Stopping Malware at the Gateway

Challenges and Solutions

Presented by:

Martin Stecher
VP Development Webwasher

2007-09-20

From Client to Gateway Anti Malware

- What is gateway Anti Malware and what data should be handled?
- Can I just put my Client Anti Malware program on a proxy and I‘m done?
- Which issues are gateway specific and how can they be solved?
- How good are callout servers as deployment option?
- Outbound protection
- Gateway solution testing

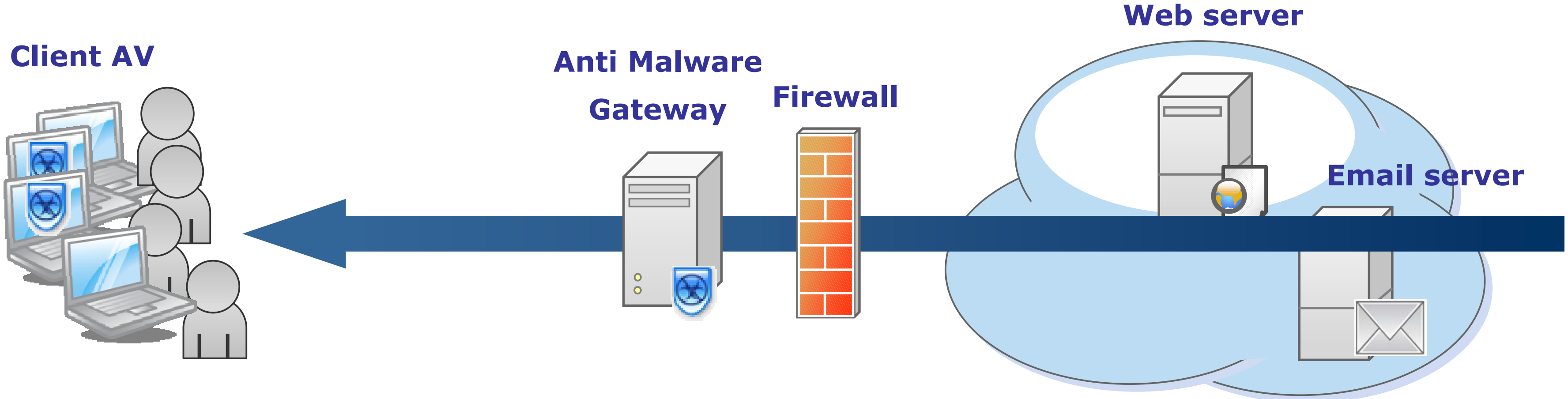
Performance

Updates

Latency

False positives

Gateway Anti Malware


Client AV

Anti Malware Gateway

Firewall

Web server

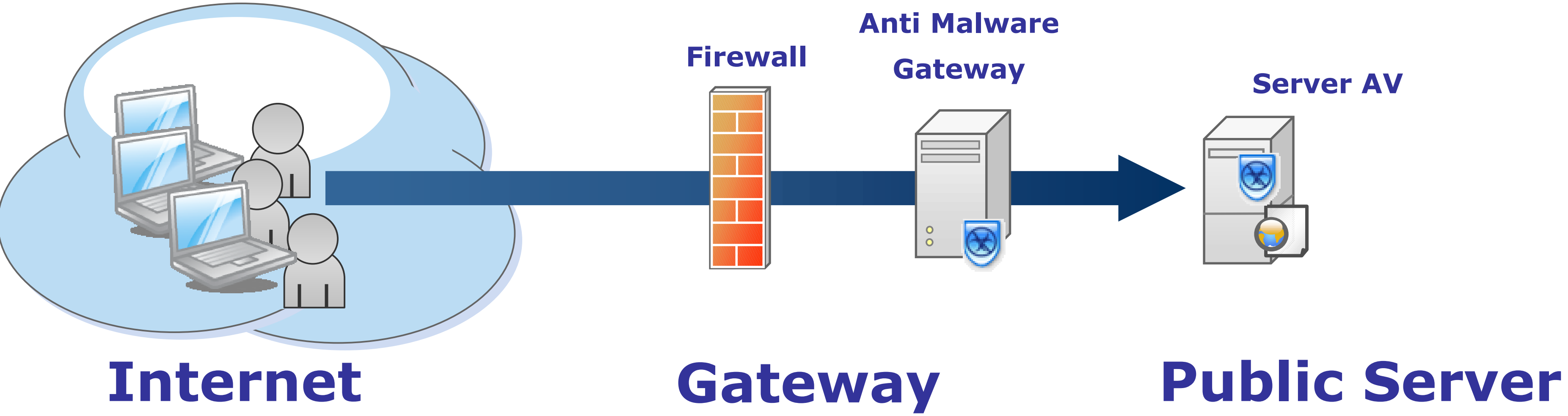
Email server

Intranet

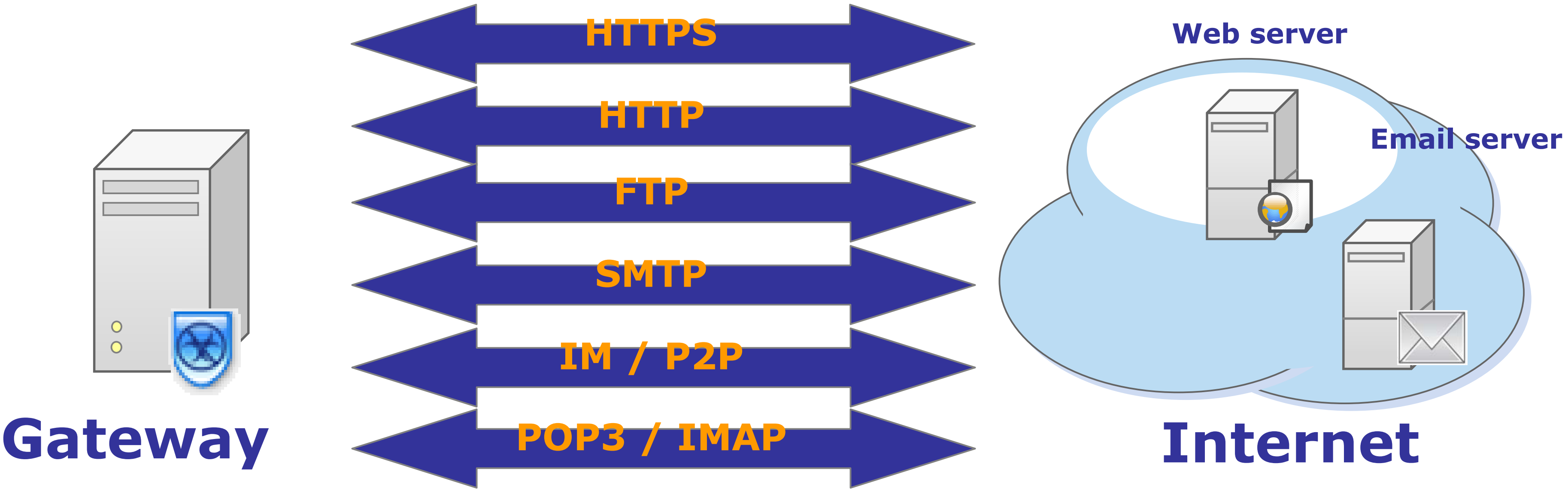
Gateway

Internet

Gateway Anti Malware (on reverse proxy)

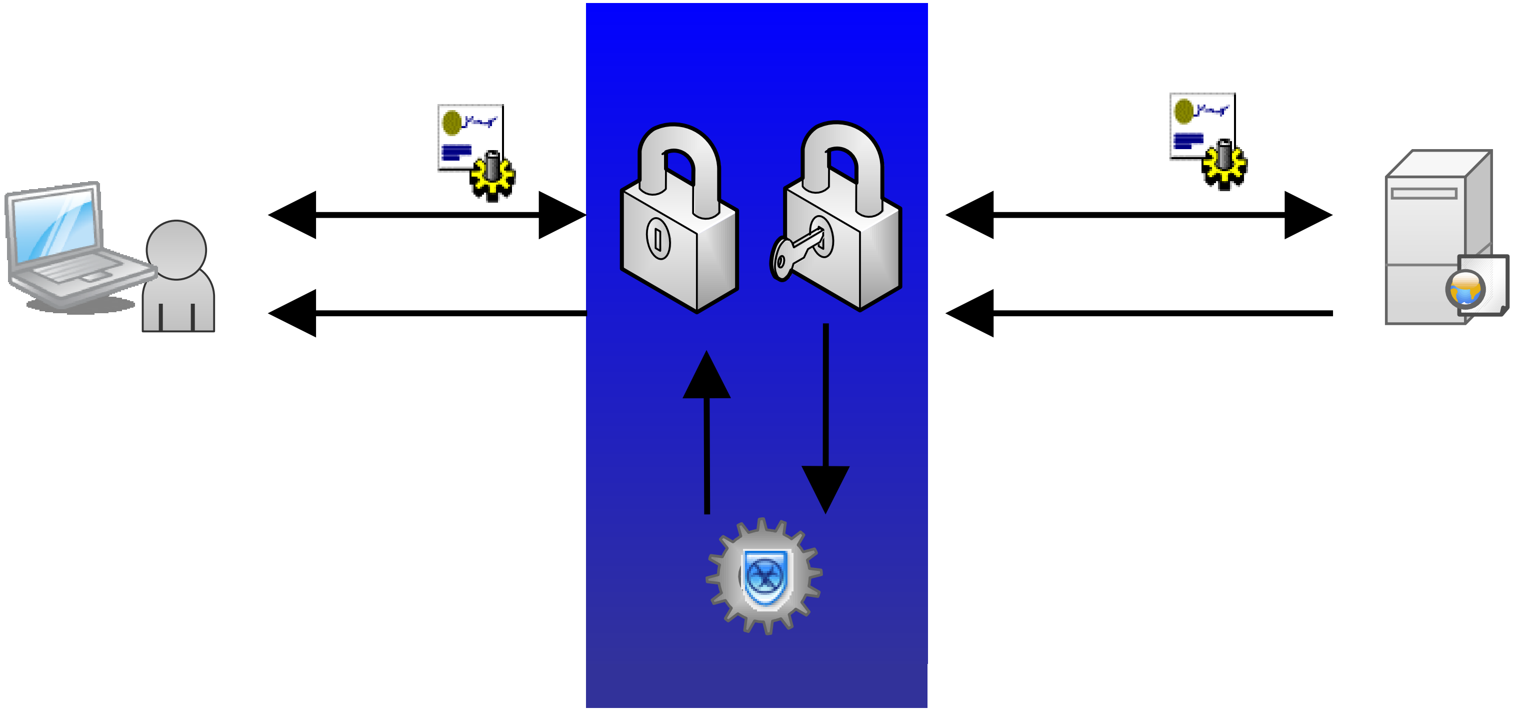


Supported Protocols



- Should HTTPS be supported too?

HTTPS Anti Malware Gateway



- The Gateway solutions must decrypt-scan-reencrypt
- A certificate verification policy must be deployed
- As forward proxy: The Gateway solution must be a certificate authority for all clients

Supported Data Formats

- No On-Access scanner
- Must be able to scan all kind of file archives
- Must be able to scan all kind of documents with embedded objects
  - MS Office Open XML (Office 2007), Office WordML (Office 2003), RTF
- Also remember malformed email project
- NULL-Byte handling of IE
- Content-Encodings: gzip and others
- Transfer-Encodings: chunked (others?)

➔A gateway scanner should ensure to block formats that it cannot decode/extract

… and also block nested archives beyond a certain level, etc.

Performance

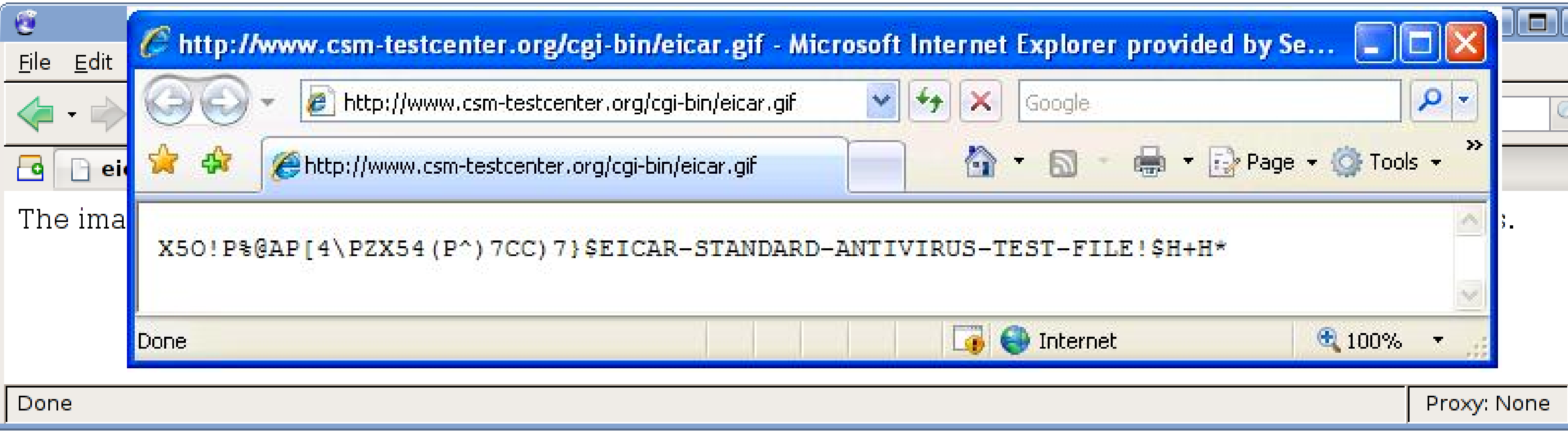
- Client anti malware performance measured when sequentially filtering a large selection of files
- Gateway anti malware must handle many connections in parallel
- Hundreds and thousands of URLs per second
- Dozens and hundreds of emails per second
- Cluster awareness!

- Media Type bypass a viable solution?
- Beware of Media Type falsification

Media Type Falsification

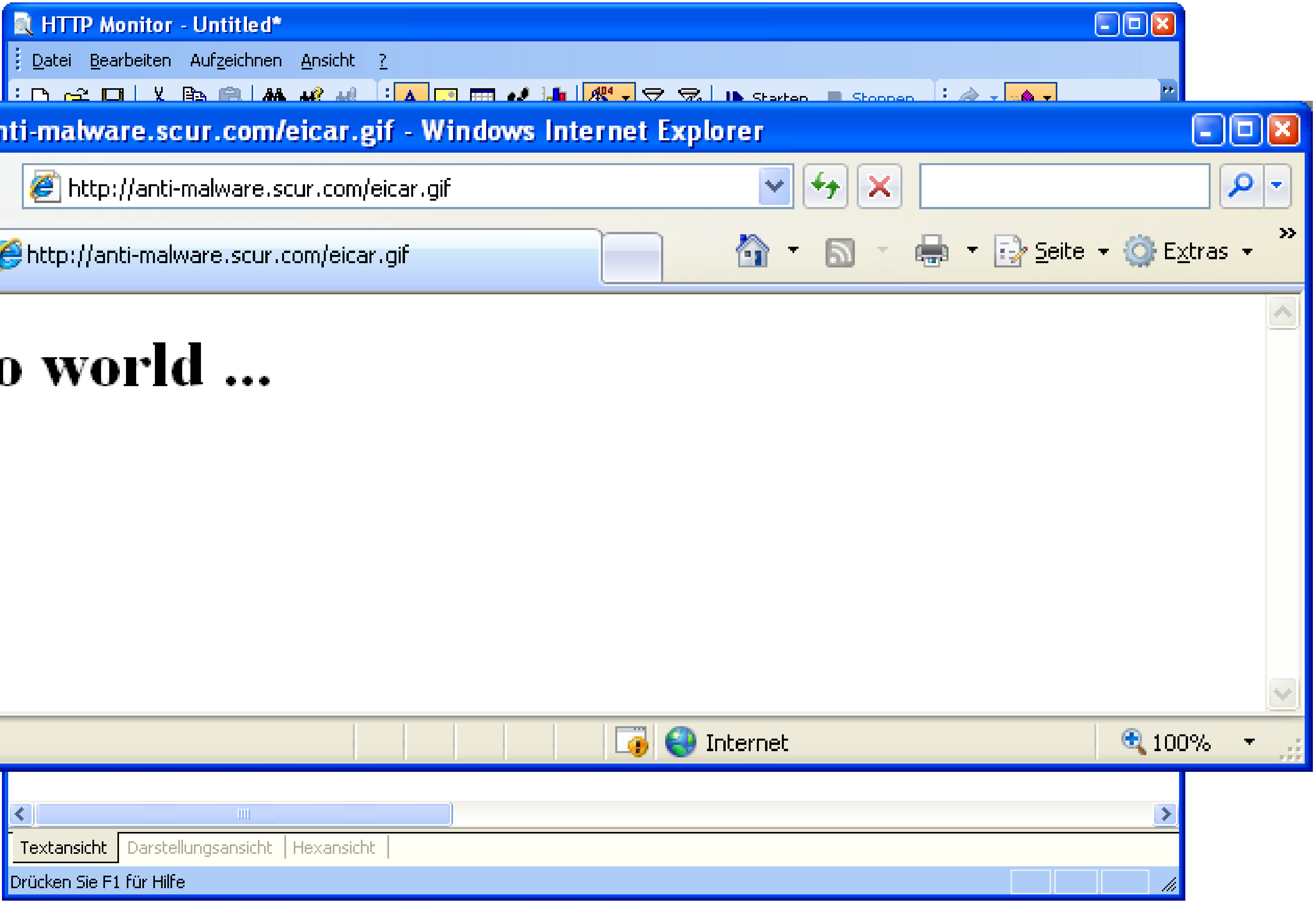
```
GET /cgi-bin/eicar.gif HTTP/1.1
Host: www.csm-testcenter.org
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2007 11:12:33 GMT
Server: Apache/2.0.54 (Debian GNU/Linu
Content-Length: 68
Connection: close
Content-Type: image/gif

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICA
```


http://www.csm-testcenter.org/cgi-bin/eicar.gif - Microsoft Internet Explorer provided by Se...
File
Edit
http://www.csm-testcenter.org/cgi-bin/eicar.gif
Google
http://www.csm-testcenter.org/cgi-bin/eicar.gif
Page
Tools
ei
The ima
s.
Done
Internet
100%
Done
Proxy: None

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Media Type Falsification (2)

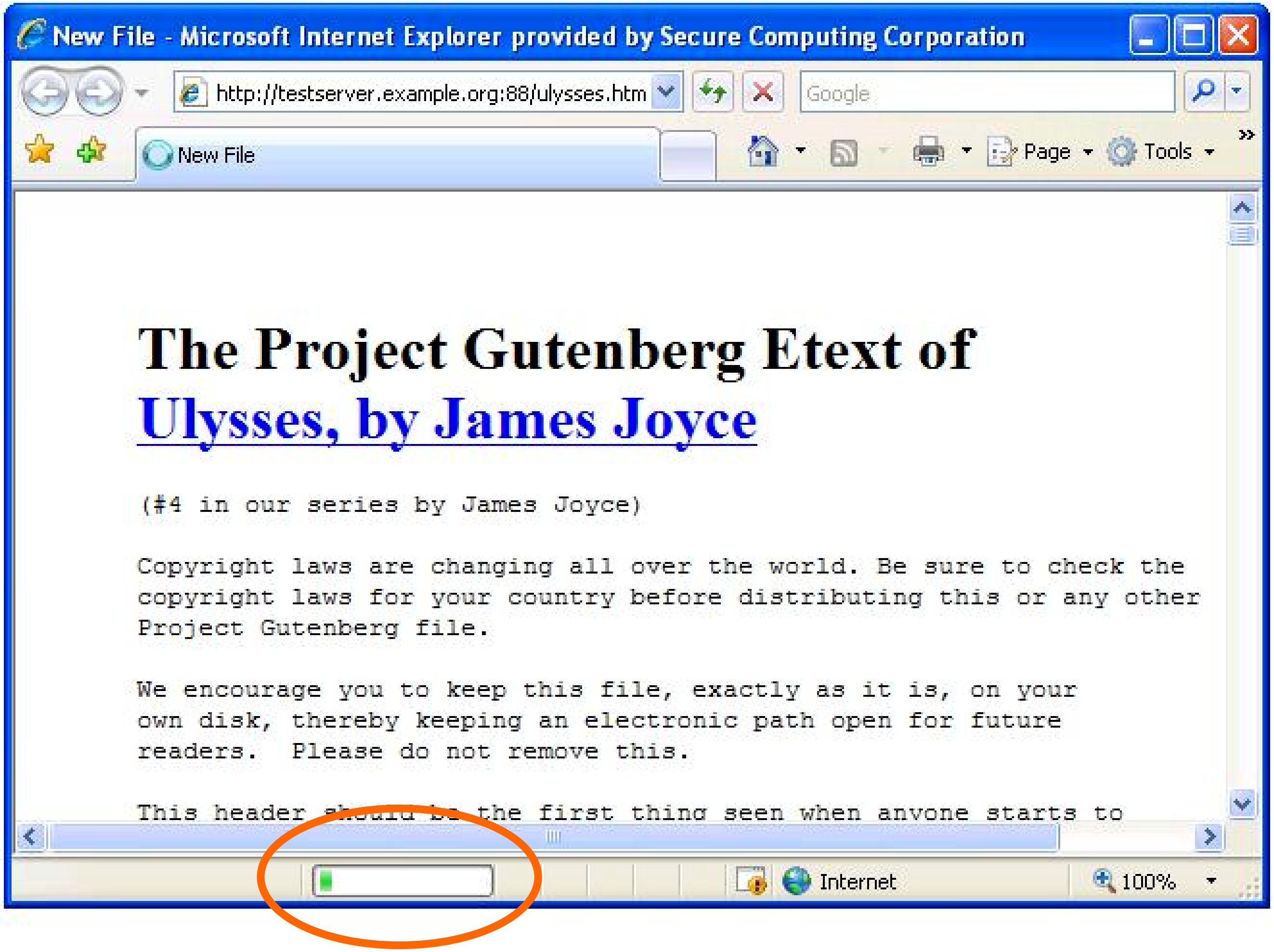


Hello world ...

HTTP Monitor - Untitled*
Datei Bearbeiten Aufzeichnen Ansicht ?
Starten Stoppen
http://anti-malware.scur.com/eicar.gif - Windows Internet Explorer
http://anti-malware.scur.com/eicar.gif
http://anti-malware.scur.com/eicar.gif
Seite
Extras
Fertig
Internet
100%
Textansicht Darstellungsansicht Hexansicht
Drücken Sie F1 für Hilfe

Latency – direct Internet connection

- Browser starts to render content while receiving data



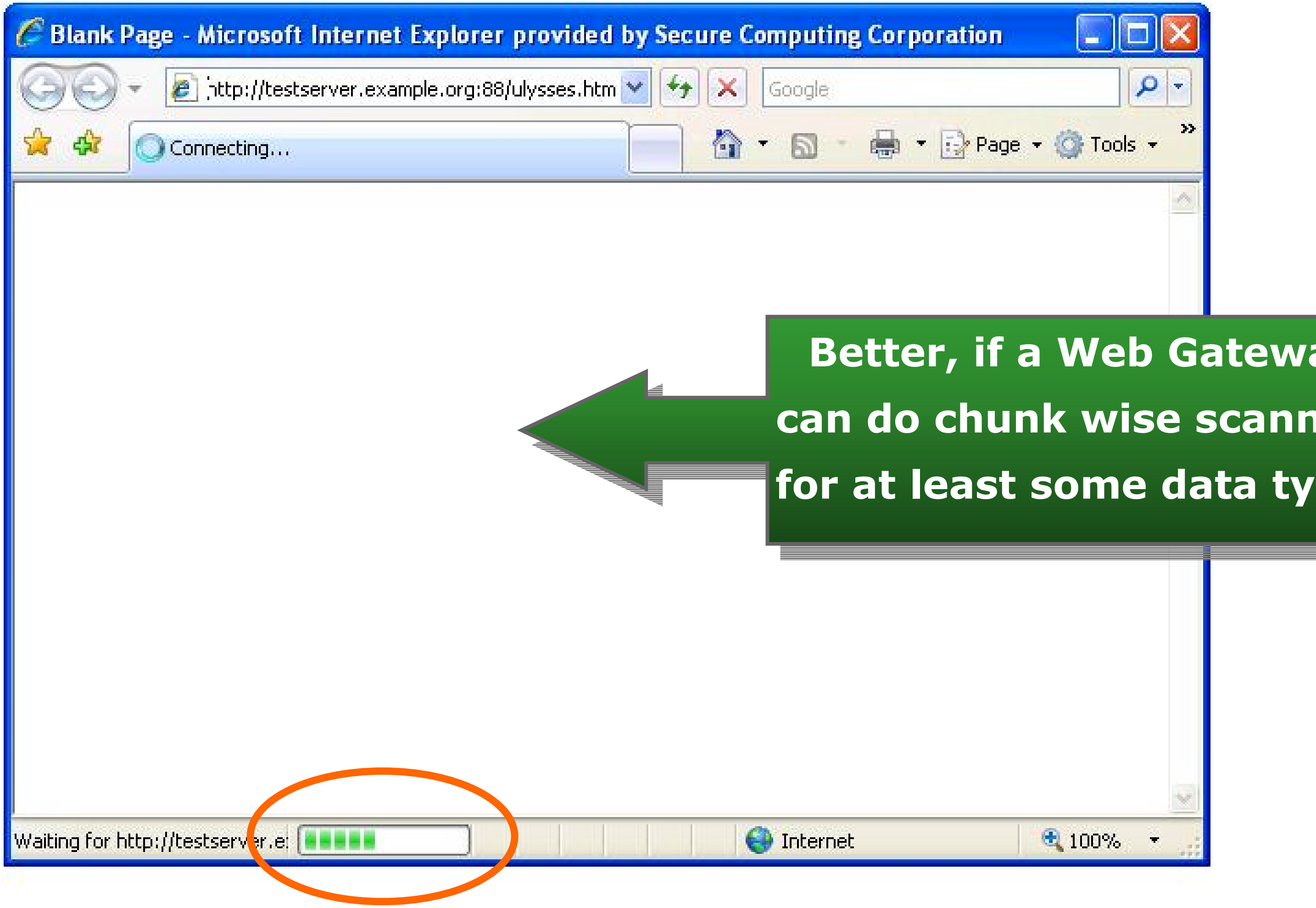
New File - Microsoft Internet Explorer provided by Secure Computing Corporation
http://testserver.example.org:88/ulysses.htm
Google
New File
Page
Tools
Internet
100%

The Project Gutenberg Etext of
Ulysses, by James Joyce

```
(#4 in our series by James Joyce)

Copyright laws are changing all over the world. Be sure to check the
copyright laws for your country before distributing this or any other
Project Gutenberg file.

We encourage you to keep this file, exactly as it is, on your
own disk, thereby keeping an electronic path open for future
readers.  Please do not remove this.

This header should be the first thing seen when anyone starts to
```

Latency – with a too easily done Web Gateway

- All traffic needs to be seen at the Web Gateway before sending on



Blank Page - Microsoft Internet Explorer provided by Secure Computing Corporation

http://testserver.example.org:88/ulysses.htm

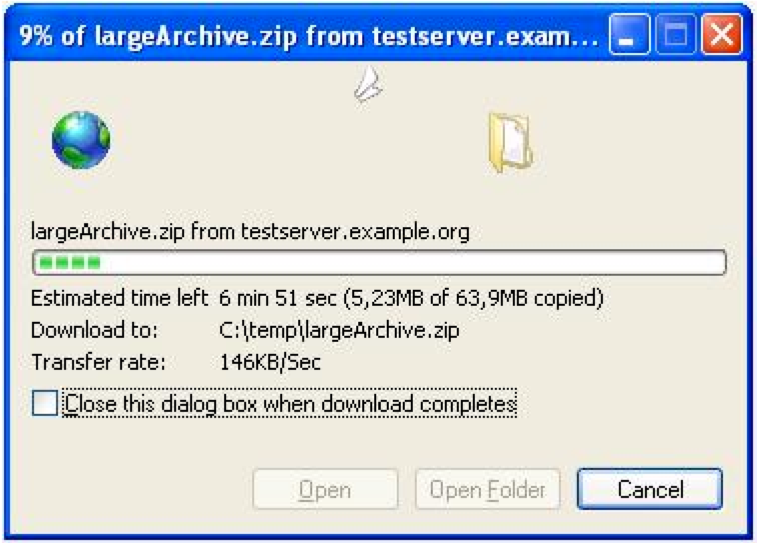
Connecting...

Waiting for http://testserver.e:

Better, if a Web Gateway can do chunk wise scanning for at least some data types

Download Progress Indication

- Download Progress Indication for file types which cannot be scanned chunk-by-chunk
- Download of a larger file, standard browser dialog:



9% of largeArchive.zip from testserver.exam...

largeArchive.zip from testserver.example.org

Estimated time left 6 min 51 sec (5,23MB of 63,9MB copied)

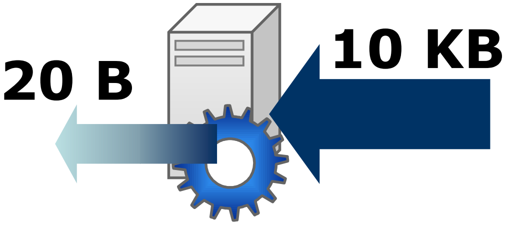
Download to: C:\temp\largeArchive.zip

Transfer rate: 146KB/Sec

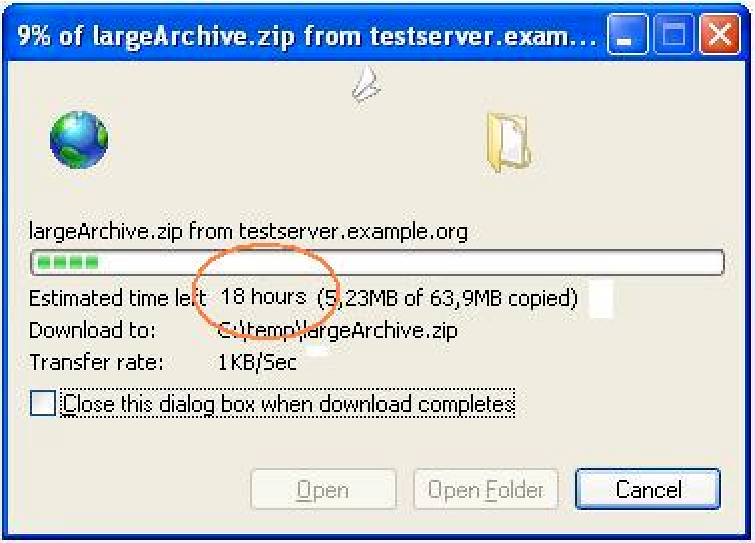
□ Close this dialog box when download completes

Data Trickling

- Forward some few bytes for each larger chunk received
- Continue doing so while processing larger files too!?!
- Advantage:
  - Easy
  - User sees some progress



- Disadvantages:
  - Infected part may already be forwarded to the client!
  - Estimated downloa
  - If infected, cannot s ort download)
  - If data can be modi timated time at all.



largeArchive.zip from testserver.example.org

Estimated time left: 18 hours (5,23MB of 63,9MB copied)

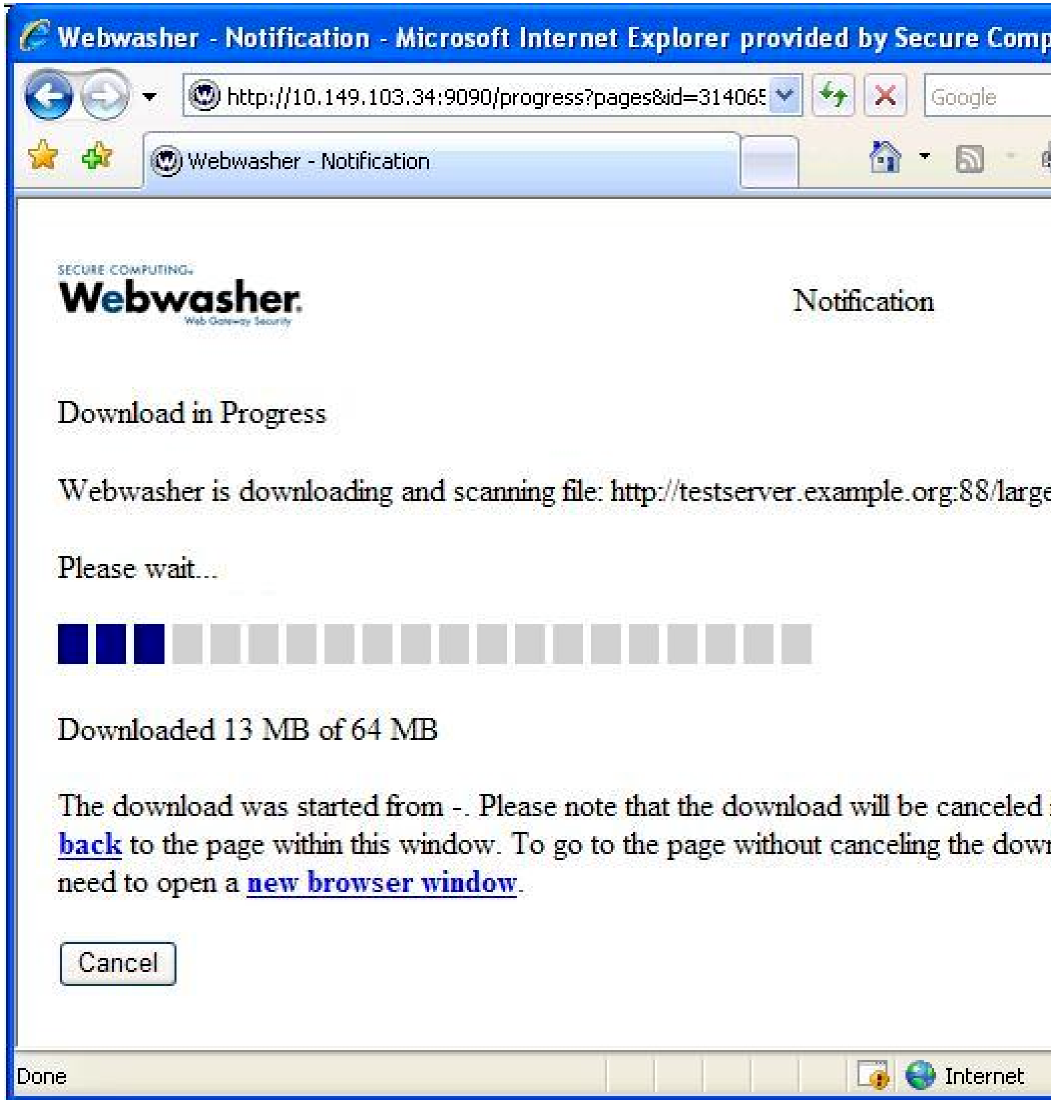
Download to: C:\temp\largeArchive.zip

Transfer rate: 1 KB/Sec

□ Close this dialog box when download completes

Patient Pages

- Shows the user what happens at the gateway
- Looks nice
- Time is accurate
- Can show infection alert
- Does not work well with Download Managers
- Problematic when end user uses “Save Target As...”


Webwasher - Notification - Microsoft Internet Explorer provided by Secure Comp
http://10.149.103.34:9090/progress?pages&id=314065
Google
Webwasher - Notification
SECURE COMPUTING
Webwasher
Web Gateway Security
Notification

Download in Progress

Webwasher is downloading and scanning file: http://testserver.example.org:88/large

Please wait...

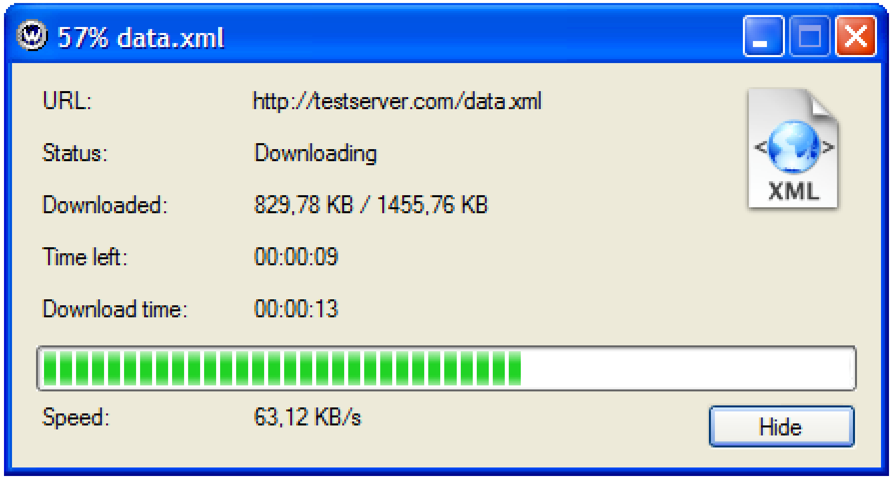
Downloaded 13 MB of 64 MB

The download was started from -. Please note that the download will be canceled back to the page within this window. To go to the page without canceling the down need to open a new browser window.

Separate Queries

- Original download is not changed in any way.
- Provides accurate feedback on what is going on, on the gateway

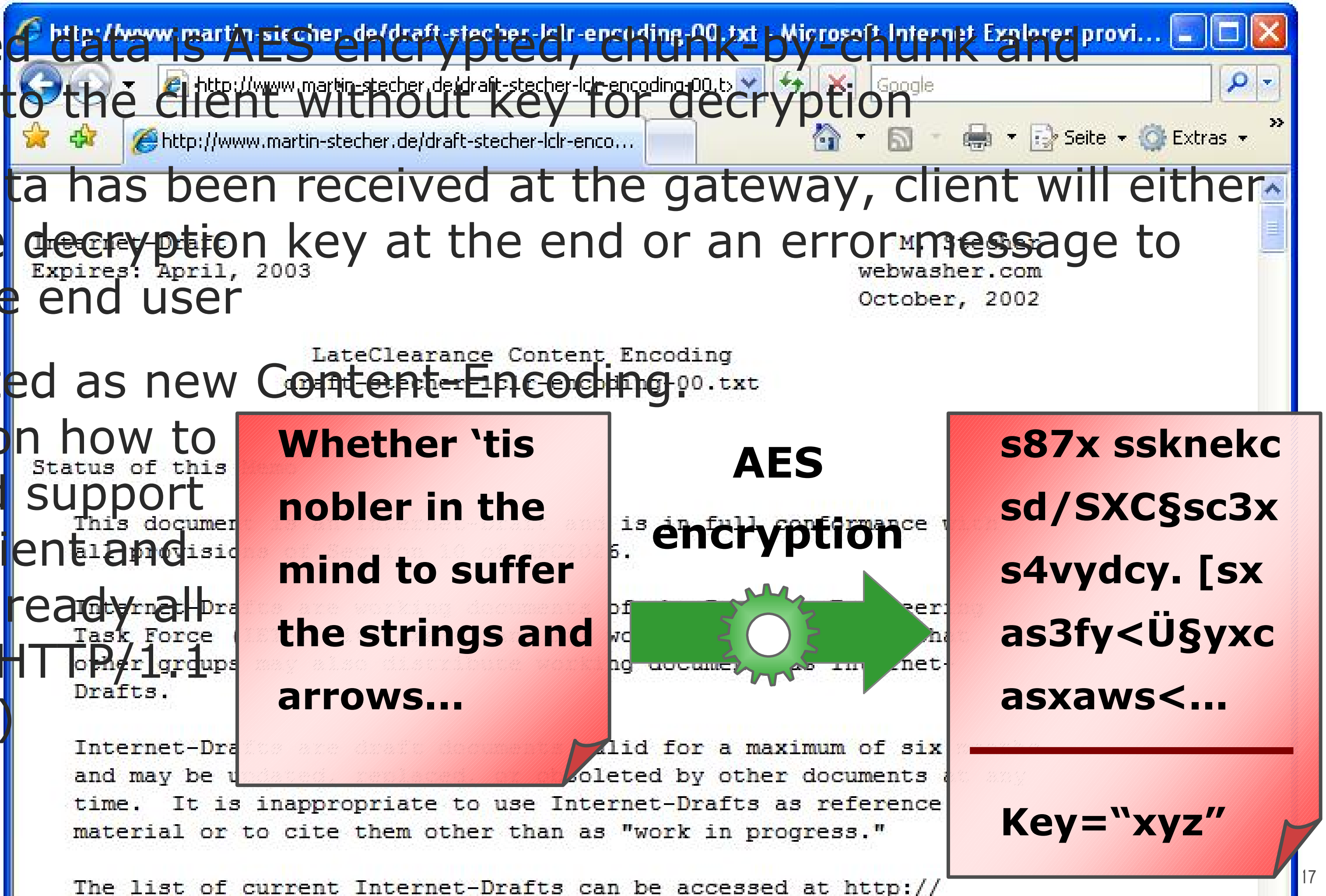
- But requires additional out of band communication on separate connection to gateway.
- So, the gateway needs to lookup transaction status and that could be on a different machine in a cluster!


57% data.xml

URL: http://testserver.com/data.xml
Status: Downloading
Downloaded: 829,78 KB / 1455,76 KB
Time left: 00:00:09
Download time: 00:00:13
Speed: 63,12 KB/s

Late Clearance Content Encoding

- Published as Internet Draft several years ago
- Very good feedback but never implemented in browsers
- Downloaded data is AES encrypted, chunk-by-chunk and forwarded to the client without key for decryption
- After all data has been received at the gateway, client will either receive the decryption key at the end or an error message to show to the end user
- Implemented as new Content-Encoding. Specification how to extend and support between client and server is already all defined in HTTP/1.1 (RFC 2616)


http://www.martin-stecher.de/draft-stecher-lclr-encoding-00.txt - Microsoft Internet Explorer provi...
http://www.martin-stecher.de/draft-stecher-lclr-encoding-00.txt
Google
http://www.martin-stecher.de/draft-stecher-lclr-enco...
Seite
Extras

```
Internet-Draft                                          M. Stecher
Expires: April, 2003                                 webwasher.com
                                                     October, 2002

                  LateClearance Content Encoding
                draft-stecher-lclr-encoding-00.txt

Status of this Memo

   This documen                          is in full conformance with
   all provisio                          6.

   Internet-Dra                          of
   Task Force (                          wo
   other groups                          ng documents as Internet-
   Drafts.

   Internet-Dra                          lid for a maximum of six
   and may be u                          soleted by other documents
   time.  It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   The list of current Internet-Drafts can be accessed at http://
```

Whether 'tis nobler in the mind to suffer the strings and arrows…

AES encryption

s87x ssknekc sd/SXC§sc3x s4vydcy. [sx as3fy<Ü§yxc asxaws<…

Key="xyz"

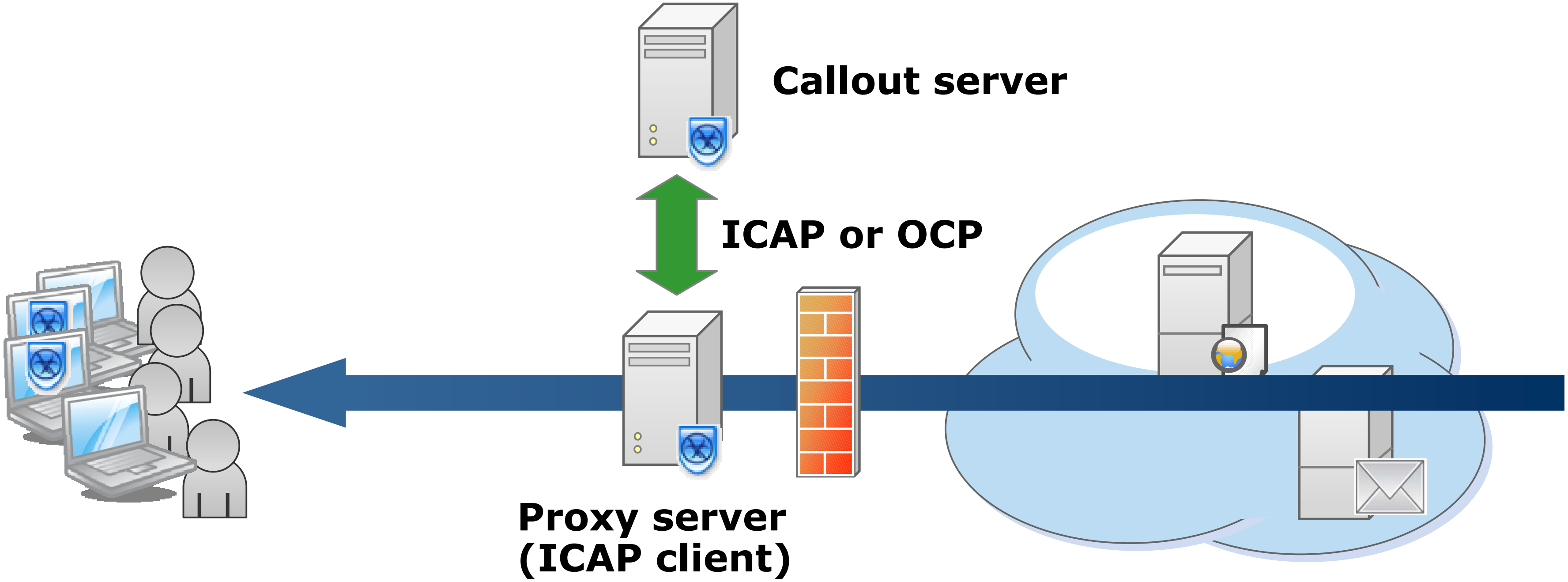
Update Strategy

- For client solutions it seems to be ok to simply restart an engine after an update
- For gateways this is a no-go:
  - Before restart existing scans need to be ended, no new scan can be started
  - The whole procedure will take many seconds while no request can be handled
- Common practice for gateway solutions:
  - Start independent second instance with updated version
  - Continue to handle existing requests on the original instance
  - All new requests go to the new instance
  - When no more requests are handled by original instance, shut it down
- Prevent pitfall:
  - Are you prepared to handle yet another update while the two instances are doing the hand-over?

False Positives

- False positives are a pain everywhere
- On a client or server scanner they can cause a desaster
- On a gateway this is less an issue
  - For Web gateways the original resource should still be reachable at that URL. A false positive can be removed by adding a white list entry and download is repeated.
  - For Email gateways make sure that it's not the only copy of the file that is being replaced by an error message.
- The default policy should be: Block when in doubt (block "mail bombs" rather than letting them thru).
- This opens up new opportunities to deploy new proactive detection methods (such as reputation based systems) on gateway solutions first!

Callout server deployment



ICAP

- Version 0.9 in 1999
- First products with version 0.95 end of 2000
- Version 1.0 ready in mid of 2001
- Took two more years before ICAP/1.0 has been published as **Informational** RFC 3507 in April 2003
- Became *de-facto* standard
- Dozens of companies support ICAP today and have joined the ICAP Forum (www.icap-forum.org)

ICAP/1.0

- Syntax is similar to HTTP/1.1
- Encapsulates HTTP request and response parts into ICAP messages:

```
RESPMOD icap://127.0.0.1:1344/wwrespmod ICAP/1.0
Host: 127.0.0.1
Encapsulated: req-hdr=0, res-hdr=137, res-body=297

GET /origin-resource HTTP/1.1
Host: www.origin-server.com
Accept: text/html, text/plain, image/gif
Accept-Encoding: gzip, compress

HTTP/1.1 200 OK
Date: Mon, 10 Jan 2000 09:52:22 GMT
Server: Apache/1.3.6 (Unix)
ETag: "63840-1ab7-378d415b"
Content-Type: text/plain
Content-Length: 68

44
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
0
```

Preview and ICAP 204 responses

- Why is that faster or more efficient than proxy chaining?

- An ICAP server usually first receives a preview – first few kB of data.
- It can then decide whether it wants to see the rest (ICAP/1.0 100 Continue response)...
- ...or whether it is not interested and the proxy shall handle the rest of the file alone
  (ICAP/1.0 204 Not Modified response)

- The same 204 response may also be allowed after all data has been received; not modified data does not need to be returned.
- But proxy needs to be able to cache the original file completely
- And it does not work if Data Trickling has been started

OPES

- While ICAP was developed a group of interested people wanted to set up a working group with in IETF about callout services.
- After a lot of discussion, the WG was founded in February 2002.
- OPES WG = Open Pluggable Edge Services Working Group
- Several RFCs have been created
  - including OCP (OPES callout protocol)
  - planned to become ICAP/2.0
- So far, this protocol has not been used in a commercial product
- The working group wound up in March 2007

- Nevertheless:
  OCP has some interesting advantages over ICAP/1.0

OCP advantages over ICAP/1.0

- The protocol core (RFC 4037) is application-agnostic.
  - ICAP was designed for HTTP only
  - OCP agents negotiate the best fitting profile
  - An HTTP profile has been developed and standardized as RFC 4236
  - An SMTP profile has been prepared

- Efficiency:
  - OCP clients and servers can send multiple transactions on a single connection
  - Sending/receiving is fully asynchronous.
  - There is no wait-for-an-answer status as with ICAP's preview response.

- Enhanced "preview" functionality:
  - Multi-stage previews (server can request at any time to get out of the loop)
  - Dynamic negotiation which part of the file can be preserved at the client and which part the server wants to refer to rather than sending back.

OCP Example

```
P: SGC 12 ({"44:ocp-test.example.com/translate?from=EN&to=DE"});
P: TS 89 12;
P: AMS 89
   AM-EL: 86
   ;
P: DUM 89 0
   AM-Part: response-header

   65:HTTP/1.1 200 OK
   Content-Type: text/plain
   Content-Length: 86


   ;
P: DUM 89 65
   AM-Part: response-body
  86:Whether 'tis nobler in the mind to suffer
   The slings and arrows of outrageous fortune
   ;
P: AME 89;
S: AMS 89
   AM-EL: 78
   ;
P: TE 89;
S: DUM 89 0
   AM-Part: response-header
```

Outbound Protection

- Gateway Outbound Protection usually refers to “Data Leakage prevention”
- And Anti Malware protection is usually concentrating on inbound traffic
- But also outbound an Anti Malware Gateway can at least be very effective to detect already infected clients!
- Detect
  - that Worms are sent from the internal network and block that
  - that Spyware is trying to phone home and block that
  - that mobile devices with old AV signatures wants to connect to the Web

Gateway Solution Testing

- Most anti-malware product tests focus on client and server programs
- Sometimes gateway products can participate but in other cases the test methodology does not allow gateway products.
- Tests for some certifications have been especially tuned for gateway products.
- The typical road blockers are
  - on-access scanner tests
  - ultra-strict false positive rate
  - disinfection requirements
  - different performance test methodology

Would be nice to see some product tests specifically for gateway products.

Questions?