Teoría de las comunicaciones

Práctica 9: Seguridad

Temas

Criptografía simétrica y asimétrica, Firma Digital, Certificados, Conexiones Seguras, Firewalls

Definiciones

DMZ: Zona demilitarizada de la red. Tipicamente ubicada en la **frontera** de la red interna.

Mensaje: M

Criptograma: C

Digesto: D

Clave simétrica: K

Clave pública de Alice: K_A^+

Clave privada de Alice: K_A^-

Encriptar M utilizando la clave Q: $E_Q(M) = C$ con $Q \in \{K, K_A^+, K_A^-\}$

Desencriptar el C utilizando la clave Q: $D_Q(C) = M$ con $Q \in \{K, K_A^+, K_A^-\}$

Aplicar Función de Hash Criptográfico: $FHC(M) = D$

Aclaración: La notación permite combinar cada algoritmo con cada tipo de clave para obtener distintos resultados. No todo algoritmo permite toda clave. Deberá aclararse qué algoritmo es el utilizado.

Ejercicio 1

Del siguiente criptograma se conoce que las letras fueron encriptadas usando un cifrado *César*.

```
pm fvb aopur aljouvsvnf jhu zvscl fvby zljbypaf
wyvisltz, aolu fvb kvua buklyzahuk aol wyvisltz
huk fvb kvua buklyzahuk aol aljouvsvnf.
--iybjl zjoulply
```

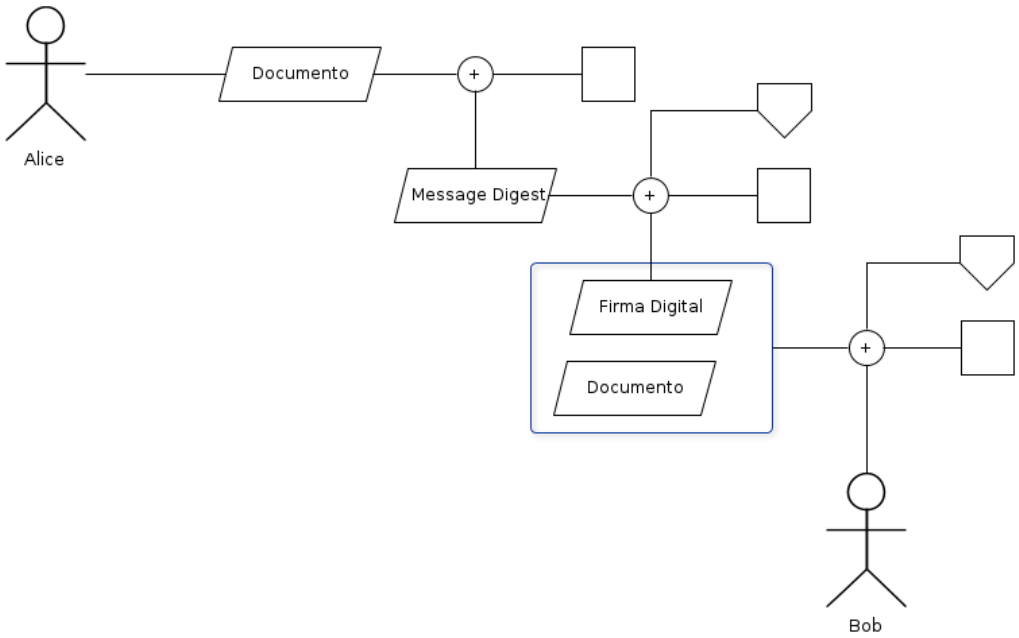
Describa una estrategia que se pueda usar para descubrir el desplazamiento.

Asumir: que el texto original contenía letras sin tildes

Ejercicio 2

Alice desea enviarle un mensaje a Bob de carácter importante. Ella quiere asegurarse de que nadie excepto Bob (incluida Trudy) pueda leerlo y que Bob pueda confiar en que el emisor es Alice.

Diseñe una solución que garantice las propiedades de Confidencialidad y No repudio.



Aclaración: Completar los cuadrados con algoritmos y las casitas con los parámetros adicionales que estos toman.

Ejercicio 3

Dado un algorítmo de clave pública (e.g.: RSA):

a. Muestre una comunicación entre Alice y Bob utilizando clave pública para garantizar confidencialidad.

b. Suponga que Trudy puede situarse en el medio de la comunicación (ie: MiTM), ¿qué podría hacer para violar la confidencialidad de la comunicación?

c. Explique qué información le faltaría a la clave pública para resolverlo.

Ejercicio 4

Certificados digitales

1. ¿Qué piezas de información contiene un certificado digital? **Ayuda:** openssl s_client www.dc.uba.ar:443.
2. Utilizando openssl genere un certificado digital para un hostname llamado $CNAME$ y muestre qué problemas acarrea. **Ayuda:** openssl req.
3. Se sabe que ssh admite autenticación por clave pública y privada además del método de challenge-response. Exiba un método para generar la clave y otro para habilitar la utilización de ella. **Ayuda:** Google.

Ejercicio 5

Muchos protocolos para establecer conexiones seguras usan handshakes para iniciar el sistema criptográfico. En este ejercicio tenga en mente SSL/TLS como sistema criptográfico a analizar.

a. De los siguientes parámetros indique la etapa del algorítmo donde se utiliza: $HELLO$, $Key-Exchange$ o $Data-sharing$.

- Parámetros Criptográficos
- Valor al azar
- Conjunto de Algoritmos de encripción
- Versión Protocolo
- Certificado del destinatario (Peer)
- Clave Maestra (Masterkey)
- Criptograma

b. Muestre mediante un diagrama de secuencia una posible implementación de un handshake para establecer una conexión. Considere los mensajes enviados, y si se envian en plano o como criptogramas. En cada caso especificar.

Ejercicio 6

El protocolo TLS es ampliamente utilizado para proteger conexiones HTTP en Internet.

a. Muestre las propiedades que garantiza el protocolo aplicado a los siguientes protocolos:

	Confidencialidad	No repudio	Integridad
SMTP			
IMAP			
HTTP			

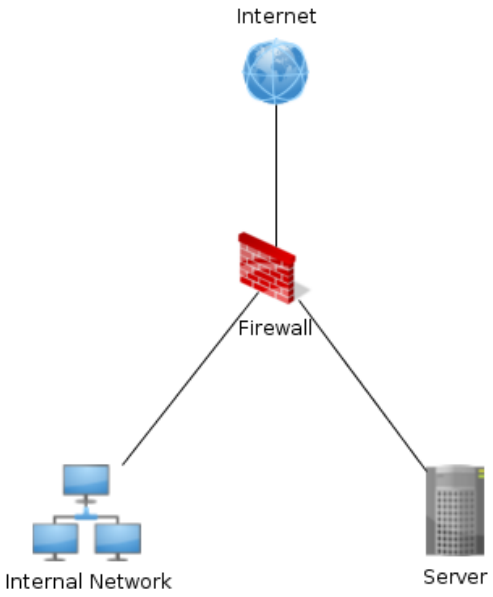
b. Clasifique los siguientes conceptos según los atributos que brinde a una comunicación.

	Confidencialidad	No repudio	Integridad
Firma digital			
Criptografía simétrica			
Certificados digitales			
Message-digest			

c. Explique cómo se relacionan los conceptos con los algorítmos criptográficos aplicados en TLS.

Ejercicio 7

El siguiente es un diagrama de una topología de la red interna de la compañía **Siliconsec**:



Donde los sevicios provistos por **Server** son:

- Webserver y HTTP Proxy
- Resolver autoritativo de dominio
- Correo saliente y entrante

Configure el Firewall de tal manera que todos los servicios se encuentren disponibles para internet pero que los usuarios pertenecientes a la red local puedan:

- Acceder a internet vía proxy
- Leer y enviar correos

Ejercicio 8

El gerente de sistemas de la empresa Garbagerino se encuentra en viaje de negocios. Durante su estadía desea conectarse a los servicios de red que acostumbra (e-mail, facebook, chat) desde el lobby del hotel. Al preguntar la contraseña de dicha red, el empleado le informa que es una red wireless sin encripción.

a. Identifique que problemas puede traer para nuestro gerente.

b. Muestre y explique los comandos para generar un tunel sobre SSH de tipo Local.

c. Al generar el tunel, el gerente observa el siguiente mensaje:

```
   ssh gerente-capo@garbagerino.com
The authenticity of host 'garbagerino.com (156.93.26.2)' can't be established.
RSA key fingerprint is 5a:23:ba:45:e4:b2:24:bc:02:f8:ed:bc:46:73:73:36.
```

```
Are you sure you want to continue connecting (yes/no)?
```

¿Cómo podría verificar la identidad del servidor?

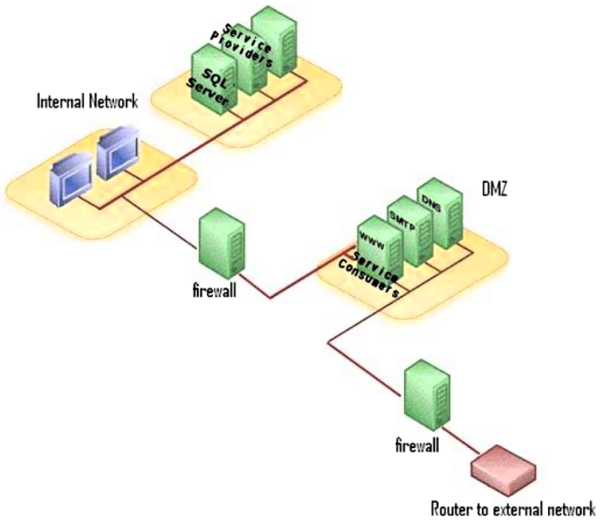
Ejercicios de Parcial

Ejercicio 9

Nos presentan la topología de red de la figura y nos dan la responsabilidad de definir y configurar las reglas de filtrado. El firewall externo tiene un módulo que chequea los correos que pasan por él y en caso de encontrar virus los filtra. El chequeo de virus se realiza sobre las partes Mime. Se pide:

a. Indicar todas las reglas necesarias que permitan el correcto funcionamiento de la red. Se debe poder:
   - Acceder a Internet desde las red interna.
   - Descargar mails desde la red interna.
   - Acceso universal a la DMZ.
   - Interactuar de forma segura con el servidor web.

b. Un nuevo requerimiento de seguridad indica que todos los mails pasarán a ser enviados de manera cifrada. La técnica que se eligió para realizar esto es enviar SMTP normal pero sobre la capa de TLS para modificar lo menos posible las tecnologías existentes. Sin embargo, la política de verificar el virus de todos los mails sigue siendo obligatoria. ¿Cómo repercute esta nueva norma en la verificación de los virus? En caso de requerirse algún cambio para mantener la política indíquelo.



Ejercicio 10

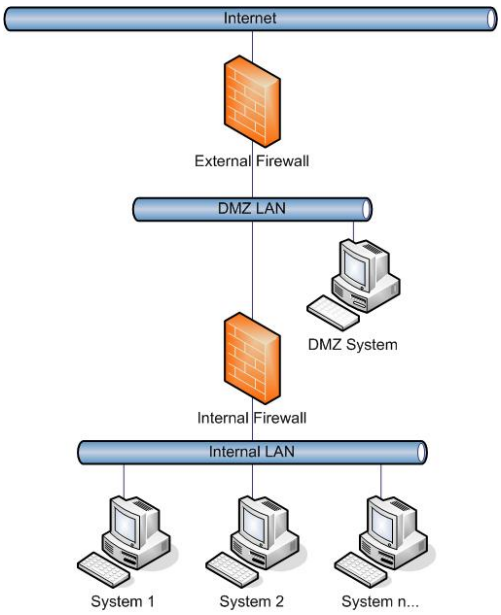
Nos contratan para diagramar la red de una empresa. Se especifica que la red contará con unas 50 máquinas aproximadamente, para los empleados, donde es crucial mantener los mayores niveles de seguridad posibles. A estos hosts solo se les permite el acceso a internet para usar la web y la web en versión segura. Además, la empresa posee un servidor SMTP de donde salen y llegan los mails del dominio de la empresa y desde donde los hosts de los empleados deben poder descargar sus mails. Por último, se especifica que dentro de la red se debe hostear un servidor de DNS con la información del dominio. Se pide:

a. Exponga un esquema de como diagramaría usted la red sabiendo que se cuenta con fondos para comprar un solo firewall del tipo que se desee. Explicite direccionamiento, tipo y reglas de firewall.

b. En el momento de implementar la red se decidió dar soporte para que el protocolo de descarga de mails use la capa de TLS para comunicarse con sus clientes. ¿La propiedad de integridad sobre los correos desde el server hasta los hosts está asegurada por esta capa?. En caso de responder afirmativamente a la pregunta, describa un mecanismo que se use para este fin.

Ejercicio 11

Una organización desea usar un sistema de firewall para proteger sus instalaciones con la topología que se presenta en la figura. El servidor en la DMZ ofrece los siguientes servicios



- Web. (seguro y no seguro)
- Mail. (saliente y entrante para la organización)
- DNS. (es resolver y además autoritativo de la zona)

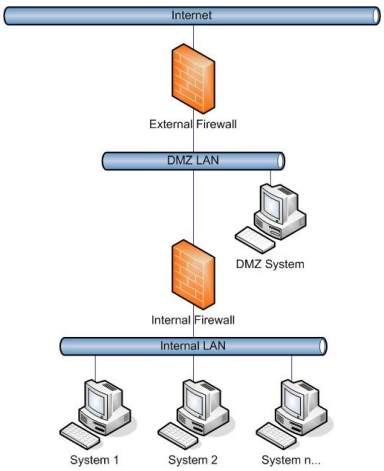
Desde la red interna solo está permitido acceder a los servicios de la DMZ y a un servidor externo (con IP conocida en internet). Por último se conoce que la compañia posee solamente un firewall de tipo stateful y varios stateless.

a. Detalle como organizar y configurar los firewalls de manera de cumplir con la política enunciada.

b. Pasado un tiempo se desarrollo un servicio web seguro (HTTPS) en el servidor externo para asegurar confidencialidad. Además, requiere autenticidad del lado de la organización (cliente). Disponiendo solamente de un certificado de la organización validado por una CA, proponga un esquema para lograr que los pedidos de la organización cumplan con los requerimientos de autenticidad.

Ejercicio 12

Dada la topología de red de la figura nos dan la responsabilidad de configurar los firewalls de la misma. Se sabe que en el segmento DMZ hay un servidor web que debe ofrecer



- Web. (seguro y no seguro)
- Mail. (saliente y entrante para la organización)
- DNS. (es resolver y además autoritativo de la zona)

Además, en la zona DMZ hay otro servidor con una base de datos. Desde la red interna se debe descargar el contenido del mismo todos las noches para tener una copia segura del mismo. Esto se hace con un servicio de replicación corriendo sobre un puerto conocido. Desde el exterior no se debe poder acceder a este servidor. Los hosts de la red interna deben tener permitido acceder a todos los servicios de la DMZ solamente.

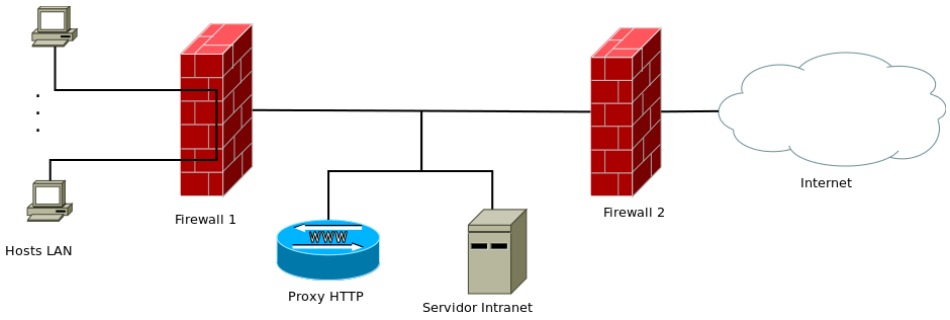
a. Indicar todo lo necesario respecto a los firewalls y explicitar las configuraciones correspondientes para el correcto funcionamiento de la red dada la política enunciada. Explicitar todas las asunciones que se hagan.

b. Es recurrente en la empresa que ocurran peleas internas entre los empleados endilgandose la responsabilidad por tareas no realizadas. Por lo tanto se pide implementar algún mecanismo para garantizar la propiedad de NO REPUDIO en todos los mensajes que se mandan internamente. Describa un mecanismo posible para lograr el requerimiento.

Ejercicio 13

La empresa Sinegociamostegarco diseñó un nuevo esquema de seguridad para la red interna colocando los servicios accedidos desde internet en una DMZ. Ésta cuenta con el servicio de intranet (sobre HTTP) para que los empleados

carguen las horas y tareas en las que fueran esclavizados cada mes y un Proxy HTTP para resolver los recursos HTTP provenientes de la intranet.



Sin embargo no es clara la política de seguridad que tiene la empresa y por eso se pide:

1. Configurar ambos firewalls teniendo en cuenta que el servidor Proxy también es el *DNS Resolver*.
2. Establecer un criptosistema para garantizar la autenticidad del Proxy y del servidor de la intranet. Enumere los elementos utilizados y explique cómo esta solución impide ataques de *Man in the middle*. Si hacen falta cambios en las tablas de firewalling.

Bibliografía

Computer Networks: A systems approach. 5ta Edición. *Peterson & Davie.* Capítulo 8: Network Security.