Pontificia Universidad Católica Madre y Maestra

Campus: Santo Tomás de Aquino

Departamento de Ingeniería

Diseño de Sistemas

Rediseño del internet

Javier Falcón (2016-5265)

Santo Domingo, 07/12/2018

Contenido

Problemas principales del internet.

Es interesante concebir la idea de que una de las invenciones más importantes en la historia de la humanidad haya sido diseñada contemplando todo menos la seguridad. Los creadores del internet han asegurado que el diseño de su arquitectura debía cuidarse de ataques militares, pero nunca creyeron que los mismos usuarios del internet podrían, algún día, llegaran a atacarse entre sí usando la red. A raíz de esto, surge una interrogante bastante interesante: ¿Podemos agregar seguridad a algo que no fue pensado para ser seguro? Ha sido difícil, pero se ha logrado de lograr mecanismos que reduzcan el riesgo.

Una de las vulnerabilidades que más críticas recibe es el hecho de que los protocolos son frágiles. Esto puede observarse en los tipos de ataque de *Denial of Service* o *Botnet.* Estos ataques se encargan de explotar la capa de transporte, la cual está interna en el protocolo TCP/IP, por lo que uno de los puntos de refuerzo está dentro de ese ambiente.

- Problemas de seguridad: entre los problemas de seguridad está la infestación de worms para crear botnets. Muchas veces consiguen acceder a las listas de rutas de los protocolos BGP y, con las direcciones IP robadas, intentar abrir conexiones hasta que alguna se abra y ellos puedan infectar el dispositivo con worms.
- Problemas de SPAM: los hackers, con herramientas automatizadas, logran conseguir dominios de correo y los bombardean de mensajes hasta que se fuerza al receptor a recibirlos.
- Problemas de SYN-flood attacks: uno de los ataques más comunes son los intentos de *Denial of Service*, en los cuales se intentan abrir conexiones masivas en un servidor y no se le responde con el mensaje de ACK, dejando al servidor esperando por confirmación y ocupando puertos hasta que no puede procesar más solicitudes y deniega el servicio a las conexiones lícitas.

Descripción del diseño de solución.

En vista de que una gran parte de los ataques explotan el protocolo TCP/IP, mi solución se basa en un rediseño de este protocolo, a través de la adición de una nueva capa denominada ***Monitoring layer.*** Esta nueva capa se encargará de hacer análisis de los paquetes, capturándolos y guardándolos temporalmente para tenerlos preparados para la siguiente fase. Allí se extrae información de los headers del paquete para poder analizar de dónde vienen y hacia dónde van. El objetivo de esto es poder detectar ataques de SYN-flood, utilizando un *bucket* que almacenará las cantidades de solicitudes de paquetes SYN y decrementará su número cuando el servidor reciba el paquete con tag ACK. De esta manera, si llega una gran cantidad de solicitudes SYN y no son liberadas, se detectará un ataque y se registrará su patrón.

Escenarios:

1) Un atacante que controla un botnet intenta generar un ataque de SYN-Flood por segunda vez. Se utiliza como artefacto la capa de transporte del protocolo TCP/IP en tiempo normal de operación. La capa de monitoreo reconoce el patrón y rechaza las solicitudes. El servidor sigue respondiendo las solicitudes válidas.
2) Un atacante intenta robar las listas de rutas del protocolo GBP que almacena el ISP. Utiliza las direcciones en las rutas como artefacto en tiempo normal de operación. El certificador de llaves de cliente lo reconoce como no seguro y lo rechaza.

Documentación del diseño:

- **Diagrama de estructura modular:**

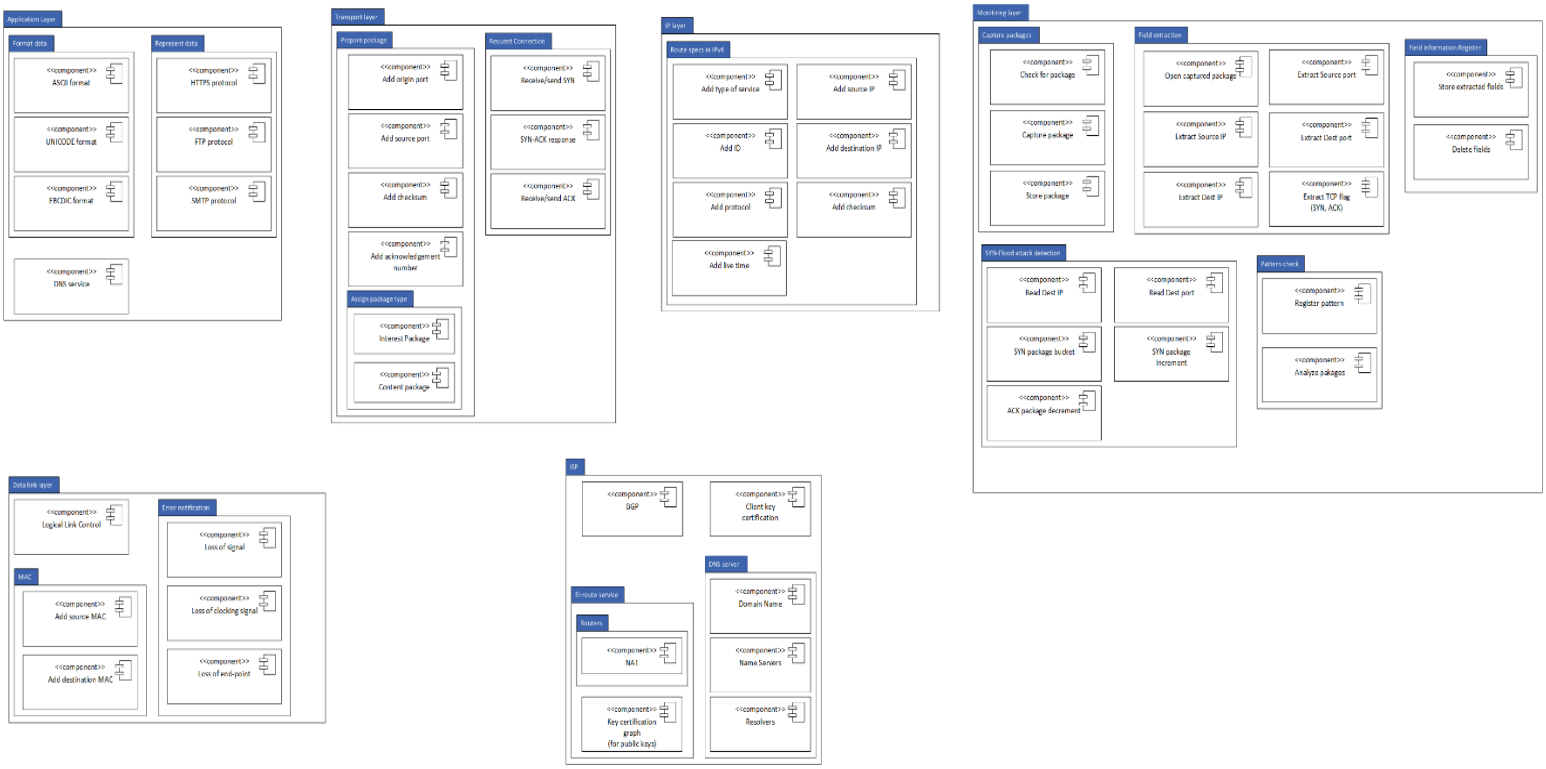
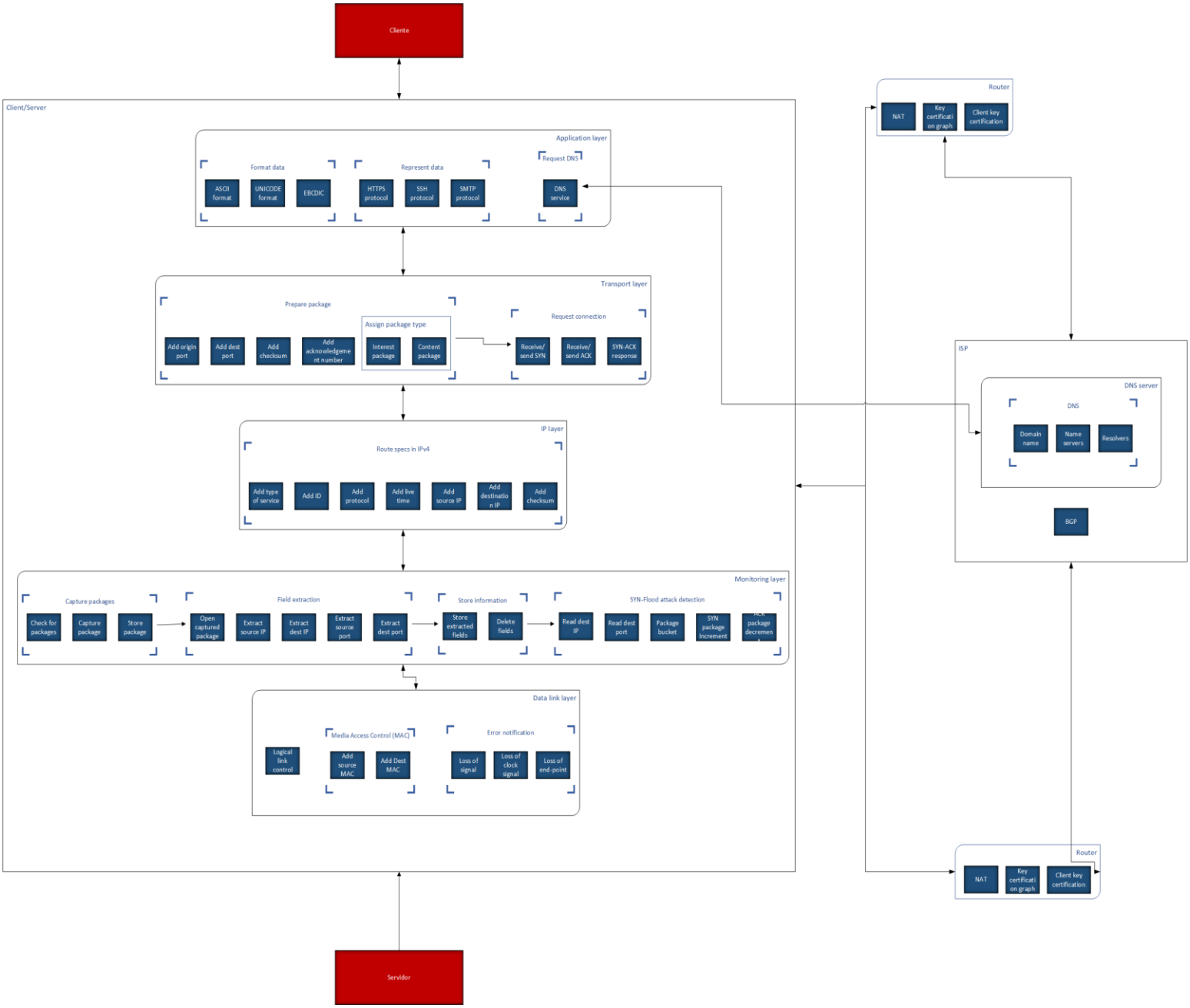


Diagrama de Componentes y Conectores



- Diagrama de despliegue: