MUM – Uruguay 2017
Firewall basado en Zonas

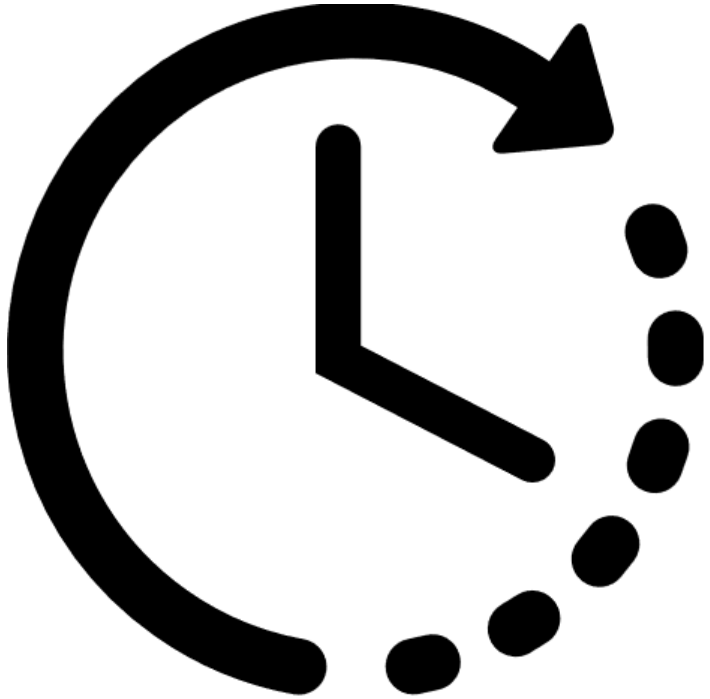
Por: Ing. José Miguel Cabrera
Ecatel SRL

Resumen

El firewall es una funcionalidad obligatoria de configurar para un buen desempeño de una red, sin embargo, con muchas interfaces y usuarios puede volverse una tarea complicada.

La funcionalidad “Interface List” de MikroTik te permite una mejor administración estableciendo zonas de acuerdo a la interfaz de ingreso.

Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de Firewall
- Estructura de Zonas
- Demostración

Acerca de la empresa

Es una empresa que se dedica a la **implementación de proyectos** integrando principalmente equipos de la marca Mikrotik, si es necesario combinados con otras marcas.

Brindamos ***capacitaciones*** **de MikroTik.**

Contáctenos

info@ecatel.com.bo

+591 776 25848

facebook.com/EcatelSRL

Acerca del disertante

- **Nombre:** Jose Miguel Cabrera Dalence
- **Nacionalidad:** Boliviano
- **Profesión:** Ing. en Redes y Telecomunicaciones (UTEPSA)
- **Posgrado:** Especialista en Educación Superior Tecnológica (UAGRM)

Experiencia Laboral:

- Jefe de Proyectos en Ecatel SRL (2015 a la fecha)
- Instructor Mikrotik (2015 a la fecha)
- Jefe Nacional de Telecomunicaciones Banco Fassil (2010-2015)
- Docente Universitario en Utepsa y UAGRM (2011-2016).

Acerca del disertante

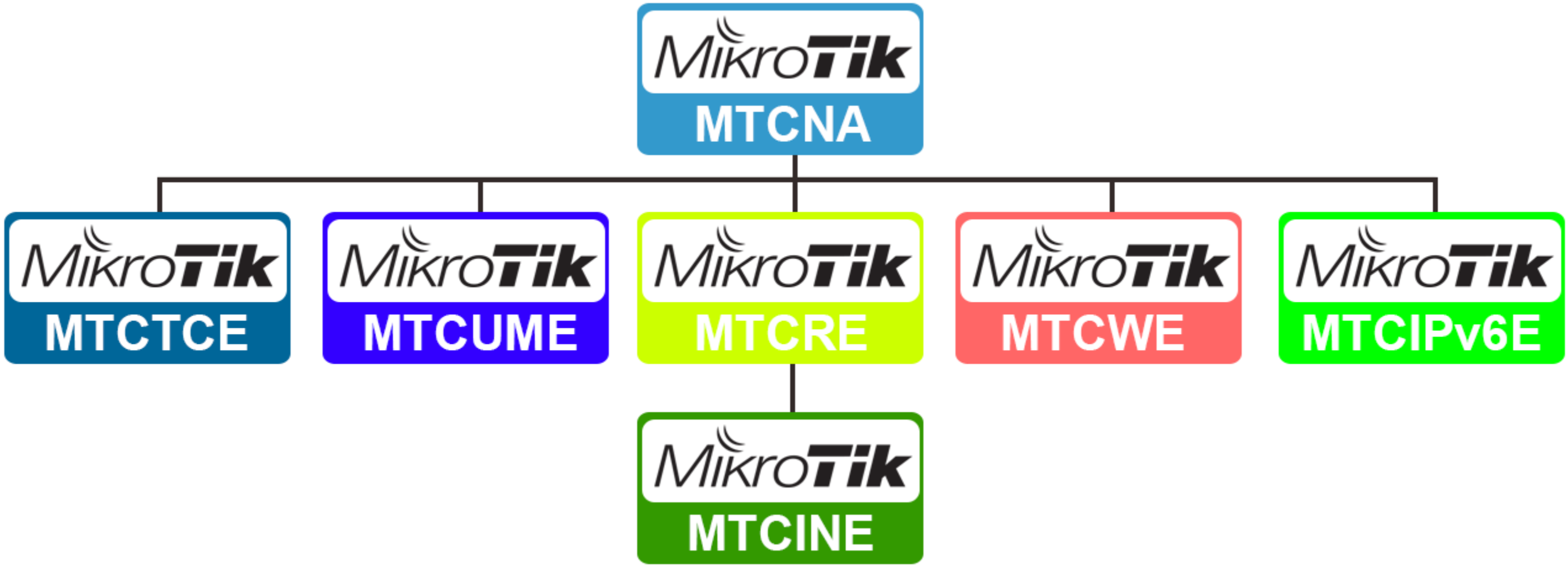
Certificaciones:

- **Mikrotik:** MTCNA, MTCWE, MTCRE, MTCINE, MTCUME, MTCTE, MTCIPv6E, Trainer
- **Cisco:** CCNP Security, CCNA R&S, CCNA Security

Conferencias y Capacitaciones:

- **Conferencista:** Argentina, Bolivia, Paraguay y Uruguay.
- **Se capacitó en:** Bolivia, Perú, Ecuador y Estados Unidos
- **Entrenador MikroTik:** Bolivia, Chile, Paraguay, Perú y Uruguay

Programa de Certificaciones



NST

NETSolutions

MikroTik TRAINING CENTER

Montevideo, Uruguay

MTCNA
Noviembre 2017

EcaTel SRL

MikroTik TRAINING CENTER

Montevideo, Uruguay

MTCTCE
Noviembre 2017

EcaTel SRL

NST

NETSolutions

NST-Group es una empresa dedicada al desarrollo de soluciones informáticas basadas en las mejores prácticas, metodología y administración del conocimiento, apuntando al mercado de pequeñas, medianas y grandes empresas.

http://nst.com.uy

Montevideo, Uruguay
PROXIMO CURSO: 2018

MTCNA

Lunes 12, Martes 13 y Miércoles 14 de Marzo

Desde las 09:00 am - 06:30pm

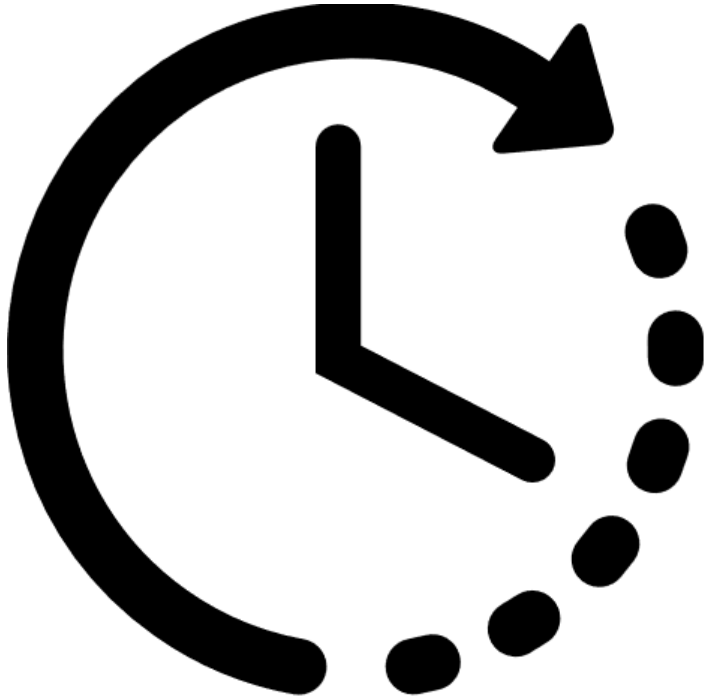
MikroTik TRAINING CENTER

MTCRE

Jueves 15 y Viernes 16 de Marzo

Desde las 09:00 am - 06:30pm

Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- **Conceptos de Firewall**
- Estructura de Zonas
- Demostración

Firewall

Es una funcionalidad de MikroTik diseñada para bloquear el acceso no autorizado, en la red LAN o hacia/desde Internet.

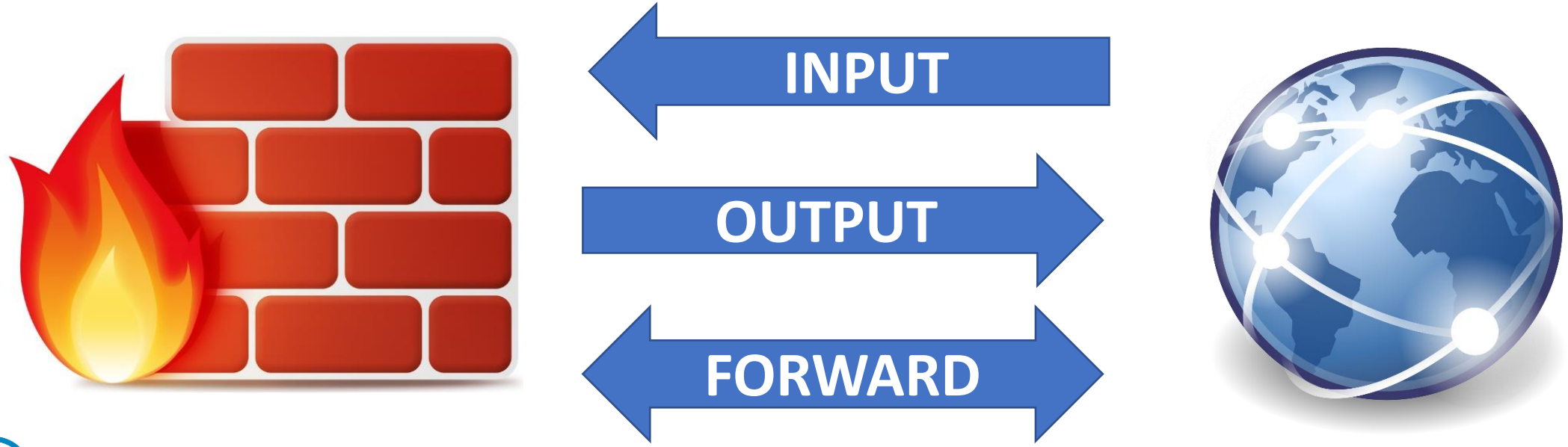
Evita que los usuarios no autorizados tengan acceso a la red privada.

¿COMO CREAR UNA REGLA DE FIREWALL?

1. SELECCIONAR “CHAIN”
2. CREA LA(S) CONDICION(ES)
3. ESCOGE LA “ACTION”

CHAIN

Es la forma como se agrupan las conexiones. Existen 3 cadenas (chain) predeterminadas:

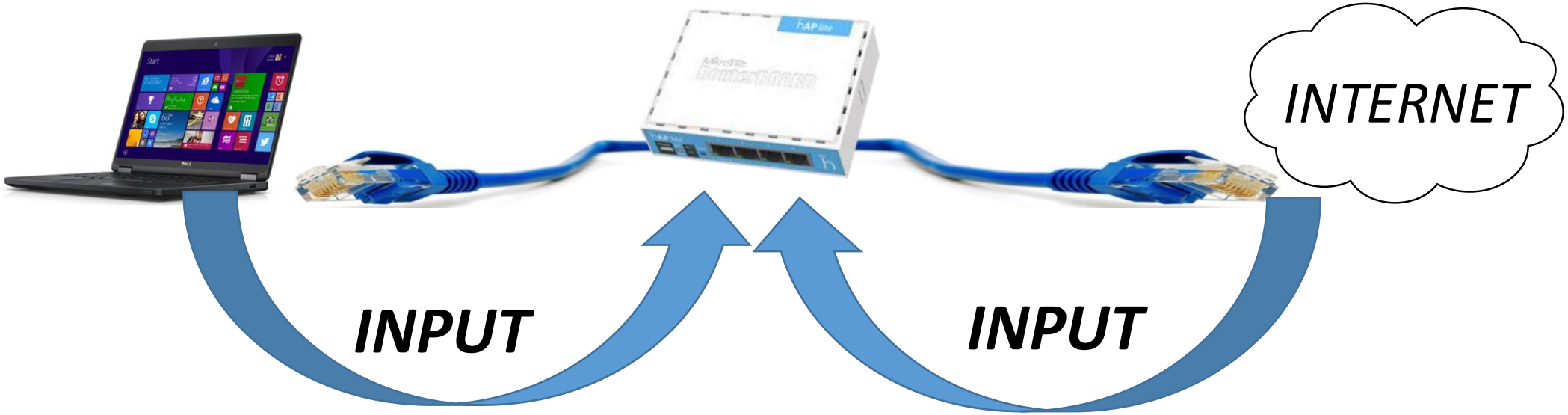


INPUT

Agrupas las conexiones donde:

- La IP de Destino es una Ip configurada en el router. No importa en qué interfaz
- **Protege** al router (de ataques DDoS, **Fuerza bruta**, accesos no autorizados, etc.)

CHAIN INPUT

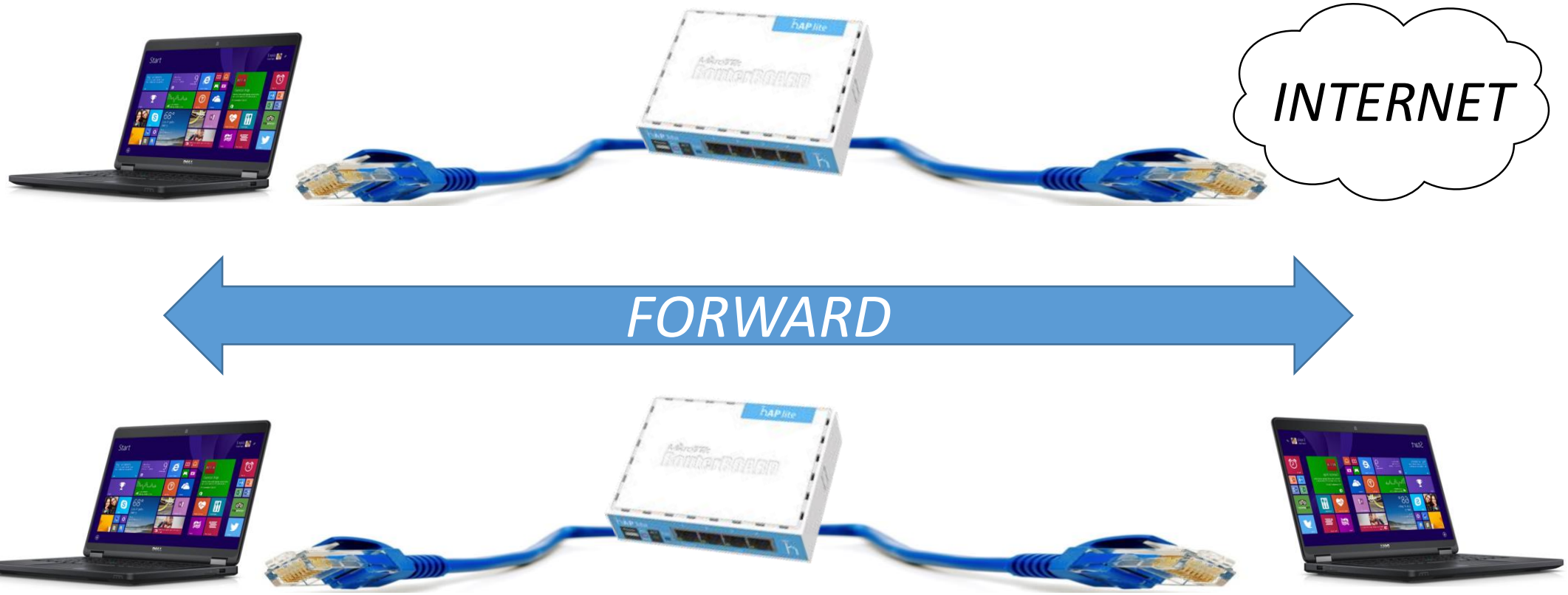


FORWARD

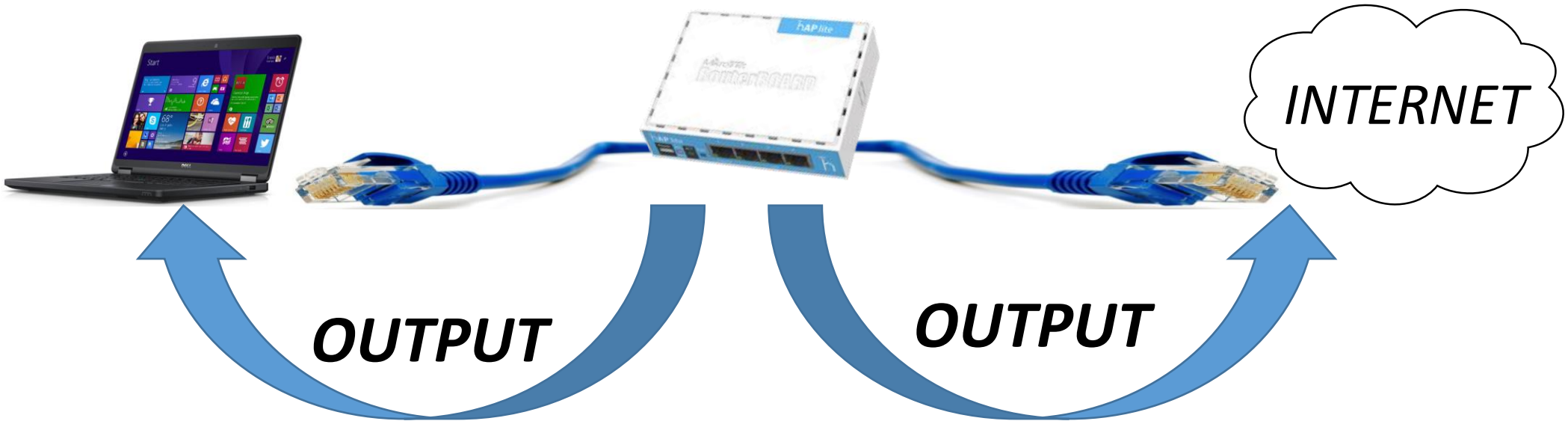
Agrupas las conexiones donde:

- El router solo actúa como “cartero”
- Utilizado para filtrar paquetes que **pasan a través** del router
- **Protege** o restringe **a los usuarios de la red**

CHAIN FORWARD



CHAIN OUTPUT



CONDICION

Conjunto de criterios configurados por el Administrador del firewall,

cuyo cumplimiento ocasiona una acción (action).

Condición:
Si robas

ACCION

Acción:
Vas a la carcel

CONDICION

El firewall puede leer las cabeceras del paquete IP para buscar el criterio (condición):

- Dirección IP de Origen / Destino
- Protocolo
- Puerto
- Muchos más criterios

SERVICIO	PUERTO
HTTP	80
SMTP	25
POP3	110
IMAP	143
HTTPS	443
TELNET	23
FTP	21
SSH	22
DNS	53

ACTION

Es la acción que tomará el RouterOS con el paquete que cumpla los criterios configurados

Las más populares son:

- **Accept:** El paquete sale del firewall. Pasa
- **Drop:** El paquete es descartado.

REPASANDO

En un concierto existe seguridad al ingreso:

- Controlan que tengas un ticket
- Si lo tienes, pasas.
- De lo contrario, no puedes entrar.

¡Eso hace el Firewall...!!!

Estado de la Conexión
(connection-state)

¿Qué pasa si estas en el concierto, quieres salir y volver a entrar?

Estado de la Conexión

(connection-state)

1. Llegaste al ingreso del concierto. El guardia no te conoce, muestras tu ticket y te deja ingresar (**Conexión Nueva**)
2. Quieres salir un momento, te sellan el brazo. Cuando quieres volver a ingresar SI tienes SELLO, pasas (**Conexión Establecida**)

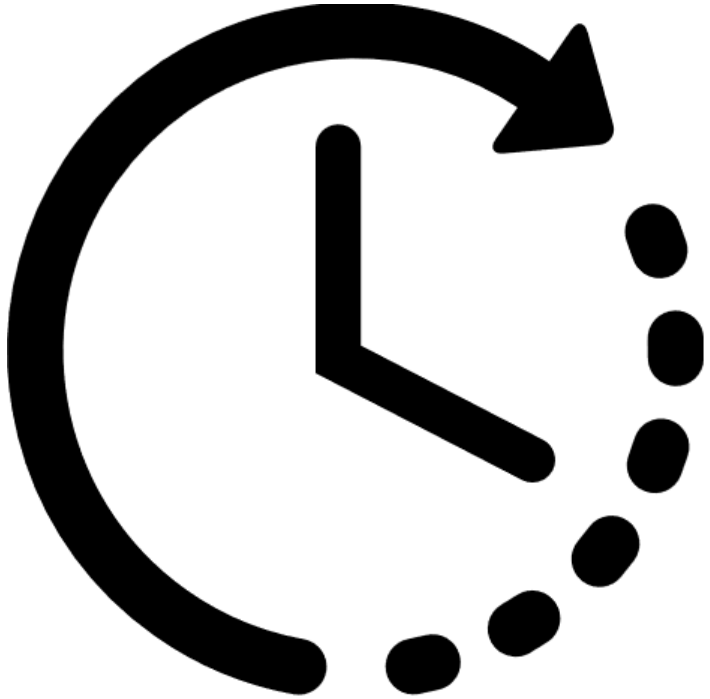
Estado de la Conexión
(connection-state)

3. Llega “el jefe” con una persona y dice “él viene conmigo” por más que no tenga ticket, lo dejan ingresar (**Conexión Relacionada**)

Estado de la Conexión
(connection-state)

- **New:** El primer paquete de una conexión.
- **Established:** un paquete que pertenece a una conexión existente
- **Related:** un paquete que está relacionado con uno establecido, como los errores ICMP o un paquete que inicia la conexión de datos FTP

Scheduler



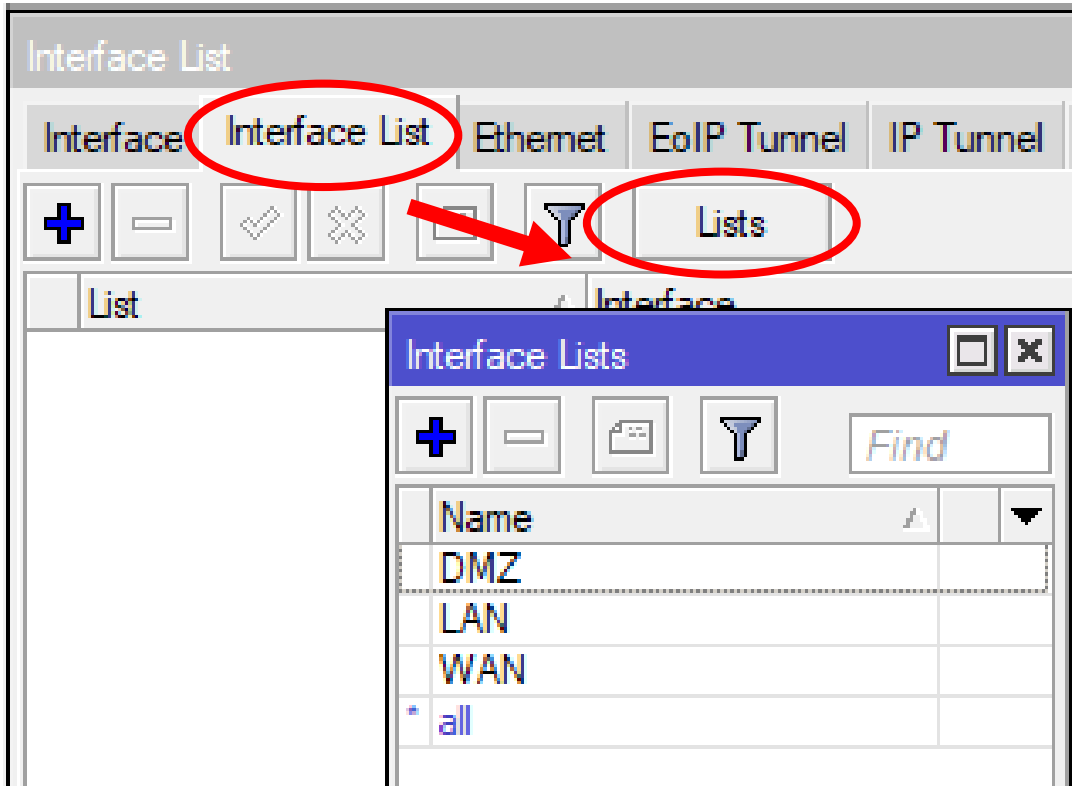
- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de Firewall
- **Estructura de Zonas**
- Demostración

Zonas de Firewall

Muchos fabricantes de Firewall utilizan zonas de seguridad, que es agrupar las interfaces.

- ***Zona Interna (inside):*** *Interfaces de* LAN
- ***Zona Externa (outside):*** La interfaz de WAN
- ***Zona DMZ:*** Interfaz donde se conectan servidores que deben estar disponibles desde Internet.

Interface List



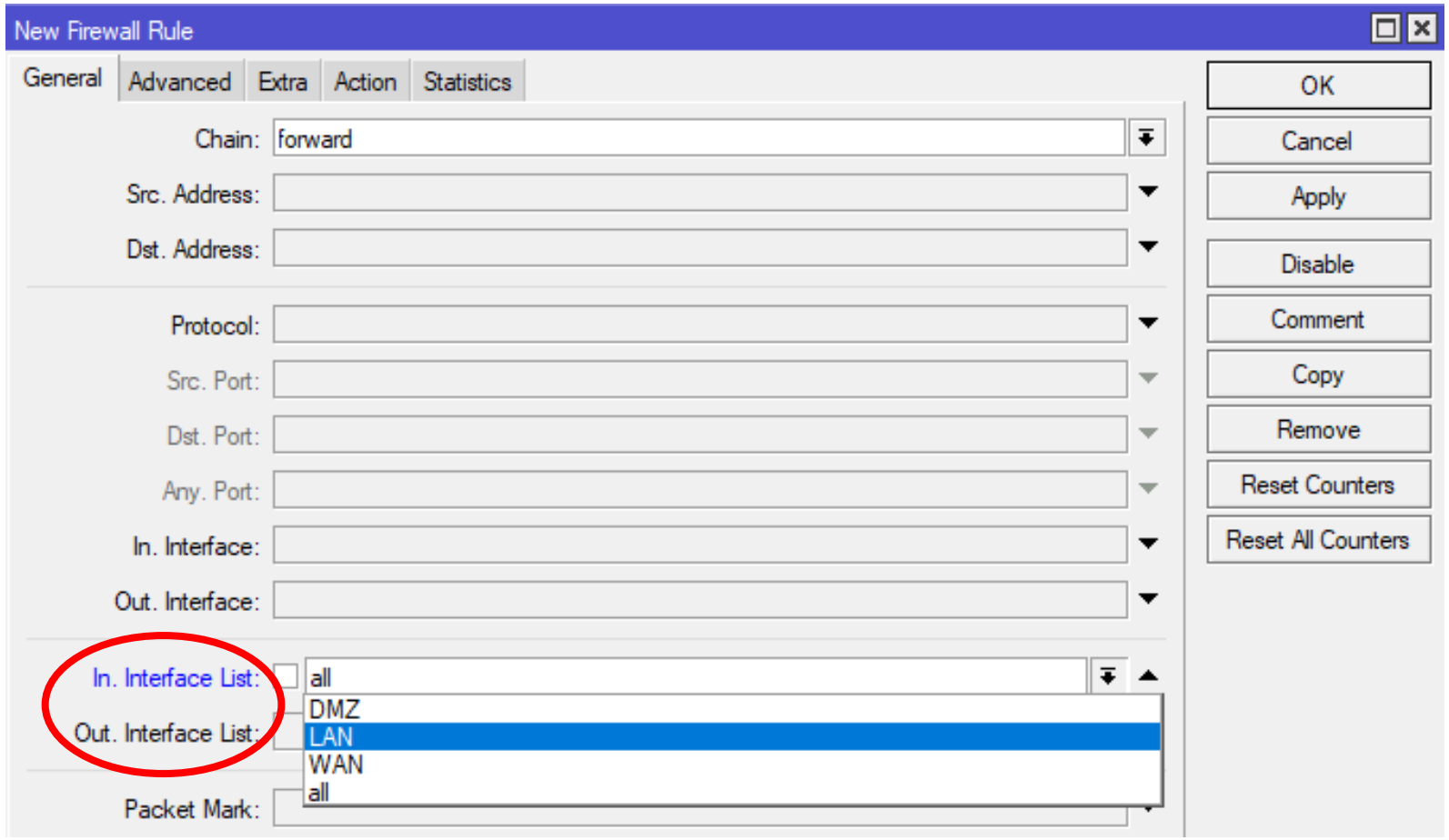
Esta opción de MikroTik permite definir un conjunto de interfaces para una administración más sencilla en el firewall.

Con esto podemos crear nuestras zonas de seguridad

Interface List

Luego puedes usar estas listas en tu regla de firewall

Puedes usarla en el sentido "In" como "Out"



Interface List

Los nombres y el uso puedes definirlos de acuerdo a tu conveniencia. Por ejemplo: Usar una lista para la telefonía IP, otro para Cámaras IP.

Es el momento de ponerse creativo.

Ejemplo Firewall

Observemos este esquema. Se desea implementar reglas de firewall.

Requerimientos

1. Solo se permite conexiones entrantes hacia Winbox por internet
2. No se desea trafico intervlan
3. Desde Oficina Central pueden acceder libremente
4. Pueden navegar en Internet sin restricción
5. La última regla debe ser un drop a todo.

Paso 1

Vamos a crear 3 Listas de interfaces (zonas)

- ✓ LAN: Donde agruparemos las interfaces vlan
- ✓ Internet: La interfaz donde conecto el internet
- ✓ WAN: Donde conecto el enlace privado hacia la oficina central

Paso 1

Ejecutamos estos comandos en “New Terminal”

```
/interface list
    add name=WAN
    add name=Internet
    add name=LAN
```

Paso 2

Añadimos las interfaces a las listas:

```
/interface list member
    add interface=ether1 list=Internet
    add interface=ether2 list=WAN
    add interface=vlan30 list=LAN
    add interface=vlan31 list=LAN
    add interface=vlan32 list=LAN
```

Paso 3

"Solo se permite conexiones entrantes hacia Winbox por internet"

```
/ip firewall filter
  add action=accept chain=input \
    in-interface-list=Internet\
    protocol=tcp dst-port=8291
  add action=accept chain=input \
    in-interface-list=Internet\
    connection-state=established,related
  add action=drop chain=input \
    in-interface-list=Internet
```

Paso 4

"No se desea trafico intervlan"

```
/ip firewall filter
  add action=drop chain=forward \
    in-interface-list=LAN \
    out-interface-list=LAN
```

Nota: El caracter \ debe escribirse o puede omitirse si se escribe todo el comando en una sola linea

Paso 5

“Desde Oficina Central pueden acceder libremente”

```
/ip firewall filter
  add action=accept chain=forward \
    in-interface-list=WAN
  add action=accept chain=forward \
    connection-state=established,related
```

Paso 6

“Pueden navegar en Internet sin restricción”

```
/ip firewall filter
  add action=accept chain=forward \
    in-interface-list=LAN \
    out-interface-list=Internet
```

Paso 7

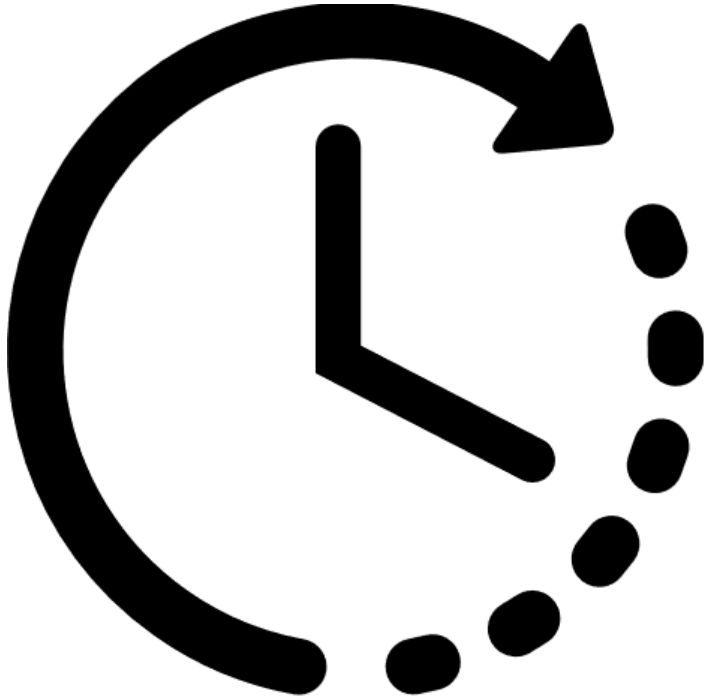
"La última regla debe ser un drop a todo."

```
/ip firewall filter
  add action=drop chain=forward
```

Conclusion

Se cumplieron todos los requerimientos planteados, por supuesto que puede añadirse nuevos permisos de acuerdo a los requerimientos de cada red.

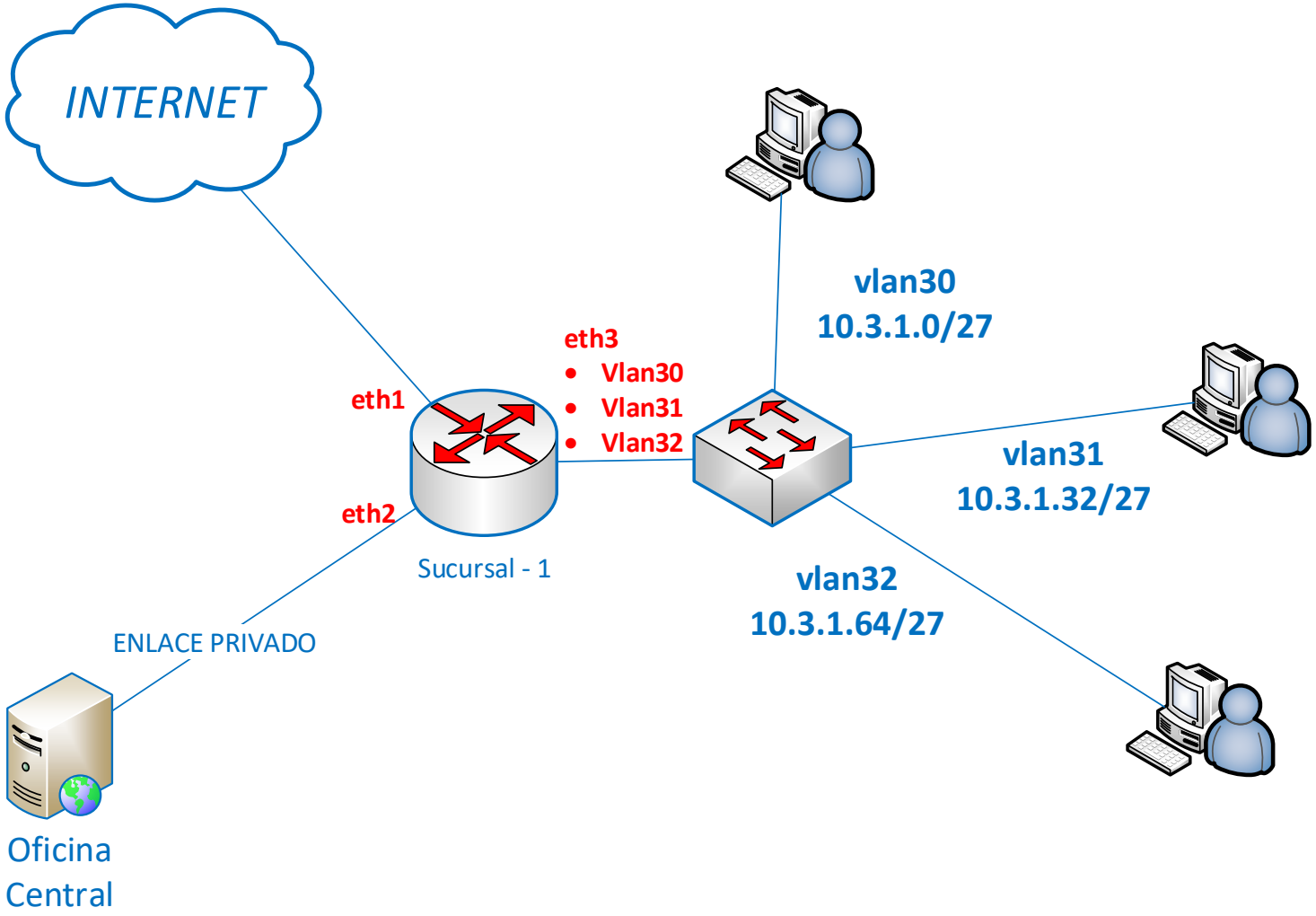
Scheduler



- Presentación de la empresa
- Presentación del expositor
- Oferta de Cursos de Certificación
- Conceptos de Firewall
- Estructura de Zonas
- **Demostración**


¡SHOW TIME!
DEMOSTRACION
EcaTel SRL

Ejemplo Firewall



NETSolutions

FlashStart INTERNET PROTECTION

FlashStart es una tecnología de filtrado de Internet y mitigación de malware basada en la nube para pequeñas y medianas empresas, instituciones educativas, Gobierno y cualquier otra persona. FlashStart **no requiere hardware o software adicional** y se integra fácilmente con dispositivos de acceso de terceros. En tan sólo 5 minutos, FlashStart puede ser conectado, ofreciendo filtrado y monitoreo fiable y sin complicaciones.

http://www.netsolutions.com.uy

EcaTel SRL

¡Gracias!