UTN.BA UNIVERSIDAD TECNOLÓGICA NACIONAL FACULTAD REGIONAL BUENOS AIRES | Centro de e-Learning Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

UTN.BA | Centro de e-Learning
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Módulo 1:

Diseño de redes seguras

Unidad 4:

Redes informáticas – Seguridad Aplicada

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Presentación

En esta cuarta y última unidad del módulo, nos introducimos en la comprensión de la temática correspondiente a redes seguras, servicios necesarios y procesos a aplicar.

Uso correcto de las Access-list, basándonos en Sistemas IOS de CISCO.

Exposición del primer final obligatorio del módulo.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Objetivos

Que los participantes logren…

- Conocer los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.

- Aprender a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.

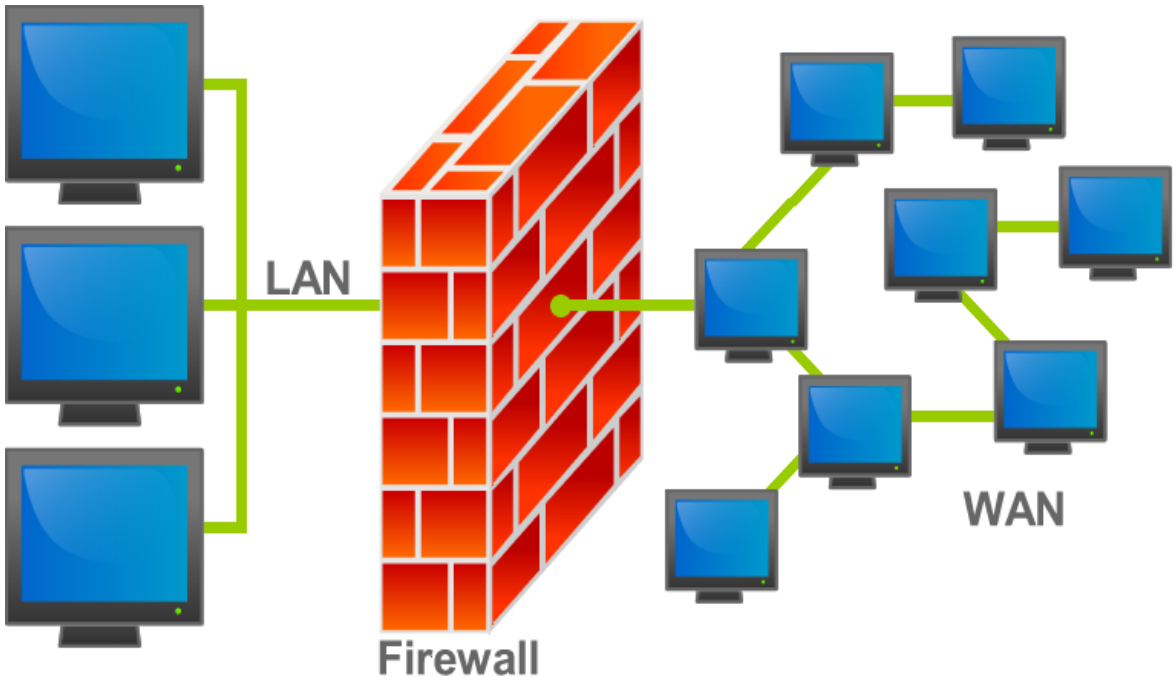
Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bloques temáticos

1. Dispositivos de seguridad (funcionalidades y modo de uso).
2. Estructuración de una red segura.
3. Armado de una red segura.
4. Ejercicio Final de módulo.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Dispositivos de Seguridad



Anteriormente hablamos de varios dispositivos, entre ellos, el firewall, ahora veremos las maneras de cómo usarlo y que es lo que nos ofrece para protegernos de ataques o de intrusos.

Un firewall, tiene como condición principal (siempre y cuando esté bien configurado) bloquear todo acceso no autorizado.

Primer consejo, antes de ponerlo en la red, sería bueno saber **que proteger, como proteger y donde proteger.**

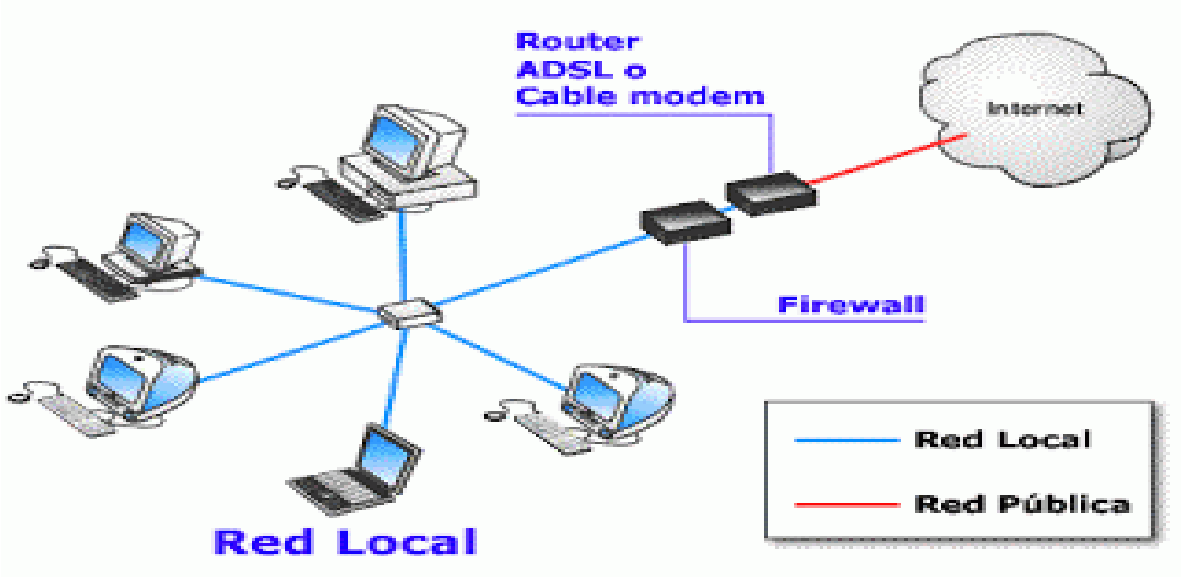
Nos encontraremos dentro de sus servicios con **ACLs** (listas de acceso), **VPN** (virtual private network), **NAT** (network address translation).

Cuando hablamos de saber **que proteger**, es poner en importancia y determinar cuáles son los activos más importantes de la red.

Pueden ser equipos, servicios o hasta un determinado tipo de tráfico (cifrado de datos por ejemplo).

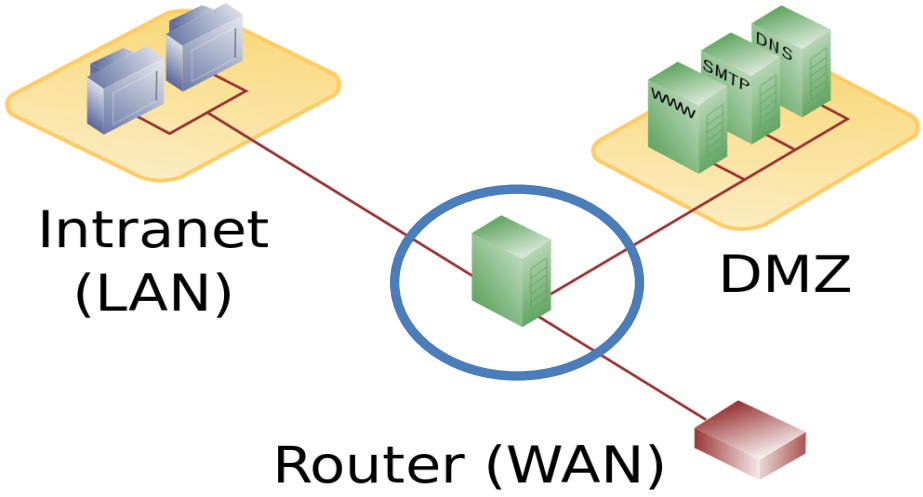
No es lo mismo, proteger un equipo que se usa para repositorio que un servidor principal web de la empresa.

El **que proteger**, lo determinaremos haciendo un análisis de riesgo de la red, donde sabremos el nivel de importancia.



Un ejemplo muy común de donde poner un firewall en la red, en este caso, el que proteger, sería toda la red local.

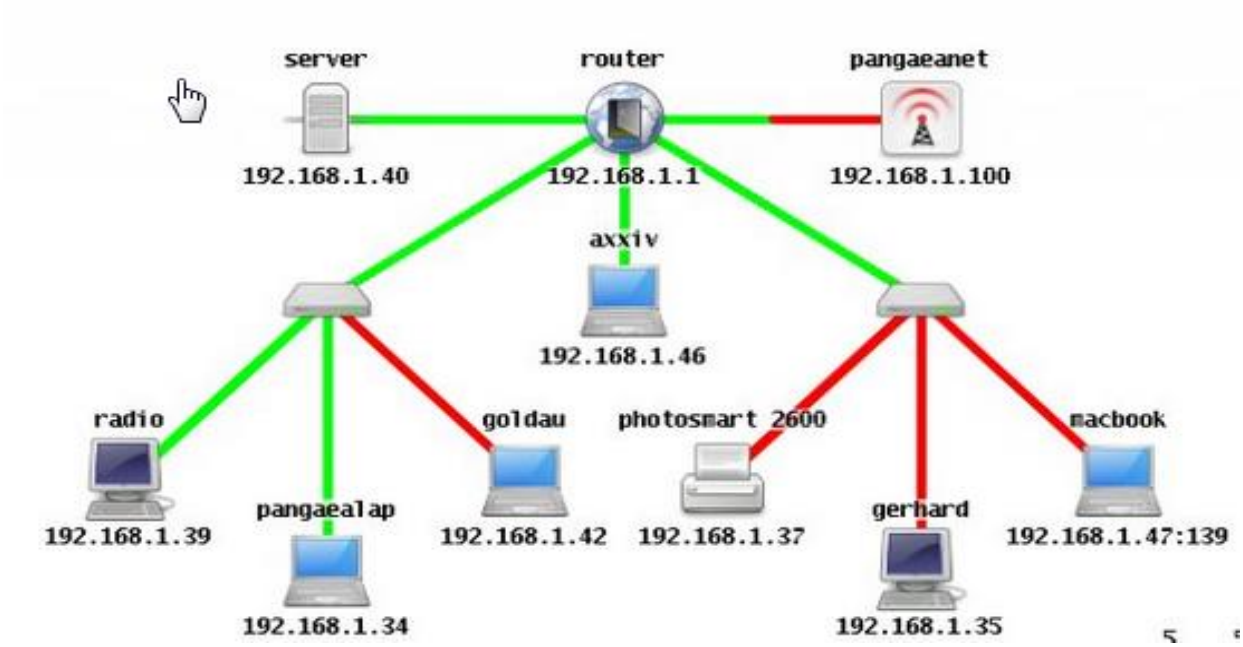
Otro ejemplo, es que interceda entre los servicios que se necesitan publicar a Internet y la red **LAN**.



Ejercicio Número 1 Unidad 4

A continuación se expondrá un gráfico, donde el alumno/a será el que tome la decisión de dónde ubicar un Firewall.

Es de libre interpretación y no lleva corrección, todos tienen que poner su punto de vista y defender su postura.



Datos a tener en cuenta: sabiendo que los enlaces rojos, tienen prioridad de salida a Internet por la antena, y los verdes prioridad de acceso al servidor más importante de la topología.

El instructor creará un post EXCLUSIVO, para que cada uno ponga su opción y expliquen el porqué de la misma.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

El cómo proteger, sería teniendo en cuenta parte de los servicios que nos ofrezca el firewall (**ACLs, NAT, VPN**) y el buen uso y configuración de los mismos.

¿Qué es una ACL?

Es una forma de determinar los ***permisos de acceso*** apropiados a un determinado objeto, dependiendo de ciertos criterios del ***proceso*** que hace el pedido.

Estas operaciones podrían incluir lectura, escritura y ejecución sobre un destino.

Los criterios serían: el origen del tráfico; el destino del tráfico; el protocolo usado.

Funciona a través del firewall o router que analizan cada paquete, comparándolo con la **ACL** correspondiente y compara la **ACL** línea por línea.

Si encuentra una coincidencia, toma la acción correspondiente (**PERMIT** o **DENY**), y ya no revisa los restantes renglones.

Es por eso que hay que listar los comandos desde los casos más específicos, hasta los más generales.

Recordar:

- ⇨ Esencialmente son listas de condiciones para poder acceder a una red o dispositivo.
- ⇨ Son una herramienta muy poderosa para controlar el acceso en ambos sentidos: tanto desde como hacia la red.
- ⇨ Pueden filtrar tráfico no deseado, y son utilizadas para implementar políticas de seguridad.
- ⇨ Al aplicar una lista de acceso, se obliga al router a analizar cada paquete que atraviesa la interfase en una dirección específica, reduciendo de esta manera la performance del dispositivo.
- ⇨ Cada paquete es comparado con cada línea de la lista de acceso en orden secuencial según han sido ingresadas.
- ⇨ La comparación se realiza hasta que se encuentra una coincidencia.

⇨ NO OLVIDAR – El final implícito de todo lista de acceso es una denegación de todo tráfico: deny all

¡Las excepciones tienen que estar antes de la regla general!

¿Y CUAL ES LA REGLA GENERAL?

Si no encuentra una coincidencia en ninguno de los renglones, rechaza automáticamente el tráfico

```
RTA#config t
RTA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RTA(config)#access-list 1 permit 192.168.3.0 0.0.0.255
RTA(config)#access-list 1 permit 192.168.5.0 0.0.0.255
!---Implied "Deny Any"
```

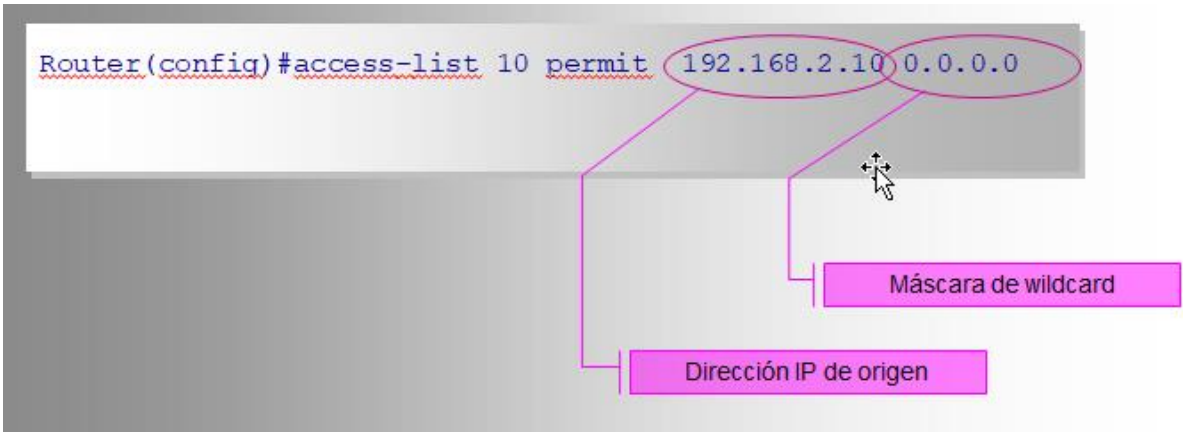
Consideren que hay un "deny any" implícito, al final de cada ACL

Existen muchas maneras de crear un **ACL**, dependemos de qué tipo de tecnología se use, escribiéndola o por intermedio de opciones en la aplicación que se esté corriendo.

En CISCO, por ejemplo, hay 2 tipos de **ACL más conocidas**, las **extendidas** y las **estándar**, y se pueden configurar tanto en routers como firewalls.

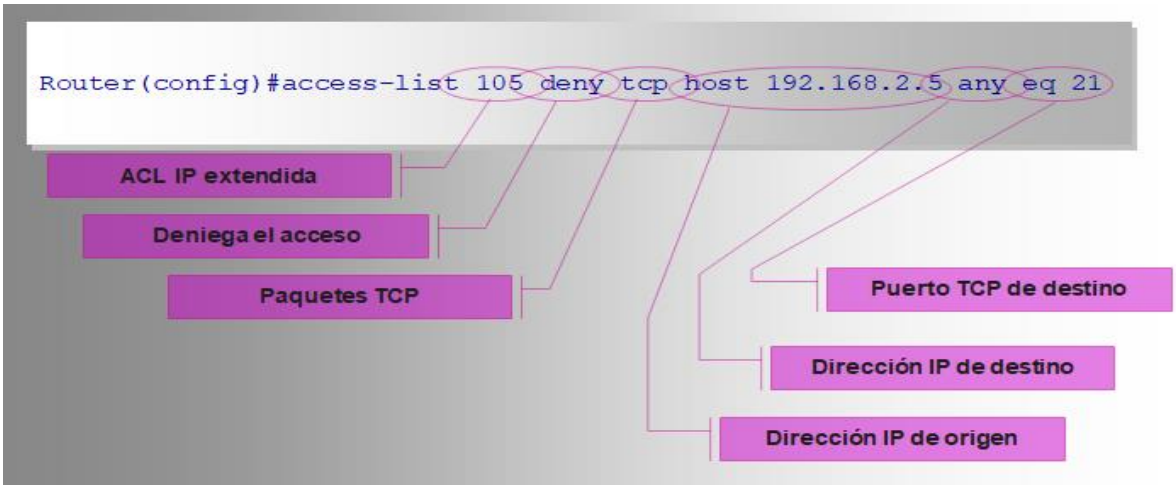
⇨ **Listas de Acceso Estándar**

- **IP –** Filtran paquetes IP considerando solamente la dirección IP de origen.



⇨ **Listas de Acceso Extendidas**

- **IP –** Filtran paquetes IP considerando tanto la dirección de origen como la de destino, y los números de puerto del encabezado de capa de transporte.



TIPS:

⇨ **Solo se puede asignar una lista de acceso por interface.**

⇨ **Organice su lista de acceso de modo que los criterios más específicos estén al inicio.**

⇨ **Si en algún momento se agrega una nueva línea a la lista, esta se ubicará al final de la misma.**

⇨ **No se puede remover una línea de una lista de acceso.**

⇨ **Al menos que su lista termine con un comando permit, todo los paquetes que no coincidan con alguno de los criterios serán descartados.**

⇨ **Toda lista de acceso debe tener al menos un comando permit.**

⇨ **Primero cree la lista de acceso, y luego aplícala a la interfaz.**

⇨ **Las listas de acceso están diseñadas para filtrar el tráfico que atraviesa el router. No filtran el tráfico originado en el router.**

⇨ **Ubique las listas de acceso estándar lo más cerca posible del destino.**

⇨ **Ubique las listas de acceso extendidas lo más cerca posible del origen.**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejemplo:

Quiero permitir únicamente el host (**10.10.10.20**)

La sintaxis podría ser la siguiente:

Access-list 1 permit IP host 10.10.10.20

Obsérvese que de cumplirse esta ACL, los demás equipos tendrán el **deny** implícito.

¿Por qué?

Se expone que únicamente esa IP tendrá permiso, y al no poner más direcciones **IP**, por ende niega todo tráfico.

Otro ejemplo:

Quiero permitir el acceso de la red (**20.20.20.0**) hacia la red (**30.30.30.0**) pero que el equipo con **IP**: **20.20.20.5** no lo tenga

La sintaxis podría ser la siguiente:

Access-list 101 deny IP host 20.20.20.5 30.30.30.0 0.0.0.255

Access-list 101 permit IP 20.20.20.0 0.0.0.255 30.30.30.0 0.0.0.255

¿Por qué?

Primero negamos la específica, que sería la **IP 20.20.20.5** y luego le exponemos lo que si le permitimos.

Cualquier otra dirección **IP** que no sea de las expuestas, **NO** estaría permitida.

Hay que prestar mucha atención, porque el solo hecho de no exponer una/las direcciones IP, podría resultar incómodo encontrar por qué un equipo tiene tráfico y el otro no, a menos que uno sepa que la culpa la tiene la ACL.

Lo más utilizado, es poner primero lo más específico y luego lo genérico (o sea lo que sabemos que se tiene que negar por defecto).

Otro ejemplo:

Tengo dos redes, la red **10.10.10.0** y la red **20.20.20.0.**

La red **10.10.10.0** NO tiene permitido salir a internet (**200.200.200.200**) y la red **20.20.20.0** SI.

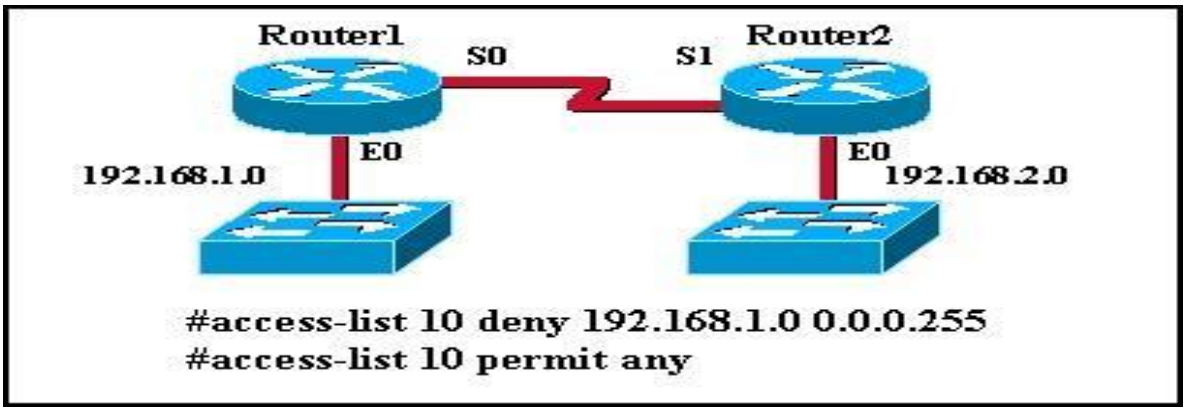
Access-list 101 permit IP 20.20.20.0 0.0.0.255 host 200.200.200.200

(Aquí se permite TODA la red **20.20.20.0** a la **200.200.200.200**)

Y no escribo más nada..... ¿PORQUE?

Porque una de las reglas de las **ACLs**, es que la última línea es un **DENY IMPLICITO**, o sea niega todo lo restante que no esté.

Un ejemplo gráfico:

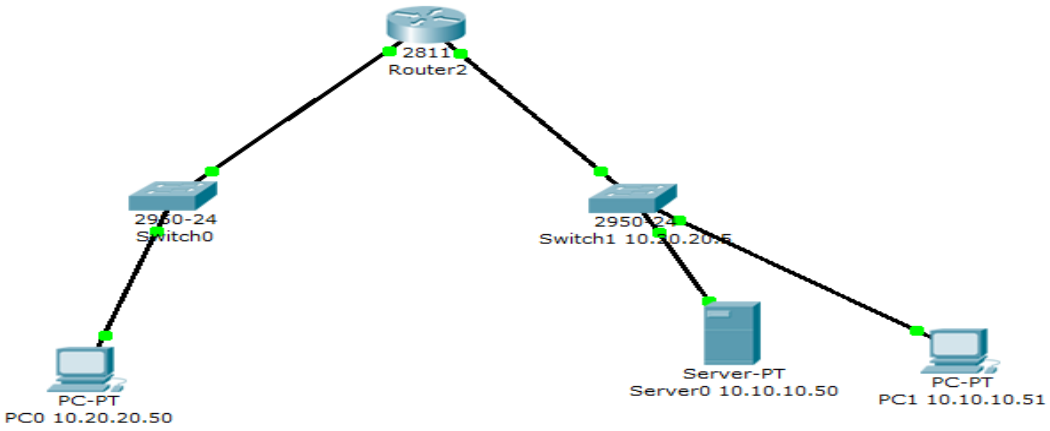


Esas **ACLs** (sin importar en qué router se aplique) lo que nos indica que el tráfico de la RED 192.168.1.0 no está permitido, o sea el único tráfico será el de la RED 192.168.2.0 que si podrá llegar al otro lado.

Pero tenemos un problema, es una posible incidencia de seguridad, ya que estamos negando algo de forma correcta, pero estamos permitiendo redes que quizás no conozcamos al configurar la **ACL** con el permit **ANY**.

Ejercicio Número 2 Unidad 4

Escribir un ACL que permita el tráfico de la PC0 a la PC1 y otro ACL que permita el tráfico de la PC0 al server.



A tener en cuenta:

Un solo dispositivo se representa en una ACL con el identificador HOST o con la wildcard 0.0.0.0.

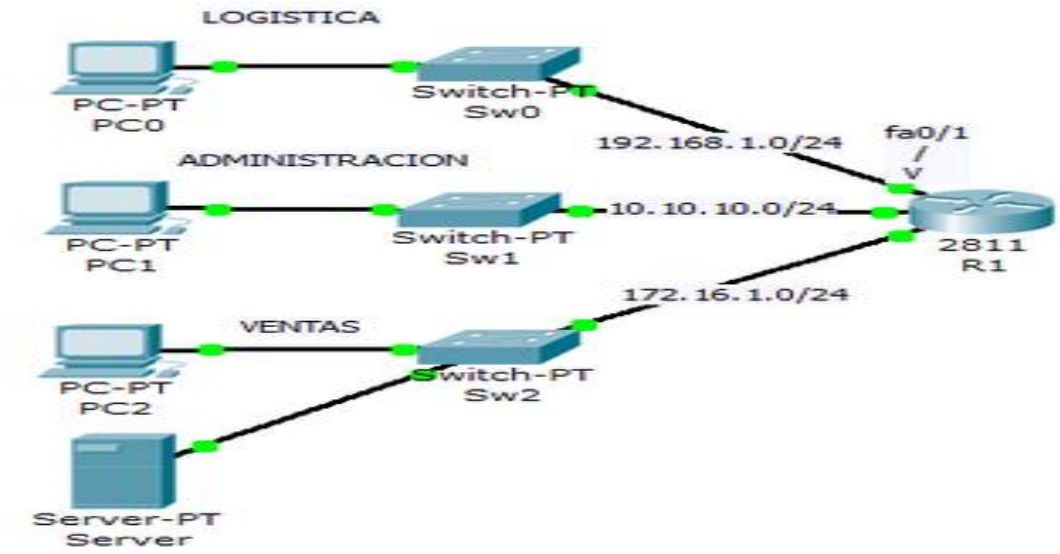
Ejemplos:

access-list 1 permit ip host 10.10.10.10 host 10.10.10.11

access-list 1 permit ip 10.10.10.10 0.0.0.0 10.10.10.11 0.0.0.0

Ambas cumplen el mismo objetivo, que es permitir el host 10.10.10.10 hacia el host 10.10.10.11, son maneras diferentes de configurarlas.

Consigna: Logística y Ventas pueden verse entre sí, pero no pueden ver a Administración, sin embargo Administración puede ver a todas.



RECORDAR: en este caso, son redes /24, por ende, wildcard es 0.0.0.255

TIPS EJERCICIO

Si te interesa el estudio de las ACL, les recomiendo estas lecturas:

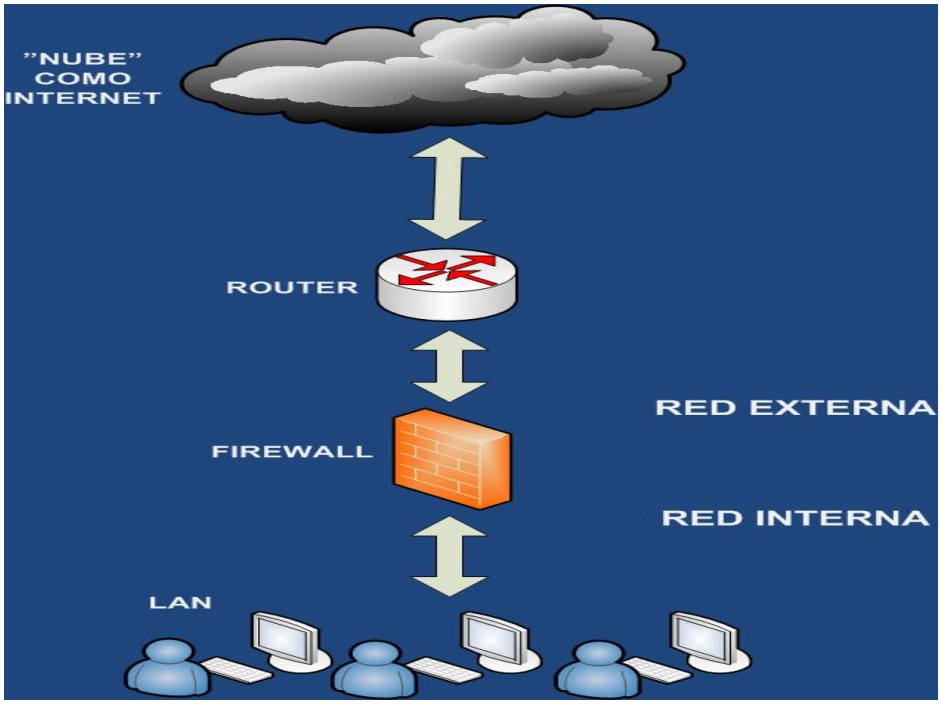
http://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

http://www.oocities.org/hilmarz/cisco/acl.htm

Tener en cuenta que estos links están referidos a equipamiento **CISCO.**

Si te interesa el estudio de las configuraciones de los routers & switches **CISCO**, les recomiendo que se bajen el **PACKET TRACER** como para arrancar, sino pueden bajarse el **GNS3** (***http://www.gns3.net/download/***) que es un emulador real de **IOS** de Cisco (requiere mucha memoria **RAM**).

El donde proteger, se implementará en un área que sea activo el firewall, o sea teniendo en cuenta los servicios o dispositivos a proteger, la ubicación del mismo será a mayor importancia para que afecte lo que necesitamos proteger.



Ejemplo de donde ponerlo teniendo en cuenta la protección hacia dentro desde Internet, separando la red interna de la externa

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Estructuración de una red segura

Cuando estamos al frente de una red, lo primero que se debería hacer es un relevamiento de todos los dispositivos involucrados y luego podremos tener una idea de si hay que modificar la topología o dejarla como esta.

Sabiendo que disponemos de equipos relacionados con la protección de datos, los mismos tendrían que estar posicionados en un sector que el acceso a esos datos cumplan con el propósito que necesitamos.

¿Sirve poner un firewall detrás de una red, lo dejamos configurado por defecto, o peor aún, a un servidor importante tiene acceso libre desde Internet de cualquier intruso?

De eso se trata la estructuración, de proteger los activos, la información confidencial, etc., de una manera eficiente y segura, teniendo en cuenta el posicionamiento de los dispositivos de seguridad o de los sistemas que tengamos para la protección.

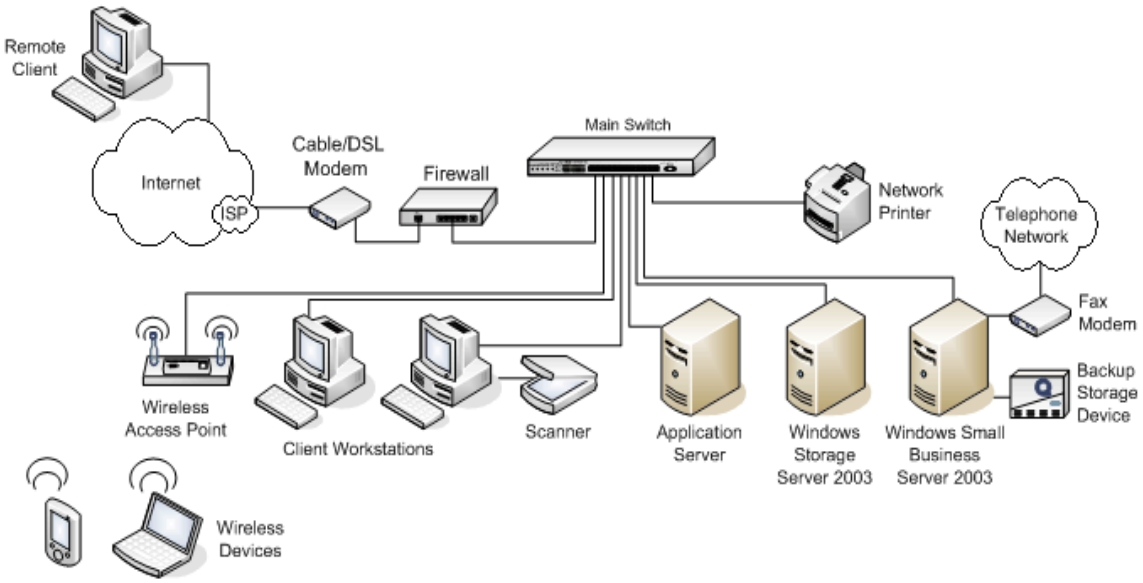
- Relevamiento de la red
- ¿Que proteger? ¿Qué activos?
- ¿En qué sector de la red están los mismos? ¿Podrían estar en otro lado?
- ¿Que dispongo para protegerlos?
- ¿Dónde los protejo o sea donde instaló el sistema de seguridad?
- ¿Está bien como lo deje? ¿Hay otras opciones? ¿En caso de que haya un acceso indebido, tengo una posibilidad de contingencia?

A veces puede resultar que uno se confunda por no saber cuál es la correcta ubicación de un dispositivo de seguridad o servicio, hay cientos de escenarios posibles, no hay un estándar para poder ubicarlos, entonces queda realizar estos puntos, comprenderlos y llevarlos a la práctica, de acuerdo al escenario que uno se encuentre.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Número 3 Unidad 4

De acuerdo a la metodología enseñada, poner en práctica los 6 puntos en este dibujo de red, Exponer en el foro.



Recomendaciones:

1- Realizar un relevamiento
2- Determinar (improvisando) qué dispositivos se consideran proteger
3- Chequear si se encuentran bien posicionados dentro de la topología
4- Aplicar más medidas de seguridad si hicieran falta
5- ¿En caso de que se caiga la red, tengo alguna medida de backup?

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Armado de una red segura

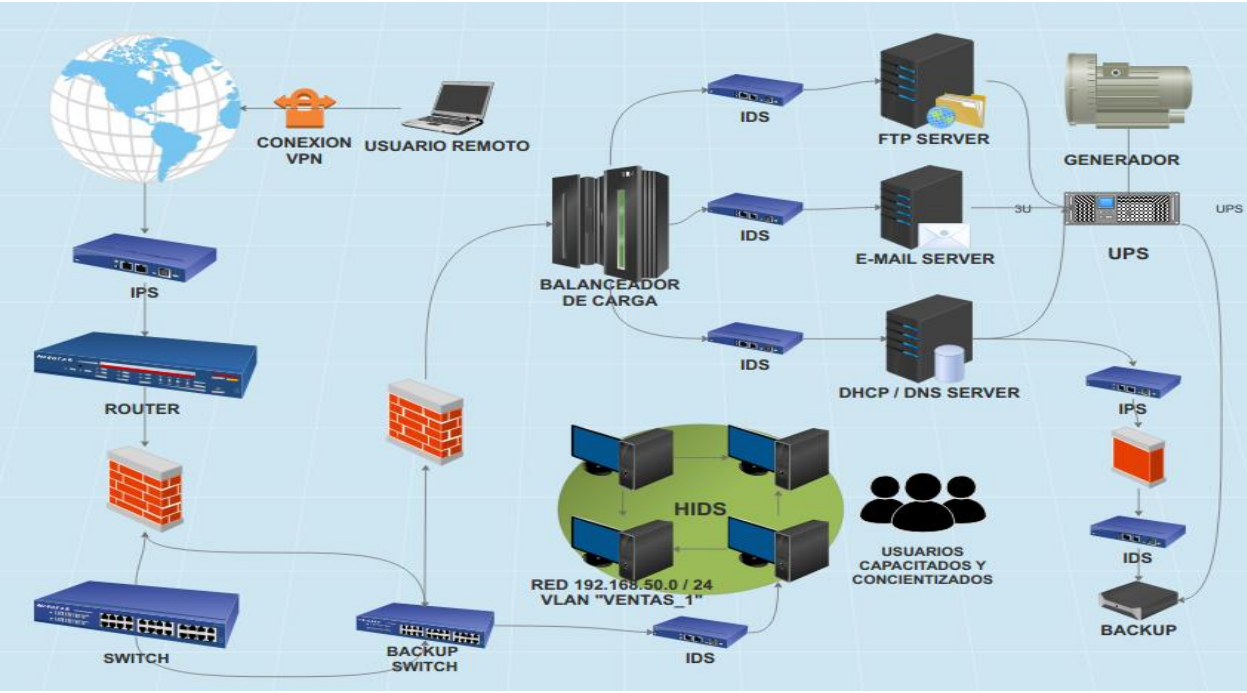
A lo largo de todo lo aprendido hasta ahora, hemos mencionado Dispositivos de seguridad (**Firewall**), servicios (**DMZ, NAT, ACL, etc.**).

¿La pregunta del millón es: cómo armar una red segura?

Implementando una metodología de protección y buen uso de todo lo relacionado llamado "seguridad".

Chequear todos los dispositivos, usar métodos de actualización de software, antivirus, control de acceso físicos, cámaras, etc.

¿Cómo llevarlo a la práctica? Lo realizarán ustedes a través del final que se encuentra a continuación, luego de algunos TIPS a tener en cuenta.



Uno podría considerar que mirando esta topología tiene muy buena seguridad, pero si lo miramos más detalladamente, se verán procesos que se reiteran, que se encuentran mal aplicados y utilizados, tener 10 FW no es la solución, al contrario se suman más puntos de fallas en un relevamiento de seguridad.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Dispositivos de Seguridad

Tipos de Firewall existentes a tener en cuenta

Filtrado de Paquetes

Proxy-Gateways de Aplicaciones

Dual-Homed Host

Screened Host

Screened Subnet

Inspección de Paquetes

Firewalls Personales

Sistemas de detección de intrusos (IDS)

Disponemos de:

•N-IDS : garantiza la seguridad dentro de una red

•H-IDS : garantiza la seguridad en un host

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Network IDS (N-IDS)

Nos ofrece una forma de sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal

•Hardware exclusivo

•Adaptadores de red en modo promiscuo

•Invisible

•No tienen IP

•Usualmente dos adaptadores

•Interno / Externo

Host IDS (H-IDS)

- **Analizan la información particular almacenada en registros**
- **Capturan paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión**
- **Chequea: Registros del sistema / Mensajes / Lastlogs / Wtmp**

Puede detectar:

- **Ataques por denegación de servicio**
- **Puertas traseras**
- **Troyanos**
- **Ejecución de códigos malignos**
- **Ataques de desbordamiento de búfer**
- **Intentos de acceso no autorizado**

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Ejercicio Final Módulo 1

Imaginen a la siguiente red:

Dos routers, cada uno conectado a un **ISP** (proveedor de servicio) distinto, y en nuestra red (**LAN**) hacia ellos a través de un switch de capa 3.

Contra ese switch de capa 3 hay 5 switches más conectados, también de capa 3, de los cuales en cada SW, están tomados todos los puertos con **PCs** (16) (razonemos de cuantos puertos serán los switches y cuántos puertos necesitamos para poder conectarlos entre sí).

No hay implementado ningún dispositivo de seguridad, ni ningún servicio, desarrollar la idea de poner y que agregar (sin límites), respetando únicamente la topología seleccionada, sumando a diagramar la topología de cómo lo armaron.

TIP: una red segura, no es solamente poner un firewall, sino también pensar en cada host.....

2 TIP: se respetara la idea de cada uno, eso significa que no hay una sola topología correcta.

3 TIP: si cada puerto está ocupado por una PC, obviamente tengo que tener algún puerto en el SW para poder conectarlos entre sí (ver o buscar fotos de switches y se darán cuenta de lo que escribí).

SON 16 PCs por cada SW, no hace falta dibujar todas las PCs, poner un identificador sirve.

4 TIP: de acuerdo a lo expuesto, se dará como devolución si la topología es la más adecuada, por ende, usen ejemplos expuestos en las unidades.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Dudas y/o Consultas sobre el final

- Los finales tienen que ser entregados en formato .DOC sin excepciones
- No tienen que superar los 10MB de tamaño de archivo
- Una vez lo terminan, lo suben al foro llamado Final de Módulo Número 1.
- En este caso, la fecha de entrega y finalización estará expuesta en este foro
- Las correcciones se harán de acuerdo a respetar la fecha de entrega, cuanto más se tarde en subir, más se tardará en evaluarlo, dado que hay que priorizar a los alumnos/as que entregan en fecha.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy IMPORTANTE que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learni the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU