suomicom

Walled Garden Framework

By: Jouko Maksimainen

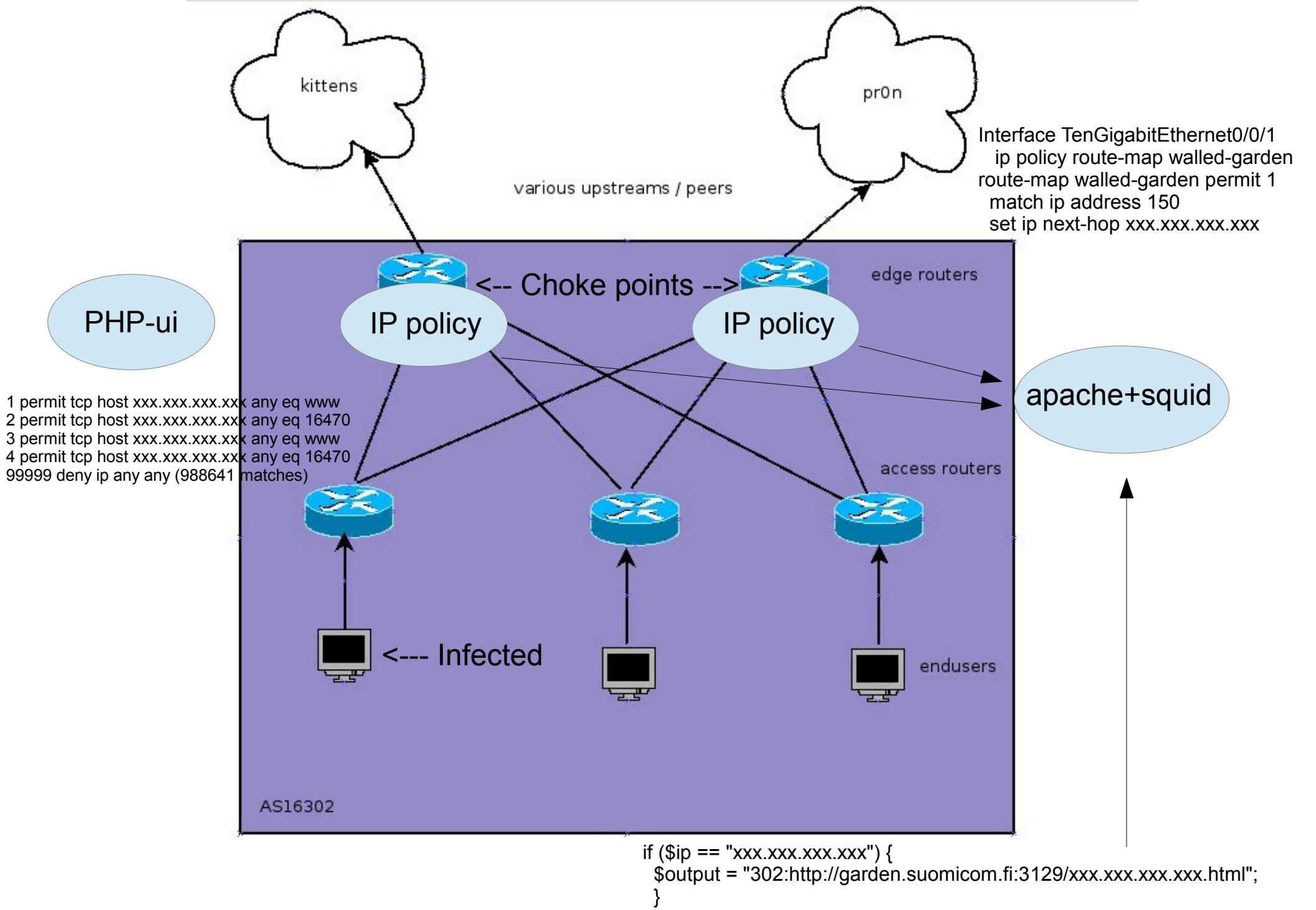
suomicom

Problem description: infected hosts

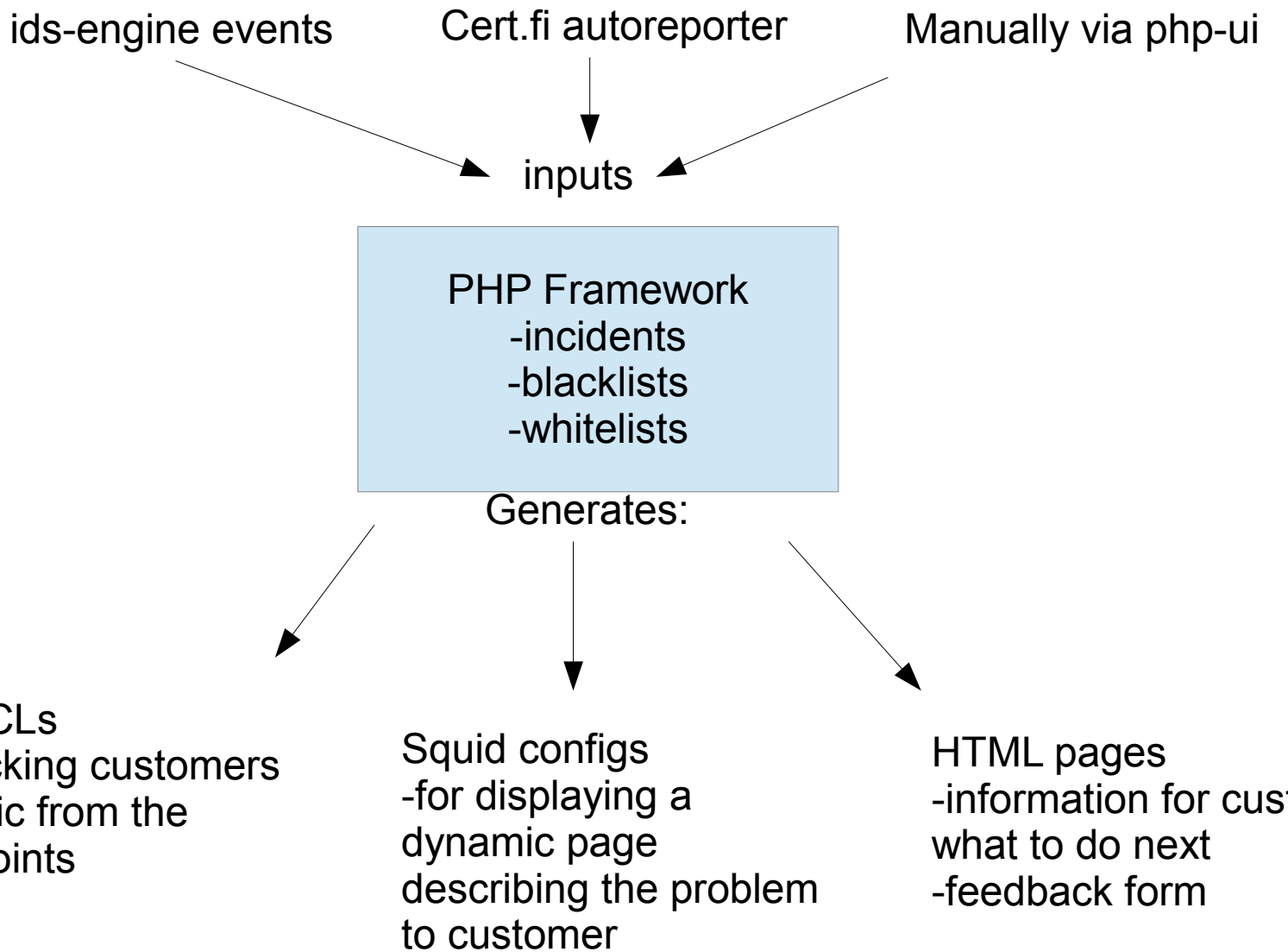
- get rid of malicious traffic

- inform the user about a problem

- mechanize all you can, offload some work from helpdesk/service desk (automatized system)


kittens
pr0n
various upstreams / peers
Interface TenGigabitEthernet0/0/1
ip policy route-map walled-garden
route-map walled-garden permit 1
match ip address 150
set ip next-hop xxx.xxx.xxx.xxx
edge routers
<-- Choke points -->
PHP-ui
IP policy
IP policy
apache+squid
1 permit tcp host xxx.xxx.xxx.xxx any eq www
2 permit tcp host xxx.xxx.xxx.xxx any eq 16470
3 permit tcp host xxx.xxx.xxx.xxx any eq www
4 permit tcp host xxx.xxx.xxx.xxx any eq 16470
99999 deny ip any any (988641 matches)
access routers
<--- Infected
endusers
AS16302
if ($ip == "xxx.xxx.xxx.xxx") {
$output = "302:http://garden.suomicom.fi:3129/xxx.xxx.xxx.xxx.html";
}

Walled Garden



Walled Garden

MENU

RULES
-list
-search
-add

BLACKLIST
-list
-add

WHITELIST
-list
-add

SC Walled Garden 0.5

Listing active rules

ID	Incident description (shown to client)	Template	Message from customer	Rule created	Rule modified	Logstring (internal note)	Timeout (min)	State	
108	Datasource: B, Malware type: ZeroAccess, C&C: 70.189.34.36/16470, AS: 22773, DNS name: ip70-189-34-36.lf.br.cox.net			2013-10-21 15:10:06	2013-10-23 13:37:26	Imported from email	3600	ACTIVE!	Edit incident
Rules:	Add new rule				IP	Port	Protocol	State	
	delete this rule				70.189.34.36	16470	tcp	ACTIVE!	Edit rule
	delete this rule				188.127.[redacted]	80	tcp	ACTIVE!	Edit rule

ID	Incident description (shown to client)	Template	Message from customer	Rule created	Rule modified	Logstring (internal note)	Timeout (min)	State	
105	Datasource: B, Malware type: ZeuS, C&C: 173.193.197.194/80, AS: 36351, C&C url: /, DNS name: fuxgdtmnbdzlrdjrbafcynr.info			2013-10-21 15:10:06	2013-10-23 13:37:33	Imported from email	3600	ACTIVE!	Edit incident
Rules:	Add new rule				IP	Port	Protocol	State	
	delete this rule				79.134.[redacted]	80	tcp	ACTIVE!	Edit rule

ID	Incident description (shown to client)	Template	Message from customer	Rule created	Rule modified	Logstring (internal note)	Timeout (min)	State	
104	Datasource: B, Malware type: ZeroAccess, C&C: 68.231.30.9/16470, AS: 22773, DNS name: ip68-231-30-9.ph.ph.cox.net			2013-10-21 15:10:06	2013-10-23 13:37:37	Imported from email	3600	ACTIVE!	Edit incident
Rules:	Add new rule				IP	Port	Protocol	State	
	delete this rule				68.231.30.9	16470	tcp	ACTIVE!	Edit rule
	delete this rule				188.127.[redacted]	80	tcp	ACTIVE!	Edit rule

suomicom
enemmän kuin laajakaista

Internet-yhteyttänne on rajoitettu

Koneellisessa seurannassa on havaittu, että yhteyttänne (IP-osoitteessa 79.134.113.149) käyttää jokin haittaohjelmalla saastunut tietokone tai muu laite. Tästä johtuen liikenteesi ohjataan hetkeksi tälle sivulle tiedotustarkoituksessa.
Jotta välttyisitte jatkossa tältä ilmoitukselta, tulee teidän puhdistaa haitallista liikennettä aiheuttava laite tai poistaa se pikimmiten verkosta. Voitte käyttää tietokoneen puhdistuksessa tunnettujen tietoturvayhtiöiden palveluita, joiden linkkejä löydätte alempaa.

Yrityskäyttäjän kannattaa ensisijaisesti ottaa yhteyttä omaan lähitukeen ongelman ratkaisemiseksi.

IN ENGLISH

An infection has been detected on your computer or network connected device
(on IP-address 79.134.113.149) and web traffic is temporarily redirected to this infopage.
To fix the problem, please clean your infected devices with an anti-malware software or physically remove the device from the network. You may find the links below helpful when cleaning your computer.

In case you are a corporate user, please contact your local IT-support about the matter.

F-Secure Online Scanner

Norton Security Scan

Kaspersky lab Free Virus Scan

Tarkempia teknisiä tietoja ongelman aiheuttajasta / Technical details about the problem:

```
Datasource: B, Malware type: ZeuS, C&C: 173.193.197.194/80, AS: 36351, C&C url:
/, DNS name: fuxgdtmnbdzlrdjrbafcynr.info,tcp:80
```

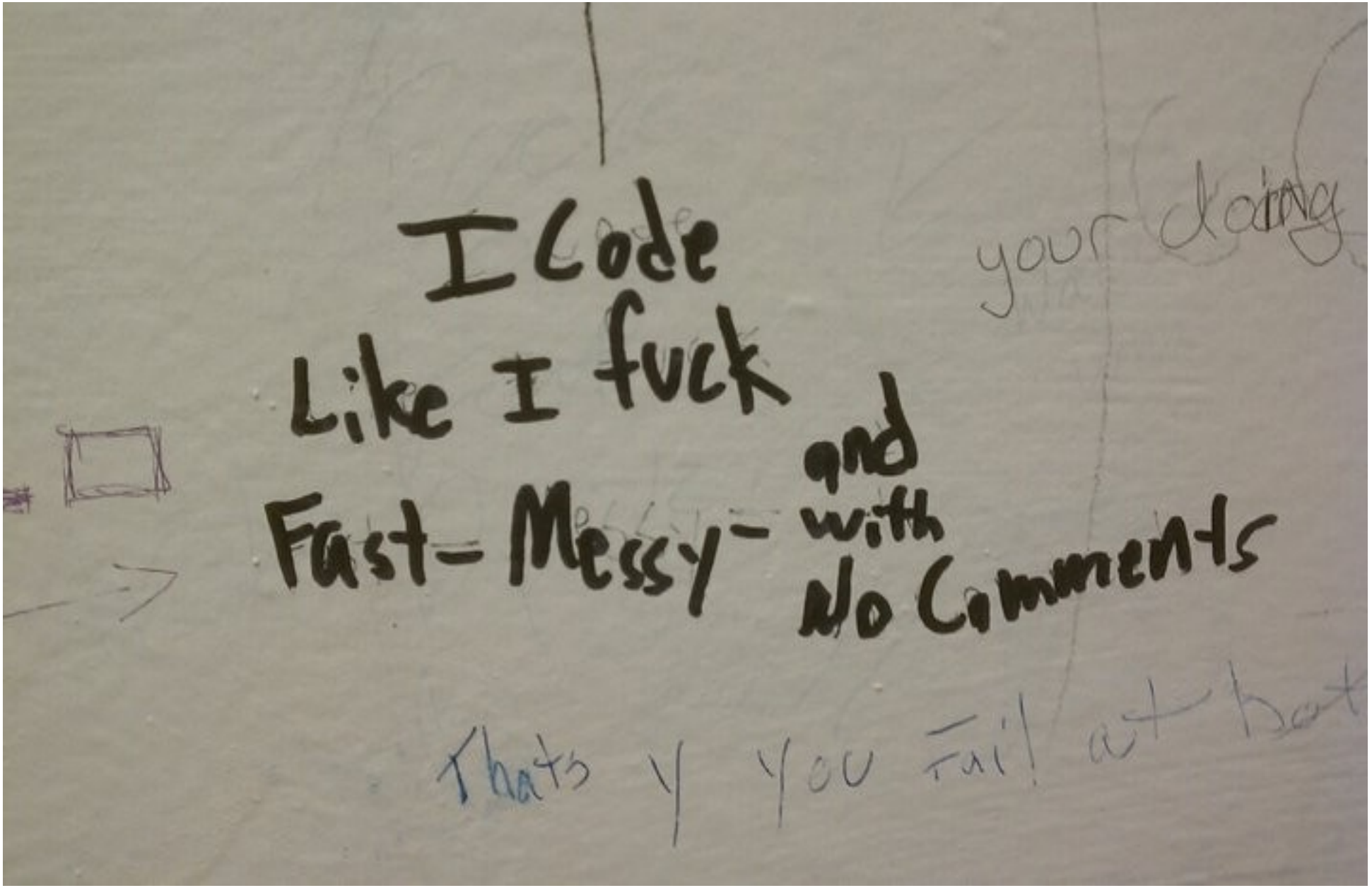
suomicom

Features

- Support for white/blacklists
- Templates for different kind of incidents
- Events from IDS (in unified2 format) and email attachments (IMAP)
- Feedback to help-desk's email/ticketing system directly from customer
- Easy way to manipulate traffic (leaving or incoming to your network)
- GPL, open source, do what you wish (or don’t!)

suomicom

Disclaimer:



suomicom

THANK YOU!

- Project on sourceforge:

kittengarden.sourceforge.net

Questions?