Guía 9 – Configuración de una DMZ

Contenido de la guía

Objetivo general de la guía.

- Crear una red DMZ en el escenario de la EMPRESAY, que presente servicios a clientes externos y anónimos de la EMPRESAY de forma que los servicios internos no sean expuestos.

Objetivos específicos.

- Configurar una DMZ
- Configurar un servidor DNS externo para la resolución de los servicios públicos.
- Configurar el servidor DNS interno para utilizar como reenviador al servidor DNS externo.
- Crear reglas para NAT
- Comprobar la redirección de servicios públicos.

Nomenclatura de la guía:

En esta guía se ha utilizado el siguiente formato:

- Fuente courrier en negrita para los comandos que deben digitarse, por ejemplo:
  `root@front-end:~# ps aux |grep sshd`
- Texto con resaltado en amarillo, para la información que debe visualizar cuando realice algún procedimiento o comando. Puede contener color rojo dentro del fondo amarillo.

```
root@front-end:~# mcedit /etc/resolv.conf
search empresay.com.sv
nameserver   192.168.60.2
```

- Las notas o consideraciones se destacan con: **Nota:**

I. Indicaciones sobre la guía

1.1 Descripción del escenario global.

Usted y su equipo de trabajo han sido contratados para configurar una red DMZ que contiene los servicios de un DNS externo y un servidor HTTP a usuarios externos y anónimos de la EMPRESAY, manteniendo la seguridad de los servicios internos de la empresa. Es decir, mantener la configuración del Firewall que se ha utilizado en los escenarios anteriores.

- El servidor DNS deberá resolver solo las peticiones externas (desde Internet), acordes a los ítems 6 y 7 del cuadro 3, el servidor DNS externo se convertirá en el único reenviador del servidor DNS interno.
- El servidor HTTP deberá tener una página en HTML o PHP que muestre un mensaje diferente del HTTP del servidor02
- Los usuarios públicos pueden acceder al sitio web tanto desde equipos de escritorio como dispositivos móviles (usar Android)

Para realizar el desafío se debe:

- Instalar el servidor BIND 9.X en uno de los equipos Core Plus, (está en la libertad de instalar BIND en otra distribución de Linux, si los recursos de hardware le permiten hacer esto).
- Utilizar MaSSHandra para la administración remota de los servidores.
- Analizar la configuración de la sección 1.2 que más se les facilite para desarrollar el escenario.
- Puede utilizar cualquier sistema operativo para ejecutar la conexión de los clientes públicos (pub01 y pub02)
- Comenzar a trabajar con el uso de una página en PHP que consulte cualquier tabla en la base de datos der servidor02, esto será requerido en la evaluación práctica grupal

En la siguiente figura se ilustra el escenario de red para la guía

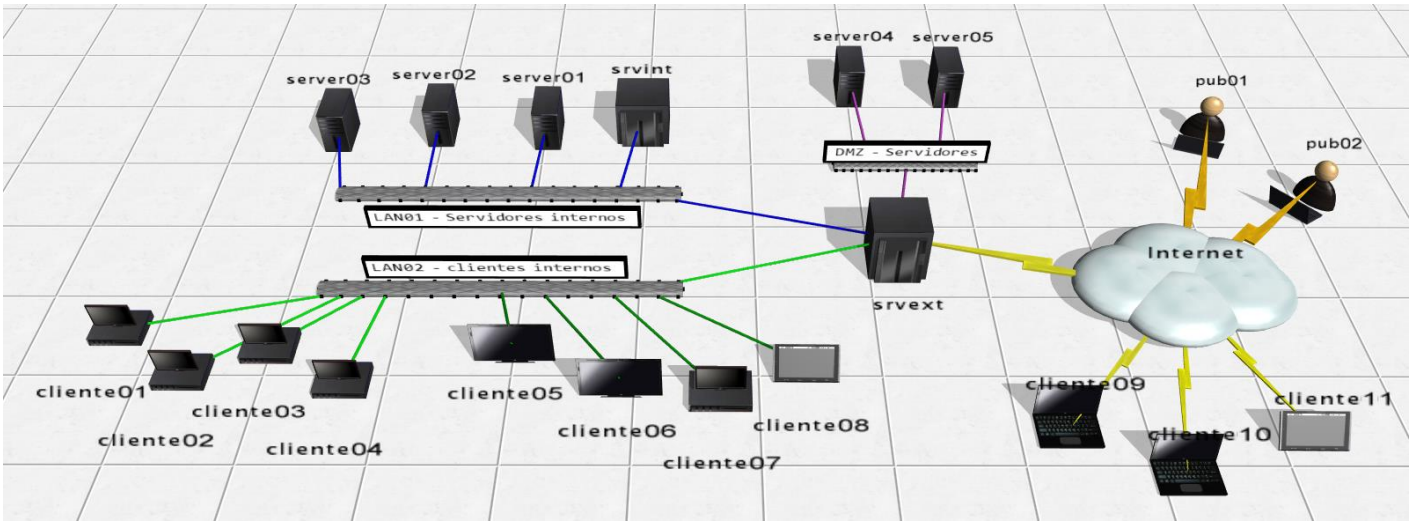


Figura 1 – Diagrama del escenario de la nube privada y pública de la EMPRESAY.

Servicios y clientes en los equipos a utilizar			
ID	**Nombre Equipo**	**Servicios / Software**	**S.O.**
1	srvext	DHCP, Router, Firewall, NAT, VPN	**Zentyal 4.X**
2	servint	DNS, AD, FS	**Zentyal 4.X**
3	servidor01	Servidor SSH, Servidor Web	CorePlus 7.X
4	servidor02	Servidor SSH, Servidor VNC,	CorePlus 7.X
5	servidor03	Servidor SSH, Servidos SMB, Servidor MySQL	CorePlus 7.X
6	cliente01	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
7	cliente02	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
8	cliente03	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
9	cliente04	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	CorePlus 7.X
10	cliente05	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 8, 10
11	cliente06	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 8, 10
12	cliente07	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Ubuntu 14.04
13	cliente08	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Android x86
14	cliente09	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Windows 7, 10
15	cliente10	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Ubuntu 14.04
14	cliente11	Clientes: SSH, SCP, VNC, Web, MySQL, SMB	Android x86

Cuadro 1 – Descripción de los equipos del escenario de la EMPRESAY

La red IPv4 de la EMPRESAY para cada equipo se detalla en el siguiente cuadro:

Direcciones MAC e IPv4 para los equipos de la EMPRESAY				
ID	**Equipo**	**Dirección MAC**	**Tipo IPv4**	**IPv4**
1	serext	02:AA:E0:Y:X:01	Dinámica	La del ISP
		02:AA:E1:Y:X:02	Estática	192.168.**60+Y**.1
		02:AA:E2:Y:X:03	Estática	192.168.**50**+Y.1
2	srvint	02:BB:00:Y:X:00	Estática	192.168.**60**+Y.2
3	servidor01	02:BB:00:Y:X:01	Reservada	192.168. **60+Y**.11
4	servidor02	02:BB:00:Y:X:02	Reservada	192.168. **60+Y**.12
5	servidor03	02:BB:00:Y:X:03	Reservada	192.168. **60+Y**.13
6	cliente01	02:CC:00:Y:X:01	Reservada	192.168.**50**+Y.11
7	cliente02	02:CC:00:Y:X:02	Dinámica	192.168.**50**+Y.12
8	cliente03	02:CC:00:Y:X:03	Dinámica	192.168.**50**+Y.13
9	cliente04	02:CC:00:Y:X:04	Dinámica	192.168.**50**+Y.14
10	cliente05	02:CC:00:Y:X:05	Dinámica	192.168.**50**+Y.15
11	cliente06	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.16
12	cliente07	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.17

Cuadro 2 – Datos generales de red para el escenario de la EMPRESAY según equipo de trabajo

Nota: Para garantizar que no exista una dirección MAC, una IPv4, un host y un dominio duplicado en la red del laboratorio, se utilizará la siguiente nomenclatura:

- Y = representa el número del grupo de trabajo, y se utilizan dos dígitos
- X = representa el número del estudiante, se utilizan dos dígitos

Ejemplos:	**Grupo 7 y estudiante 1**	**Grupo 05 y estudiante 2**	**Grupo 11 y estudiante 3**
02:BB:00:**Y**:**X**:01	02:BB:00:**07**:**01**:01	02:BB:00:**05**:**02**:01	02:BB:00:**11**:**03**:01
empresa**Y**.com.sv	empresa**07**.com.sv	empresa**05**.com.sv	empresa**11**.com.sv
192.168.**50+Y**.3	192.168.5**7**.3	192.168.5**5**.3	192.168.**61**.3

Nota: Imprima o elabore en una hoja con los datos de grupo y número de alumno, de forma que no halla consultas redundantes, pérdida de tiempo o errores ocasionados por la mala configuración de la red en el laboratorio.

Servicios y clientes en los equipos a utilizar				
ID	**Equipo / Nombre de host**	**Dirección IPv4**	**Alias**	**FQDN**
1	srvext	192.168.50+Y.1 192.168.60+Y.1 192.168.70+Y.1	router01	srvext.empresay.com.sv
2	servint	192.168.**60+Y**.2	fs01	servint.empresay.com.sv
3	servidor01	192.168. **60+Y**.11	www	servidor01.empresay.com.sv
4	servidor02	192.168. **60+Y**.12	bd01	servidor02.empresay.com.sv
5	servidor03	192.168. **60+Y**.13	fs02	servidor03.empresay.com.sv
6	servidor04	192.168. **70+Y**.14	---	servidor04.empresay.com.sv
7	servidor05	192.168. **70+Y**.15	www mail smtp	servidor05.empresay.com.sv

Cuadro 3 – Datos de resolución para equipos

1.2 Consideraciones técnicas para el laboratorio.

Recursos requeridos:

- Un equipo o MV con servidor **srvext**.
- Un equipo o MV con servidor **srvint**.
- Tres servidores TinyCore 7.X o superior (con servicio HTTP de preferencia)
- Cuatro clientes TinyCore 7.X o superior con aplicaciones cliente que estarán en la nube (simulando Internet)
- Conexión a Internet.
- Los servicios DHCP y DNS deberán estar bien configurados, proveyendo todos los datos de la red de la empresa EMPRESAY (sustituir Y por el número de grupo)
- El servidor **srvext** deberá tener salida a Internet.
- MaSSHandra para Windows
- WinSCP o FileZilla para Windows.
- Notepad+++ para Windows (opcional)

Consideraciones:

- Si utiliza máquinas virtuales se utilizará VirtualBox versión 5.X (De preferencia), y para cada equipo se utilizarán las direcciones físicas del cuadro 2.
- Escriba en un papel todas las direcciones IPv4 de su red, utilice el valor de Y con el número de grupo asignado, por ejemplo: Y=grupo01 192.168.50+**Y**.1 = 192.168.168.51.1 (ver cuadro 2)
- La máquina virtual del servidor01 se puede clonar las veces que sea necesario para obtener los servidores de la red LAN01, los clientes de la red LAN02 y equipos de la DMZ
- Utilice un fondo de escritorio con el nombre de cada servidor y cliente para identificar mejor cada equipo.
- Verifique que utiliza la dirección MAC para cada grupo y alumno.
- El equipo **srvext** tendrá tres interfaces y Puede configurarse de la siguiente manera:

Configuración 01 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge a la tarjeta Ethernet de la computadora
Adaptador 2	eth1	Bridge a una loopback de MS o Ethernet
Adaptador 3	eth2	Bridge a una loopback de MS o Ethernet
Adaptador 4	eth3	Bridge a una loopback de MS o Ethernet
• Este escenario es útil si, se desean repartir las servidores y clientes virtuales entre dos o más computadoras del laboratorio. • Si es Windows donde está VirtualBox, se debe crear una loopback para micrososoft: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test • Si es Linux donde está VirtualBox, se debe crear una loopback tipo tap0 • Solo los Adaptadores con bridge a tarjetas Ethernet pueden comunicarse con otros equipos virtuales que se ejecutan en otra computadora del centro de cómputo. • Siempre se debe configurar la dirección IPv4 de la interfaz eth0 de srvext y el GW por default.		

Configuración 02 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	NAT
Adaptador 2	eth1	Bridge a una loopback de Micrososft
Adaptador 3	eth2	Bridge a una loopback de Micrososft
Adaptador 4	eth3	Bridge a una loopback de Micrososft
• Este escenario es útil si hay una configuración de portal cautivo en la red Wifi, o si la comunicación es complicada de realizar • En Windows: se debe crear una loopback: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test • En Linux: Se debe crear una loopback tipo tap0 • No es necesario configurar la dirección eth0 del servidor srvext (siempre será dinámica con el valor 10.0.2.15)		

Configuración 03 para las NIC de srvext con VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge o NAT
Adaptador 2	eth1	Conexión a LAN interna (lan01)
Adaptador 3	eth2	Conexión a LAN interna (lan02)
Adaptador 4	eth3	Conexión a LAN interna (lan03)
• Este escenario es útil si se utiliza una laptop o computadora de escritorio que necesite permisos para instalar dispositivos. • No necesita crear interfaces loopback, por lo que hacer pruebas de comunicación es muy complejo		

Nota: Si se utilizan el escenario 01 o el escenario 02 se debe crear una interfaz loopback con las direcciones para la red LAN01 y LAN02

Por ejemplo:

```
C:\Users\cuchillac>ipconfig
Configuración IP de Windows
Adaptador de LAN inalámbrica Wi-Fi:
   Sufijo DNS específico para la conexión. . : uni.edu.sv
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.3.223
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.10.3.254
Adaptador de Ethernet loopback:
   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.50.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.60.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.70.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

1.3 Teoría técnica requerida

Pendiente de finalizar

Para impedir que las personas externas a la compañía puedan obtener información de la red interna, utilice servidores DNS independientes para la resolución de nombres internos y de Internet. Su espacio de nombres DNS interno debe estar alojado en los servidores DNS detrás del servidor de seguridad de su red. Su presencia DNS externa en Internet debe administrarla un servidor DNS en una red perimetral (conocida también como DMZ, zona desmilitarizada o subred apantallada). Para proporcionar la resolución de nombres de Internet en hosts internos, puede hacer que sus servidores DNS internos utilicen un servidor de envío para enviar las consultas externas a su servidor DNS externo. Párrafo tomado de: https://msdn.microsoft.com/es-es/library/cc780338(v=ws.10).aspx

Si el servidor que ejecuta el servicio del Servidor DNS es un equipo de hosts múltiples, limite el servicio del Servidor DNS sólo para escuchar en la dirección IP de interfaz utilizada por sus clientes DNS y servidores internos. Por ejemplo, un servidor que actúa como servidor proxy puede tener dos tarjetas de interfaz de red, una para la intranet y otra para Internet. Si dicho servidor ejecuta también el servicio del Servidor DNS, puede configurar el servicio para que sólo escuche el tráfico DNS en la dirección IP utilizada por la tarjeta de interfaz de red de la intranet

Si el servidor que ejecuta el servicio del Servidor DNS es un controlador de dominio, utilice listas de control de acceso (ACL) de Active Directory para proteger el control de acceso del servicio del Servidor DNS.

Su infraestructura debe disponer de al menos tres DNS, los cuales se recomienda que estén replicados para alta disponibilidad (es decir, seis servidores DNS):

- El primer DNS es el encargado de responder a las peticiones externas que pregunten sobre un dominio de nuestra infraestructura y por tanto es el encargado de resolver las IP públicas de nuestra red. Éste debe estar en una zona dedicada y propia de la infraestructura, y dicho DNS no debe permitir peticiones recursivas y por supuesto peticiones desde nuestra infraestructura.
- El segundo DNS se encontrará en la red perimetral o DMZ. Contiene las IP privadas de los servidores de DMZ y a su vez será el encargado de consultar a los DNS externos de la infraestructura si recibe peticiones, si y solo si, de activos pertenecientes a la red perimetral o del DNS interno.
- El tercer DNS será el interno, que responderá única y exclusivamente a peticiones de los activos de la red interna y en caso de no disponer de la respuesta, siempre deberá preguntar al DNS de la red perimetral de la infraestructura y jamás, repito, JAMÁS, a un DNS externo de Internet.

Cuando se utiliza DNS externo:
Configuración de DNS para correo entrante
DNS desempeña un papel fundamental en la entrega de correo de Internet. Para recibir correo de Internet, se necesita la configuración siguiente:

- Debe existir un registro de intercambio de correo (MX) para su servidor de correo en el servidor DNS externo. Puede emplear la herramienta Nslookup para determinar si los registros MX están configurados correctamente. Asegúrese de que los servidores de correo que utiliza como servidores cabeza de puente o como servidores de correo de Internet tienen un registro MX en los servidores DNS externos.
- Para que los servidores DNS externos resuelvan el registro MX de su servidor de correo y se pongan en contacto con él, éste debe ser accesible desde Internet. Puede utilizar el programa telnet para determinar si otros servidores pueden tener acceso a su servidor de correo.
- Exchange Server debe estar configurado para ponerse en contacto con un servidor DNS o para resolver nombres DNS externos.
- El servidor DNS debe estar configurado correctamente.

Tomado de: https://technet.microsoft.com/es-es/library/aa996996(v=exchg.65).aspx

Ejemplos de protección de los datos de la empresa
http://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzakk/rzakkscenario5.htm

Tomado de: http://www.securityartwork.es/2011/06/30/¡no-quiero-a-mi-dns/
Se puede ver como se puede para la infección de malware por el uso de DNS (Sinkhole,) http://www.securityartwork.es/2011/06/30/¡no-quiero-a-mi-dns/, manual de Sinkhole https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

Información de bind en Español (http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns_bind9.html)

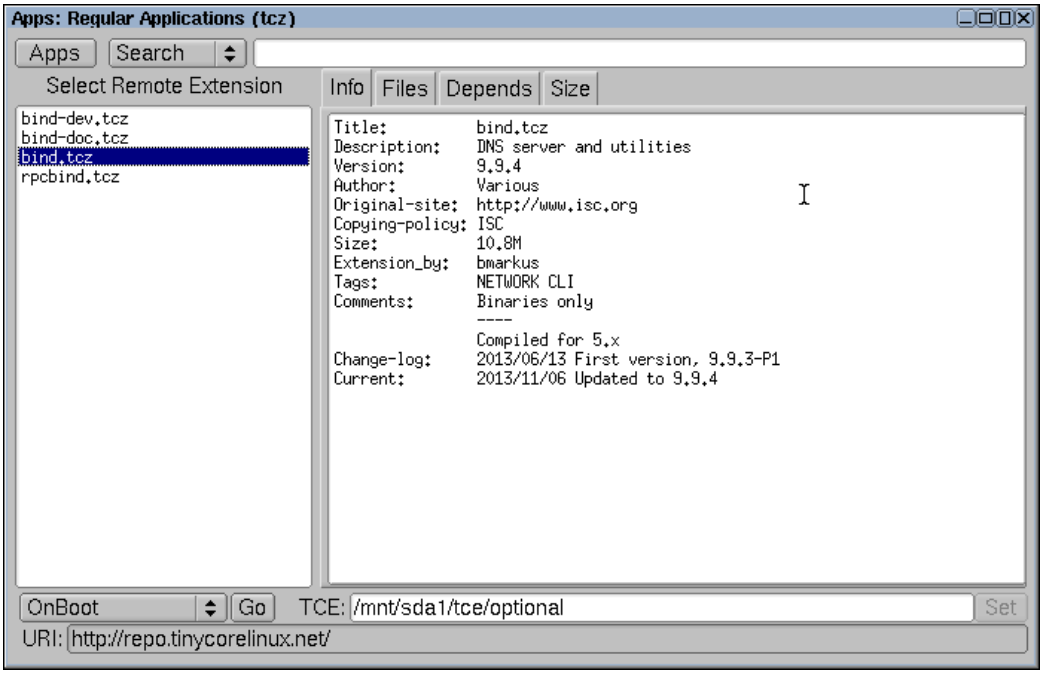
II. Desarrollo de la guía.

2.1 Instalación y configuración de los servicios en la DMZ

Paso 1 Instalar el servicio DNS.

1.1 Abrir el administrador de APP

1.2 digitar bind



1.3 Seleccionar OnBoot

1.4 Instalar bind.tcz y bind-doc.tcz

Otra forma de instalar por consola

```
tc@servidor03:~$ tce-load -wi bind
bind.tcz          100% |***********************************|   128k  0:00:00 ETA
bind.tcz: OK

tc@servidor03:~$ tce-load -wi bind-doc.tcz
Downloading: bind-doc.tcz
Connecting to repo.tinycorelinux.net (89.22.99.37:80)
bind-doc.tcz          100% |*******************************|   128k  0:00:00 ETA
bind-doc.tcz: OK
```

Paso 2. Verifique que se han instalado los archivos

Digite los siguientes comandos

```
tc@servidor03:~$ ll /tmp/tcloop/bind/usr/local/
total 0
drwxr-xr-x    2 root     root            91 Nov  6  2013 bin/
drwxr-xr-x    2 root     root            32 Nov  6  2013 etc/
drwxr-xr-x    2 root     root             3 Nov  6  2013 lib/
drwxr-xr-x    2 root     root           491 Nov  6  2013 sbin/
drwxr-xr-x    2 root     root             3 Nov  6  2013 share/
drwxr-xr-x    3 root     root            26 Nov  6  2013 var/

tc@servidor03:~$ ll /tmp/tcloop/bind/usr/local/bin/
total 5141
-rwxr-xr-x    1 root     root       1328972 Nov  6  2013 dig
-rwxr-xr-x    1 root     root       1319284 Nov  6  2013 host
-rwxr-xr-x    1 root     root          3216 Nov  6  2013 isc-config.sh
-rwxr-xr-x    1 root     root       1318644 Nov  6  2013 nslookup
-rwxr-xr-x    1 root     root       1292944 Nov  6  2013 nsupdate

tc@servidor03:~$ ll /tmp/tcloop/bind/usr/local/sbin/
total 16879
-rwxr-xr-x    1 root     root          3840 Nov  6  2013 arpaname
-rwxr-xr-x    1 root     root        368032 Nov  6  2013 ddns-confgen
-rwxr-xr-x    1 root     root          9888 Nov  6  2013 dnssec-checkds
-rwxr-xr-x    1 root     root         26578 Nov  6  2013 dnssec-coverage
-rwxr-xr-x    1 root     root       1239576 Nov  6  2013 dnssec-dsfromkey
-rwxr-xr-x    1 root     root       1240244 Nov  6  2013 dnssec-keyfromlabel
-rwxr-xr-x    1 root     root       1248052 Nov  6  2013 dnssec-keygen
-rwxr-xr-x    1 root     root       1235480 Nov  6  2013 dnssec-revoke
-rwxr-xr-x    1 root     root       1240136 Nov  6  2013 dnssec-settime
-rwxr-xr-x    1 root     root       1274000 Nov  6  2013 dnssec-signzone
-rwxr-xr-x    1 root     root       1239640 Nov  6  2013 dnssec-verify
-rwxr-xr-x    1 root     root          7740 Nov  6  2013 genrandom
-rwxr-xr-x    1 root     root         67780 Nov  6  2013 isc-hmac-fixup
-rwxr-xr-x    2 root     root       1813980 Nov  6  2013 lwresd
-rwxr-xr-x    2 root     root       1813980 Nov  6  2013 named
-rwxr-xr-x    1 root     root       1298644 Nov  6  2013 named-checkconf
-rwxr-xr-x    1 root     root       1227992 Nov  6  2013 named-checkzone
lrwxrwxrwx    1 root     root            15 Nov  6  2013 named-compilezone -> named-checkzone
-rwxr-xr-x    1 root     root       1215060 Nov  6  2013 named-journalprint
-rwxr-xr-x    1 root     root        101236 Nov  6  2013 nsec3hash
-rwxr-xr-x    1 root     root        238224 Nov  6  2013 rndc
-rwxr-xr-x    1 root     root        367836 Nov  6  2013 rndc-confgen
```

Paso 3. Crear el directorio de trabajo del servidor Bind

3.1 digite el siguiente comando

```
tc@servidor03:/usr/share$ sudo mkdir /usr/local/etc/namedb
```

3.2 verifique que lo ha creado correctamente

```
tc@servidor03:~$ ll /usr/local/etc/ |grep name
drwxr-xr-x    2 root     root           260 Jun 21 06:16 namedb/
```

3.3 Asigne los permisos al usuario tc en el directorio namedb

```
tc@servidor03:~$ sudo chown tc:staff /usr/local/etc/namedb* -R

tc@servidor03:~$ ll /usr/local/etc/ |grep name
drwxr-xr-x    2 tc       staff          260 Jun 21 06:16 namedb/
```

3.4 Copiar las llaves del servidor Bind (opcional)

Digitar el siguiente comando en una sola línea

```
tc@servidor03:~$ sudo cp /usr/local/etc/bind.keys
/usr/local/etc/namedb/bind.keys
```

Paso 4. Crear el archivo de configuración

4.1 Crear el archivo de configuración del servidor Bind

```
tc@servidor03:~$ sudo touch /usr/local/etc/named.conf
```

4.2 Escribir el siguiente contenido.

```
tc@servidor03:~$ mcedit /usr/local/etc/named.conf

//Yo lo preparee
include "/usr/local/etc/namedb/bind.keys";

options {
      // Directorio principal
      directory "/usr/local/etc/namedb";
      // Permitir acceo al cache -> None
      //allow-query-cache { none; };
      // Operación predeterminada
      //allow-query { any; };
      // Proveer recursividad -> No
      //recursion no;
      //reenviadores, DNS de los ISP
      forwarders { 8.8.8.8; 192.168.1.13; };
      }
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "db.127";
};
```

```
zone "0.in-addr.arpa" {
        type master;
        file "db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "db.255";
};

zone "empresay.com.sv" {
        type master;
        file "db.empresay.com.sv";
};

zone "70.168.192.in-addr.arpa" {
        type master;
        file "db.70.168.192";
};
```

Nota: Para mayor compresión del archivo se sugiere leer los siguientes enlaces:
http://www.mpipks-dresden.mpg.de/~mueller/docs/suse10.1/suselinux-manual_en/manual/sec.dns.bind.html
http://www.mpipks-dresden.mpg.de/~mueller/docs/suse10.1/suselinux-manual_en/manual/sec.dns.named.html
https://linuxconfig.org/linux-dns-server-bind-configuration

4.3 Verificar que o haya errores en el archivo de configuración

```
root@servidor03:~# named-checkconf
```

Nota: Solo si existe algún error se mostrará un mensaje en la pantalla.

Paso 5. Crear los archivos de zona.

Se deberán crear los archivos con las zonas directa e inversa para empresay.com.sv y se deberán agregar las zonas que permiten la resolución local y hacia los servidores de Internet

Nota: En el anexo se colocan los archivos de las zonas de apoyo.

5.1 Crear los siguientes archivos vacíos

Usar el comando **touch** para crear dentro **de /usr/local/etc/namedb** los siguientes archivos vacíos:

```
db.0
db.127
db.255
db.empty
db.local
db.root
zones.rfc1918
db.empresay.com.sv
db.70.168.192
```

5.2 Escriba el contenido del archivo de zona directa

```
tc@servidor03:~$ mcedit /usr/local/etc/namedb/db.empresay.com.sv
$TTL 2D
empresay.com.sv. IN SOA      servidor04  servidor04.empresay.com.sv. (
            2016062022  ; serial
            1D          ; refresh
            2H          ; retry
            1W          ; expiry
            2D )        ; minimum

            IN NS       servidor04
            IN MX       10 mail.empresay.com.sv.

srvext          IN A        192.168.70.1
srvint          IN A        192.168.60.2
servidor04      IN A        192.168.70.4
servidor05      IN A        192.168.70.5
www             IN CNAME    servidor05
smtp            IN CNAME    servidor05
mail            IN CNAME    servidor05
```

5.3 Escriba el contenido del archivo de zona inversa.

```
tc@servidor03:~$ cat /usr/local/etc/namedb/db.70.168.192

$TTL 2D
$ORIGIN 70.168.192.in-addr.arpa.
@       IN      SOA     servidor04.empresay.com.sv. servidor04.empresay.com.sv. (
                        2016062022      ;serial number
                        8H              ;refresh
                        2H              ;retry
                        4W              ;expiration
                        1D )            ;
;
                NS      servidor04.empresay.com.sv.
;
1       PTR     srvext.empresay.com.sv.
2       PTR     srvint.empresay.com.sv.
4       PTR     servidor04.empresay.com.sv.
5       PTR     servidor05.empresay.com.sv.
```

5.4 Verificar estructura de las zonas directa e inversa

```
tc@servidor03:~$named-checkzone                                    empresay.com.sv
/usr/local/etc/namedb/db.empresay.com.sv

zone empresay.com.sv/IN: empresay.com.sv/MX 'mail.empresay.com.sv' is a CNAME (illegal)
zone empresay.com.sv/IN: loaded serial 2016062040
OK

tc@servidor03:~$named-checkzone 70.168.192.in-addr.arpa
/usr/local/etc/namedb/db.70.168.192

zone 70.168.192.in-addr.arpa/IN: loaded serial 2016062040
OK
```

Paso 5. Inicializar servidor DNS

5.1 Iniciar manualmente el servidor DNS

```
tc@servidor03:~$ sudo named -c /usr/local/etc/named.conf
```

5.2 Verificar que el servicio haya iniciado

```
tc@servidor03:~$ netstat -atpn

netstat: showing only processes with your user ID
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 192.168.70.4:53         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
netstat: /proc/net/tcp6: No such file or directory
```

5.3 Apagar el servidor DNS

```
tc@servidor03:~$ sudo killall named
```

5.4 Verificar que se haya apagado

```
tc@servidor03:~$ netstat -atpn

netstat: showing only processes with your user ID
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
netstat: /proc/net/tcp6: No such file or directory
```

Paso 6. Pruebas de consulta

6.1 Configure los valores IPv4 del servidor04

IPv4 192.168.70.4/24, DNS 172.168.70.4 y el GW 192.168.70.1

6.2 Resuleva de forma directa, e inversa.

Digitar los siguientes comandos

```
tc@servidor03:~$ nslookup servidor04.empresay.com.sv
Server:         192.168.70.4
Address:        192.168.70.4#53

Name:   servidor04.empresay.com.sv
Address: 192.168.70.4

tc@servidor03:~$ nslookup www.empresay.com.sv
Server:         192.168.70.4
Address:        192.168.70.4#53

www.empresay.com.sv     canonical name = servidor05.empresay.com.sv.
```

```
Name:   servidor05.empresay.com.sv
Address: 192.168.70.5

tc@servidor03:~$ nslookup 192.168.70.5
Server:         192.168.70.4
Address:        192.168.70.4#53

5.70.168.192.in-addr.arpa       name = servidor05.empresay.com.sv.



tc@servidor03:~$ dig servidor04.empresay.com.sv

; <<>> DiG 9.9.4 <<>> servidor04.empresay.com.sv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42746
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;servidor04.empresay.com.sv.    IN      A

;; ANSWER SECTION:
servidor04.empresay.com.sv. 172800 IN   A       192.168.70.4

;; AUTHORITY SECTION:
empresay.com.sv.        172800  IN      NS      servidor04.empresay.com.sv.

;; Query time: 4 msec
;; SERVER: 192.168.70.4#53(192.168.70.4)
;; WHEN: Tue Jun 21 08:28:44 UTC 2016
;; MSG SIZE  rcvd: 85

tc@servidor03:~$ dig www.empresay.com.sv

; <<>> DiG 9.9.4 <<>> www.empresay.com.sv
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55224
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.empresay.com.sv.           IN      A

;; ANSWER SECTION:
www.empresay.com.sv.    172800  IN      CNAME   servidor05.empresay.com.sv.
servidor05.empresay.com.sv. 172800 IN   A       192.168.70.5

;; AUTHORITY SECTION:
empresay.com.sv.        172800  IN      NS      servidor04.empresay.com.sv.

;; ADDITIONAL SECTION:
servidor04.empresay.com.sv. 172800 IN   A       192.168.70.4

;; Query time: 7 msec
;; SERVER: 192.168.70.4#53(192.168.70.4)
```

```
;; WHEN: Tue Jun 21 08:28:53 UTC 2016
;; MSG SIZE  rcvd: 130

tc@servidor03:~$ dig 192.168.70.5

; <<>> DiG 9.9.4 <<>> 192.168.70.5
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 17900
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;192.168.70.5.                  IN      A

;; Query time: 5 msec
;; SERVER: 192.168.70.4#53(192.168.70.4)
;; WHEN: Tue Jun 21 08:29:20 UTC 2016
;; MSG SIZE  rcvd: 41
```

Paso 7. Guardar los cambios en el Core Plus.

Debido a que la versión de Core Plus fue diseñada para sistemas operativos tipo LIVE, será necesario indicar los archivos y directorios que serán persistentes

```
tc@servidor03:~$ mcedit /opt/.filetool.lst
opt
home
etc/passwd
etc/shadow
usr/local/etc/ssh
var/www
usr/local/etc/httpd/httpd.conf
etc/my.cnf
usr/local/mysql/data
var/run/mysqld
usr/local/etc/samba/smb.conf
usr/local/etc/samba/private/passdb.tdb
usr/local/etc/named.conf
usr/local/etc/namedb
tmp/tcloop/bind/
opt/eth0.sh
```

2.2 Instalación der servidor Web.

Utilice un clon del servidor02

Nota: Recuerde que el servidor Apache no se ejecuta automáticamente, si se desea se puede configurar para que inicie en cada arranque, esto aparece en la primera guía del primer módulo.

2.3 Configuración del srvext

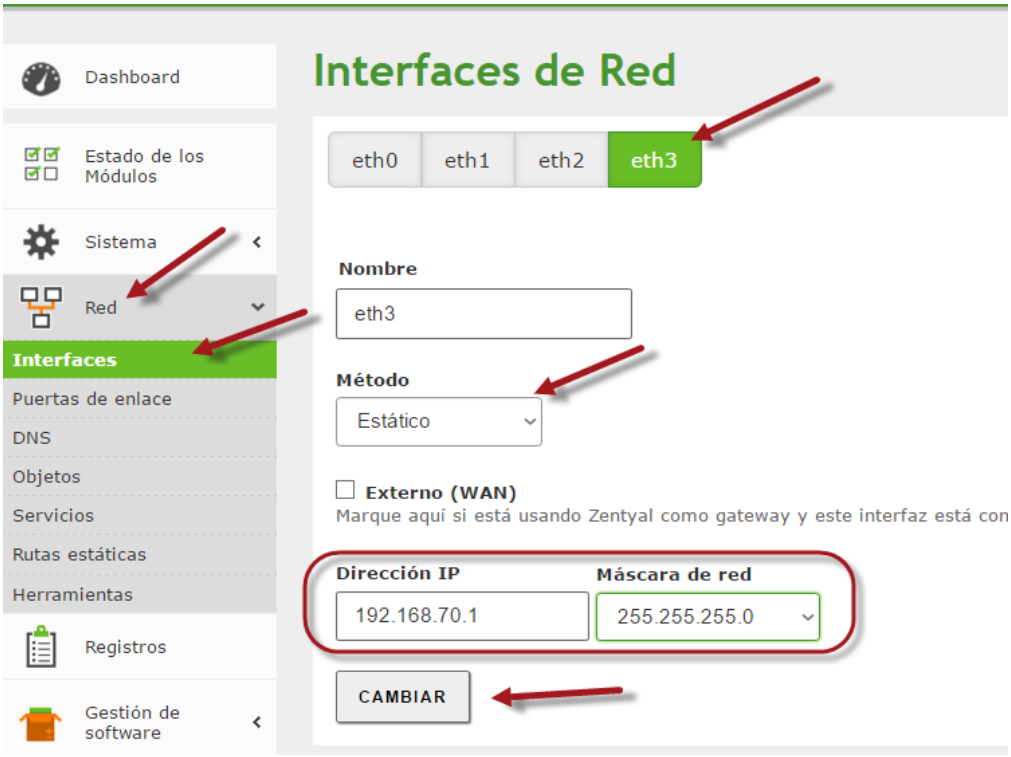
Paso 1. Agregar una cuarta tarjeta de red.

1.1 Ingresar a Red / Interfaces

1.2 Seleccionar eth3

1.3. Definir los valores de la interfaz

- Tipo de configuración: Estática
- IPv4: 192.168.70.1 / 255.255.255.0



1.4 Dar clic en botón "Cambiar"

1.5 Dar clic en botón "Guadar cambios"

Paso 2. Verificar la configuración IPv4 de la interfaz eth3

Digitar el siguiente comando:

```
root@srvext:~# ip addr list
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 127.0.1.1/8 scope host secondary lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP group default qlen 1000
    link/ether 02:aa:e0:00:00:01 brd ff:ff:ff:ff:ff:ff
```

```
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP group default qlen 1000
    link/ether 02:aa:e1:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.1/24 brd 192.168.60.255 scope global eth1
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP group default qlen 1000
    link/ether 02:aa:e2:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.1/24 brd 192.168.50.255 scope global eth2
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP group default qlen 1000
    link/ether 02:aa:e3:00:00:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.70.1/24 brd 192.168.70.255 scope global eth3
       valid_lft forever preferred_lft forever
```

Paso 3. Crear reglas de filtrado de paquetes para comprobar comunicación entre la DMZ y srvext (opcional)

A continuación, se recomeinda crear las siguientes reglas de filtyrado para probar conectividad entre la DMZ y la red LAN1, después se deben eliminar. No es necesario contar con estas reglas, sin embargo ayudará a establecer la comunicación.

I. Hacer ping entre la DMZ y srvext, para comprobar la comunicación IPv4
II. Permitir a los servidores de la DMZ navegar en Internet (sólo HTTP), así se comprueba la resolución interactiva, y tráfico IPv4.

3.1 Seleccionar menú Cortafuegos / Filtrado de paquetes
3.2 Seleccionar Desde redes internas hacia Zentyal

Parámetros de la regla a crear:

- Origen: Objeto con las dos direcciones IPv4 de la DMZ
- Destino: **Any**.

- Servicio: **Any ICMP**
- Descripción: **Borrar, Permitir ICMP desde LAN3 a SRVEXT**

3.3 Seleccionar detro de Filtrado de paquetes, Redes internas

3.4 Añadir regla que permita nevegación HTTP en la DMZ

Parámetros de la regla a crear:

- Origen: Objeto con las dos direcciones IPv4 de la DMZ
- Destino: **Any**.
- Servicio: **HTTP**
- Descripción: **Borrar, Permitir a red LAN3 acceso a sitios WEB**

Paso 4. Verificar la aplicación de las reglas temporales (opcional)

4.1 Comprobar la comunicación IPV4 entre la DMZ y el srvext (opcional)

```
tc@servidor03:~$ ping -c 3 192.168.70.1

PING 192.168.70.1 (192.168.70.1): 56 data bytes
64 bytes from 192.168.70.1: seq=0 ttl=64 time=0.914 ms
64 bytes from 192.168.70.1: seq=1 ttl=64 time=0.936 ms
64 bytes from 192.168.70.1: seq=2 ttl=64 time=0.983 ms
--- 192.168.70.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.914/0.944/0.983 ms

tc@servidor01:~$ ping -c 3 192.168.70.1
PING 192.168.70.1 (192.168.70.1): 56 data bytes
64 bytes from 192.168.70.1: seq=0 ttl=64 time=0.795 ms
64 bytes from 192.168.70.1: seq=1 ttl=64 time=0.964 ms
64 bytes from 192.168.70.1: seq=2 ttl=64 time=0.919 ms
--- 192.168.70.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.795/0.892/0.964 ms
```

4.2 Comprobar la navegación Web en la DMZ

Ingresar al servidor05 y navegar en Internet

2.4 Modificar el reenviador del DNS interno para que apunte al DNS externo.

Paso 1. Ingresar a la herramienta de configuración Web de SRVINT

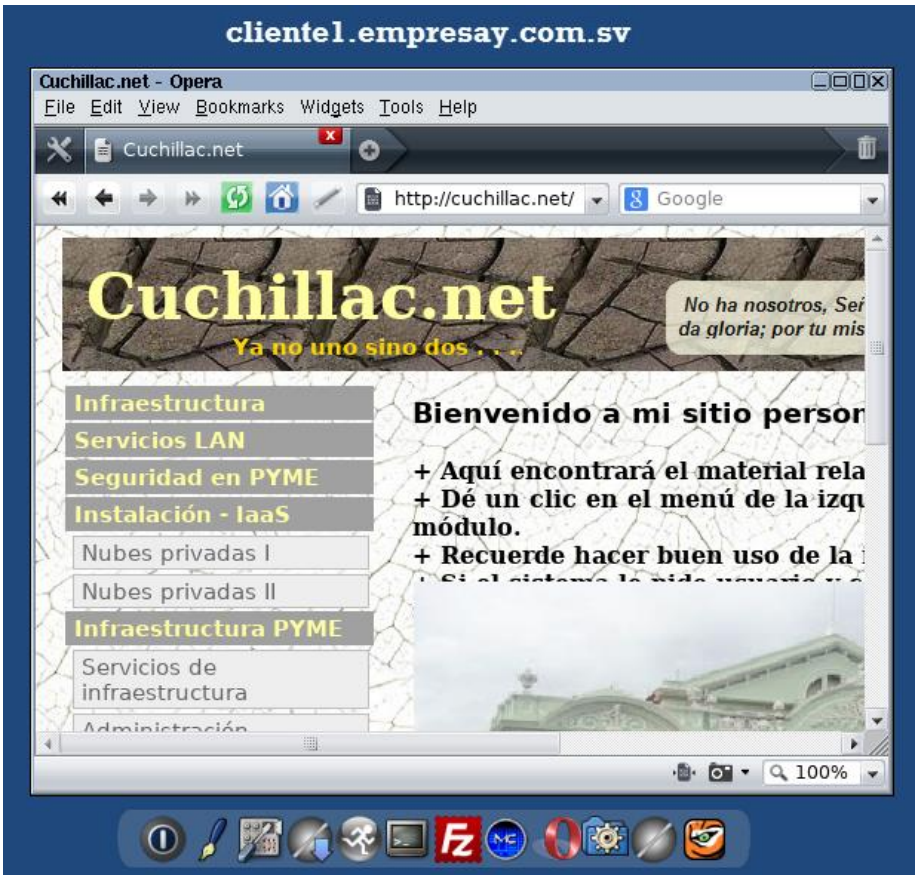
1.1 Ingresar a la herramientas web de Zentyal
1.2 Seleccionar DNS
1.3 Eliminar los reenviadores anteriores

Nota: Recuerde que, si no tiene el servidor DNS externo, ya no se podrá navegar en Internet

1.4 Agregar como reenviador la dirección IPv4 del servidor04
1.5 Guardar los cambios.

Paso 2. Comprobar navegación de los clientes de la LAN1

Ingrese desde el cliente1 y navegue en la Internet

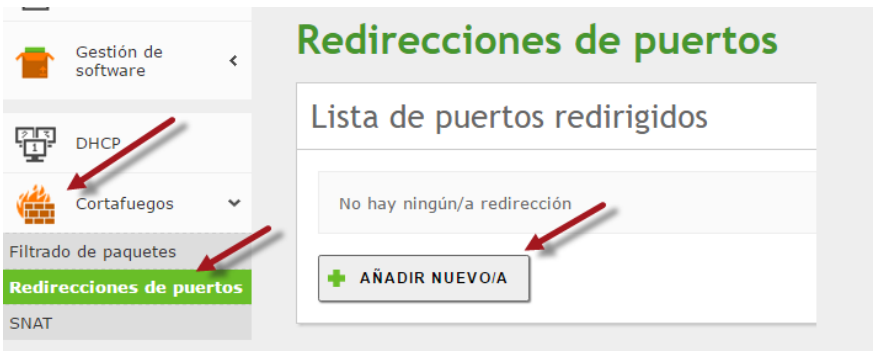


2.5 Crear reglas NAT para la DMZ

Paso 1. Acceder al menú de configuración de reglas de reenvío.

1.1 Ingresar al menú Cortafuegos / "Redirecciones de puertos"

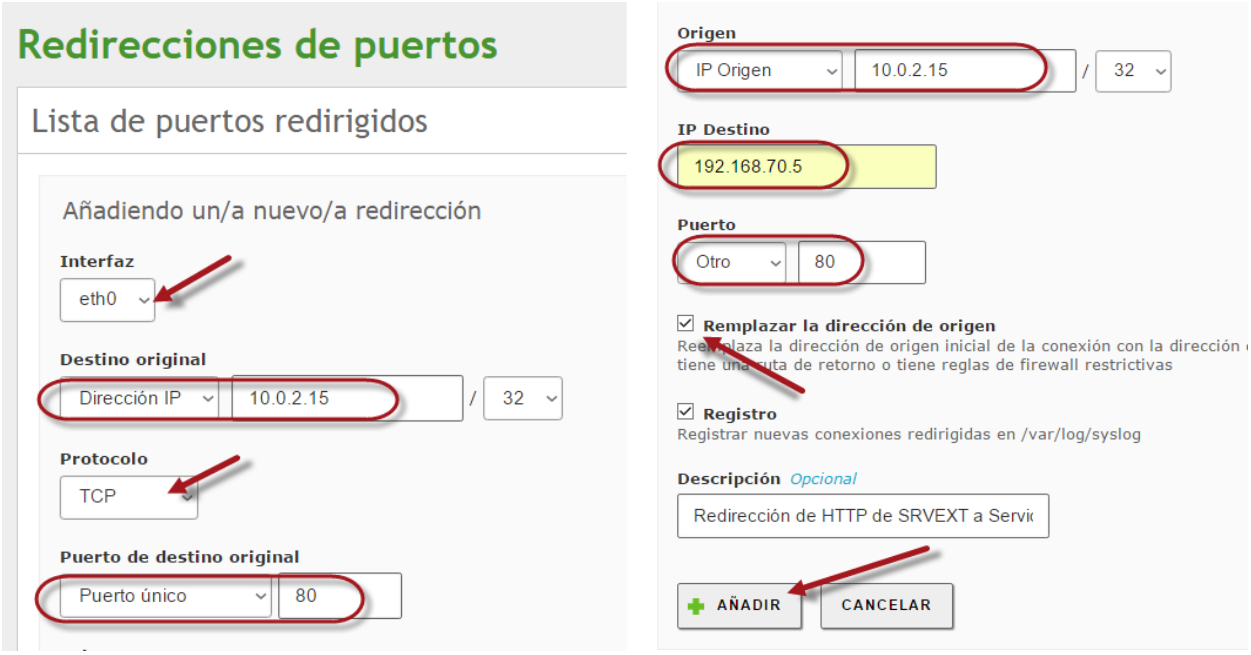
1.2 Dar clic en botón "Añadir nuevo/a"



Paso 3. Definir las opciones de la regla del NAT

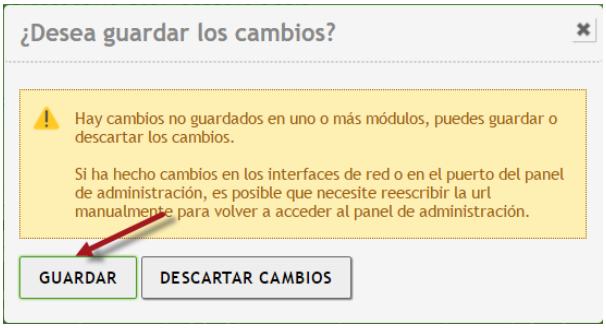
Parámetros para crear la regla del NAT

- Interfaz: **eth0**
- Destino original: **10.0.2.15/32** (debe ser la dirección IPv4 de la eth0, puede utilizar el valor **Zentyal**)
- Protocolo: **TCP**
- Puerto de destino original: **80**
- Origen: **10.0.2.15/32**
- IP Destino: **192.168.70.5**
- Puerto: **80**
- Reemplazar dirección de origen: **Activado**
- Registro: **Activado**
- Descripción de la regla: Redirección de HTTP de SRVEXT hacia server05



1.4 Dar Clic e botón "+Añadir"

1.5 Guardar los cambios



Paso 2. Verificar que se haya creado la regla NAT

Digitar en la consola de srvext

```
root@srvext:~# iptables -t nat -L -n

Chain PREROUTING (policy ACCEPT)
target     prot opt source       destination
premodules  all  --  0.0.0.0/0    0.0.0.0/0
DNAT        tcp  --  10.0.2.15    10.0.2.15   tcp dpt:80 to:192.168.70.5:80

Chain INPUT (policy ACCEPT)
target     prot opt source       destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source       destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source       destination
postmodules  all  --  0.0.0.0/0   0.0.0.0/0
SNAT        tcp  --  10.0.2.15   192.168.70.5  tcp dpt:80 ctstate DNAT
to:192.168.70.1
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain postmodules (1 references)
target     prot opt source               destination

Chain premodules (1 references)
target     prot opt source               destination
```

Paso 3. Verificar el proceso de redirección

Consideraciones en un escenario real

1. La tarjeta eth0 está conectada a un MODEM provisto por el ISP.
2. La dirección eth0 de srvext es una dirección pública estática (podría ser DHCP[1])
3. Existe un registro del dominio en servidores DNS tipo TLD, por ejemplo, SVNET, que contiene la dirección IPv4 pública del equipo srvext
4. Cualquier equipo en Internet puede consultar a los DNS de primer nivel y llegar así a la dirección IPv4 pública del servidor srvext.
5. No hay inconvenientes.

Consideraciones del escenario en laboratorio CASO NAT con VirtualBox

1. La interfaz eth0 está conectada como NAT dentro de VirtualBox.
2. La eth0 es dinámica y siempre obtendrá el valor de 10.0.2.15/24
3. Como el NAT de VirtualBox no tiene DNS, se puede utilizar el archivo **hosts** del equipo cliente donde se ejecuta VirtualBox, y no se puede conectarse
4. Para que el sistema operativo donde se ejecuta VirtualBox pueda llegar al servicio hay que crear reglas de NAT en la herramienta de configuración de VirtualBox.
5. Inconveniente: No se puede redireccionar tráfico desde otros equipos del laboratorio.

Consideraciones del escenario en laboratorio CASO BRIDGE a una Ethernet con VirtualBox

1. La interfaz eth0 está conectada como BRIDGE dentro de una red LAN, por ejemplo, 10.10.3.0/24
2. La eth0 es dinámica y obtendrá un valor del DHCP de la red LAN, (puede ser configurada estáticamente)
3. Como lo más probable es que no se pueda configurar editar la base de datos del servidor DNS de la red LAN del laboratorio, se debe utilizar el archivo **hosts** del equipo cliente donde se desea conectarse.
4. Cualquier equipo de la red LAN (por ejemplo, 10.10.3.0/24) puede llegar así a la dirección IPv4 del eth0 del servidor srvext, la cual simula ser una IPv4 pública.
5. Inconveniente: Cómo no se puede editar la tabla de ruteo del Gateway del laboratorio las computadoras de la empresay no podrán navegar a Internet.

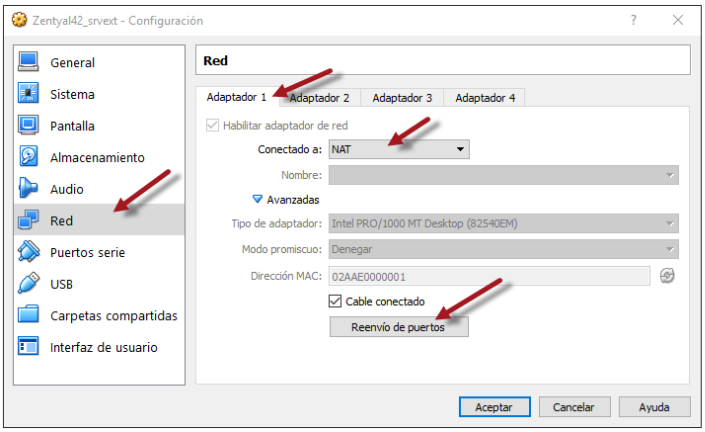
3.1 Caso BRIDGE

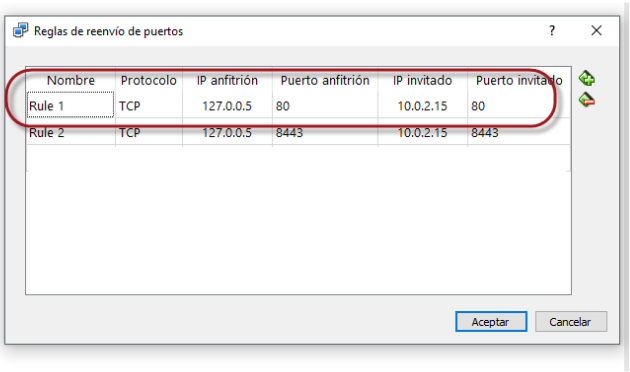
Desde la computadora 10.10.3.155 coloque la dirección 10.10.3.154 (eth0 de srvext)

[1] Para entornos empresariales las direcciones IPv4 provistas por los ISP son generalmente configuradas como estáticas.

3.2 Caso NAT

Hay que crear una regla que permita reenviar el tráfico de la máquina donde está instalado VirtualBox a eth0 de srvext.





III. Tareas

Desarrolle los siguientes puntos, serán considerados para el examen teórico y el examen práctico grupal.

1. ¿Es el mismo resultado en términos de resolución, utilizar un DNS con vistas que dos DNS (uno externo y otro interno)?

2. ¿Cuál es la diferencia entre NAT estático y NAT dinámico?

3. ¿Qué es el PAT overriding?

4. ¿Qué es el pre routing y post routing?

5. Realizar una consulta vía php en el servidor05 hacia la base de datos del servidor MariaDB de la red LAN01
   - El servidor05 tendrá una página principal con un enlace hacia una página PHP
   - La página PHP del servidor05 deberá establecer la conexión utilizando las credenciales de usuario: "**ususelect/123456**" hacia la base de datos del MariaDB del servidor02
   - La página PHP debe mostrar el contenido de la base de datos del servidor MariaDB
   - El servidor01 tendrá una página principal con un enlace hacia una página PHP
   - La página PHP del servidor01 tendrá un formulario que deberá permitir agregar, mostrar y borrar registros de la base de datos MariaDB en el servidor02
   - La página PHP del servidor01 deberá utilizar en la conexión hacia MariaDB las credenciales de usuario: "**usumodify/123456**"

Anexos

A1. Archivos de apoyo para DNS

```
tc@servidor03:~$ mcedit /usr/local/etc/namedb/db.0
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
```

```
tc@servidor03:~$ mcedit /usr/local/etc/namedb/db.127
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

```
tc@servidor03:~$ cat /usr/local/etc/namedb/db.255
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
```

```
tc@servidor03:~$ cat /usr/local/etc/namedb/db.empty
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
```

```
tc@servidor03:~$ cat /usr/local/etc/namedb/db.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

```
tc@servidor03:~$ cat /usr/local/etc/namedb/db.root

;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Jan 3, 2013
;       related version of root zone:   2013010300
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
```

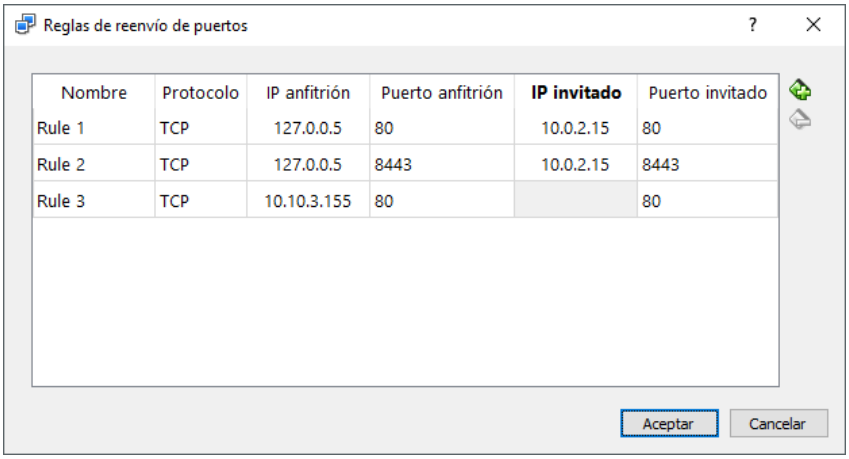
```
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
;
; FORMERLY C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2F::F
;
; FORMERLY NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
H.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:1::803F:235
;
; FORMERLY NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.     3600000      AAAA  2001:7FE::53
;
; OPERATED BY VERISIGN, INC.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:C27::2:30
;
; OPERATED BY RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.     3600000      AAAA  2001:7FD::1
;
; OPERATED BY ICANN
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:3::42
;
; OPERATED BY WIDE
;
```

```
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.     3600000      AAAA  2001:DC3::35
; End of File
```

```
tc@servidor03:~$ cat /usr/local/etc/namedb/zones.rfc1918
zone "10.in-addr.arpa"      { type master; file "/etc/bind/db.empty"; };

zone "16.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "17.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "18.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "19.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "20.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "21.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "22.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "23.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "24.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "25.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "26.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "27.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "28.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "29.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "30.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };
zone "31.172.in-addr.arpa"  { type master; file "/etc/bind/db.empty"; };

zone "168.192.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
```

A2. Configuración alterna para permitir acceso de otros equipos de la misma red LAN usando NAT de VirtualBox


```
root@srvext:~# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
premodules  all  --  0.0.0.0/0            0.0.0.0/0
DNAT       tcp  --  0.0.0.0/0            10.0.2.15           tcp dpt:80
to:192.168.70.5:80

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
postmodules  all  --  0.0.0.0/0            0.0.0.0/0
SNAT       tcp  --  0.0.0.0/0            192.168.70.5        tcp dpt:80 ctstate DNAT
to:192.168.70.1
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain postmodules (1 references)
target     prot opt source               destination

Chain premodules (1 references)
target     prot opt source               destination
```



Desde otro equipo de la red