[Publish] - 12. Restringir el acceso a los puertos de servidor remoto (TCP 3389 y TCP 22)

El hallazgo de seguridad **"Restringir el acceso a los puertos de servidor remoto (TCP 3389 y TCP 22)"** se enfoca en uno de los vectores de ataque más comunes y peligrosos: el acceso administrativo directo desde internet.

- **Puerto 22 (SSH - Secure Shell):** Es el puerto estándar para la administración remota de servidores Linux.
- **Puerto 3389 (RDP - Remote Desktop Protocol):** Es el puerto estándar para la administración remota de servidores Windows.

Cuando un Grupo de Seguridad (Security Group) permite el acceso a estos puertos desde el origen `0.0.0.0/0` (cualquier lugar en internet), estás exponiendo la "llave de entrada" a tus servidores a todo el mundo. Esto invita a un flujo constante de ataques automatizados, incluyendo:

- **Ataques de Fuerza Bruta:** Bots que intentan adivinar contraseñas de usuario sin cesar.
- **Explotación de Vulnerabilidades:** Si se descubre una vulnerabilidad en el servicio SSH o RDP, tu servidor es un objetivo inmediato.
- **Ataques de Denegación de Servicio:** El servicio de administración puede ser saturado, impidiendo el acceso legítimo.

> **La mejor práctica es nunca exponer los puertos de administración directamente a internet.**

Análisis de los Grupos de Seguridad Reportados

Los siguientes Grupos de Seguridad han sido identificados por tener reglas que permiten el acceso público y sin restricciones a los puertos 22 (SSH) o 3389 (RDP).

Tipo	Nombre	Número de cuenta
SecurityGroup	sg-004420139ef66c611	890342916428
SecurityGroup	sg-0047c008ab5f01e34	002670977573
SecurityGroup	sg-0065732d7afa61eff	002670977573

SecurityGroup	sg-00749c8d73da5982b	890342916428
SecurityGroup	sg-007bc5f2b845302b9	398984081329
SecurityGroup	sg-0088f856f8391df6a	398984081329
SecurityGroup	sg-008e76e5ce0ceaa5a	002670977573
SecurityGroup	sg-00987d6bc4be94335	002670977573
SecurityGroup	sg-010adc6798ab1ba8a	002670977573
SecurityGroup	sg-0128bc1461282b353	002670977573
SecurityGroup	sg-0128d083cfbcd6f44	002670977573
SecurityGroup	sg-013dcf552c7e855f5	002670977573
SecurityGroup	sg-014489373872eac51	002670977573
SecurityGroup	sg-016b960ea0f1c8210	002670977573
SecurityGroup	sg-017228607010fe652	002670977573
SecurityGroup	sg-018ade9e48a77a326	002670977573
SecurityGroup	sg-01afe7aceeb90a24a	002670977573
SecurityGroup	sg-01e531d22160c650c	002670977573
SecurityGroup	sg-01ec2731e0a325e34	498798756906

SecurityGroup	sg-020398277218d7ea6	890342916428
SecurityGroup	sg-020db01ae9208cd23	002670977573
SecurityGroup	sg-0242e6ac458cd02f1	002670977573
SecurityGroup	sg-0242e86db7085441b	890342916428
SecurityGroup	sg-026126cd9a03e0529	398984081329
SecurityGroup	sg-027c556297ee31d89	890342916428
SecurityGroup	sg-027d518f1bf036472	002670977573
SecurityGroup	sg-02a6b1c62d5fd223d	498798756906
SecurityGroup	sg-02be2885446d2383d	613703092215
SecurityGroup	sg-03114107618987d38	002670977573
SecurityGroup	sg-0315f5571e4e27c75	890342916428
SecurityGroup	sg-0339def3604f9cfba	002670977573
SecurityGroup	sg-035f00069cc6c2e1e	996126991518
SecurityGroup	sg-0371c34385d5dd785	890342916428
SecurityGroup	sg-03a9ecd569e9e85b1	002670977573
SecurityGroup	sg-03aa8e152bc6540fe	398984081329

SecurityGroup	sg-03b4dcdc65dccedc9	002670977573
SecurityGroup	sg-041b5cddfc4858c86	002670977573
SecurityGroup	sg-0424ae4c6a01ddf4b	002670977573
SecurityGroup	sg-0428132cf2f2de53b	002670977573
SecurityGroup	sg-042bfd8b3fd64aa62	002670977573
SecurityGroup	sg-042d81e2e592a84eb	996126991518
SecurityGroup	sg-04a39e4e9b9bbbdbf	002670977573
SecurityGroup	sg-04e42437c140de6ff	002670977573
SecurityGroup	sg-0516784a94227df7f	890342916428
SecurityGroup	sg-0581f3a1531188fa8	890342916428
SecurityGroup	sg-05979750def5b179c	002670977573
SecurityGroup	sg-059e040dfa27a0c32	996126991518
SecurityGroup	sg-05dd47153bb9d2092	002670977573
SecurityGroup	sg-05df910077a52f2bc	002670977573
SecurityGroup	sg-05e44118345066093	890342916428
SecurityGroup	sg-05e944a9f97b16d23	002670977573

SecurityGroup	sg-05ea4376a4bd9cdc3	398984081329
SecurityGroup	sg-0673241e83a5e2f2e	498798756906
SecurityGroup	sg-069fa4096ed0c7042	002670977573
SecurityGroup	sg-06a9b5d16308df2d1	002670977573
SecurityGroup	sg-06c54f3026477bc7c	002670977573
SecurityGroup	sg-06da238dcbe47a006	002670977573
SecurityGroup	sg-070d375fed3ea0f3a	002670977573
SecurityGroup	sg-0716906206484a347	002670977573
SecurityGroup	sg-072e80edc0a298b5c	002670977573
SecurityGroup	sg-07687a6415873cede	002670977573
SecurityGroup	sg-077cc892edea8e0d9	002670977573
SecurityGroup	sg-07bb8b9eac6246663	890342916428
SecurityGroup	sg-07bdead20df822f88	002670977573
SecurityGroup	sg-07ce953714962276e	002670977573
SecurityGroup	sg-07f30a27c2bec63f7	002670977573

SecurityGroup	sg-0819b9a863b87ecff	890342916428
SecurityGroup	sg-0836b19967dc240a0	002670977573
SecurityGroup	sg-088111eab41940eab	002670977573
SecurityGroup	sg-08866e0cad529bc34	002670977573
SecurityGroup	sg-08a5721db88f25cf6	398984081329
SecurityGroup	sg-08b1eb7c4e724a113	002670977573
SecurityGroup	sg-08f3cb3cad4bf4f6a	002670977573
SecurityGroup	sg-0908986fc6f14895c	002670977573
SecurityGroup	sg-090f85d5feba61699	890342916428
SecurityGroup	sg-096166ecbd1a127fc	002670977573
SecurityGroup	sg-097d590da85217816	613703092215
SecurityGroup	sg-098e332ca784c58d5	398984081329
SecurityGroup	sg-099b947faf3cdf720	002670977573
SecurityGroup	sg-09baf9c1cbbe2ceef	398984081329
SecurityGroup	sg-0a0dfdfb541c674ad	890342916428
SecurityGroup	sg-0a2cf214090f339e7	002670977573
SecurityGroup	sg-0a35e80b7206327d5	002670977573
SecurityGroup	sg-0a7ba20f8986cebb9	002670977573

SecurityGroup	sg-0a7c5cfe76d89fb6d	002670977573
SecurityGroup	sg-0aaac0a6ca571a618	002670977573
SecurityGroup	sg-0ae19593765ed137f	613703092215
SecurityGroup	sg-0ae578f533dfe68b0	002670977573
SecurityGroup	sg-0b266a136495717da	002670977573
SecurityGroup	sg-0b4c5f0d6891686ac	890342916428
SecurityGroup	sg-0b6c1712838b382be	398984081329
SecurityGroup	sg-0b7a660336cb9195e	613703092215
SecurityGroup	sg-0ba7b7a8247dbf32f	002670977573
SecurityGroup	sg-0bd19aa712dfc4ac6	002670977573
SecurityGroup	sg-0be7beac597ad7f1c	002670977573
SecurityGroup	sg-0bf1110ba525aeb17	002670977573
SecurityGroup	sg-0bff8145005d9a7ff	890342916428
SecurityGroup	sg-0c014c0ad9e62af50	002670977573
SecurityGroup	sg-0c243725ef6d3b231	002670977573
SecurityGroup	sg-0ca374a100c6fc766	002670977573
SecurityGroup	sg-0cf77b7d6efe45b26	002670977573

SecurityGroup	sg-0cf8c6c950c35e7ef	002670977573
SecurityGroup	sg-0d13865f674a419a4	002670977573
SecurityGroup	sg-0d3efdddaf2c45cf4	002670977573
SecurityGroup	sg-0d4513944c23879e5	002670977573
SecurityGroup	sg-0d7ce52e20e16e790	002670977573
SecurityGroup	sg-0d7f540d755fc0d98	002670977573
SecurityGroup	sg-0d90a8c820ea3f82f	002670977573
SecurityGroup	sg-0d994cf1854147435	002670977573
SecurityGroup	sg-0db6cfe131187471b	002670977573
SecurityGroup	sg-0dbe26909bfc4d3d3	002670977573
SecurityGroup	sg-0dc8bf77d07a25257	002670977573
SecurityGroup	sg-0de6f2e428d65964a	002670977573
SecurityGroup	sg-0dfa2d8ce7015e691	002670977573
SecurityGroup	sg-0e06b4dd11224f581	890342916428
SecurityGroup	sg-0e2162127a0f11923	498798756906
SecurityGroup	sg-0e6836036cb252ce2	002670977573

SecurityGroup	sg-0e98b01b25d774ea6	890342916428
SecurityGroup	sg-0eb30e9593db8105a	002670977573
SecurityGroup	sg-0ebad0a5eef1ff2b4	002670977573
SecurityGroup	sg-0ee46248ae4bae16c	002670977573
SecurityGroup	sg-0f409ca22a5ffd35f	002670977573
SecurityGroup	sg-0f55d0642f7bf59a4	002670977573
SecurityGroup	sg-0f7faef7ea83d512c	890342916428
SecurityGroup	sg-0f829b55fd96a93d4	890342916428
SecurityGroup	sg-0fb8e96e202316688	002670977573
SecurityGroup	sg-0fc05448b7dc05d65	002670977573
SecurityGroup	sg-0fdb26e470370ea82	002670977573
SecurityGroup	sg-0fe0b35f1a659cf3e	002670977573
SecurityGroup	sg-0ffdad916564e13af	996126991518
SecurityGroup	sg-12564a62	398984081329
SecurityGroup	sg-675f4317	398984081329
SecurityGroup	sg-6aca6722	613703092215
SecurityGroup	sg-74ad5402	613703092215
SecurityGroup	sg-7818240f	613703092215
SecurityGroup	sg-a05c40d0	398984081329

Preguntas para tu Equipo (Acción Requerida)

La necesidad de acceso administrativo es legítima, pero debe hacerse de forma segura.

1. **¿Quién necesita acceso administrativo a las instancias protegidas por estos grupos de seguridad?**
2. **¿Desde dónde se conectan?** ¿Es desde una oficina con una IP estática, a través de una VPN corporativa, o es para un proveedor externo?
3. **¿Podemos reemplazar el acceso directo por un método más seguro?** La recomendación principal de AWS es utilizar **AWS Systems Manager Session Manager**.

Consideraciones de Costo

- **Modificar Reglas de Grupo de Seguridad:** Esta acción es **gratuita**.
- **AWS Systems Manager Session Manager:** El uso de Session Manager para el acceso a instancias EC2 es **gratuito**.

Conclusión sobre Costos:

Asegurar los puertos de administración no solo no tiene costo, sino que la solución recomendada (Session Manager) también es gratuita y elimina la necesidad de gestionar servidores bastion, lo que puede incluso reducir costos.

Cómo Solucionarlo: Eliminar el Acceso Público

Opción A: Restringir el Acceso a IPs Específicas (Solución Inmediata)

1. Navega a la consola de **EC2** > **Grupos de Seguridad**.
2. Selecciona el grupo de seguridad y ve a **Editar reglas de entrada**.
3. Localiza la regla para el puerto 22 o 3389 con origen `0.0.0.0/0`.
4. Cambia el **Origen (Source)** a la dirección IP específica de tu oficina o VPN (ej. `200.100.50.1/32`).
5. Guarda los cambios.

Opción B: Implementar AWS Systems Manager Session Manager (La Mejor Práctica)

Esta es la solución más segura y recomendada.

1. **Asegurar Permisos:** Verifica que tus instancias tengan un rol de IAM con la política administrada `AmazonSSMManagedInstanceCore` adjunta.
2. **Eliminar Reglas Inseguras:** Una vez que confirmes que puedes acceder a tus instancias a través de Session Manager, **elimina por completo** las reglas de entrada para los puertos 22 y 3389 del grupo de seguridad.

3. **Acceder a través de Session Manager:**
    - En la consola de EC2, selecciona la instancia.
    - Haz clic en **Conectar**.
    - Elige la pestaña **Session Manager** y haz clic en **Conectar**.
    - Esto abrirá una terminal de shell segura directamente en tu navegador, sin necesidad de claves SSH ni puertos abiertos.

Recomendación

Se recomienda que se adopte **AWS Systems Manager Session Manager** como el método estándar para el acceso administrativo a todas las instancias EC2. Como medida inmediata, restrinjan todas las reglas de SSH y RDP abiertas para permitir el acceso únicamente desde rangos de IP autorizados y conocidos. La exposición de estos puertos a todo internet es un riesgo inaceptable que debe ser mitigado con la máxima prioridad.

Referencias

Security group rules for different use cases - Amazon Elastic Compute Cloud