Remote Access VPN & Network Routing Lab W/ Microsoft Server 2025 & RRAS

Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Windows Server 2025, Windows 10 Pro, VirtualBox |
PORTFOLIO WEBSITE: https://www.saintmaiden.site/

EXECUTIVE SUMMARY:

PROBLEM:	SOLUTION:	IMPACT:
Offsite staff require access to internal server resources without exposing network services directly to the public internet. They work at coffee shops, hotel lounges, and work from home most of the time.	**Designed and deployed an isolated dual-NIC remote access VPN gateway using Windows Server 2025 running RRAS, NAT, and PPTP encryption.**	**Secured perimeter access, enforced strict dial-in authentication, and validated secondary protocol routing (RDP) through an encrypted tunnel.**

TECHNICAL TOPOLOGY/SPECIFICATIONS:

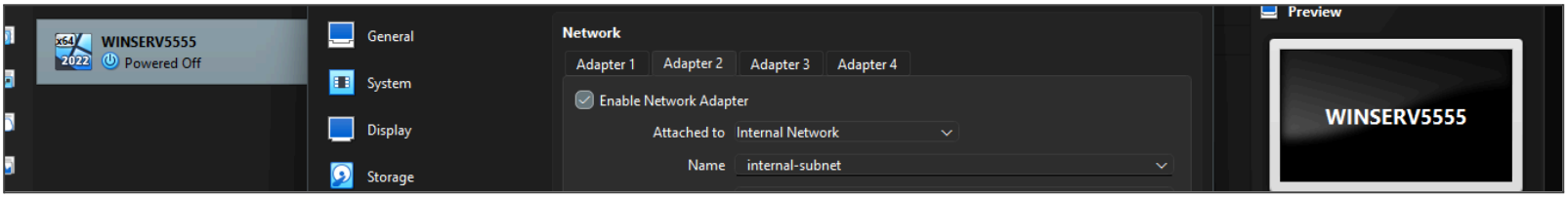
COMPONENT/ROLE	SYSTEM/SPACE NAME	NETWORK MODE & ACCESS	SERVICES & ROLES
VPN Gateway	**WINSERV5555**	**Adapter 1: WAN/NAT (DHCP) Adapter 2: Internal (10.0.0.1/24)**	**Routing & Remote Access Service (RRAS), NAT, PPTP Engine, MS CHAP v2**
Remote Client	**WINCLIENT555**	**Adapter 1: Internal (10.0.0.10/24) Gateway: (10.0.0.1)**	**Windows 10 Pro, Native VPN Client, RDP Client**
Encrypted Tunnel	**Lab-VPN**	**Virtual PPP Adapter**	**Assigned Pool (192.168.100.100-192.168.100.150), Point-To-Point Tunneling**

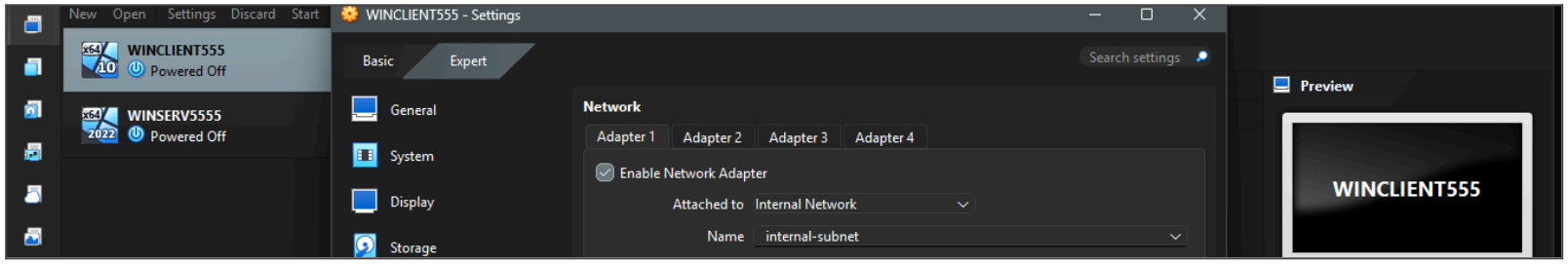
PHASE 1: DUAL-NIC STATIC IP FOUNDATION & TROUBLESHOOTING

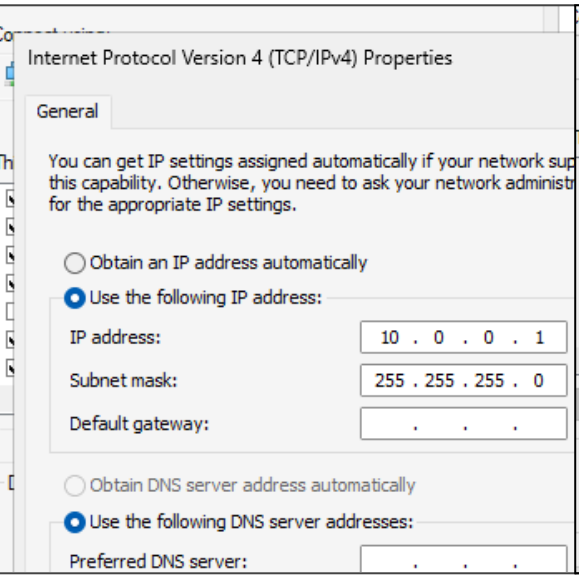
ACTION: **Configured static IP addressing [10.0.0.1/24] on Adapter 2 for WINSERV5555 and [10.0.0.10/24] on WINCLIENT555. Verified Layer 3 Connectivity (Network Layer/IP (Internet Protocol).**

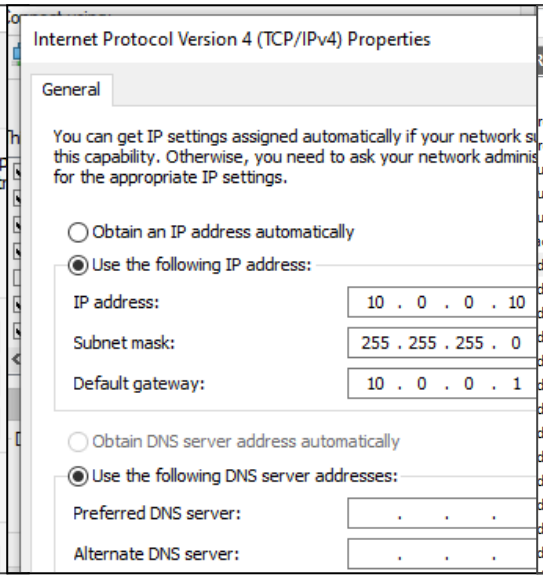
TROUBLESHOOTING ISSUE: **Initial pings timed out multiple times. Mitigated this issue by enabling "File and Printer Sharing (Echo Request - ICMPv4-in)" in wf.msc on WINSERV5555 and making sure WINSERV5555 and WINCLIENT555 corresponded on the same internal network [Internal-Subnet].**

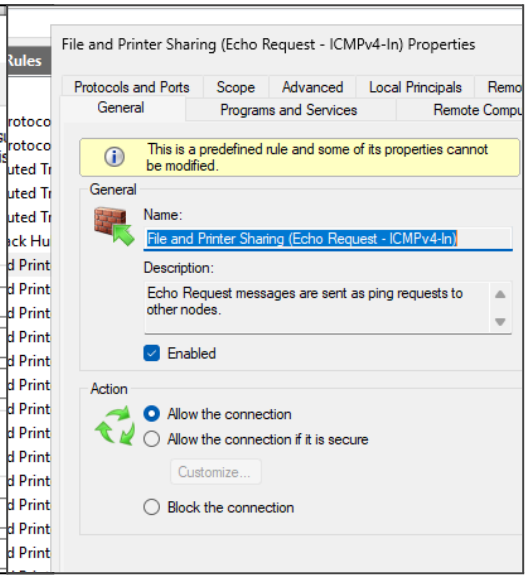
WHY?: **Establishes a deterministic private subnet baseline and ensures local host firewalls permit basic network discovery before layering on VPN tunneling.**









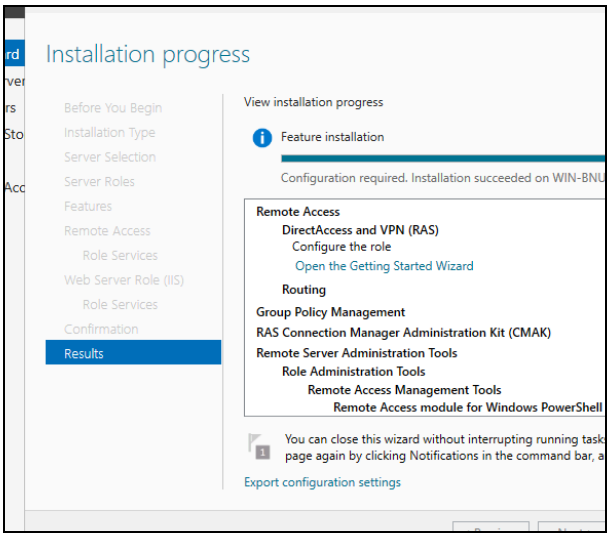


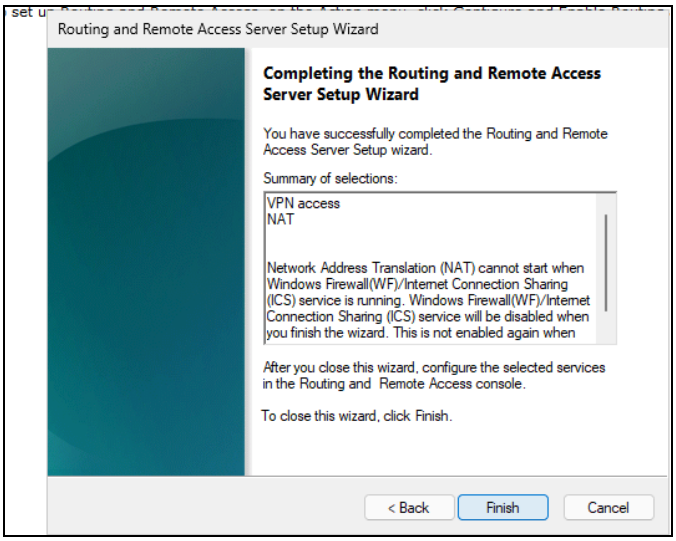
PHASE 2: RRAS DEPLOYMENT & DIAL-IN SECURITY CONTROL

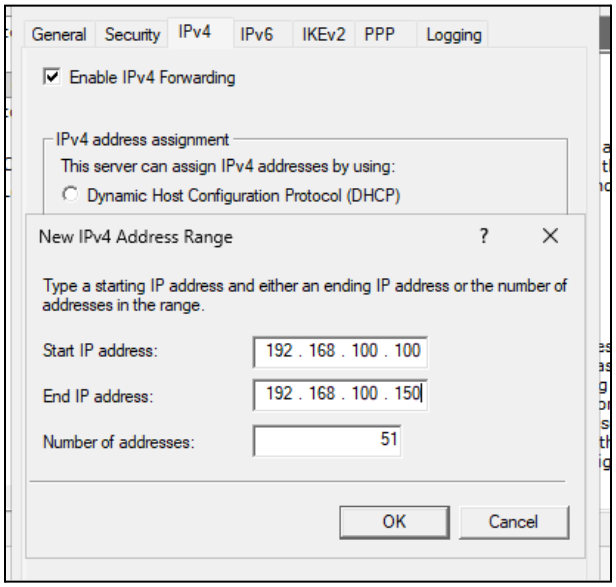
ACTION: **Installed Remote Access role via Server Manager. Configured RRAS using Custom Configuration (VPN & NAT), specified static IP pool [192.168.100.100-150], and enabled MS-CHAP v2 authentication.**

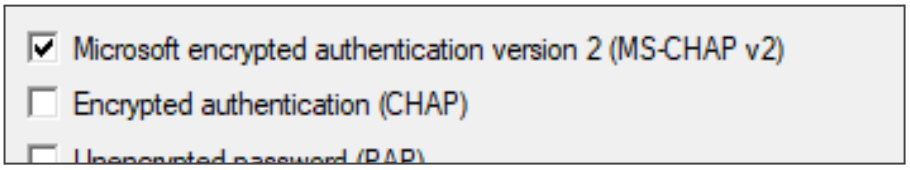
DIAL-IN GOVERNANCE: **Navigated to Computer Management (compmgmt.msc)> Local Users And Groups > Users > Properties > Dial-In Tab and checked “Allow Access”**

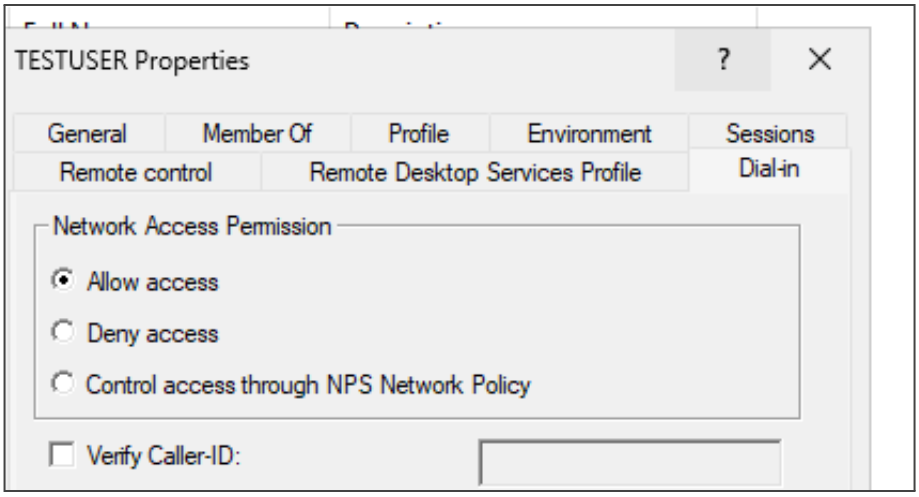
WHY?: **Enforces Zero-Trust perimeter security by requiring explicit account-level dial-in permissions and encrypted authentication before leasing tunnel IP addresses.**











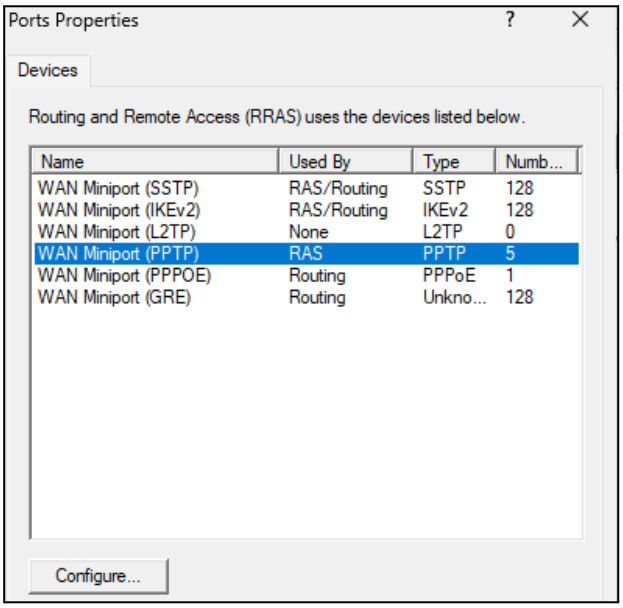
PHASE 3: RRAS PORT BINDING & FIREWALL HARDENING

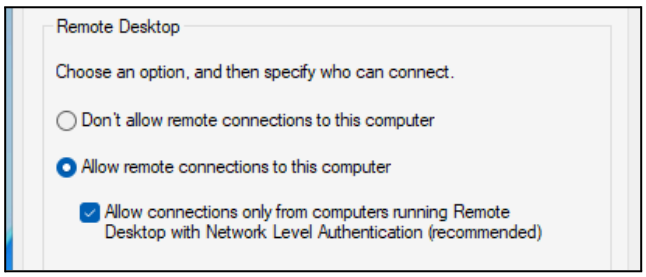
ACTION: Configured protocol bindings and firewall traversal for PPTP and GRE traffic.

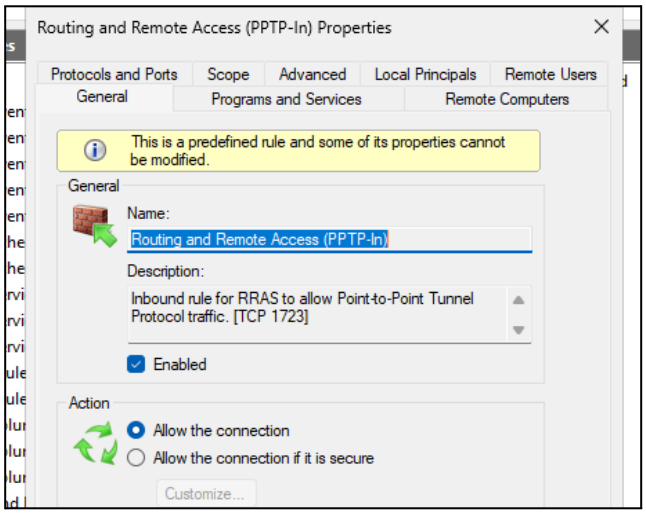
TROUBLESHOOTING ISSUE 1: Missing Ports. PPTP Miniports failed to appear in RRAS. Resolved by accessing RRAS Ports properties, configuring WAN Miniport PPTP for 5 inbound ports, enabling remote access, and restarting RRAS service.

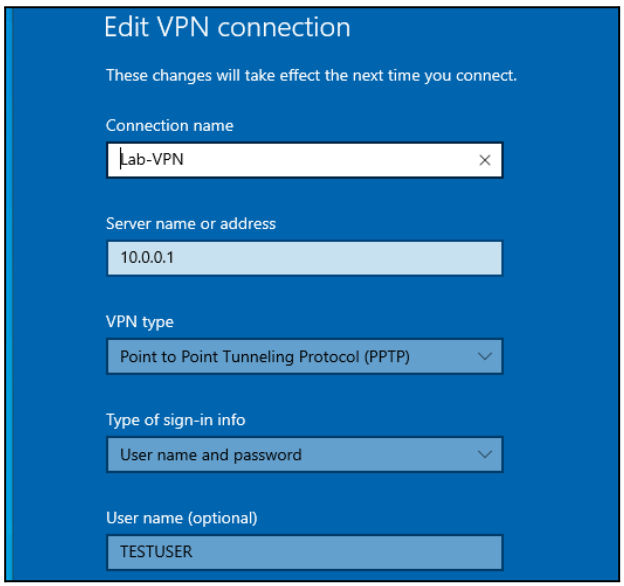
TROUBLESHOOTING ISSUE 2: Error 807/Handshake Failure. Client failed to complete tunnel negotiation. Resolved by locking client VPN properties to PPTP and enabling PPTP In/Out and GRE In/Out rules in wf.msc on WINSERV5555.

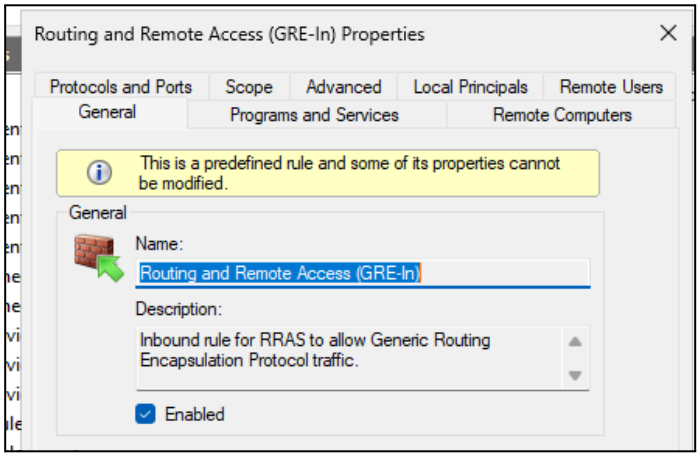
WHY?: Explicit protocol and firewall matching ensure GRE protocol (IP Protocol 47/Cisco Systems) encapsulation passes cleanly through the server interface without premature connection drops.











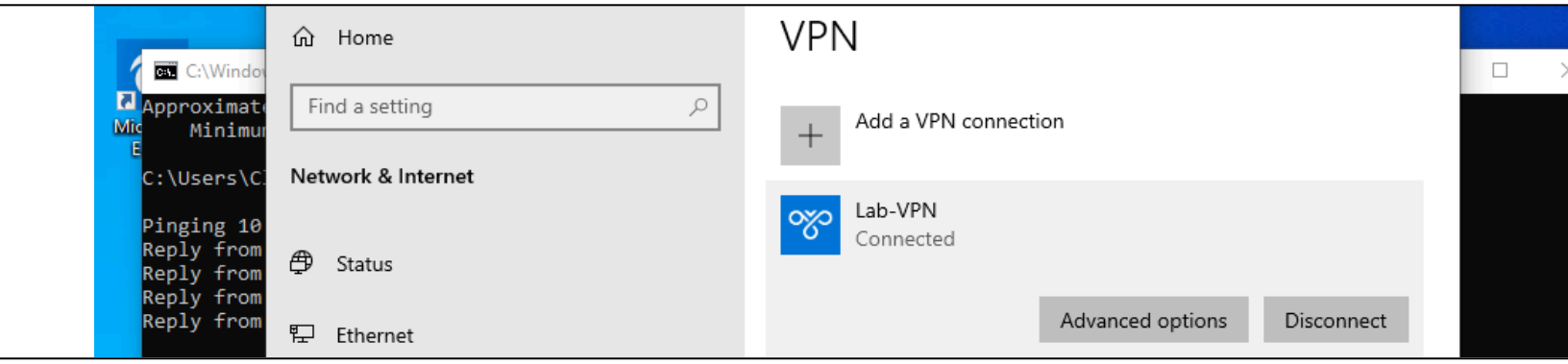
PHASE 4: TUNNEL ESTABLISHMENT & ENCRYPTED TRAFFIC VERIFICATION

ACTION: **Initiated [Lab-VPN] connection from WINCLIENT555 using configured user credentials.**

TUNNEL VERIFICATION: **Executed [ipconfig] on WINCLIENT555 to verify active [PPP Adapter Lab-VPN] with leased IP [192.168.100.101].**

ENCRYPTED DATA FLOW TEST: **Executed [ping 192.168.100.101] from client to server gateway via the tunnel, confirming bidirectional traffic. Encapsulation and decryption is active.**

WHY?: **Validates that authentication succeeded and that traffic is actively being routed through the virtual PPP interface rather than unencrypted local interfaces (e.g. coffee shop wifi).**




```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ccb8:3d6f:614c:1551%5
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

PPP adapter Lab-VPN:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.100.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

C:\Users\Client>ping 192.168.100.101

Pinging 192.168.100.101 with 32 bytes of data:
Reply from 192.168.100.101: bytes=32 time=2ms TTL=128
Reply from 192.168.100.101: bytes=32 time<1ms TTL=128
Reply from 192.168.100.101: bytes=32 time<1ms TTL=128
Reply from 192.168.100.101: bytes=32 time<1ms TTL=128

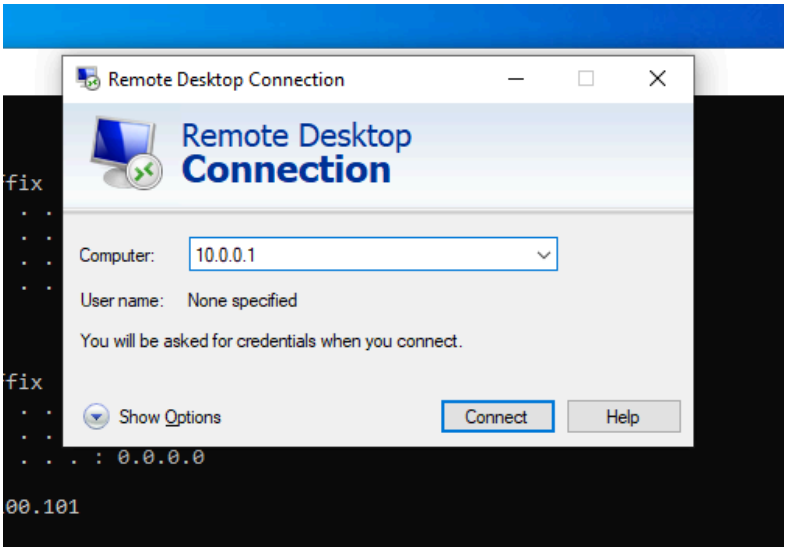
Ping statistics for 192.168.100.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

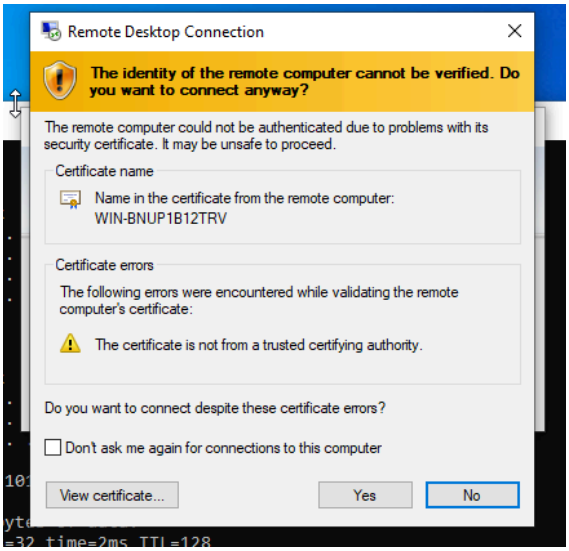
C:\Users\Client>
```

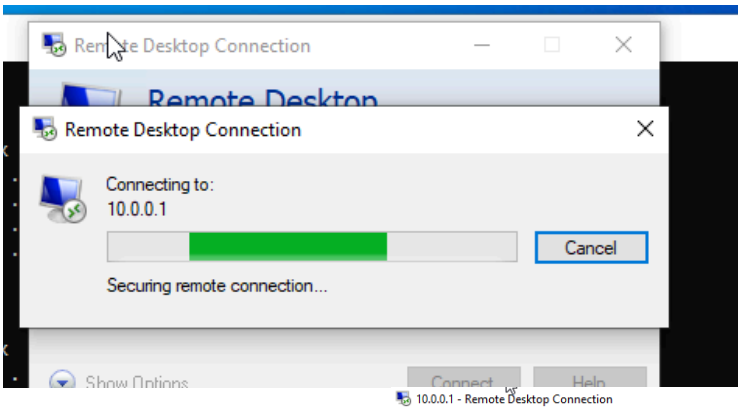
PHASE 5: SECONDARY PROTOCOL VALIDATION (RDP OVER VPN)

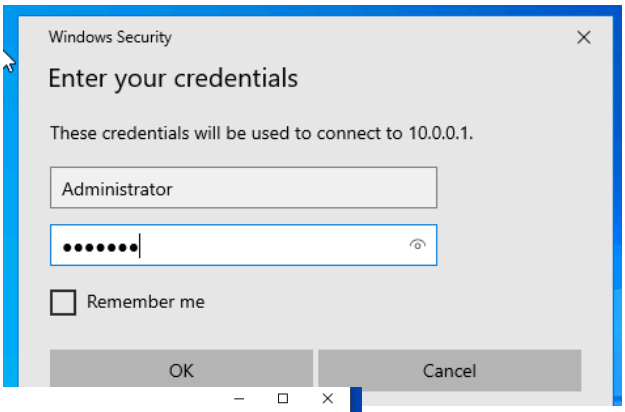
ACTION: **Enabled Remote Desktop on WINSERV5555 [sysdm.cpl]. Launched Remote Desktop Connection [mstsc] on WINCLIENT555 and established an interactive session to [10.0.0.1] over the active tunnel.**

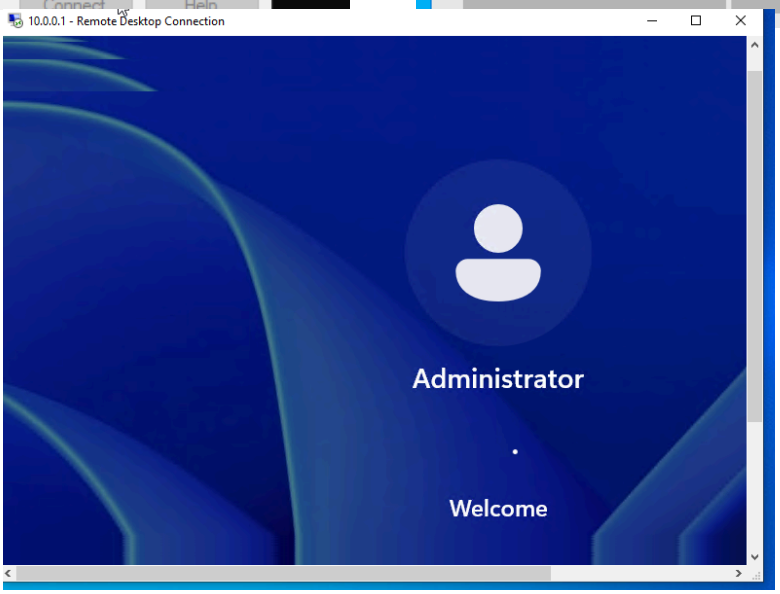
WHY?: **Proves end-to-end operational readiness by demonstrating that encrypted remote access tunnels properly transport high-layer enterprise protocols [RDP] to managed internal assets.**











TECHNICAL SUMMARY:

SECURITY & NETWORKING DOMAIN	TECH & CONTROLS CONFIGURED
GATEWAY INFRASTRUCTURE	Windows Server 2025 RRAS, Dual-NIC Routing, NAT
TUNNEL SECURITY	PPTP Protocol, MS-CHAP v2 Authentication, Dial-in Access Control
FIREWALL & TRAFFIC CONTROL	ICMPv4 Pass-Through, GRE Protocol Rules, Custom Inbound/Outbound Filters
ADDRESS MANAGEMENT	Static Internal Subnet (10.0.0.0/24), Static IPv4 VPN Pool (192.168.100.x)
SYSTEM VALIDATION	PPP Adapter Lease Verification, ICMP Tunnel Test, RDP over VPN

RESULT & BUSINESS IMPACT:

- **ENCRYPTED REMOTE ACCESS:** Established a secure remote connection path over non-secure networks using PPTP and MS-CHAP v2.
- **HARDENED ACCESS CONTROLS:** Restricted unauthorized connections by mandating explicit user dial-in permissions in Active Directory/SAM
- **RESOLVED NETWORK BLOCKS:** Identified and remediated firewall blocking (GRE/ICMP) and port binding issues during deployment.
- **VERIFIED ENTERPRISE UTILITY:** Confirmed full support for remote administration tools by successfully executing Remote Desktop (RDP) over the encrypted tunnel.

Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Windows Server 2025, Windows 10 Pro, VirtualBox |
PORTFOLIO WEBSITE: https://www.saintmaiden.site/