|  |  |
| --- | --- |
|  | |
| Case study Connecting and securing network  2024-2025 | |
| **Bosch Tom**  **Depovere Koen**  **Mitch Mommers** | Graduaat Netwerk- en systeembeheer |
|  |
| Campus Geel, Kleinhoefstraat 4, BE-2440 Geel |

8865

Inhoudsopgave

[Case Study 5](#_Toc177333726)

[Overview and Objectives 6](#_Toc177333727)

[1 Create network documentation 7](#_Toc177333728)

[1.1 Objectives 7](#_Toc177333729)

[1.2 Input: Provide required specifications for the network 7](#_Toc177333730)

[1.3 The output should include 7](#_Toc177333731)

[2 Build the LAN for SafeUS – router on a stick 8](#_Toc177333732)

[2.1 Objectives 8](#_Toc177333733)

[2.2 Input 8](#_Toc177333734)

[2.3 The output should include: 8](#_Toc177333735)

[3 Build the LAN for site SafeEU – collapsed core + access layer 9](#_Toc177333736)

[3.1 Objectives 9](#_Toc177333737)

[3.2 Input 9](#_Toc177333738)

[3.3 The output should include: 9](#_Toc177333739)

[4 Add static routing to the LAN and WAN 10](#_Toc177333740)

[4.1 Objectives: configure static routing 10](#_Toc177333741)

[4.2 Input: Provide required specifications 10](#_Toc177333742)

[4.3 The output should include: 10](#_Toc177333743)

[5 Build a centralized DHCP solution for SafeEU. 11](#_Toc177333744)

[5.1 Objectives: 11](#_Toc177333745)

[5.2 Input: 11](#_Toc177333746)

[5.3 The output should include: 11](#_Toc177333747)

[6 Build single area OSPF in LAN and WAN 12](#_Toc177333748)

[6.1 Objectives: configure dynamic routing 12](#_Toc177333749)

[6.2 Input 12](#_Toc177333750)

[6.3 The output should include: 12](#_Toc177333751)

[7 Build WAN 13](#_Toc177333752)

[7.1 Objectives: configure WAN 13](#_Toc177333753)

[7.2 Input 13](#_Toc177333754)

[7.3 The output should include: 13](#_Toc177333755)

[8 Add Monitoring, TFTP server and syslog 14](#_Toc177333756)

[8.1 Objectives: Network Management 14](#_Toc177333757)

[8.2 Input 14](#_Toc177333758)

[8.3 The output should include: 14](#_Toc177333759)

[9 Add firewall to networks 15](#_Toc177333760)

[9.1 Objectives 15](#_Toc177333761)

[9.2 Input 15](#_Toc177333762)

[9.3 The output should include: 15](#_Toc177333763)

[10 Add provider connectivity with BGP and Network address translation 16](#_Toc177333764)

[10.1 Objectives: 16](#_Toc177333765)

[10.2 Input: 16](#_Toc177333766)

[10.3 The output should include: 16](#_Toc177333767)

[11 Add security with ACL and firewall policy 17](#_Toc177333768)

[11.1 Objectives: 17](#_Toc177333769)

[11.2 Input 17](#_Toc177333770)

[11.3 The output should include: 17](#_Toc177333771)

[12 Add Site-to-Site VPN 18](#_Toc177333772)

[12.1 Objectives 18](#_Toc177333773)

[12.2 Input 18](#_Toc177333774)

[12.3 The output should include 18](#_Toc177333775)

[13 Build Connection to Cloud 19](#_Toc177333776)

[13.1 Objectives 19](#_Toc177333777)

[13.2 Input 19](#_Toc177333778)

[13.3 The output should include 19](#_Toc177333779)

Case Study

Dear student,

This document contains the guidelines for the preparation of your case study.

**Description**

During this case study, you will gradually build a network for an organization. The building process will happen in different phases. The case study will be executed by small teams of students. The team members for each team are selected by the teacher.

Each phase has specific requirements:

* You will come prepared before you start each phase. Your preparation should include at least **a drawing** of what you are going to build, and **a test plan** that you will execute at the end of the phase to ensure the setup is working as expected. It is advisable to prepare your configuration files with a simulation tool.
* You will build **“as-build” documentation** at the end of each phase, to ensure you can rebuild the setup at a later point in time.

You will build the network on hardware devices in the classroom.

The “as build” documentation is created in MS-Word (Thomas More template) and contains:

* Diagrams
* Configuration files including comments

The “as-build” documentation will be submitted into Canvas before each deadline.

At the start of each lesson, we will have a short review of the technology utilized during the phase at stake.

You can call on **coaching** from your lecturer **during classroom hours**.

Overview and Objectives

During this case study you will build and configure a network for a small and medium-sized office for the company AllSafe. AllSafe has 2 subsidiary offices, SafeUS and SafeEU. SafeUS has one office in New York and one office in Chicago. SafeEU has an office in Brussels.

You will require and utilize the skills that you learned throughout the different networking courses. This case study is broken down in several phases to build up the network. Each phase focuses on specific topics in the network. Each phase has a detailed list of requirements. It is crucial that you read and understand each requirement to complete the project. It is expected that you utilize the **Cisco** **best practices** to configure the devices (e.g. configure description, …).

This case study requires that you accomplish the following:

1. Create network documentation.
2. Build a LAN network utilizing “router on a stick” for SafeUS.
3. Build a LAN network utilizing a “collapsed core” network for SafeEU.
4. Add static routing to the LAN and WAN.
5. Build a centralized DHCP solution for SafeEU.
6. Build single area OSPF in LAN and WAN.
7. Build WAN with OSPF.
8. Add Monitoring, TFTP server and syslog.
9. Add firewall to networks.
10. Add provider connectivity with BGP and Network address translation.
11. Add security with ACL and firewall policy.
12. Add VPN with GRE over IPsec Site-to-Site VPN.
13. Build connection to Cloud.

Further information about these steps can be found later in this document.

The picture below shows the final network topology at the end of the case study.

A diagram of a computer network

Description automatically generated

# Create network documentation

## Objectives

* + Learn to create network documentation.
  + Understand the difference between a logical and a physical network diagram
  + Learn to utilize a network documentation tool (e.g. Visio)
  + Exercise on IP-subnetting.

## Input: Provide required specifications for the network

* The company SafeUS has two offices:
  + New York (NY): 250 users
  + Chicago (CHI): 50 users
* The company SafeEU has one office:
  + Brussels (BRU): 300 users
* WAN topology
  + The offices of SafeEU are connected via a private network.
  + The offices of SafeUS are connected via a private network.
  + The sites New York and Brussels are connected through the provider.
* LAN topology
  + Every site contains following VLANs
    - Data VLANs: The data vlans will connect wired devices
      * Vlan 10: DATA vlan
      * Vlan 20: Wireless vlan
      * Vlan 100: MGMT vlan
      * Vlan 200: SERVERS vlan
* IP addressing
  + LAN addressing: 10.0.0.0/8
  + WAN addressing: 172.16.0.0/16

## The output should include

* Logical network diagram (in Visio)
* Physical network diagram (in Visio)
* IP address planning (in Excel)

# Build the LAN for SafeUS – router on a stick

## Objectives

* Rehearsal of the basic concepts
* *Provide the answer for phase 1 to avoid rubbish in – rubbish out*
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input

* Switches:
  + Basic switch configuration (ready for remote access via vty)
  + Setup VLAN’s
    - Vlan 10: DATA vlan
    - Vlan 20: Wireless vlan
    - Vlan 100: MGMT vlan
    - Vlan 200: SERVERS vlan
  + Configure access ports
  + Configure trunk ports
* Router:
  + Basic router configuration (ready for remote access via vty)
  + Configure inter-vlan routing with Router on a stick.
  + Configure static route (SR) between routers of Chicago and New York
* Use static IP addressing for clients.

## The output should include:

* Documentation
* Configuration files + description
  + Configuration Router + sub-interfaces
  + Configuration Switch + vlans
* Test plan
* Test results

# Build the LAN for site SafeEU – collapsed core + access layer

## Objectives

* Collapsed core and access layer topology setup.
* Increase capacity between core switches.
* Layer-3 redundancy in the LAN – HSRP
* Understand timing for fail-over
* Create test plan.
  + For SVI
  + For HSRP
  + For STP
* Execute the test plan and troubleshoot.
* Document test results.

## Input

* Basic switch configuration (ready for remote access via vty)
* Configure VLANs
* Configure STP topology
  + Use Rapid PVST+
* Configure inter-vlan routing in collapsed core setup (SVI)
* Configure etherchannel between core switches.
* Configure HSRP on core switches.
  + HSRP Active -Standby setup + pre-empting
* Core switches should be root bridge and secondary root bridge.
* The L3 switch of Brussels is the active gateway for the vlans of Brussels.
* Make sure that the STP root bridge is the same as the active gateway.
* Add bpdu guard on switch interfaces (<https://www.youtube.com/watch?v=Vv5TOIG37dg>)
* Use static IP addressing for clients.

## The output should include:

* Documentation
* Configuration files + descriptions
  + Configuration 2 x Core Switch
  + Configuration 2 x Access switch
* Test plan
* Test results

# Add static routing to the LAN and WAN

## Objectives: configure static routing

* Configure the network with static routing
* Understand that there is no redundancy
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input: Provide required specifications

* Add Router (FW\_NY) to network (we will replace this by firewall in later stage)
* Add Router (FW\_BRU) to network (we will replace this by firewall in later stage)
* Configure static routing in LAN and WAN between routers and between routers.
* Configure default route.
* Configure floating static routes.
* Configure DHCP for New York and Chicago (don’t forget relay agent).

## The output should include:

* Documentation
* Configuration files + descriptions
  + Configuration Routers
  + Configuration Switches
* Test plan + test results (show commands)

# Build a centralized DHCP solution for SafeEU.

## Objectives:

* Install and configure centralized DHCP for SafeEU.
* Create test plan for DHCP solution.
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input:

* Install a DHCP server and connect it to the server vlan of Brussels.
* Configure a DHCP server and DHCP relay agent.
* Configure the DHCP pools for data vlans of Brussels.
* Configure DHCP options on the DHCP scopes.

## The output should include:

* Documentation
* Configuration
* Test plan
* Test results

# Build single area OSPF in LAN and WAN

## Objectives: configure dynamic routing

* Configure OSPF on routers.
* Understand that OSPF provides redundancy
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input

* Configure routed ports on Layer-3 switches.
* Configure the network with OSPF
  + Propagate the networks of New York and Chicago through OSPF.
  + Propagate the networks of Brussels through OSPF.
* Add Router (FW\_BRU) to network (we will replace this by firewall in later stage)
* Configure and propagate the default route through OSPF.
* Configure floating static routes.

## The output should include:

* Documentation
* Configuration files + descriptions
  + Configuration Routers
* Test plan + test results (show commands)

# Build WAN

## Objectives: configure WAN

* Build WAN network with provider.
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input

* Add Router (R\_Provider) to network.
* Configure connection between Routers FW\_NY and R\_Provider.
* Configure connection between Routers FW\_BRU and R\_Provider.
* Configure the WAN with OSPF.

## The output should include:

* Documentation
* Configuration files + descriptions
  + Configuration Routers
* Test plan + test results (show commands)

# Add Monitoring, TFTP server and syslog

## Objectives: Network Management

* Install and configure monitoring server.
* Install and configure TFTP and Syslog server.
* Configuration management (TFTP) – backup and deploy configuration from the server
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input

* Install Zabbix server.
* Configure Zabbix server to monitor the switches and routers.
* Install Tftpd64 (<https://pjo2.github.io/tftpd64/>)
* Configure syslog on routers to send messages to syslog server.
* Configure routers to back up the configuration to TFTP server
* Configure devices/Restore configurations from TFTP server
* Configure the routers to send syslog to the syslog server

## The output should include:

* Documentation
* Configuration files + descriptions
  + Configuration Zabbix server
  + Configuration TFTP server
  + Configuration Syslog server
  + Configuration Routers and switches
* Testplan

# Add firewall to networks

## Objectives

* Install and configure firewalls.
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input

* Install Palo Alto Firewalls.
* Configure network setting on the PA FW.

## The output should include:

* Documentation
* Configuration
* Test plan
* Test results

# Add provider connectivity with BGP and Network address translation

## Objectives:

* Configure BGP
* Configure network address translation (NAT)
* Create test plan
* Execute the test plan and troubleshoot
* Document test results

## Input:

* Configure BGP with ASxxx
* Configure PAT for Brussels to hide behind the IP address of the WAN interface of the firewall Brussels.
* Configure PAT for New York and Chicago to hide behind the IP address of the WAN interface of the firewall New York.
* Add redundant connection between the firewalls and R\_provider.

## The output should include:

* Documentation
* Configuration
* Test plan
* Test results
* Show that NAT is working (show commands)

# Add security with ACL and firewall policy

## Objectives:

* Add L4 network protection with perimeter firewall.
* Add security through ACL’s between vlans (segmentation).
* Protect devices within management vlan.
* Secure remote administrative access to a device using the vty lines.
* Protect STP
* Protect MAC address table attacks

## Input

* L3 switches:
  + Configure ACL so that no data is allowed to pass between data vlans.
  + Configure ACL where DHCP traffic is allowed to DHCP server.
  + Configure ACL to secure the remote administrative access for the network devices.
* Firewall:
  + Configure security policy on firewall.
* Switches:
  + Implement Port security
    - With dynamically learned MAC address.
    - Secure Unused ports.
* Implement DHCP snooping.

## The output should include:

* Documentation
* Configuration
* Test plan
* Test results

# Add Site-to-Site VPN

## Objectives

* Create GRE over IPsec Site-to-Site VPN tunnel between Brussels and New York

## Input

* Setup tunnel via GRE.
* Setup tunnel via IPSec pre-shared keys.
* Configure OSPF between New-York and Brussels.

## The output should include

* Documentation
* Configuration
* Test plan
* Test results
  + Show that tunnel is active.

# Build Connection to Cloud

## Objectives

* Learn to build a safe connection to a cloud provider.

## Input

## The output should include

* Documentation
* Configuration
* Test plan
* Test results