

Real-World Scenario 9-6: Planning Network Security

Scenario: You have been given a new assignment at your organization's newly built sister office. You have been tasked with installing several security technologies to protect the LAN and the WLAN.

Take a look at the following table, which includes a list of problems that you need to tackle. In the Your Solution column, enter the device, technology, or other solution that you would employ for each situation. Be concise and brief in your answers. This Real-World Scenario spans the content within Chapters 6 through 9.

Issue	Your Solution
E-mail and web servers need to be separated from the LAN.	
The WAP is not running any encryption.	
Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent capability.	
You have discovered that several computers' wired connections suffer from EMI. They contain confidential information and are potential victims for wiretapping.	
The firewall is not configured for the proper type of packet filtering.	

Issue	Your Solution
<p>Users on the network need to be protected from malicious content on websites.</p>	
<p>You are concerned about anomalous packets and want them to be removed from the network if they are found.</p>	
<p>There is a long-distance wired connection between the firewall and the extranet. There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping.</p>	

Real-World Scenario 9-6 Solution

As you can see, being in charge of the security for a network can be a lot of work—a full-time job perhaps, given the size of a network. Remember that you are attempting to do the following:

- Ensure that *confidential* files remain secret.
- Keep the *integrity* of your data intact.
- Make sure that data is still *available* to the appropriate persons.

Use the CIA approach to help govern your actions as a security administrator. Add layers of security so that you end up with a solid defense-in-depth plan, ultimately protecting your network and data on multiple levels. See the following table for some possible solutions to the issues you face.

Issue	Your Solution
E-mail and web servers need to be separated from the LAN.	Implement a DMZ.
The WAP is not running any encryption.	Configure WPA2 and AES.
Your boss wants additional authentication for the wireless network above and beyond the WAP's inherent capability.	Utilize a RADIUS server or similar external authentication device.
You have discovered that several computers' wired connections suffer from	Replace unshielded twisted-pair (UTP) connections with shielded twisted-pair (STP).

Issue	Your Solution
EMI. They contain confidential information and are potential victims for wiretapping.	
The firewall is not configured for the proper type of packet filtering.	Implement SPI, and increase the level of NAT filtering if necessary.
Users on the network need to be protected from malicious content on websites.	Use a proxy server with a content filter.
You are concerned about anomalous packets and want them to be removed from the network if they are found.	Install an inline NIPS between the firewall and the Internet or in between the firewall and the switch.
There is a long-distance wired connection between the firewall and the extranet. There are areas of the building that are not particularly secure and could be accessed by malicious insiders who could possibly attempt wiretapping.	Use fiber-optic connections between the firewall and extranet. Install a CCTV system.

Simulation: Complete the simulation "9-6: Planning Network Security."