

que dispositivo podría incluir la funcionalidad de un firewall: router

Verdadero o falso: Cuando selecciono una Región del AWS debo considerar principalmente la distancia geográfica que existe entre mi empresa y la Región.
Falso la distancia es con los clientes.

Verdadero o falso: El load balancer de AWS solamente permite realizar el balanceo del puerto 80 (HTTP)

Falso. El load balancer de AWS permite realizar el balanceo del tráfico en diferentes puertos, incluidos el puerto 80 (HTTP), el puerto 443 (HTTPS), el puerto 25 (SMTP), el puerto 143 (IMAP) y el puerto 465 (SMTPS).

Verdadero o falso: El servicio de Elastic IP de AWS es un servicio que permite usar una dirección IP en diferentes instancias:

Verdadero. De forma predeterminada, todas las cuentas de AWS están limitadas a cinco (5) direcciones IP elásticas por región.

Una DMZ es:

- ☐ Es el segmento de red que se conecta directamente al Internet.
- ☒ Red que se ubica entre la red interna de una organización e Internet.
- ☐ Red interna de la organización.
- ☐ Es un segmento de red totalmente segura.

correcta es: b. Red que se ubica entre la red interna de una organización e Internet. Una DMZ (zona desmilitarizada) es una red que se ubica entre la red interna de una organización e Internet. Se utiliza para alojar servidores que están expuestos a Internet, como servidores web, servidores de correo electrónico y servidores de archivos. La DMZ está protegida de la red interna por un firewall que limita el tráfico que puede ingresar a la red interna.

Verdadero o falso: El "Health Check" del Load Balancer permite verificar si el Load Balancer está funcionando correctamente.

- ☒ Verdadero
- ☐ Falso

El enunciado es incorrecto. El "Health Check" del Load Balancer no verifica si el propio Load Balancer está funcionando correctamente, sino que se utiliza para

verificar el estado y la salud de las instancias o servidores que están detrás del Load Balancer.

Un firewall protege del(los) siguiente(s) ataque(s).

- ☐ Phishing
- ☐ Dumpster diving
- ☒ Denial of Service (DoS)
- ☐ Shoulder surfing

- Denial of Service (DoS): Un ataque DoS es un ataque que tiene como objetivo hacer que un sistema o servicio sea inaccesible. Un firewall puede ayudar a proteger contra los ataques DoS al bloquear el tráfico malicioso que se dirige a su sistema o servicio.

El AWS EC2 es un servicio de tipo

- ☒ IaaS
- ☐ PaaS
- ☐ SaaS
- ☐ BPaaS

La opción correcta es "a. IaaS". AWS EC2 (Elastic Compute Cloud) es un servicio de la nube de Amazon Web Services que proporciona capacidades de cómputo en la nube bajo el modelo de infraestructura como servicio (IaaS). Permite a los usuarios alquilar máquinas virtuales (instancias) y administrar su propia infraestructura virtualizada, i

El dispositivo que atrae a los atacantes mediante vulnerabilidades implementadas a propósito y funciona como un señuelo se llama:

- ☐ Firewall
- ☒ Honeypot
- ☐ IDS
- ☐ IPS

Seleccione la opción que no es un requerimiento de un IDS:

- ☐ Correr continuamente
- ☐ Tener tolerancia ante fallos
- ☒ Tener un nivel de detección de intrusión del 100%
- ☐ Tener la escalabilidad para monitorear un gran número de sistemas

(IDS) no pueden garantizar una detección del 100%.

En un IDS, ¿qué es más importante?

- ☐ Evitar los falsos positivos en detección de intrusiones
- ☒ Evitar los falsos negativos en detección de intrusiones
- ☐ Detectar los falsos positivos
- ☐ Detectar los falsos negativos

El "Security Group" de AWS es una solución de:

- ☐ Firewall de tipo proxy
- ☒ Firewall de filtrado de puertos
- ☐ IP estática para servidores virtuales
- ☐ Ninguna de las anteriores

La respuesta correcta es b. Firewall de filtrado de puertos. Los grupos de seguridad de Amazon Web Services (AWS) son una función de seguridad que le permite controlar el tráfico de entrada y salida de sus instancias de Amazon Elastic Compute Cloud (EC2).

¿Cuáles son las fortalezas de un IDS basado en Red?

- ☒ Se reduce el costo total de propiedad (TCO)
- ☐ Detección de ataques de manera centralizada
- ☒ Facilidad de implementación y administración
- ☒ Detección detallada por host

- Detección de ataques de manera centralizada: Un IDS basado en red puede monitorear todo el tráfico de red, lo que le permite detectar ataques que se dirigen a varios hosts.
- Facilidad de implementación y administración: Un IDS basado en red puede ser implementado y administrado con relativa facilidad, lo que lo hace una buena opción para organizaciones con recursos limitados.

El estado de una instancia de AWS EC2 que permite su eliminación es:

- ☐ Stop
- ☒ Terminate
- ☐ Eliminate
- ☐ Reboot

El protocolo por defecto para administrar instancias de Linux en AWS es _____

- ☐ RDP
- ☐ HTTP
- ☒ SSH
- ☐ HTTPS

Uno de los requerimientos de los IDS es:

rtual2.espe.edu.ec/evaluaciones.cgi?wAccion=verevaluacion&wid_evaluacion=51906&id_curso=46159

9:40

Sistema Virtual de Educación [Evaluaciones]

- ☐ Funcionar en forma intermitente
- ☐ Proveer un máximo overhead en el sistema
- ☐ Configurarse solamente de acuerdo a un white list de actividades válidas
- ☒ Permitir reconfiguración dinámica

Seleccione la opción más adecuada con respecto a un Firewall:

- ☐ Filtra tráfico de red
- ☐ Puede ser de tipo hardware y software
- ☐ Sigue unas reglas (configuraciones) establecidas
- ☒ Todas las opciones son correctas

El servicio de AWS que entrega el servicio de una dirección de IPv4 pública estática se llama:

- ☐ Static IP
- ☒ Elastic IP
- ☐ Public IP
- ☐ Instance IP

El propósito de un firewall es:

- ☒ Prevenir conexiones no deseadas de red
 - ☐ Filtrar malwares
 - ☐ Evitar la sobrecarga de procesamiento de las computadoras
 - ☐ Compartir una conexión de Internet entre varias computadoras
-

El protocolo por defecto para administrar las instancias de Windows en AWS es _____

- ☒ RDP

Un firewall de filtrado de paquetes puede realizar controles de conexión basado en:

- ☐ Direcciones IP
 - ☐ Puertos fuente
 - ☐ Puertos destino
 - ☐ TCP Flags
 - ☒ Todas las opciones son correctas.
-

Cuál de las siguientes opciones entrega un mayor nivel de disponibilidad en AWS?

- ☐ Una sola máquina virtual de características robusta
 - ☐ Redundancia de máquinas virtuales en el mismo Availability Zone
 - ☒ Redundancia de máquinas virtuales en diferentes Availability Zones
 - ☐ Todas las anteriores tienen el mismo nivel de disponibilidad
-

Dentro de Amazon Web Services (AWS), una Availability Zone (Zona de Disponibilidad) es una ubicación física aislada con su propia infraestructura y suministro eléctrico y de red. Al distribuir tus recursos (como instancias de EC2 y bases de datos) en diferentes Availability Zones, puedes lograr una mayor resiliencia y disponibilidad. Esto se debe a que si una Availability Zone experimenta una interrupción, los recursos en otras zonas pueden continuar funcionando sin verse afectados.

¿Cuál es la limitación de un Firewall de filtro de paquetes?

- ☒ No puede prevenir ataques de bugs de aplicaciones
- ☐ No puede filtrar la conexión basado en direcciones IP
- ☐ Consume muchos recursos computacionales
- ☐ No puede filtrar la conexión basado en puertos

El firewall de filtrado de paquetes puede ser implementado en la siguiente capa del ISO/OSI.

- ☐ Capa de aplicación
- ☐ Capa de sesión
- ☐ Capa de presentación
- ☒ Capa de transporte

Capa de transporte

El firewall de filtrado de paquetes opera en la capa de transporte del modelo OSI. Esta capa se encarga de establecer, mantener y finalizar las conexiones de comunicación y se enfoca en el enrutamiento y la administración de extremo a extremo del flujo de datos. Los firewalls de filtrado de paquetes toman decisiones sobre permitir o bloquear el tráfico de red en función de información como direcciones IP, puertos y banderas TCP en esta capa.

Verdadero o falso: El balanceador de carga clásico requiere la creación de un "Target Group".

- ☒ Verdadero
- ☐ Falso