

Graded Exercises

B3 – Network Security 1

Graded Exercises



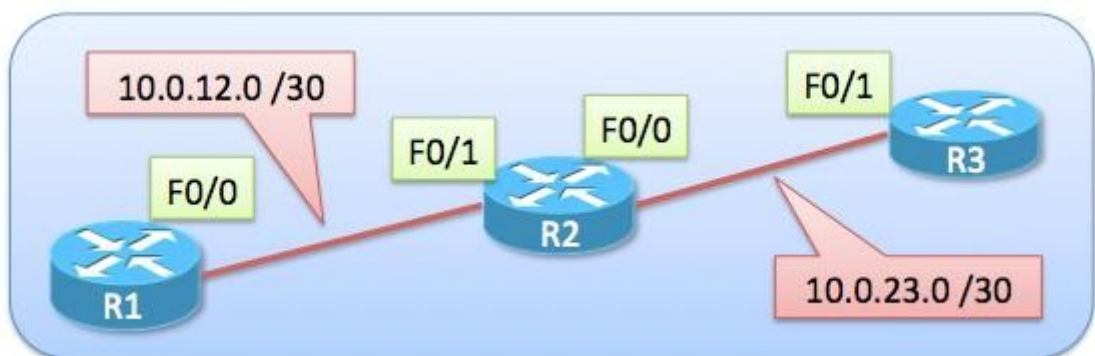
Version : 1.0
Auteur : SLA-Labs
Statut : Final



1. Questions

1. What does AAA standing for?
2. Which layer 4 protocol does TACACS+ use?
3. What is the global command to enable AAA on a device (Router or Switch)?
4. When using SSH, with which key does the sender use to encrypt its data? Its own private key? Its own public key? The receiver's public key? The receiver's private key?
5. What is the difference between CBAC and IP session Filtering?
6. What command will prevent your LAN to be attacked by a rogue DHCP server?
7. What is the protocol used to prevent broadcast loop when you have redundancy with switches?

2. Configuration



The .net is the EndLabNS1-19nov.net and the IOS image is C2600-AD.BIN

1. Refer to the exhibit, configure the host name and configure password to access to the privileged mode : **cisco** , for all the routers.
2. Configure the IP addresses as following:
 - R1 Fa0/0 : 10.0.12.1 /30
 - R1 Fa0/1 : 10.0.12.2 /30
 - R2 Fa0/0 : 10.0.23.1 /30
 - R2 Fa0/1 : 10.0.23.2 /30
3. Configure a static route on R1 pointing to the subnet 10.0.23.0 /30 and one on R3 pointing to the subnet 10.0.12.0 /30
4. Configure SSH using keys of 768 bits on R3, You will have to create a username **labo** with the password **cisco**, and use the local database of the router.
5. On R2, configure CBAC to permit and inspect SSH traffic, from R1 to R3. The CBAC Rule will be SSH-Inspect. Only traffic from R1 to R2 using SSH or TELNET has to be permitted.