

Lab Setup Guide

Pre-Requisites

- FortiToken for iOS or Android
- FortiClient VPN for Windows, Mac, or Chromebook
- GNS3 for network simulation
- Putty for Windows or Royal TSX for Mac for remote access

Client-Specific Network Configuration Guide

Welcome to my Network Lab! This write-up is dedicated to helping you set up and configure a comprehensive network environment for an experimental project requested by a client. The client's requirements include building a secure network with specific specifications.

- A secure internal Windows domain.
- An internal Microsoft IIS webserver.
- An internal Windows 10 workstation.
- A public webserver.
- A public FTP server.
- A LAN network on 10.128.0.0/24.
- A DMZ network on 10.128.10.0/24.
- A guest network on 10.128.99.0/24.

Whether you're a seasoned network administrator or just starting, this guide will assist you in creating a robust network infrastructure that meets these specific requirements. This project is an exciting experiment designed to fulfill your client's needs for a secure and efficient network environment. Dive in and explore the resources and instructions provided to get your lab up and running.

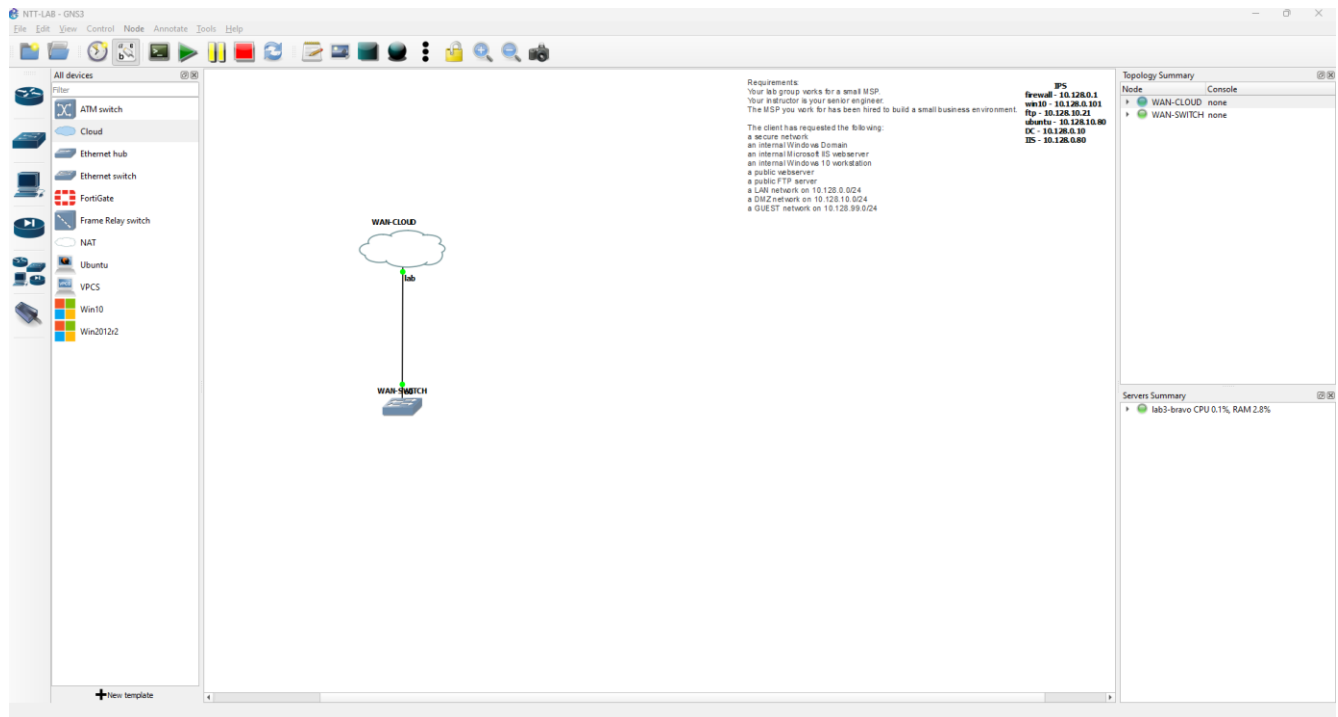
Next Steps

Follow the stage-specific instructions to build out the small business environment. Refer to the lab documentation for step-by-step guidance and troubleshooting tips.

Network Configuration and Security Steps

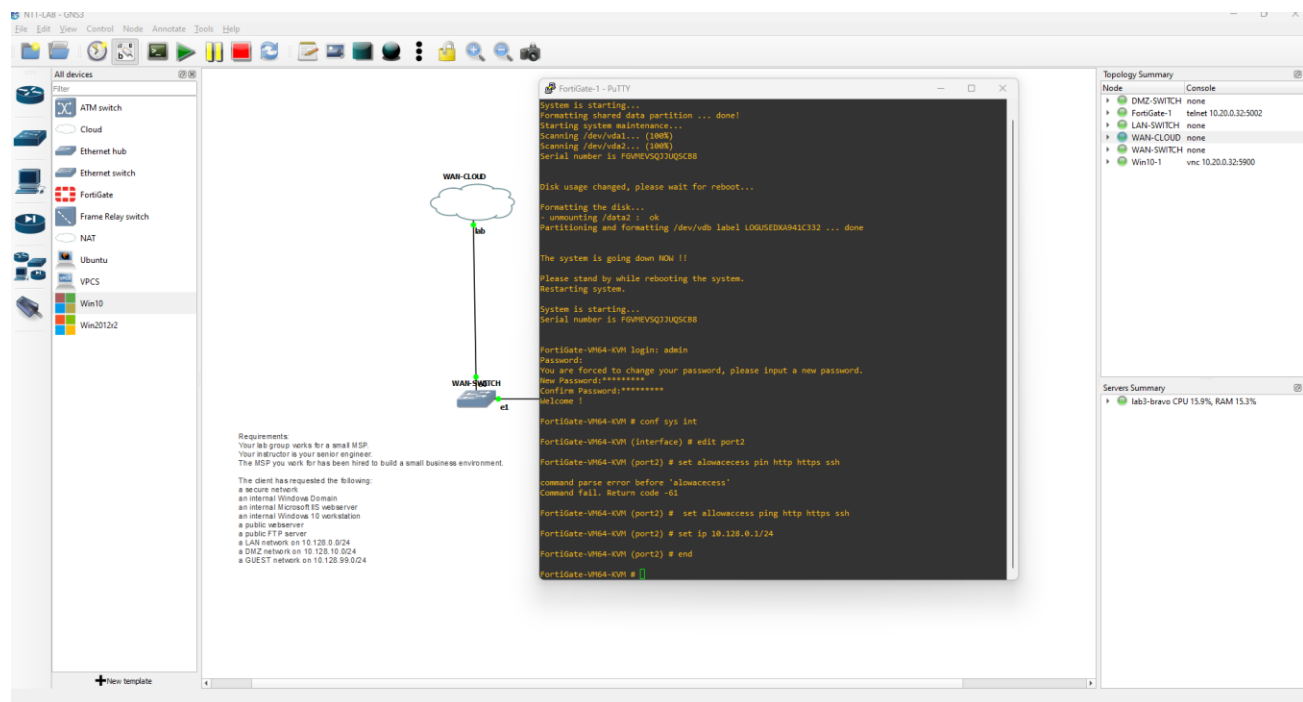
Slide 1 Instructions:

- Start the GNS3 application and create a new project for your network topology.
- In the GNS3 workspace, drag and drop a 'Cloud' node onto the canvas to represent the WAN link.
- Next, add a 'Switch' and place it on the canvas to represent the WAN switch in your network topology.
- Connect the 'Cloud' node to the 'Switch' using a cable tool to establish the link between the WAN and your network.
- Review the project requirements listed on the right side of the GNS3 workspace, which detail the network components you need to configure, including:
 - Secure network setup
 - Internal and public servers
 - Workstations
 - Network segments with specific IP address ranges



Slide 2 Instructions:

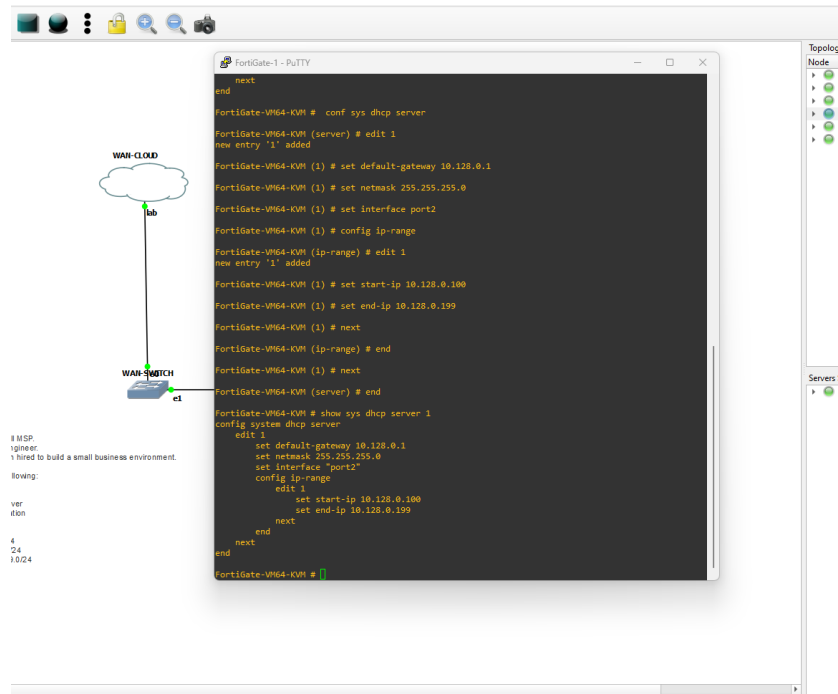
- Open a terminal session to the FortiGate firewall using PuTTY or another SSH client.
- Log in to the FortiGate device with the default username, which is typically 'admin'.
- You will be prompted to change the default password upon the first login for security purposes. Enter a new password as requested and confirm it.
- Begin initial configuration of the FortiGate firewall by entering the command-line interface (CLI) configuration mode. This is typically done by typing **config system interface**.
- Edit the specific interface you wish to configure, which is **port2** in this context, by entering **edit port2**.
- Attempt to set the allowed access methods on **port2** to include HTTP, HTTPS, and SSH. If you encounter a command error as shown, ensure you are using the correct syntax which should be **set allowaccess http https ssh**.
- Assign an IP address to **port2** using the command **set ip 10.128.0.1/24**. This sets the interface to the desired IP address and subnet mask.
- End the configuration session for **port2** by typing **end** to apply the changes.



Slide 3 Instructions:

- Continue configuring the FortiGate firewall by setting up a DHCP server for network clients connected to **port2**.
- Enter the DHCP server configuration mode using **config system dhcp server**.
- Create a new DHCP server instance by entering **edit 1** (assuming this is the first DHCP server instance you're creating).
- Define the default gateway for DHCP clients with **set default-gateway 10.128.0.1**. This IP should be the interface IP of **port2** configured earlier.
- Set the netmask for the DHCP scope with **set netmask 255.255.255.0**.
- Associate the DHCP server with **port2** using **set interface port2**.
- Enter the IP range configuration mode to define the range of addresses that the DHCP server will offer to clients with **config ip-range**.
- Add a new IP range entry with **edit 1**.
- Set the start of the IP range with **set start-ip 10.128.0.100**.
- Set the end of the IP range with **set end-ip 10.128.0.199**.
- Exit the IP range configuration mode with **next**.

- Exit the DHCP server configuration mode with **end**.
- Optionally, verify the DHCP server configuration using **show system dhcp server**.



Slide 4 Instructions:

- On the Windows 10 client virtual machine within GNS3, open the Command Prompt.
- Verify the IP configuration details by executing **ipconfig /all**. Look for the following:
 - DHCP Enabled: Yes
 - Autoconfiguration Enabled: Yes
 - IPv4 Address: Check that the address is within the range you specified in the DHCP server configuration (10.128.0.100 to 10.128.0.199).
 - Subnet Mask, Default Gateway, and DHCP Server: Ensure these are correctly assigned (should match the settings from the FortiGate DHCP configuration).
 - DNS Servers: Verify if the DNS server addresses are correctly assigned.
- Test connectivity to the default gateway by pinging it: **ping 10.128.0.1**. You should receive replies if the network is correctly configured.

- If you don't get a response from the gateway or if the IP configuration is incorrect, troubleshoot the network settings on the client and check the FortiGate interface and DHCP settings.
- If the Windows 10 client is unable to get an IP address or cannot ping the default gateway, ensure that the GNS3 network adapter is connected and configured correctly and that the FortiGate firewall is allowing DHCP traffic on **port2**.

```

QEMU (Win10-1) - TightVNC Viewer
Command Prompt
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8560:8922:4839:f8be%7(Preferred)
IPv4 Address. . . . . : 10.128.0.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, November 28, 2023 4:21:58 PM
Lease Expires . . . . . : Tuesday, December 5, 2023 4:21:57 PM
Default Gateway . . . . . : 10.128.0.1
DHCP Server . . . . . : 10.128.0.1
DHCPv6 IAID . . . . . : 118242625
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-23-10-85-00-0C-29-7B-A4-A5
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled

C:\Users\IEUser>ping 10.128.0.1

Pinging 10.128.0.1 with 32 bytes of data:
Reply from 10.128.0.1: bytes=32 time=1ms TTL=255
Reply from 10.128.0.1: bytes=32 time=1ms TTL=255
Reply from 10.128.0.1: bytes=32 time=1ms TTL=255
Reply from 10.128.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.128.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\IEUser>
  
```

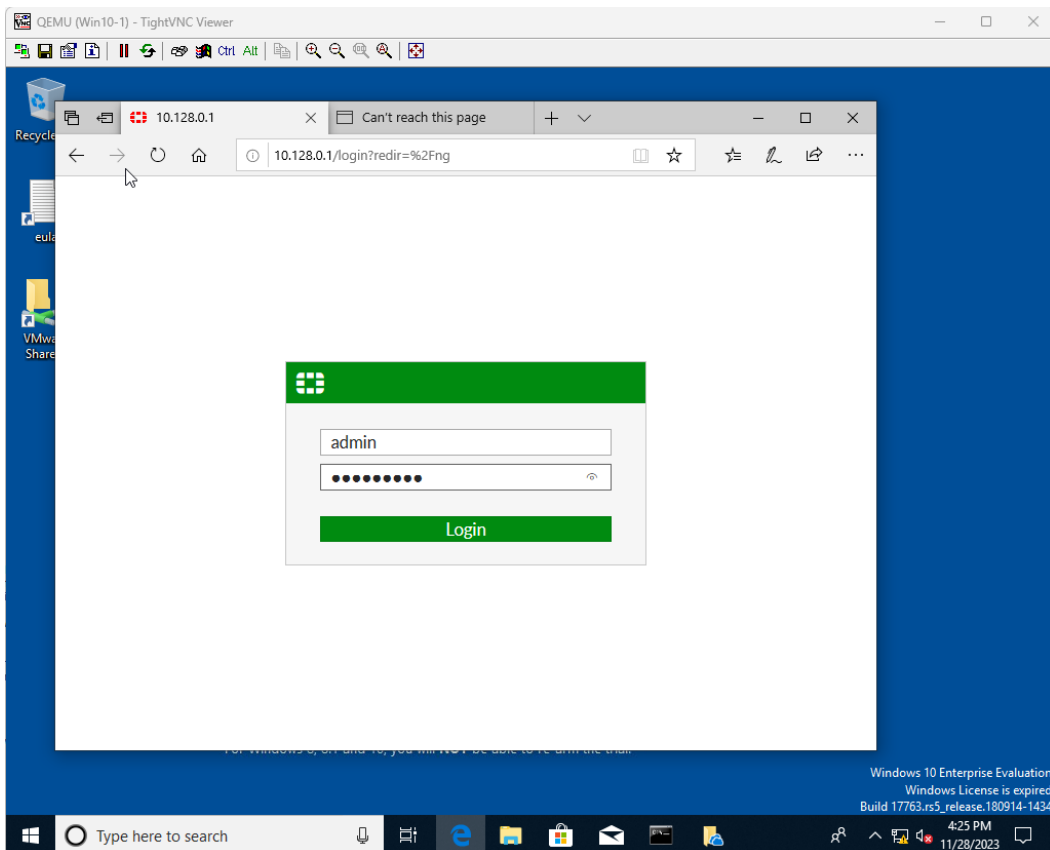
Windows 10 Enterprise Evaluation
Windows License is expired
Build 17763.rs5_release.180914-1434

4:23 PM
11/28/2023

Slide 5 Instructions:

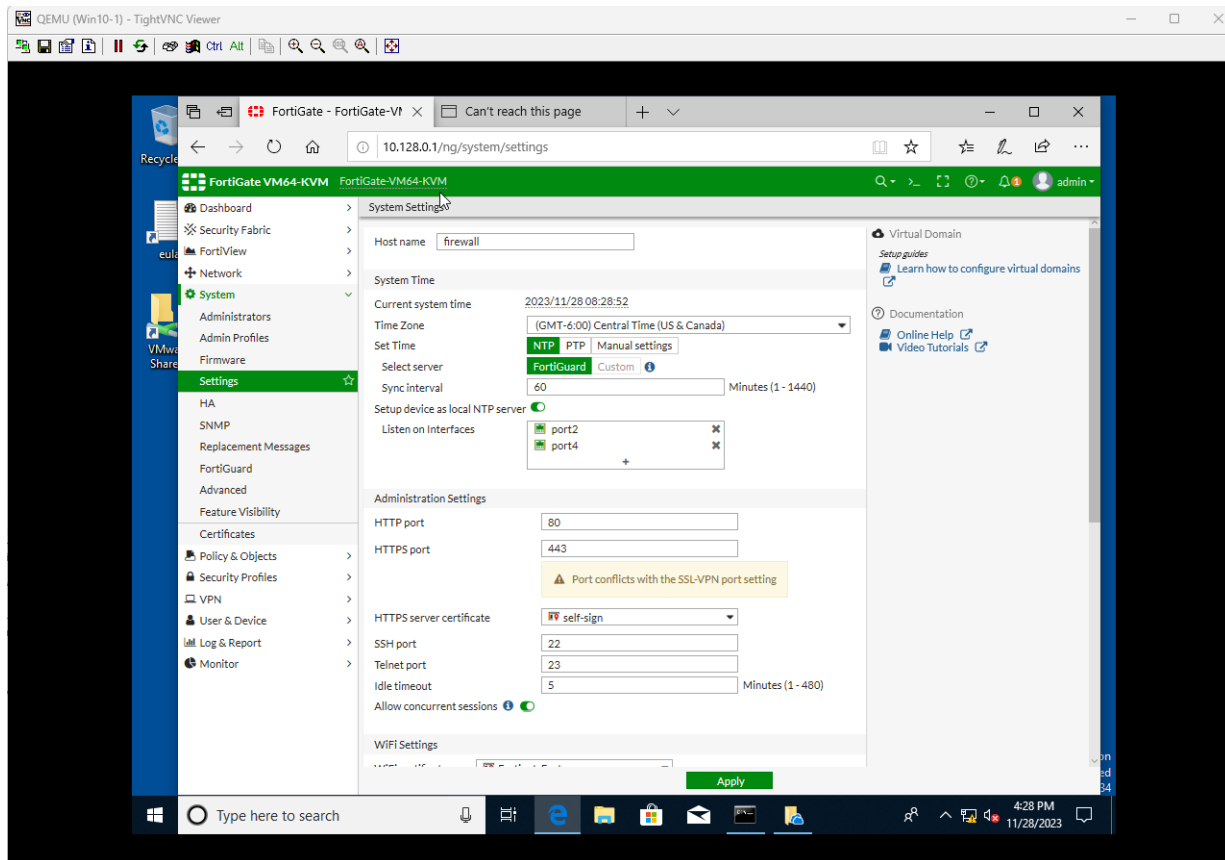
- On the Windows 10 client within GNS3, open a web browser.

- Attempt to access the FortiGate firewall's web-based management interface by entering the firewall's IP address into the browser's address bar:
<http://10.128.0.1>.
- If the login page does not load (as indicated by "Can't reach this page"), check the following:
 - Confirm that the client's IP configuration is correct and that it is on the same network as the FortiGate's interface **port2**.
 - Ensure that the firewall rules on FortiGate are configured to allow HTTP access to the management interface from the subnet assigned to **port2**.
 - Verify network connectivity by pinging the FortiGate's IP address from the command prompt: **ping 10.128.0.1**.
 - Check that the FortiGate services are running and that the HTTP service is enabled on **port2**.
- If the page loads but you cannot log in, ensure that you are using the correct credentials that were set up during the initial FortiGate configuration.



Slide 6 Instructions:

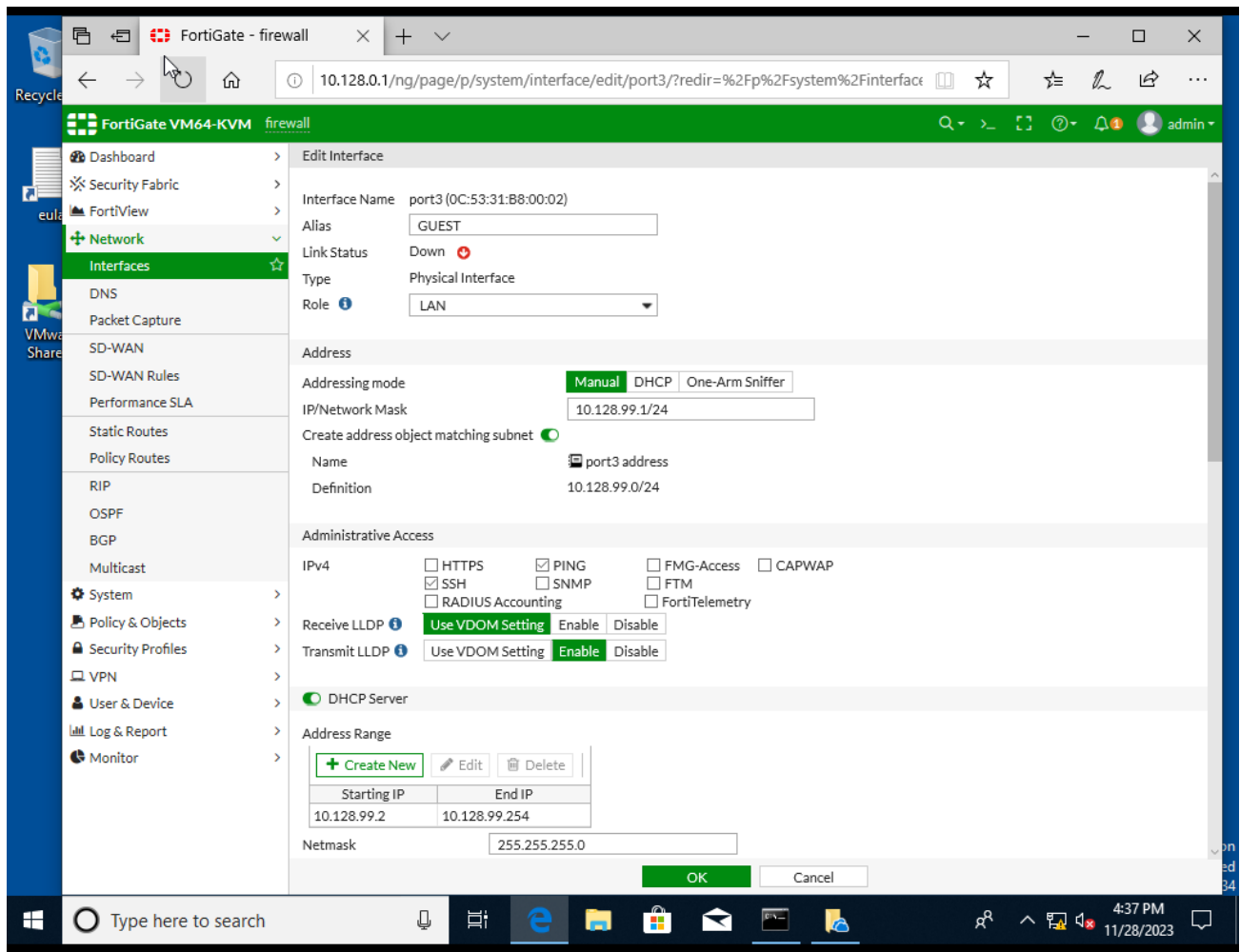
- Log into the FortiGate web interface from the Windows 10 client VM.
- Navigate to the 'System' settings, then 'Settings' to access the system configuration options.
- Verify or configure the following settings as needed:
 - **Host Name:** Confirm or set the host name for the FortiGate device, such as 'firewall'.
 - **System Time:** Configure the correct time zone for the firewall. Set up the NTP (Network Time Protocol) server settings to ensure the firewall has the correct time, which is critical for logging and security purposes. You can use the default FortiGuard servers or specify a custom NTP server.
 - **Listen on Interfaces:** Select the interfaces that the NTP service should listen on, typically including the internal interfaces such as 'port2'.
 - **Administration Settings:** Confirm the HTTP and HTTPS ports for web administration (default values are typically 80 for HTTP and 443 for HTTPS). Adjust if necessary and resolve any port conflicts.
 - **HTTPS server certificate:** Choose an HTTPS server certificate. The default setting is usually a self-signed certificate, but in a production environment, a certificate from a trusted CA would be recommended.
 - **SSH Port:** Verify the SSH port number for secure command-line management access.
 - **Telnet Port:** Disable Telnet if it is not needed, as it is not secure.
 - **Idle Timeout:** Set the idle timeout value for the admin session.
- Click 'Apply' to save the system settings.



Slide 7 Instructions:

- In the FortiGate web interface on the Windows 10 client, navigate to the 'Network' section and then 'Interfaces'.
- Select the interface you wish to configure for guest access, typically labeled as **port3** or similar.
- Set the addressing mode to 'Manual' and assign an IP/Network Mask to the interface, such as **10.128.99.1/24**. This will be the default gateway for the guest network.
- Under the 'Role' setting, ensure 'LAN' is selected to designate this interface as part of the internal network.
- Under 'Administrative Access', enable the required services such as HTTP, HTTPS, PING, or SSH according to your network's administrative needs.
- Scroll down to the 'DHCP Server' section and enable it by toggling the switch if it's not already enabled.

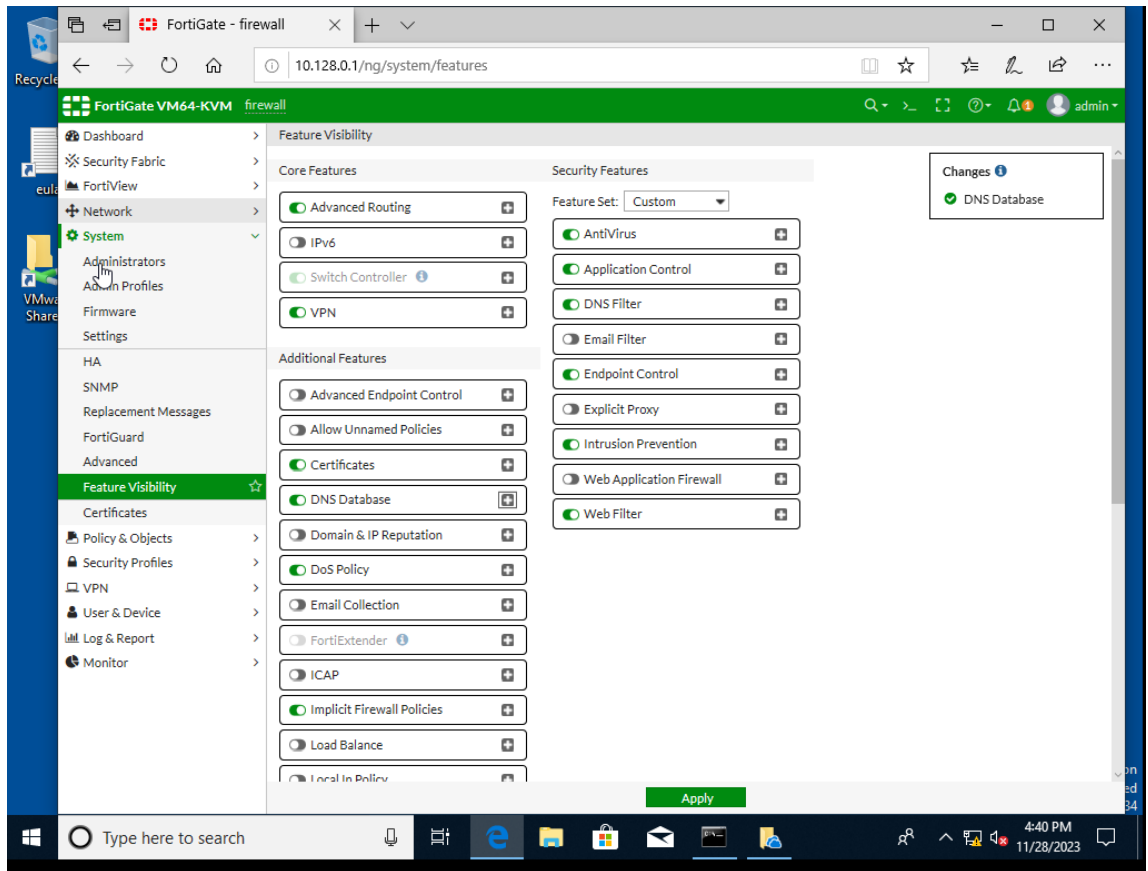
- Configure the DHCP Address Range for the guest network. Click on 'Create New' to add a new DHCP range.
- Input the desired range, e.g., **Start IP: 10.128.99.2** and **End IP: 10.128.99.254**, which will define the pool of IP addresses that the DHCP server can assign to guest devices.
- Confirm the netmask is set correctly, which in this case should be **255.255.255.0**.
- Click 'OK' to apply the settings.



Slide 8 Instructions:

- In the FortiGate VM's web interface on the Windows 10 client, go to the 'System' section and click on 'Feature Visibility'.

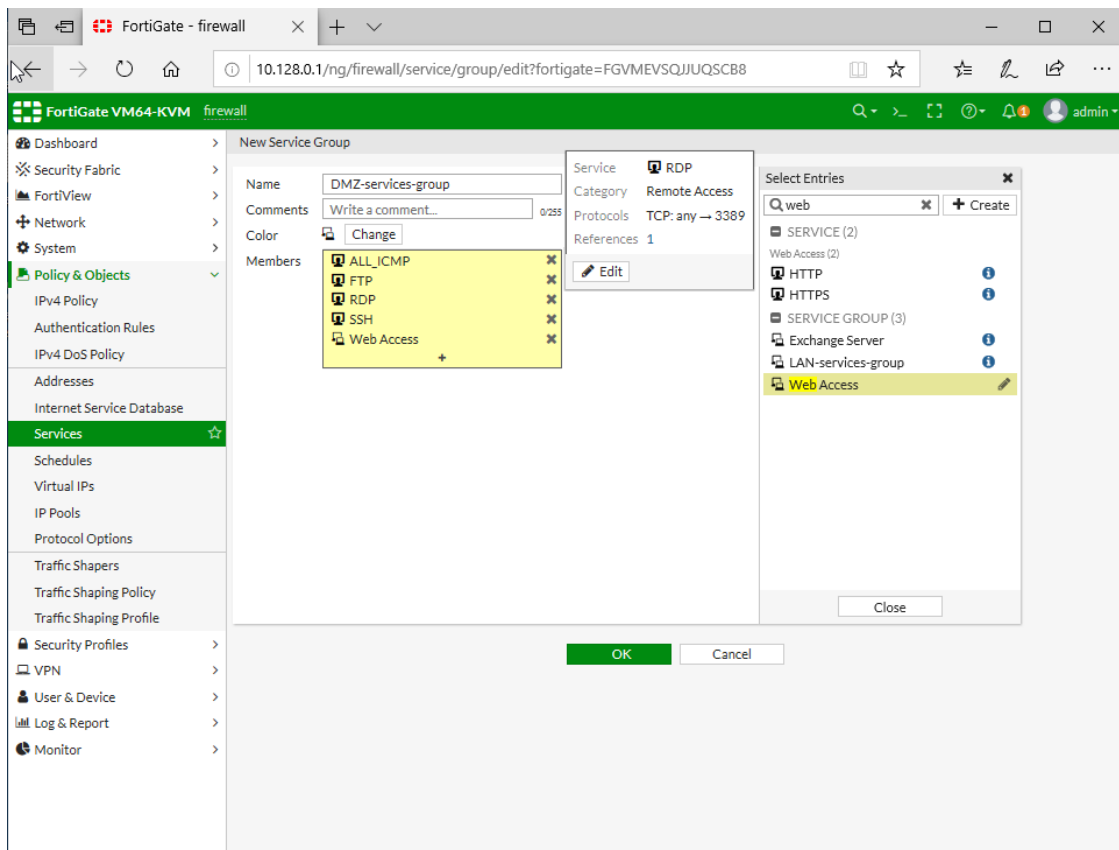
- You will see a list of core and additional features that can be enabled or disabled depending on your network requirements. This controls what options are available in the web interface.
- For core features:
 - Enable 'Advanced Routing' if you plan to use dynamic routing protocols like OSPF or BGP.
 - Ensure 'IPv6' is enabled if your network supports IPv6 addressing.
 - Verify 'VPN' is enabled if you require Virtual Private Network capabilities.
 - Check 'AntiVirus', 'Application Control', 'DNS Filter', 'Web Filter', and any other security features you need for protecting your network.
- For additional features:
 - Toggle on 'Certificates' to manage SSL certificates for secure communications.
 - Enable 'DNS Database' if you want to configure a local DNS database.
 - Consider enabling 'Domain & IP Reputation' for enhanced security based on reputation scores.
 - 'DoS Policy' should be enabled to protect against Denial of Service attacks.
 - Adjust other features like 'Email Filter', 'Explicit Proxy', 'Intrusion Prevention', etc., as per your security policy.
- After configuring the visibility of features according to your network's needs, click 'Apply' to save the changes.



Slide 9 Instructions:

- Access the FortiGate VM's web interface from the Windows 10 client.
- Navigate to 'Policy & Objects' and select 'Services' to manage the service groups and services used in firewall policies.
- To create or modify a service group (such as 'DMZ-services-group'), perform the following steps:
 - Click on the 'New Service Group' button if you need to create a new group, or select an existing group to edit.
 - Name the group appropriately, for example, 'DMZ-services-group' to identify the services allowed for the DMZ (Demilitarized Zone) segment of your network.
 - Add a comment if needed for administrative purposes.
 - You can change the color to visually distinguish this group in the interface list.

- Add members to the group by selecting from predefined services like FTP, HTTP, HTTPS, RDP, SSH, etc., or create custom services as required.
- Ensure that the services required for operation in the DMZ, such as web access (HTTP and HTTPS), are included.
- Verify the service category and protocols are correct for each service. For example, for web access, the service should be categorized under 'Remote Access' and use TCP protocol with the standard ports for HTTP (80) and HTTPS (443).
- Once all necessary services are added to the group, click 'OK' to save the configuration.



Slide 10 Instructions:

- Open the FortiGate VM web interface on the Windows 10 client.
- Navigate to the 'Network' section and select 'DNS' to configure DNS settings.

- You will see two sections: 'DNS Service on Interface' and 'DNS Database':
 - Under 'DNS Service on Interface', you can assign DNS services to specific interfaces such as LAN, GUEST, and DMZ. Click 'Create New' to add a new DNS service or select an existing interface to edit its DNS settings. Set the mode to 'Recursive' if you want the FortiGate to perform recursive DNS resolution.
 - For the 'DNS Database', this is where you can define your own DNS records and zones. Since there are 'No matching entries found', you can create a new DNS zone by clicking 'Create New'.
 - In the new zone, you would specify the domain name for which the FortiGate is authoritative, and you can add records such as A, AAAA, CNAME, MX, etc., that will resolve within your network.
- After configuring DNS services for each interface, ensure that the DNS settings are correct and match the intended network design, particularly if you are segmenting networks with different DNS requirements (e.g., a separate DNS server for guests versus internal users).
- Once all configurations are complete, click 'Apply' to save the settings.

The screenshot shows the FortiGate VM64-KVM firewall interface. The left sidebar contains a navigation menu with categories like Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, Log & Report, and Monitor. The 'Network' category is expanded, and 'DNS Servers' is selected. The main content area is titled 'DNS Service on Interface' and contains a table of DNS servers. Below this is the 'DNS Database' section, which is currently empty.

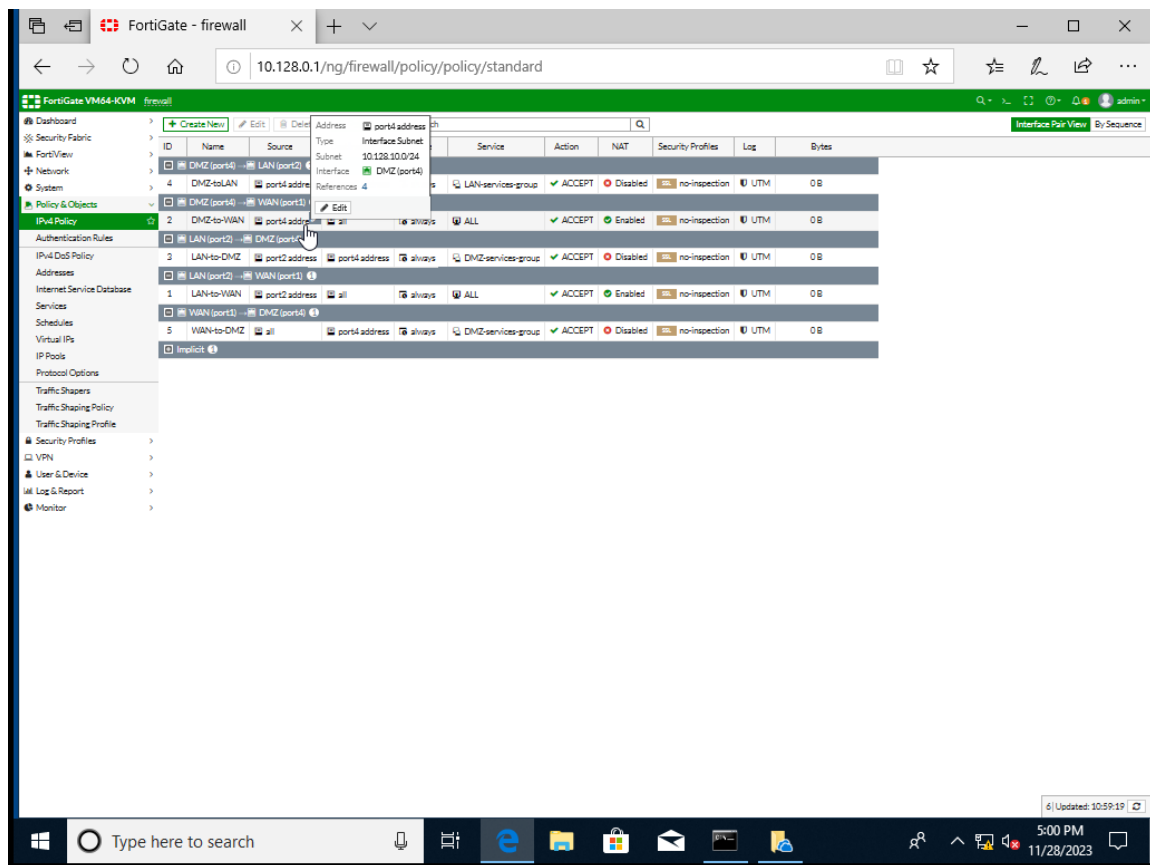
Interface	Mode	DNS Filter
LAN (port2)	Recursive	
GUEST (port3)	Recursive	
DMZ (port4)	Recursive	

DNS Zone	Domain Name	Type	View	TTL (seconds)	# of Entries
No matching entries found					

Slide 11 Instructions:

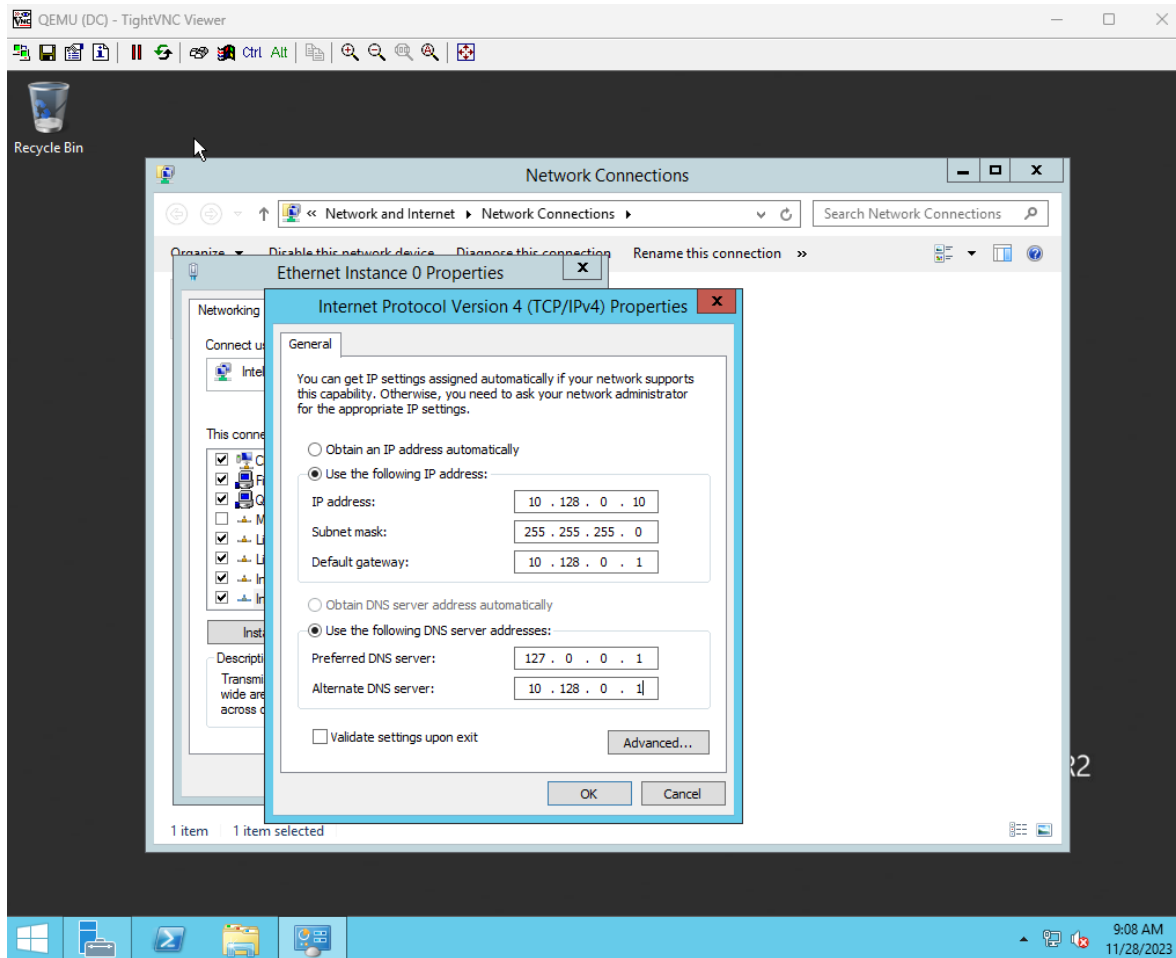
- Access the FortiGate VM64-KVM firewall interface.
- Navigate to the 'Policy & Objects' section and then to 'IPv4 Policy'. This area allows you to define and manage access control policies that determine the traffic flow through the firewall.
 - Each line represents a specific policy rule with details about source, destination, schedule, service, action, and other attributes.
 - The source and destination columns typically contain the names of the predefined address objects or groups that specify which IP addresses the policy applies to.
 - The 'Action' column indicates whether the policy will allow or deny traffic matching its criteria.

- To add a new policy, click on the '+ Create New' button located at the top left of the policy list.
 - In the new policy setup, you will need to specify the incoming and outgoing interfaces, source and destination addresses, schedule for when the policy is active, and the services it applies to.
 - Under 'Action', choose whether this policy will allow or deny the traffic. If allowing, you can also specify if NAT will be applied.
 - Security profiles can be attached to the policy to apply various security measures like antivirus scans, web filtering, application control, and more.
- After setting up your policy, click 'OK' to save and apply the changes. If you are editing an existing policy, ensure that the changes are correct and do not inadvertently block or allow traffic that should be handled differently.
- It's good practice to review the policy list to ensure that the rules are in the correct order, as the firewall processes them top-down, stopping at the first match.



Slide 12 Instructions:

- Open the Network and Sharing Center on the Windows machine you are configuring.
- Navigate to the Ethernet settings by clicking on the Ethernet link. This will typically be labeled with the connection name, such as "Ethernet" or "Local Area Connection".
- Within the Ethernet status window, click on 'Properties'. You may require administrative privileges to access these settings.
- In the Ethernet Properties window, scroll down and select 'Internet Protocol Version 4 (TCP/IPv4)' then click on 'Properties'.
- You have the option to obtain an IP address automatically if DHCP is enabled on the network, or to use a specific IP address:
 - To set a static IP address (as shown in the slide), select 'Use the following IP address':
 - Enter the IP address: **10.128.0.10**
 - Subnet mask: **255.255.255.0** (This is a standard subnet mask for a /24 network)
 - Default gateway: **10.128.0.1** (This should be the IP address of your router or default gateway device)
- Additionally, set the DNS server addresses if required:
 - Preferred DNS server: **127.0.0.1** (This suggests the machine uses itself as the DNS server, which might be the case if it's running a DNS service)
 - Alternate DNS server: **10.128.0.1** (This might be your network's secondary DNS server, possibly your gateway or a dedicated DNS server)
- After entering the IP settings, select 'Validate settings upon exit' to ensure that there are no immediate issues with the configuration.
- Click 'OK' to save the settings and close the properties window. Your network connection will likely reset to apply these settings.
- If necessary, test the connection by pinging the default gateway or another known address on the network to confirm connectivity.



Slide 13 Instructions:

- Open Windows PowerShell or Command Prompt with administrative privileges on the Windows Server.
- Begin by testing connectivity to the default gateway to ensure network configuration is correct:
 - Type **ping 10.128.0.1** and press Enter.
 - If successful, you should see replies indicating that the packets are reaching the default gateway.
- Next, verify external connectivity by pinging a well-known public DNS server:
 - Type **ping 8.8.8.8** and press Enter.
 - If successful, this confirms that the server has internet access.

- For a more comprehensive test, you can perform a ping to a common domain to ensure DNS resolution is functioning:
 - Type **ping google.com** and press Enter.
 - Successful replies indicate that the server can resolve domain names, which implies properly working DNS settings.
- Review the ping statistics for each test to ensure there is no packet loss and that the time taken for the round trip is within acceptable limits. This is critical for assessing network health and connectivity.
- If there are any issues with the pings, you may need to troubleshoot network settings, check firewall configurations, or verify that DNS services are operational on the server.
- Once all pings are successful, it's recommended to conduct further network services testing if required, such as using **tracert** to follow the path packets take to their destination or using **nslookup** to directly query DNS servers.
- Document any irregularities or issues observed during the testing for further analysis or to inform network administrators for potential network enhancements.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> ping 10.128.0.1

Pinging 10.128.0.1 with 32 bytes of data:
Reply from 10.128.0.1: bytes=32 time=1ms TTL=255
Reply from 10.128.0.1: bytes=32 time<1ms TTL=255
Reply from 10.128.0.1: bytes=32 time<1ms TTL=255
Reply from 10.128.0.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.128.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Administrator> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=6ms TTL=55
Reply from 8.8.8.8: bytes=32 time=6ms TTL=55
Reply from 8.8.8.8: bytes=32 time=6ms TTL=55
Reply from 8.8.8.8: bytes=32 time=5ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 6ms, Average = 5ms
PS C:\Users\Administrator> ping google.com

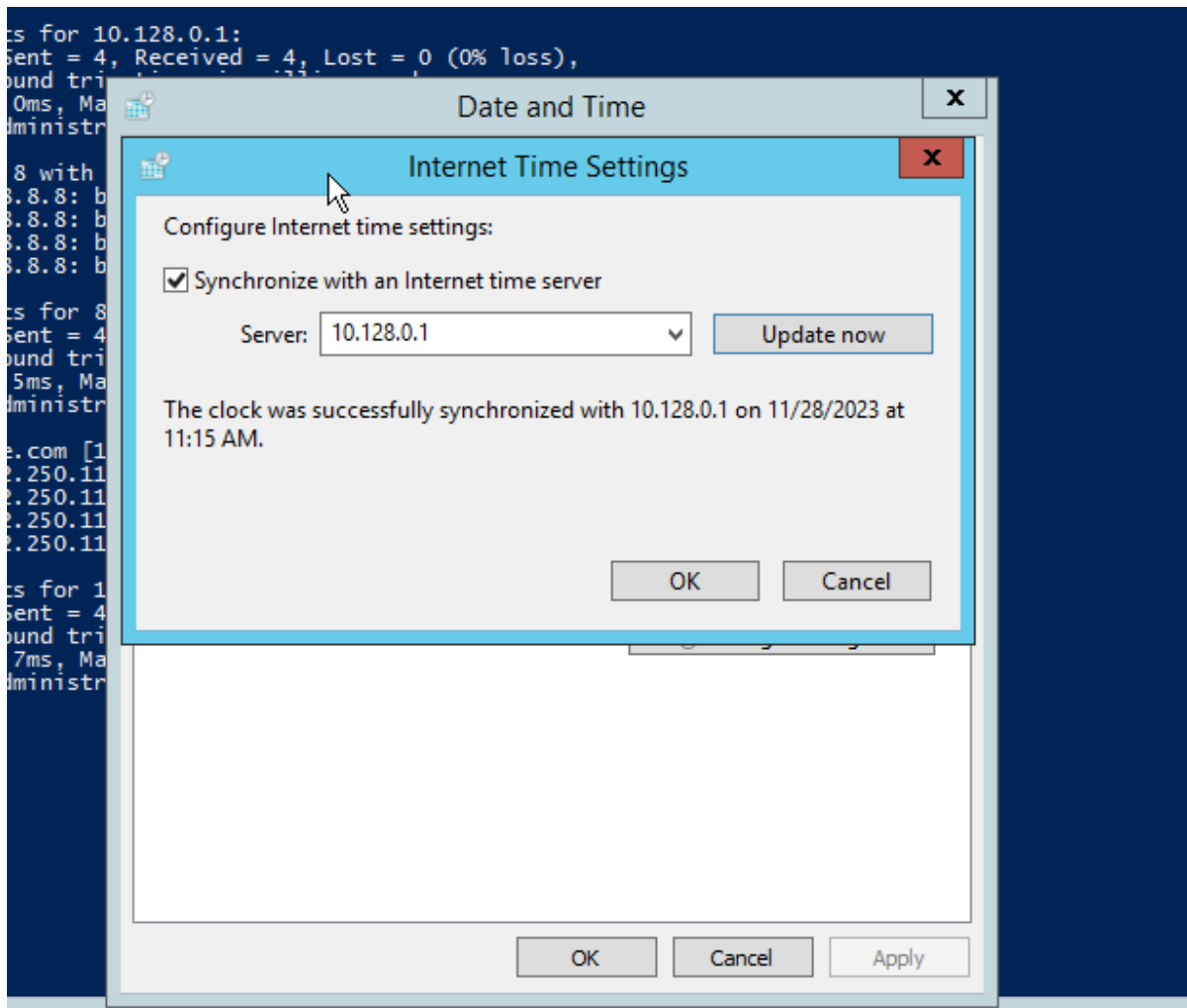
Pinging google.com [142.250.115.102] with 32 bytes of data:
Reply from 142.250.115.102: bytes=32 time=8ms TTL=105
Reply from 142.250.115.102: bytes=32 time=7ms TTL=105
Reply from 142.250.115.102: bytes=32 time=7ms TTL=105
Reply from 142.250.115.102: bytes=32 time=7ms TTL=105

Ping statistics for 142.250.115.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 8ms, Average = 7ms
PS C:\Users\Administrator>
  
```

Slide 14 Instructions:

- Access the Date and Time settings on the Windows Server or client machine by right-clicking on the time display in the taskbar and selecting "Adjust date/time" or accessing through the Control Panel.
- Navigate to the Internet Time tab, which allows you to synchronize the system clock with an internet time server for accurate timekeeping.
- To configure the settings:
 - Click on the "Change settings..." button (if it's greyed out, you may need administrative privileges).
 - Check the box for "Synchronize with an Internet time server".

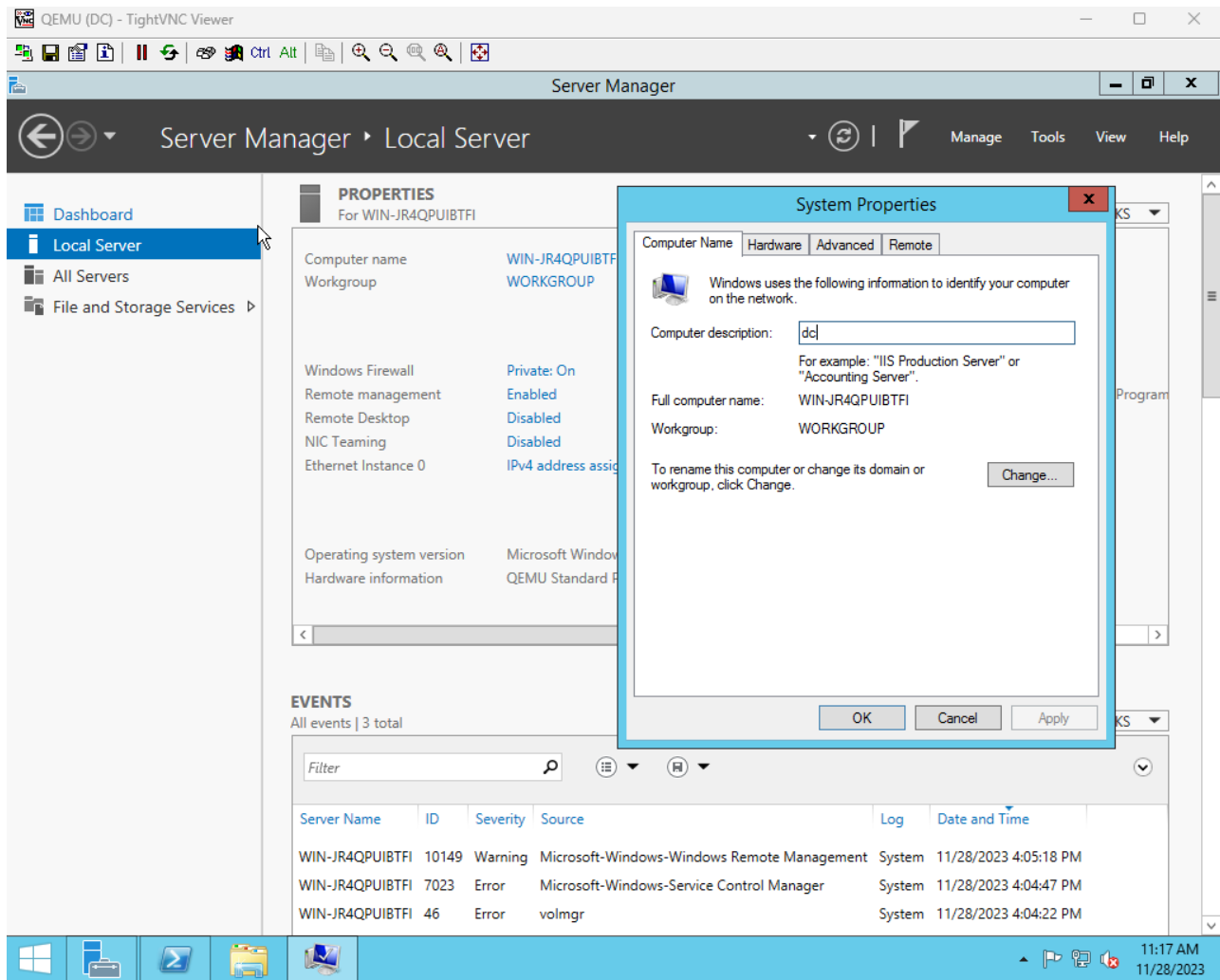
- In the "Server" field, enter the IP address or domain name of the preferred NTP server. In this case, **10.128.0.1** is being used, which likely refers to an internal time server.
 - Click "Update now" to manually synchronize the time.
- After clicking "Update now", the system should attempt to connect to the time server and update the system clock accordingly. If successful, you will see a confirmation message indicating the last successful sync time.
- Confirm the changes by clicking "OK" or "Apply". This will ensure that the settings are saved and the system clock remains accurate.
- It's important to ensure that the time is synchronized, especially in a domain environment where Kerberos authentication relies on time accuracy between servers and clients.
- If the synchronization fails, you should check the network connectivity to the NTP server, ensure the server is operational, and verify that no firewall is blocking the NTP port (default UDP 123).
- Document the successful synchronization for maintenance logs and troubleshooting future time-related issues.



Slide 15 Instructions:

- Open Server Manager if it's not already open. This is usually found in the taskbar or can be searched for in the Start menu.
- In the Server Manager, click on 'Local Server' on the left-hand panel. This will show you an overview of the local server's properties.
- Locate 'Computer name' in the 'Properties' section. If you need to change the computer name or join a domain/workgroup, proceed with the following steps.
- Click on the 'Change...' button. This will open the 'System Properties' dialog box.
- In the 'Computer Name' tab of the 'System Properties' dialog box, you will see the current computer name and the workgroup or domain it belongs to.
- To change the computer name:

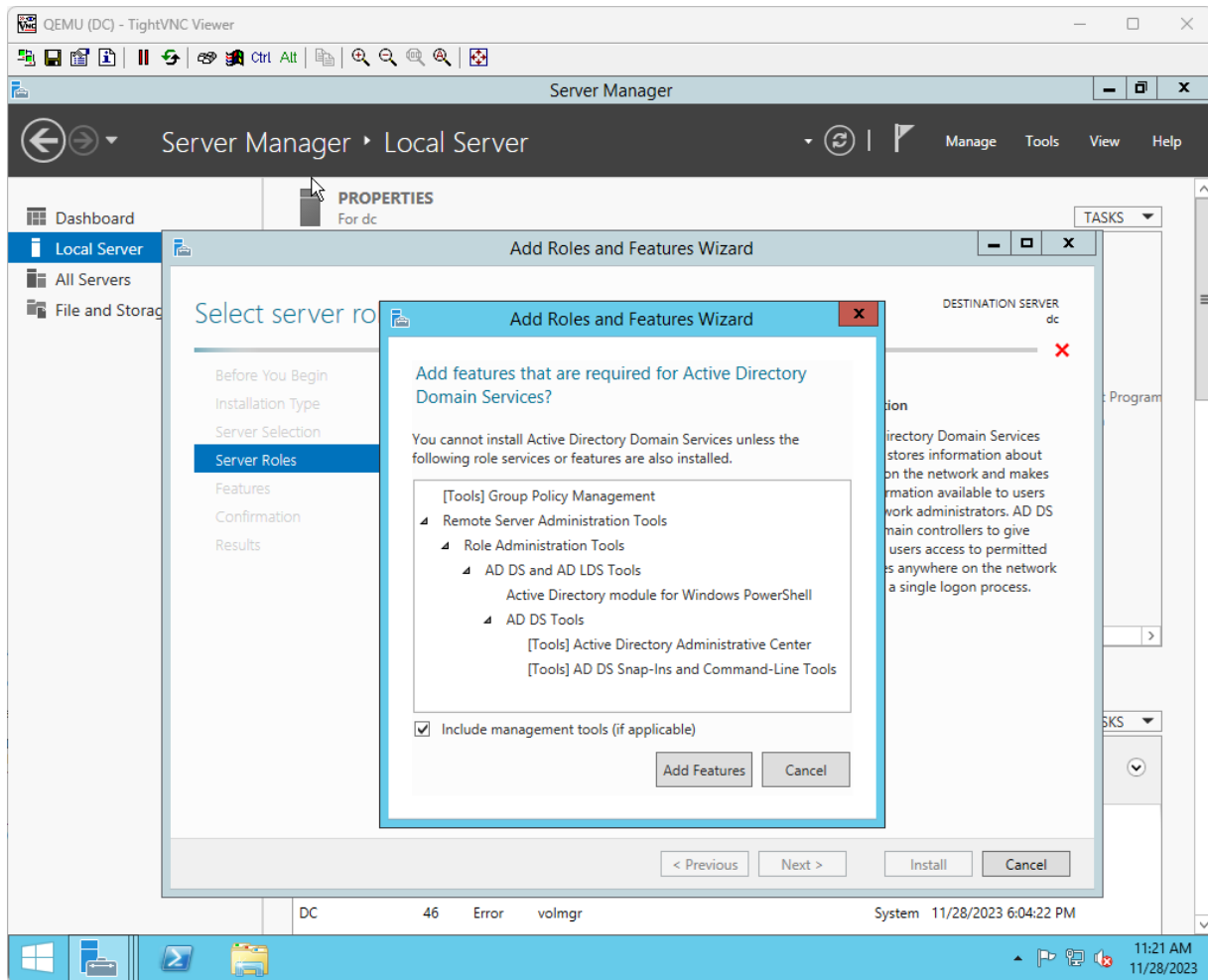
- Click the 'Change...' button.
- Enter the new computer name in the 'Computer name' field. In this scenario, it looks like the intention might be to change it or join a domain.
- To join a domain, select the 'Domain' radio button and enter the domain name in the text field. If you want to work in a workgroup environment, select 'Workgroup' and enter the workgroup name.
- Click 'OK' once you've made your changes. A prompt may appear asking for credentials if you're joining a domain.
- After clicking 'OK', you may be prompted to restart the computer for the changes to take effect.
- Ensure you document the changes made, and if this is a server, plan the reboot accordingly to minimize the impact on services.
- Verify network settings and ensure the server has the correct IP configuration to communicate with the domain controller if joining a domain.



Slide 16 Instructions:

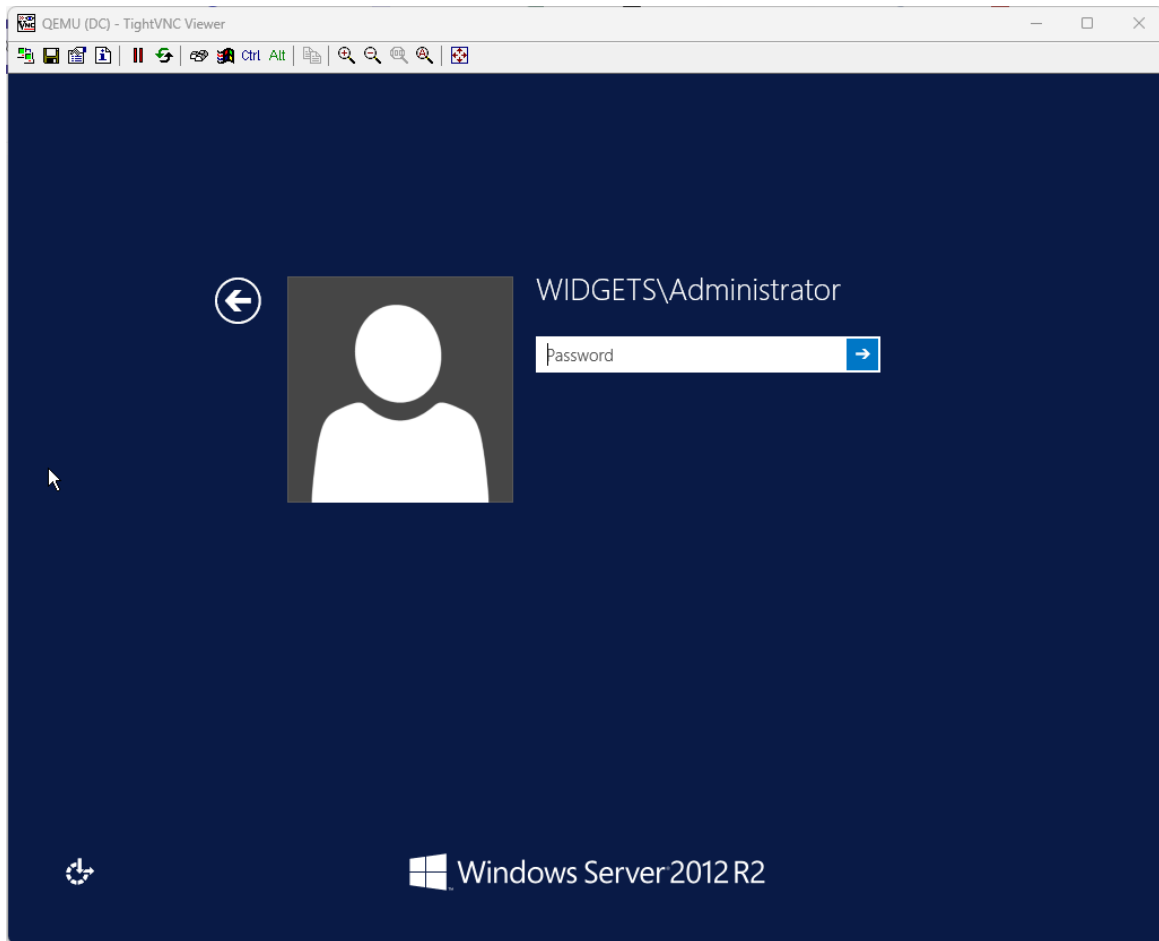
- In Server Manager, ensure you have selected the 'Roles' category on the left-hand panel. If not, click on 'Roles' to proceed.
- On the 'Roles' page, click 'Add Roles and Features' to open the Add Roles and Features Wizard.
- The wizard will guide you through the installation process:
 - On the 'Before You Begin' page, read the information provided and click 'Next' to proceed.
 - Select the 'Role-based or feature-based installation' option and click 'Next'.
 - Choose the appropriate server from the server pool and click 'Next'.

- On the 'Select server roles' page, find and check the 'Active Directory Domain Services' role. A new window will pop up, indicating additional features that are required for Active Directory Domain Services.
- Review the additional features required. It typically includes tools like Group Policy Management and role administration tools that are necessary for effective AD DS management.
- Ensure 'Include management tools (if applicable)' is checked to get the AD DS Snap-Ins and Command-Line Tools along with the server role.
- Click 'Add Features' on the pop-up window to add the required features for Active Directory Domain Services to your selection.
- Back on the 'Select server roles' page, with 'Active Directory Domain Services' checked, click 'Next' to continue.
- If there are additional features or roles you wish to install at this time, you can select them as well. Otherwise, just click 'Next' until you reach the 'Confirmation' page.
- Review your selections on the 'Confirmation' page. Optionally, you can check the 'Restart the destination server automatically if required' option. Be aware this will reboot your server without further prompting, which could impact users if this is a production environment.
- Click 'Install' to begin the installation of the Active Directory Domain Services role and any selected features. The installation process may take some time.
- Once the installation is complete, you will need to promote the server to a domain controller, which involves additional configuration steps and potentially another server restart.
- Document the changes, and if necessary, plan for a maintenance window to minimize the impact on services for further steps in promoting the server to a domain controller.



Slide 17 Instructions:

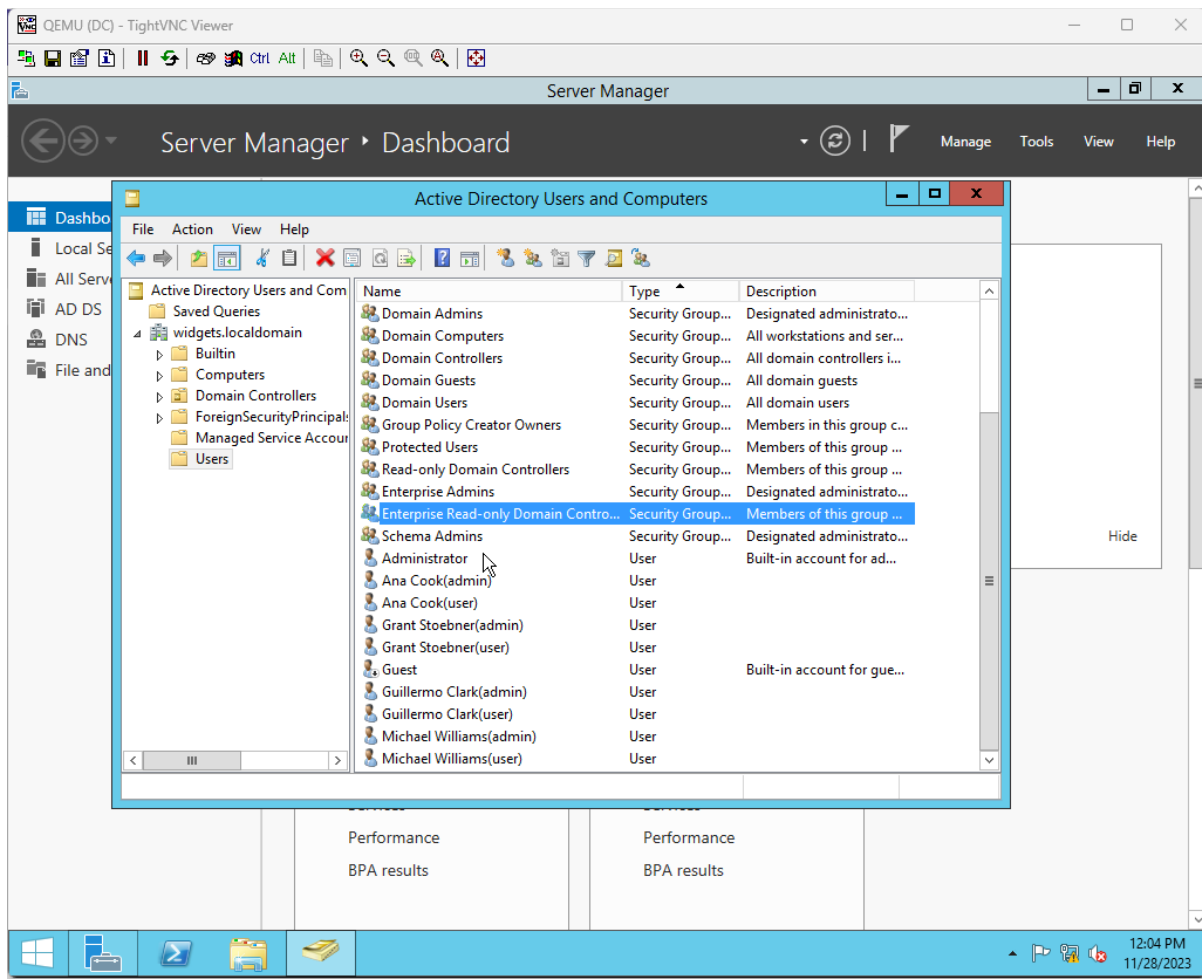
- At the Windows Server login screen, click on the 'Administrator' account to select it.
- Enter the password for the Administrator account in the password field.
- Press 'Enter' or click the arrow button to the right of the password field to log in.
- If the server is part of a domain, ensure you are logging in with the domain administrator account by checking the domain before the username, e.g., **WIDGETS\Administrator**.
- If the password is entered incorrectly, you will receive a notification. Re-enter the password carefully and attempt to log in again.
- Once logged in, you can proceed with server management tasks as required.



Slide 18 Instructions:

- Access the Active Directory Users and Computers management console through the Server Manager Dashboard.
- Navigate to the domain of interest, in this case, **widgets.localdomain**.
- To view or manage user accounts and groups, expand the domain structure.
- Click on 'Users' to see a list of user accounts.
- If you need to modify a user's properties, right-click on the user's name and select 'Properties.'
- You can also manage group memberships by right-clicking on the respective groups under the 'Users' OU (Organizational Unit).

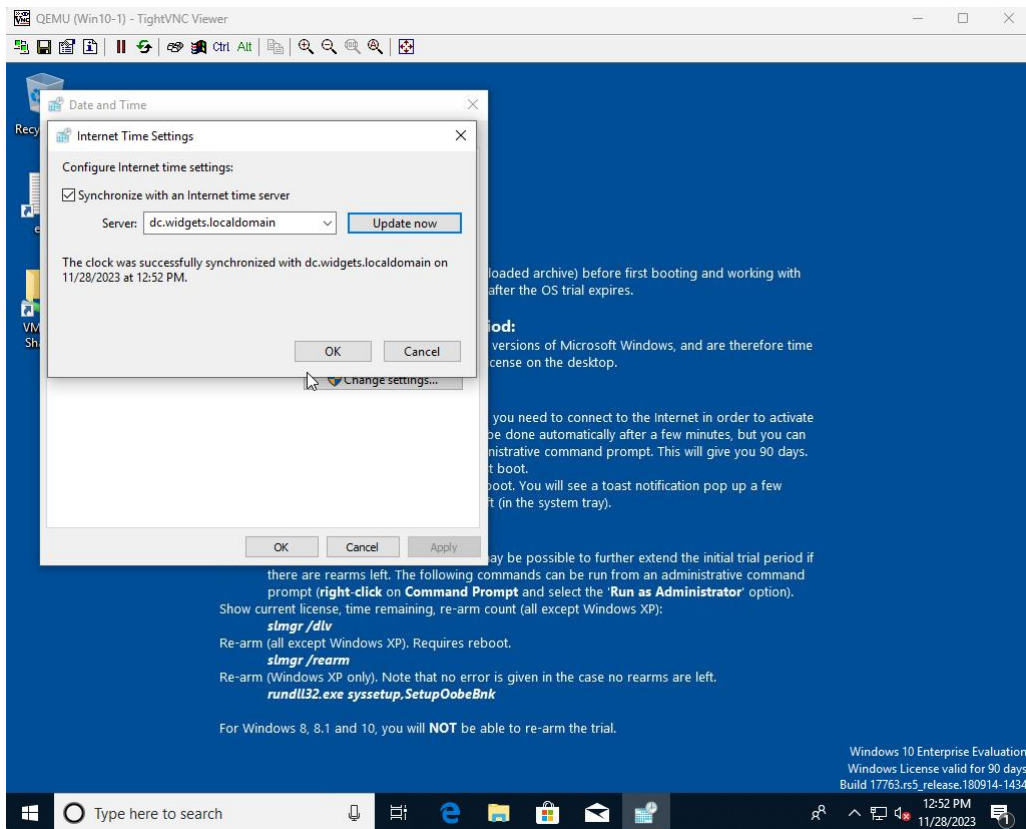
- For more detailed management tasks, you can utilize the 'Action' menu at the top or right-click on the domain, OU, or specific users or groups for a context menu with more options.
- Make sure to apply any changes you make by clicking 'OK' or 'Apply' in the properties windows.
- To close the console when finished, simply click the 'X' at the top right corner or go to 'File' and then 'Exit.'



Slide 19 Instructions:

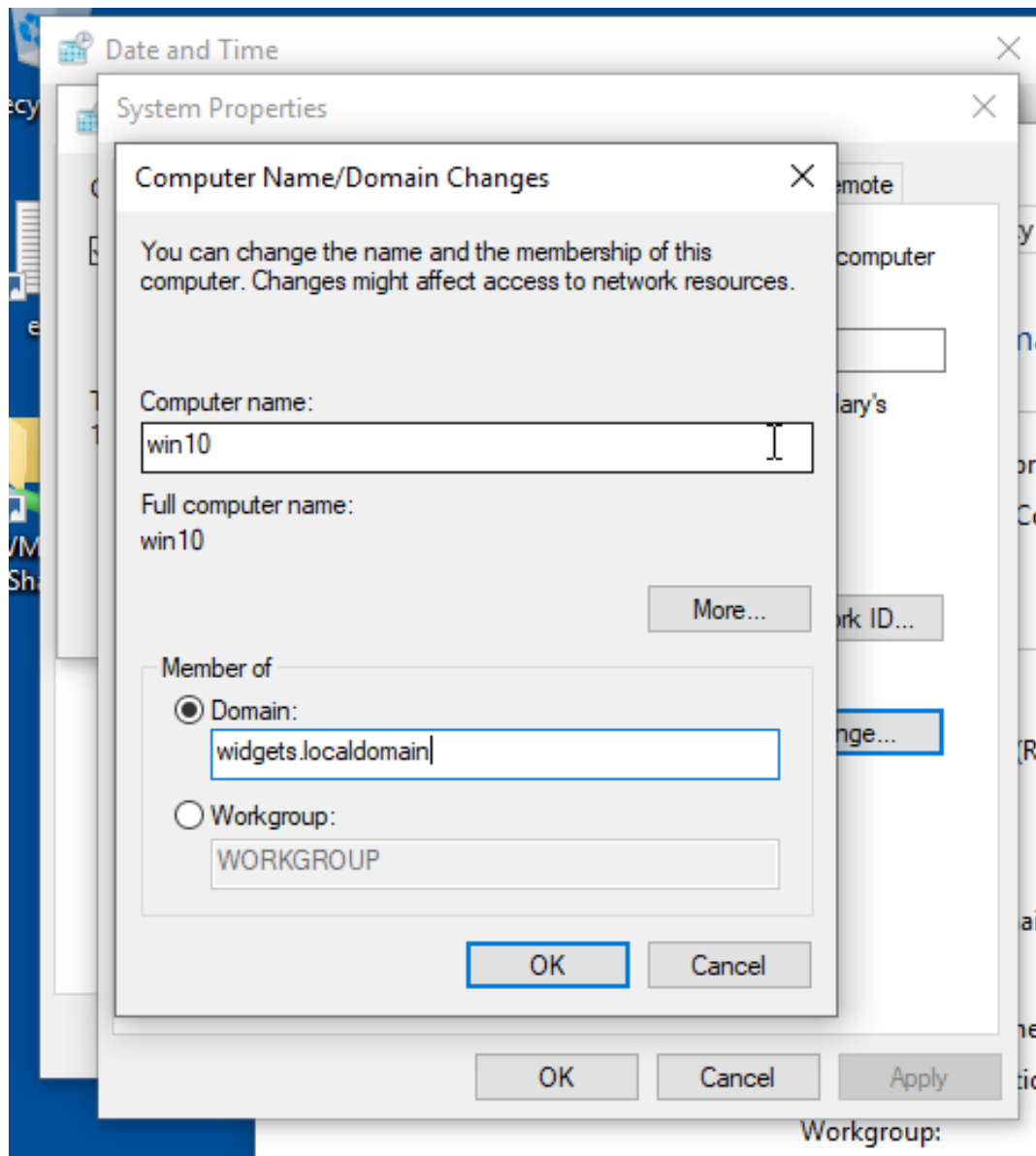
- Open the "Date and Time" settings on your Windows 10 machine by right-clicking on the time display on the taskbar and selecting "Adjust date/time" or through the Control Panel.
- In the "Date and Time" dialog box, navigate to the "Internet Time" tab.

- Click on "Change settings..." to configure internet time settings.
- Ensure the checkbox "Synchronize with an Internet time server" is selected.
- From the server dropdown, select "dc.widgets.localdomain" as the time server to synchronize with. This should be your domain controller configured to provide time services.
- Click "Update now" to synchronize immediately.
- Once the synchronization is successful, you should see a confirmation message with the timestamp of the last successful sync.
- Click "OK" to close the Internet Time Settings dialog.
- Click "OK" again to exit the Date and Time dialog box.
- If any changes were made or the synchronization was updated, a notification might appear or you may see the time adjust on your system clock in the taskbar.



Slide 20 Instructions:

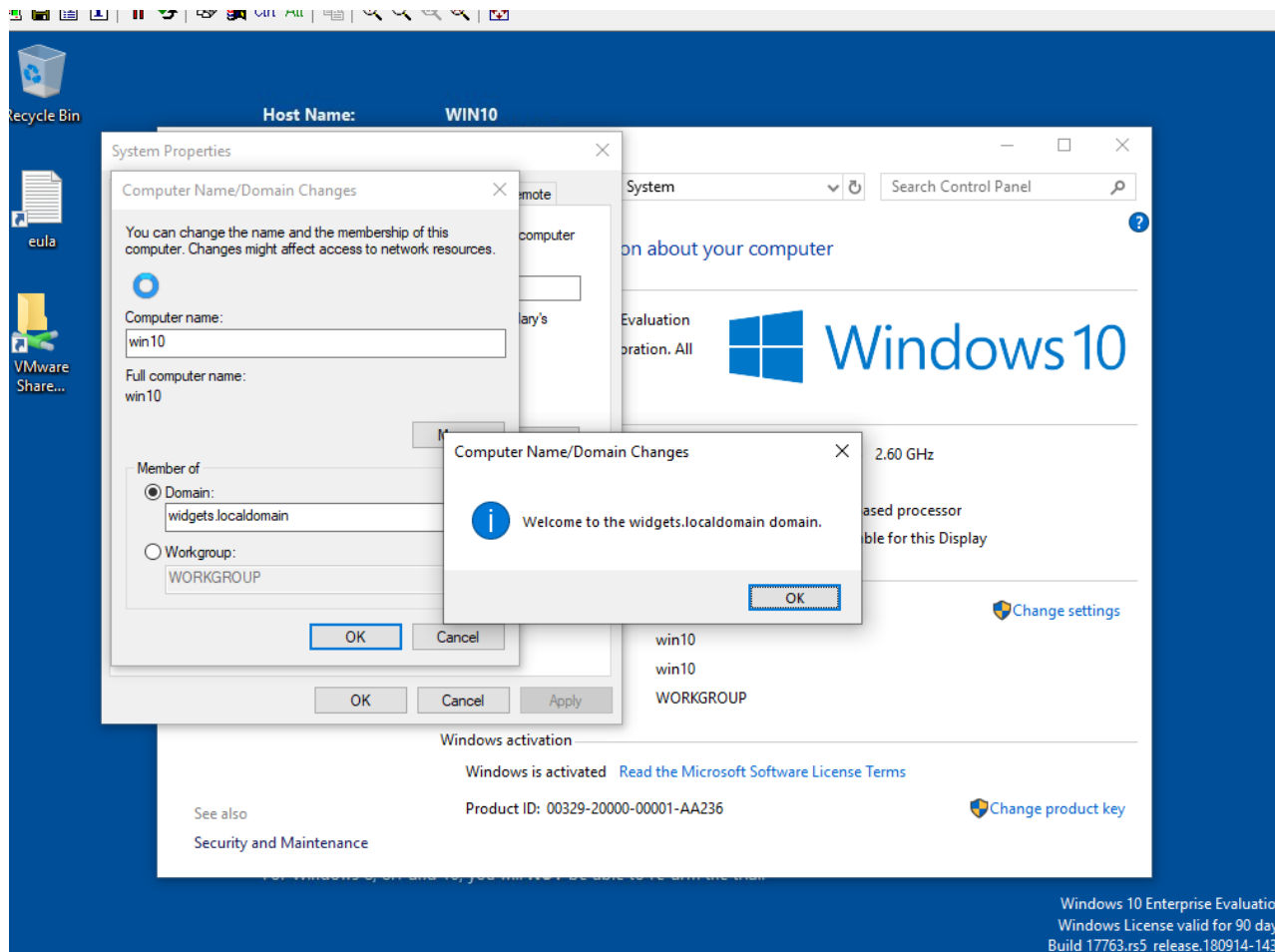
- Access the System Properties dialog box by right-clicking on 'This PC' or 'Computer' on the desktop or in File Explorer and selecting 'Properties'. Then click on 'Advanced system settings'.
- In the System Properties window, go to the 'Computer Name' tab.
- Click on 'Change...' to rename the computer or change its domain or workgroup.
- Under 'Member of', select the 'Domain' radio button to join the computer to a domain.
- In the text field for 'Domain', enter 'widgets.localdomain' which is the name of the domain you want to join.
- After entering the domain name, click 'OK'. You will be prompted to enter credentials that have permission to join the domain.
- Enter the username and password of an account that has the authority to join the domain, then click 'OK'.
- If the domain join is successful, you will receive a welcome message to the domain.
- You will be prompted to restart the computer for the changes to take effect. Save any open work and then click 'OK' to restart.
- After restarting, the computer will be a member of the 'widgets.localdomain' domain.



Slide 21 Instructions:

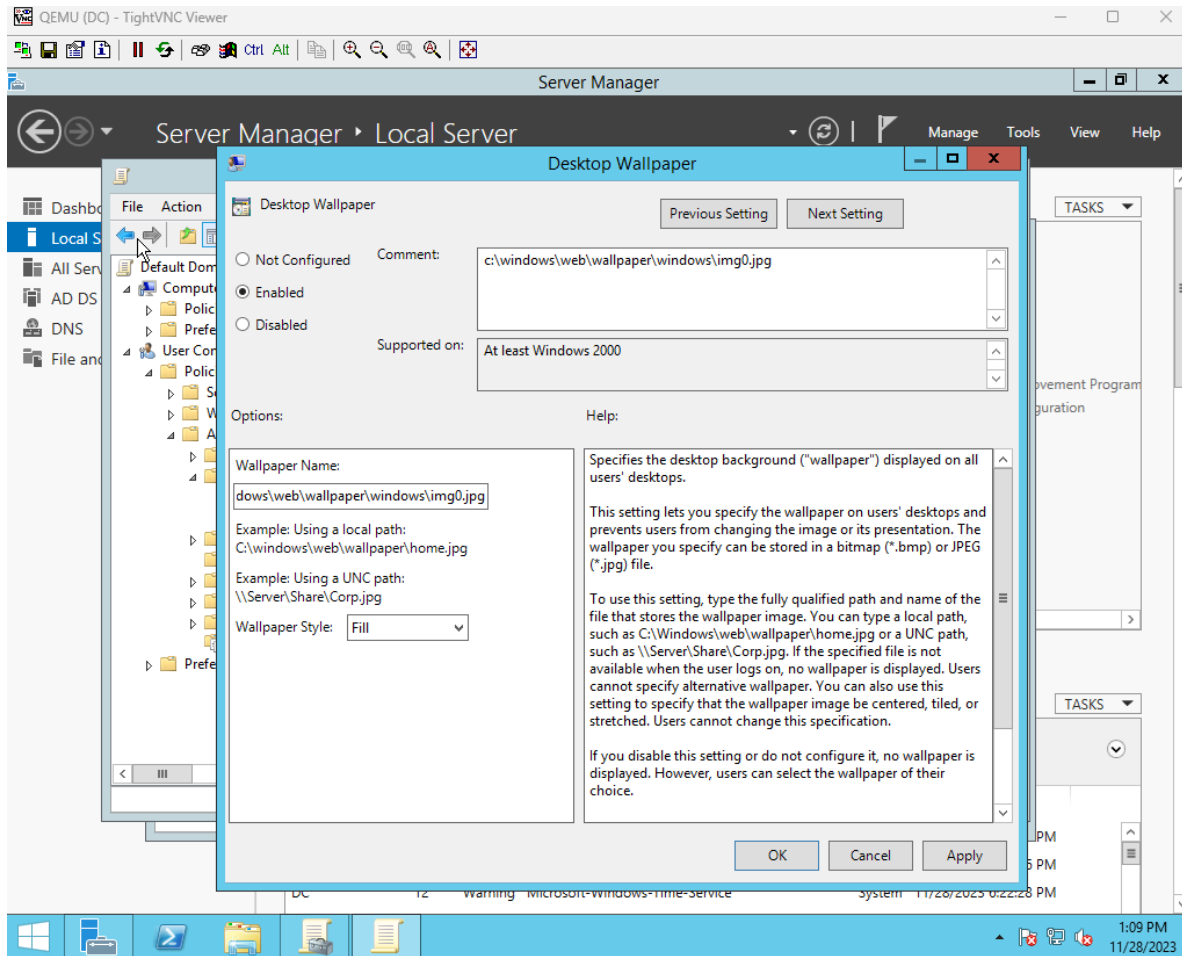
- Navigate to the 'System Properties' by searching for 'This PC' on your desktop, right-clicking on it, and selecting 'Properties'. Then, click on 'Advanced system settings'.
- On the 'System Properties' window, click the 'Computer Name' tab.
- Click the 'Change...' button to open the 'Computer Name/Domain Changes' window.
- Here, you can change the computer name or join a domain. Since 'win10' is already the computer name, you should focus on the 'Member of' section.

- In the 'Member of' section, you can see that the computer is already a member of the domain 'widgets.localdomain'. If it were not, you would select the 'Domain' radio button and enter the domain name.
- Once the correct domain is listed, click 'OK'. If you changed the domain, you would be prompted to enter the username and password for a user account with permission to join the domain.
- After entering valid credentials, a welcome message to the domain should appear.
- You will then be prompted to restart the computer to apply these changes. Make sure to save any open work before restarting.
- After the restart, the computer will be a part of the specified domain, and you can log in with domain user credentials.



Slide 22 Instructions:

- Open 'Server Manager' in your Windows Server environment.
- In 'Server Manager', navigate to the 'Local Server' tab from the left-hand panel.
- On the right side, find and click on 'Desktop Wallpaper' under the 'Policies' section.
- This will open the 'Desktop Wallpaper' policy setting. You can configure the desktop wallpaper that is displayed on all users' desktops within this setting.
- If you wish to enable a desktop wallpaper, select the 'Enabled' option.
- Specify the wallpaper path by typing the fully qualified path and name of the file that stores the wallpaper image in the 'Wallpaper Name' field. For example:
 - If using a local path: **C:\windows\web\wallpaper\windows\img0.jpg**
 - If using a network path (UNC): **\\Server\Share\Corp.jpg**
- Choose the 'Wallpaper Style' from the dropdown menu. Options typically include 'Fill', 'Fit', 'Stretch', 'Tile', and 'Center'.
- After making your selections, click 'OK' to apply the changes.
- The policy setting will take effect after the user logs off and logs back on, or after the system is restarted.
- If the policy should not be applied, you can select 'Not Configured' or 'Disabled' to leave the wallpaper settings as they are, allowing users to choose their own wallpaper.



Slide 23 Instructions:

- Open Windows PowerShell with administrative privileges on your Domain Controller.
- To update group policies, execute the command **gpupdate /force**. This command refreshes local and Active Directory-based Group Policy settings, including security settings.
- After the policies are updated, you might want to verify the application of certain policies. To do so, you can use the **gpresult** command or the Resultant Set of Policy (RSOP) snap-in.
- For detailed policy application results, use the **gpresult /R** command, which displays the Resultant Set of Policy information for the user and computer.

- In the PowerShell window, review the output under the 'Applied Group Policy Objects' section to confirm which policies have been applied. If there are any issues with policies not applying, they will be listed under 'The following GPOs were not applied because they were filtered out' along with the reason for the filtering.
- Check the 'Computer Settings' and 'User Settings' sections to see detailed information on what policies are active and their respective settings.
- If there are any Group Policy Objects (GPOs) that are expected to apply but aren't listed, troubleshoot accordingly. Common reasons for GPOs not applying include security filtering, WMI filtering, or incorrect organizational unit (OU) placement.
- The PowerShell window also shows which domain the computer is a part of under 'User Settings', the login server, and the Group Policy slow link threshold.
- If necessary, use additional Group Policy management and troubleshooting tools like the Group Policy Management Console (GPMC) or log files for more in-depth analysis.
- Remember to document any changes or findings during this process for future reference and possible audit requirements.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2013 Microsoft Corporation. All rights reserved.

Created on 11/28/2023 at 1:12:59 PM

RSOP data for WIDGETS\Administrator on DC : Logging Mode

-----
OS Configuration:      Primary Domain Controller
OS Version:            6.3.9600
Site Name:              Default-First-Site-Name
Roaming Profile:       N/A
Local Profile:          C:\Users\Administrator
Connected over a slow link?: Yes

COMPUTER SETTINGS
-----
CN=DC,OU=Domain Controllers,DC=wildcats,DC=localdomain
Last time Group Policy was applied: 11/28/2023 at 1:12:33 PM
Group Policy was applied from:      dc.wildcats.localdomain
Group Policy slow link threshold:   500 kbps
Domain Name:                        WIDGETS
Domain Type:                         Windows 2008 or later

Applied Group Policy Objects
-----
Default Domain Controllers Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

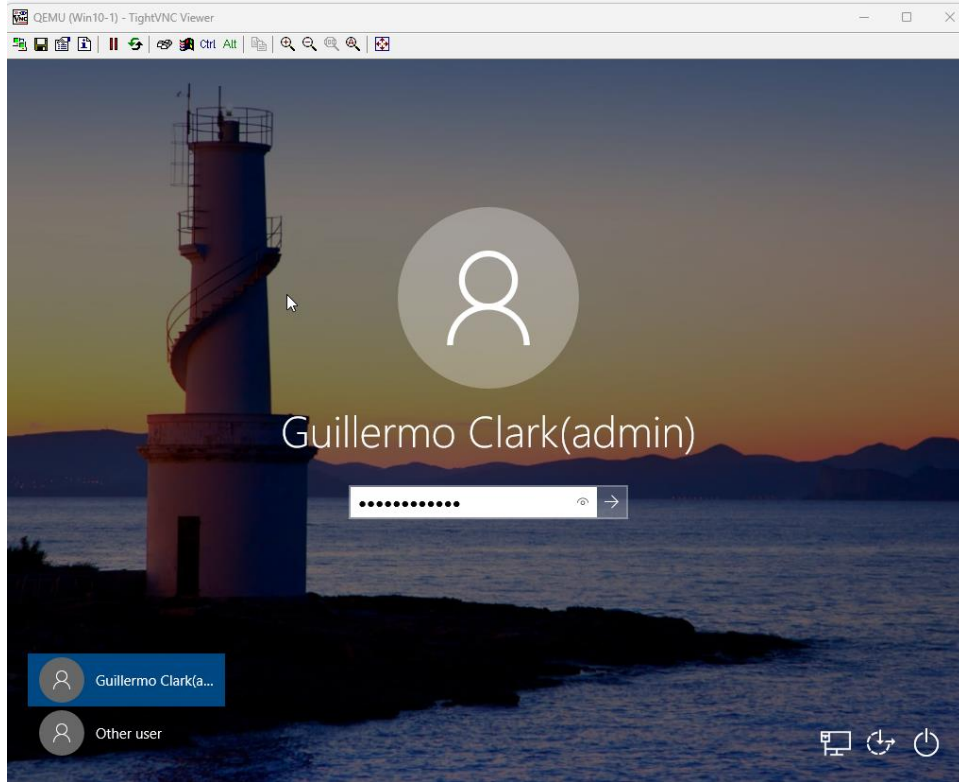
The computer is a part of the following security groups
-----
BUILTIN\Administrators
  
```

DC	10154	Warning	Microsoft-Windows-Windows Remote Management	System	11/28/2023 6:40:30 PM
DC	12	Warning	Microsoft-Windows-Time-Service	System	11/28/2023 6:40:26 PM
DC	12	Warning	Microsoft-Windows-Time-Service	System	11/28/2023 6:22:28 PM

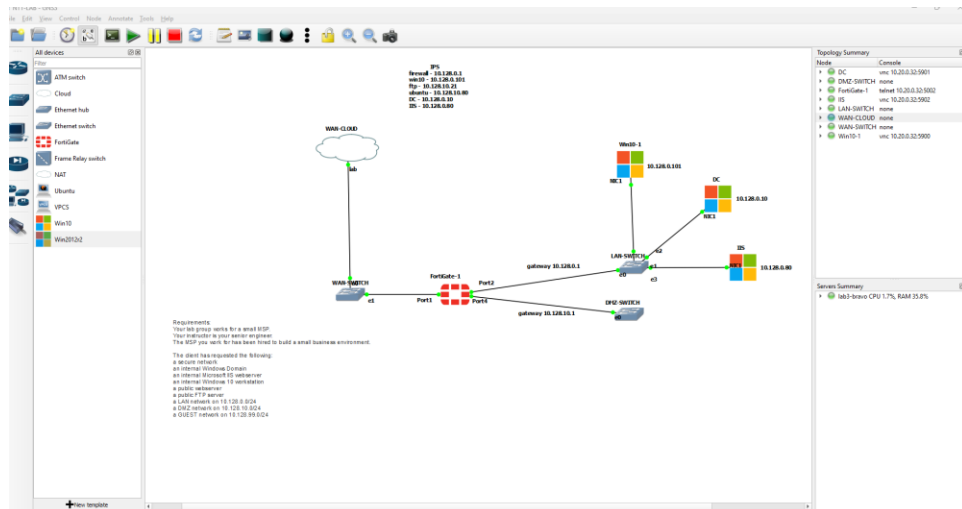
1:13 PM
11/28/2023

Slide 24 Instructions:

- Enter the password for the "(admin)" account.
- Click the arrow or press Enter to proceed.

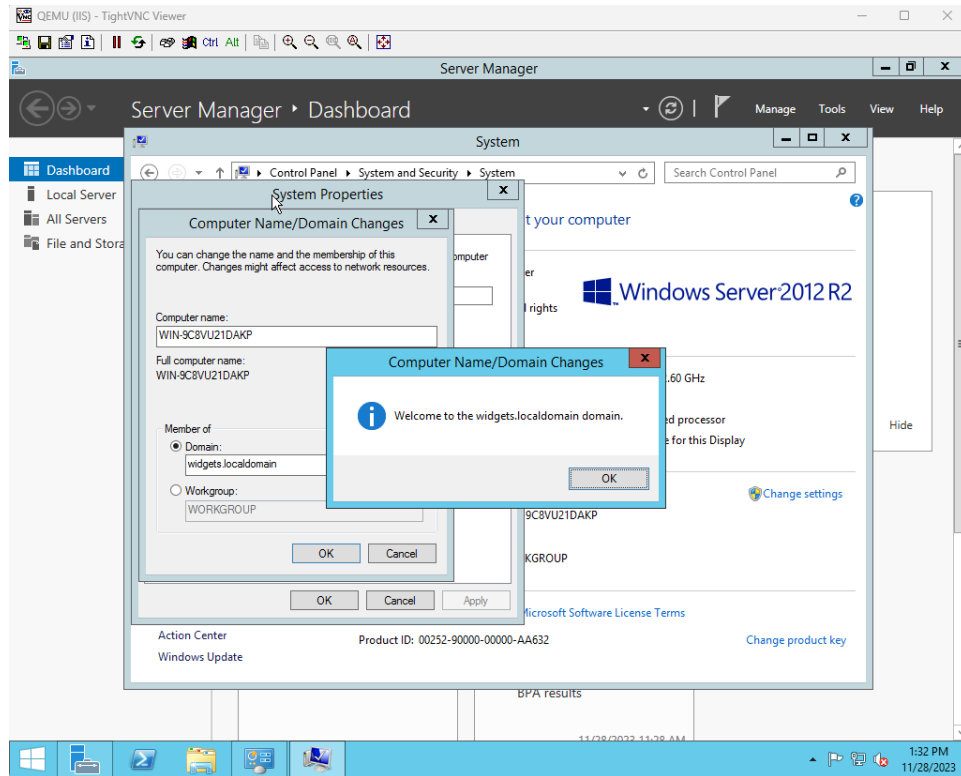
**Slide 25 Instructions -**

- Locate the device representing the Windows Server 2012 and install it, additionally name it "IIS" server.
- Within the server's properties, ensure that its name is set to "IIS."



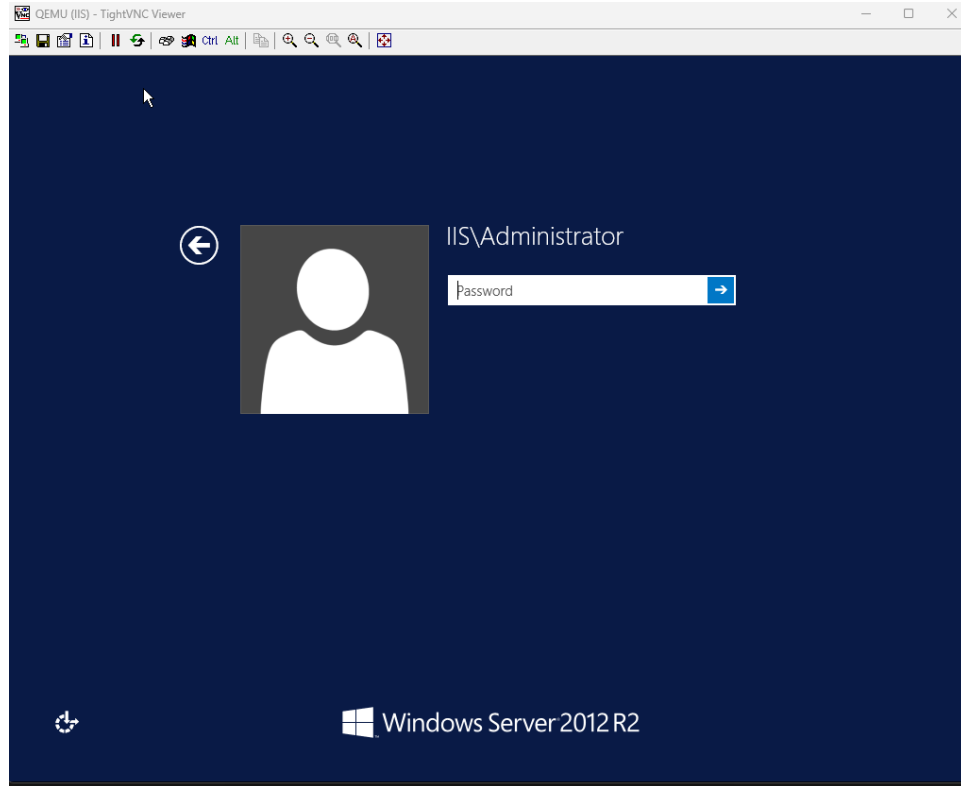
Slide 26 Instructions

- In your GNS3 environment, access the "IIS" server.
- Open the Server Manager on the "IIS" server. You can typically find it in the "Administrative Tools" or a similar menu.
- Inside Server Manager, navigate to "Local Server" on the left navigation pane.
- In the "Local Server" properties, locate the current computer name, and click on it to open the "System Properties" window.
- In the "System Properties" window, go to the "Computer Name" tab.
- Click the "Change" button to open the "Computer Name/Domain Changes" window.
- In this window, change the computer name to your desired name, such as "IIS."
- Below the computer name field, select the "Domain" radio button.
- Enter "widgets.localdomain" in the text field next to "Domain."
- Click the "OK" button to apply the changes.
- You will be prompted to provide credentials to join the "widgets.localdomain" domain. Enter the appropriate username and password with the necessary permissions to join the domain.
- After successfully joining the domain, you may need to restart the server for the changes to take effect.



Slide 27 Instructions

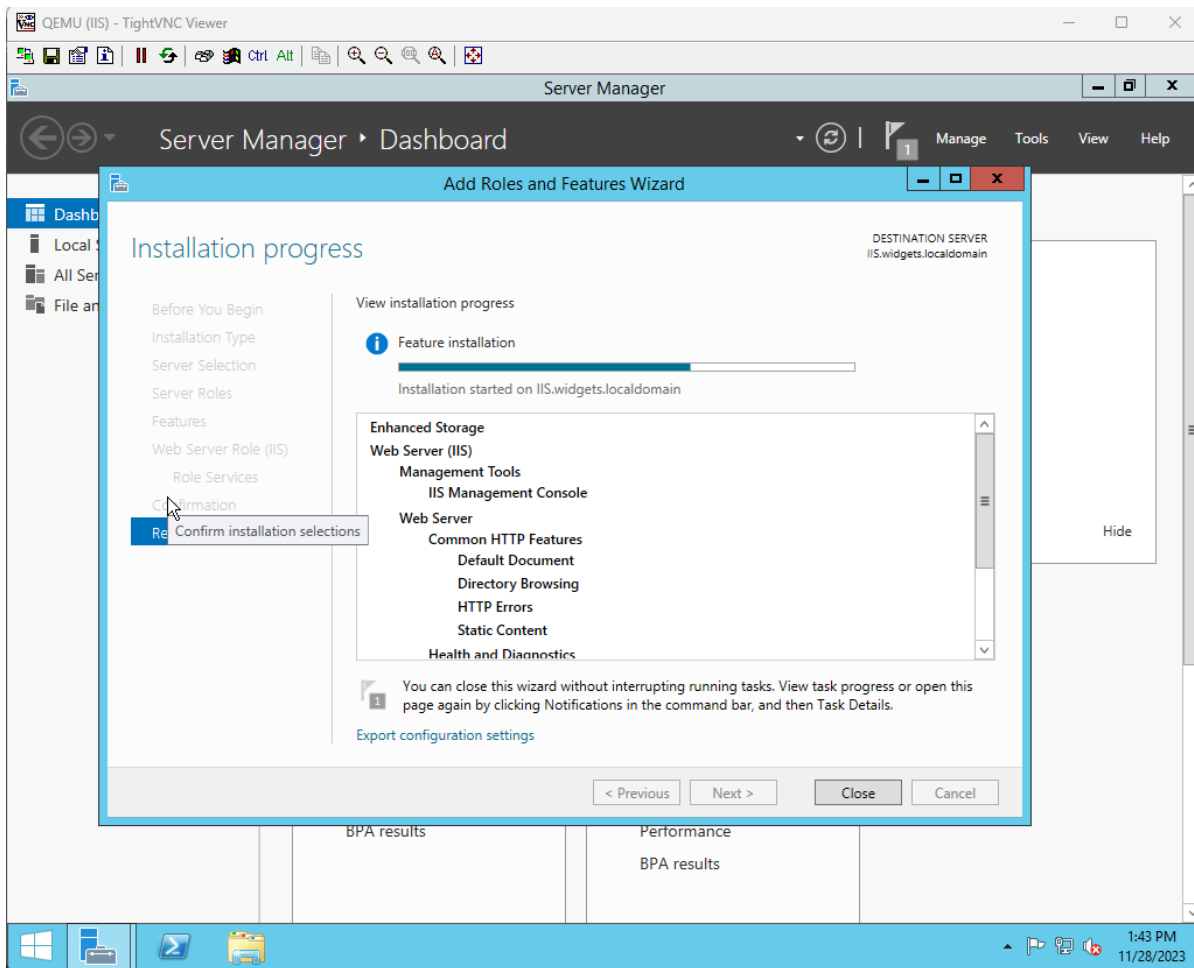
- Ensure that you have completed the previous steps to change the computer name and add the server to the "widgets.localdomain" domain, as instructed in slide 26.
- In your GNS3 environment, access the "IIS" server.
- To restart the server, you can typically do one of the following:
 - Click on the "Start" menu, then click on the power icon and select "Restart."
 - Open a command prompt or PowerShell and enter the command: **shutdown /r /t 0**
- Wait for the server to complete the restart process. It may take a few moments.
- After the server has restarted, you can log in as the "IIS/Administrator" account.
- On the login screen, enter the username as "IIS/Administrator" and provide the corresponding password.
- Press Enter or click "Sign In" to log in.
- You should now be logged in as the "IIS/Administrator" user on the server.



Slide 28 Instructions:

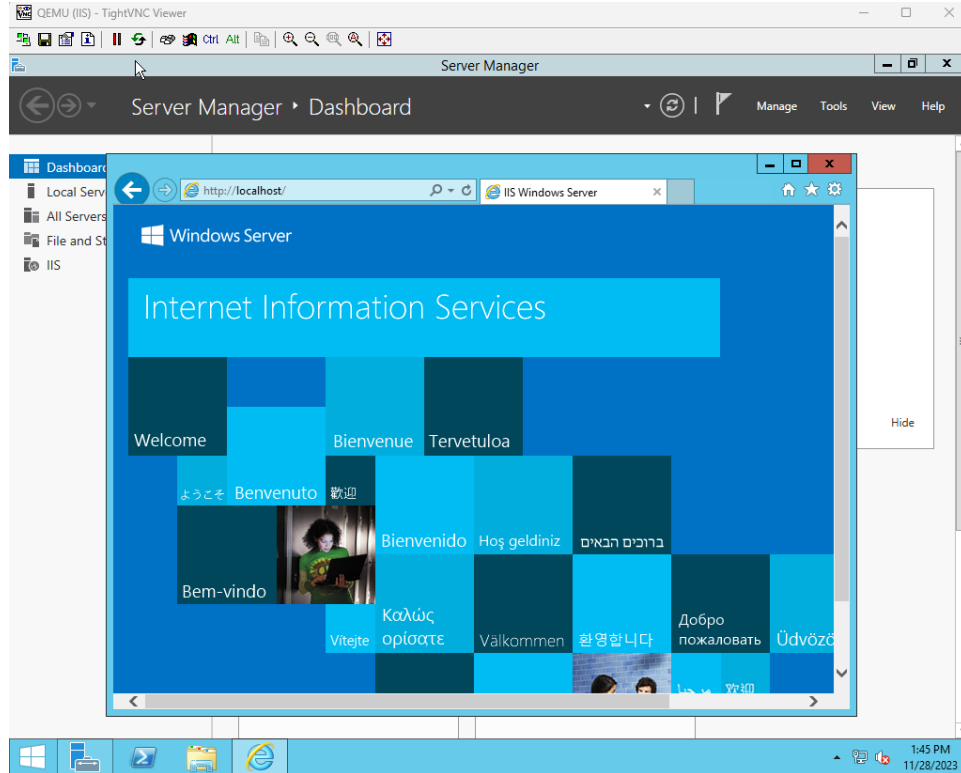
- In your GNS3 environment, ensure that you are logged in as "IIS/Administrator" on the server, as instructed in slide 27.
- Open the Server Manager on the "IIS" server. You can typically find it in the "Administrative Tools" or a similar menu.
- Inside Server Manager, locate and click on the "Add roles and features" option. This will open the "Add Roles and Features Wizard."
- In the "Add Roles and Features Wizard," click "Next" to proceed.
- In the "Select installation type" section, leave the default selection (Role-based or feature-based installation) and click "Next."
- In the "Select destination server" section, ensure that the correct server (the "IIS" server) is selected. It should be pre-selected for you. Click "Next."
- In the "Select server roles" section, scroll down or search for "Web Server (IIS)" and check the corresponding box to select it.

- A pop-up window may appear, indicating that additional features are required. Click "Add Features" to include the required features for the web server.
- Click "Next" to proceed.
- In the "Select features" section, you can leave the default selections as they are since the necessary features for the web server have been added automatically. Click "Next."
- Review the information on the "Web Server Role (IIS)" screen. You can click "Next" to proceed.
- In the "Select role services" section, you can customize the specific components and services you want to install with IIS. Make your selections based on your requirements.
- Click "Next" to continue.
- Review the summary of your selections. If everything looks correct, click "Install" to begin the installation process.
- The wizard will install the selected roles and features. Wait for the process to complete.
- Once the installation is finished, you will receive a confirmation message. Click "Close" to exit the wizard.



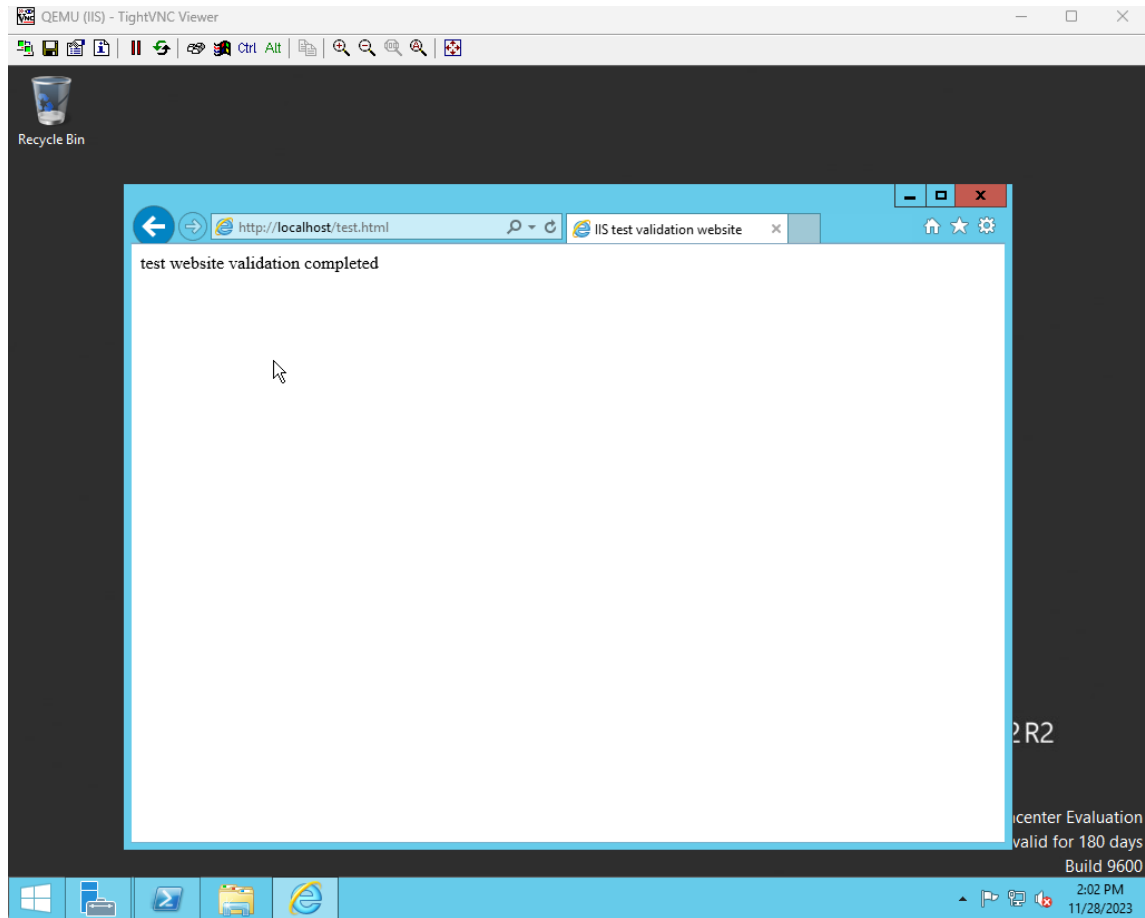
Slide 29 Instructions:

- Open a web browser on the "IIS" server. You can typically find a web browser icon in the "Start" menu.
- In the web browser's address bar, type "localhost" (without quotes) and press Enter.
- The browser should load a web page hosted on the "IIS" server, indicating that the localhost is working.
- You may see a default web page or a specific web application depending on the configuration of your "IIS" server.
- This step confirms that the web server is functioning correctly, and you can access web content hosted on the server using the "localhost" address.



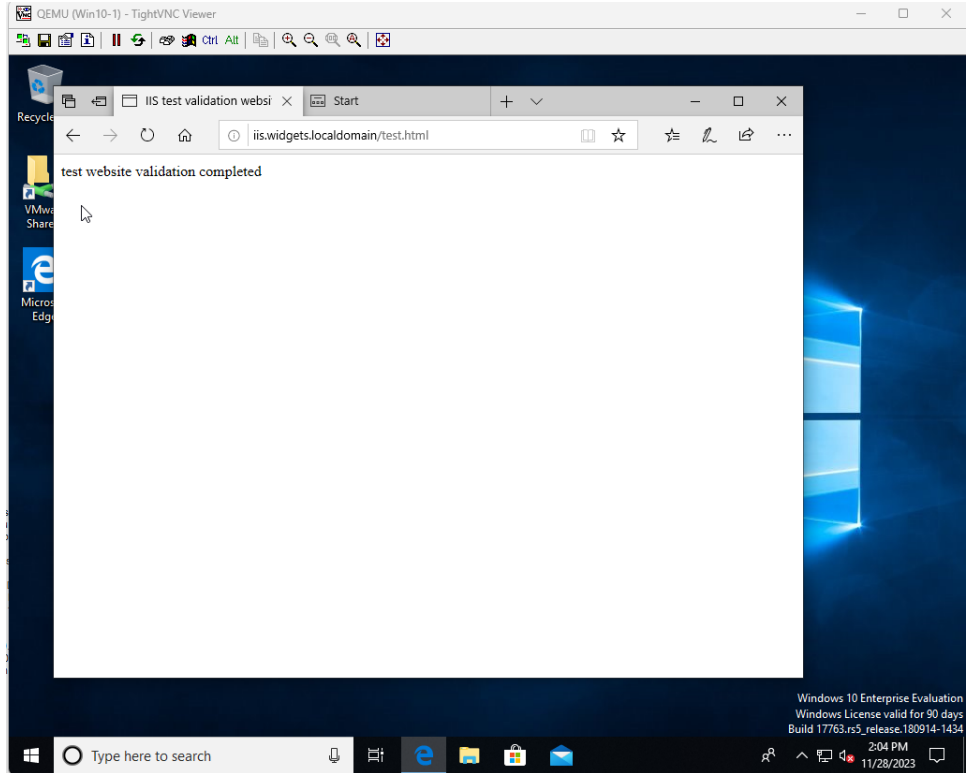
Slide 30 Instructions:

- Open a web browser on the "IIS" server. You can typically find a web browser icon in the "Start" menu.
- In the web browser's address bar, type the following URL:
 "<http://localhost/test.html>" (without quotes) and press Enter.
- The browser should load the "test.html" web page hosted on the "IIS" server.
- Confirm that the content of the "test.html" page displays the message "Test website validation completed."



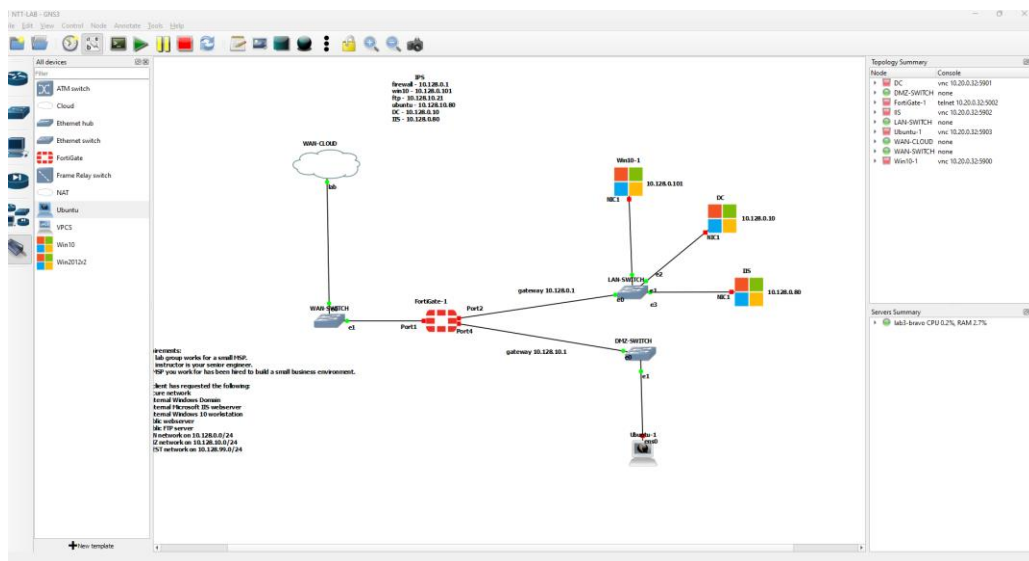
Slide 31 Instructions:

- From your Windows 10 machine (client machine), open a web browser.
- In the web browser's address bar, type the following URL:
"[http://\[IP_address_of_IIS_server\]/test.html](http://[IP_address_of_IIS_server]/test.html)" (replace "[IP_address_of_IIS_server]" with the actual IP address of the IIS server) and press Enter.
- The browser should load the "test.html" web page hosted on the IIS server.
- Confirm that the content of the "test.html" page displays the message "Test website validation completed."



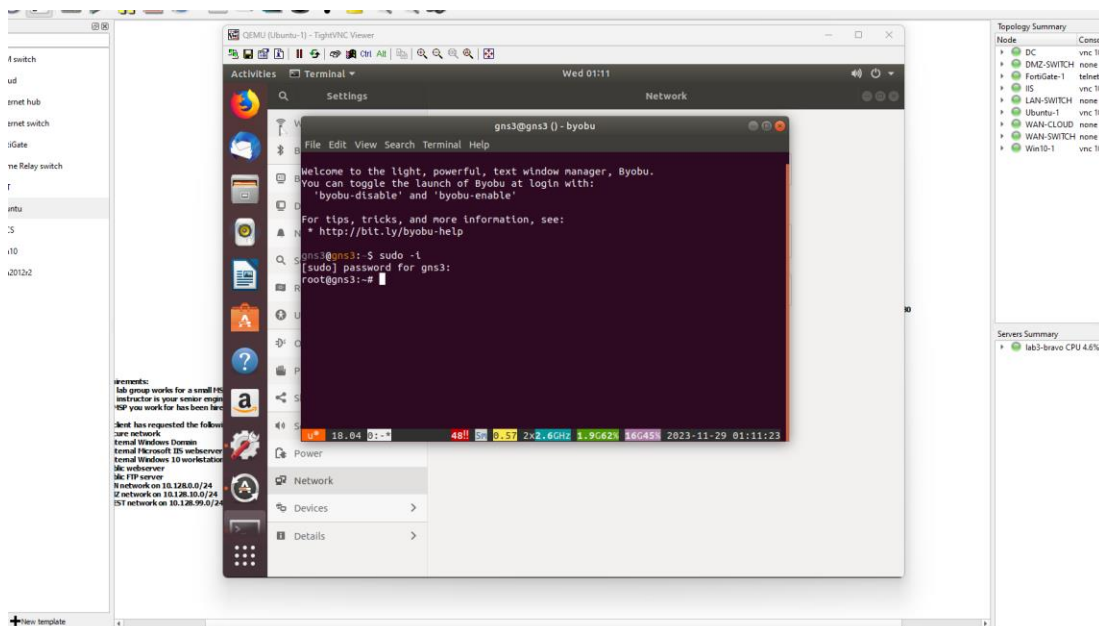
Slide 32 Instructions:

- In your GNS3 environment, locate the Ubuntu Server virtual machine.
- Drag and add the Ubuntu Server to the DMZ switch.



Slide 33 Instructions:

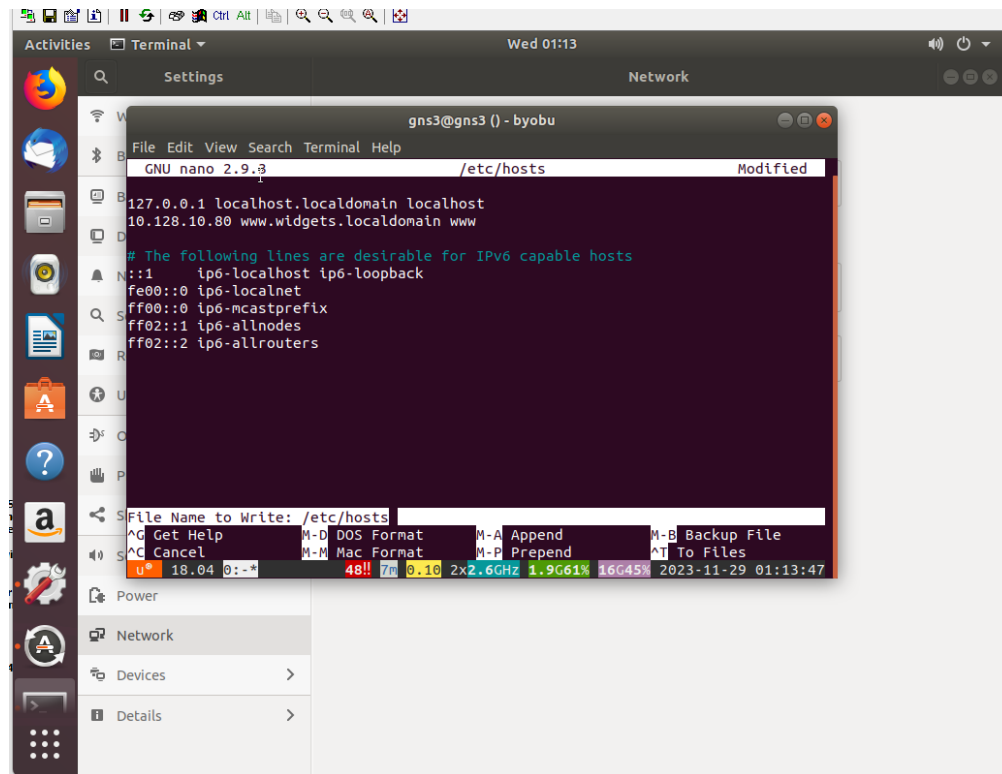
- In your Ubuntu Server virtual machine, open a terminal window.
To log in as the root user with GNS3 credentials.
- You will be prompted to enter your current user's password. Provide the password GNS3 and press Enter.
- After successful authentication, you will have root access in the terminal, indicated by the change in the command prompt.



Slide 34 Instructions:

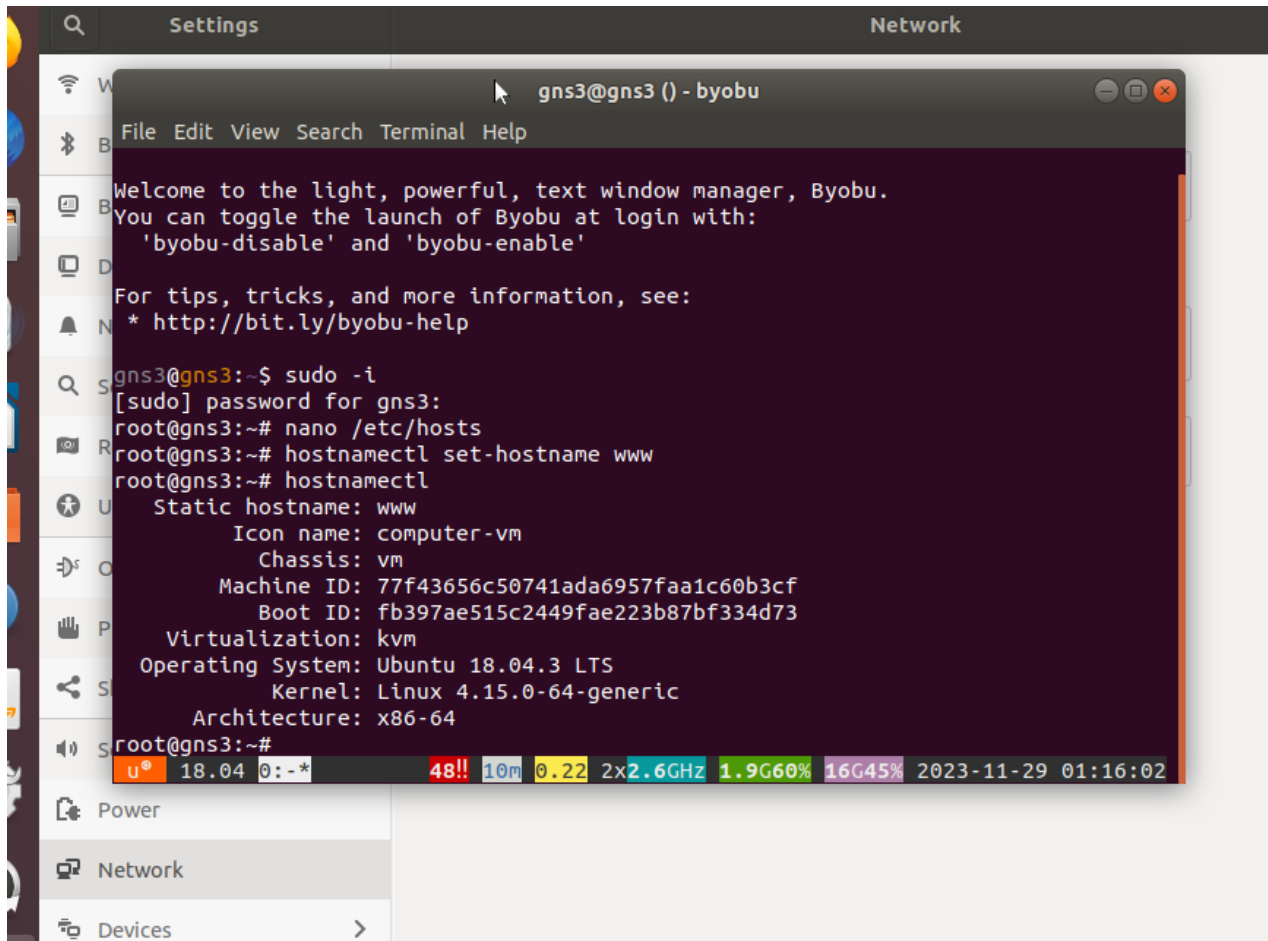
- In your Ubuntu Server terminal, navigate to the "/etc" directory using the "cd /etc" command.
- Open the "hosts" file using a text editor. You can use the "nano" text editor with the "sudo nano hosts" command.
- In the "hosts" file, add the following lines:
 - 127.0.0.1 localhost.localdomain localhost
 - 10.128.10.80 www.widgets.localdomain www

- Save the changes by pressing Ctrl + O, then press Enter.
- Exit the text editor by pressing Ctrl + X.



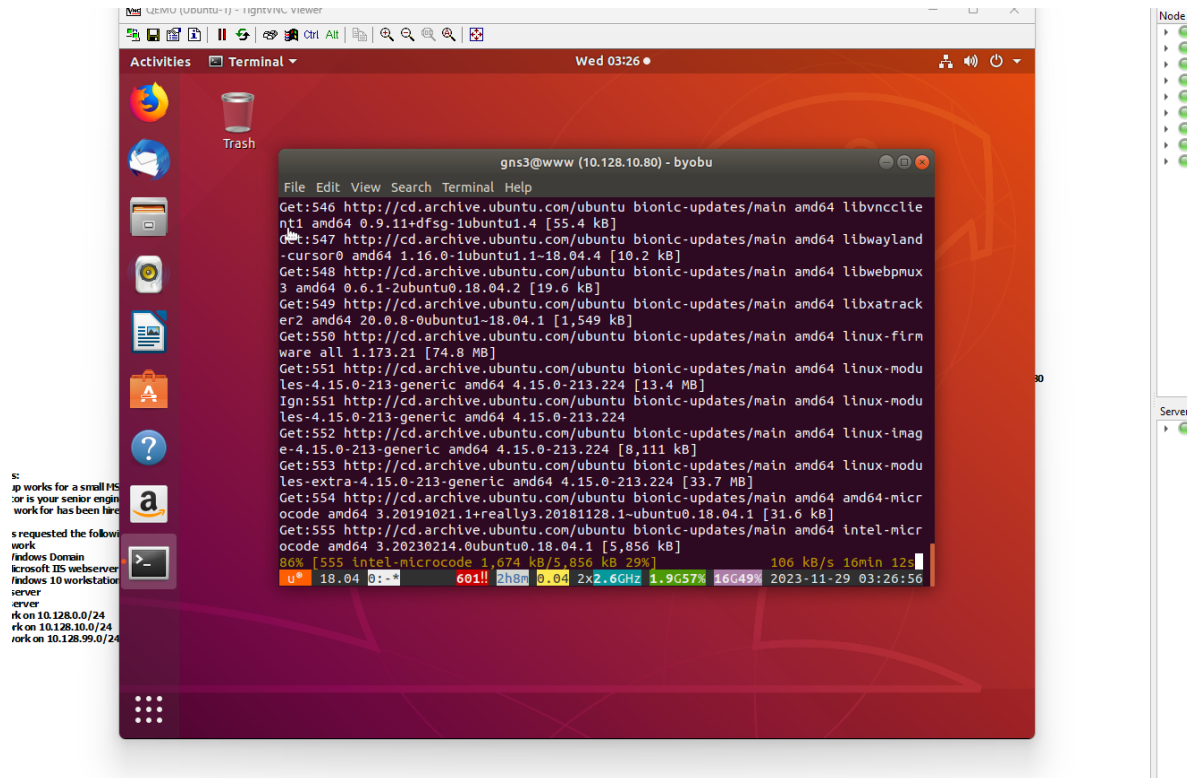
Slide 35 Instructions:

- In your Ubuntu Server terminal, use the following command to set the hostname to "www":
sudo hostnamectl set-hostname www
- To verify the hostname change, enter the following command:
hostnamectl
- This command will display information about the system's hostname, including the updated hostname "www."



Slide 36 Instructions:

- After making configuration changes or updates to your system, it's recommended to perform the following steps in your Ubuntu Server terminal:
- Update the package list to ensure your system is aware of the latest available packages by running the following command:
sudo apt-get update
- Next, upgrade the installed packages, which includes applying security updates and bug fixes, by running the following command:
sudo apt-get dist-upgrade
- Running these steps will guarantee that the changes you've made are successfully applied to your system.



Slide 37 Instructions:

In your Ubuntu Server terminal, enable and start the Apache web server using the following commands:

- Enable the Apache web server to start on boot: **sudo systemctl enable apache2**
- Start the Apache web server immediately: **sudo systemctl start apache2**

This ensures that Apache is both enabled to start on boot and is immediately started.

Allow incoming traffic to the Apache web server by configuring the Uncomplicated Firewall (UFW) to allow Apache traffic:

- Allow Apache traffic through the firewall: **sudo ufw allow apache**

This step opens the necessary ports for Apache to receive web traffic.

Download DokuWiki by retrieving the DokuWiki stable release from the official source using the following command:

- Fetch the DokuWiki archive to your server for installation: **wget <https://download.dokuwiki.org/src/dokuwiki/dokuwiki-stable.tgz>**


```

QEMU (Ubuntu-1) - TightVNC Viewer
Wed 04:22
Activities Terminal
gns3@www (10.128.10.80) - byobu
File Edit View Search Terminal Help
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.2) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1.6) ...
root@www:~# systemctl enable --now apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@www:~# ufw allow Apache
Rules updated
Rules updated (v6)
root@www:~# wget https://download.dokuwiki.org/src/dokuwiki/dokuwiki-stable.tgz
--2023-11-29 04:21:45-- https://download.dokuwiki.org/src/dokuwiki/dokuwiki-stable.tgz
Resolving download.dokuwiki.org (download.dokuwiki.org)... 138.201.137.132, 2a01:4f8:172:3483::2
Connecting to download.dokuwiki.org (download.dokuwiki.org)|138.201.137.132|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4043928 (3.9M) [application/octet-stream]
Saving to: 'dokuwiki-stable.tgz'

dokuwiki-stable.tgz  7%[>] 304.59K  13.9KB/s  eta 4m 36s
0% 18.04 0s- 0h3m 0.31 2x2.6GHz 1.9G55% 16G53% 2023-11-29 04:22:09

```

Slide 38 Instructions:

- Open a terminal window on your Ubuntu server where you will configure the Apache virtual host for DokuWiki.
- Elevate your privileges to root using the command **sudo su -** to ensure you have the necessary permissions to edit configuration files.
- Access the Apache virtual host configuration file for DokuWiki by entering the nano text editor command: **sudo nano /etc/apache2/sites-available/dokuwiki.conf**.
- Locate the **<VirtualHost *:80>** block to configure your DokuWiki site. This tells Apache to listen on port 80 for incoming connections for the specified ServerName.
- Set the **ServerName** directive to the desired domain name for your DokuWiki installation, such as www.widgets.localdomain.
- Specify the **DocumentRoot** directive to the directory where DokuWiki is installed, **/var/www/html/dokuwiki**.

- Within the **<Directory>** block for the DokuWiki installation path, set the **AllowOverride** directive to **All** to enable the use of .htaccess files for directory-level configuration.
- Add the **Require all denied** directive to restrict access to the directory by default for security purposes.
- If you are using the **mod_authz_core** module, include the following directives to configure access control:
 - **Order allow,deny** establishes the order in which allow and deny directives are evaluated.
 - **Deny from all** as a security measure, denies access to the directory from all users.
- Check that the **ErrorLog** and **CustomLog** directives are set correctly to specify where Apache will log errors and access requests.
- After ensuring all configurations are correct, press **Ctrl + O** to write the changes to the file, then press **Enter** and **Ctrl + X** to exit nano.
- Apply the changes by restarting the Apache service using the command: **sudo systemctl restart apache2**.
- Verify that the DokuWiki site is operational by accessing <http://www.widgets.localdomain> in a web browser.

```

root@www: ~
GNU nano 2.9.3 /etc/apache2/sites-available/docuwiki.conf Modified

<VirtualHost *:80>
  ServerName www.widgets.localdomain
  DocumentRoot /var/www/html/dokuwiki

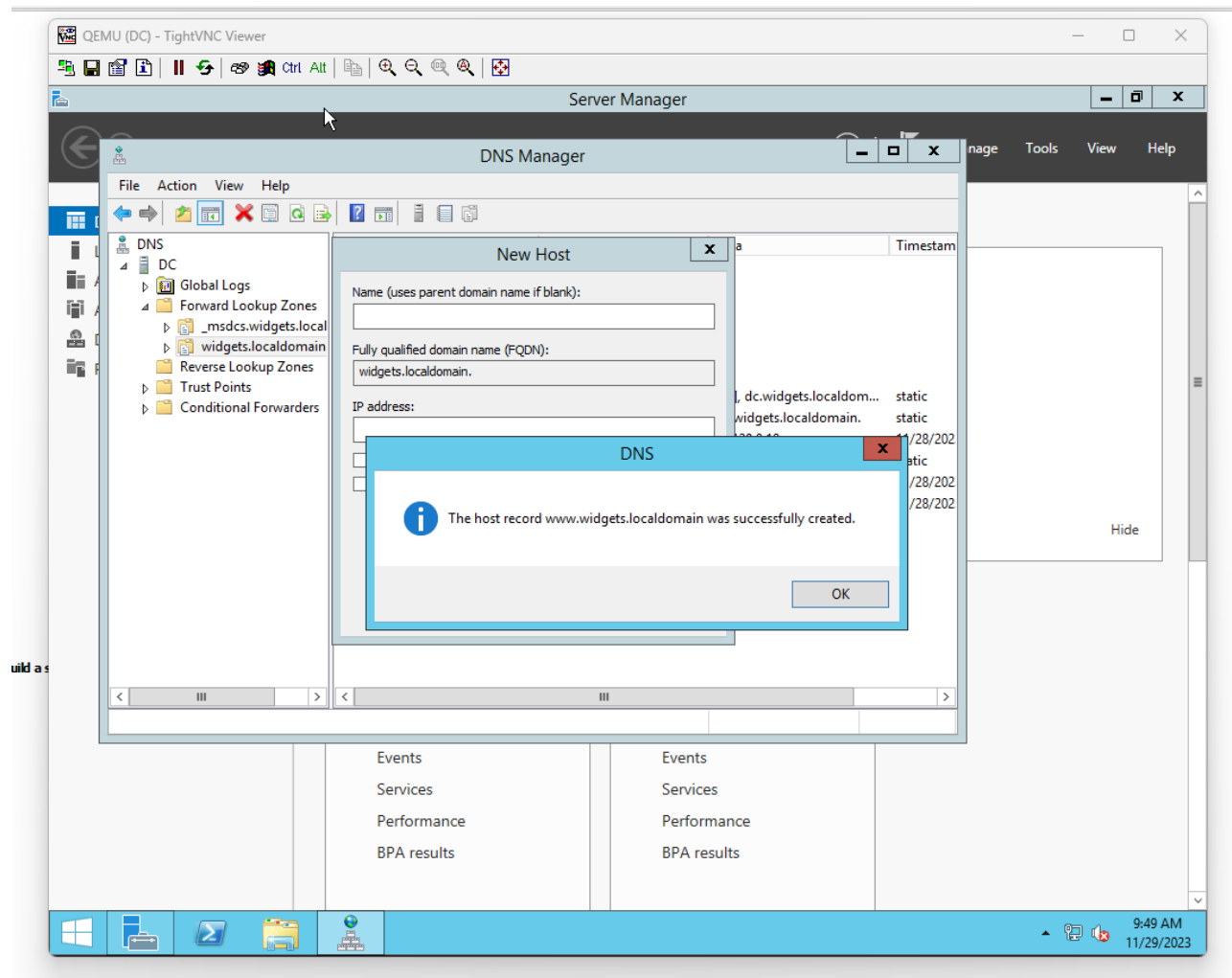
  <Directory ~ "/var/www/html/dokuwiki/(bin|conf|data|inc/)">
    <IfModule mod_authz_core.c>
      AllowOverride All
      Require all denied
    </IfModule>
    <IfModule !mod_authz_core.c>
      Order allow,deny
      Deny from all
    </IfModule>
  </Directory>

  ErrorLog /var/log/apache2/dokuwiki_error.log
  CustomLog /var/log/apache2/dokuwiki_access.log combined
</VirtualHost>

```

Slide 39 Instructions:

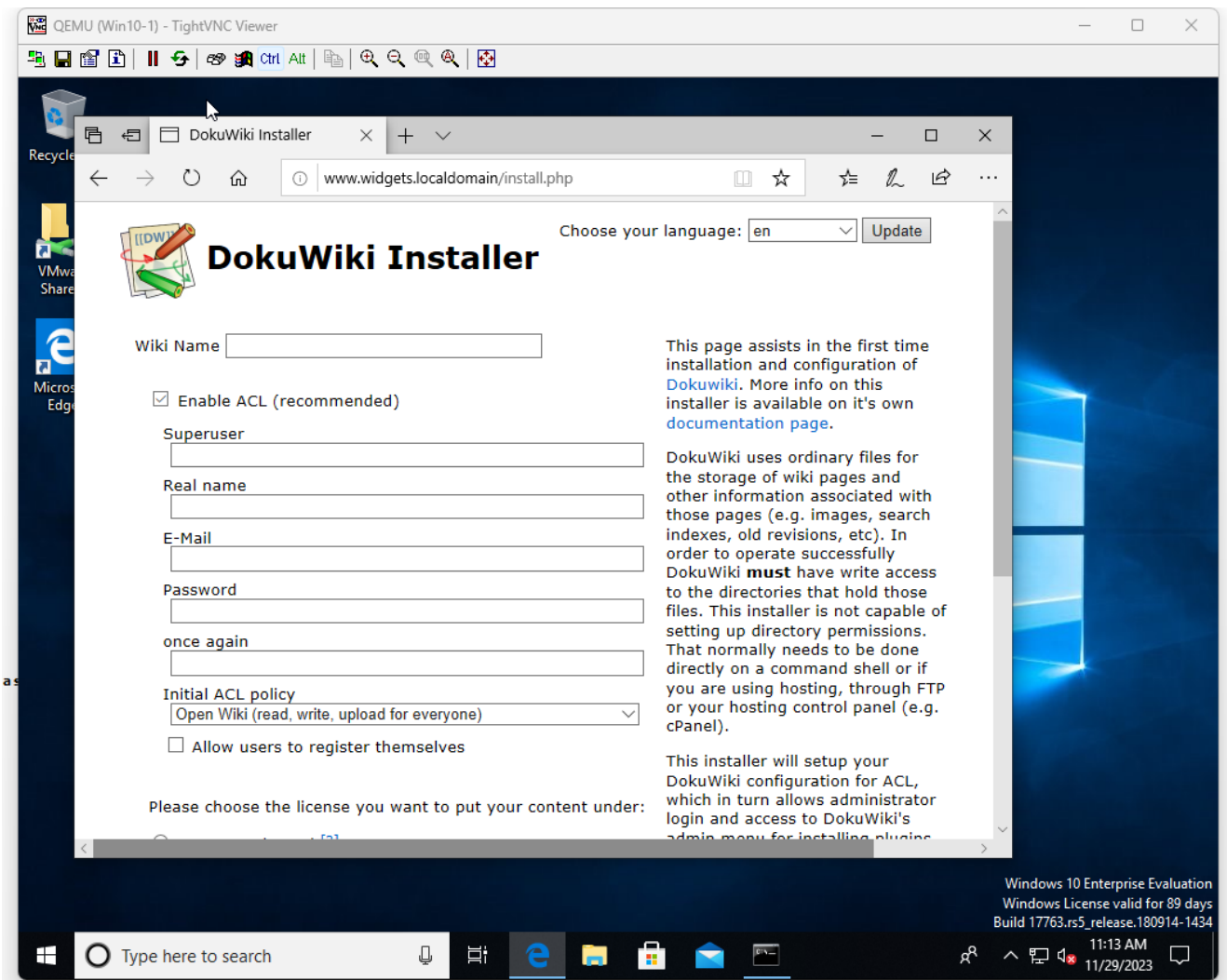
- On the DC server, open the DNS Manager.
- Navigate to the Forward Lookup Zones.
- Right-click on **widgets.localdomain** and choose "New Host (A or AAAA)".
- Enter the desired host record details and corresponding IP address.
- Click "Add Host" to create the new record.
- Confirm the successful creation of the host record when prompted.



Slide 40 Instructions:

- On your Windows 10 server, open a web browser and navigate to the DokuWiki installer by entering <http://www.widgets.localdomain/install.php>.
- On the DokuWiki Installer page, fill in the "Wiki Name" field with your desired wiki name.
- Check the box to "Enable ACL (Access Control List)" for user permissions management.
- Fill in the "Superuser" section with your chosen admin username.
- Enter your "Real name", "E-Mail", and a secure "Password". Confirm the password by entering it again in the "once again" field.

- Select an "Initial ACL policy" from the dropdown menu. The default setting is usually appropriate for most installations.
- If desired, check the option "Allow users to register themselves" to enable user self-registration.
- Choose the content license for your wiki content from the available options.
- Complete the installation by clicking the button to install DokuWiki.



Slide 41 Instructions:

- Access the Widgets Network Documentation Wiki by going to <http://www.widgets.localdomain/doku.php?id=start> in your web browser on the Win10 server.
- Review the network documentation provided on the main page, which includes details of the firewall and Windows 10 host configurations.
- Verify the hostnames and fully qualified domain names (FQDNs) for the firewall and Win10 server are correctly documented.
- Confirm the IP configurations and associated network details, such as DHCP settings, LAN connections, and DNS services, are accurately recorded.
- Update or add any additional information as necessary to ensure the documentation is current and comprehensive for the Widgets environment.

The screenshot shows a web browser window titled 'QEMU (Win10-1) - TightVNC Viewer'. The browser address bar shows the URL www.widgets.localdomain/doku.php?id=start. The page content includes a search bar, navigation links (Recent Changes, Media Manager, Sitemap), and a main heading 'Welcome to the widets.localdomain Wiki!'. Below the heading, there is a sub-heading 'firewall' followed by a code block containing network configuration details. The code block for 'firewall' is as follows:

```
hostname = firewall
FQDN = firewall.widgets.localdomain (needs to be created on dc)
network info:
wan is port1 on dhcp from cloud, connected to WAN-SWITCH
lan is port2 on 10.128.0.1/24, connected to LAN-SWITCH
dmz is port4 on 10.128.10.1/24, connected to DMZ-SWITCH
guest is port3 on 10.128.99.1/24, not connected
```

Below the 'firewall' section, there is a sub-heading 'win10' followed by a code block containing network configuration details. The code block for 'win10' is as follows:

```
hostname = win10
FQDN = win10.widgets.localdomain
a-record created = dynamically on dc.widgets.localdomain
network info: dcp, LAN network
```

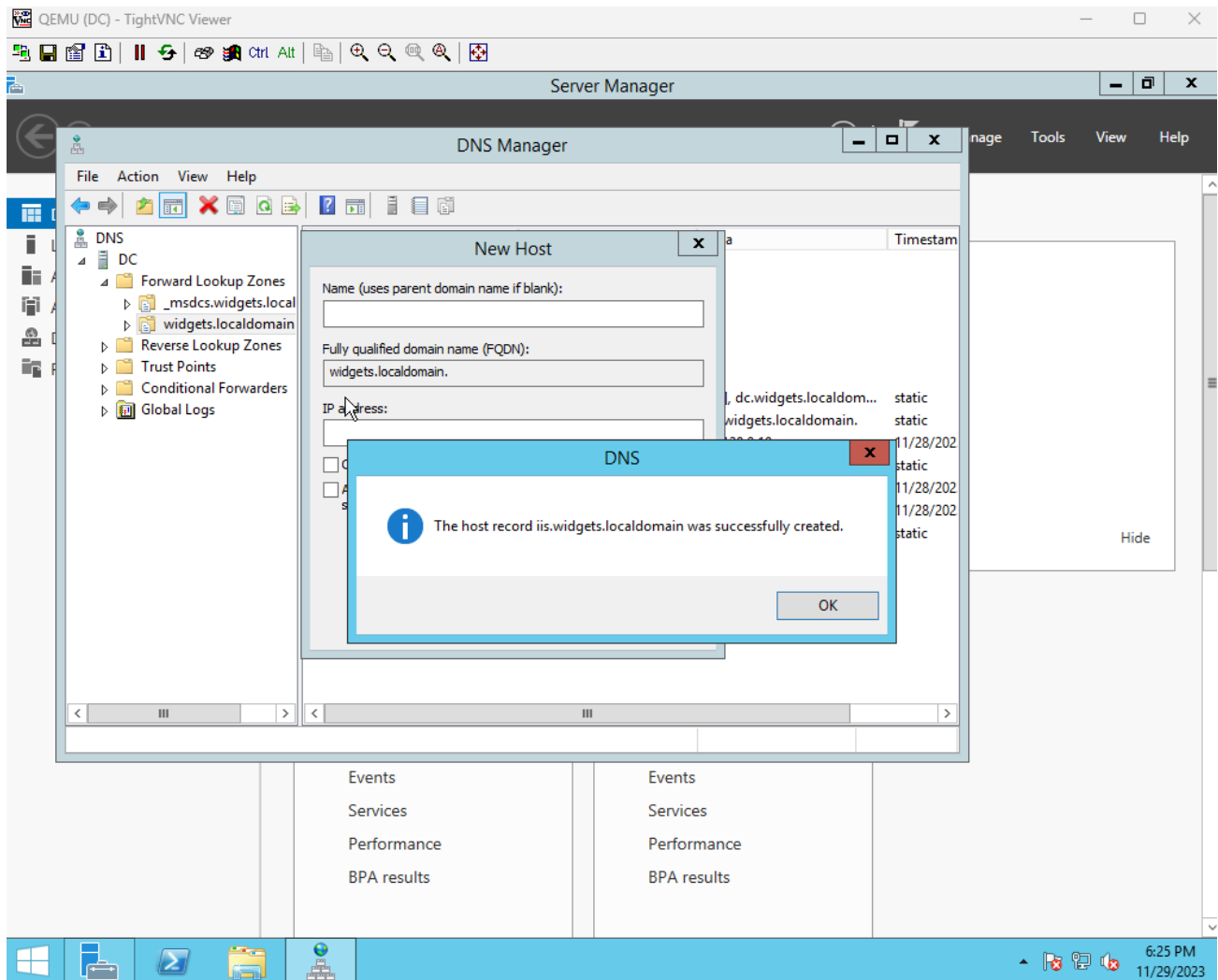
Below the 'win10' section, there is a sub-heading 'dc' followed by a code block containing network configuration details. The code block for 'dc' is as follows:

```
hostname = dc
FQDN = dc.widgets.localdomain
a-record created = automatically on dc.widgets.localdomain
network info: static, 10.128.0.10/24, LAN network
services: AD and DNS services
```

The browser window also shows a taskbar at the bottom with the Windows logo, a search bar, and several application icons. The system tray shows the time as 6:20 PM on 11/29/2023.

Slide 42 Instructions:

- On the DC server, open the DNS Manager through the Server Manager.
- Expand the 'Forward Lookup Zones' folder in the DNS Manager.
- Right-click on the **widgets.localdomain** zone and select "New Host (A or AAAA)..."
- In the 'New Host' dialog, enter "iis" in the 'Name' field to create a record for "iis.widgets.localdomain".
- Input the IP address for the IIS server in the 'IP address' field.
- Click "Add Host" to create the new DNS entry.
- Click "OK" in the confirmation window that states the host record for "iis.widgets.localdomain" was successfully created.



Slide 43 Instructions:

- On your Win10 server, open the FortiGate firewall interface in a web browser.
- Log in as an administrator.
- Navigate to 'Policy & Objects' and then to 'IPv4 Policy'.
- Review the list to confirm existing policies, especially the rule allowing TCP port 80, which is typically used for HTTP traffic.
- To add a new policy, click 'Create New'.
- Configure the policy with the necessary interface pairs, source, destination, and ensure you set the 'Service' to include 'HTTP' which uses TCP port 80.
- Set the 'Action' to 'ACCEPT' to allow the traffic.
- Save the new policy by clicking 'OK' or 'Apply'.

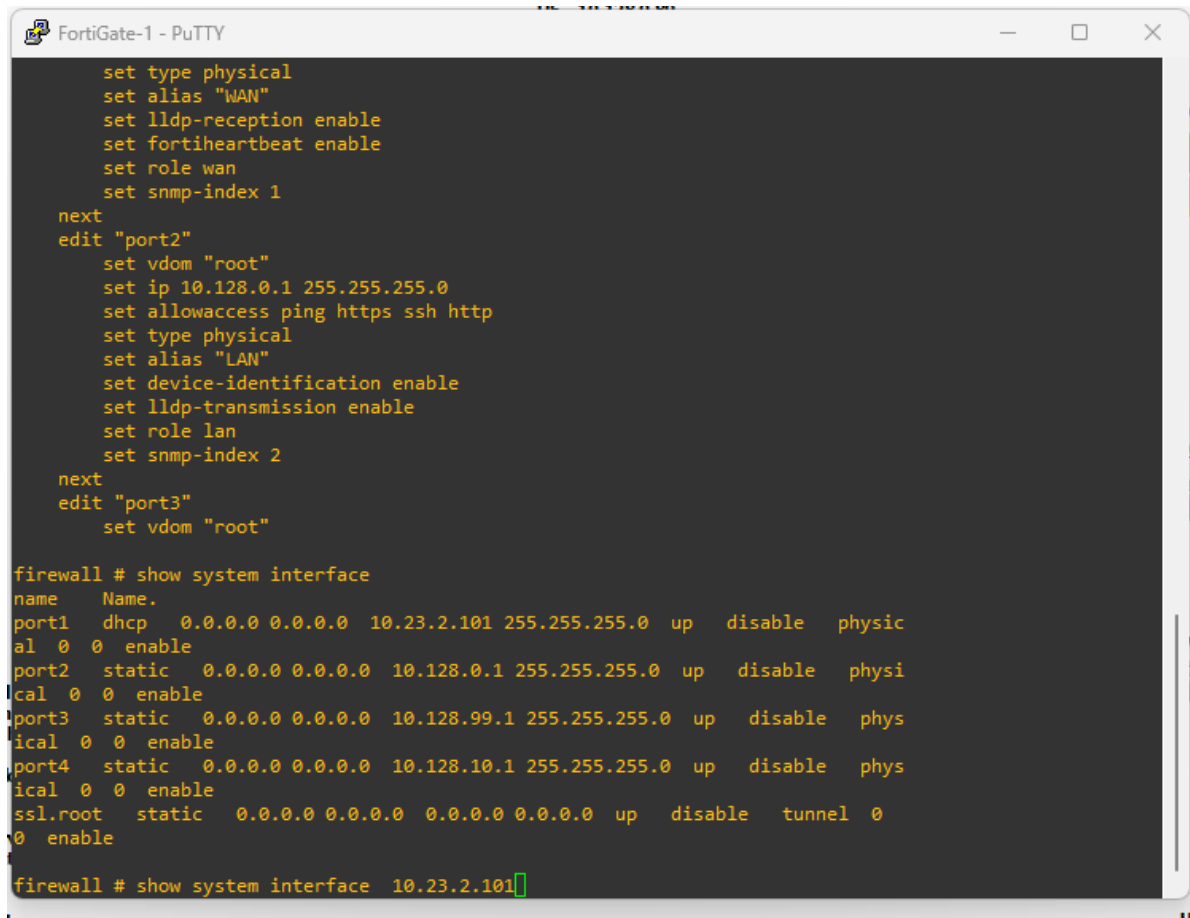
The screenshot shows the FortiGate VM64-KVM firewall interface. The left sidebar contains a navigation menu with the following items: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects (selected), Authentication Rules, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, and Security Profiles. The main content area is titled 'firewall' and shows the 'IPv4 Policy' configuration page. The page has a green header with 'FortiGate VM64-KVM firewall' and a search bar. Below the header, there are buttons for '+ Create New', 'Edit', 'Delete', and 'Policy Lookup'. The main content area is titled 'Interface Pair View' and shows a table of existing policies. The table has columns for ID, Name, Source, Destination, Schedule, Service, Action, and N. The table contains the following rows:

ID	Name	Source	Destination	Schedule	Service	Action	N
	DMZ (port4) → LAN (port2)						1
	DMZ (port4) → WAN (port1)						1
	LAN (port2) → DMZ (port4)						1
	LAN (port2) → WAN (port1)						1
	WAN (port1) → DMZ (port4)						1
5	WAN-to-DMZ	all	www_tcp_80	always	DMZ-services-group	ACCEPT	1
	Implicit						1

At the bottom of the page, there is a status bar showing '6 | Updated: 12:35:32' and a refresh button. The Windows taskbar is visible at the bottom of the screen, showing the search bar and several application icons.

Slide 44 Instructions:

- In the SSH terminal session to your FortiGate firewall, identify the configuration details for "port1".
- Note the "port1" configuration is labeled with the alias "WAN", indicating this port is connected to the wide area network (WAN).
- Recognize that "port1" is set to obtain an IP address via DHCP, which in this context is likely provided by the WAN-side, such as a cloud service or ISP.
- The configuration implies that "port1" is connected through a WAN switch to the cloud, making it accessible from the internet.
- The displayed command **show system interface** with the IP address 10.23.2.101 would show detailed information for that interface if executed, confirming its accessibility and status.



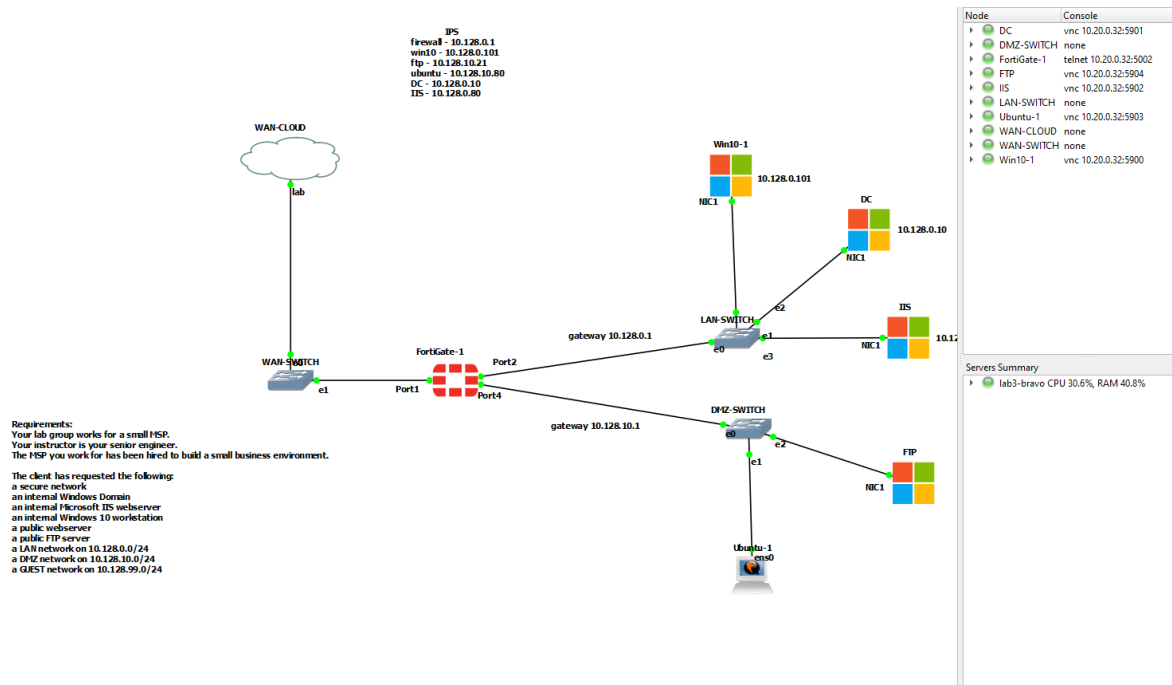
```
FortiGate-1 - PuTTY
set type physical
set alias "WAN"
set lldp-reception enable
set fortiheartbeat enable
set role wan
set snmp-index 1
next
edit "port2"
set vdom "root"
set ip 10.128.0.1 255.255.255.0
set allowaccess ping https ssh http
set type physical
set alias "LAN"
set device-identification enable
set lldp-transmission enable
set role lan
set snmp-index 2
next
edit "port3"
set vdom "root"

firewall # show system interface
name      Name.
port1     dhcp  0.0.0.0 0.0.0.0 10.23.2.101 255.255.255.0 up  disable  physic
al 0 0 enable
port2     static 0.0.0.0 0.0.0.0 10.128.0.1 255.255.255.0 up  disable  phys
ical 0 0 enable
port3     static 0.0.0.0 0.0.0.0 10.128.99.1 255.255.255.0 up  disable  phys
ical 0 0 enable
port4     static 0.0.0.0 0.0.0.0 10.128.10.1 255.255.255.0 up  disable  phys
ical 0 0 enable
ssl.root  static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable  tunnel 0
0 enable

firewall # show system interface 10.23.2.101
```

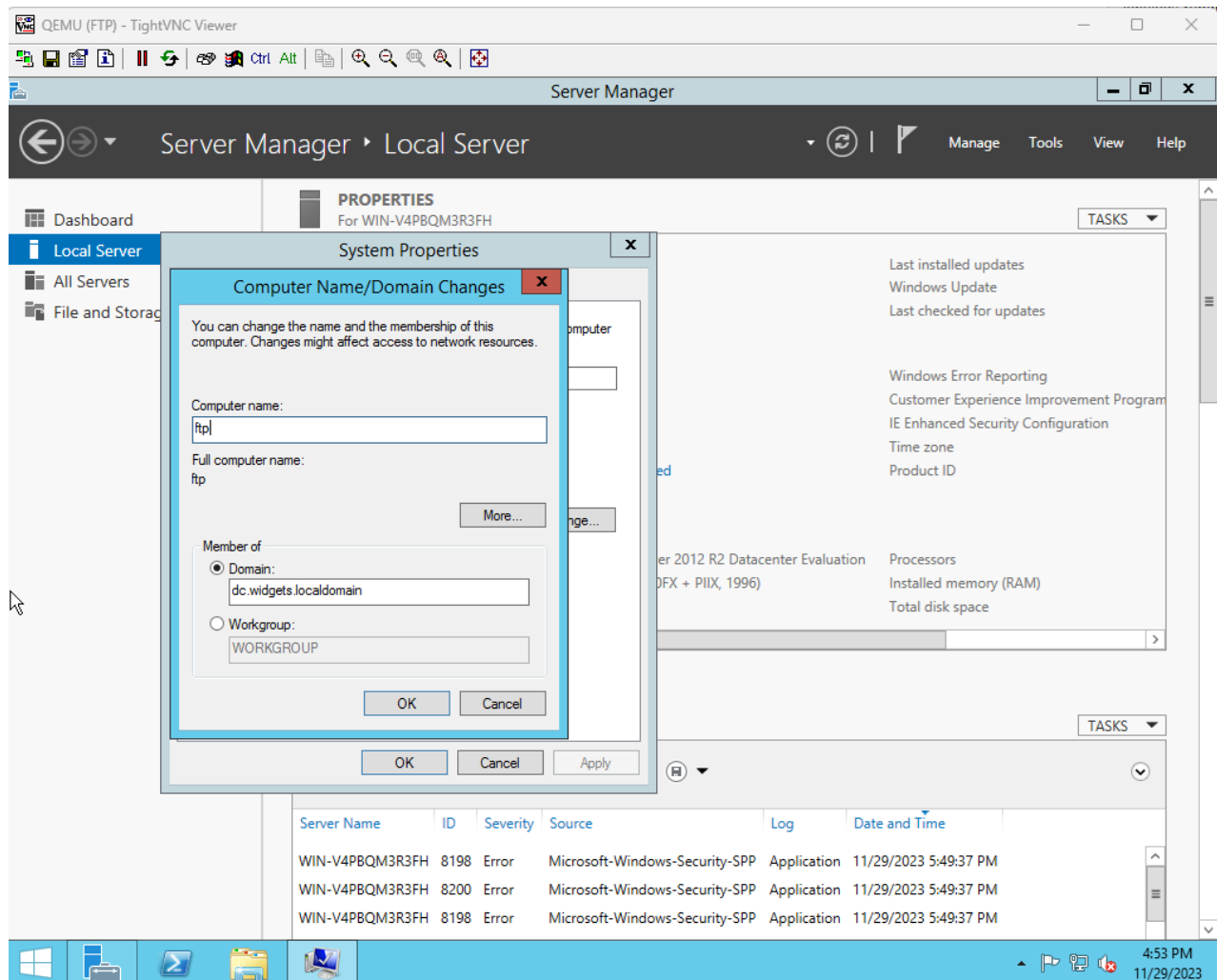
Slide 45 Instructions:

- Review the network diagram for the small business environment setup by your MSP (Managed Service Provider) group.
- Note the addition of an FTP server within the network, indicated by the FTP label and connected to the DMZ-SWITCH.
- The FTP server has a dedicated network interface card (NIC1) with the IP configuration set within the DMZ subnet, 10.128.10.0/24, to ensure it is segregated from the internal LAN for security.
- Verify that the WAN-SWITCH connects to the FortiGate-1 firewall's Port1, which is set to interface with the WAN-CLOUD, symbolizing internet connectivity.
- Check that the internal Windows Domain (DC) and IIS web server are connected to the LAN-SWITCH, while the Ubuntu server is connected to the DMZ-SWITCH, each with their respective IP addresses as per the client's request.
- Confirm that the IP addressing scheme matches the client's requirements for a secure network, internal domain, IIS webserver, Windows 10 workstation, public webserver, public FTP server, LAN network, DMZ network, and guest network.
- Ensure that the gateway addresses for the LAN (10.128.0.1) and DMZ (10.128.10.1) networks are correctly configured in the FortiGate-1 firewall to facilitate proper routing between the different network segments.



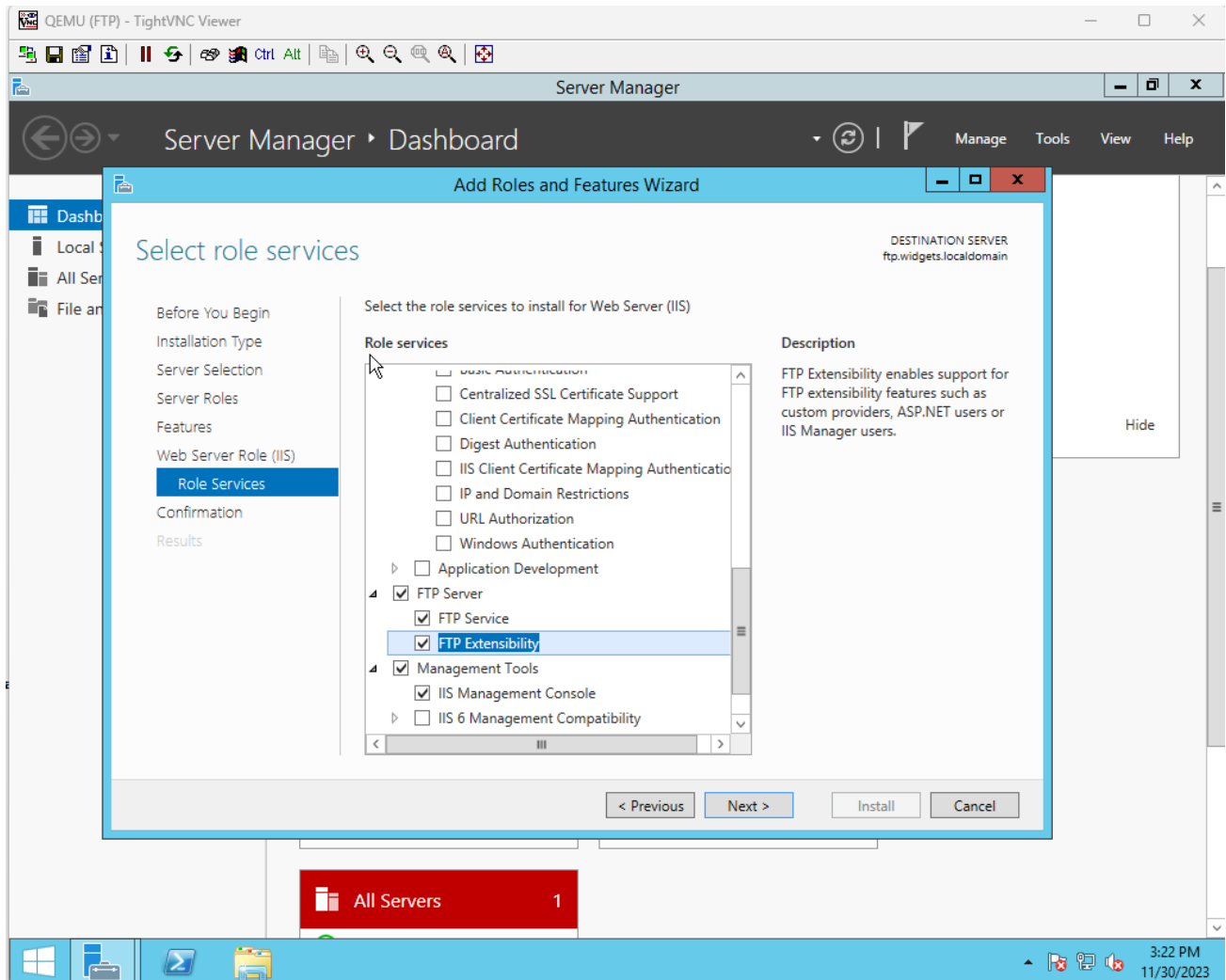
Slide 46 Instructions:

- On the FTP server, open the Server Manager.
- Navigate to the 'Local Server' tab.
- Click on 'Computer name' to open the System Properties dialog box.
- In the 'Computer Name' tab, click the 'Change...' button to rename the computer or change its domain or workgroup membership.
- Change the 'Computer name' to 'ftp' to reflect its role as an FTP server.
- Under 'Member of', select the 'Domain' radio button and enter 'dc.widgets.localdomain' to join the server to the specified domain.
- Click 'OK' to apply the changes. You will be prompted to restart the server for the changes to take effect.



Slide 47 Instructions:

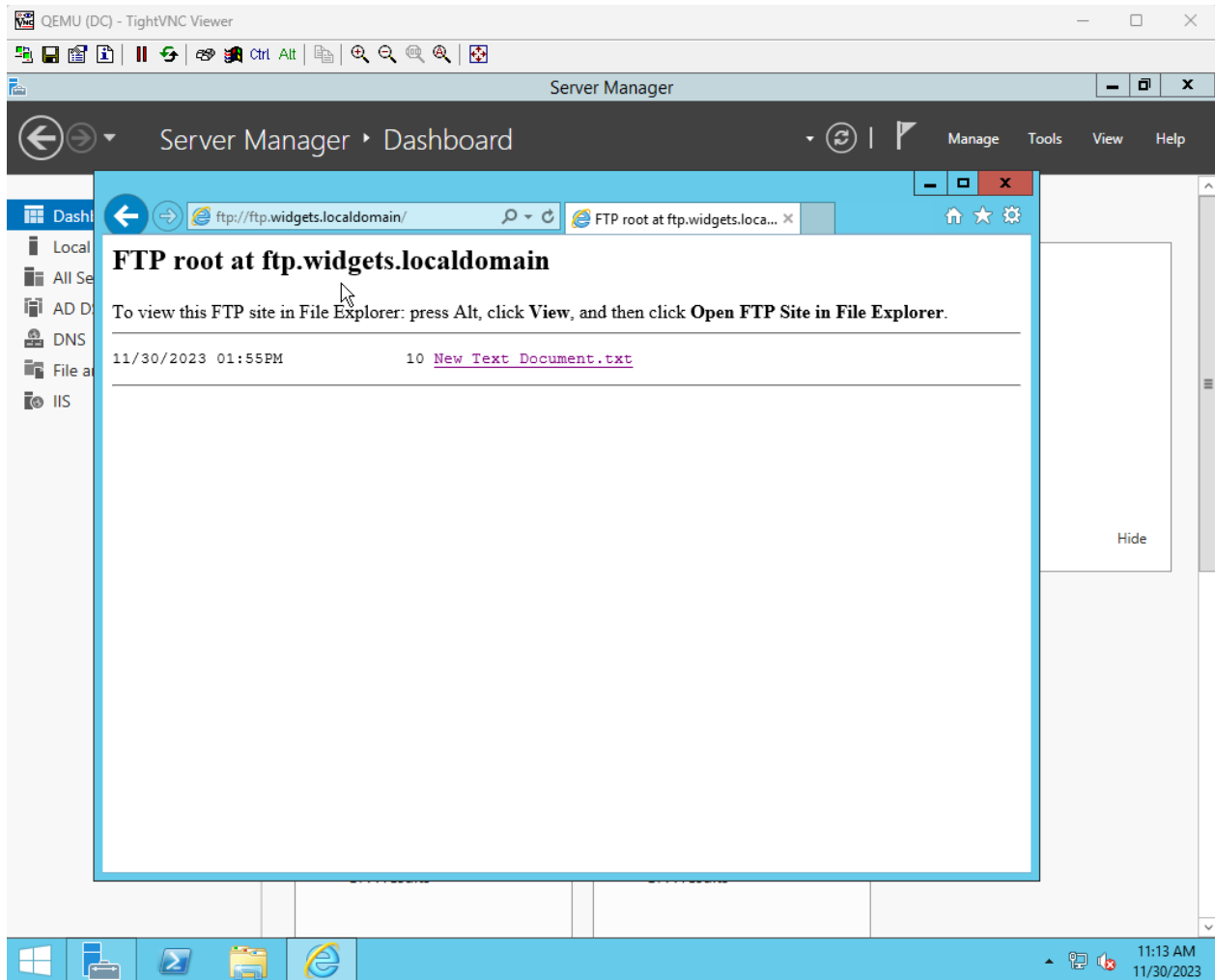
- On the FTP server, open the Server Manager.
- Click on "Add Roles and Features" to launch the wizard.
- Proceed to the "Select role services" section under the Web Server Role (IIS).
- In the "Role services" pane, check the box for "FTP Service" to install the basic FTP server features.
- Also, check "FTP Extensibility" for advanced functionality, such as integration with IIS Manager and ASP.NET support for FTP.
- Review your selections, then click "Next" to proceed.
- On the next screen, confirm the installation selections and click "Install" to begin adding the FTP server role services to your system.



Slide 48 Instructions:

- On the Domain Controller (DC) server, open Internet Explorer.
- Navigate to the FTP site by entering the address <ftp://ftp.widgets.localdomain/> in the browser's address bar.
- The browser window should display the FTP root directory for **ftp.widgets.localdomain**.

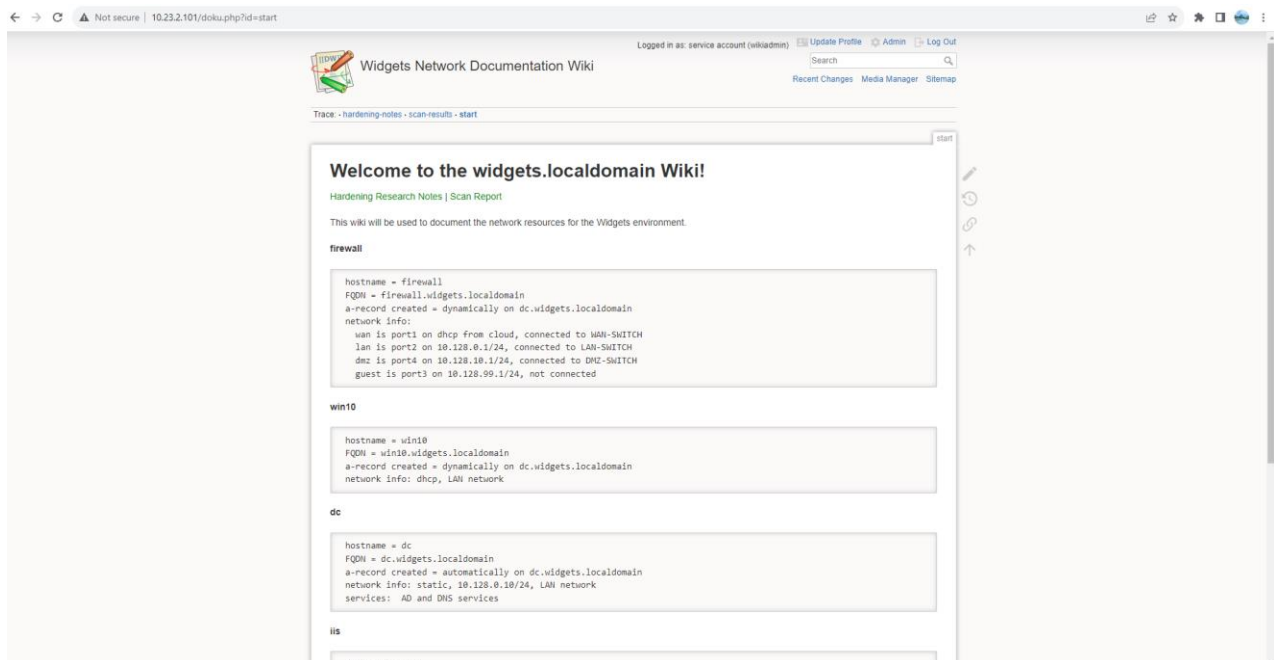
- To open and manage the FTP site in Windows File Explorer, press **Alt**, click **View**, and then select **Open FTP Site in File Explorer**.
- Verify the presence of files or directories, such as the listed "New Text Document.txt", confirming the FTP server is operational and accessible.



Slide 49 Instructions:

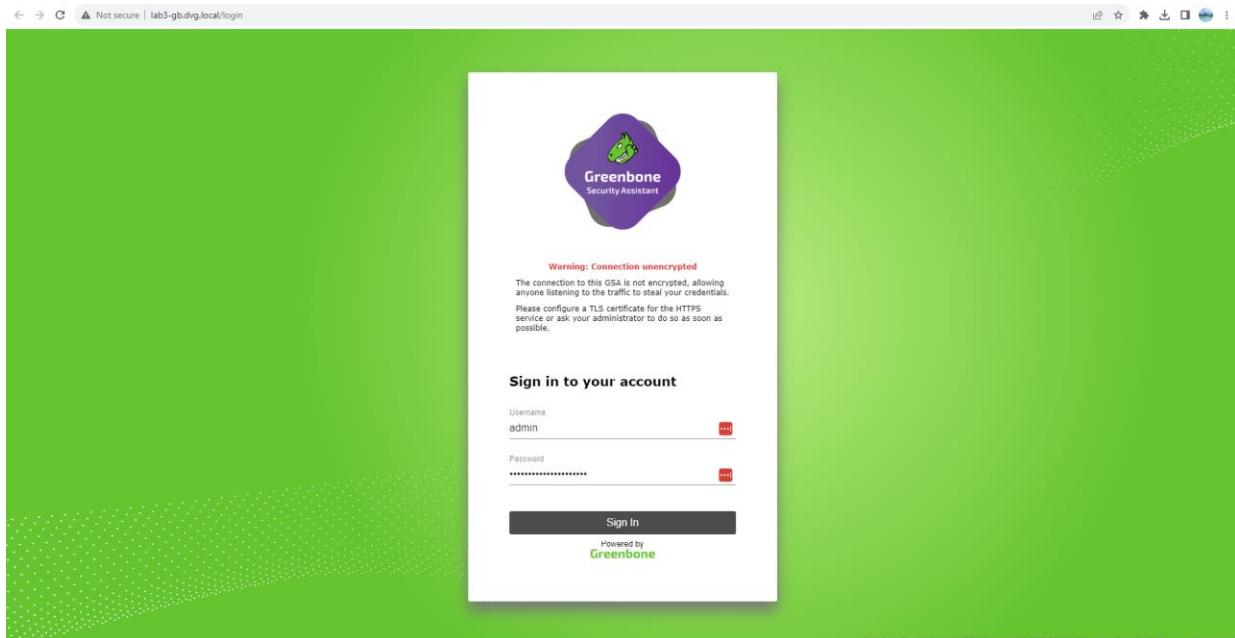
- Open a web browser and access the Widgets Network Documentation Wiki by typing in the IP address of the server hosting the wiki, followed by **/doku.php?id=start**.
- Review the main page to verify that it displays a welcome message and the network resource documentation for the Widgets environment.

- Check the details under the 'firewall' section, confirming the hostname, FQDN, and network interface assignments are correctly listed.
- Under 'win10', ensure the hostname, FQDN, and network information are accurately documented, including DHCP settings.
- Verify the 'dc' (Domain Controller) information is correct, noting the FQDN, A-record creation, network info, and listed services (AD and DNS services).
- Confirm the 'iis' section is present with the appropriate details, though not visible in the current view, it should be consistent with the provided network configuration.
- Ensure all network segments such as LAN, DMZ, and guest networks are documented with their respective IP ranges and connection points as per the client's infrastructure.
- Utilize the wiki's interface to navigate to other sections or to make edits where necessary, by using the options to update profiles, admin configurations, or logging out as indicated at the top right of the page.



Slide 50 Instructions:

- In your web browser, go to the Greenbone Security Assistant login interface at the address shown in the address bar.
- In the 'Username' field, type 'admin'.
- In the 'Password' field, enter the password associated with the 'admin' account.
- Click the 'Sign In' button to access the Greenbone Security Assistant dashboard.
- Once logged in, proceed to set up and run a vulnerability scan as required.



Slide 51 Instructions:

- Access the Greenbone Security Assistant and review the 'Reports' section for the latest vulnerability scan results.
- Examine the vulnerabilities, particularly the one with a high severity score of 10.0, which indicates a critical risk.
- Note that the IP address 10.23.2.100 is common across all listed vulnerabilities, pointing to security issues on a single host.

- The vulnerabilities related to SSL/TLS such as "Weak Cipher Suites," "Deprecated SSLv2 and SSLv3 Protocol Detection," and others suggest the need for updates and configuration changes to strengthen encryption protocols.
- The report's findings, especially the presence of high-severity vulnerabilities, signal the urgent need for network hardening measures to enhance security.
- Based on the report, prioritize the vulnerabilities for remediation, beginning with the highest severity and working down, addressing issues such as weak encryption algorithms and outdated protocols.
- Plan to update the affected systems, enforce stronger security policies, and possibly conduct a follow-up scan after remediation to ensure all issues have been addressed.

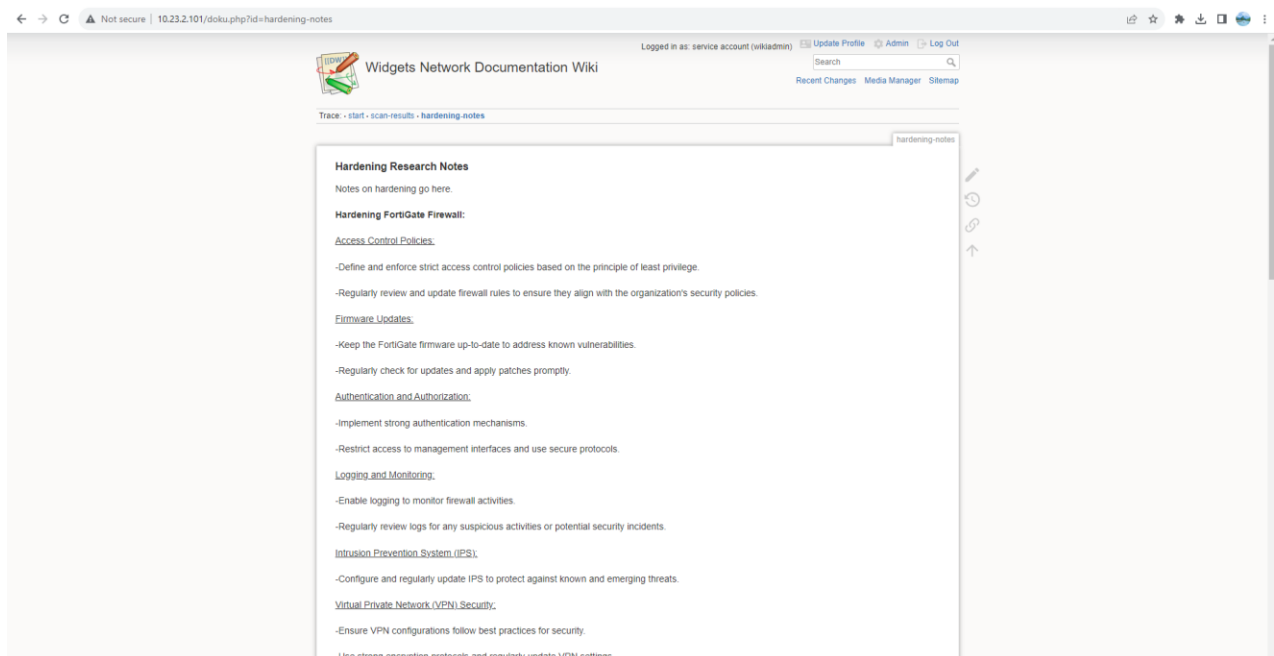
Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (Info)	97 %	10.23.2.100		general/tcp	Mon, Nov 27, 2023 4:11 PM UTC
SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
Weak (Small) Public Key Size(s) (SSH)	5.3 (Medium)	80 %	10.23.2.100		22/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 1024 bits	5.3 (Medium)	80 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	10.23.2.100		22/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: Report 'Null' Cipher Suites	5.0 (Medium)	98 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3 (Medium)	80 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	80 %	10.23.2.100		22/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	3.7 (Low)	80 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	80 %	10.23.2.100		443/tcp	Mon, Nov 27, 2023 4:13 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.23.2.100		general/tcp	Mon, Nov 27, 2023 4:13 PM UTC
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	10.23.2.100		22/tcp	Mon, Nov 27, 2023 4:13 PM UTC

(Applied filter: apply_overrides=0 levels=host rows=100 min_qod=70 first=1 sort-reverse=severity)

Slide 52 Instructions:

- In your web browser, navigate to the Widgets Network Documentation Wiki page specifically for 'Hardening Research Notes'.
- Review the outlined notes, which are meant to guide the hardening process for the network, particularly the FortiGate Firewall.

- The notes begin with 'Access Control Policies', stressing the importance of defining and enforcing strict access control policies based on the principle of least privilege.
- Next, 'Firmware Updates' are highlighted, underscoring the need to keep the FortiGate firmware up-to-date and to apply patches promptly.
- Under 'Authentication and Authorization', the notes recommend implementing strong authentication mechanisms and restricting access to management interfaces using secure protocols.
- 'Logging and Monitoring' emphasize enabling logging to monitor firewall activities and regularly reviewing logs for any suspicious activities or potential security incidents.
- For 'Intrusion Prevention System (IPS)', configure and regularly update IPS to protect against known and emerging threats.
- Lastly, 'Virtual Private Network (VPN) Security' section advises ensuring VPN configurations follow best practices for security and to use strong encryption protocols.
- Use these notes as a checklist to perform network hardening, starting with the most critical areas identified in the vulnerability scan report



The screenshot shows a web browser window displaying a document titled "Hardening Research Notes" on the "Widgets Network Documentation Wiki". The browser's address bar shows the URL "10.23.2.101/doku.php?id=hardening-notes". The document content is as follows:

Hardening Research Notes
Notes on hardening go here.

Hardening FortiGate Firewall:

Access Control Policies:

- Define and enforce strict access control policies based on the principle of least privilege.
- Regularly review and update firewall rules to ensure they align with the organization's security policies.

Firmware Updates:

- Keep the FortiGate firmware up-to-date to address known vulnerabilities.
- Regularly check for updates and apply patches promptly.

Authentication and Authorization:

- Implement strong authentication mechanisms.
- Restrict access to management interfaces and use secure protocols.

Logging and Monitoring:

- Enable logging to monitor firewall activities.
- Regularly review logs for any suspicious activities or potential security incidents.

Intrusion Prevention System (IPS):

- Configure and regularly update IPS to protect against known and emerging threats.

Virtual Private Network (VPN) Security:

- Ensure VPN configurations follow best practices for security.
- Use strong encryption protocols and regularly update VPN settings.