Devolutions

[NEW] Use Case: How Organizations That Use RDP Can Avoid Complexity, Reduce Costs & Boost Network Visibility by Using Devolutions Gateway Instead of a VPN

MANY ORGANIZATIONS BOOST SECURITY WITH A VIRTUAL PRIVATE NETWORK (VPN)

Microsoft's Remote Desktop Protocol (RDP) should never be exposed directly on the Internet (port 3389). As such, many organizations boost security with a virtual private network (VPN).

However, there are some key problems with this approach:

- **VPN servers are notoriously difficult to deploy.**
- **VPN clients often tunnel all traffic through the private network — which can significantly degrade network performance.**
- **While the cost/benefit ratio of using a VPN may be acceptable for large corporate networks, it is typically not suitable for small, isolated networks.**

Another way to look at this is to say that VPNs are a general-purpose solution applied to a specific problem (RDP), which makes them ill-suited for the job.

Fortunately, there is a practical solution that addresses all of these challenges: Use **Devolutions Gateway** in conjunction with **Devolutions Server** and **Remote Desktop Manager**.

In our new use case (which includes how-to steps), you will discover how this approach:

- **Establishes robust security** by enforcing multi-factor authentication (MFA) on all Devolutions' Gateway RDP connections.
- **Turns complexity into simplicity** by replacing a bloated VPN deployment with an easy-to-use, lightweight Devolutions Gateway instance.
- **Improves network performance** by restricting tunneling to RDP connections, so there is no negative impact on other network traffic.
- **Increases functionality and versatility** by making secure just-in-time (JIT) RDP access possible without using a VPN. This also enables detailed centralized session tracking and auditing.

Click here to instantly download the Use Case [PDF].

Click here for a full list of Use Cases that are also available for download.