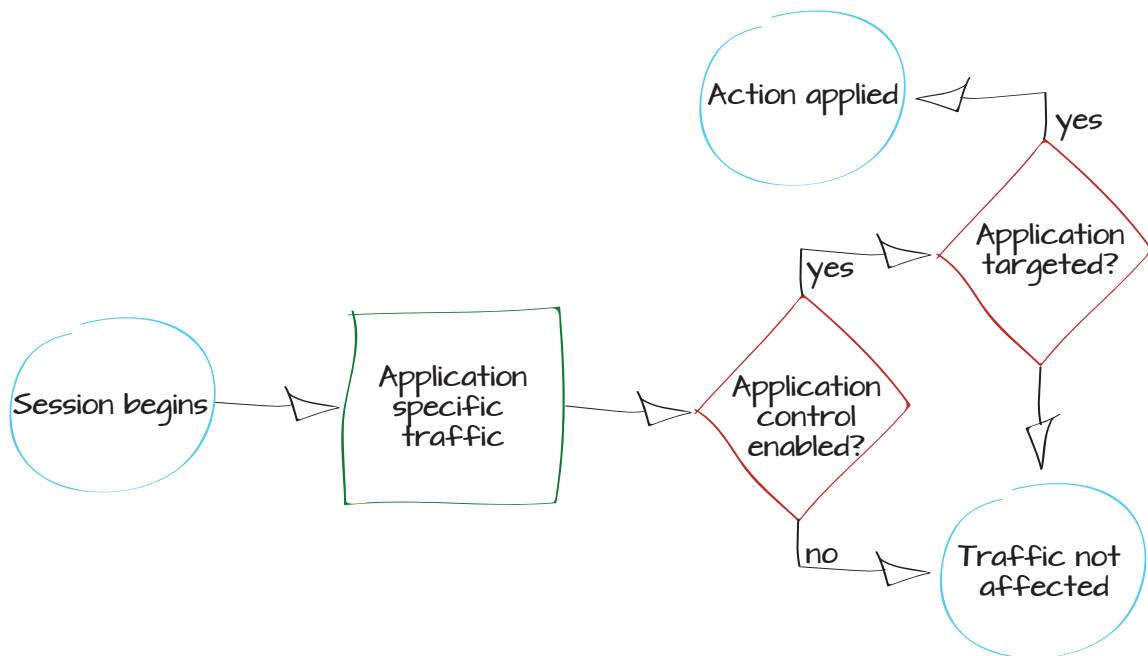


# Controlling network access using application control

This example uses application control to monitor traffic and determine what applications are contributing to high bandwidth usage or distracting employees. After this is determined, a different application sensor is used to block those applications from having network access.

1. Creating an application sensor to monitor network traffic
2. Adding the monitoring sensor to a security policy
3. Reviewing the application control monitor
4. Creating an application sensor to block applications
5. Adding the blocking sensor to a security policy
6. Results



## Creating an application control sensor to monitor traffic

Go to **Security Profiles > Application Control > Application Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor list for monitoring application traffic.

Select **Create New** to add a new application filter. Leave all **Filter Options** selected.

Ensure that you set the **Action** to **Monitor**. At this stage in the process, you are monitoring the traffic to locate any problems that may be occurring, rather than blocking applications.

Name

Comments  0/255

Sensor Type  Filter Based  Specify Applications

[Filter Options]

Category	Popularity	Technology	Risk
<input checked="" type="checkbox"/> Botnet	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Browser-Based	<input checked="" type="checkbox"/> Botnet
<input checked="" type="checkbox"/> Game	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Client-Server	<input checked="" type="checkbox"/> Excessive-Bandwidth
<input checked="" type="checkbox"/> Media	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Network-Protocol	<input checked="" type="checkbox"/> None
<input checked="" type="checkbox"/> Proxy	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Peer-to-Peer	
<input checked="" type="checkbox"/> Storage.Backup	<input checked="" type="checkbox"/> ☆☆☆☆☆		
<input checked="" type="checkbox"/> eMail			
<input checked="" type="checkbox"/> General.Interest			
<input checked="" type="checkbox"/> IM			
<input checked="" type="checkbox"/> File.Sharing			
<input checked="" type="checkbox"/> P2P			
<input checked="" type="checkbox"/> Social.Networking			
<input checked="" type="checkbox"/> Remote.Access			
<input checked="" type="checkbox"/> Update			
<input checked="" type="checkbox"/> VoIP			

Application Name	Category	Technology	Popularity	Risk
012mail	eMail	Browser-Based	☆☆☆☆☆	
0zz0	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
1und1.Mail	eMail	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Browse.Upload.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Search.Download.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2ch	Social.Networking	Browser-Based	☆☆☆☆☆	
2ch_Post	Social.Networking	Browser-Based	☆☆☆☆☆	
3PC	Network.Service	Network-Protocol	☆☆☆☆☆	
4shared	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
6cn	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
9PFS	Network.Service	Network-Protocol	☆☆☆☆☆	
9PTV	P2P	Peer-to-Peer	☆☆☆☆☆	Excessive-Bandwidth
24lm	IM	Client-Server	☆☆☆☆☆	Excessive-Bandwidth
51.Com	Social.Networking	Browser-Based	☆☆☆☆☆	

1 / 164 [ Total: 226 ]

Action  Monitor  Block  Reset  Traffic Shaping


## Adding the monitoring sensor to a security policy


Go to **Policy > Policy > Policy**.


Edit the security policy that allows internal users to access the Internet. Under **Security Profiles**, enable **Application Control** and set it to use the new filter.


Policy Type  Firewall  VPN


Policy Subtype  Address  User Identity  Device Identity


Incoming Interface  


Source Address  

Outgoing Interface  

Destination Address  

Schedule  

Service  

Action  

Enable NAT

- Use Destination Interface Address
- Use Dynamic IP Pool
- Use Central NAT Table

Fixed Port


**Logging Options**

- No Log
- Log Security Events
- Log all Sessions

**Security Profiles**

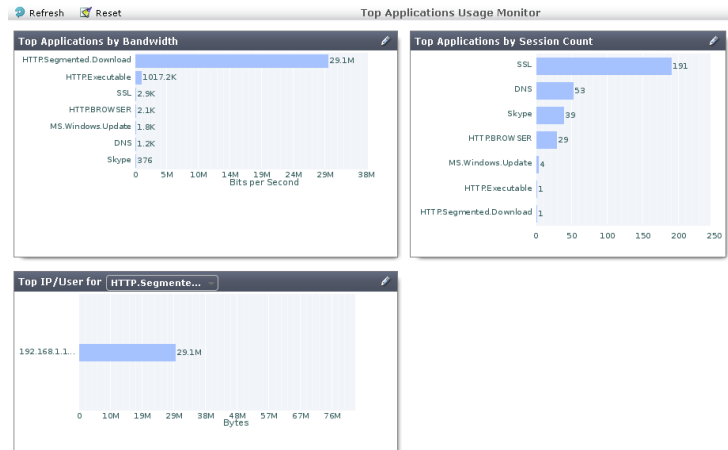
AntiVirus

Web Filter

Application Control  

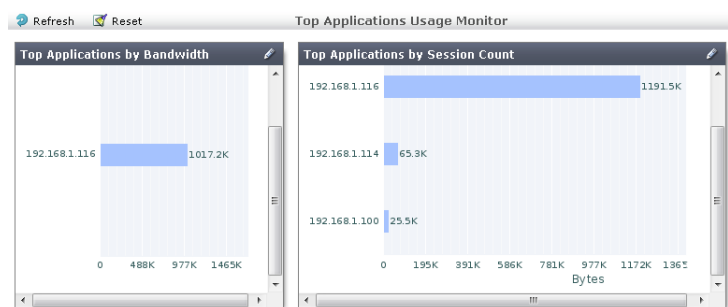
## Reviewing the application control monitor

Go to **Security Profiles > Monitor > Application Monitor** to see the results found by the application sensor.



Select a bar to see further details on the usage statistics.

In the example, you can see an occurrence of an HTTP segmented download, which typically occurs during Peer-to-Peer (P2P) downloads. To avoid this from occurring in the future, P2P applications must be blocked.



## Creating an application sensor to block applications

Go to **Security Profiles > Application Control > Application Sensors** and create a new sensor list for blocking application traffic.

Name:

Comments:  0/255

Select **Create New** to add a new application filter.

In the **Category** list, select the application categories you wish to block. As well as blocking P2P, other types of applications can be selected that are known to distract employees.

Ensure that you set the **Action** to **Block**.

## Adding the blocking sensor to a security policy

Go to **Policy > Policy > Policy**.

Edit the firewall policy allowing internal users to access the Internet. Under **Security Profiles**, enable **Application Control** and set it to use the new filter.

Sensor Type:  Filter Based  Specify Applications

Filter Options

Category	Popularity	Technology	Risk
<input type="checkbox"/> Botnet	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Browser-Based	<input checked="" type="checkbox"/> Botnet
<input type="checkbox"/> Game	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Client-Server	<input checked="" type="checkbox"/> Excessive-Bandwidth
<input checked="" type="checkbox"/> Media	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Network-Protocol	<input checked="" type="checkbox"/> None
<input type="checkbox"/> Proxy	<input checked="" type="checkbox"/> ☆☆☆☆☆	<input checked="" type="checkbox"/> Peer-to-Peer	
<input type="checkbox"/> Storage.Backup	<input checked="" type="checkbox"/> ☆☆☆☆☆		
<input type="checkbox"/> eMail			
<input checked="" type="checkbox"/> General.Interest			
<input type="checkbox"/> IM			
<input type="checkbox"/> File.Sharing			
<input type="checkbox"/> Network.Service			
<input type="checkbox"/> P2P			
<input type="checkbox"/> Remote.Access			
<input checked="" type="checkbox"/> Social.Networking			
<input type="checkbox"/> Update			
<input type="checkbox"/> VoIP			

Application Name	Category	Technology	Popularity	Risk
Oz20	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Browse.Upload.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Search.Download.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2ch	Social.Networking	Browser-Based	☆☆☆☆☆	
2ch_Post	Social.Networking	Browser-Based	☆☆☆☆☆	
4shared	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
6cn	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
9PTV	P2P	Peer-to-Peer	☆☆☆☆☆	Excessive-Bandwidth
24im	IM	Client-Server	☆☆☆☆☆	Excessive-Bandwidth
51.Com	Social.Networking	Browser-Based	☆☆☆☆☆	
51.Com_BBS	Social.Networking	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
51.Com_Music	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
51.Com_Posting	Social.Networking	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
51.Com_Webdisk	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth

Action:  Monitor  Block  Reset  Traffic Shaping

Policy Type:  Firewall  VPN

Policy Subtype:  Address  User Identity  Device Identity

Incoming Interface: internal

Source Address: all

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Enable NAT

- Use Destination Interface Address
- Use Dynamic IP Pool
- Use Central NAT Table

Fixed Port

Click to add...

**Logging Options**

- No Log
- Log Security Events
- Log all Sessions

**Security Profiles**

- AntiVirus: default
- Web Filter: default
- Application Control: Block\_app-sensor





## Results

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see the sensor is working and blocking the traffic from the selected application types, including the P2P application Skype.

Select an entry to view more information, including the application name and the device the traffic originated on.

	Application Name	Application Control List	Application Category	Application Control Acti
	Skype	Block_app-sensor	P2P	drop-session
2	Skype	Block_app-sensor	P2P	drop-session
	Skype	Block_app-sensor	P2P	drop-session
	Skype	Block_app-sensor	P2P	drop-session
		Block_app-sensor		

<b>Dst</b>	 157.55.56.147	<b>Virtual Domain</b>	root
<b>Received</b>	252	<b>Source Country</b>	Reserved
<b>Application Name</b>	 Skype	<b>Src NAT IP</b>	172.20.120.124
<b>Sent / Received</b>	248 B / 252 B	<b>Device Type</b>	Windows PC
<b>Duration</b>	88	<b>Sent</b>	248
<b>Src NAT Port</b>	5878	<b>Application Details</b>	
<b>Device</b>	 00:0c:29:4b:d7:cc	<b>Service</b>	40041/tcp
<b>Protocol</b>	6	<b>byod_name</b>	
<b>Destination Country</b>	United States	<b>Application Control List</b>	Block_app-sensor
<b>Dst Port</b>	40041	<b>roll</b>	65499
<b>Status</b>	deny	<b>Timestamp</b>	Wed Dec 5 22:36:10 2012
<b>Application ID</b>	10	<b>OS Name</b>	Windows
<b>Sequence Number</b>	13720	<b>Policy ID</b>	8
<b>Src Interface</b>	internal	<b>Src</b>	192.168.1.114
<b>Level</b>	notice 	<b>Application Category</b>	P2P
<b>Src Port</b>	5878	<b>Application Control Action</b>	drop-session
<b>logid</b>	13	<b>Sub Type</b>	forward
<b>Threat</b>		<b>Tran Display</b>	snat
<b>Date/Time</b>	1 minute ago (Wed Dec 5 22:36:10 2012)	<b>Dst Interface</b>	wan1