Array NETWORKS
Access. Security. Performance.

SSO by HTTP POST GUIDE

Oct 2007

2009-11-18

Design Spec

When the SPX detects a client request for the login page URL which has been configured on SPX box, we'll issue a POST request to the backend server and perform the SSO functionality

The response pages maybe are:

- Login succeeded page (the page client requested is one configured login URL)
- The real page which client wants to see but not login succeeded page
- Login page (when SSO failed)

SSO kicks in only once per login per URL

Administrator only can define 64 URLs which should do SSO process per virtual site

If user logout from the backend server, he will have to login manually to backend server or logout from SPX and login to the SPX over again (because the session is new, the session can do SSO POST once again).

SSO POST related CLI commands

Global shell

virtual site session reuse off <virtual site id>

(session reuse must be off when you need to use SSO POST)

Virtual site shell

sso on

sso post <hostname> <login url> <username field> <password field> [post host] [post url] [other post fields] [bookmark] (every parameter usage method refers to app_guide)

(the pair of <hostname> and <login url> should be unique per virtual site; when backend server's port is not 80, please configure <hostname> like 10.1.1.1:8080)

no sso post <hostname> <login url>

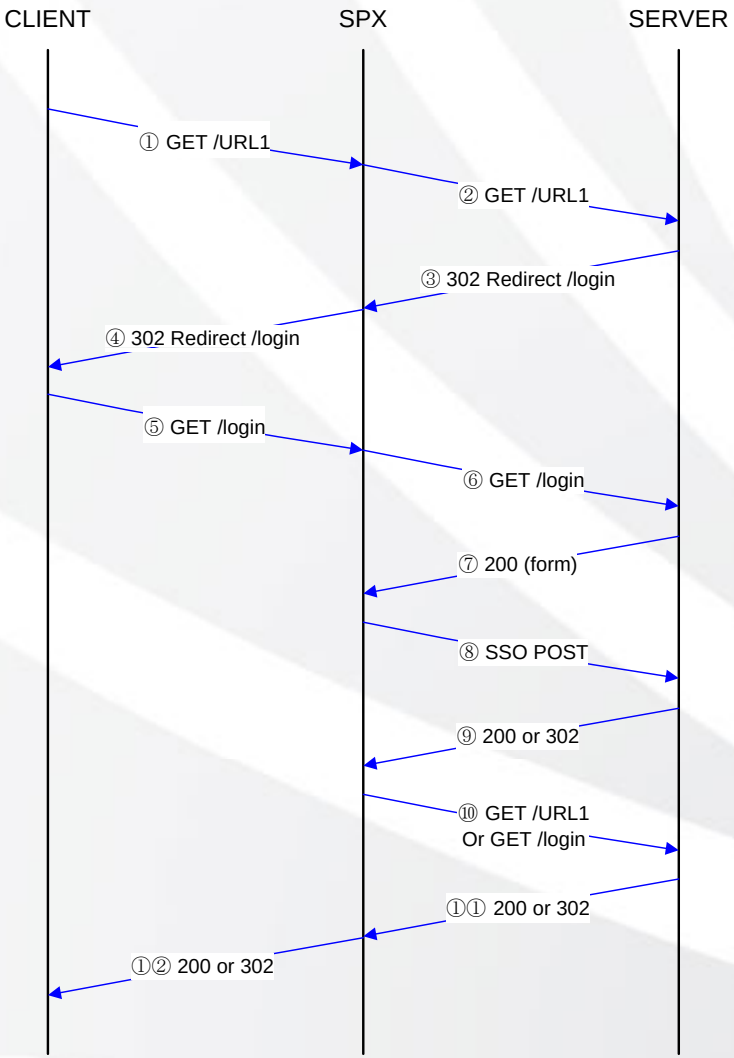
[show | clear] sso config (clear the SSO POST rules and set "sso off")

[show | clear] sso post (only clear the SSO POST rules)

portal link <link url> <link text> [position]

(the portal link command is not necessary)

SSO POST Process



If the link configured in “portal link” is the login URL, will go to step 5 directly; otherwise, will start from step 1 (when start from step 1, customer’s system must response with 302 to let client IE redirect to /login URL)

After client side send out GET /login (step 5), SPX will find out the request needs to do SSO POST by the configuration of “sso post” rule

At step 8, SPX will assemble one POST package x by the parameter in the “sso post” rule (so, before we configure “sso post” rule, we must know the POST package content when client do the direct access)

At step 10, SPX will resend the GET request cached by the step 5 or step 1 (the purpose of step 10 is let client user see the actual login page when the username and password on SPX is different from the backend system; and when client start from step 1, after successfully login to ba ckend system via POST from SPX, client user can see the URL1 page directly –
this is the real meaning of SSO actually)

Scenario of Customer System

- Before configure SSO on SP, we must analyze the HTTP trace when using direct access
- After client sends out GET /URL1 (step 1), if backend server response with “200 OK” (the response page is the login page), we must not configure URL1 in the “portal link” at that time; we must configure /login url on the portal
- **When using direct access, after login to backend server successfully, in the IE url bar, input the /login url directly (try to GET /login page after login) to see whether the backend server will response with real login page or not (if the backend server response with real login page and let user to login again, SORRY, we can not support it now)**
- WRM must be enabled when you want to use SSO POST
- SSO POST also supports the HTTP traffic from L4 VPN

Configuration Example

Port = 80

sso on

sso post "10.3.52.80" "discuz/logging.php?action=login" "username" "password" "" "/discuz/logging.php?action=login&" "questionid=0&answer=&loginsubmit=%E6%8F%90+%C2%A0+%E4%BA%A4" "disable"

(sso post “10.3.52.80” “discuz/logging.php?action=login” “username” “password” “10.3.52.80” “discuz/logging.php?action=login&” “questioned=0&answer=&loginsubmit=%E6%8F%90+%C2%A0+%E4%BA%A4” “disable”

IS totally same with the above CLI)

portal link "http://10.3.52.80/discuz/logging.php?action=login" "sso test" 1

Configuration Example (Cont.)

Port != 80

sso on

sso post "10.3.52.80:8080" "discuz/logging.php?action=login" "username" "password" "" "/discuz/logging.php?action=login&" "questionid=0&answer=&loginsubmit=%E6%8F%90+%C2%A0+%E4%BA%A4" "disable"

(sso post “10.3.52.80:8080” “discuz/logging.php?action=login” “username” “password” “10.3.52.80:8080” “discuz/logging.php?action=login&” “questioned=0&answer=&loginsubmit=%E6%8F%90+%C2%A0+%E4%BA%A4” “disable”
IS totally same with the above CLI)

portal link "http://10.3.52.80:8080/discuz/logging.php?action=login" "sso test" 1

Because the configuration of SSO POST totally rely on the implementation of backend server, so I will make one example of “step by step” to descript how to configure it

Configure – Step by Step (OWA2003)

Firstly, please note that if the backend server is using HTTPS, the configuration of SSO POST is totally same with the server which using HTTP (because the SSO POST handled in the proxy module, and so, the HTTPS port number will not influence the SSO POST)

The following example is based on our customer ZJSY which using one HTTPS OWA 2003 server

Step 1 – under direct access

The Following steps should be done by using direct access to backend server (without using SPX box)

1. Find out the page which includes the input box of USERNAME and PASSWORD (the screenshot is on next slide)

   We can get the parameter ***<hostname> <login url>*** of "**sso post**"

   <hostname> - "mail.pdiwt.com.cn"

   <login url> - "/exchweb/bin/auth/owalogon.asp"

Then, we can configure the above link on the portal by using *portal link*

"https://mail.pdiwt.com.cn/exchweb/bin/auth/owalogon.asp" "web mail access" (after we finish the SSO POST rule configuration, when client user click the portal link of "web mail access", SSO POST will be triggered)

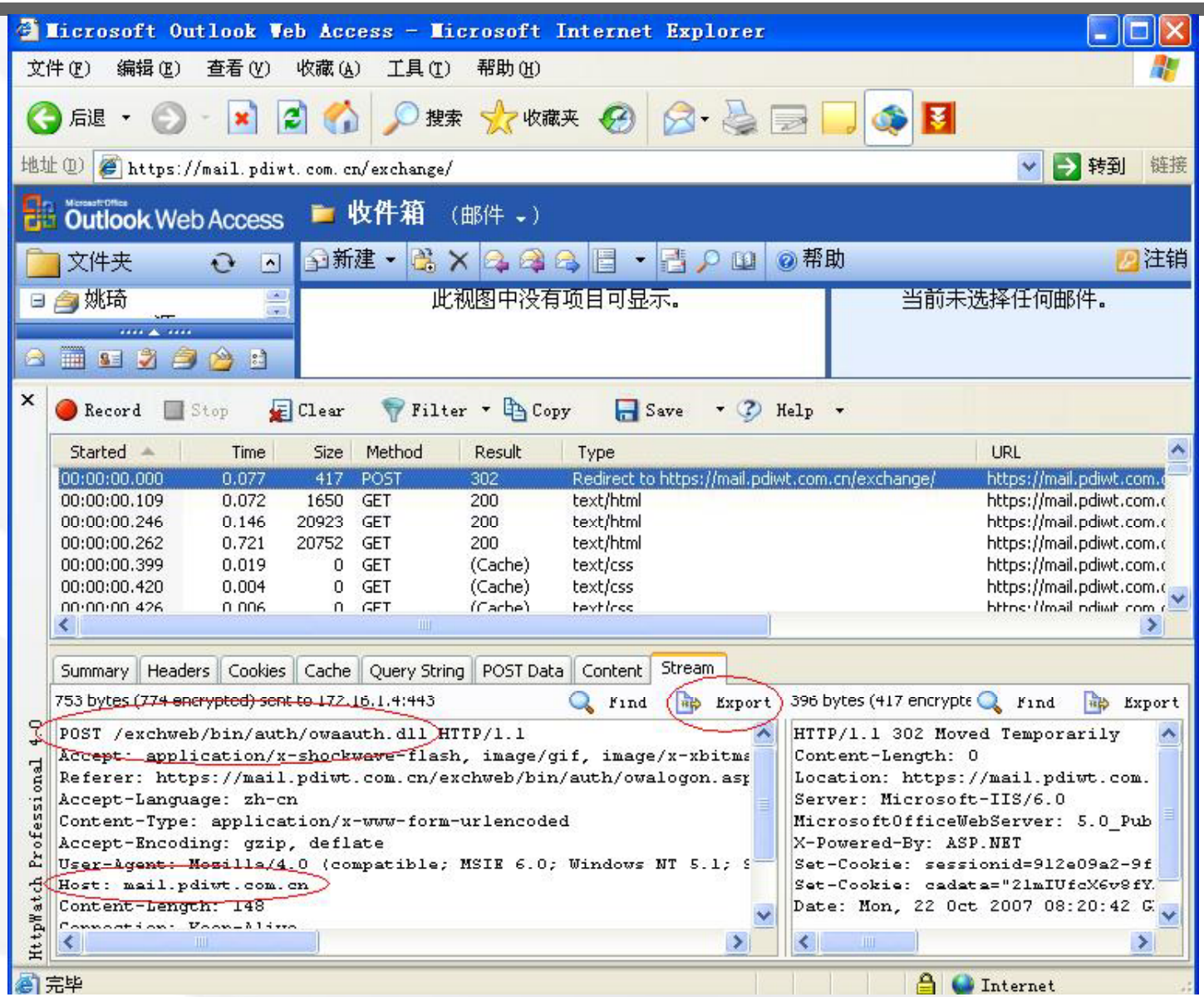
Step 1 – Screenshot 1

Step 2 – under direct access

2. Input USERNAME and PASSWORD, and then, click the “login” button to submit the login message to backend server (before clicking the “login” button, please enable the “HttpWatch” for getting the TOTAL package of POST request) - (the screenshot is on next slide)

NOTE: even though, the text from the screenshots is in Chinese but the highlighted information is the main focus.

Step 2 – Screenshot 2



Step 3 – under direct access

3. Export the POST request by using HttpWatch and analyze the package

POST **/exchweb/bin/auth/owaauth.dll** HTTP/1.1
Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer:
https://mail.pdiwt.com.cn/exchweb/bin/auth/owalogon.asp?url=https://mail.pdiwt.com.cn/exchange/&reason=2
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: **mail.pdiwt.com.cn**
Content-Length: 148
Connection: Keep-Alive
Cache-Control: no-cache

destination=https%3A%2F%2Fmail.pdiwt.com.cn%2Fexchange%2F&flags=0&username=yaoqi&password=123456&SubmitCreds=%B5%C7%C2%BC&forcedownlevel=0&trusted=0

Step 3 – Con.

By analyzing the POST request, we can get the parameters ***<username field> <password field> [post url]*** and ***[other post fields]*** of "***sso post***"

<username field> - "username"

<password field> - "password"

[post url] – "/exchweb/bin/auth/owaauth.dll"

[other post fields] – "destination=https%3A%2F%2Fmail.pdiwt.com.cn%2Fexchange%2F&flags=0&SubmitCreds=%B5%C7%C2%BC&forcedownlevel=0&trusted=0"

Till now, we got correct value for all parameters of the "sso post" command

Configure the "sso post" by using above value

Step 3 – Caution

When the login URL contains encoded characters, please convert these encoded characters into normal characters. For example, customer's login page is "/amserver/UI/Login?goto=http%3A%2F%2Fportal.sxmcc.com.cn%3A80%2Fportal%2Fdt" whose host is "portal.sxmcc.com.cn".

Then, we need to configure the SSO POST on SPX box via CLI:

sso post "portal.sxmcc.com.cn" "/amserver/UI/Login?goto=http://portal.sxmcc.com.cn:80/portal/dt" "IDToken1" "IDToken2" "" "/amserver/UI/Login?module=LDAP" "disable"

Step 4 – via SP

Login the vsite of SPX and click the link on the portal to see if the SSO POST work

NOTE: SSO kicks in only once per login per URL

If you are not sure that if the SPX sends out the POST request to backend server, please capture the network package on the backend server or on the SPX box (the detailed debug method is on next slide) to ensure it

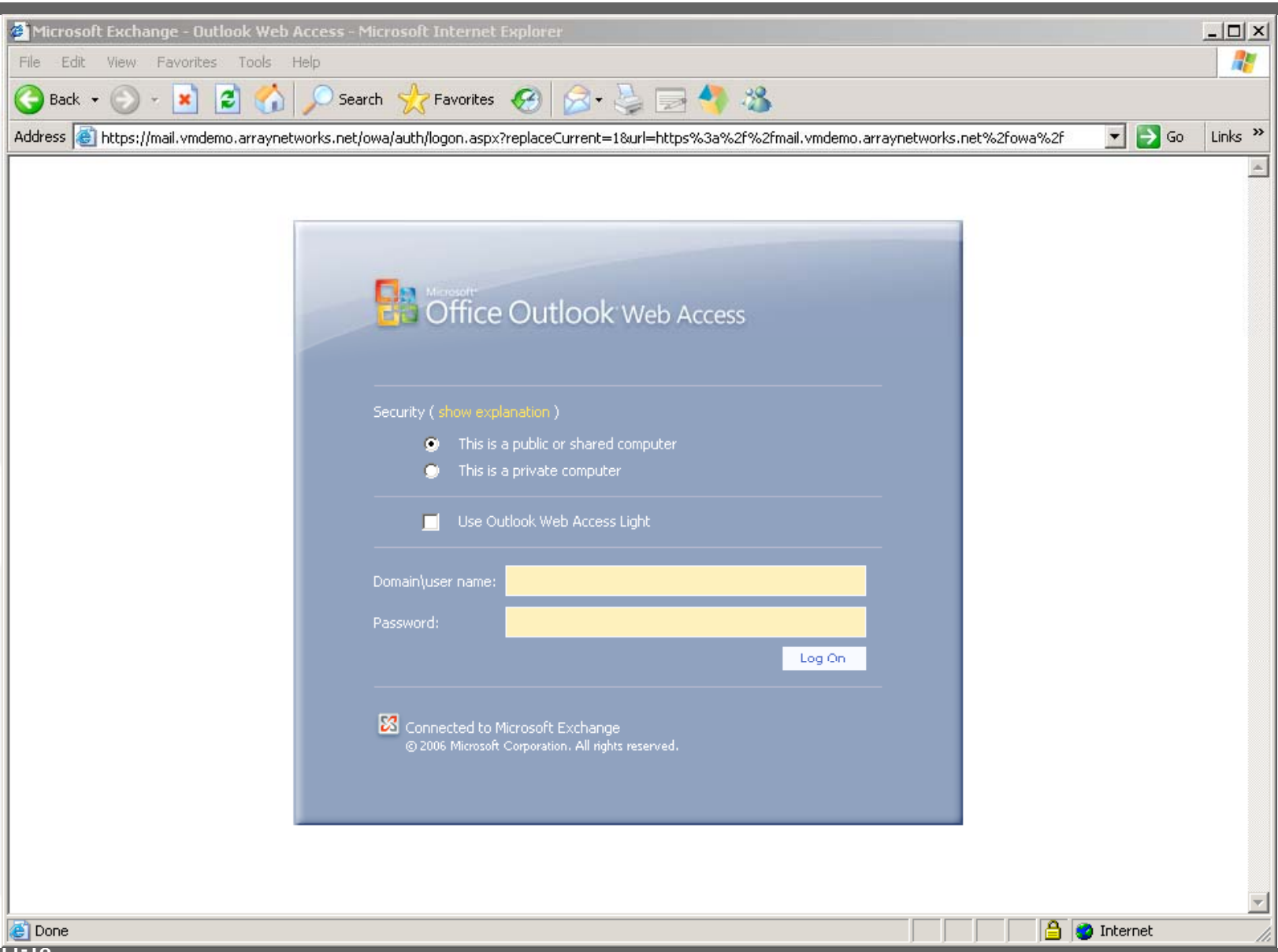
The brief method for ensure if the SSO POST triggered:

- debug enable
- debug module sproxy negotiate
- show debug out (the message will indicate if the SSO POST triggered)
- debug disable

Configure – Step by Step (OWA2007)

The following example is based on Exchange 2007 server

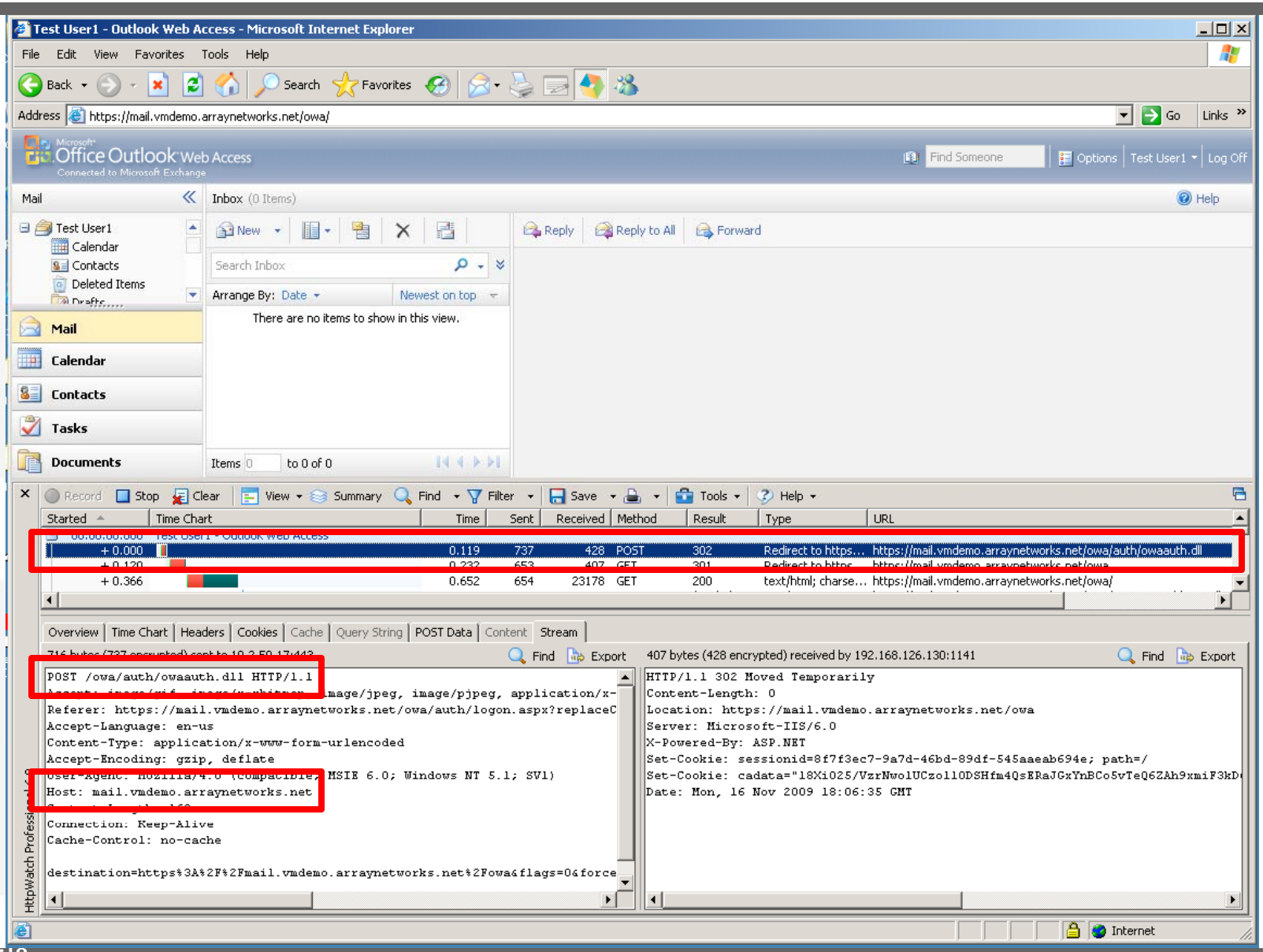
Step 1 – Screenshot 1 (OWA2007)



Step 2 – under direct access (OWA2007)

2. Input USERNAME and PASSWORD, and then, click the “login” button to submit the login message to backend server (before clicking the “login” button, please enable the “HttpWatch” for getting the TOTAL package of POST request) - (the screenshot is on next slide)

Step 2 – Screenshot 2 (OWA2007)



Step 3 – under direct access (OWA2007)

3. Export the POST request by using HttpWatch and analyze the package

POST **/owa/auth/owaauth.dll** HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: https://mail.vmdemo.arraynetworks.net/owa/auth/logon.aspx?replaceCurrent=1&…
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: **mail.vmdemo.arraynetworks.net**
Content-Length: 160
Connection: Keep-Alive
Cache-Control: no-cache

destination=https%3A%2F%2Fmail.vmdemo.arraynetworks.net%2Fowa&flags=0&forcedownlevel=0&trusted=0&username=test@vmdemo.arraynetworks.net&password=click1&isUtf8=1

Step 3 – Con. (OWA2007)

By analyzing the POST request, we can get the parameters *<username field>* *<password field>* *[post url]* and *[other post fields]* of "*sso post*"

<username field> - "username"

<password field> - "password"

[post url] – "/owa/auth/owaauth.dll"

[other post fields] – "destination=https://mail.vmdemo.arraynetworks.net/owa&isUtf8=1"

(by the testing, if you use "destination=https%3A%2F%2Fmail.vmdemo.arraynetworks.net%2Fowa&isUtf8=1" instead of the above string; the sso works unstable)

Till now, we got correct value for all parameters of the "sso post" command

Configure the "sso post" by using above value

Debug SSO POST

debug enable
debug on
debug module sproxy negotiate
debug trace tcp all
< show debug out > -- optional
debug off
debug disable

Send the array_debug.tar.gz to engineer and give the trace without SPX. The trace should start from GET /url1 or GET /login (the first page should be same with the “portal link” you configured on the SPX) and login successfully; after login successfully, please re-access /login page again (before capture the direct trace, please cleanup the tmp file and cookies from IE options firstly).

Array NETWORKS
Access. Security. Performance.

Thanks!