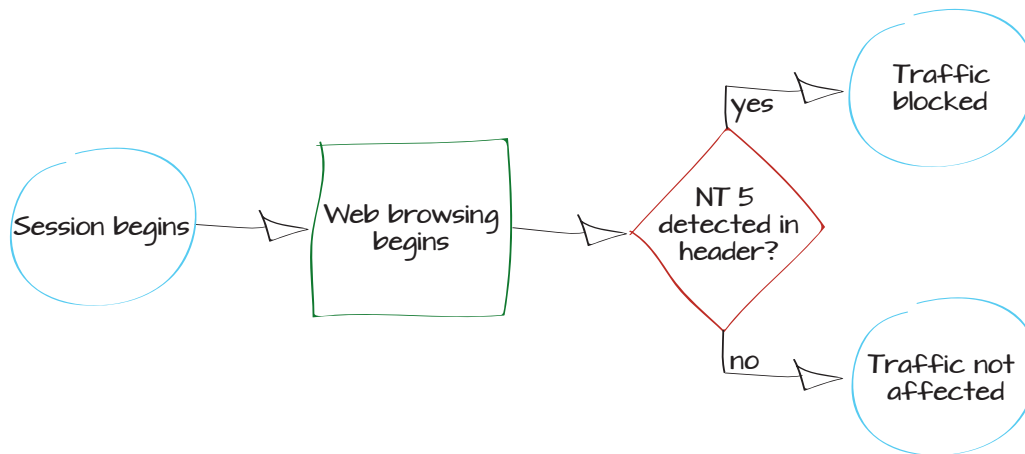


Using a custom signature to block web traffic from Windows XP

When a computer's operating system lacks vendor support, it becomes a threat to the network because newly discovered exploits will not be patched. Using the FortiGate application control feature, you can choose to restrict these computers from accessing external resources.

This recipe shows how to use application control to block web traffic from PCs running on Windows operating systems using NT 5, including Windows XP and Windows Server 2003.

1. Creating a custom application control signature
2. Creating an application control sensor
3. Adding the sensor to the outbound traffic security policy
4. Results



Creating a custom application control signature

Go to **Security Profiles > Application Control > Application List** and select **Create New**.

Use the following text to create the signature:



Make sure to remove all hard line breaks from the signature. To ensure all breaks have been removed, click and drag the bottom right corner of the signature box until the text appears in a single line.

```
F-SBID( --attack_id 8151;
--vuln_id 8151; --name "Windows.
NT.5.Web.Surfing"; --default_
action drop_session; --service
HTTP; --protocol tcp; --app_
cat 25; --flow from_client;
--pattern "Windows NT 5."; --no_
case; --context header; )
```

The signature will appear at the top of the application list and be listed in the **Web.Others** category.

Creating an application sensor

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.

Name	<input type="text" value="Windows.NT.5.Web.Su"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Signature	<pre>F-SBID(--attack_id 8151; --vuln_id 8151; --name "Windows.NT.5.Web.Surfing"; --default_action drop_session; --service HTTP; --protocol tcp; --app_cat 25; --flow from_client; --pattern "Windows NT 5."; --no_case; --context header;)</pre> <input type="button" value="Submit Signature"/>

Application Name	Category
APP Windows.NT.5.Web.Surfing	Web.Others

Name	<input type="text" value="Block Windows NT 5"/>
Comments	<input type="text" value="Comments"/> 0/255
	<input checked="" type="checkbox"/> Allow and Log DNS Traffic

After selecting **OK**, select **Create New** to add the new signature.

In order to locate the correct signature, select **Show more...** under **Category**, then select only **Web.Others**.

Set **Sensor Type** to **Specify Applications**. The new signature will appear at the top of the list. Select the signature, then set **Action** to **Block**.

The signature will now appear as part of the sensor.

Sensor Type Filter Based Specify Applications

Filter Options Basic Advanced

🔍 Type to search applications

Application Name	Category
Windows.NT.5.Web.Surfing	Web.Others
1and1	Web.Others
5GBfree	Web.Others
A2hosting	Web.Others
AOL	Web.Others
AT&T.Synaptic	Web.Others
AffinityLive	Web.Others
AffinityLive_New.Project	Web.Others
Amazon.AWS_EC2	Web.Others
Android	Web.Others
Answerbase	Web.Others
Answerbase_Answer.Question	Web.Others
Answerbase_Ask.Question	Web.Others
Aplus	Web.Others

Action

Name

Comments 0/255

Allow and Log DNS Traffic

Category	Action	Application
Web.Others	Block	Windows.NT.5.Web.Surfing
	Monitor	All Other Known Applications
	Monitor	All Other Unknown Applications

Adding the sensor to the outbound traffic security policy

Go to **Policy > Policy > Policy** and edit the policy controlling your outbound traffic.

Under **Security Policies**, enable **Application Control** and set it to use the new sensor. In order to also block HTTPS traffic, enable **SSL/SSH Inspection** and set it to use the **default** sensor.



Enabling SSL/SSH Inspection will cause web browsers to experience a certificate error. To avoid this, see [“Preventing security certificate warnings when using SSL inspection”](#) on page 271.

Results

When a PC running one of the affected operating systems attempts to connect to the Internet using a browser, the connection will fail. This includes Windows virtual machines.

PCs running on other operating systems, including later versions of Windows, will not be affected.

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 Fixed Port

Use Dynamic IP Pool

Logging Options

No Log

Log Security Events

Log all Sessions

Security Profiles

<input type="radio"/> AntiVirus	default
<input type="radio"/> Web Filter	default
<input checked="" type="radio"/> Application Control	Block Windows NT 5
<input type="radio"/> IPS	default
<input type="radio"/> Email Filter	default
<input type="radio"/> DLP Sensor	default
<input checked="" type="radio"/> SSL/SSH Inspection	default

Go to **Log & Report > Traffic Log > Forward Traffic** to see logs of the blocked traffic.

In the example, the blocked computer (IP address 192.168.100.112) was running Windows XP.



This recipe will only block web traffic from computers running the affected operating systems. If you wish to block these computers from being on the network entirely, further action will be necessary. However, the logs generated by this recipe can be used to identify the computers you wish to block.

#	Policy ID	Date/Time	Source	Destination	Security Event	Security Act
1	1	10:32:25	192.168.100.112	184.150.152.177 (img.youtube.com)	app-ctrl	⊗
2	1	10:30:27	192.168.100.111	108.160.165.12 (www.dropbox.com)	app-ctrl	⊗
3	1	08:43:27	192.168.100.112	173.194.64.100 (s.ytimg.com)	app-ctrl	⊗
4	1	10:17:33	192.168.100.112	213.180.204.25 (mail.yandex.com)	app-ctrl	⊗
5	1	08:59:14	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	⊗
6	1	08:58:36	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	⊗
7	1	08:58:16	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	⊗
8	1	08:57:00	192.168.100.112	87.250.250.25 (mail.yandex.com)	app-ctrl	⊗
9	1	08:54:03	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	⊗
10	1	08:53:09	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	⊗
11	1	08:52:42	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	⊗
12	1	08:52:28	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	⊗
13	1	08:50:00	192.168.100.112	173.194.64.100 (s.ytimg.com)	app-ctrl	⊗
14	1	08:50:00	192.168.100.112	173.194.64.100 (s.ytimg.com)	app-ctrl	⊗
15	1	08:48:35	192.168.100.112	23.41.245.231 (ocsp.entrust.net)	app-ctrl	⊗
16	1	08:44:42	192.168.100.112	173.194.64.100 (s.ytimg.com)	app-ctrl	⊗
17	1	08:43:27	192.168.100.112	173.194.64.100 (s.ytimg.com)	app-ctrl	⊗