Overview of Remote Desktop Gateway

By Archiveddocs

Archived: 2026-04-06 03:34:52 UTC

Applies To: Windows Server 2008 R2

Remote Desktop Gateway (RD Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be Remote Desktop Session Host (RD Session Host) servers, RD Session Host servers running RemoteApp programs, or computers with Remote Desktop enabled.

RD Gateway uses the Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.

RD Gateway provides many benefits, including:

- RD Gateway enables remote users to connect to internal network resources over the Internet, by using an encrypted connection, without needing to configure virtual private network (VPN) connections.
- RD Gateway provides a comprehensive security configuration model that enables you to control access to specific internal network resources. RD Gateway provides a point-to-point RDP connection, rather than allowing remote users access to all internal network resources.
- RD Gateway enables most remote users to connect to internal network resources that are hosted behind firewalls in private networks and across network address translators (NATs). With RD Gateway, you do not need to perform additional configuration for the RD Gateway server or clients for this scenario.

  Prior to this release of Windows Server, security measures prevented remote users from connecting to internal network resources across firewalls and NATs. This is because port 3389, the port used for RDP connections, is typically blocked for network security purposes. RD Gateway transmits RDP traffic to port 443 instead, by using an HTTP Secure Sockets Layer/Transport Layer Security (SSL/TLS) tunnel. Because most corporations open port 443 to enable Internet connectivity, RD Gateway takes advantage of this network design to provide remote access connectivity across multiple firewalls.
- The Remote Desktop Gateway Manager enables you to configure authorization policies to define conditions that must be met for remote users to connect to internal network resources. For example, you can specify:
  - Who can connect to internal network resources (in other words, the user groups who can connect).
  - What network resources (computer groups) users can connect to.

    - Whether client computers must be members of Active Directory security groups.
    - Whether device redirection is allowed.
    - Whether clients need to use smart card authentication or password authentication, or whether they can use either method.

- You can configure RD Gateway servers and Remote Desktop Services clients to use Network Access Protection (NAP) to further enhance security. NAP is a health policy creation, enforcement, and remediation technology that is included in Windows Server® 2008 R2, Windows Server® 2008, Windows® 7, Windows Vista®, and Windows® XP Service Pack 3. With NAP, system administrators can enforce health requirements, which can include software requirements, security update requirements, required computer configurations, and other settings.

Note

Computers running Windows Server 2008 R2 or Windows Server 2008 cannot be used as NAP clients when RD Gateway enforces NAP. Only computers running Windows 7, Windows Vista, or Windows XP SP3 can be used as NAP clients when RD Gateway enforces NAP.

```
For information about how to configure RD Gateway to use NAP for health policy enforcement for Remote Desktop S
```

- You can use RD Gateway server with Microsoft Internet Security and Acceleration (ISA) Server to enhance security. In this scenario, you can host RD Gateway servers in a private network rather than a perimeter network, and host ISA Server in the perimeter network. The Secure Sockets Layer (SSL) connection between the Remote Desktop Services client and ISA Server can be terminated at the ISA Server, which is Internet-facing.

  For information about how to configure ISA Server as an SSL termination device for RD Gateway server scenarios, see the Remote Desktop Services page on the Windows Server 2008 R2 TechCenter (https://go.microsoft.com/fwlink/?linkid=140433).

- Remote Desktop Gateway Manager provides tools to help you monitor RD Gateway server status and events. By using Remote Desktop Gateway Manager, you can specify events (such as unsuccessful connection attempts to the RD Gateway server) that you want to monitor for auditing purposes.

- Remote Desktop Gateway Manager

Source: https://technet.microsoft.com/en-us/library/cc731150.aspx