Comunicaciones y Redes 2022

TRABAJO PRÁCTICO N°5 (UNIDAD N°5)

# Archivo de respuestas

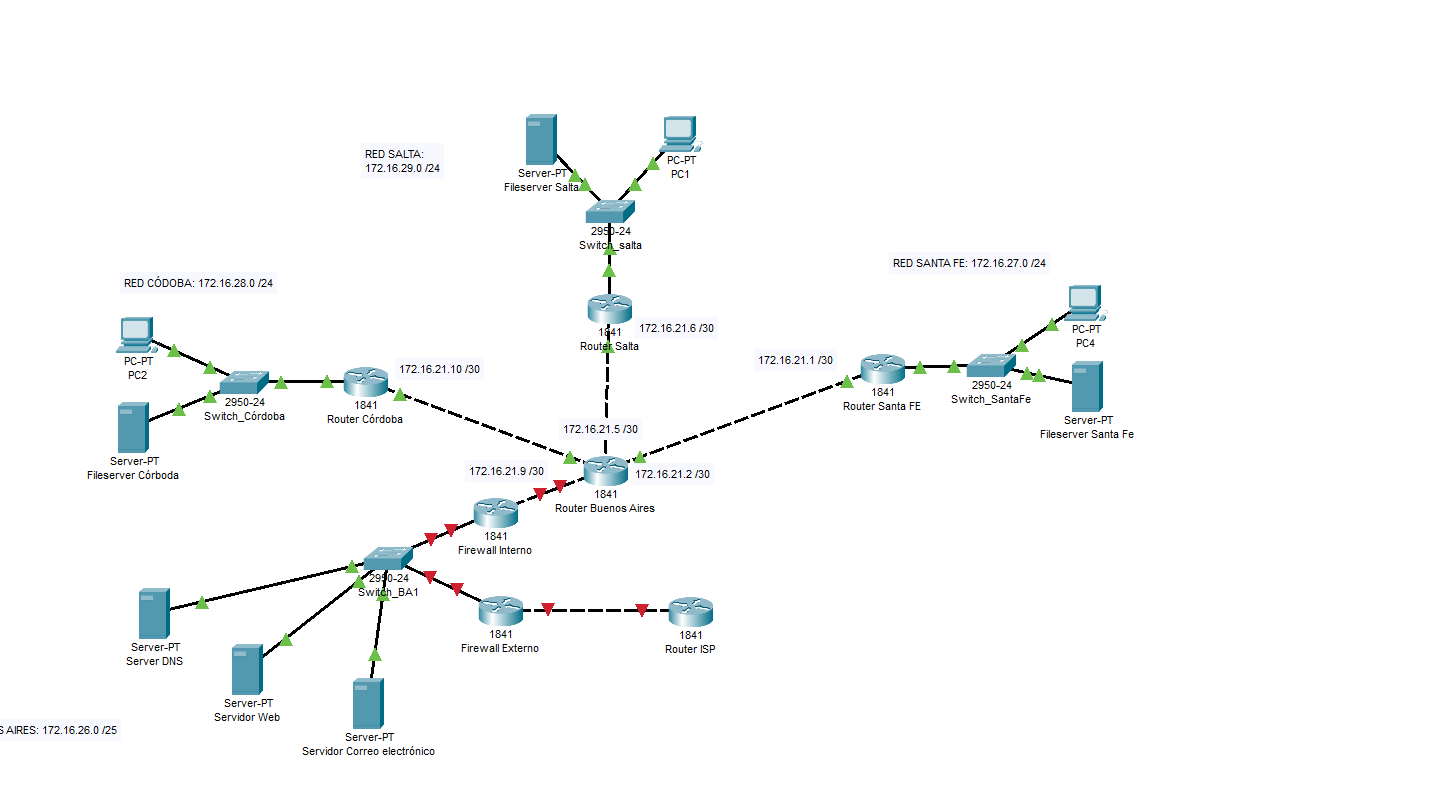
# Equipo de trabajo

|  |  |
| --- | --- |
| Apellido, Nombre | Legajo Nº |
| De Bonis, Esteban |  |
| Mosmann, Juan Ignacio |  |
| Tamborini Criscueli, Agustín Ariel | 168012-2 |

# Diseñar una solución de firewall

Para proteger todo el tráfico de red que pasa por la sede de Buenos Aires vamos a tener que implementar dos Firewalls ubicados entre el “Router Buenos Aires” (que nos comunicará con el resto de la red interna) y el “Router ISP” (que nos proporcionará acceso a internet y mediante el cual ingresará tráfico de red). De esta forma, todos los servidores de la sede junto con su correspondiente Switch quedarán en una zona desmilitarizada (DMZ), garantizándoles protección tanto de la red externa como de la red interna y brindando la oportunidad a la organización de definir políticas por separado.

En el enunciado nos aclara que el consumo máximo de red obtenido fue de 0.4 Gbps (400 Mbps). Por este motivo optamos por elegir el Firewall Check Point 1450, ya que el rendimiento del firewall por si mismo es de 1.1 Gbps y alcanza un rendimiento de prevención de intrusiones (IPS) de 225 Mbps. Tomando ambas métricas funcionando en conjunto con el control de aplicaciones alcanza un rendimiento de 210 Mbps; y si ponemos en funcionamiento detalles como filtrado de URL, Antivirus, Anti Bots y la funcionalidad de SandBlast ZeroDay Protection se alcanza un rendimiento de 150 Mbps. Creemos que con esos rendimientos podemos alcanzar un nivel de protección adecuado para las necesidades de la empresa planteadas en el enunciado. Además, cuenta con 6 puertos LAN más un puerto DMZ, por lo que tenemos la posibilidad de implementar nuevas sedes a futuro (o nuevos módulos de la red interna) sin necesidad de reemplazar el Hardware seleccionado.



# Diseñar listas de control de acceso (ACL)

Enunciar las reglas de la lista de control de acceso según el escenario planteado en el punto 2 (2.1 a 2.5) (agregar las filas necesarias según la cantidad de reglas)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Origen[[1]](#footnote-1) | Destino[[2]](#footnote-2) | Protocolo[[3]](#footnote-3) | Puerto | Acción[[4]](#footnote-4) |
| Cualquiera | 172.16.26.5/25 | UDP | 53 | Aceptar |
| Cualquiera | 172.16.26.6/25 | TCP | 25 | Aceptar |
| Cualquiera | 172.16.26.6/25 | TCP | 110 | Aceptar |
| Cualquiera | 172.16.26.6/25 | TCP | 995 | Aceptar |
| Cualquiera | 172.16.26.6/25 | TCP | 587 | Aceptar |
| Cualquiera | 172.16.26.7/25 | TCP | 80 | Aceptar |
| Cualquiera | 172.16.26.7/25 | TCP | 443 | Aceptar |
| (172.16.26.110/25: 172.16.26.120/25) | Cualquiera | TCP | 3389 | Aceptar |
| Cualquiera | Cualquiera | TCP | \* | Denegar |
| Cualquiera | Cualquiera | UDP | \* | Denegar |

1. Opciones: Ip, (Ip1, Ip5, Ip6), (Ip1:Ip6), Cualquiera [↑](#footnote-ref-1)
2. Opciones: Ip, (Ip1, Ip5, Ip6), (Ip1:Ip6), Cualquiera [↑](#footnote-ref-2)
3. Opciones: TPC, UDP [↑](#footnote-ref-3)
4. Opciones: Aceptar, Denegar [↑](#footnote-ref-4)