

Making Gmail Read Only

The following procedure is to be carried out make Gmail readonly, i.e. mails can not be sent or saved as drafts.

1. Create an application as shown in the below screenshots. Make sure that correct category and sub category is selected for ease of use. Put in a discription for better understanding of the application.

The screenshot shows the 'Application' configuration window with the 'Configuration' tab selected. The 'General' section is active, showing the following fields:

- Name:** Gmail-ReadOnly
- Shared:**
- Category:** collaboration
- Sub Category:** email
- Technology:** browser-based
- Risk:** 2

The 'Characteristics' section contains several checkboxes, most of which are unchecked:

- Capable of File Transfer
- Excessive Bandwidth Use
- Tunnels Other Applications
- Has Known Vulnerabilities
- Used by Malware
- Evasive
- Pervasive
- Prone to Misuse
- Continue scanning for other Applications

The 'Description' field contains the text: "The user would be able to access mails , but would not be able to send mails or chat. Even saving of drafts would not be possible."

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

2. Set the TCP or UDP ports used by this protocol, the general TCP time out values is 300, select the parent APP as Gmail-base.

The screenshot shows the 'Application' configuration window with the 'Advanced' tab selected. The 'Defaults' section is active, showing the following fields:

- Default Port:** tcp/80
- IP protocol:** (empty)
- ICMP Type:** 1-255
- ICMP6 Type:** 1-255

The 'Timeouts' section shows the following values:

- Timeout:** 0-60-4800
- TCP Timeout:** 0-60-4800
- UDP Timeout:** 0-60-4800

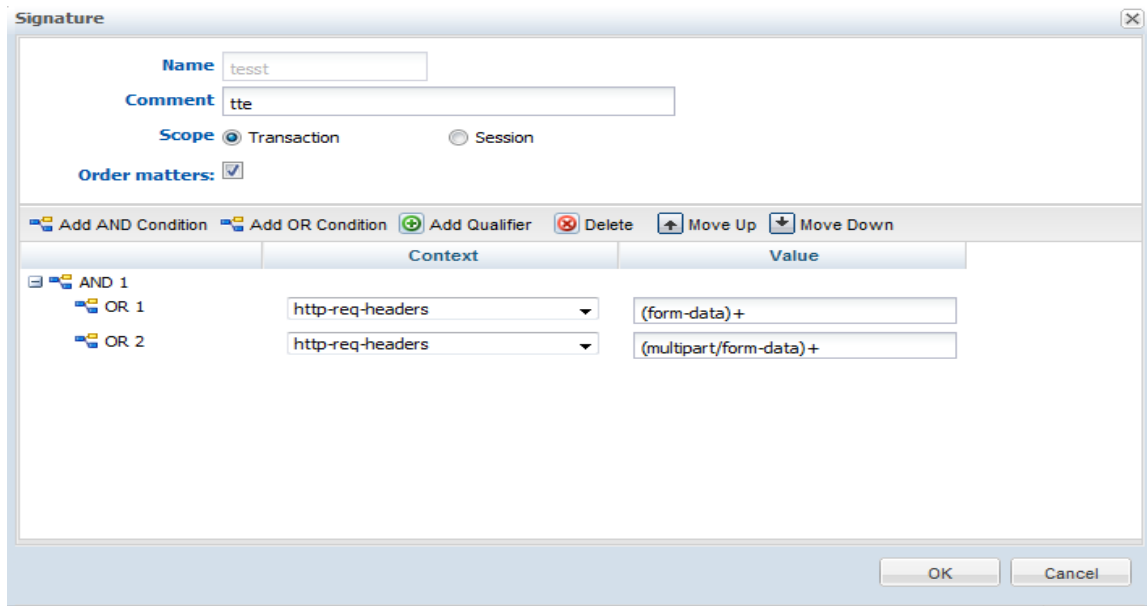
The 'Engine' section shows the 'Parent App' set to gmail-base.

The 'Scanning' section (activated via Security Profiles) shows the following checkboxes:

- File Types
- Viruses
- Spyware
- Data Patterns

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

- Click on new tab under signatures, the following pop up will appear, create the signature as shown below.

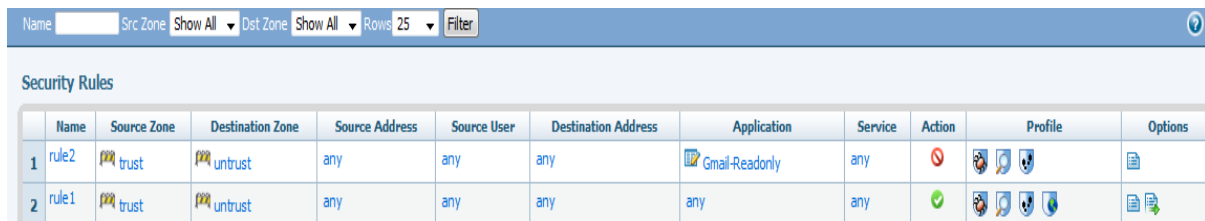


The image shows a 'Signature' configuration dialog box. It has the following fields and options:

- Name:** tesst
- Comment:** tte
- Scope:** Transaction (selected), Session
- Order matters:**
- Buttons:** Add AND Condition, Add OR Condition, Add Qualifier, Delete, Move Up, Move Down
- Table:**

	Context	Value
AND 1		
OR 1	http-req-headers	(form-data)+
OR 2	http-req-headers	(multipart/form-data)+
- Buttons:** OK, Cancel

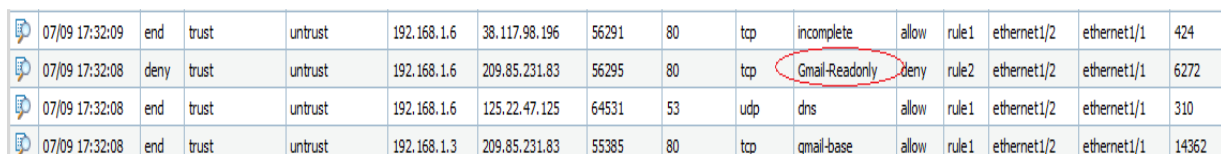
- Create a rule from trust to un-trust blocking the newly created application and commit the configuration.



The image shows a 'Security Rules' configuration table with the following columns: Name, Source Zone, Destination Zone, Source Address, Source User, Destination Address, Application, Service, Action, Profile, and Options.

	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile	Options
1	rule2	trust	untrust	any	any	any	Gmail-Readonly	any	Deny		
2	rule1	trust	untrust	any	any	any	any	any	Allow		

- Check the traffic logs to see if the respective traffic is getting blocked.



The image shows a traffic logs table with the following columns: Time, Action, Source Zone, Destination Zone, Source Address, Source User, Destination Address, Port, Protocol, Application, Action, Rule, Profile, and Bytes.

07/09 17:32:09	end	trust	untrust	192.168.1.6	38.117.98.196	56291	80	tcp	incomplete	allow	rule1	ethernet1/2	ethernet1/1	424
07/09 17:32:08	deny	trust	untrust	192.168.1.6	209.85.231.83	56295	80	tcp	Gmail-Readonly	deny	rule2	ethernet1/2	ethernet1/1	6272
07/09 17:32:08	end	trust	untrust	192.168.1.6	125.22.47.125	64531	53	udp	dns	allow	rule1	ethernet1/2	ethernet1/1	310
07/09 17:32:08	end	trust	untrust	192.168.1.3	209.85.231.83	55385	80	tcp	gmail-base	allow	rule1	ethernet1/2	ethernet1/1	14362