Guía de Seguridad

Fecha de publicación: 08/07/2022

Tema: Guía para restringir el acceso al centro de administración de servidores de correo.

Objetivo: Proveer una guía para la limitación de acceso a las interfaces de administración web de los servidores de correo Zimbra y Exchange.

Índice

Interfaces de administración de servidores de correo

Algunos de los servidores de correo más utilizados son Microsoft Exchange Server y Zimbra para sistemas operativos Microsoft Windows y distribuciones basadas en Linux respectivamente. La administración de los servidores de correo por lo general puede llevarse a cabo a través de interfaces de administración web (Panel de Administración) accesibles desde los navegadores. A continuación, detallaremos más al respecto de los riesgos asociados a dichas interfaces y las alternativas de mitigación de dichos riesgos.

Servidor Microsoft Exchange Server

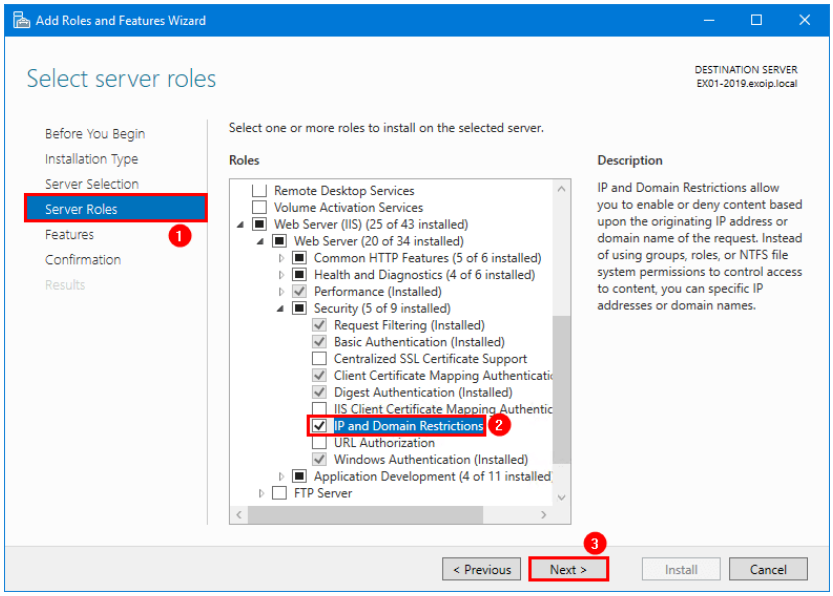
El Centro de Administración de Exchange (EAC, por sus siglas en inglés) es la interfaz de administración principal para Microsoft Exchange Server versión 2013 o posterior.

De forma predeterminada, el acceso al EAC no está restringido, y el acceso a Outlook en la web (formalmente conocido como Outlook *Web App*), todavía necesita credenciales válidas para iniciar sesión en el EAC, se recomienda a las organizaciones restringir el acceso al EAC para las conexiones de cliente desde Internet o sea fuera de la red corporativa. A continuación, se describen los pasos necesarios para la restricción al EAC.

Definición del rol de restricciones de IP y de Dominio

Para instalar el rol Restricciones de DOMINIO e IP, se recomienda seguir los siguientes pasos:

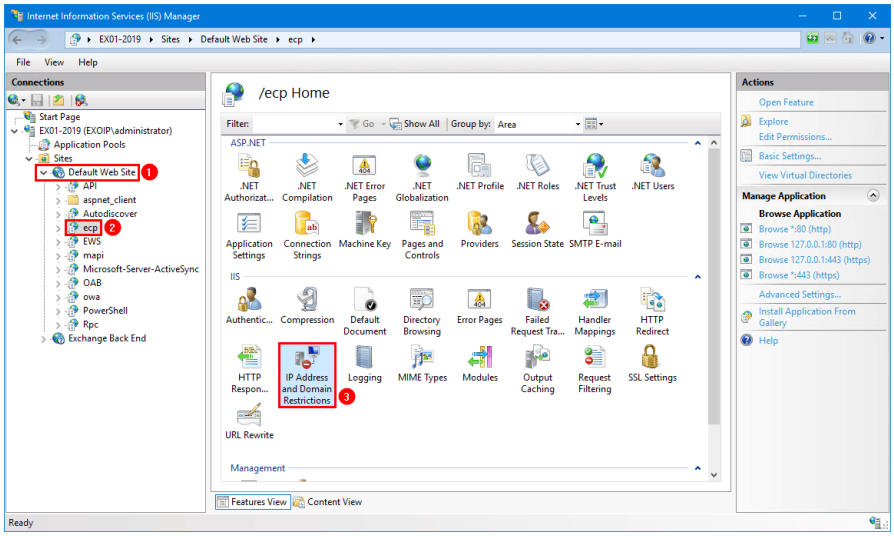
- **Iniciar sesión** en Exchange Server.
- Iniciar el **Administrador del servidor.**
- Hacer clic en **Administrar > Agregar roles y características.**
- Seguir el asistente y seleccionar **Exchange Server**.
- Ir a la pestaña **Roles de servidor**.
- Expandir Servidor web (IIS) > servidor web > seguridad.
- Comprobar el rol **Restricciones de IP y dominio**.
- Hacer clic en Siguiente.
- Finalizar la instalación.



Configuración de dirección IP y restricciones de Dominio en IIS

Siga los pasos a continuación para iniciar las restricciones de dominio y dirección IP:

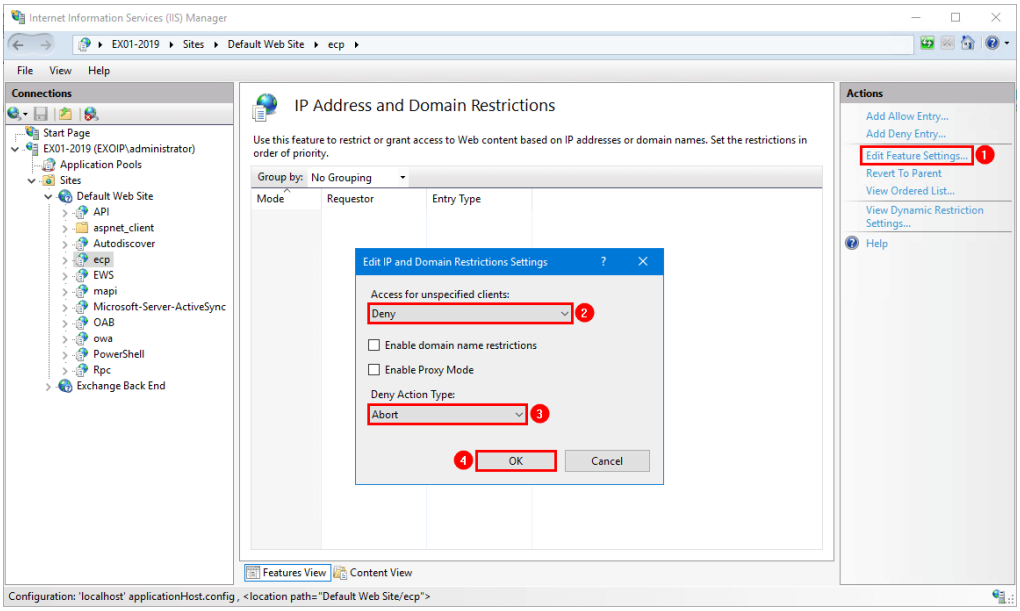
- Abrir el **Administrador de IIS** en Exchange Server.
- Expandir sitio > sitio web predeterminado.
- Hacer clic en ecp.
- Hacer doble clic en Dirección IP y restricciones de dominio.



Editar la configuración de la función

Para deshabilitar el acceso externo a ECP en Exchange Server se debe tener en cuenta los siguientes pasos:

- Hacer clic en Editar configuración de funciones.
- Establecer el acceso para clientes no especificados en **Denegar**.
- Establecer el tipo de acción denegar en **Anular**.
- Hacer clic en **Aceptar**.

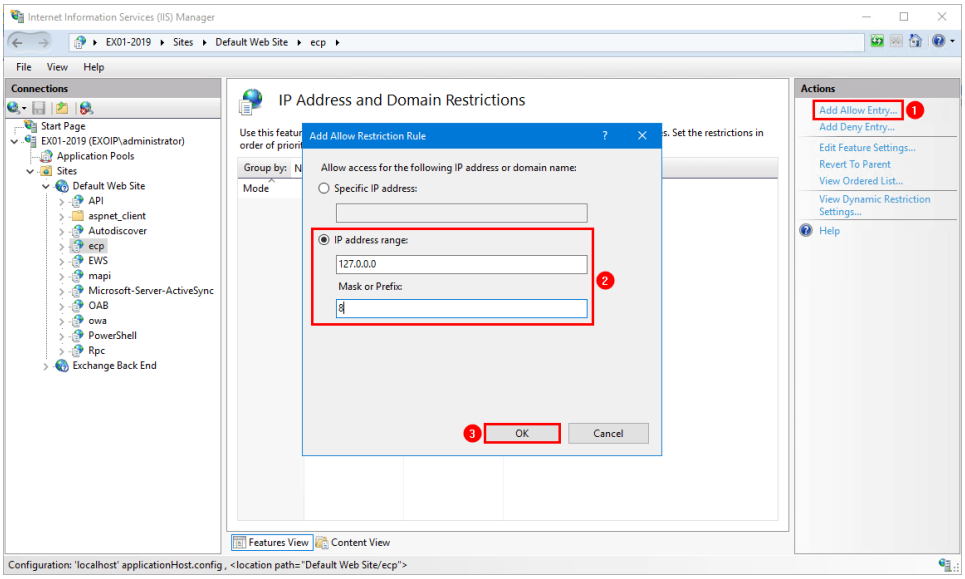


Permitir que localhost tenga acceso a Exchange Server

Para permitir que el localhost obtenga el acceso al servidor de Exchange, se deben de seguir los siguientes pasos

- Hacer clic en **Agregar** entrada permitida.
- **Agregar** el intervalo de direcciones IP 127.0.0.0 con el prefijo 8.
- Hacer clic en **Aceptar**.

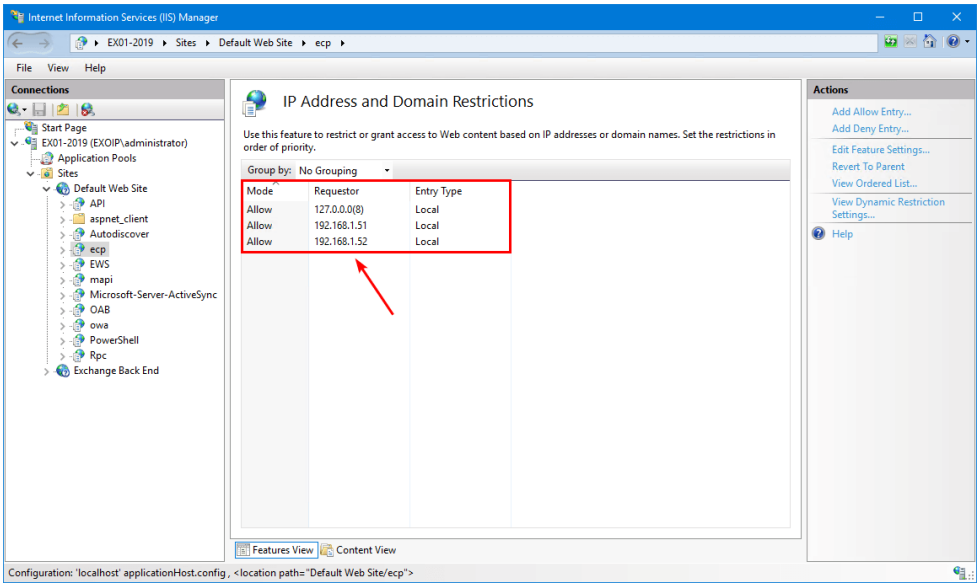
Supongamos que desea agregar la máscara de subred en lugar del prefijo. Eso sería 255.0.0.0.



Nota: No se recomienda permitir el acceso ECP en toda la LAN interna. En caso de tener servidores de administración, agregar las direcciones IP a la lista de permitidos.

En este ejemplo, se tiene los siguientes sistemas en la lista de permitidos:

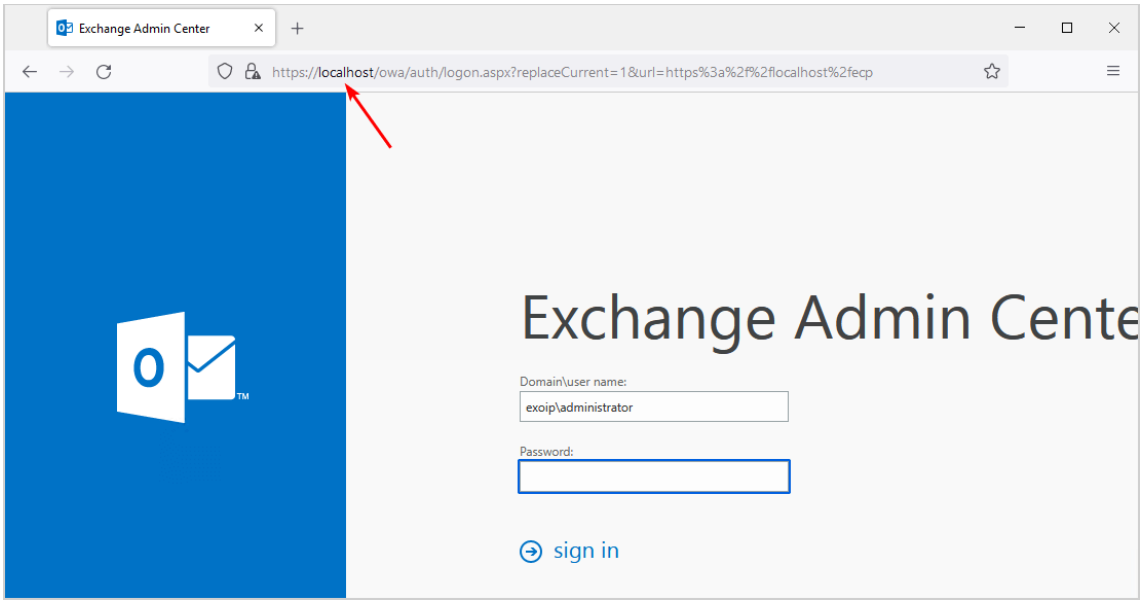
- 127.0.0.0(8) (localhost)
- 192.168.1.51 (Servidor de administración)
- 192.168.1.52 (Exchange Server)



Verificar el acceso al Exchange Control Panel (ECP)

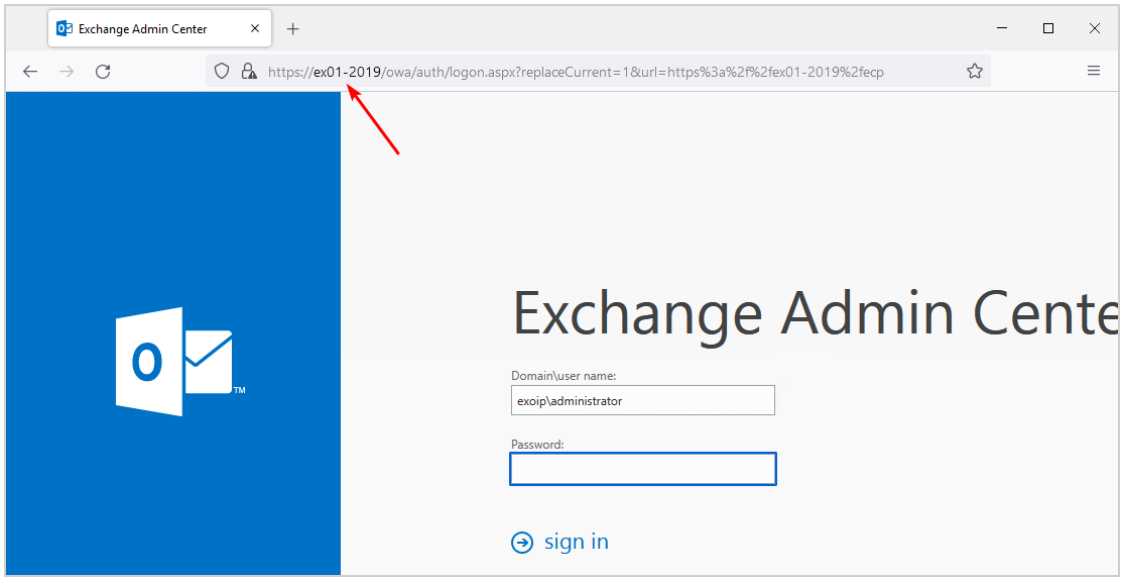
El acceso público al Exchange Control Panel (ECP) debe ser deshabilitado ya que este puede ser considerado un riesgo de seguridad ante un posible ataque de fuerza bruta, por ejemplo, por lo que es conveniente bloquearlo en el firewall. El firewall de la organización es el primer punto para bloquear el acceso externo, es por ello por lo que debemos tener en cuenta los siguientes pasos para deshabilitar el acceso externo a ECP en Exchange Server:

- Iniciar ECP desde Exchange Server. Asegurarse de insertar el nombre de host local **https://localhost/ecp**. Se visualizará la pantalla de inicio de sesión, posteriormente iniciar sesión.

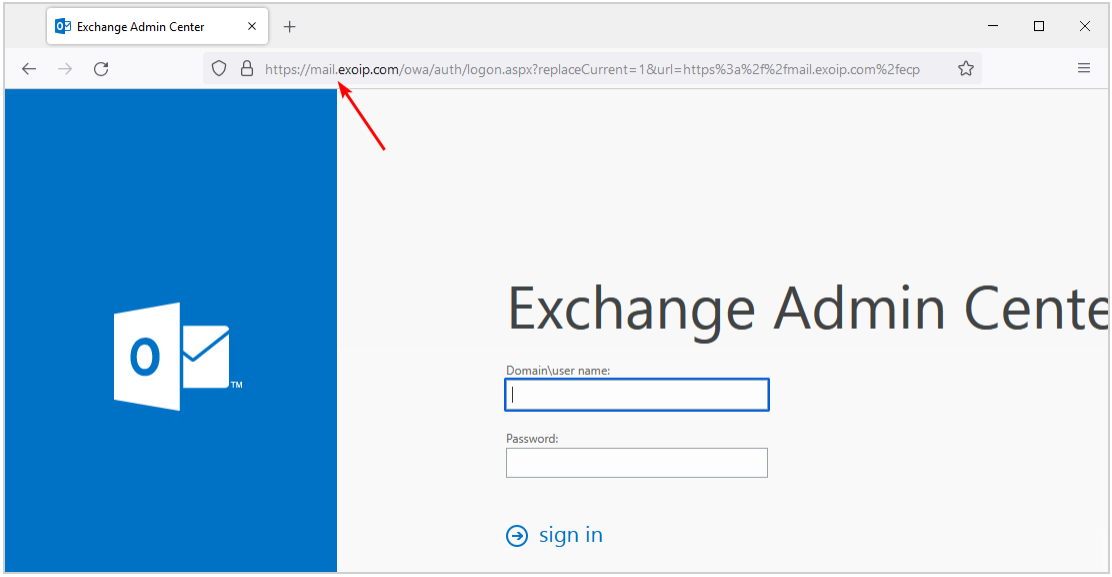


- Iniciar ECP desde las direcciones IP de la lista de permitidos, se debe insertar el nombre de host de Exchange Server. Por ejemplo, **https://EX01-2019/ecp**. Se visualizará la pantalla de inicio de sesión, posteriormente iniciar sesión.

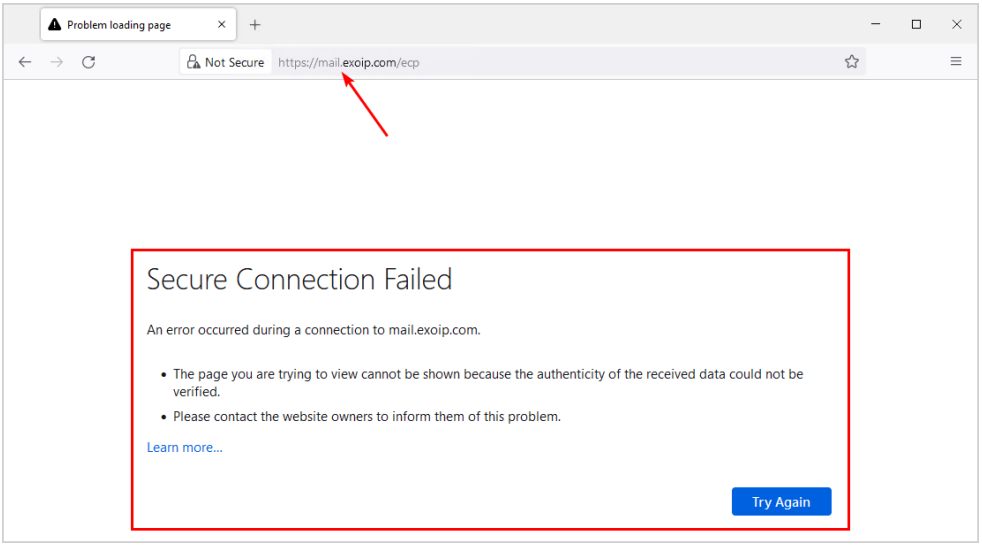
Nota: La navegación al nombre de host ecp (https://EX01-2019/ecp) de Exchange Server desde Exchange Server no funcionará. Sin embargo, funcionará en otros sistemas permitidos. En su lugar, use localhost o el nombre DNS interno.



- Iniciar ECP desde las direcciones IP de la lista de permitidas. Asegúrese de insertar el DNS interno de Exchange Server. Por ejemplo, **https://mail.exoip.com/ecp**. Se visualizará la pantalla de inicio de sesión, para posteriormente iniciar sesión.



- Al intentar iniciar ECP desde un sistema IP externo o no agregado, no se mostrará el Centro de administración de Exchange (ECP) y se anulará la conexión.



A continuación, veremos las alternativas relacionadas a los servidores de correo Zimbra.

Servidor Zimbra

La Consola de Administración (admin console) es la herramienta que permite al administrador del servidor de correo Zimbra, monitorear todos los procesos del servidor, configurar dominios, cuentas de usuarios, clase de servicios, entre otros. Por razones de seguridad se recomienda restringir el acceso a dicha consola de administración para conexiones de clientes desde el internet. La restricción de dicho acceso puede ser implementada a través de reglas de firewall.

Establecer reglas de firewall

Se deben tener en cuenta algunos principios generales para garantizar la seguridad de la información del servidor y eso incluye la configuración adecuada del firewall de la organización y del sistema operativo de servidor en el que se ejecuta el Zimbra. Un sistema de filtrado de tráfico de red configurado de manera óptima es capaz de neutralizar la mayor parte de las amenazas cibernéticas.

Zimbra utiliza activamente varios puertos de red para conexiones externas e intrasistema. Es por eso por lo que lo óptimo para ello será la creación de la llamada "Lista Blanca" o "Política Drop por defecto" en las reglas del firewall. Es decir, primero prohibir toda conexión a

cualquier puerto en el servidor, y luego abrir solo aquellos que son necesarios para el funcionamiento normal del servidor.

Para conexiones externas, Zimbra puede utilizar los siguientes puertos, que incluyen:

- Puerto 7071 por defecto en las versiones modernas de Zimbra.
- 25 puertos para correo entrante en postfix.
- Puerto 80 para conexión insegura al cliente web de Zimbra.
- Puerto 110 para recibir correo de un servidor remoto utilizando el protocolo POP3.
- 143 puerto de acceso IMAP.
- Puerto 443 para una conexión segura a Zimbra Web Client.
- 587 puerto de entrada de conexión.
- Puerto 993 para acceso seguro al correo electrónico a través de IMAP.
- Puerto 995 para recibir correo de forma segura desde un servidor remoto utilizando el protocolo POP3.
- 5222 puerto para conectarse al servidor a través de XMPP.
- Puerto 5223 para una conexión segura al servidor a través de XMPP.
- Puerto 9071 para una conexión segura a la consola del administrador.

Además de las conexiones externas, en Zimbra hay muchas conexiones internas que también se producen en varios puertos. Por lo tanto, al incluir dichos puertos en la "lista blanca", vale la pena asegurarse de que solo los usuarios locales puedan conectarse a ellos. El listado de puertos internos sería el siguiente:

- Puerto 389 para conexión LDAP insegura.
- Puerto 636 para una conexión LDAP segura.
- Puerto 3310 para conectarse al antivirus ClamAV.
- Puerto 5269 para la comunicación entre servidores ubicados en el mismo clúster utilizando el protocolo XMPP.
- Puerto 7025 para intercambio de correo local a través de LMTP.
- Puerto 7047 utilizado por el servidor para convertir archivos adjuntos.
- Puerto 7071 para acceso seguro a la consola del administrador.
- Puerto 7072 para descubrimiento y autenticación en nginx.
- 7073 puerto para descubrimiento y autenticación en SASL.
- Puerto 7110 para acceder a servicios internos POP3.
- 7143 puerto para acceso a servicios internos IMAP.
- 7171 puerto para acceder al demonio de configuración zbra zmconfigd.
- Puerto 7306 para acceder a MySQL.
- 7780 puerto para acceder al servicio de ortografía.
- Puerto 7993 para acceso seguro a servicios IMAP internos.

- Puerto 7995 para acceso seguro a servicios internos POP3.
- Puerto 8080 para acceder a servicios HTTP internos.
- Puerto 8443 para acceder a servicios HTTPS internos.
- 8735 puerto para comunicación entre buzones.
- 8736 puerto para acceder al servicio de configuración distribuida de Zextras.
- Puerto 10024 para la comunicación de Amavis con Postfix.
- Puerto 10025 para la comunicación de Amavis con OpenDKIM.
- Puerto 10026 para configurar las políticas de Amavis.
- 10028 puerto de comunicación Amavis con filtro de contenido.
- Puerto 10029 para acceder a archivos Postfix.
- Puerto 10032 para la comunicación de Amavis con el filtro antispam SpamAssassin.
- 23232 puerto para acceder a los servicios internos de Amavis.
- 23233 puerto para acceder a snmp-respondedor.
- Puerto 11211 para acceder a memcached.

Tenga en cuenta que, si en el caso de que Zimbra funcione en un solo servidor, puede hacerlo con un conjunto mínimo de puertos abiertos. Pero si Zimbra está instalado en varios servidores en su organización, entonces tendrá que prever la utilización de los demás puertos como el 25, 80, 110, 143, 443, 465, 587, 993, 995, 3443, 5222, 5223, 7071, 9071. Tal conjunto de puertos abiertos para la conexión asegurará la interacción normal entre servidores. A continuación, se presentan varias alternativas de solución mediante firewall.

Configurar Zimbra Firewall mediante UFW

Debido a los ataques recientes contra puertos UDP, no se recomienda habilitar el puerto UDP de Memcache en el firewall: puerto 11211/udp. Solo se dejará abierto el puerto TCP, que está a salvo de estos ataques. Para la configuración de puertos, se deben seguir los siguientes pasos:

1. Crear un perfil de aplicación para UFW llamado Zimbra:

```
$ sudo vim /etc/ufw/applications.d/zimbra
```

2. Agregar el siguiente comando:

```
[Zimbra]
title=Zimbra Collaboration Server
description=Open source server for email, contacts, calendar, and more.
ports=22,25,80,110,143,161,389,443,465,514,587,993,995,7071,8443,11211/tcp
```

```
[Zimbra]

title=Zimbra Collaboration Server

description=Open source server for email, contacts, calendar, and more.

ports=22,25,80,110,143,161,389,443,465,514,587,993,995,7071,8443,11211/
tcp
```

3. Habilitar perfil de aplicación en ufw

```
$ sudo ufw allow Zimbra

$ sudo ufw enable
```

4. Agregar el puerto ssh también.

```
$ sudo ufw allow ssh
```

Nota: En caso de cambiar el perfil de Zimbra, se debe actualizar con los siguientes comandos:

```
$ sudo ufw app update Zimbra

Rules updated for profile 'Zimbra'

Skipped reloading firewall
```

5. Para una instalación de un solo servidor, Memcache no se utiliza fuera del servidor local. Considere la posibilidad de enlazarlo a la dirección IP de bucle invertido (*loopback*). Utilice los siguientes comandos para ello:

```
$ sudo su - zimbra

zmprov ms zmhostname zimbraMemcachedBindAddress 127.0.0.1

zmprov ms zmhostname zimbraMemcachedClientServerList 127.0.0.1
```

6. A continuación, reiniciar el servicio Memcached.

```
$ sudo su - zimbra -c "zmmemcachedctl restart"
```

Configurar Zimbra Firewall usando Firewalld

1. Confirmar que el firewall está en estado de ejecución.

```
$ sudo firewall-cmd --state running
```

2. Si no se está ejecutando, inícielo usando.

```
$ sudo systemctl start firewalld
```

3. Configurar los puertos y servicios de Zimbra en el firewall.

```
$ sudo firewall-cmd --add-service={http,https,smtp,smtps,imap,imaps,pop
3,pop3s} --permanent

$ sudo firewall-cmd --add-port 7071/tcp --permanent

$ sudo firewall-cmd -add-port 8443/tcp --permanent
```

4. Recargar la configuración de firewall

```
$ sudo firewall-cmd --reload
```

5. Confirmar la configuración de tiempo de ejecución mediante los comandos:

```
$ sudo firewall-cmd --list-all

public

target: default
```

```
icmp-block-inversion: no

interfaces:

sources:

services: dhcpv6-client http https imap imaps pop3 pop3s smtp smtps snm
p ssh

ports: 7071/tcp  8443/tcp

...
```

Restricción específica del acceso al panel de administración

- Se recomienda, restringir siempre el acceso al puerto 7071 (*admin console*) a una red o dirección IP de confianza. Para UFW, esto se hace usando el comando:

```
$ sudo ufw allow from 192.168.1.10 to any port 7071

$ sudo ufw allow from 192.168.1.0/24 to any port 7071
```

- Con firewalld, puede usar Reglas enriquecidas.

```
$ sudo firewall-cmd --permanent --zone=public --add-rich-rule 'rule fam
ily="ipv4" \

source address="192.168.1.10/32" port protocol="tcp" port="7071" accept
'

$ sudo firewall-cmd --reload
```

Buenas prácticas en ciberseguridad

Con el fin de fortalecer el estado general de la ciberseguridad de las organizaciones, el CERT-PY ha adoptado un marco de mejores prácticas de ciberseguridad, en el cual se detalla la gestión de los puertos lógicos expuestos a internet, específicamente en el control CIS Control 9: Limitación y control de puertos de red, protocolos y servicios.

Referencias:

- https://www.alitajran.com/disable-external-access-to-ecp-exchange/#h-conclusion
- https://www.codetwo.com/admins-blog/how-to-disable-external-access-to-ecp/
- OfficeDocs-Exchange/disable-exchange-admin-center-access.md at public · MicrosoftDocs/OfficeDocs-Exchange · GitHub
- Restringir acceso al panel ECP en Exchange Server 2013 - Blog de Cenabit
- https://computingforgeeks.com/zimbra-firewall-configuration-ufw-ubuntu-firewalld-centos/
- https://www.tecmint.com/block-ssh-and-ftp-access-to-specific-ip-and-network-range/
- https://forums.zimbra.org/viewtopic.php?t=67028
- https://wiki.zimbra.com/wiki/Firewall_Configuration
- https://blog.zimbra.com/2022/06/update-on-june-2022-zimbra-patch-release/
- https://github.com/MicrosoftDocs/OfficeDocs-Exchange/blob/public/Exchange/ExchangeServer/about-documentation/exchange-admin-center-keyboard-shortcuts.md