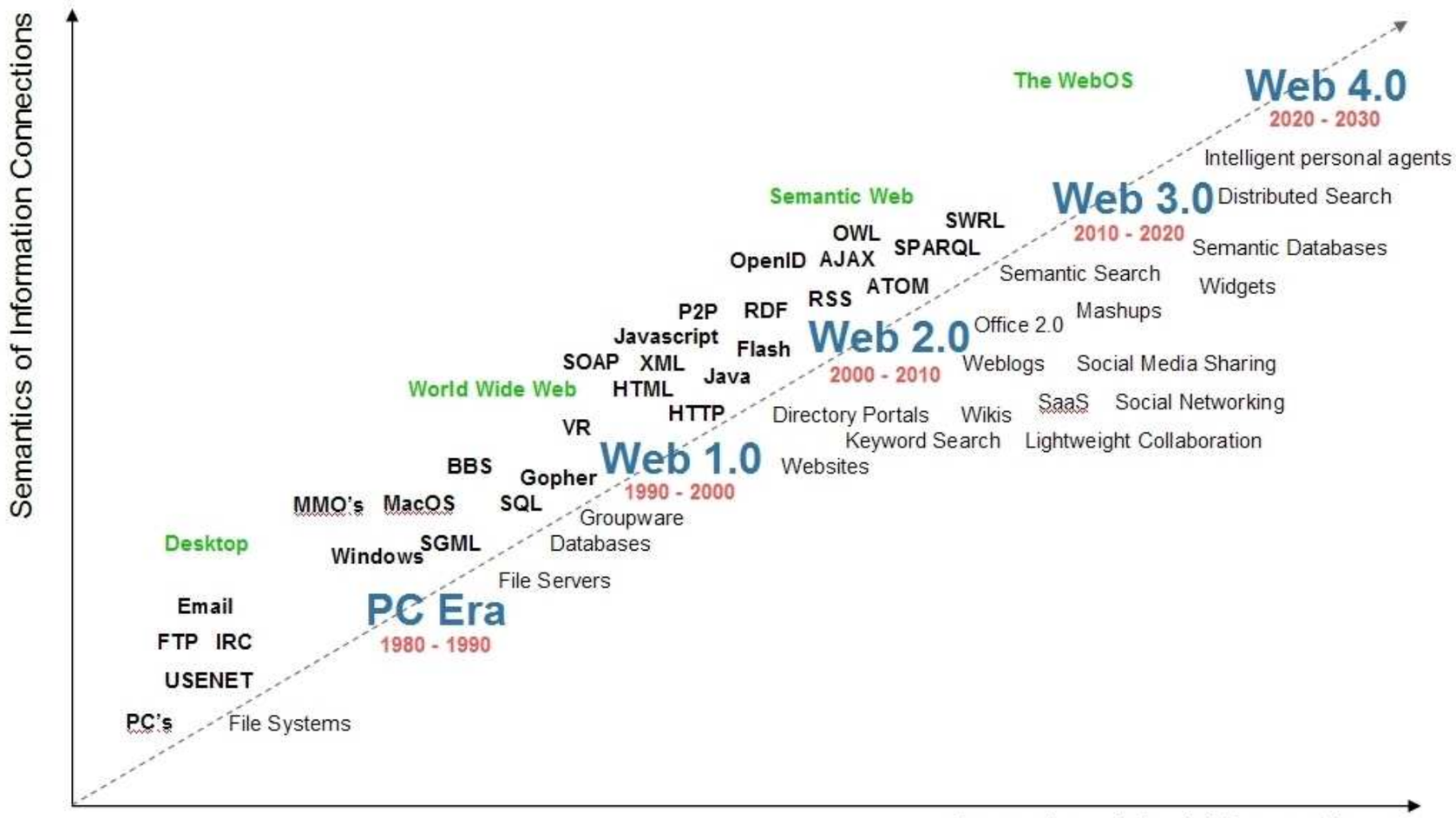
WEB 3.0 i sigurnost aplikacija

Goran Peteh
gopeteh@cisco.com
System Engineer, CCSP

WEB 3.0 i sigurnost aplikacija



My web history... nxoc01.cern.ch...

vrijeme

www

ja

Vanja

1990	1994	2004/2005	2006	2009
nxoc01.cern.ch	broj web siteova 10,000	broj web siteova 56,923,000	broj web siteova 105,244,000	broj web siteova 185,497,000
Nisam imao blage veze da postoji internet	Kupio prvo računalo u podrumu jedne danas poznate IT kompanije 	Voditelj Cisco NetAkademije  14.06.2004. 	Systems Engineer at Cisco Systems  26.06.2006. 	Korisnik sam: LinkedIN Facebook Gmail Gtalk MySpace YouTube Skype Sametime  Korisnik:

www.cisco.com

Warning – Disclaimer - Upozorenje

Neither Cisco or the presentor encourages the use of any methods and/or tools mentioned within this presentation without the expresses aproval and signed agreement with the owner of the IT infrastructure in question.

The unathorised usage of the aforementioned tools and/or methods could lead to legal prosecution and severe penalties.

Sigurnost jučer, danas, sutra

Sigurnost jučer, danas, sutra

www.remote-exploit.org

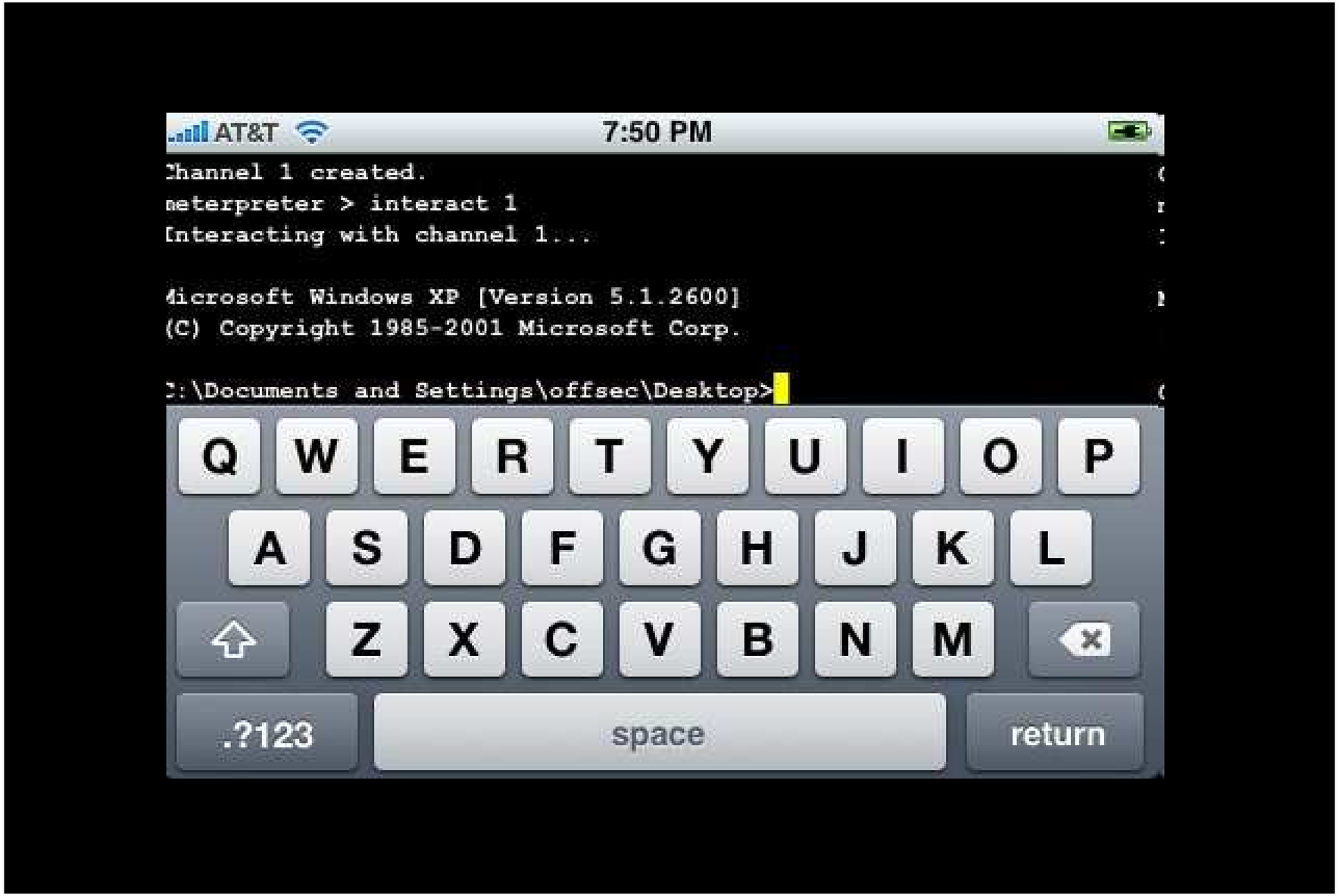
Sigurnost jučer, danas, sutra

www.metasploit.com

Demo 1

Demo 2 – buši, buši...


AT&T
7:41 PM
=[msf v3.1-release
+ -- --=[262 exploits - 117 payloads
+ -- --=[17 encoders - 6 nops
=[46 aux
msf > use windows/browser/ms06_001_wmf_setabortproc
msf exploit(ms06_001_wmf_setabortproc) > set
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return


AT&T
7:50 PM
Channel 1 created.
meterpreter > interact 1
Interacting with channel 1...
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\offsec\Desktop>
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
.?123
space
return

Introducing Cisco's ACE Web App Firewall

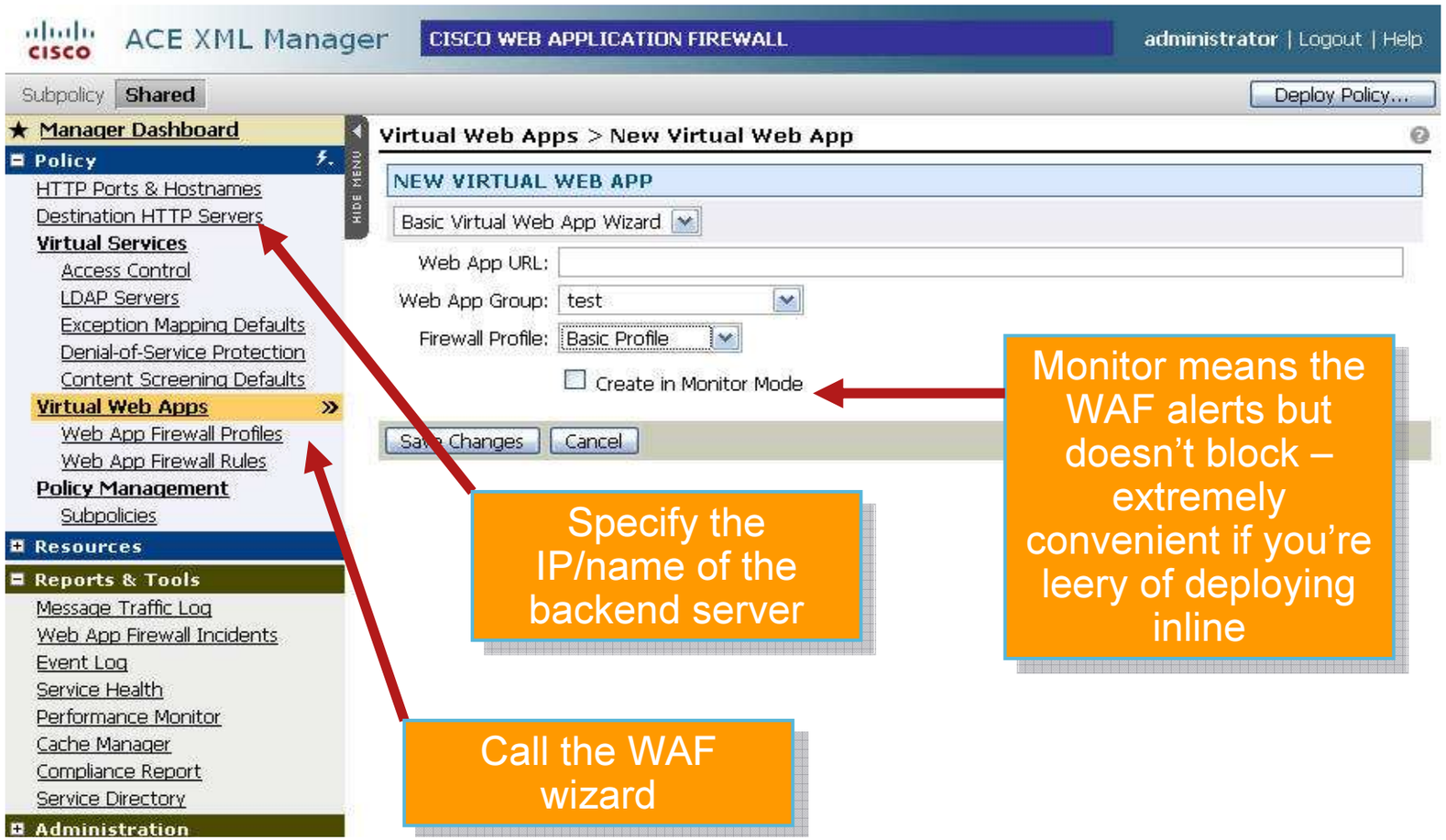
- Builds on top of industry-leading ACE XML Gateway platform
- Simple software upgrade to install Web Application Firewall

Web Application Firewall	Protects your custom HTTP/HTML applications from high-impact web-borne attacks
SOA/Web Services/XML Threat Defense	Secures and offload web services transactions

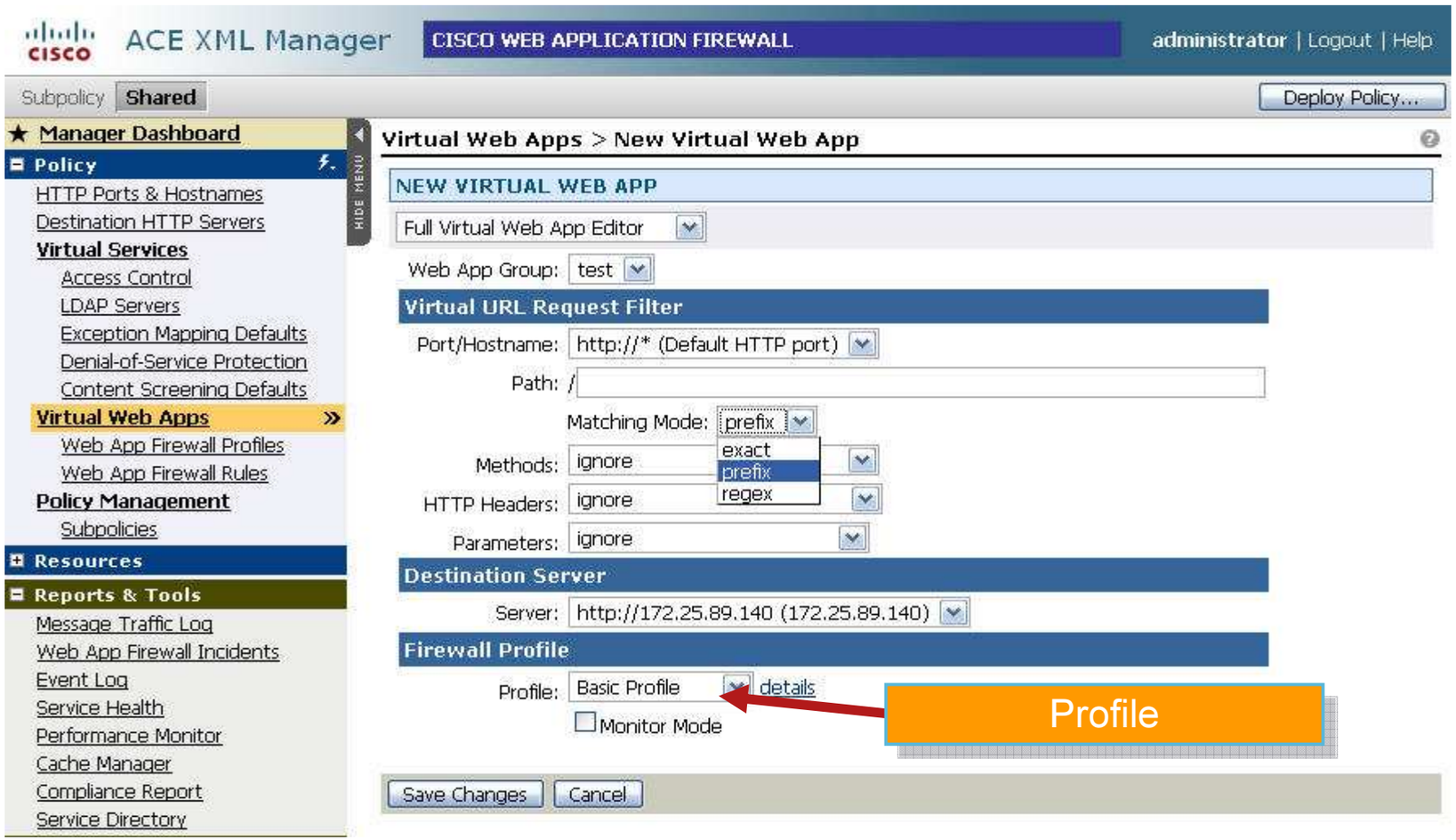
Cross-Site Scripting (XSS) attacks

- **What is it?**
  - –A malicious script is echoed back into HTML returned from a trusted web site. The scripts executes locally on the client.
  - –Extremely widespread – some experts estimate 70%-80% of websites are vulnerable
- **What are the implications?**
  - –Web Site Defacement
  - –Session IDs stolen (cookies exported to hacker's site)
  - –Browser security compromised – control given to hacker
  - –All data sent between client and server potentially hijacked

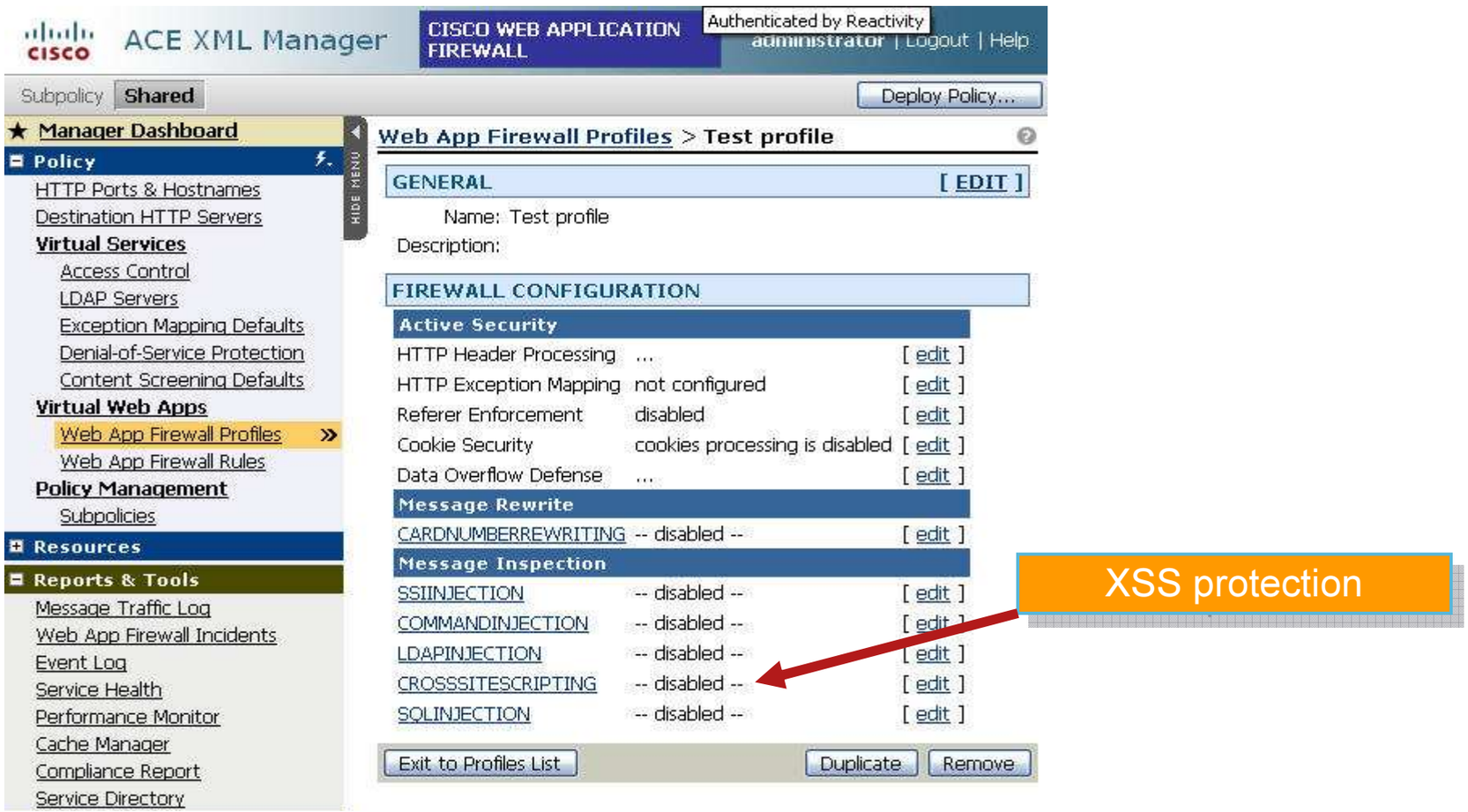
Getting started with the Cisco ACE WAF



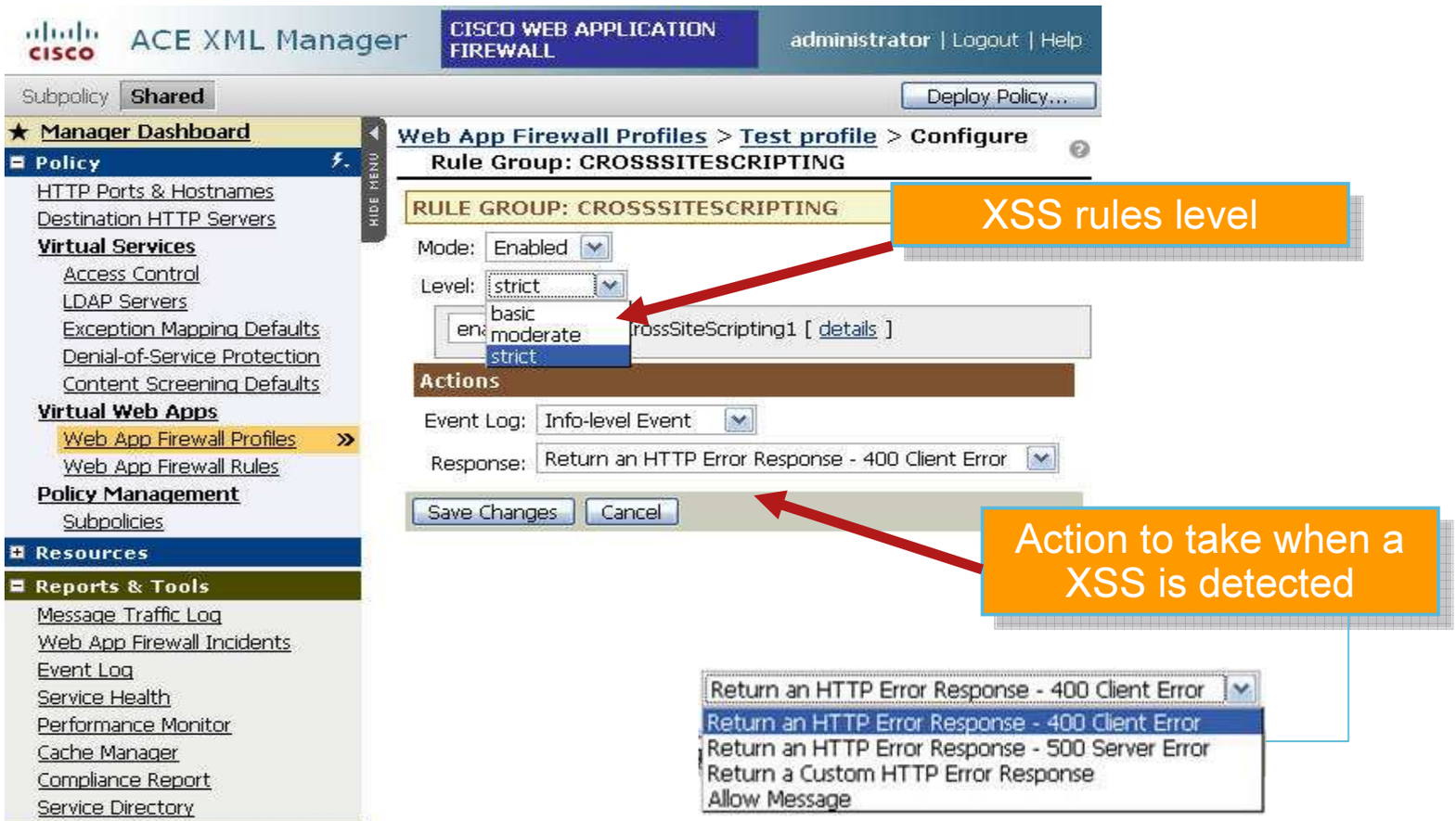
Getting started with the Cisco ACE WAF



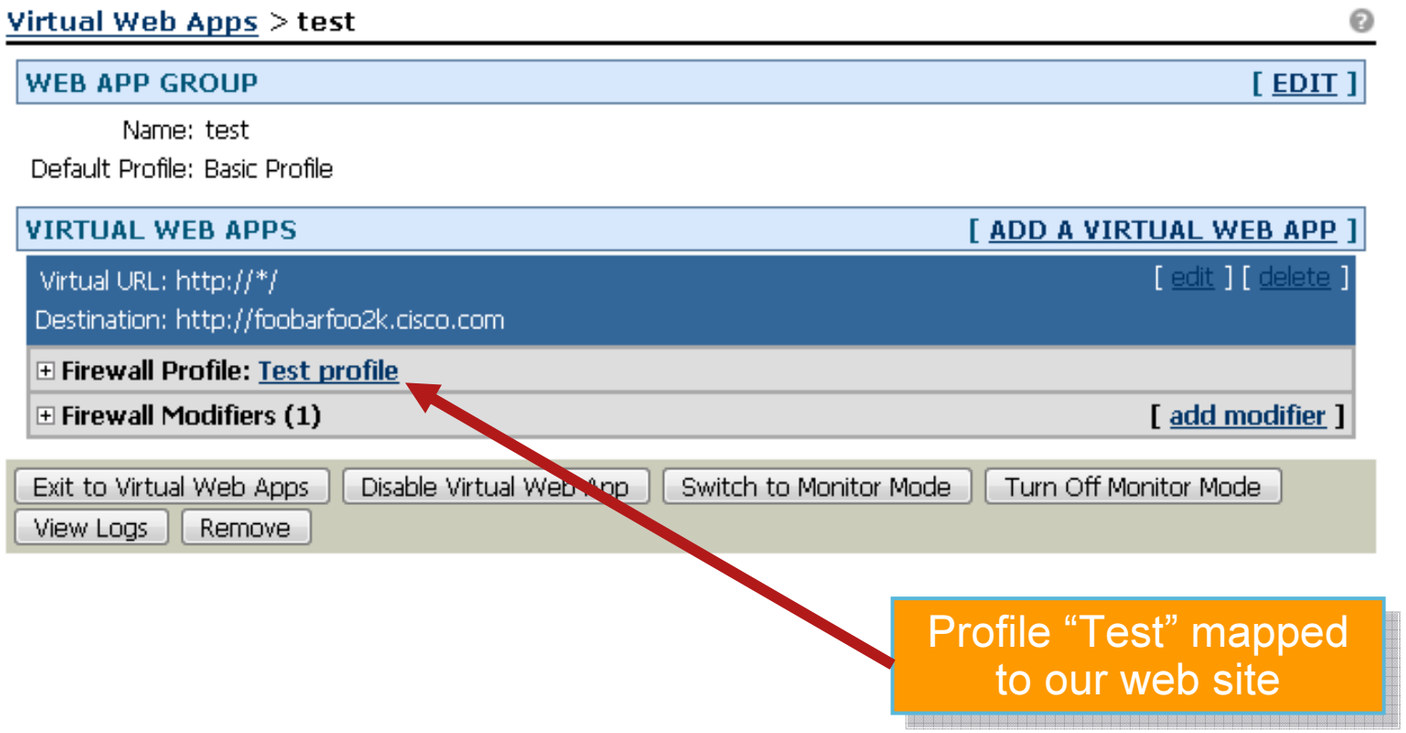
Protecting the web site from XSS



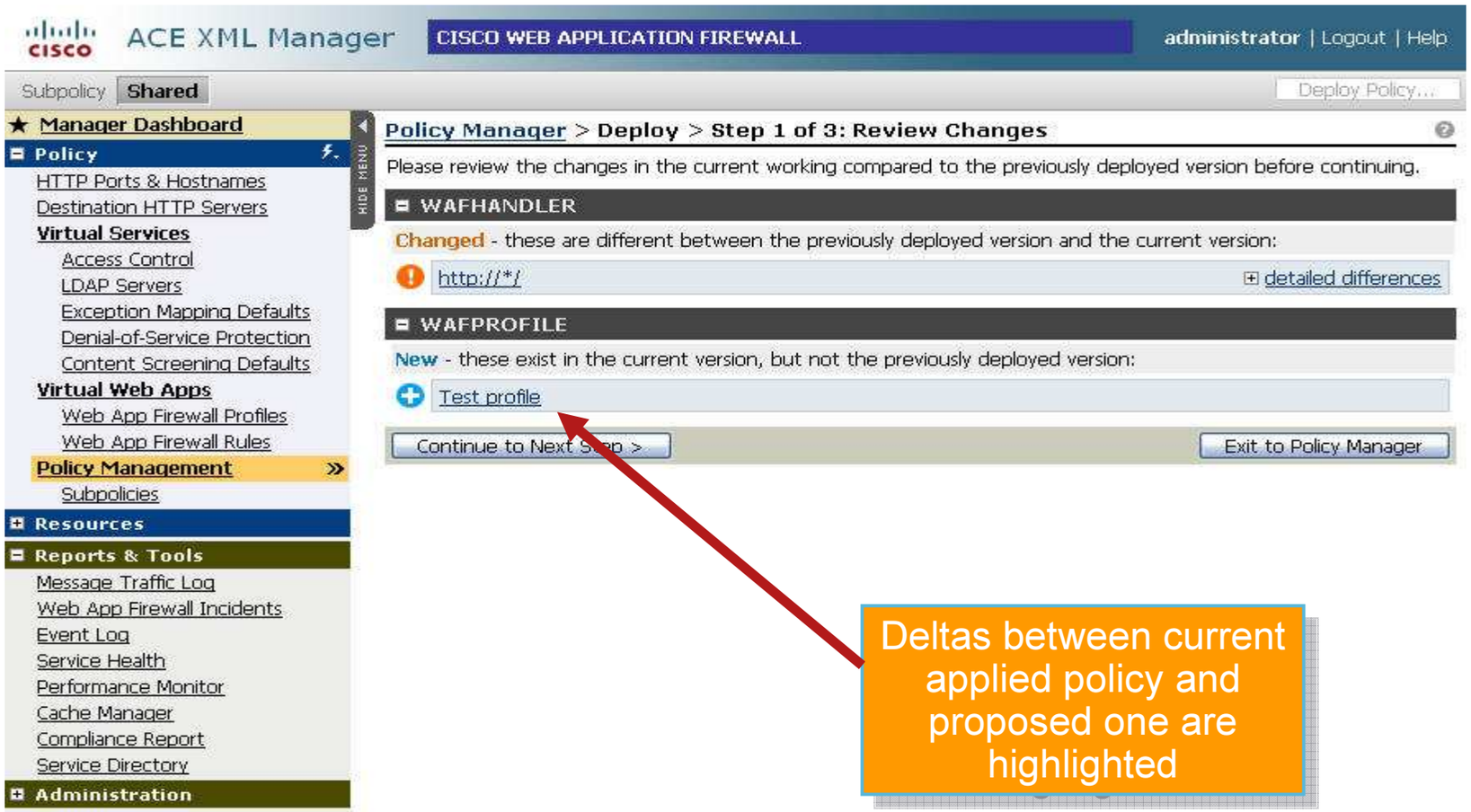
Fine-tuning a security profile



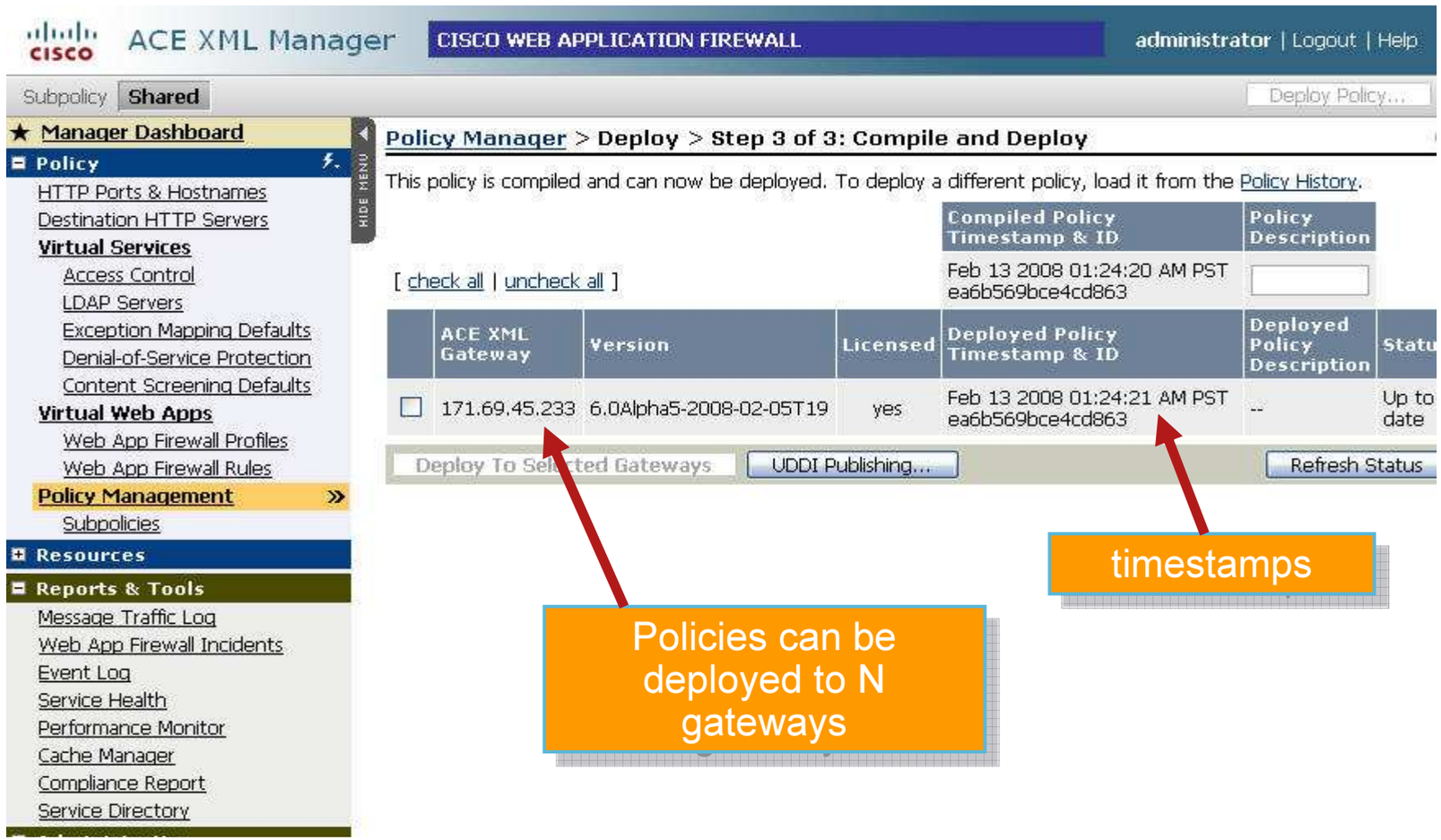
Associate the profile to the web site



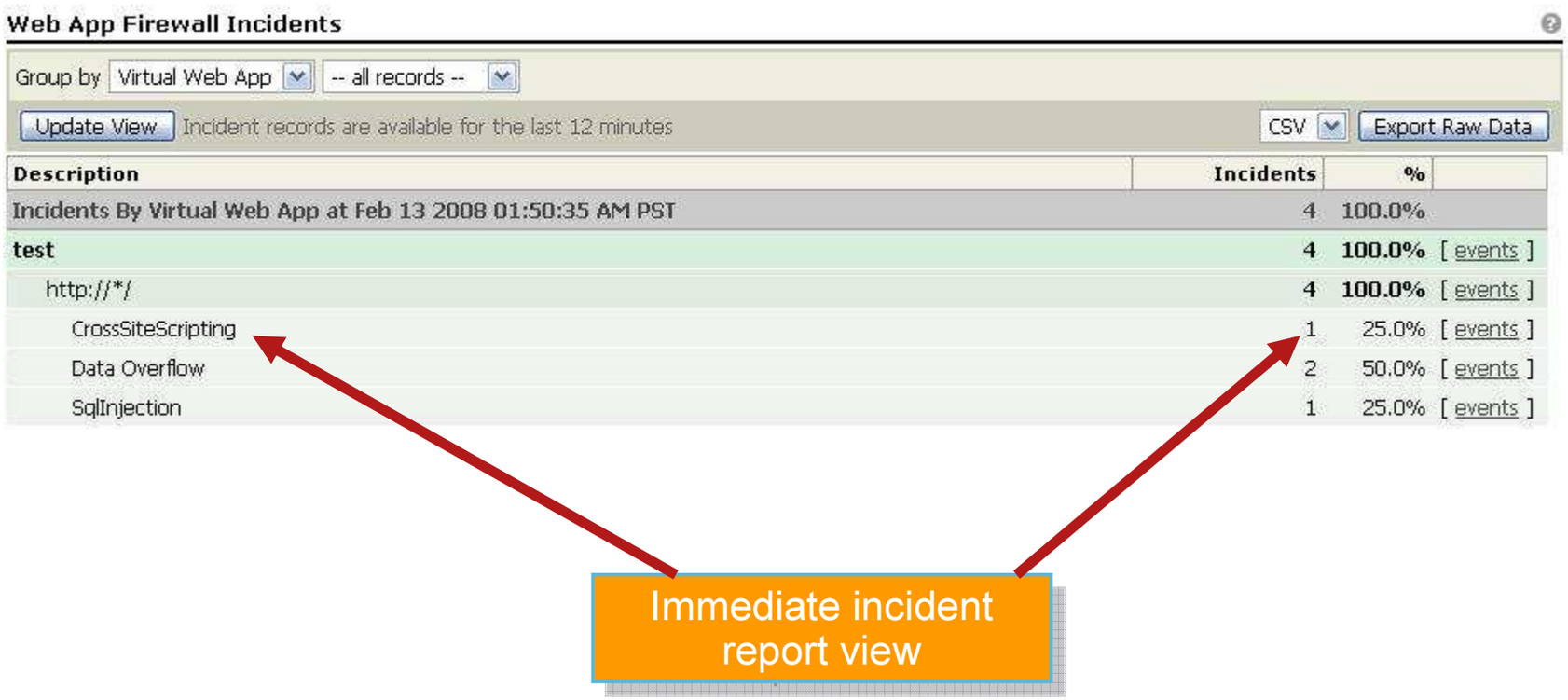
Deploy the policy to the WAF gateway(s)



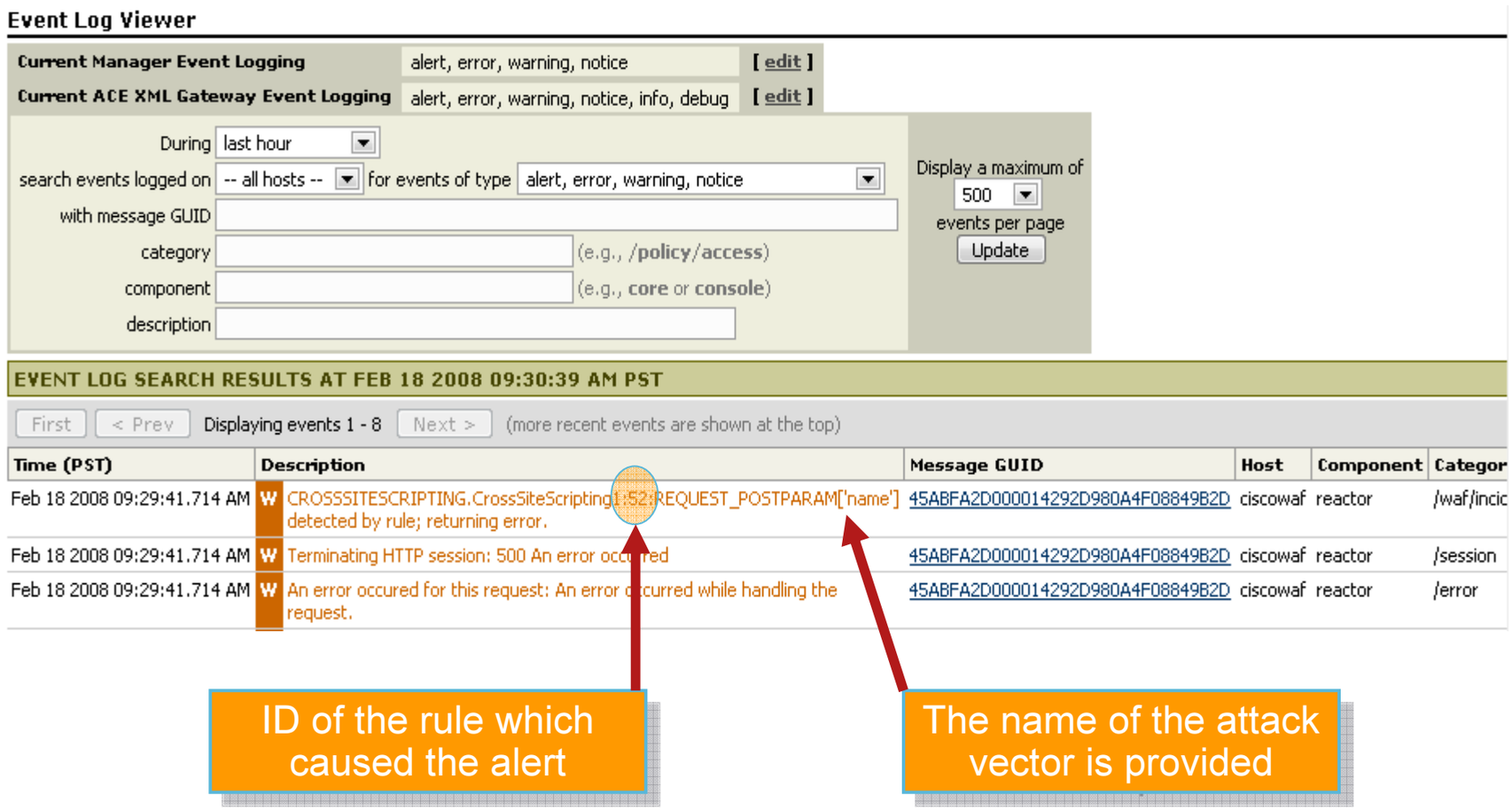
Verification of successful deployment



The web site is under attack!



Let's drill down



Detailed security event drill down

EVENT LOG SEARCH RESULTS AT FEB 18 2008 09:34:51 AM PST

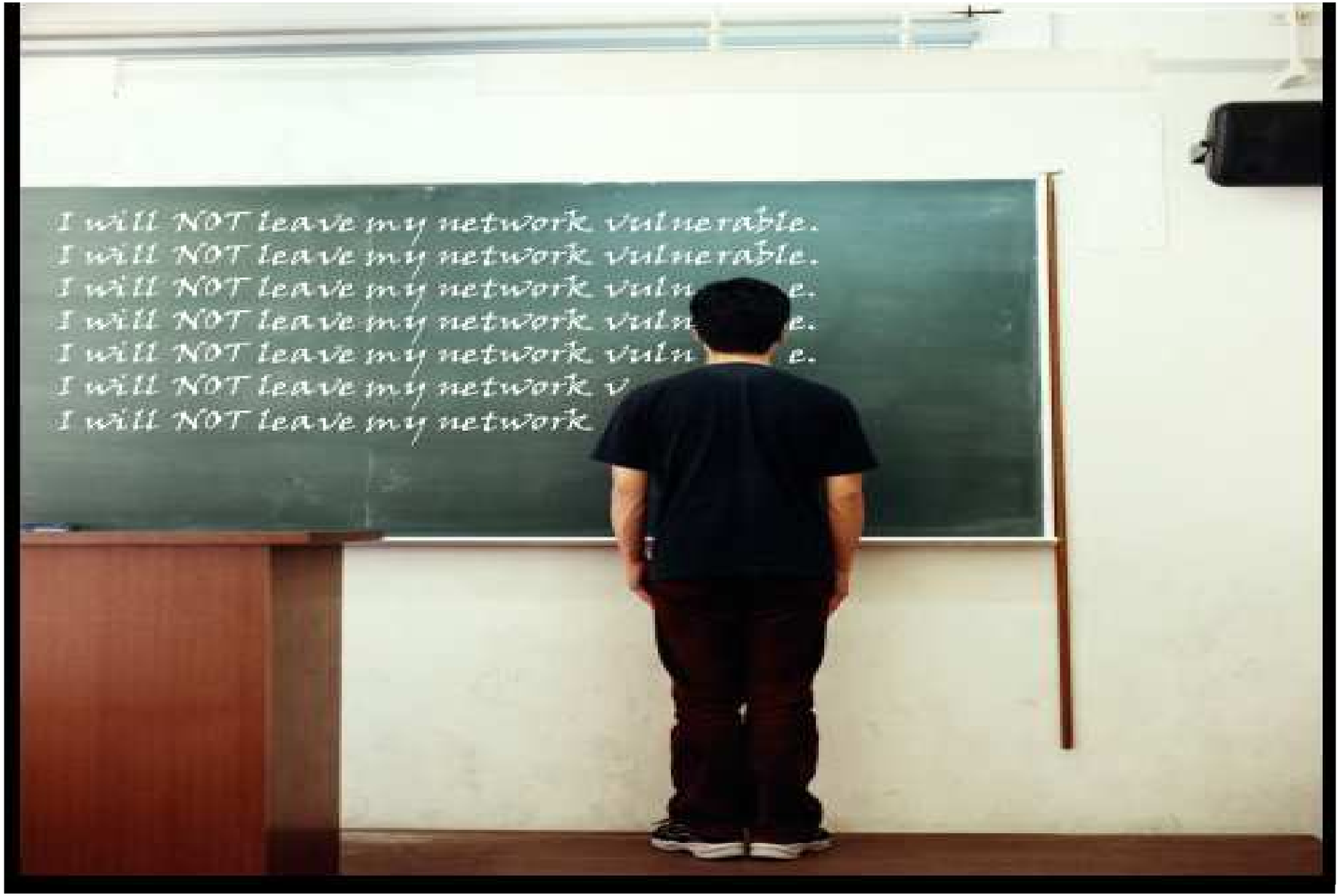
First | < Prev | Displaying events 1 - 14 | Next > | (more recent events are shown at the top)

Time (PST)		Description
Feb 18 2008 09:29:41.714 AM	D	Awaiting new request on inbound connection
Feb 18 2008 09:29:41.714 AM	W	CROSSSITESCRIPTING.CrossSiteScripting1:52:REQUEST_POSTPARAM['name'] detected by rule; returning error.
Feb 18 2008 09:29:41.714 AM	W	Terminating HTTP session: 500 An error occurred
Feb 18 2008 09:29:41.714 AM	W	An error occured for this request: An error occurred while handling the request.
Feb 18 2008 09:29:41.714 AM	I	No policy-specific error handler for WAF.CROSSSITESCRIPTING.CrossSiteScripting1:$(SIG_MATCH_SIGID):$(SIG_MATCH_INPUT_NAME):
Feb 18 2008 09:29:41.713 AM	I	Checking limit 1
Feb 18 2008 09:29:41.713 AM	I	Checking limit 0
Feb 18 2008 09:29:41.713 AM	I	Checking 3 limits
Feb 18 2008 09:29:41.713 AM	I	Accepted a new HTTP POST request from 171.69.141.0 for /SCRIPTS/xss.php
Feb 18 2008 09:29:41.713 AM	I	HTTP POST request for /SCRIPTS/xss.php from 171.69.141.0 matched Port 'Default HTTP port'; checking for handler
Feb 18 2008 09:29:41.713 AM	I	Performing normalization on '/SCRIPTS/xss.php' with mode 7211
Feb 18 2008 09:29:41.713 AM	D	HTTP Trace IN: Content-Type: application/x-www-form-urlencoded Content-Length: 58 name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
Feb 18 2008 09:29:41.711 AM	D	HTTP Trace IN: POST /SCRIPTS/xss.php HTTP/1.1 Host: foobarfoo2k.cisco.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.12) Gecko/20080201 Firefox/2.0.0.12 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Connection: keep-alive Referer: http://foobarfoo2k.cisco.com/SCRIPTS/xss.php Cookie: cec_user_id=cpaggen; SMIDENTITY=zv5hvichtfb9t4nGfXC5vsozOJXocY3BBaVM0802pEHDUDb4mPvEBkbi0dOg+xO//TRZiz0UpMcRa3IWnmLDn3PaHSz74dXfY3ILI

Full dump of incoming request

What the user/hacker/victim sees

- The error message are HTTP return code are fully customizable! You can return your own HTML code and for example redirect the hacker to the main page.


I will NOT leave my network vulnerable.
I will NOT leave my network vulnerable.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network vuln e.
I will NOT leave my network v
I will NOT leave my network


CISCO