BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : Thomas GRENIER	**N° candidat :** 230382822
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 24 / 04 / 2026

Organisation support de la réalisation professionnelle

Intitulé de la réalisation professionnelle

Installer et mise en service d'un Pare Feu

Période de réalisation : 06/10/2025 au 06/02/2026 **Lieu :** Ecoris Chambery

Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Pendant ma formation en BTS SIO, j'ai obtenu des accès à un serveur pour la création d'un réseau d'entreprise. Pour pouvoir sécuriser mon réseau, j'ai donc décidé de mettre en place un Firewall qui me servirait à sécuriser mon réseau et également mettre en place différents services

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources matérielles :

- Pfsenseserveur
- Poste Windows
- 4 cartes réseaux disponible

Ressources logiciels:

Navigateur Internet
OpenVPN
DHCP Service
Filtrage de flux

Ressources documentaires :

- Reddit
- IT Connect
- support de cour
- Github
- Claude AI
- Shéma réseau de l'infrastructure mis en place dans mon réseau

Modalités d'accès aux productions[3] et à leur documentation[4]

La procédure de ma réalisation professionnelle sur la mise en service de mon Firewall sera mis a disposition sur mon portfolio
Elle sera également présente et mise à disposition sur un document partagé.
Cette procédure décrit les différentes étapes de l'installation et la configuration de mon projet et les différentes étapes de réalisations qui m'on permis de le finaliser.

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Pour commencer, afin de garantir une sécurité sur mon réseau, j'ai décidé d'installer un Pare feu entre le réseau fourni par Ecoris et mes machines. J'ai donc choisi d'utiliser Pfsense comme service de firewall.

J'ai commencé dans un premier temps à installer le serveur et à mettre en place le service DHCP sur les interfaces WIFI ainsi que DMZ

J'ai poursuivi par la configuration de ma zone DMZ et des règles de sécurité sur celle-ci.

Ensuite, j'ai paramétrer les règles de sécurité sur toutes les autres interfaces.

J'ai continué avec la mise en place de mon portail captif WIFI sur l'interface voulu avec le reglage de celui-ci.

Une fois celui-ci fini, j'ai donc procéder à la mise en service de OpenVPN sur mon Pfsense. Pour cela, il a été nécessaire de créer des utilisateurs pour permettre la connexion et également la configuration de Certificat serveur et utilisateur.

J'ai fini par l'installation d'un module d'import de configuration pour l'appliquer sur un client et ainsi vérifier le bon fonctionnement des différents services mis en places.
J'ai ensuite fini par installer différents logiciels automatiquement comme Google Chrome et également OpenVPN

PROCÉDURE DE CONFIGURATION

pfSense – Pare-feu & Routeur

Portail Captif • DMZ • DHCP • Filtrage • VPN

Table des matières

1. Introduction et Vue d'ensemble

Ce document décrit l'ensemble des configurations effectuées sur le pare-feu pfSense déployé sur le réseau. Il couvre les quatre grandes thématiques suivantes :

- Portail Captif – authentification des utilisateurs avant accès Internet
- Zone DMZ – isolation des serveurs exposés
- Service DHCP – attribution dynamique des adresses IP
- Règles de filtrage – contrôle du flux réseau
- VPN – accès distants sécurisés

pfSense est un système d'exploitation open-source basé sur FreeBSD, dédié aux fonctions de pare-feu et de routeur. Il s'administre intégralement via une interface web (WebGUI) accessible sur HTTPS.

1.1 Architecture réseau retenue

Interface	Nom logique	Réseau	Rôle
hn0	WAN	192.168.12.0/24	Connexion Internet sur le pfsense d'Ecoris
hn1	LAN	192.168.4.0/24	Réseau local – utilisateurs /serveurs
hn2	DMZ	10.0.10.0/24	Zone démilitarisé
hn3	PORTAIL	192.168.10.0/24	Zone portail captif wifi

2. Installation et Accès Initial

2.1 Installation de pfSense

- Créer une nouvelle machine sur Hyper V
- Booter sur le support d'installation
- Accepter les conditions de licence
- Choisir « Install pfSense »
- Sélectionner le disque de destination et confirmer
- Laisser le système redémarrer et retirer le support

2.2 Configuration initiale des interfaces

- Au premier démarrage, attribuer les interfaces à WAN, LAN via le menu console
- Confirmer l'adresse IP du LAN (192.168.4.254/24)
- Depuis un poste client sur le LAN, ouvrir un navigateur web
- Accéder à l'URL : https://192.168.4.254
- Se connecter avec les identifiants par défaut :
  - Utilisateur : admin
  - Mot de passe : pfsense
- Suivre l'assistant « Setup Wizard » pour la configuration de base (hostname, fuseau horaire, DNS, mot de passe admin)

Note : Le mot de passe admin a été laissé par défaut afin de limiter les possibles problèmes de connexions.

3. Configuration du Service DHCP

Le service DHCP de pfSense distribue automatiquement les paramètres réseau aux équipements clients sur chaque interface.

3.1 Activation et paramétrage – Interface DMZ

- Aller dans Services > DHCP Server
- Sélectionner l'onglet DMZ
- Cocher « Enable DHCP server on DMZ interface »
- Renseigner les paramètres :

Paramètre	Valeur
Range – From	10.0.10.10
Range – To	10.0.10.250
Gateway	10.0.10.254
DNS Server 1	192.168.4.1

- Cliquer sur Save puis Apply Changes

4. Configuration de la Zone DMZ

La DMZ (Demilitarized Zone) héberge les serveurs accessibles depuis Internet (web, mail, FTP…) tout en les isolant du réseau LAN interne. pfSense gère cette segmentation via une interface dédiée et des règles de filtrage spécifiques.

4.1 Création de l'interface DMZ

- Aller dans Interfaces > Assignments
- Sélectionner le port réseau disponible (ex : hn2) dans la liste « Available network ports »
- Cliquer sur Add
- Cliquer sur le lien de la nouvelle interface pour la configurer
- Renseigner les paramètres :

Champ	Valeur
Enable	Coché
Description	DMZ
IPv4 Configuration Type	Static IPv4
IPv4 Address	10.0.10.254/24
Block private networks	Décoché

Champ	Valeur
Block bogon networks	Décoché

- Cliquer sur Save puis Apply Changes

4.2 Règles de pare-feu sur la DMZ (voir aussi Section 5)

Les règles suivantes définissent la politique de sécurité de la DMZ :

- La DMZ peut accéder à Internet (HTTP/HTTPS sortant)
- La DMZ NE peut PAS accéder au LAN (isolation stricte)
- Le LAN peut initier des connexions vers la DMZ (administration)

4.3 Publication de services (NAT Port Forwarding)

- Aller dans Firewall > NAT > Port Forward
- Cliquer sur Add
- Renseigner la règle (HTTP vers serveur web)

Champ	Valeur exemple
Interface	WAN
Protocol	TCP
Destination (WAN address)	WAN address
Destination port range	80 (HTTP)
Redirect target IP	10.0.10.1
Redirect target port	80
Description	HTTP vers serveur web DMZ
Filter rule association	Add associated filter rule

- Cliquer sur Save puis Apply Changes

5. Règles de Filtrage (Firewall)

pfSense applique les règles de filtrage par interface, dans le sens entrant. L'ordre des règles est primordial : la première règle qui correspond à un flux est appliquée.

5.1 Principes généraux

- Politique par défaut : tout trafic non explicitement autorisé est bloqué
- Les règles sont évaluées de haut en bas (ordre d'affichage)
- Placer les règles les plus spécifiques en premier
- Utiliser les alias pour regrouper IPs et ports

5.2 Règles sur l'interface LAN

- Aller dans Firewall > Rules > LAN

Action	Protocol	Source	Destination	Port dest.	Description
Pass	TCP	LAN subnet	any	443	Navigation web
Pass	TCP/UDP	LAN subnet	any	123	NTP
Block	any	LAN subnet	any	any	Blocage par défaut

5.3 Règles sur l'interface DMZ

- Aller dans Firewall > Rules > DMZ

Action	Protocol	Source	Destination	Port dest.	Description
Block	any	DMZ subnet	LAN subnet	any	Blocage accès réseau interne
Pass	TCP/UDP	DMZ subnet	any	53	DNS sortant
Block	any	DMZ subnet	any	any	Blocage par défaut

5.4 Règles sur l'interface WAN

- Aller dans Firewall > Rules > WAN

Action	Protocol	Source	Destination	Port dest.	Description
Pass	TCP	any	WAN address	443	HTTPS entrant (portail VPN)
Pass	UDP	any	WAN address	1194	OpenVPN entrant

Action	Protocol	Source	Destination	Port dest.	Description
Pass	TCP	Any	10.0.10.1	80	http sur DMZ

6. Configuration du Portail Captif

Le portail captif intercepte les connexions HTTP/HTTPS des clients non authentifiés et les redirige vers une page de connexion. Il est particulièrement adapté aux réseaux Wi-Fi invités, aux salles de formation ou aux espaces publics.

6.1 Activation du portail captif

- Aller dans Services > Captive Portal
- Cliquer sur Add pour créer une nouvelle zone
- Renseigner un nom de zone (Fake_WIFI)
- Cliquer sur Save & Continue

6.2 Paramètres généraux de la zone

- Dans l'onglet Configuration de la zone, activer « Enable Captive Portal »
- Sélectionner l'interface concernée (ex : LAN ou PORTAIL)

Paramètre	Valeur recommandée	Description
Idle timeout	60 (minutes)	Déconnexion après inactivité
Hard timeout	1440 (minutes)	Session max : 24h
Pass-through credits per MAC	2	Reconnexions auto par adresse MAC
Concurrent user logins	Désactivé	Une session par utilisateur
Enable logout popup window	Activé	Fenêtre de déconnexion

6.3 Règles de filtrage du portail captif

Le portail captif ajoute automatiquement des règles dynamiques. Des règles statiques supplémentaires peuvent être configurées :

- Dans la zone portail, aller dans « Allowed IP Addresses » pour whitelister des IPs sans authentification
- Dans « Allowed Hostnames », whitelister des domaines (ex : mise à jour Windows)
- Dans Firewall > Rules >WIFI, bloquer l’accès au LAN et a la DMZ mais autorisé l’accès au WAN

7. Configuration VPN

pfSense supporte plusieurs protocoles VPN. Ce document couvre OpenVPN (accès distant)

7.1 OpenVPN – Accès distant utilisateurs

7.1.1 Création de l'Autorité de Certification (CA)

- Aller dans System > Cert. Manager > Authorities
- Cliquer sur Add

Champ	Valeur recommandée
Descriptive name	CA-TGHLAB-OPENVPN
Method	Create an internal Certificate Authority
Key length	2048
Digest Algorithm	SHA256
Lifetime	3650 jours (10 ans)
Common Name	CA-TGHLAB-OPENVPN
Country Code	FR
Organization	Ecoris

- Cliquer sur Save

7.1.2 Création du certificat serveur

- Aller dans System > Cert. Manager > Certificates
- Cliquer sur Add/Sign

Champ	Valeur
Method	Create an internal Certificate
Descriptive name	VPN-SSL-REMOTE-ACCESS
Certificate Authority	CA-TGHLAB-OPENVPN
Key length	2048 bits
Digest Algorithm	SHA256
Lifetime	3650 jours
Common Name	vpn.LAB.local
Certificate Type	Server Certificate

7.1.3 Configuration du serveur OpenVPN

- Aller dans VPN > OpenVPN > Servers
- Cliquer sur Add

Champ	Valeur recommandée
Server Mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Local Database
Protocol	UDP on IPv4 only
Device Mode	tun – Layer 3 Tunnel Mode
Interface	WAN
Local port	1194
TLS Configuration	Use a TLS Key (coché)
TLS Key Usage Mode	TLS Authentication
Peer Certificate Authority	CA-TGHLAB-OPENVPN
Server certificate	VPN-SSL-REMOTE-ACCESS
Encryption Algorithm	AES-256-CBC
Auth Digest Algorithm	SHA256
IPv4 Tunnel Network	172.16.40.0/24
IPv4 Local network(s)	192.168.4.0/24
Redirect IPv4 Gateway	Décoché (split tunneling)
Concurrent connections	100
Compression	Refuse any not-stub compression
DNS Server 1	192.168.4.1

- Cliquer sur Save

7.1.4 Règles de filtrage OpenVPN

- Aller dans Firewall > Rules > WAN et vérifier la règle UDP 1194 (créée automatiquement si coché)
- Aller dans Firewall > Rules > OpenVPN et ajouter :

Action	Protocol	Source	Destination	Description
Pass	ICMP	any	any	Ping autorisé
Pass	TCP/UDP	any	any	53 – DNS

7.1.5 Export des configurations clients

- Installer le package « openvpn-client-export » depuis System > Package Manager
- Aller dans VPN > OpenVPN > Client Export
- Sélectionner le serveur OpenVPN configuré
  - Choisir le format d'export Bundled Configuration

- Copier le dossier sur le partage réseau pour le rendre accessible.

7.2 Création d’utilisateurs locaux

- Aller dans System > User Manager
- Créer les accès de l’utilisateur avec un mot de passe
- Cocher l’option Click to create a user certificate

— Fin du document —