UNIMINUTO
Corporación Universitaria Minuto de Dios

John R. Correa

Administrador de Seguridad de la Información.

UNIMINUTO
Corporación Universitaria Minuto de Dios

Agenda

3. Implementando un servidor FIREWALL en IPv6.
3.1. Filtrado ICMPv6.
3.2. Instalación de paquetes necesarios para el servidor Iptables6.
3.3. Reglas básicas.

UNIMINUTO
Corporación Universitaria Minuto de Dios

3. Implementando un servidor Firewall en IPv6.

IPv6 Firewall

Tradicionalmente se han definido reglas de control de trafico en los dispositivos de control de acceso a los servidores

Las mejores practicas recomiendan de igual forma implementar estos controles en cada Servidor, apoyándose en los denominados HOST Firewall, iptables es uno de ellos.

Para el caso de IPv6 podemos mantener estas mejores practicas como punto de partida para la definición de los controles de acceso que se requieran.

La versión de iptables para IPv6 se llama ip6tables. Y su función es la de administrar el filtrado de paquetes IPv6.

UNIMINUTO
Corporación Universitaria Minuto de Dios

IPv6 Firewall

En Internet se puede conseguir gran variedad de politicas o recomendaciones de reglas de control para cada servicio que se publique, estas mismas son una opcion valida para usar en Ip6tables.

Pero debemos tener en cuenta que el protocolo IPv6 presenta algunas diferencias respecto a IPv4, por lo que algunas reglas presentan ciertas modificaciones.

El elemento mas critico en este grupo de diferencias es el protocolo ICMPv6.

UNIMINUTO
Corporación Universitaria Minuto de Dios

Filtrado de ICMPv6

En IPv4 es una practica común denegar el protocolo ICMP en las reglas de Firewall, para evitar algunos ataques que se ha presentado a través de este protocolo.

En un Firewall de Servidor a diferencia de IPv4, el protocolo ICMP en IPv6 (ICMPv6) juega un rol de alta importancia. Una red IPv6 no funcionara adecuadamente si no se permiten ciertos tipos de mensajes ICMPv6.

El RFC 4890 señala las "Recomendaciones de filtrado de Mensajes ICMPv6
en Firewalls“

Filtrado de ICMPv6

Se identifican 4 categorías de filtrado ICMPv6 para el filtrado en Servidores

A. Trafico que no debe eliminarse
B. Trafico que generalmente no debería eliminarse
C. Trafico que debe eliminarse
D. Trafico debe tener una política definida

Filtrado de ICMPv6

A. Trafico que no debe eliminarse
Address Configuration and Router Selection messages:

- Router Solicitation (Type 133)
- Router Advertisement (Type 134)
- Neighbor Solicitation (Type 135)
- Neighbor Advertisement (Type 136)
- Inverse Neighbor Discovery Solicitation (Type 141)
- Inverse Neighbor Discovery Advertisement (Type 142)

Link-Local Multicast Receiver Notification messages:

- Listener Query (Type 130)
- Listener Report (Type 131)
- Listener Done (Type 132)
- Listener Report v2 (Type 143)

UNIMINUTO
Corporación Universitaria Minuto de Dios

Filtrado de ICMPv6

SEND Certificate Path Notification messages:

- Certificate Path Solicitation (Type 148)
- Certificate Path Advertisement (Type 149)

Multicast Router Discovery messages:

- Multicast Router Advertisement (Type 151)
- Multicast Router Solicitation (Type 152)
- Multicast Router Termination (Type 153)

Filtrado de ICMPv6

Se identifican los tipos echo request (128) and echo response (129), ya que no deben eliminarse si se recomienda controlar cuantos de ellos se deben responder, para evitar un ataque DoS Cuando no se usa autoconfiguración stateless, porque usamos IPs fijas se puede considerar bloquear los mensajes 133 (RA) y 134 (RS), para no ir en contravía del RFC, se propone usar la política REJECT

En el encabezado ICMPv6 se usa el campo hop limit para contabilizar el numero de veces que un paquete ha sido enrutado (TTL en Pv4)

Basado en esto se puede usar este campo para permitir solo aquellos mensajes de cierto tipo que aun no hayan sido enrutados

UNIMINUTO
Corporación Universitaria Minuto de Dios

Filtrado de ICMPv6

B. Trafico que generalmente no debería eliminarse.

Mensajes de Error

- Time Exceeded (Type 3) - Code 1
- Parameter Problem (Type 4) - Code 0

Filtrado de ICMPv6

C. Trafico que debe eliminarse

- Router Renumbering (Type 138)

Mensajes de Movilidad Ipv6

- Home Agent Address Discovery Request (Type 144)
- Home Agent Address Discovery Reply (Type 145)
- Mobile Prefix Solicitation (Type 146)
- Mobile Prefix Advertisement (Type 147)

Mensajes en etapa experimental

- Seamoby Experimental (Type 150)

Filtrado de ICMPv6

D. Trafico debe tener una política definida

Redirect messages
- Redirect (Type 137)

Node Information messages
- Node Information Query (Type 139)
- Node Information Response (Type 140)

Error messages not currently defined by IANA:
- Unallocated Error messages
  (Types 5-99 inclusive and 102-126 inclusive)

3.2. Instalación de paquetes necesarios para el servidor Iptables6.

La instalación de ip6tables en CentOS-7X se realiza ejecutando el siguiente comando:

#yum -y install ip6tables

Establecer políticas por defecto para la tabla filter:

Se establecerá la política como política por defecto la eliminación de los paquetes IPv6 de entrada y salida, de tal forma que solo se permitirán los paquetes que explícitamente se identifiquen

ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
ip6tables -P OUTPUT DROP

UNIMINUTO
Corporación Universitaria Minuto de Dios

Limpieza de reglas Ip6tables

Se limpiaran las reglas actuales, de tal forma que solo se aplique la regla por defecto DROP

```
ip6tables -F INPUT
ip6tables -F FORWARD
ip6tables -F OUTPUT
ip6tables -F
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Se permitirá todo el tráfico para todos los protocolos siempre y cuando este se origine en la interfaz localhost ([::])

```
ip6tables -A INPUT -s ::1 -d ::1 -j ACCEPT
```

Permitimos solo aquellos mensajes ICMPv6 de entrada que permitan una operación correcta de la conectividad IPv6

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT
ip6tables -A INPUT -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
```

Reglas Básicas:

Para aquellos paquetes ICMPv6 de entrada que podrían presentar algún riesgo, pero que debemos mantener, los permitimos pero controlando su fuljo

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-request -m limit --limit 900/min -j ACCEPT

ip6tables -A INPUT -p icmpv6 --icmpv6-type echo-reply -m limit --limit 900/min -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Para aquellos paquetes ICMPv6 que se requieren para la comunicación en los link local, los permitimos siempre y cuando no hayan sido previamente enrutados

```
ip6tables -A INPUT -p icmpv6 --icmpv6-type router-advertisement -m hl --hl-eq 255 -j ACCEPT

ip6tables -A INPUT -p icmpv6 --icmpv6-type neighbor-solicitation -m hl --hl-eq 255 -j ACCEPT

ip6tables -A INPUT -p icmpv6 --icmpv6-type neighbor-advertisement -m hl --hl-eq 255 -j ACCEPT

ip6tables -A INPUT -p icmpv6 --icmpv6-type redirect -m hl –hl-eq 255 -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Todos los demás paquetes ICMPv6 de entrada podrán ser registrados antes de que sean descartados por la política para ICMPv6 DROP

```
ip6tables -A INPUT -p icmpv6 -j LOG --log-prefix "dropped ICMPv6"

ip6tables -A INPUT -p icmpv6 -j DROP
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Ahora permitimos los paquetes ICMPv6 de salida que el Servidor debe poder enviar hacia cualquier subred

```
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Los mensajes NDP hacia la red local deben ser permitidos

```
ip6tables -A OUTPUT -p icmpv6 –icmpv6-type neighbour-solicitation -m hl --hl-eq 255 -j ACCEPT

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type neighbour-advertisement -m hl --hl-eq 255 -j ACCEPT

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-solicitation -m hl --hl-eq 255 -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Antes de rechazar algunos paquetes ICMPv6 que pueden representar algún riesgo, los registramos y luego le aplicamos la política REJECT

```
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-advertisement
-j LOG --log-prefix "ra ICMPv6 type"

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type redirect -j LOG –log-
prefix "redirect ICMPv6 type"

ip6tables -A OUTPUT -p icmpv6 --icmpv6-type router-advertisement
-j REJECT
ip6tables -A OUTPUT -p icmpv6 --icmpv6-type redirect -j REJECT
```

Reglas Básicas:

Los demás paquetes ICMPv6 serán permitidos.

```
ip6tables -A OUTPUT -p icmpv6 -j ACCEPT
```

Agregamos las reglas que autoricen los paquetes de conexión al Servicio SSH

```
ip6tables -A INPUT -p tcp --destination-port 22 -j ACCEPT

ip6tables -A OUTPUT -p tcp –source-port 22 -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Agregamos las reglas que autoricen los paquetes de conexión al Servicio Servidor HTTP y HTTPS

```
ip6tables -A INPUT -p tcp --destination-port 80 -j ACCEPT

ip6tables -A OUTPUT -p tcp –source-port 80 -j ACCEPT

ip6tables -A INPUT -p tcp --destination-port 443 -j ACCEPT

ip6tables -A OUTPUT -p tcp –source-port 443 -j ACCEPT
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

Reglas Básicas:

Para salvar las reglas implementadas y garantizar que estas se apliquen al reinicio del servidor

```
service ip6tables save
```

Consultamos las reglas de control que están vigentes

```
ip6tables -L -nv
```

UNIMINUTO
Corporación Universitaria Minuto de Dios

GRACIAS