

## Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI (DAT-NT-006)

Le présent rapport a pour but de définir la politique de filtrage réseau du nouveau Système d'Information de XANADU. Cette politique s'appuie sur une approche de sécurité positive : on n'autorise que ce qui est réellement nécessaire, tout le reste est bloqué. Elle se fonde également sur la segmentation prévue par le plan d'adressage VLAN et respecte l'organisation des règles recommandée par l'ANSSI, telle qu'elle apparaît dans la note technique DAT-NT-006.

La mise en place de ce filtrage n'est pas un simple choix technique. La récente menace de rançongiciel qui a visé XANADU oblige à renforcer l'ensemble du SI et à appliquer une défense en profondeur. L'objectif est de garantir la confidentialité, l'intégrité et la disponibilité des données, tout en assurant une traçabilité claire des flux. Dans ce contexte, le filtrage réseau constitue la première barrière contre les tentatives d'intrusion et les mouvements latéraux.

### I. Justification architecturale et modèle de contrôle

Mettre en place une politique de filtrage efficace implique d'avoir une architecture réseau adaptée. Il faut pouvoir séparer clairement les fonctions critiques, comme l'administration ou les services essentiels, des zones utilisateurs. La segmentation joue ici un rôle central : elle permet de limiter l'impact d'un incident de sécurité et de respecter les délais de retour à la normale (RTO) fixés pour les services critiques, soit moins de 4 heures.

#### I.1 Pourquoi une segmentation et un double Pare-feu sont nécessaires

Pour garantir une défense en profondeur efficace, il est proposé d'adopter une architecture avec deux niveaux de pare-feu, de façon à répartir les risques et cloisonner les flux.

Pare-feu périphérique (FW Périphérique) : il gère les communications avec l'extérieur (WAN, Internet, Office 365) et peut aussi servir de passerelle sécurisée pour les télétravailleurs via VPN SSL. Il est principalement chargé de protéger le SI contre les menaces venant de l'extérieur.

Pare-feu interne (FW Interne / Firewall de segmentation) : c'est lui qui contrôle le routage et le filtrage entre tous les réseaux internes (inter-VLAN). C'est sur ce pare-feu que la politique ANSSI DAT-NT-006 est appliquée en priorité, puisqu'il supervise les flux métiers et d'administration critiques.

La segmentation VLAN permet d'isoler les services sensibles (VLAN 20) et le plan de contrôle (VLAN 10) des zones de travail des utilisateurs (VLAN 30) et des sites distants (VLAN 40), qui représentent des surfaces d'attaque plus importantes.

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

## I.2 Définition des zones de sécurité et plan d'adressage

Le plan d'adressage est conçu pour refléter les niveaux de confiance et les rôles de chaque zone. Séparer physiquement ou via VLAN les plans de contrôle et de données est une pratique essentielle pour protéger l'intégrité du SI.

Placer le Contrôleur de Domaine (DC) et le stockage des sauvegardes dans le VLAN 10 (NET\_MGMT) est une décision clé. En isolant le DC, qui détient les clés de l'annuaire et des GPO, tout accès aux services d'authentification (Kerberos, LDAP) depuis d'autres VLANs doit passer par le FW interne. Cela permet de journaliser ces accès et de mettre en place des contrôles stricts, renforçant l'intégrité et la traçabilité des opérations sur les éléments les plus critiques de l'infrastructure.

**Tableau 1 : Plan d'adressage et zones de sécurité XANADU (objets réseau)**

VLAN ID	Nom de la zone ou Objet réseau	Plage IP proposée	Équipements clés	Niveau de confiance
10	NET_MGMT	176.16.10.0/24	DC/DNS, Serveur Syslog, Stockage Sauvegarde	Très haut
20	NET_SRV	176.16.20.0/24	SVR ERP (Présentation/A pp/DB), NAS/Fichiers, Imprimantes	Haut
30	NET_USR	176.16.30.0/24	Postes clients Atlantis	Moyen
40	NET_LAB	176.16.40.0/24	Postes clients Springfield, Serveurs Linux Lab	Moyen
50	NET_EXPOSED	176.16.50.0/24	VPN Endpoint, Reverse Proxy (Futures évolutions)	Faible (DMZ )

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

### I.3. Convention de Nommage et Définition des Services

L'ANSSI souligne l'importance de définir clairement chaque objet afin de rendre la politique de filtrage plus lisible et plus facile à maintenir. Pour cela, une convention de nommage fonctionnelle sera appliquée :

- Réseaux : NET\_VLAN\_ID
- H\_Role\_Nom
- SVC\_Protocole\_Fonction

**Tableau 2 : Définition des Objets Services Critiques (Ports et Protocoles)**

Objet Service	Port(s)	Protocole	Description
SVC_AD_CORE	TCP/UDP 53, 88, 389, 445, 636, 3268, 3269, 49152-65535 (RPC)	TCP/UDP	DNS, Kerberos, LDAP, SMB, Global Catalog, RPC
SVC_ERP_PRES	TCP 443	TCP	Accès sécurisé (HTTPS) à l'interface de présentation ERP
SVC_ERP_APP	TCP 8069	TCP	Communication Serveur Présentation vers Application Odoo (Port par défaut)
SVC_ERP_DB	TCP 5432	TCP	Communication Serveur Application vers PostgreSQL
SVC_SMB	TCP 445	TCP	Partage de fichiers (CIFS/SMB)
SVC_MGMT_SSH	TCP 22	TCP	Administration sécurisée (Linux/Windows)
SVC_SYSLOG	UDP 514	UDP	Envoi de journaux centralisé
SVC_NTP	UDP 123	UDP	Synchronisation horaire
SVC_BACKUP	TCP 9876	TCP	Flux PUSH de l'agent de sauvegarde

# Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI (DAT-NT-006)

## II. Organisation de la politique selon le DAT-NT-006

La politique de filtrage du FW Interne suit le modèle en six sections de l'ANSSI. Les trois premières sont essentielles pour sécuriser le pare-feu lui-même.

### II.1. Section 1 : Flux vers le pare-feu (R1)

Cette section limite l'accès au pare-feu aux seuls serveurs et postes d'administration dans NET\_MGMT (VLAN 10), via SSH ou HTTPS. Tous les accès sont journalisés pour garantir une traçabilité complète.

### II.2. Section 2 : Flux émis par le pare-feu (R2)

Le pare-feu doit :

- envoyer ses journaux vers le serveur Syslog/SIEM (NET\_MGMT, UDP 514)
- se synchroniser avec le DC pour des horodatages précis

### II.3. Section 3 : Protection du pare-feu (R3)

Tout trafic non autorisé par les sections 1 et 2 est bloqué (Drop) et journalisé. Cela protège le plan de contrôle même en cas d'erreur dans les règles suivantes.

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

Tableau 3 : Politique de filtrage - Sections 1, 2 et 3

Ordre	Section	Source	Destinati on	Protocol e/Servic e	Action	Journalis ation	Justificat ion
1	S1	NET_MG MT	Interface FW	SVC_MG MT_SSH (22), 443	Autoriser	Oui	Administ ration et gestion sécurisé e du FW depuis la zone de Manage ment.(R1 )
2	S1	NET_MG MT	Interface FW	SNMP (161/UD P)	Autoriser	Non	Supervisi on par le serveur central. (R1)
3	S2	Interface FW	NET_MG MT	SVC_SYS LOG (514/UD P)	Autoriser	Non	Envoi des journaux du FW vers le serveur centralis é. (R2)
4	S2	Interface FW	NET_MG MT	SVC_NT P (123/UD P)	Autoriser	Non	Synchron isation horaire du FW pour l'intégrité des logs. (R2)
5	S3	ANY	Interface FW	ANY	Interdire( DROP)	Oui	Règle de protectio n absolue : bloque tout trafic non-légiti

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

							me ciblant le FW. (R3)
--	--	--	--	--	--	--	------------------------

### III. Mise en Œuvre des Règles Métier (Section 4)

La Section 4 concerne les flux métiers (R4) , organisés par type : Infrastructure, Application, Fichiers, MCO. Les règles définissent les sources, destinations et services autorisés.

#### III.1. Flux d'infrastructure critique

L'Active Directory et les services associés sont centralisés sur H\_DC\_01 (VLAN 10). Les clients (NET\_USR, NET\_LAB) et serveurs (NET\_SRV) doivent pouvoir accéder au DC pour DNS, Kerberos, LDAP, LDAPS, GPO/SYSVOL et RPC. Le passage par le FW interne garantit la traçabilité et protège le DC même si un VLAN utilisateur est compromis.

#### III.2. Flux de l'ERP 3-Tiers (Odoo/PostgreSQL)

Les serveurs ERP sont dans NET\_SRV (VLAN 20). Les flux autorisés :

- Client vers présentation (Tiers 1) : HTTPS (443)
- Présentation vers application (Tiers 2) : TCP 8069
- Application vers base de données (Tiers 3) : TCP 5432

Pour limiter les risques intra-VLAN, chaque serveur doit avoir un pare-feu hôte configuré, autorisant uniquement le trafic nécessaire entre les tiers.

#### III.3. Flux de partage de fichiers (NAS/SMB)

H\_NAS\_01 (VLAN 20) est accessible :

- NET\_USR : TCP 445 (SMB)
- Direction/Juridique : accès étendu selon les besoins métiers

Le contrôle fin des droits (lecture seule ou lecture/écriture) est géré par SMB/NTFS et Active Directory, le pare-feu se chargeant de la segmentation réseau.

#### III.4. Flux inter-sites (VLAN 40)

Le site distant (NET\_LAB) peut :

- accéder à H\_ERP\_PRES via HTTPS (lecture seule)
- accéder à H\_NAS\_01 via SMB (lecture seule)

Le Bureau d'étude peut accéder aux serveurs du laboratoire via SSH (22) pour gestion et transfert de données.

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

### III.5. Flux de sauvegarde

Le stockage de sauvegarde est isolé dans NET\_MGMT (VLAN 10). Seuls les serveurs de production et le DC peuvent pousser des données vers le stockage. Tout trafic inverse est bloqué, assurant qu'une compromission du stockage ne puisse pas atteindre les serveurs de production.

### III.6. Synthèse des Règles Métiers (Section 4)

Tableau 4 : Politique de Filtrage - Flux Métiers Critiques

Ordre	Priorité	Source	Destination	Protocole/Service	Action	Journalisation	Description (Flux Métier & Sécurité)
100	INFRA	NET_USR (30), NET_SRV (20), NET_LAB (40)	H_DC_01 (10)	SVC_AD_CORE (53, 88, 389, 445, etc.)	Autoriser	oui	Authentification et services d'annuaire (Flux critique vers le plan de contrôle).
105	INFRA	NET_USR (30), NET_SRV (20), NET_LAB (40)	H_DC_01 (10)	DHCP (67/68/UDP)	Autoriser	Non	Requêtes DHCP vers le contrôleur de domaine/serveur DHCP.
110	MCO	ANY (Tous)	H_DC_01 (10)	SVC_NTP (123/UDP)	Autoriser	Non	Synchronisation horaire globale du SI (via DC).
115	ERP	NET_USR (30), NET_LAB (40)	H_ERP_PROD (20)	HTTPS (443/TCP)	Autoriser	Non	Accès utilisateur au frontend ERP (Sécurisation SSL/TLS).
120	ERP	H_ERP_PROD (20)	H_ERP_APP (20)	SVC_ERP_APP (8069/TCP)	Autoriser	Oui	Tiers 1 vers Tiers 2 ERP (Journalisation pour traçabilité applicative).
125	ERP	H_ERP_APP (20)	H_ERP_DB (20)	SVC_ERP_DB (5432/TCP)	Autoriser	Oui	Tiers 2 vers Tiers 3 (Base de données). Flux

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

				CP)			interne critique.
130	FICHIER	NET_USR (30)	H_NAS_01 (20)	SVC_SMB (445/TCP)	Autoriser	Non	Accès bureautique R/W aux partages centralisés.
135	FICHIER	NET_LAB (40)	H_NAS_01 (20)	SVC_SMB (445/TCP)	Autoriser	Oui	Accès (Logique R/O) aux données du Bureau d'étude.
140	INTER-SITE	NET_USR (30) (BE)	NET_LAB (40) (SVR LINUX)	SVC_MGMT_SSH (22/TCP)	Autoriser	Oui	Accès R/W du Bureau d'étude aux serveurs du Laboratoire.
145	IMPRIMANTE	NET_USR (30)	H_COPIEUR (20)	TCP 9100, 515, 631	Autoriser	Non	Flux d'impression.
150	SAUV	NET_SRV (20), H_DC_01 (10)	NET_MGMT (10) (Stockage)	SVC_BACKUP (9876/TCP)	Autoriser	Oui	Flux de sauvegarde unidirectionnel PUSH vers le stockage de sécurité.
155	SAUV	NET_MGMT (10)	NET_SRV (20), H_DC_01 (10)	ANY	Interdire (Drop)	Oui	Sécurité critique : Empêche le stockage de sauvegarde de compromettre les serveurs de production.

#### IV. Politique de filtrage globale (Sections 5 et 6)

##### IV.1. Section 5 : Règle R5

Cette section, recommandée par l'ANSSI, vise à réduire le bruit dans les journaux du pare-feu.

Le trafic NetBIOS et autres diffusions locales inutiles entre VLANs est bloqué. Cela empêche la surcharge des logs et limite les informations non pertinentes envoyées au serveur Syslog.

Exemple de règle R5 (Tableau 5) : bloquer tout trafic broadcast ou protocole hérité non nécessaire à l'exploitation du SI.

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

Ordre	Section	Source	Destination	Protocole/Service	Action	Journalisation	Description
900	S5	ANY (Sauf 10)	ANY	NetBIOS (UDP 137, 138), LLMNR	Interdire (Drop)	Non	Suppression du trafic de broadcast inter-VLANs pour alléger les journaux.

#### IV.2. Section 6 : Règle d'interdiction finale (R6)

La R6 applique le principe de sécurité positive : tout ce qui n'est pas explicitement autorisé est interdit. Elle est toujours en dernière position et utilise l'action Drop pour tout trafic ANY. La journalisation est activée pour tracer toutes les tentatives d'accès non prévues, qu'elles soient accidentelles ou malveillantes.

#### V. Politique de filtrage du pare-feu périphérique

Le FW Périphérique sépare Internet (WAN) du SI interne. Il bloque par défaut les flux entrants et contrôle strictement les flux sortants.

##### V.1. Flux sortants

- Office 365 / navigation : NET\_USR, NET\_LAB, NET\_SRV vers TCP 443 (HTTPS). Le HTTP (80) est bloqué pour garantir le chiffrement.
- Mises à jour critiques : NET\_SRV et NET\_MGMT peuvent accéder uniquement aux IP des services de mise à jour Microsoft et Linux.

##### V.2. Flux entrants et télétravail

Le trafic WAN vers SI est interdit par défaut (Drop) avec journalisation. Seuls les flux en réponse à des requêtes internes sont autorisés. Un accès VPN sécurisé est prévu pour le télétravail afin de protéger l'intégrité et disponibilité des données.

Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI  
(DAT-NT-006)

Tableau 6 : Politique de filtrage - Flux FW Périphérique

Ordre	Section	Source	Destination	Protocole/Service	Action	Journalisation	Description (Flux Périphérique)
1	S4 Sortant	NET_USR (30), NET_LAB (40), NET_SRV	WAN (Internet)	SVC_HTTPS (443/TCP)	Autoriser	Non	Accès sécurisé à O365 et navigation web.
2	S4 Sortant	NET_MGMT (10), NET_SRV (20)	WAN (Updates /Microsoft/NTP)	SVC_HTTPS (443/TCP), SVC_NTP (123/UDP)	Autoriser	Oui	Mises à jour des systèmes d'exploitation et synchronisation horaire externe (pour les serveurs).
3	S4 Entrant	WAN (Internet)	H_VPN_ENDPOINT (50)	TCP 443 ou 1194	Autoriser	Oui	Accès VPN sécurisé (si le service est déployé en DMZ).
4	S4 Entrant	WAN (Internet)	ANY(Autres VLANs)	ANY	Interdire (DROP)	Oui	Blocage par défaut de tout trafic entrant non sollicité.
999	S6	ANY	ANY	ANY	Interdire (DROP)	Oui	Règle d'interdiction finale du FW Périphérique (modèle positif).

## Politique de Filtrage de Réseau de XANADU selon le Modèle d'Organisation ANSSI (DAT-NT-006)

### VI. Conclusions et recommandations opérationnelles

La politique de filtrage, alignée sur les recommandations de l'ANSSI, assure un niveau de sécurité élevé pour le SI de XANADU, basé sur le moindre privilège et le cloisonnement strict.

#### VI.1. Sécurité multi-couches

- Micro-segmentation ERP : Les pare-feux hôtes sur H\_ERP\_APP et H\_ERP\_DB limitent la propagation latérale des menaces intra-VLAN.
- Contrôle d'accès applicatif : Les droits lecture seule pour le Laboratoire sur les dossiers partagés sont gérés via SMB/NTFS et Active Directory. Le pare-feu ne fait que segmenter le trafic.
- Sauvegarde unidirectionnelle : Les flux initiés par le stockage (NET\_MGMT) vers la production (NET\_SRV) sont interdits, préservant l'intégrité des données face aux rançongiciels

#### VI.2. Gestion et pérennité de la politique

- Journalisation et traçabilité : Tous les flux critiques et règles importantes (S1 à S6) sont journalisés et centralisés dans NET\_MGMT (VLAN 10).
- Maintenance régulière : Revue de la politique au moins une fois par an pour supprimer les règles obsolètes et adapter le filtrage aux besoins métier.
- Désactivation des flux implicites : Tous les flux légitimes (DNS, NTP, etc.) doivent être définis manuellement dans les sections appropriées pour éviter tout accès par défaut.