CCNA Security Lab Workbook (640-553)

Passing the Cisco Certified Network Associate Security 640-553 certification exam is difficult enough if you are fully prepared by attending a Cisco CCNA Security class with an instructor and you have access to all the proper books and equipment. But what happens when you go home as it is not reasonable for you to retain all that information you would have been exposed to in a one week boot camp? You will need to setup a CCNA Security lab in your home or work to really absorb all those concepts and cement them into your brain through actual hands-on application. This is where our CCNA Security 640-553 Lab Workbook can help you! Our CCNA Security 640-553 Lab Workbook was designed with the knowledge that most of our customers can't afford a large lab. Some people can only afford the bare minimum two router lab. That is why we have this specially designed CCNA Security Lab Workbook that will cover the concepts with a simple CCNA Security lab of two Cisco 2600XM routers and two Cisco 2950 switches. What if you don't have those exact units? Well, most of the labs(about 75%) will still work with a little tweaking as long as your routers have the Firewall feature set. Then you can also complete about another 5% of the labs if your routers have the Crypto feature set. So will you be able to do them all? Not exactly, but you can do many of them and you will still be able to learn as you see the concepts and the reasoning behind each lab as you progress through the CCNA Security lab workbook. So let's take a look at the labs covered in this CCNA Security 640-553 Lab Workbook. Chapter 1: Configuring Administrative Access & Roles On A Router Lab 1-1: Scenario, Configuration & Background Lab 1-2: Configuring Administrative Access; Local, VTY & SSH Lab 1-3: Configuring Administrative Roles Using CLI Chapter 2: Securing Administrative Access Using AAA & RADIUS Lab 2-1: Scenario, Configuration & Background Lab 2-2: Configure WinRadius and AAA using SDM Lab 2-3: Configure AAA with RADIUS using CLI Chapter 3: Configure AutoSecure Lab 3-1: Scenario, Configuration & Background Lab 3-2: Configure AutoSecure; Banners, Passwords, SSH, CBAC Lab 3-3: Verify AutoSecure Results Chapter 4: Configure CBAC and Zone-Based Firewall Lab 4-1: Scenario, Configuration & Background Lab 4-2: Configure a Context-Based Access Control(CBAC) Firewall Lab 4-3: Configure a Zone-Based Firewall Lab 4-4: Modify Policies of the Firewall Chapter 5: Configuring Intrusion Prevention System Lab 5-1: Scenario, Configuration & Background Lab 5-2: Configure Syslog & Modify IPS Signatures Chapter 6: Securing Layer 2 Switches Lab 6-1: Scenario, Configuration & Background Lab 6-2: Configure SSH Lab 6-3: Secure Trunk & Access Ports Lab 6-4: Enable Port Fast & BPDU Guard Lab 6-5: Configure SPAN & Monitor Traffic with WireShark Chapter 7: Configuring Syslog & SNMP Traps to Monitor Network Traffic Lab 7-1: Scenario, Configuration & Background Lab 7-2: Install Kiwi Syslog Server & Configure Logging Lab 7-3: Configure SNMP Traps & Verify Logs Chapter 8: Cisco Security Policy Builder Lab 8-1: Scenario, Configuration & Background Lab 8-2: Using Cisco Security Policy Builder Lab 8-3: Apply Security Configuration - Routers Lab 8-4: Apply Security Configuration - Switches Chapter 9: Configuring a Remote Access VPN Server & Client Lab 9-1: Scenario, Configuration & Background Lab 9-2: Configuring a Remote Access VPN Server Lab 9-3: Configuring a VPN Client & Connecting Chapter 10: Configuring a Site to Site VPN Using Cisco SDM & CLI Lab 10-1: Scenario, Configuration & Background Lab 10-2: Configuring a Site to Site VPN Using SDM Lab 10-2: Configuring a Site to Site VPN Using CLI Chapter 11: Configuring a Site to Site VPN Using Adaptive Security Appliances(ASA 5500s) Bonus Labs* Lab 11-1: Scenario, Configuration & Background Lab 11-2: Configuring a Site to Site VPN Using ASA 5500s Download | **Size:** 5.00 GB **[This hidden password content is only available for our VIP member. Become VIP Member NOW**