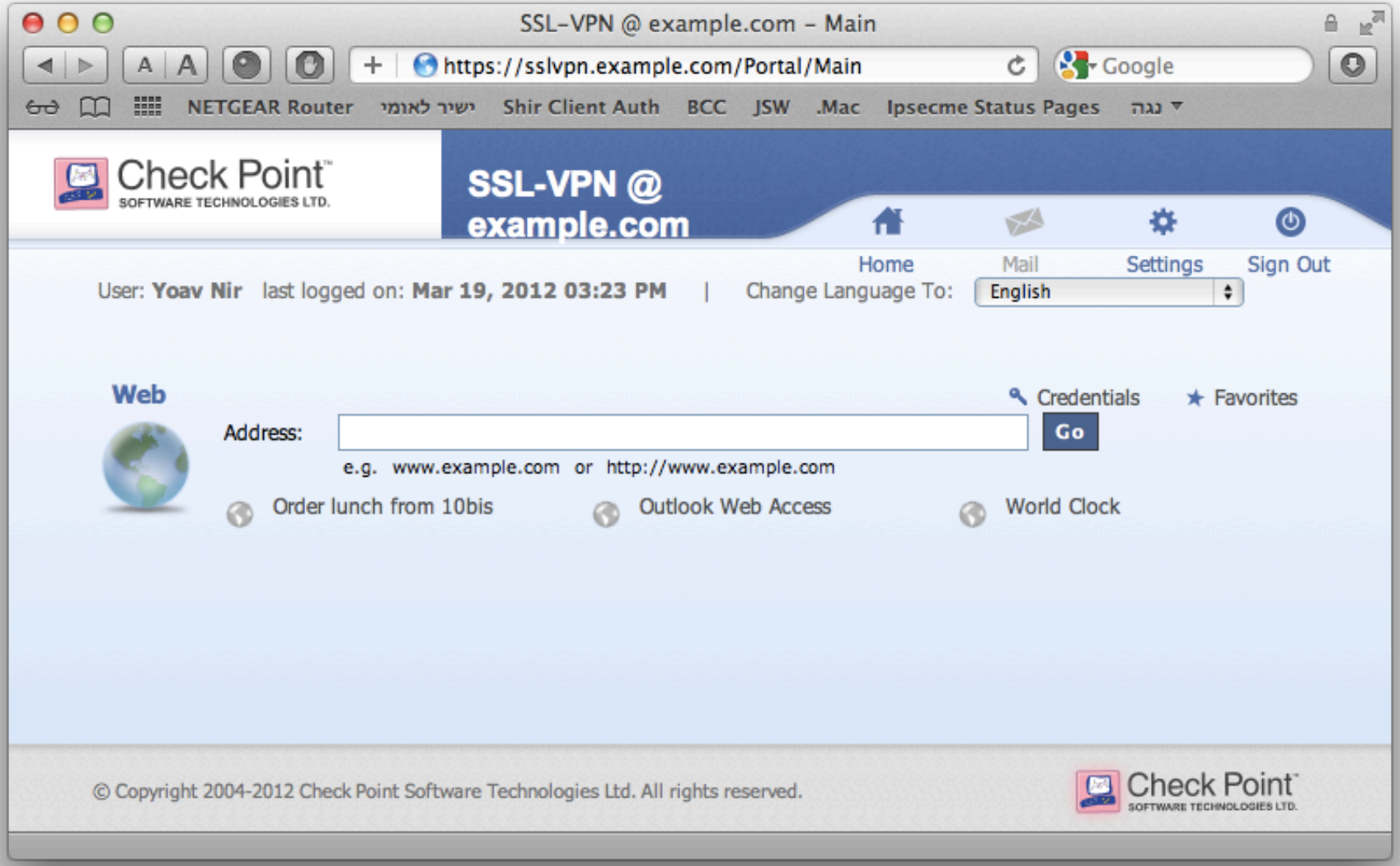
Extended Origins

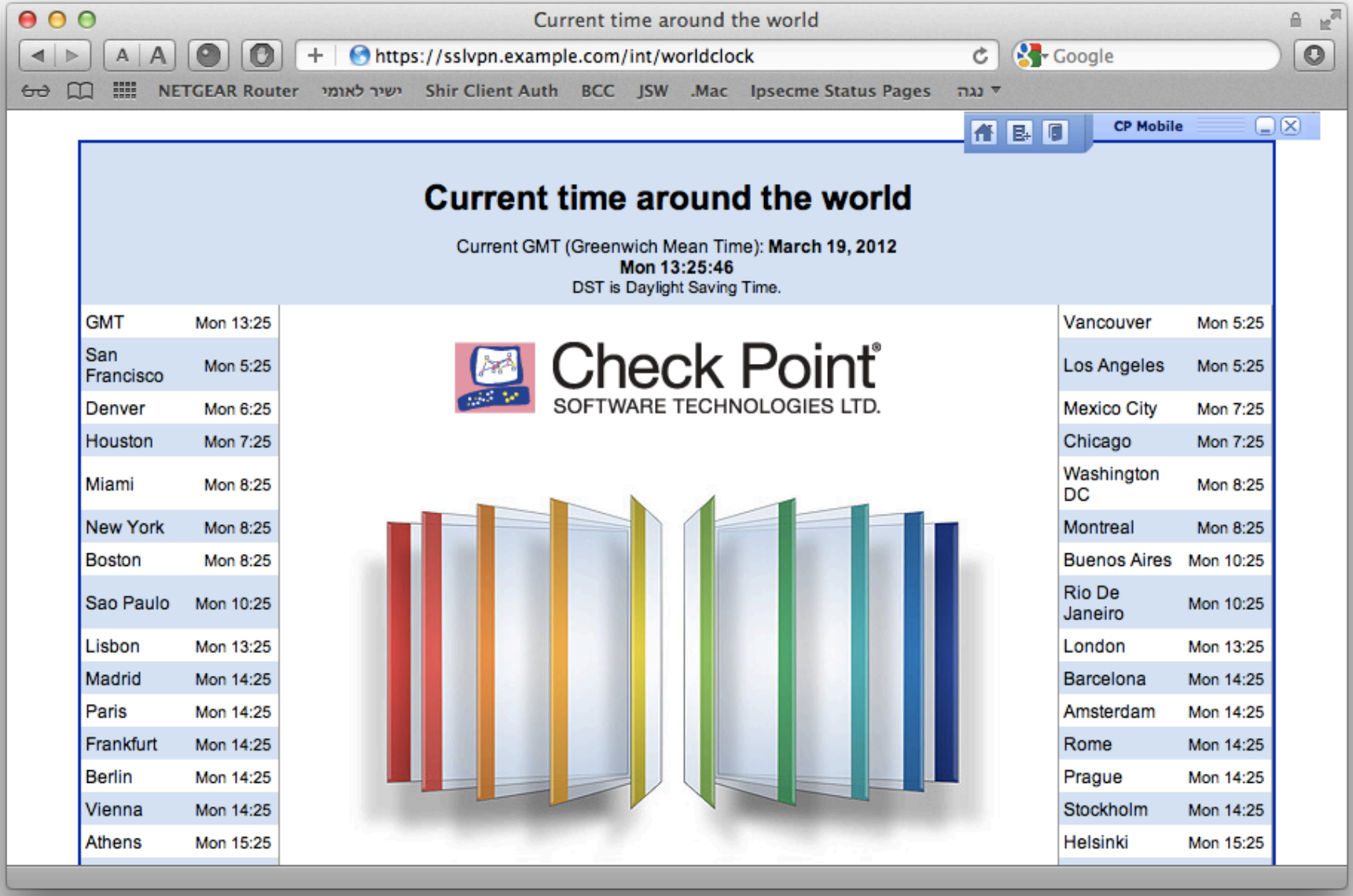
draft-nir-websec-extended-origin

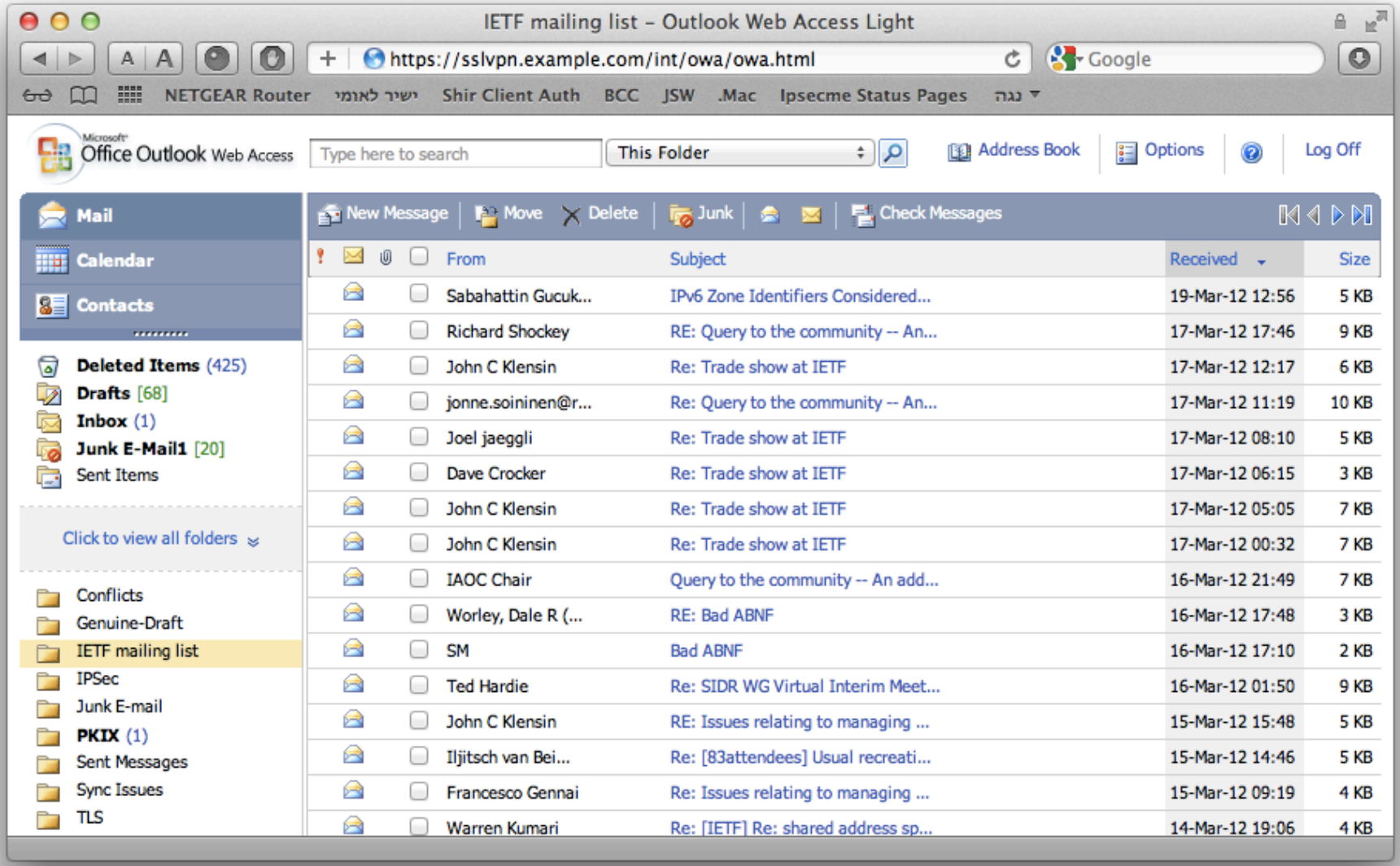
What's the Problem

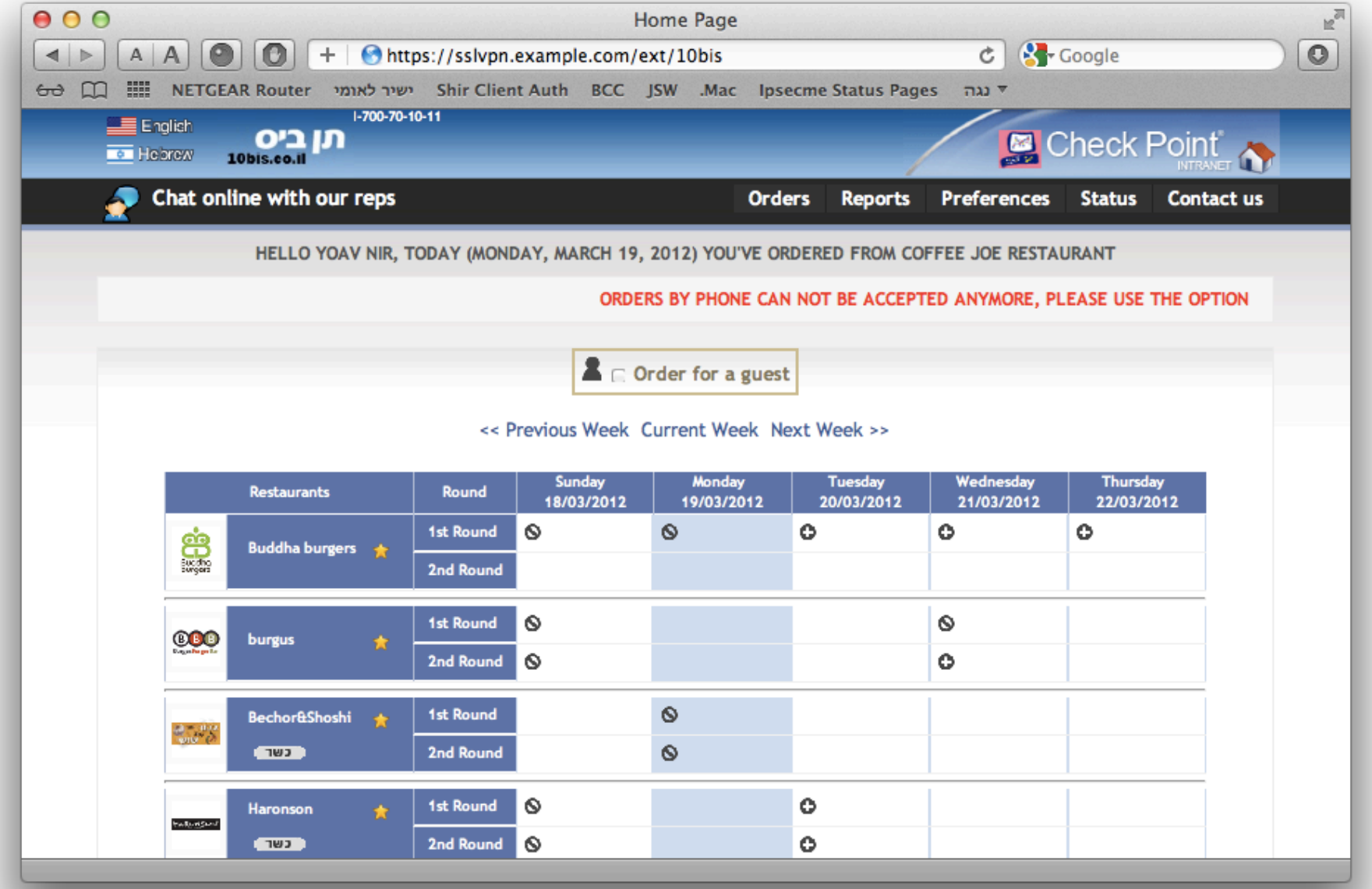
- Reverse proxies such as SSL VPNs hide multiple real servers behind them
- All these servers appear to have the same origin, but they're different servers
- Browsers treat all the pages as if they're part of the same origin.
  - Scripts
  - Cookies


SSL-VPN @ example.com – Sign In
https://sslvpn.example.com/Login
Google
NETGEAR Router
ישיר לאומי
Shir Client Auth
BCC
JSW
.Mac
Ipsecme Status Pages
נגה
Check Point
SOFTWARE TECHNOLOGIES LTD.
SSL-VPN @ example.com
Standard Sign In
User name:
Yoav Nir
Password:
Certificate Sign In
Change Language To:
English
Sign In
© Copyright 2004-2012 Check Point Software Technologies Ltd. All rights reserved.


SSL-VPN @ example.com - Main
https://sslvpn.example.com/Portal/Main
Google
NETGEAR Router
ישיר לאומי
Shir Client Auth
BCC
JSW
.Mac
Ipsecme Status Pages
נגה
Check Point
SOFTWARE TECHNOLOGIES LTD.
SSL-VPN @ example.com
Home
Mail
Settings
Sign Out
User: Yoav Nir last logged on: Mar 19, 2012 03:23 PM
Change Language To:
English
Web
Credentials
Favorites
Address:
Go
e.g. www.example.com or http://www.example.com
Order lunch from 10bis
Outlook Web Access
World Clock
© Copyright 2004-2012 Check Point Software Technologies Ltd. All rights reserved.
Check Point
SOFTWARE TECHNOLOGIES LTD.


Current time around the world
https://sslvpn.example.com/int/worldclock
Google
NETGEAR Router
ישיר לאומי
Shir Client Auth
BCC
JSW
.Mac
Ipsecme Status Pages
נגה
CP Mobile
Current time around the world
Current GMT (Greenwich Mean Time): March 19, 2012
Mon 13:25:46
DST is Daylight Saving Time.
GMT Mon 13:25
San Francisco Mon 5:25
Denver Mon 6:25
Houston Mon 7:25
Miami Mon 8:25
New York Mon 8:25
Boston Mon 8:25
Sao Paulo Mon 10:25
Lisbon Mon 13:25
Madrid Mon 14:25
Paris Mon 14:25
Frankfurt Mon 14:25
Berlin Mon 14:25
Vienna Mon 14:25
Athens Mon 15:25
Check Point
SOFTWARE TECHNOLOGIES LTD.
Vancouver Mon 5:25
Los Angeles Mon 5:25
Mexico City Mon 7:25
Chicago Mon 7:25
Washington DC Mon 8:25
Montreal Mon 8:25
Buenos Aires Mon 10:25
Rio De Janeiro Mon 10:25
London Mon 13:25
Barcelona Mon 14:25
Amsterdam Mon 14:25
Rome Mon 14:25
Prague Mon 14:25
Stockholm Mon 14:25
Helsinki Mon 15:25


IETF mailing list – Outlook Web Access Light
https://sslvpn.example.com/int/owa/owa.html
Google
NETGEAR Router
Shir Client Auth
BCC
JSW
.Mac
Ipsecme Status Pages
Office Outlook Web Access
Type here to search
This Folder
Address Book
Options
Log Off
Mail
Calendar
Contacts
Deleted Items (425)
Drafts [68]
Inbox (1)
Junk E-Mail1 [20]
Sent Items
Click to view all folders
Conflicts
Genuine-Draft
IETF mailing list
IPSec
Junk E-mail
PKIX (1)
Sent Messages
Sync Issues
TLS
New Message
Move
Delete
Junk
Check Messages
From
Subject
Received
Size
Sabahattin Gucuk... IPv6 Zone Identifiers Considered... 19-Mar-12 12:56 5 KB
Richard Shockey RE: Query to the community -- An... 17-Mar-12 17:46 9 KB
John C Klensin Re: Trade show at IETF 17-Mar-12 12:17 6 KB
jonne.soininen@r... Re: Query to the community -- An... 17-Mar-12 11:19 10 KB
Joel jaeggli Re: Trade show at IETF 17-Mar-12 08:10 5 KB
Dave Crocker Re: Trade show at IETF 17-Mar-12 06:15 3 KB
John C Klensin Re: Trade show at IETF 17-Mar-12 05:05 7 KB
John C Klensin Re: Trade show at IETF 17-Mar-12 00:32 7 KB
IAOC Chair Query to the community -- An add... 16-Mar-12 21:49 7 KB
Worley, Dale R (... RE: Bad ABNF 16-Mar-12 17:48 3 KB
SM Bad ABNF 16-Mar-12 17:10 2 KB
Ted Hardie Re: SIDR WG Virtual Interim Meet... 16-Mar-12 01:50 9 KB
John C Klensin RE: Issues relating to managing ... 15-Mar-12 15:48 5 KB
Iljitsch van Bei... Re: [83attendees] Usual recreati... 15-Mar-12 14:46 5 KB
Francesco Gennai Re: Issues relating to managing ... 15-Mar-12 09:19 4 KB
Warren Kumari Re: [IETF] Re: shared address sp... 14-Mar-12 19:06 4 KB


Home Page
https://sslvpn.example.com/ext/10bis
Google
NETGEAR Router
ישיר לאומי
Shir Client Auth
BCC
JSW
.Mac
Ipsecme Status Pages
נגה
English
Hebrew
1-700-70-10-11
10bis.co.il
Check Point
INTRANET
Chat online with our reps
Orders
Reports
Preferences
Status
Contact us
HELLO YOAV NIR, TODAY (MONDAY, MARCH 19, 2012) YOU'VE ORDERED FROM COFFEE JOE RESTAURANT
ORDERS BY PHONE CAN NOT BE ACCEPTED ANYMORE, PLEASE USE THE OPTION
Order for a guest
<< Previous Week
Current Week
Next Week >>
Restaurants
Round
Sunday 18/03/2012
Monday 19/03/2012
Tuesday 20/03/2012
Wednesday 21/03/2012
Thursday 22/03/2012
Buddha burgers
1st Round
2nd Round
burgus
1st Round
2nd Round
Bechor&Shoshi
כשר
1st Round
2nd Round
Haronson
כשר
1st Round
2nd Round

The proposal

- Add a new attribute to a web resource returned in the HTTP response
- Mark different parts of the big website as belonging to different origins
- Format is like this:

```
Extended-Origin: owa1; path=/int/owa
```

The Proposal

- Origin changes from a 3-tuple:
  <https ; sslvpn.example.com ; 443>
- to a 4-tuple:
  <https ; sslvpn.example.com ; 443 ; owa1>

- The path parameter is used to partition the website.

Alternate Solution

- Partition using different FQDN:
  - owa1.sslvpn.example.com
  - lunch.sslvpn.example.com
  - worldclock.sslvpn.example.com
- Cons:
  - You need lots of different certificates or a wildcard certifiate – high cost
  - Adding a server requires adding a DNS entry.
- Yes, SSL VPN products offer this option.

Yet Another Alternate Solution

- Same as last slide, but add a “reverse proxy” record in the DNS.

```
lunch.sslvpn.example.com IN
 RPROXY sslvpn.example.com
```

- Then the browser goes to the proxy.
- Cons:
  - Seems harder to implement
  - Opens the doors to many attacks if not protected by DNSSEC
    - Maybe even if it is.

QUESTIONS?