



Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

Environnement technologique pour la certification

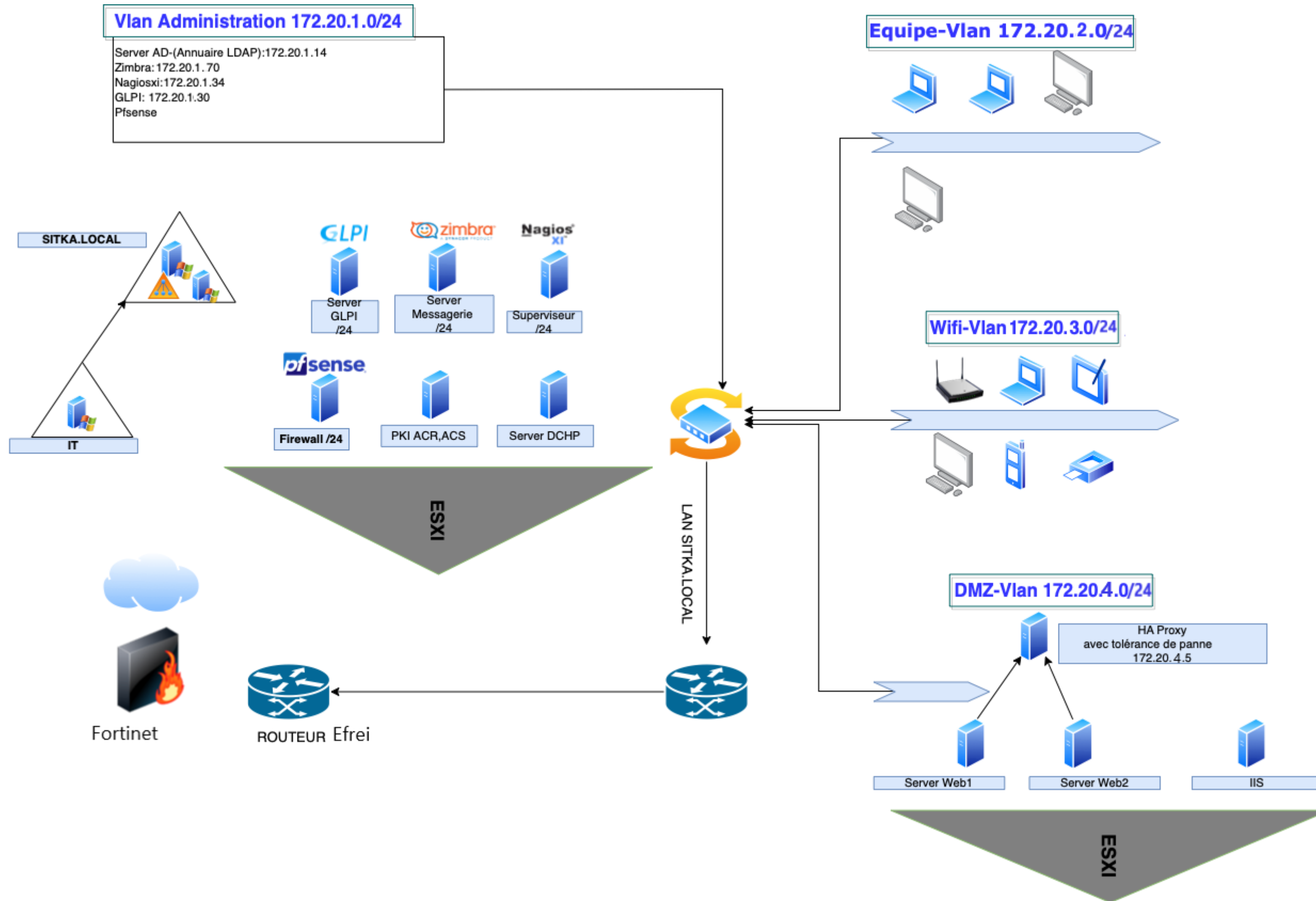
Plateforme

Environnement Technologique d’Apprentissage

Serveurs				
• Serveurs	• Utilisateurs	• Mot de Passe	• @IP	• Nom d'hôte
• ESXI 1/2	• root	• Bts2025@	• 172.20.1.250	• ESXI https://esxi.sitka.local/
• ACR (PKI)	• Administrateur	• Bts2025@	• 172.20.1.12	• ACR.sitka.local http://acr.sitka.local/certsrv
• ACS (PKI)	• Administrateur	• Bts2025@	• 172.20.1.13	• ACS.sitka.local http://acs.sitka.local/certsrv
• Ares (DNS secondaire)	• Administrateur	• Bts2025@	• 172.20.1.14	• ares.sitka.local
• Kratos1(DHCP-failover)	• Administrateur	• Bts2025@	• 172.20.1.5	• Kratos1.sitka.local
• Kratos2(DHCP-failover)	• Administrateur	• Bts2025@	• 172.20.1.6	• Kratos2.sitka.local
• W2022 core (serveur de fichier)	• Administrateur	• Bts2025@	• 172.20.1.8	• data.sitka.local
• hermes (CD1+DNS)	• Administrateur	• Bts2025@	• 172.20.1.2	• hermes.sitka.local
• neptune(CD2)	• Administrateur	• Bts2025@	• 172.20.1.3	• neptune.sitka.local
• neptune2CD3)	• Administrateur	• Bts2025@	• 172.20.1.4	• neptune2.sitka.local
• Zimbra (messagerie)	• Interface "admin"	• Bts2025@	• 172.20.4.2 :7071	• xmail.sitka.local https:// xmail.sitka.local :7071 • xmail.sitka.local https:// xmail.sitka.local :8443 • xmail.sitka.local
	• Interface "user"		• 172.20.4.2 :8443	
	• Console "root "		• 172.20.4.2	
• GLPI /fusion Inventory	• Console "root "	• Bts2025@	• 172.20.1.8	• glpi.sitka.local http://glpi.sitka.local
	• interface" glpi"			
• OCS	• Console "root " • interface" admin"	• Bts2025@	• 172.20.1.7	• ocs.sitka.local http://ocs.sitka.local
• NAGIOSXI (supervision)	• root • Interface "nagiosadmin"	• Bts2025@	• 172.20.1.9	• nagiosxi.sitka.local http://nagiosxi.sitka.local
• haproxy	• root	• 1	• 172.20.4.5	• Haproxy http://haproxy.sitka.local
• Ha1			• 172.20.4.3	• HA1 http://ha1.sitka.local
• Ha2			• 172.20.4.4	• HA http://ha2.sitka.local
• Heimdall(pfsense)	• Admin		• 172.20.1.1 • 172.20.2.1 • 172.20.3.1 • 172.20.4.1	• heimdall.sitka.local https:// heimdall.sitka.local

Adressage			
• Services	• VLAN	• Réseaux/MSR	• Affectation des Ports
• Administration	• 10	• 172.20.1.0/24	• [0/1 ->0/ 6]
• Equipes	• 20	• 172.20.2.0/24	• [0/7 -> 0/12]
• Wifi	• 30	• 172.20.3.0/24	• [0/13 -> 0/14]
• DMZ	• 40	• 172.20.4.0/24	• [0/16 -> 0/17]
Adresse interfaces Vlan 10	172.20.1.5		

Schémas infrastructure



Cahier des Charges

<div>BTS SERVICES INFORMATIQUES AUX ORGANISATIONS</div> <div>Épreuve E5 - Administration des systèmes et des réseaux (option SISR)</div> <div>ANNEXE 8-A : Outil d’aide à l’appréciation de l’environnement technologique mobilisé par la personne candidate</div>	SESSION 2023
--	--------------

CONTRÔLE DE L’ENVIRONNEMENT TECHNOLOGIQUE

En référence à l’annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification ¹	Ecole <div></div>	SISR
-----------------------------	--	------

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)	Remarques de la commission d’interrogation
Un service d’authentification	Remote Authentication Dial-In User Service (RADIUS), Service d'annuaire Active Directory (Serveur 2022)	
Un SGBD	MySQL, SQL-Server, Maria DB	
Un accès sécurisé à internet	NAT, ACL, Proxy, Pfsense	
Un environnement de travail collaboratif	Zimbra, DropBox, Google docs, One drive	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (<i>open source</i>)	VMWARE Sphère 8.0 pour la partie virtualisation Environnement Microsoft : Windows Server 2022 R2, Windows 10 Environnement Linux : Ubuntu, Debian	

ANNEXE 8-A (suite) : Modèle d’attestation de respect de l’annexe II.E – « Environnement technologique pour la certification » du référentiel

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)	Remarques de la commission d’interrogation
Une solution de sauvegarde	Sauvegarde intégrée à Windows Serveur 2022 R2 NAS, onCloud	
Des ressources dont l'accès est sécurisé et soumis à habilitation	SSH, Service d'annuaire Active Directory (Serveur 2022)	
Deux types de terminaux dont un mobile (type <i>smartphone</i> ou encore tablette)	Smartphone – Tablette – PC portable	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)	Remarques de la commission d’interrogation
Gestion des incidents	GLPI, GPARC	
Détection et prévention des intrusions	Wazuh, IDS: Intrusion Detection System -- NIDS (Network Based Intrusion Detection System): Snort,	
Chiffrement	SSH, ssl, https...	
Analyse de trafic	Wireshark, Moniteur réseau Windows...	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 8-A (suite) : Modèle d’attestation de respect de l’annexe II.E « Environnement technologique pour la certification » du référentiel

2. Éléments spécifiques à l’option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l’annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

2.1 L'environnement technologique supportant le système d’information de l'organisation cliente comporte au moins :

Éléments	Description de l’implantation dans le centre d’examen (nom du service ou de l’outil et caractéristiques techniques)	Remarques de la commission d’interrogation
Un réseau comportant plusieurs périmètres de sécurité	3 zones : - Réseau local LAN avec une gestion de VLAN (switch CISCO 2960) - Zone démilitarisée (DMZ) - Internet (en passant par le réseau local de l’école ou la Freebox) Pare-feu (distribution Pfsense), Routeurs filtrants Cisco 2921	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	On répond à un besoin destiné à améliorer le service rendu à l’utilisateur final : authentification, accès Wifi, DHCP, DNS, Active directory, Haproxy	
Un logiciel d'analyse de trames	Wireshark, Moniteur réseau Windows...	
Un logiciel de gestion des configurations	OCS, GLPI/Fusioninventory, GPO, GPARC	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Administration des serveurs avec : - Bureau à distance RDP pour Microsoft, Teamviewer - WinSCP - Putty (accès SSH ou Telnet)	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Nagios XI	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Réseau privé – DMZ – Internet Pare-feu (Pfsense), Routeurs filtrants (ACL) Cisco 2921	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	Haute disponibilité, identification des risques, plans de reprise de plans de continuité informatique, (QoS, DNS secondaire, Failover, Heartbeat, HSRP, Spanning-stree)	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Haute disponibilité de service (Heartbeat) ou d'éléments d'interconnexion (Routeur : HSRP, VRRP, Commutateur et Etherchannel, Spanning-stree)	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAProxy, GLBP (Gateway Load Balancing Protocol)	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	VPN site à site	
Une solution permettant le déploiement des solutions techniques d'accès	Service de déploiement : AD/GPO, FOG, OCS	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i>	Language de scripting en Shell, PowerShell	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	HIDS: Wazuh, IDS: Intrusion Detection System -- NIDS (Network Based Intrusion Detection System): Snort, Bro,	

Timéo le goat