

Examen Redes

P1: Red Fisica

1. Si bien esta es la opcion mas economica, no mejora realmente la seguridad de la red wifi existente.
2. Esta opcion es un poco mas costosa, pero ofrece un poco mas de seguridad (aunque no significativa) a diferencia de la opcion 1, la diferencia y problema es que hay que adaptar todas las oficinas para que funcionen con cable ethernet y por lo mismo esto puede dificultar el uso de dispositivos los cuales no cuenten con puertos de ethernet, lo cual puede no ser tan buena opcion. Esto implicaria o cambiar los dispositivos que no cuenten con este puerto o hacer adaptaciones a los puertos para que se puedan conectar, ambas opciones requieren de mas inversion aparte de los 1000 \$USD
3. Del mismo modo que la opcion anterior, esta brinda una capa mas de seguridad, pero sigue teniendo el problema de los puertos de ethernet, lo cual puede ser una buena opcion pero quizas un poco cara. Aunque la encriptacion si es una opcion mucho mas confiable que solo usar el cable ethernet.
4. Por ultimo, ocupar WPA3 es una muy buena opcion, igual de cara que la anterior, pero permite el uso de wifi, lo cual es una gran mejora. Ademas WPA3 tiene un sistema de autenticacion y usa encriptacion de datos individualizados, para asi tambien proteger la comunicacion inalambrica. Lo cual haria que sea una opcion mas afin que la propuesta 3 ya que esta solo tiene la encriptacion del cable ethernet, siendo menos flexible. Fuerte ante ataques de fuerza bruta.

Finalmente, me decanto por elegir la opcion 4, si bien es cara, es segura, comoda y flexible. Usamos 10.000 \$USD.

P2: Redes IP

1. Esta opcion no creo que sea realmente viable, si bien se pueden tratar en otros niveles, no descarta que estos puedan ser comprometidos.
2. El tener una VPN con IPsec proporciona una capa adicional de seguridad, ya que solo se permitiria acceso a la app y servidores a traves de esta. Esta opcion ofrece una mayor proteccion a la red corporativa.

3. Esta opcion restringe el trafico, dando seguridad al filtrar y controlar el trafico de la red. Esta opcion es mas complicada de implementar ya que al tener varios dispositivos conectados a la red, es posible que haya una sobrecarga en esta, pero esto se puede optimizar para que no suceda esto.
4. Si bien esta opcion no es costosa y proporciona cierta seguridad a los dispositivos, y como vimos en la T3, esta solucion no es suficiente, es mejor que no tener nada pero aun asi carece de la seguridad necesaria. La ocuparia, pero no unicamente.
5. La alternativa mas cara, la cual analiza todo el trafico que entra y sale, lo cual permite que se identifiquen las posibles amenazas y ataques.

La opcion que yo eligiria en base a lo anterior seria optar por implementar el VPN(2) y la IPv4 y 6, con un costo total de 20.000 \$USD

P3: Transporte

1. Dejar la conexion directa con TCP no puede ser una opcion, ya que en la informacion que se transmite entre la app y los servidores no estaria protegida.
2. Usar solo TLS para tener conexión autenticada y encriptada entre la app y los servidores es una buena opcion a la hora de tener la conexion entre la app y los servidores, dejando asi los datos sensibles de la oficina seguros y sabiendo que no fueron interceptados.
3. Esta es una opcion bastante complicada, ya que implica desarrollo de un protocolo de transporte con encriptacion y seguridad adicionales. Si bien esta opcion puede llegar a brindar control, pero implica riesgos a asociados a la implementacion que se haga, ademas de requerir mas tiempo y conocimientos.

En fin, se elige la opcion 2, ya que es la que mayor seguridad brinda. Costo: 10.000 \$USD

P4: Protocolo/Aplicacion

1. Usar esta opcion es valida en este caso, ya que la seguridad si se aborda en los otros niveles, ademas no tiene costo y no implica tener que adaptarse a un nuevo protocolo.
2. Esta alternativa es mucho mas cara, pero no creo que tenga mucho sentido desarrollarlo desde 0, ademas de que presenta mas riesgos asociados a la implementacion y puede requerir recursos extras. Otro tema importante es que

a la hora de usar encriptacion no es tan simple como llegar e inventar, se tiene que poner a prueba, ademas que tener un protocolo que la comunidad no conoce y no ha testeado puede llevar a peligros como un zero-day-vulnerability, colocando en riesgo la seguridad e integridad de la red.

En conclusion se toma como mejor opcion la 1.

P5: Diseño Servidor

1. Si bien esta es la opcion mas economica, podria implicar limitaciones en terminos de escalabilidad y estabilidad.
2. Usar los procesos pesados tiene como beneficio que se le asigna un proceso a cada app, logrando asi un mayor aislamiento entre las aplicaciones, mejorando estabilidad, no obstante, podria llegar a requerir mas recursos de memoria y procesamiento para su uso.
3. Usar multiples servidores usando procesos pesados implicaria lo mismo que en la opcion anterior pero con una mayor escalabilidad y capacidad de carga, pero es una opcion mas cara por el hecho de tener que comprarlos y mantenerlos en el tiempo.
4. Usar multiples servidores usando threads, a diferencia de la opcion anterior, esta puede llegar a requerir menos uso de recursos en terminos de memoria y procesamiento.
5. Usar la nube dinamica de Amazon con multiples servidores, con procesos pesados. Esta opcion permite escalabilidad y flexibilidad sin tener que invertir ni mantener los servidores propios.
6. Usar la nube dinamica de Amazon con multiples servidores, con threads, tiene similares caracteristicas a la opcion anterior, pero a su vez requiere de menos recursos de memoria y procesamiento.

La opcion escogida es usar la numero 6, ya que es mas barata y proporciona escalabilidad y flexibilidad. Aparte de que la seguridad esta respaldada por Amazon.

Presupuesto usado:45000

Bibliografia

- Chatgpt
- BingChat

- WPA3: qué características y ventajas tiene (wikiversus.com)
- ¿En qué se diferencia la seguridad WiFi WPA3 de WPA2? (xataka.com)
- ¿Qué es Amazon EC2? - Amazon Elastic Compute Cloud
- ¿Qué es AWS? (amazon.com)
- ¿Qué es el almacenamiento en la nube? - Explicación del almacenamiento en la nube - AWS (amazon.com)