Ciberseguridad en la Red de una Granja Web

Who am I?

Juan Carlos Gámez Granados

Doctor en Informática

Máster en Técnologías Multimedia

Ingeniero en Informática

Instructor CISCO

Responsable Academia CISCO de la Universidad de Córdoba

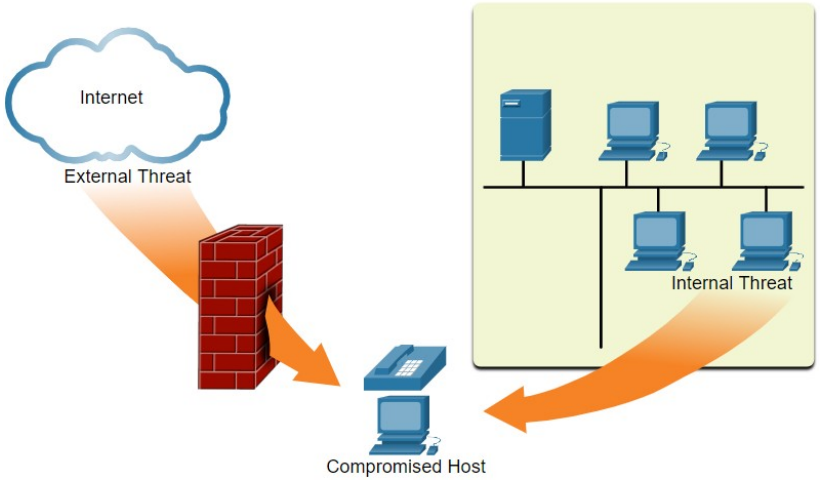
Coordinador del Aula de Ciberseguridad y Redes de la Universidad de Córdoba

Conceptos (I)

- **Activos**
  - Un activo es cualquier cosa de **valor** para la organización. Incluye personas, equipos, recursos y datos.
- **Vulnerabilidad**
  - Una vulnerabilidad es una **debilidad** en un sistema, o su diseño, que podría ser explotada por una amenaza.
- **Amenaza**
  - Una amenaza es un **peligro** potencial para los activos, los datos o la funcionalidad de la red de una empresa.
- **Exploit**
  - Un exploit es un **mecanismo** para tomar ventaja de una vulnerabilidad.

Conceptos (II)

- **Mitigación**
  - La mitigación es la **contra-medida** que reduce la probabilidad o la severidad de una posible amenaza o riesgo. La seguridad de redes consiste en técnicas de mitigación múltiples.
- **Riesgo**
  - El riesgo es la **probabilidad** de que una amenaza explote la vulnerabilidad de un activo, con el objetivo de afectar negativamente a una organización. El riesgo se mide utilizando la probabilidad de ocurrencia de un evento y sus consecuencias.
- **Vector de ataque**
  - Un vector de ataque es una **ruta** por la cual un atacante puede obtener acceso a un servidor, host o red. Los vectores de ataque se originan dentro o fuera de la red corporativa.



Conceptos (III)

- **Pérdida/Filtración de datos (I)**
  - Términos utilizados para describir cuándo los datos se pierden con o sin intención, son robados o se filtran fuera de la organización. La pérdida de datos puede generar:
    - Daño de la marca/pérdida de la reputación.
    - Pérdida de la ventaja competitiva
    - Pérdida de clientes.
    - Pérdida de ingresos.
    - Acciones legales que generen multas y sanciones civiles.
    - Costo y esfuerzo significativos para notificar a las partes afectadas y recuperarse de la transgresión.

Conceptos (IV)

- **Pérdida/Filtración de datos (II)**
  - Vectores de pérdida de datos
    - *Correo electrónico / Redes sociales*: El correo electrónico o los mensajes de mensajería instantánea interceptados podrían capturarse y descifrar el contenido.
    - *Dispositivos no encriptados*: Si los datos no se almacenan utilizando un algoritmo de cifrado, entonces el ladrón puede extraer datos confidenciales de valor.
    - *Dispositivos de almacenamiento en la nube*: Los datos confidenciales se pueden perder si el acceso a la nube se ve comprometido debido a ajustes débiles en la seguridad.
    - *Medios extraíbles*: Un riesgo es que un empleado pueda realizar una transferencia no autorizada de datos a un dispositivo USB. Otro riesgo es que el dispositivo USB que contiene datos corporativos de valor se puede extraviar.
    - *Respaldo físico*: Los datos confidenciales deben triturarse cuando ya no sean necesarios.
    - *Control de Acceso Incorrecto*: Las contraseñas o contraseñas débiles que se hayan visto comprometidas pueden proporcionar al atacante un acceso fácil a los datos corporativos.

Conceptos (V)

- **Hacker (I)**
  - Término usado para describir un atacante. Hay varios tipos:
    - *Hackers de Sombrero Blanco*: Son hackers éticos que utilizan sus habilidades de programación para fines buenos, éticos y legales. Las vulnerabilidades en la seguridad se informan a los desarrolladores para que las corrijan antes de que las vulnerabilidades puedan aprovecharse.
    - *Hackers de Sombrero Gris*: Son personas que cometen delitos y hacen cosas probablemente poco éticas, pero no para beneficio personal o ni para causar daños. Un hacker de sombrero gris puede divulgar una vulnerabilidad de la organización afectada después de haber puesto en peligro la red.
    - *Hackers de sombrero negro*: Son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red.

Conceptos (VI)

- **Hacker (II)**
  - Otros tipos:
    - *Script kiddies*: Estos son adolescentes o hackers inexpertos que corren scripts, ejecutan herramientas y exploits existentes para ocasionar daño, pero generalmente no para obtener ganancias.
    - *Agentes de Vulnerabilidad*: Son generalmente hackers de sombrero gris que intentan descubrir los exploits e informarlos a los proveedores, a veces a cambio de premios o recompensas.
    - *Hacktivistas*: Estos son hackers de sombrero gris que protestan en público contra las organizaciones o gobiernos mediante la publicación de artículos, videos, la filtración de información confidencial y la ejecución de ataques a la red.
    - *Delincuentes cibernéticos*: Son hackers de sombrero negro independientes o que trabajan para grandes organizaciones de delito cibernético.
    - *Patrocinados por el estado*: Son hackers de sombrero blanco o sombrero negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras. La mayoría de los países del mundo participan en algún tipo de hacking patrocinado por el estado.

Tipos de ataques (I)

- **Ataque de intercepción pasiva (eavesdropping)**

  Esto sucede cuando un hacker captura y "escucha" el tráfico de red. Este ataque también se conoce como sniffing o snooping.

- **Ataque de Modificación de Datos**

  Si los hackers han obtenido tráfico de la empresa, pueden alterar los datos en el paquete sin el conocimiento del remitente o del receptor.

- **Ataque de suplantación de dirección IP**

  Un atacante crea un paquete IP que parece provenir de una dirección válida dentro de la intranet corporativa.

- **Ataques basados en contraseñas**

  Si los harckers descubren una cuenta válida de usuario, los hackers tienen los mismos derechos que el usuario real. Los hackers pueden usar una cuenta válida para obtener listas de otros usuarios, información de red, cambios de servidor y configuraciones de red, y modificar, redirigir o borrar datos.

- **Ataques de Ingeniería Social**

  Usuario es el eslabón más débil (pretesting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, dumpster diving)

Tipos de ataques (II)

- **Ataque de Denegación de Servicio (DoS)**

  Un ataque de DoS impide el uso normal de una computadora o red por parte de usuarios válidos. Un ataque de DoS también puede saturar una computadora o toda la red con tráfico hasta que se apaguen por sobrecarga. Un ataque de DoS también puede bloquear tráfico; eso deriva en la pérdida de acceso a recursos de red por parte de usuarios autorizados.

- **Ataque man-in-the-middle**

  Este ataque se produce cuando los hackers se colocan entre un origen y un destino. Entonces ahora pueden monitorear, capturar y controlar la comunicación en forma activa y transparente.

- **Ataque de Claves Comprometidas**

  Si un atacante obtiene una clave secreta, esa clave se conoce como una clave de riesgo. Una clave comprometida puede utilizarse para obtener acceso a una comunicación asegurada sin que el emisor ni el receptor se enteren del ataque. (Ej. Wifi)

- **Ataque de analizador de protocolos**

  Un analizador de protocolos es una aplicación o un dispositivo que puede leer, monitorear y capturar intercambios de datos en la red y leer paquetes de red. Si los paquetes no están cifrados, un analizador de protocolos permite ver por completo los datos que los componen. (Ej: CDP)

Herramientas de ciberseg. (I)

- **Decodificadores de contraseñas**

  Las herramientas para descodificar contraseñas a menudo se les conoce como herramientas de recuperación de contraseña y pueden ser usadas para decodificar o recuperar una contraseñar. Los decodificadores de contraseñas hacen intentos repetidos para averiguar la contraseña. Ej: John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.

- **Herramientas de hacking Inalámbrico**

  Las herramientas de hacking inalámbrico se utilizan para hackear intencionalmente una red inalámbrica con el fin de detectar vulnerabilidades en la seguridad. Ej: Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and ViStumbler.

- **Escaneo de redes y herramientas de hacking**

  Las herramientas de análisis de red se utilizan para sondear dispositivos de red, servidores y hosts para puertos TCP o UDP abiertos. Ej: Nmap, SuperScan, Angry IP Scanner y NetScanTools.

- **Herramientas para elaborar paquetes de prueba**

  Estas herramientas se utilizan para sondear y probar la solidez de un firewall usando paquetes especialmente diseñados. Ej: Hping, Scapy, Socat, Yersinia, Netcat, Nping y Nemesis.

- **Sniffers de paquetes**

  Estas herramientas se utilizan para capturar y analizar paquetes dentro de redes tradicionales LAN Ethernet o WLAN. Ej: Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy y SSLstrip.

Herramientas de ciberseg. (II)

- **Detectores de Rootkits**

  Se trata de un comprobador de integridad de archivos y directorios utilizado por hackers de sombrero blanco para detectar rootkits instalados. Ej: AIDE, Netfilter y PF: OpenBSD Packet Filter.

- **Fuzzers para buscar vulnerabilidades**

  Los fuzzers son herramientas usadas por los atacantes cuando intentan descubrir las vulnerabilidades de seguridad de una computadora. Ej: Skipfish, Wapiti y W3af.

- **Herramientas de informática forense**

  Estas herramientas son utilizadas por los hackers de sombrero blanco para detectar cualquier rastro de evidencia existente en una computadora. Ej: Sleuth Kit, Helix, Maltego y Encase.

- **Depuradores**

  Los hackers de sombrero negro utilizan estas herramientas para aplicar ingeniería inversa en archivos binarios cuando programan ataques. También las utilizan los sombreros blancos cuando analizan malware. Ej: GDB, WinDbg, IDA Pro e Immunity Debugger.

Herramientas de ciberseg. (III)

- **Sistemas Operativos para hacking**

  Estos son sistemas operativos especialmente diseñados precargados con herramientas optimizadas para hacking. Ej: Kali Linux, BackBox Linux.

- **Herramientas de Cifrado**

  Las herramientas de encriptación utilizan esquemas de algoritmo para codificar los datos a fin de prevenir el acceso no autorizado a los datos encriptados. Ej: VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN y Stunnel.

- **Herramientas para atacar vulnerabilidades**

  Estas herramientas identifican si un host remoto es vulnerable a un ataque de seguridad. Ej: Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit y Netsparker.

- **Escáneres de vulnerabilidades**

  Estas herramientas analizan una red o un sistema para identificar puertos abiertos. También pueden utilizarse para escanear vulnerabilidades conocidas y explorar máquinas virtuales, dispositivos BYOD y bases de datos de clientes. Ej: Nipper, Core Impact, Nessus, SAINT y OpenVAS.

Seguridad de la Información

- Pilares de la seguridad de la información (CIA - inglés):
  - **Confidencialidad (C)**: Solamente individuos, entidades o procesos autorizados pueden tener acceso a información confidencial. Uso de algoritmos de cifrado criptográfico para cifrar y descifrar datos Ej: AES, RSA, 3DES, ...
  - **Integridad (I)**: Se refiere a proteger los datos de modificaciones no autorizadas. Uso de algoritmos de hashing criptográficos. Ej: SHA, MD5, ...
  - **Disponibilidad (A)**: Los usuarios autorizados deben tener acceso ininterrumpido a los recursos y datos importantes. Requiere implementar servicios puertas de enlace y enlaces redundantes.

Implementación de la Seg. (I)

- Control de acceso:
  - Configuración de contraseñas para acceso a Router y Switch mediantes ssh. User y SuperUser.
  - AAA:Autenticación, Autorización y Contabilidad
    - Es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

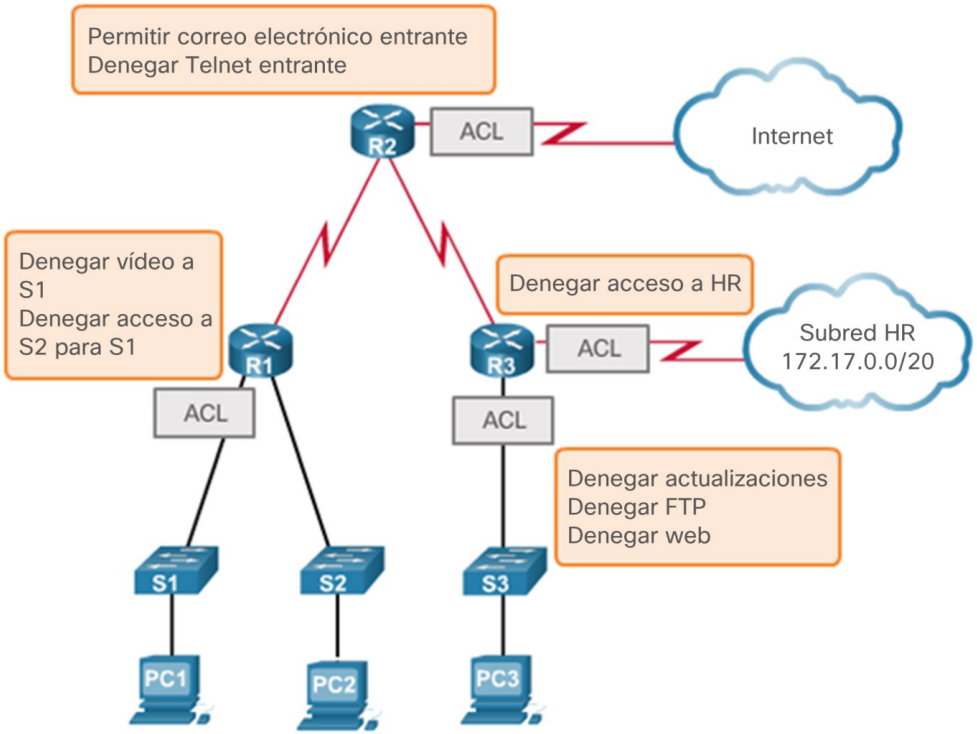
```
S1#configure terminal
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
```

```
S1#configure terminal
S1(config)#enable password contraseña
S1(config)#enable secret contraseña
S1(config)#end
```

```
S1#configure terminal
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
```

Implementación de la Seg. (II)

- Listas de control de acceso (ACL) (I):
  - Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones IP o protocolos de capa superior.
  - Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE).



Implementación de la Seg. (III)

- Listas de control de acceso (ACL) (II):
  - El filtrado de paquetes, a veces denominado “filtrado de paquetes estático”, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según determinados criterios, como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete.
  - Cuando reenvía o deniega los paquetes según las reglas de filtrado, un router funciona como filtro de paquetes.

Las ACL de entrada filtran los paquetes que ingresan a una interfaz específica y lo hacen antes de que se enruten a la interfaz de salida.

Las ACL de salida filtran los paquetes después de que se enrutan, independientemente de la interfaz de entrada.

Implementación de la Seg. (IV)

- Listas de control de acceso (ACL) (III):
  - Las ACL realizan las siguientes tareas:
  - Limitar el tráfico de red para mejorar el rendimiento de ésta.
  - Por ejemplo, si la política corporativa no permite el tráfico de video en la red, pueden configurarse y aplicarse las ACL que bloquean el tráfico de video. Esto reduce considerablemente la carga de la red y aumenta su rendimiento.
  - Brindar control de flujo de tráfico.
  - Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
  - Proporcionar un nivel básico de seguridad para el acceso a la red.
  - Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, el acceso a la red de Recursos Humanos puede restringirse a determinados usuarios.
  - Se debe decidir qué tipos de tráfico enviar o bloquear en las interfaces del router.
  - Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
  - Controlar las áreas de la red a las que puede acceder un cliente.
  - Analizar los hosts para permitir o denegar su acceso a los servicios de red.
  - Las ACL pueden permitir o denegar el acceso de un usuario a tipos de archivos, como FTP o HTTP.

Implementación de

- Listas de control de acceso (ACL) (IV):

Ejemplo 1:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
!OR
R1(config)# access-list 1 permit any
```

Ejemplo 2:

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
!OR
R1(config)# access-list 1 permit host 192.168.10.10
```

Máscaras de wildcard

Posición del bit de octeto y valor de dirección para el bit

128	64	32	16	8	4	2	1	Ejemplos
0	0	0	0	0	0	0	0	= Hacer coincidir todos los bits de dirección (coincidir todos)
0	0	1	1	1	1	1	1	= Ignorar los últimos 6 bits de dirección
0	0	0	0	1	1	1	1	= Ignorar los últimos 4 bits de dirección
1	1	1	1	1	1	0	0	= Ignorar los primeros 6 bits de dirección
1	1	1	1	1	1	1	1	= Omitir todos los bits del octeto

0 significa hacer coincidir el valor del bit de dirección correspondiente
1 significa ignorar el valor del bit de dirección correspondiente

Máscaras de comodín para establecer coincidencias con hosts y subredes IPv4

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara de comodín	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Implementación de la Seg. (VI)

- Listas de control de acceso (ACL) (V):
  - Reglas para aplicar ACL

Filtrado de tráfico en un router mediante ACL

Una lista por interfaz, por dirección y por protocolo

Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Reglas para aplicar las ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., GigabitEthernet0/0)

Implementación de la Seg. (VII)

- Listas de control de acceso (ACL) (VI):
  - Tipos de ACL (I):
    - Estándar
      - Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan.
    - Extendida
      - Las ACL extendidas filtran paquetes IPv4 según varios atributos:
      - Tipo de protocolo
      - Dirección IPv4 de origen
      - Dirección IPv4 de destino
      - Puertos TCP o UDP de origen
      - Puertos TCP o UDP de destino
      - Información optativa de tipo de protocolo para un control más preciso

Implementación de la Seg. (VIII)

- Listas de control de acceso (ACL) (VII):
  - Tipos de ACL (II):

ACL denominada:

Asignar un nombre para identificar la ACL.

- Los nombres pueden contener caracteres alfanuméricos.
- Se sugiere escribir el nombre en MAYÚSCULAS.
- Los nombres no pueden contener espacios ni signos de puntuación.
- Se pueden agregar o eliminar entradas dentro de la ACL.

ACL numerada:

Asignar un número según el protocolo que se debe filtrar.

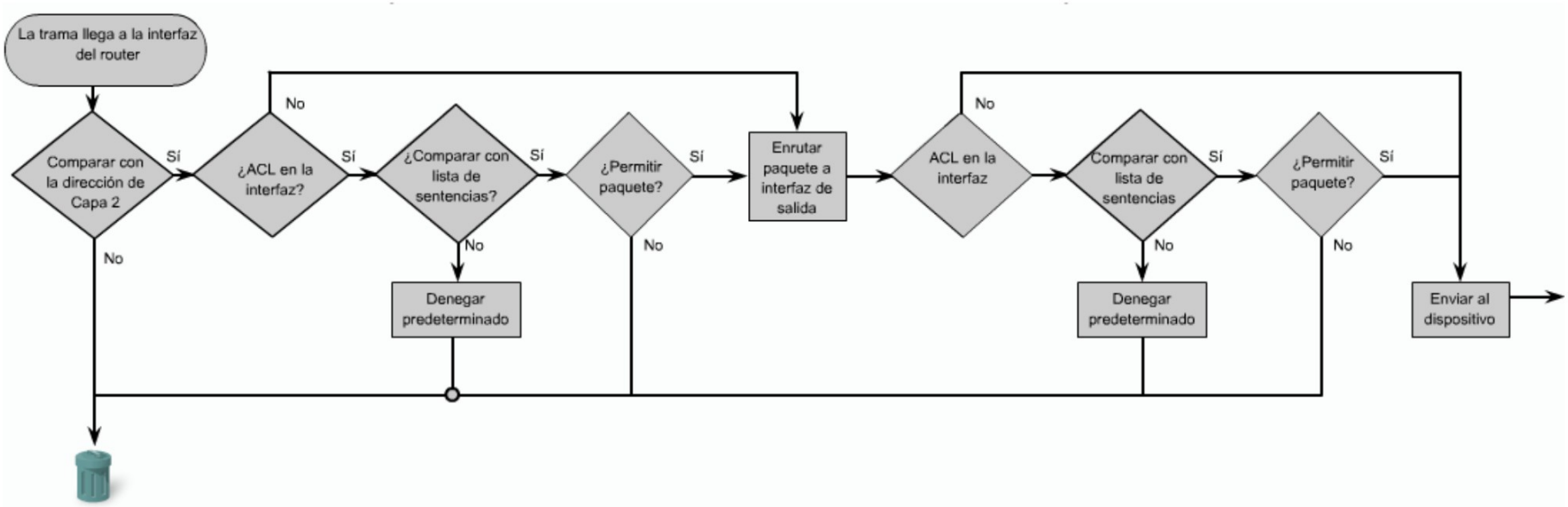
- (1 a 99) y (1300 a 1999): ACL de IP estándar
- (100 a 199) y (2000 a 2699): ACL de IP extendida

Implementación de la Seg. (IX)

- Listas de control de acceso (ACL) (VIII):
  - Funcionamiento (I):
    - Las ACL no actúan sobre paquetes que se originan en el mismo router.
    - Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.
    - Las sentencias de la ACL operan en orden secuencial.
    - Una sentencia implícita final cubre todos los paquetes para los cuales las condiciones no resultan verdaderas (implicit deny any statement/deny all traffic).
    - ACL de salida, antes de reenviar un paquete a una interfaz de salida, el router verifica la tabla de enrutamiento para ver si el paquete es enrutable.

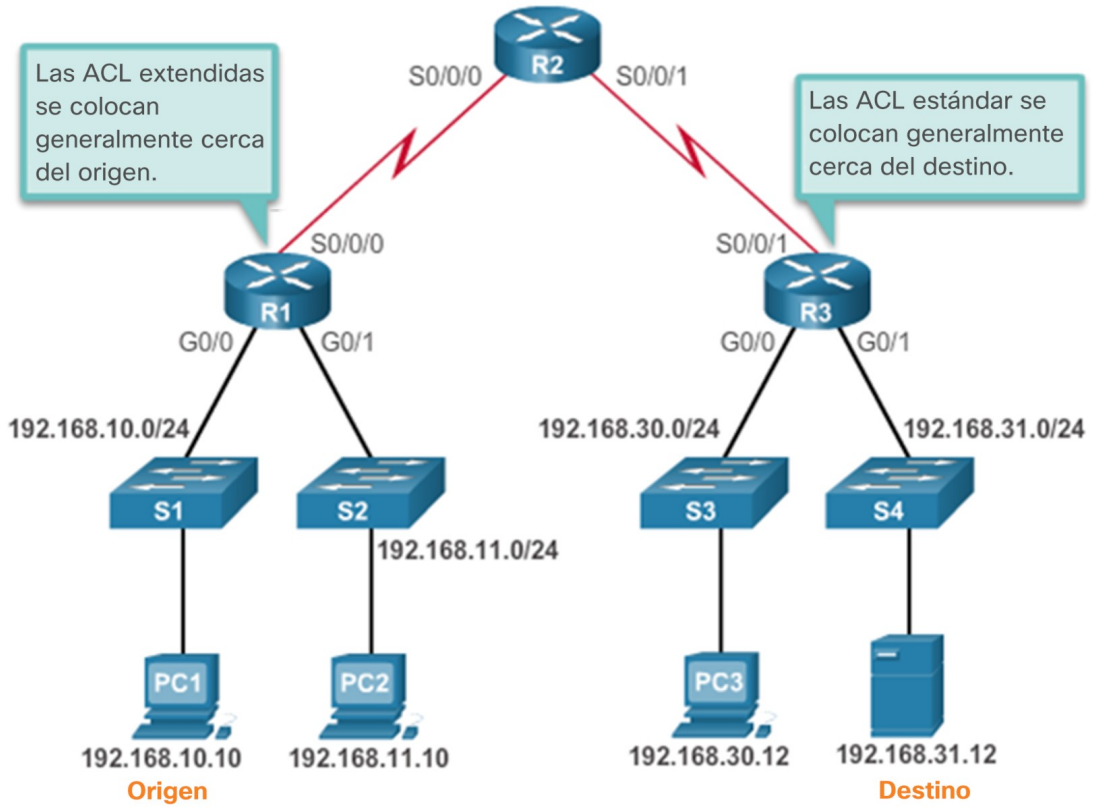
Implementación de la Seg. (X)

- Listas de control de acceso (ACL) (IX):
  - Funcionamiento (II):



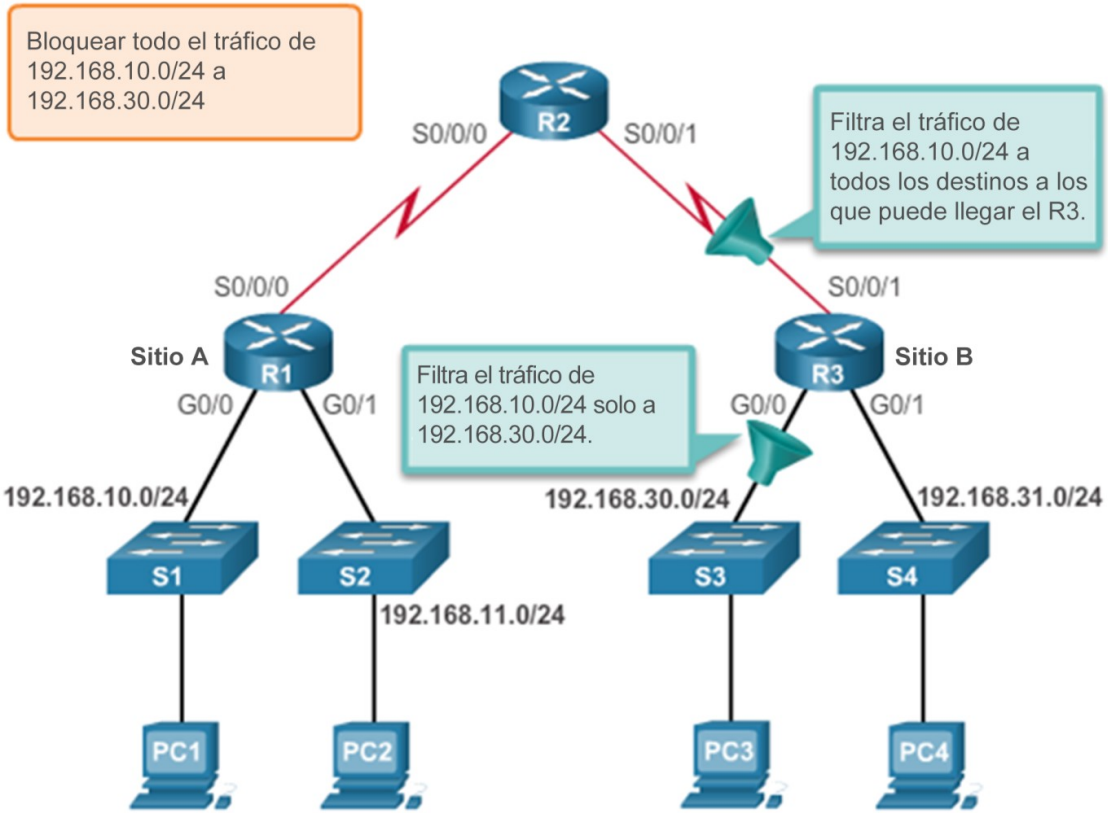
Implementación de la Seg. (XI)

- Listas de control de acceso (ACL) (XI):
  - ¿Dónde ubicar las ACL? (I):



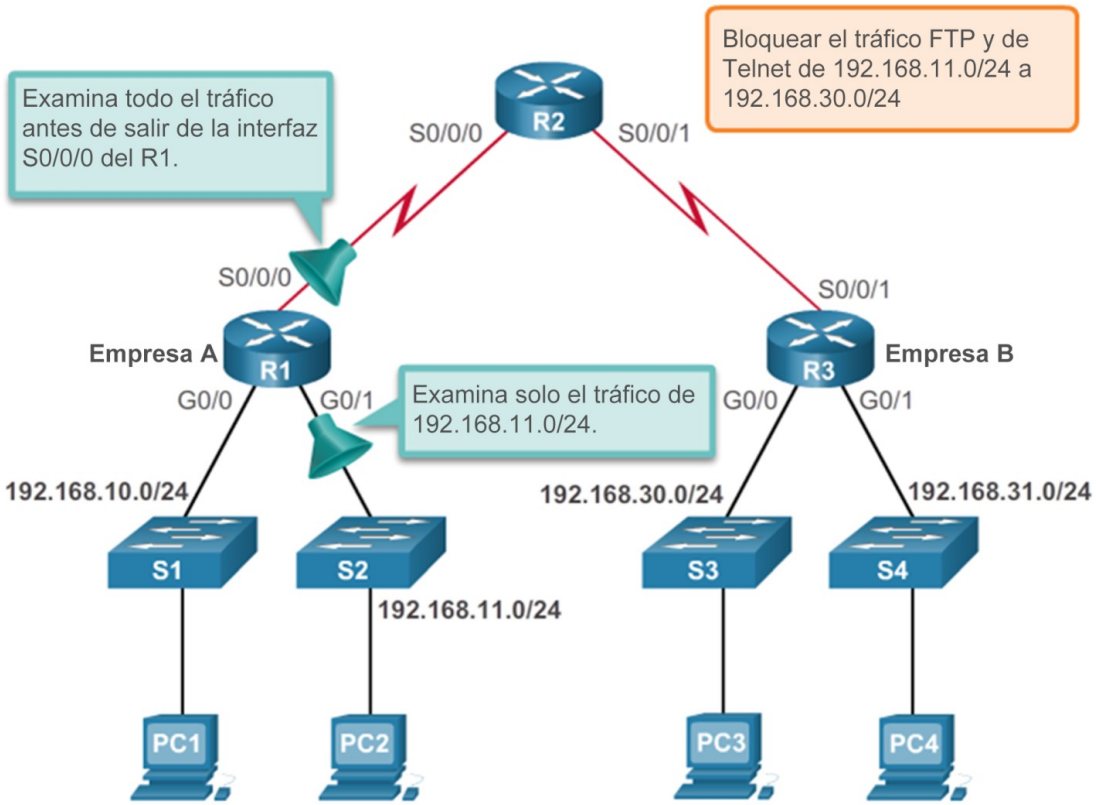
Implementación de la Seg. (XII)

- Listas de control de acceso (ACL) (XII):
  - Ejemplo ACL estándar: El administrador desea impedir que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.



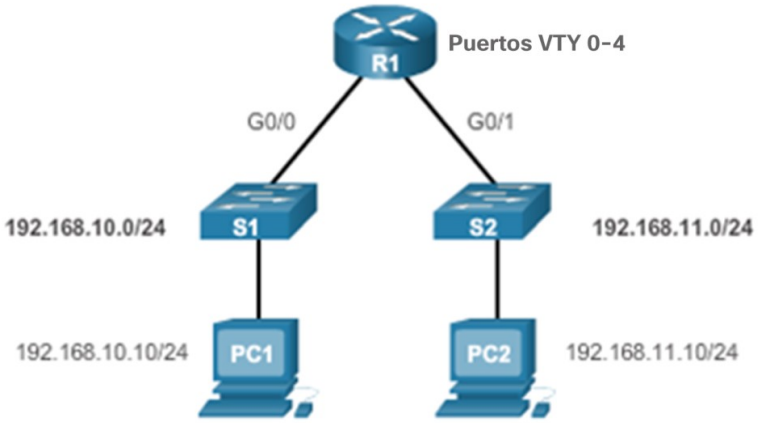
Implementación de la Seg. (XIII)

- Listas de control de acceso (ACL) (XIII):
  - Ejemplo ACL extendida: Lo que el administrador desea es denegar el tráfico de Telnet y FTP de la red 192.168.11.0/24 a la red 192.168.30.0/24 de la empresa B. Se debe permitir que el resto del tráfico de la red .11 salga de la empresa A sin restricciones.



Implementación de la Seg. (XIV)

- Listas de control de acceso (ACL) (XIV):
  - ACL para terminal: El comando access-class configurado en el modo de configuración de línea restringe las conexiones entrantes y salientes entre una VTY determinada (en un dispositivo de Cisco) y las direcciones incluidas en una lista de acceso.




```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class 21 in
R1(config-line)# exit
R1(config)# access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)# access-list 21 deny any
```

Implementación de la Seg. (XV)

- Tabla MAC (I):
  - Seguridad de puertos (port security)

Guión de configuración de seguridad de puerto

Sintaxis de comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global. Use este comando del IOS de Cisco:	`S1#configure terminal`
Especificar el tipo y número de interfaz física a configurar. Use este comando del IOS de Cisco:	`S1(config)#interface fastEthernet 0/18`
Establecer el modo de interfaz como acceso. Use este comando del IOS de Cisco:	`S1(config-if)#switchport mode access`
Activar la seguridad de puerto en la interfaz. Use este comando del IOS de Cisco:	`S1(config-if)#switchport port-security`
Establecer el número máximo de direcciones seguras en 50. Use este comando del IOS de Cisco:	`S1(config-if)#switchport port-security maximum 50`
Activar el aprendizaje sin modificaciones. Use este comando del IOS de Cisco:	`S1(config-if)#switchport port-security mac-address sticky`
Volver al modo EXEC privilegiado. Use este comando del IOS de Cisco:	`S1(config-if)#end`

Implementación de la Seg. (XVI)

- Tabla MAC (II):
  - Seguridad de puertos (port security)

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

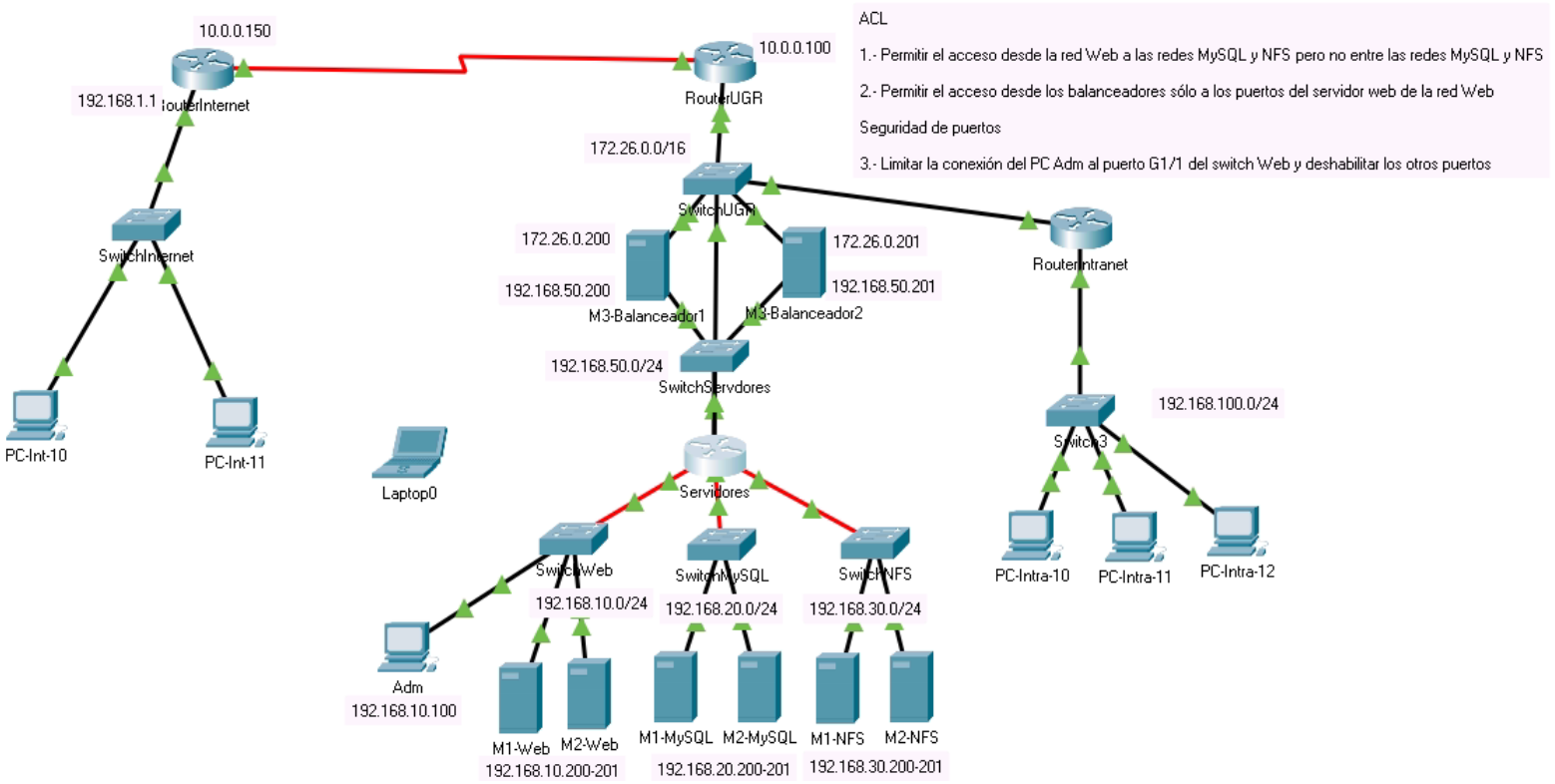
Modo	Descripción
shutdown (predeterminados)	El puerto pasa al estado de error desactivado de inmediato, apaga el LED del puerto y envía un mensaje de registro del sistema. Aumenta el contador de violaciones. Cuando un puerto seguro se encuentra en estado de error desactivado, un administrador debe volver a habilitarlo ingresando los comandos **shutdown** y **no shutdown** .
Restricción	El puerto descarta paquetes con direcciones de origen desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para caer por debajo del valor máximo o aumentar el valor máximo. Este modo hace que el contador de Infracción de seguridad se incremente y genera un mensaje de syslog.
Protección	Este modo es el menos seguro de los modos de violaciones de seguridad. El puerto descarta paquetes con direcciones de origen MAC desconocidas hasta que elimine un número suficiente de direcciones MAC seguras para colocar por debajo del valor máximo o aumentar el valor máximo. No se envía ningún mensaje syslog.

Correspondencia CCNA v6.0

- **CCNA 2 – Capítulo 7**
- **CCNA 4 – Capítulo 4**

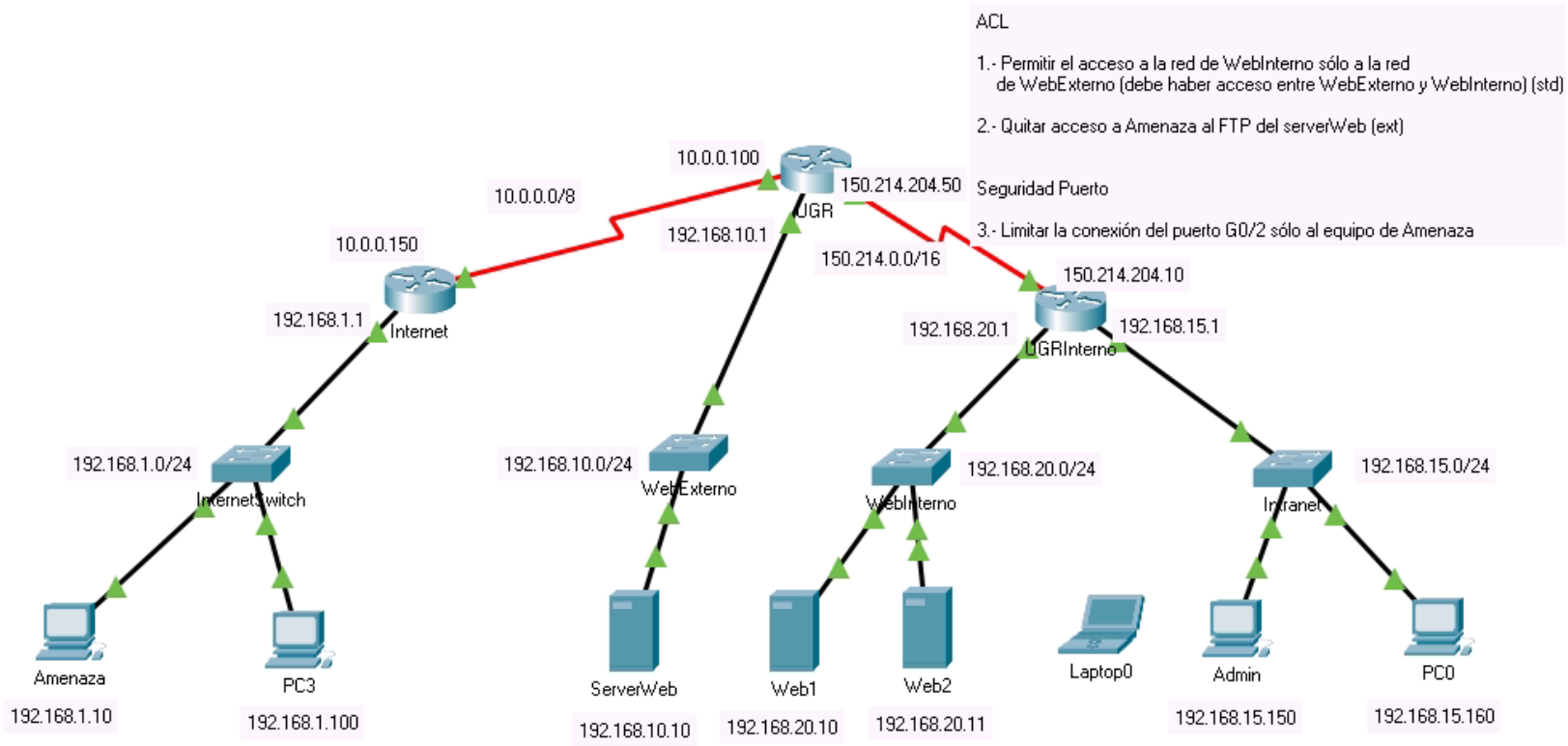
Escenario de prácticas

- En este escenario vamos a trabajar:
  - ACL estándar y extendida (router)
  - Seguridad en puertos de switch



Escenario de prácticas

- En este escenario vamos a trabajar:
  - ACL estándar y extendida (router)
  - Seguridad en puertos de switch



Ciberseguridad en la Red de una Granja Web