time, ingress/egress status, source/destination IP, ether type, packet type, ports, status, and length. The 'Packet Detail' section at the bottom provides a detailed view of the selected packet, showing the Ethernet header, IPv6 packet header, and UDP packet header.

Packet Monitor

Trace off, Buffer size 8000 KB, 18 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
Local mirroring off, Mirroring to interface: **NONE**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Tx off, Mirroring to: **0.0.0.0**, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Rx off, Receiving from: **0.0.0.0**, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK
Current Buffer Statistics: **0 Dropped**, 9 Forwarded, 0 Consumed, 9 Generated
Current Configurations: [Filters](#) [General](#) [Logging](#) [Mirroring](#)

Start Capture Stop Capture Start Mirror Stop Mirror Log to FTP server Export as: [v]

Captured Packets Items 1 to 18 (of 18)

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	10/03/2010 22:42:09.352	X2*(i)	--	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	Received	208[208]
2	10/03/2010 22:42:09.352	--	X0*	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	FORWARDED	208[208]
3	10/03/2010 22:42:13.352	X2*(i)	--	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	Received	208[208]
4	10/03/2010 22:42:13.352	--	X0*	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	FORWARDED	208[208]
5	10/03/2010 22:42:16.384	X2*(i)	--	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	Received	208[208]
6	10/03/2010 22:42:16.384	--	X0*	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	FORWARDED	208[208]
7	10/03/2010 22:42:19.384	X2*(i)	--	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	Received	208[208]
8	10/03/2010 22:42:19.384	--	X0*	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	FORWARDED	208[208]
9	10/03/2010 22:42:23.400	X2*(i)	--	fe80::b114:3855:8846:7f70	ff02::c	IPv6	UDP	53898,1900	Received	208[208]

Packet Detail

Ethernet Header
Ether Type: IPv6(0x86dd), Src=[00:22:68:a8:1c:9e], Dst=[33:33:00:00:00:0c]
IPv6 Packet Header
IP Type: UDP(0x11), Src=[fe80::b114:3855:8846:7f70], Dst=[ff02::c]
UDP Packet Header
Src=[53898], Dst=[1900], Checksum=0xd3b3, Message Length=154 bytes
Application Header

CONTROL the application traffic

View Filter: Policy Type: All

Action Type: All

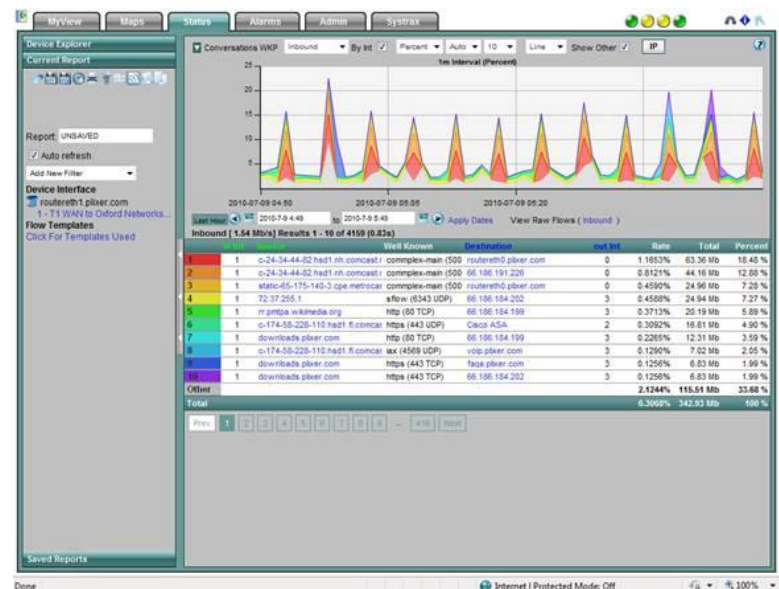
<input type="checkbox"/>	#	Name	Policy Type	Object	Action	Source	Destination	From Service	To Service	Direction	Comments	Enable	Configure
<input type="checkbox"/>	1	apps-multimedia-prioritize-low-except-execs	App Control Content	apps-category-multimedia	bwm-prioritize-low	Any	Any	N/A	N/A	Any	 	<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	2	apps-p2p-im-low-priority	App Control Content	apps-category-p2p-im	bwm-prioritize-low	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	3	apps-voip-realtime-priority	App Control Content	apps-category-voip	bwm-prioritize-realtime	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	4	apps-webmail-medium-priority	App Control Content	apps-category-webmail	bwm-prioritize-medium	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	5	block-gaming-during-work-hours	App Control Content	apps-category-gaming	Reset/Drop	Any	Any	N/A	N/A	Any	 	<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	6	block-proxies	App Control Content	proxys-to-block	Reset/Drop	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	7	business-apps-high-priority	App Control Content	business-apps-high-priority	bwm-prioritize-high	Any	Any	N/A	N/A	Any		<input checked="" type="checkbox"/>	  
<div> Add New Policy Delete Delete All </div>													

☐ 5
 block-gaming-during-work-hours
 App Control Content
 apps-category-gaming
 Reset/Drop

NetFlow/IPFIX with Extensions Reporting

■ NetFlow/ IPFIX with Extensions

1. Rating
2. Location
3. Applications
4. Intrusions
5. Viruses
6. Spyware
7. Services
8. Flow Table
9. Location
10. Users
11. URLs
12. Log
13. Interface Statistics
14. Core Utilization
15. Memory Utilization
16. VOIP
17. SPAM
18. Connected Devices
19. VPN Tunnels
20. URL Rating



What it All Means...

- Trends in technology are driving the applications into the cloud and the use of social media is now a requirement to conduct business
- **Problem:** IT is experiencing challenges with managing their networks as:
 - **THREATS** are getting more sophisticated
 - **APPLICATION** chaos is occurring on corporate networks
 - **BANDWIDTH** is being sucked by for non-productive applications
 - No way to know where network **TRAFFIC** coming from

**SonicWALL Next-Generation Firewall with
Application Intelligence, Control and Visualization**

SonicWALL Next-Generation Firewall

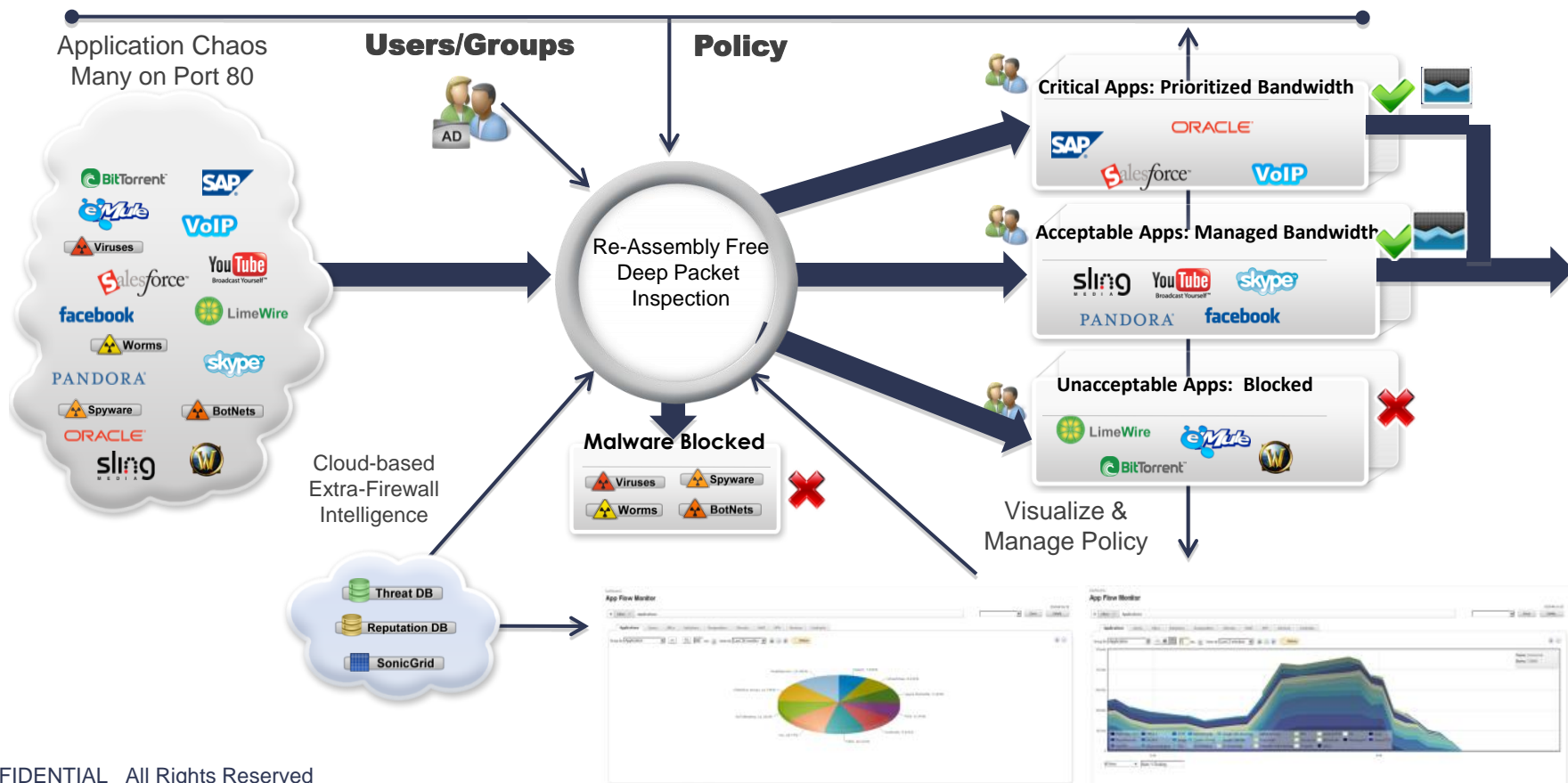
Identify



Categorize



Control



The background features a series of thin, light blue wavy lines that sweep across the top half of the slide. Below these, a solid dark blue horizontal band spans the width of the slide. The bottom half of the slide is a solid dark blue field.

Thank You!

David Buckwald

Director of Systems Engineering, Americas

