Redes de Computadores INF-256
Experiencia 3
Informe Previo

Fabrizio Ogalde 201585008-9
Branco Catalan 201354028-7

25 de agosto de 2019

1. El firewall es un software o hardware que es utilizada para controlar las comunicaciones que tengan las máquinas con la red de internet. Se basa en reglas establecidas (o generalmente predeterminadas) que indican las acciones a tomar (bloquear, cifrar, descifrar, entre otros) información entrante o saliente de la red/equipo.

   En grandes compañías o empresas se utilizan generalmente firewall de hardware. Este dispositivo evita que usuarios no autorizados tengan acceso a la red privada sobre la que trabaja el firewall. Los mensajes son examinados por el firewall (entrantes y salientes) y si no cumple con las reglas que estableció la empresa, lo bloquea e impide que pase. Su importancia es entonces proteger la red de agentes externos que sean sospechosos.

2. ACL o Access Control List son filtros de red usados por routers y algunos switches que permiten o restringen el flujo de información desde o hacia una interfaz de red. En una red con el ACL configurado, este analiza la información que pasa a través de la interfaz, comparando con el criterio establecido en la ACL y así permitiendo o prohibiendo su paso.

   Son importantes para proveer cierta seguridad en la red en interfaces que tienen una relativa alta velocidad donde los firewalls pueden ser un poco más restrictivos.

   Existen dos tipos de ACL:

   - Standard Access list: son los ACL creados solo usando la dirección IP fuente. Estas permiten o niegan todo el conjunto de protocolos. No distinguen entre TCP, UDP, entre otros.
   - Extended Access list: estas usan tanto la IP de destino como la IP fuente. También se puede especificar qué tipo de tráfico IP debe ser permitido y negado.

3. Las ACL simples sólo son capaces de evaluar las direcciones fuente, y denegar o permitir el tráfico según corresponda, es una configuración por defecto en muchos sistemas. Las ACL extendidas poseen muchos más parámetros, entre estos destacan:

   - **Direccion Fuente**: Mismo parámetro existente en ACL simple, evalua la dirección origen del segmento/datagrama.
   - **Dirección Destino**: Permite denegar segmento/datagramas dirigidos a alguna maquina específica de la red.
   - **Tipo de Protocolo**: Comprueba el protocolo de aplicación o transporte, permite filtrar en base a funcionalidades solicitadas (FTP, HTTP, SSH, etc).
   - **Puertos**: Comprueba puertos fuente y destino para protocolos tcp o udp, funciona con fines similares al filtro por dirección, pero restringido a los puertos de los host ya que estos tambien suelen responder por estándar a ciertos protocolos de aplicación (80 http, 22 ssh, etc).
   - **Opciones adicionales por protocolo**: En general cualquier *flag* o *meta-información* que se incluya en cabeceras.

   En varios sistemas que permiten gestionarlas es posible identificar a las ACL con nombres propios, o con números que definen rangos en sus parametros (1-99 y 1300-1999 para simples; 100-199 y 2000-2699 para extendidas)

4. Si, se pueden ser implementadas en routers.

   Las capacidades de una ACL son utilizadas por los Firewall para los filtros de tráfico en un determinado host, pero en general pueden ser usado para cualquier proposito relacionado al acceso/bloqueo de paquetes.

   Cuando se implementa en routers, además de servir para filtrar tráfico por completo a la red, tambien son útiles de forma distribuida para filtrar y gestionar actualizaciones de *routing*, y para listar y enrutar (no denegar completamente) tráfico entre maquinas de una red local.

Primera red

Para poder bloquear al host con ip 192.168.1.2 para cualquier acceso a través de la interfaz con ip 192.168.1.1 se utilizan los siguientes comandos:

- config terminal
  interface GigabitEthernet 0/0
  ip access-group 1 in
  access-list 1 deny host 192.168.1.2
  exit

Esto asegura que el host 192.168.1.2 no podrá obtener ningún tipo de acceso a través de la interfaz 0/0. Si se quisiera hacer lo mismo para el otro host, se realiza:

- config terminal
  interface GigabitEthernet 0/1
  ip access-group 1 in
  access-list 1 deny host 192.168.2.2
  exit