Guía de estudio - Seguridad de red y firewall en Windows Server

¡Hola! Te damos la bienvenida a esta nueva guía de estudio.

¿En qué consiste esta guía?

La seguridad de la red es un componente crítico en la administración de servidores Windows. La correcta configuración de firewalls y políticas de acceso remoto garantiza la protección contra accesos no autorizados y ciberataques.

En esta guía, abordaremos:

- Automatización de reglas de firewall para una gestión eficiente.
- Implementación de políticas de acceso remoto seguro.
- Mejores prácticas y configuraciones avanzadas.

¡Vamos con todo!

Tabla de contenidos

¡Comencemos!

Automatización de reglas de firewall

El Firewall de Windows Defender es una herramienta clave para controlar el tráfico entrante y saliente en un servidor. Su correcta configuración permite minimizar riesgos de seguridad.

Creación de reglas de firewall con PowerShell

PowerShell permite automatizar la configuración de reglas de firewall para mejorar la administración de la seguridad en la red.

- **Permitir tráfico en un puerto específico:**

```
New-NetFirewallRule -DisplayName "Permitir HTTP" -Direction Inbound
-Action Allow -Protocol TCP -LocalPort 80
```

- **Bloquear tráfico saliente a una IP específica:**

```
New-NetFirewallRule -DisplayName "Bloquear salida a 192.168.1.50"
-Direction Outbound -Action Block -RemoteAddress 192.168.1.50
```

- **Permitir tráfico sólo desde una IP de confianza:**

```
New-NetFirewallRule -DisplayName "Permitir SSH desde IP específica"
-Direction Inbound -Action Allow -Protocol TCP -LocalPort 22
-RemoteAddress 192.168.1.100
```

Gestión de reglas de firewall existentes

Para listar todas las reglas configuradas en el firewall:

```
Get-NetFirewallRule
```

Para modificar una regla existente:

```
Set-NetFirewallRule -DisplayName "Permitir HTTP" -Action Block
```

Para eliminar una regla específica:

```
Remove-NetFirewallRule -DisplayName "Bloquear salida a 192.168.1.50"
```

Políticas de acceso remoto seguro

El acceso remoto a servidores debe configurarse de manera segura para evitar accesos no autorizados y ataques de fuerza bruta.

Configuración segura de RDP (Remote Desktop Protocol)

- **Permitir solo conexiones desde direcciones IP específicas:**

```
New-NetFirewallRule -DisplayName "Permitir RDP desde IP segura"
-Direction Inbound -Action Allow -Protocol TCP -LocalPort 3389
-RemoteAddress 192.168.1.100
```

- **Deshabilitar RDP si no es necesario:**

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server' -Name "fDenyTSConnections" -Value 1
```

- **Habilitar NLA (Network Level Authentication) para mayor seguridad:**

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -Name "UserAuthentication" -Value 1
```

Implementación de VPN segura

Una VPN proporciona un canal seguro para acceder a la red de la empresa de manera remota.

- **Instalar el rol de VPN en Windows Server:**

```
Install-WindowsFeature -Name RemoteAccess -IncludeManagementTools
```

- **Configurar el servidor VPN:**

```
Install-WindowsFeature -Name Routing -IncludeManagementTools
```

- **Habilitar NAT para conexiones VPN:**

```
Set-VpnServerConfiguration -AllowNAT $true
```

Actividad guiada: Configuración Segura de RDP

1. Iniciar la máquina virtual con Windows Server Core
2. Restringir el acceso a RDP solo a direcciones IP autorizadas.
3. Habilitar Network Level Authentication para mejorar la seguridad.
4. Verificar intentos de conexión remota no autorizados en los registros del firewall.

Mejores prácticas para seguridad de red y firewall

Medida de seguridad	Descripción
Uso de reglas de firewall restrictivas	Permitir solo tráfico necesario para reducir exposición.
Implementación de listas blancas de IPs	Permitir acceso remoto solo desde direcciones confiables.
Habilitación de auditoría de eventos de firewall	Registrar intentos de acceso no autorizados.
Configuración de VPN segura	Proteger accesos remotos mediante cifrado.
Uso de autenticación multifactor (MFA)	Requerir autenticación adicional para accesos remotos.

¡Manos a la obra! - Implementación de una VPN segura

1. Iniciar la máquina virtual con Windows Server Core
2. Instalar y configurar el servicio de VPN en Windows Server.
3. Configurar NAT para permitir el tráfico de la VPN.
4. Comprobar la conectividad segura mediante la VPN desde un cliente desktop.

Reflexiona:

- ¿Por qué es importante restringir el tráfico entrante y saliente en un firewall?
- ¿Cómo puede una VPN mejorar la seguridad del acceso remoto?
- ¿Cuáles son los riesgos de permitir conexiones RDP abiertas a Internet?
- ¿Qué medidas pueden tomarse para mejorar la auditoría de eventos en el firewall?
- ¿Cómo afecta el uso de listas blancas de IPs a la seguridad de red?

La correcta configuración del firewall y la gestión del acceso remoto son fundamentales para mantener segura la infraestructura de red. La automatización de reglas de firewall con PowerShell permite una gestión eficiente, mientras que la implementación de políticas de acceso remoto seguro, como el uso de VPN y la restricción de RDP, ayuda a reducir la superficie de ataque.