Power Week 2025

#pw2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

20 novembre 9:45 - 10:45

Jean-Sébastien GUINAUDEAU
HELIAQ SOLUTIONS
jean-sebastien.guinaudeau@heliaq.fr

IBM

common FRANCE

Power Week

18 -19 - 20 novembre 2025

IBM

common FRANCE

heliaq Solutions IBM

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

- Nous parlerons « réseau », et des manières/outils permettant de déterminer depuis l'IBM i les périphériques qui communiquent avec ce dernier.

- Nous regarderons dans le détail les informations que permettent d'obtenir les outils natifs du système, comme le NETSTAT, le TRCCNN, la mise en place de filtre sur les interfaces Ethernet, et comment aller chercher dans les informations collectées : analyse PCAP, requêtes SQL dans le QHST, dans le Journal d'Audit, etc.

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

- Déterminer précisément le périmètre réseau d'une partition IBM i est souvent une étape sous-estimée lors d'une opération de « Move to Cloud », mais pourtant primordiale pour assurer la viabilité d'un tel projet.

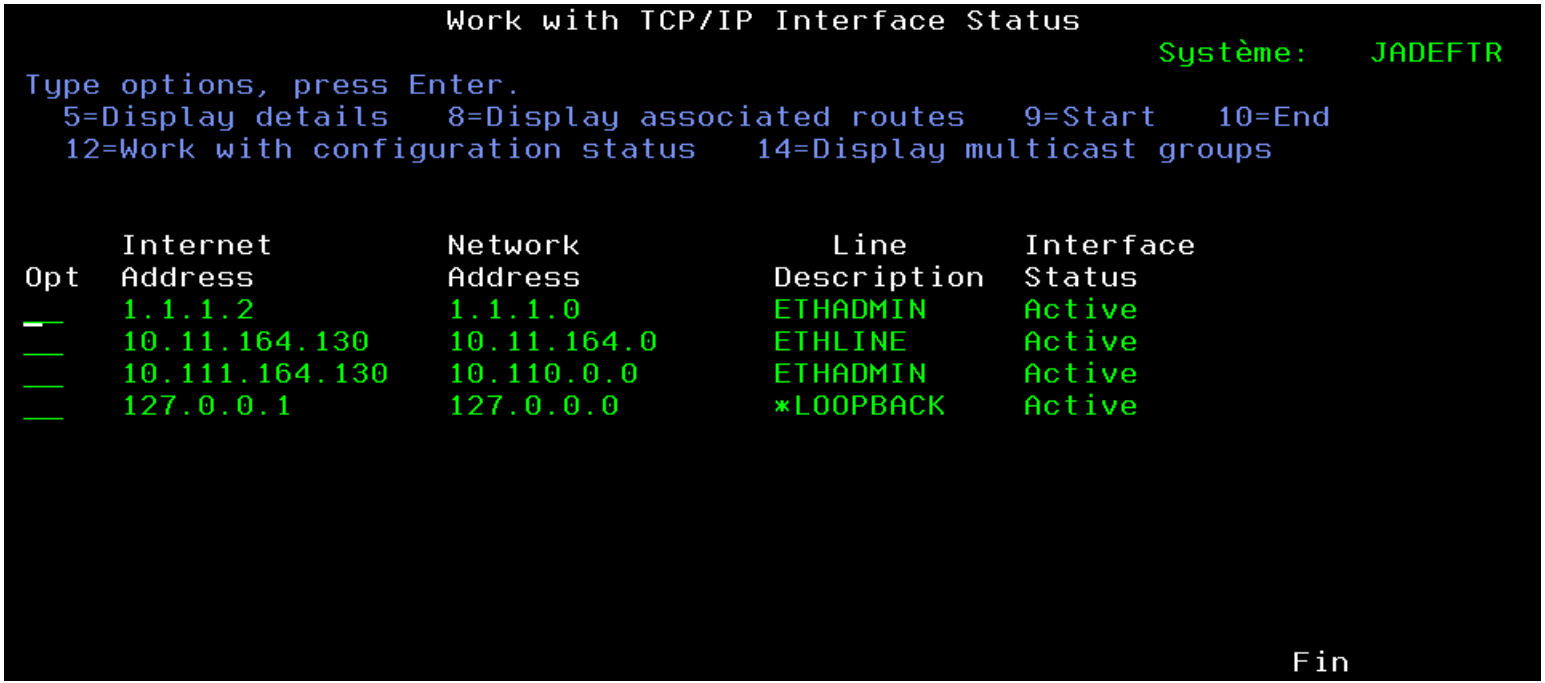
- Mais cette phase peut également être utilisée dans le cas d'un audit périmétrique, d'un projet de sécurisation de sa partition, etc.

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

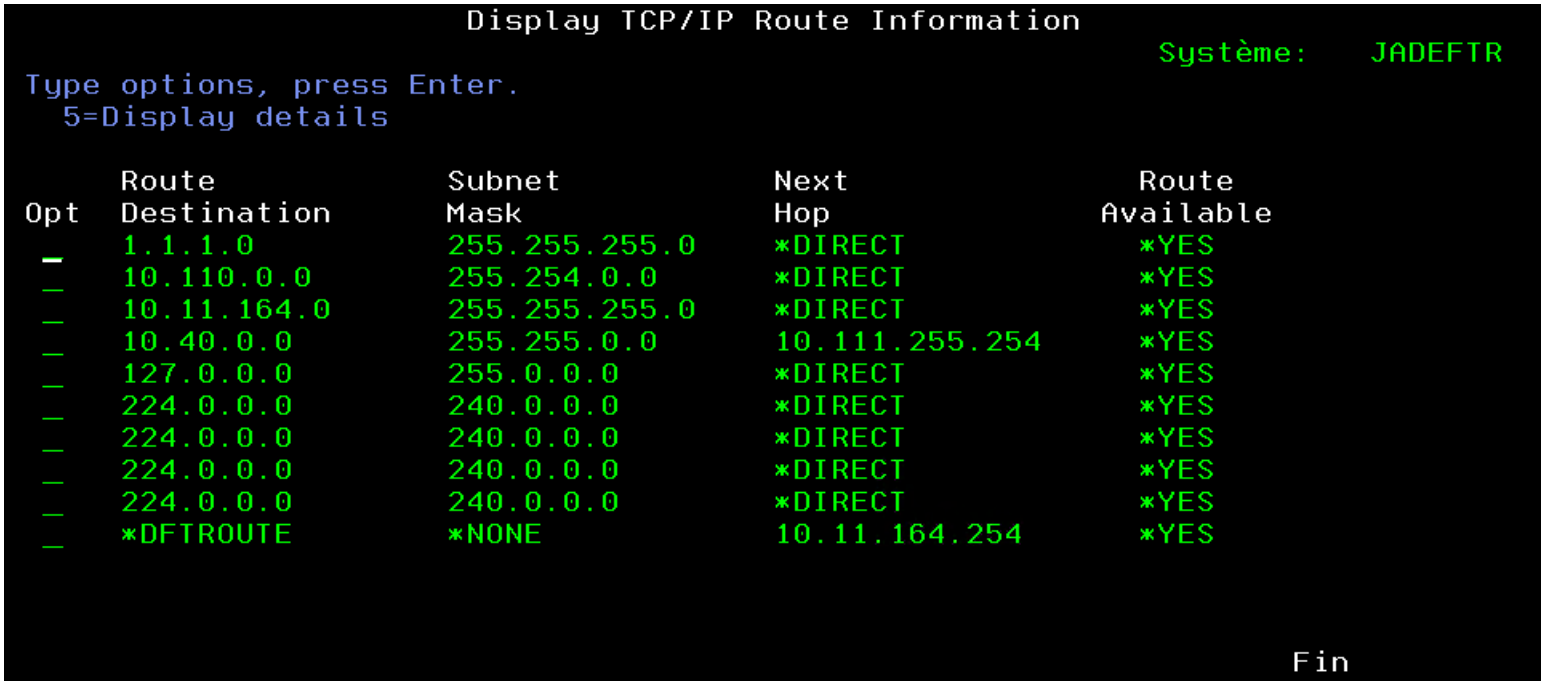
Pour se donner une idée de la configuration réseau IP en place, il est possible de lister les interfaces déclarées sur le système via la commande native NETSTAT, avec le paramètre *IFC.

On pourra compléter ces informations avec le paramètre *RTE pour connaître les routes définies.

NETSTAT *IFC (ou CFGTCP, option 1)



NETSTAT *RTE (ou CFGTCP, option 2)



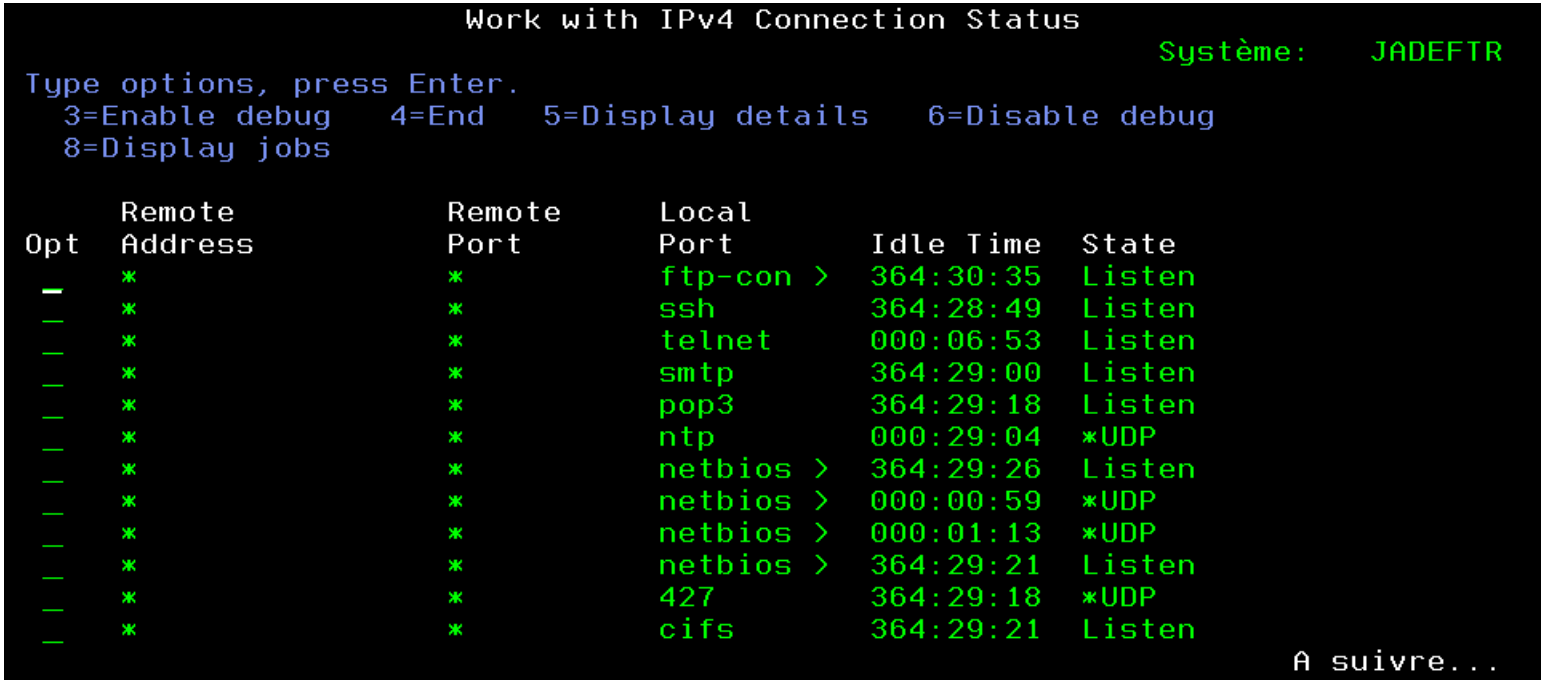
S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

On peut commencer par regarder les ports ouverts sur le système via la commande NETSTAT (utiliser le paramètre *CNN).

La commande WRKSRVTBLE donnera les noms des services associés aux numéros de ports.

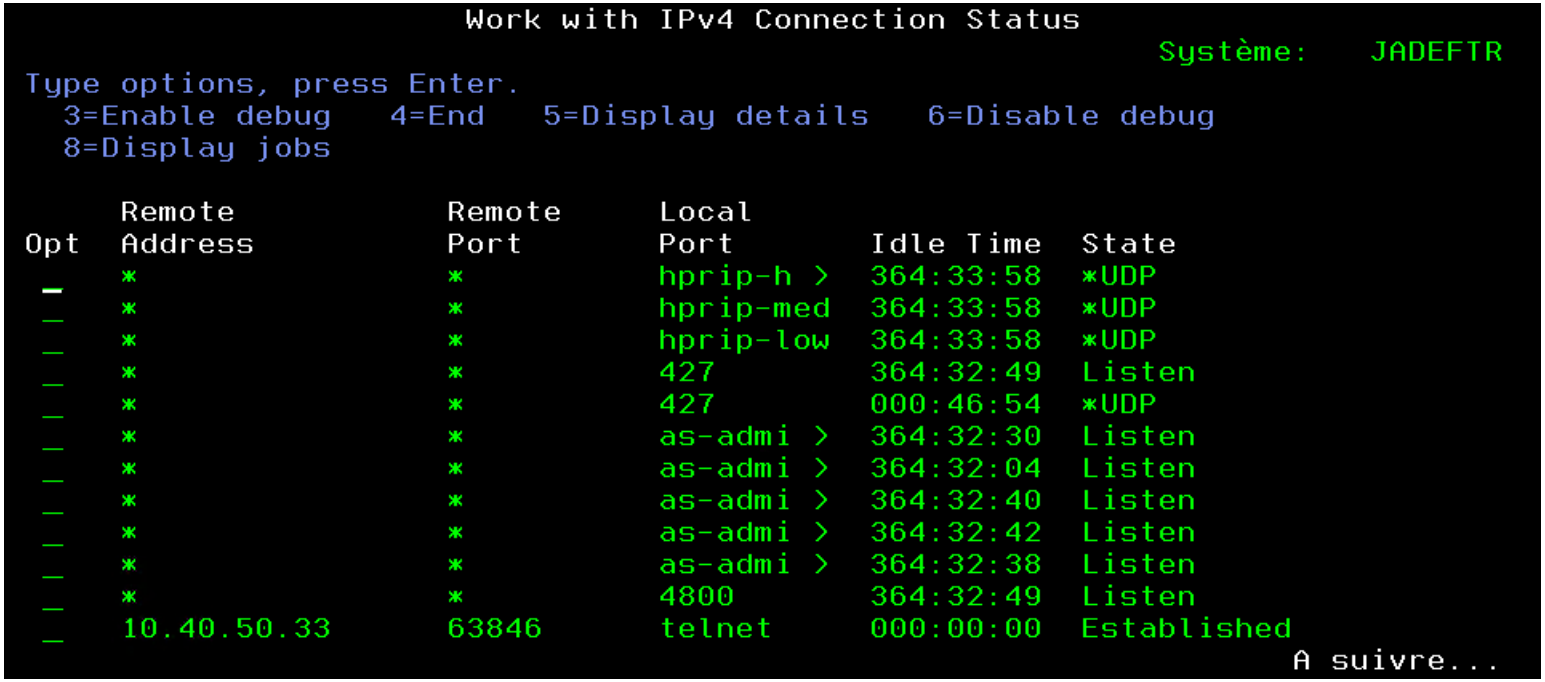
NETSTAT *CNN

En début de liste, les * indiquent les services démarrés et en attentes de connexion.



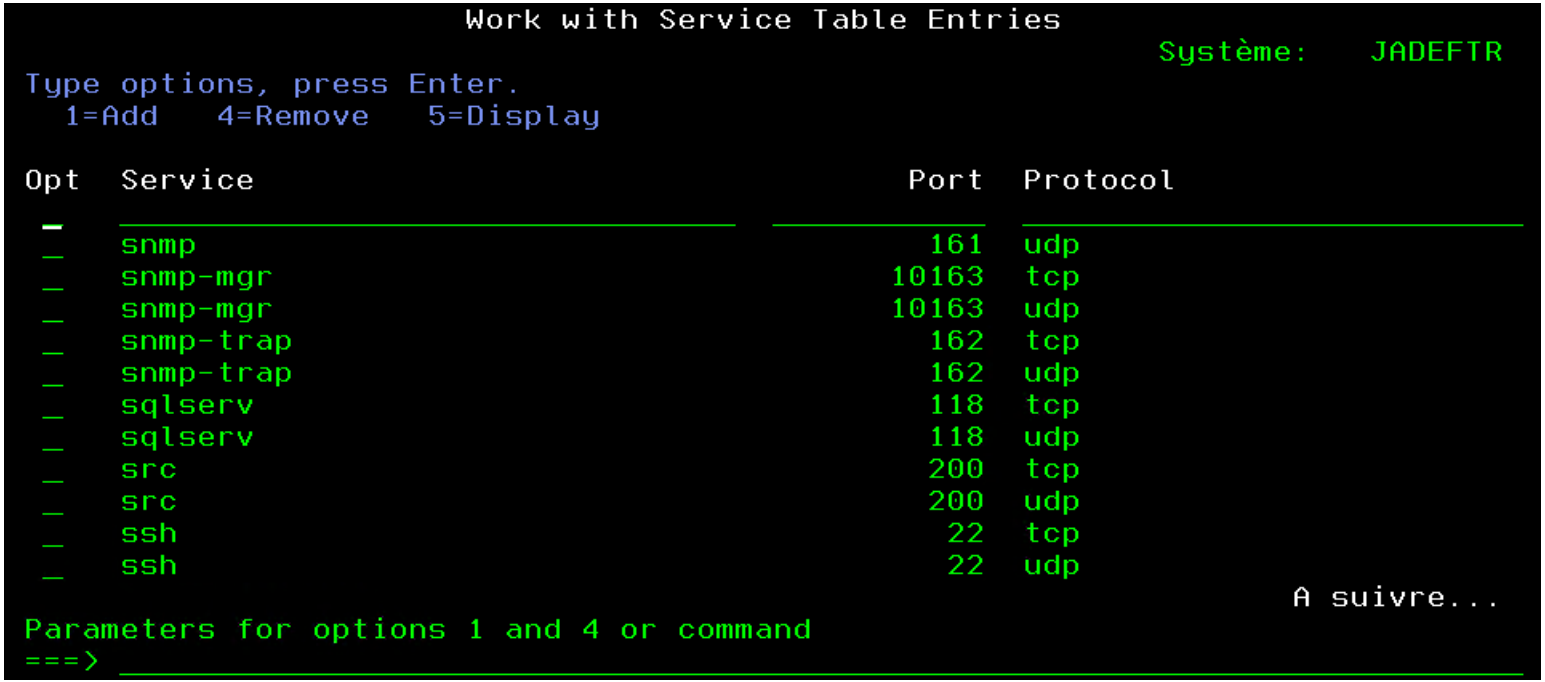
NETSTAT *CNN

En fin de liste, les adresses IP et numéros de ports indiquent les services pour lesquelles des connexions sont actives.



WRKSRVTBLE (ou CFGTCP, option 21, puis option 1)

La table des services fait la relation entre un nom de service, un numéro de port et un type de protocole. Les fameux « well-known ports »…



NETSTAT *CNN – Via les « SQL Services »

[IBM i Services (SQL)]

```
SELECT DISTINCT REMOTE_ADDRESS, REMOTE_PORT, REMOTE_PORT_NAME, LOCAL_PORT, LOCAL_PORT_NAME, CONNECTION_TYPE
    FROM QSYS2.NETSTAT_JOB_INFO
    WHERE REMOTE_ADDRESS = '0.0.0.0'
    ORDER BY LOCAL_PORT;
```

REMOTE_ADDRESS	REMOTE_PORT	REMOTE_PORT_NAME	LOCAL_PORT	LOCAL_PORT_NAME	CONNECTION_TYPE
0.0.0.0	0	-	21	ftp-control	IPV4
0.0.0.0	0	-	22	ssh	IPV4
0.0.0.0	0	-	23	telnet	IPV4
0.0.0.0	0	-	25	smtp	IPV4
0.0.0.0	0	-	110	pop3	IPV4
0.0.0.0	0	-	137	netbios-ns	IPV4
0.0.0.0	0	-	139	netbios-ssn	IPV4
0.0.0.0	0	-	427	-	IPV4

```
SELECT DISTINCT REMOTE_ADDRESS, REMOTE_PORT, REMOTE_PORT_NAME, LOCAL_PORT, LOCAL_PORT_NAME, CONNECTION_TYPE
    FROM QSYS2.NETSTAT_JOB_INFO
    WHERE REMOTE_PORT <> '0'
    ORDER BY LOCAL_PORT;
```

REMOTE_ADDRESS	REMOTE_PORT	REMOTE_PORT_NAME	LOCAL_PORT	LOCAL_PORT_NAME	CONNECTION_TYPE
10.40.50.33	54 662	-	23	telnet	IPV4
10.40.50.33	54 614	-	8 471	as-database	IPV4
127.0.0.1	36 367	-	8 473	as-file	IPV4
10.40.50.33	54 615	-	8 475	as-rmtcmd	IPV4
127.0.0.1	28 423	-	8 475	as-rmtcmd	IPV4
127.0.0.1	8 475	as-rmtcmd	28 423	-	IPV4
127.0.0.1	8 473	as-file	36 367	-	IPV4

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Il y a la possibilité d'utiliser un outil natif appelé TRCCNN (disponible à partir de la 7.2), permettant l'enregistrement des flux IP traités par le système.

Les traces sont enregistrées localement, et il est ensuite possible de les exporter au format PCAP.

TRCCNN

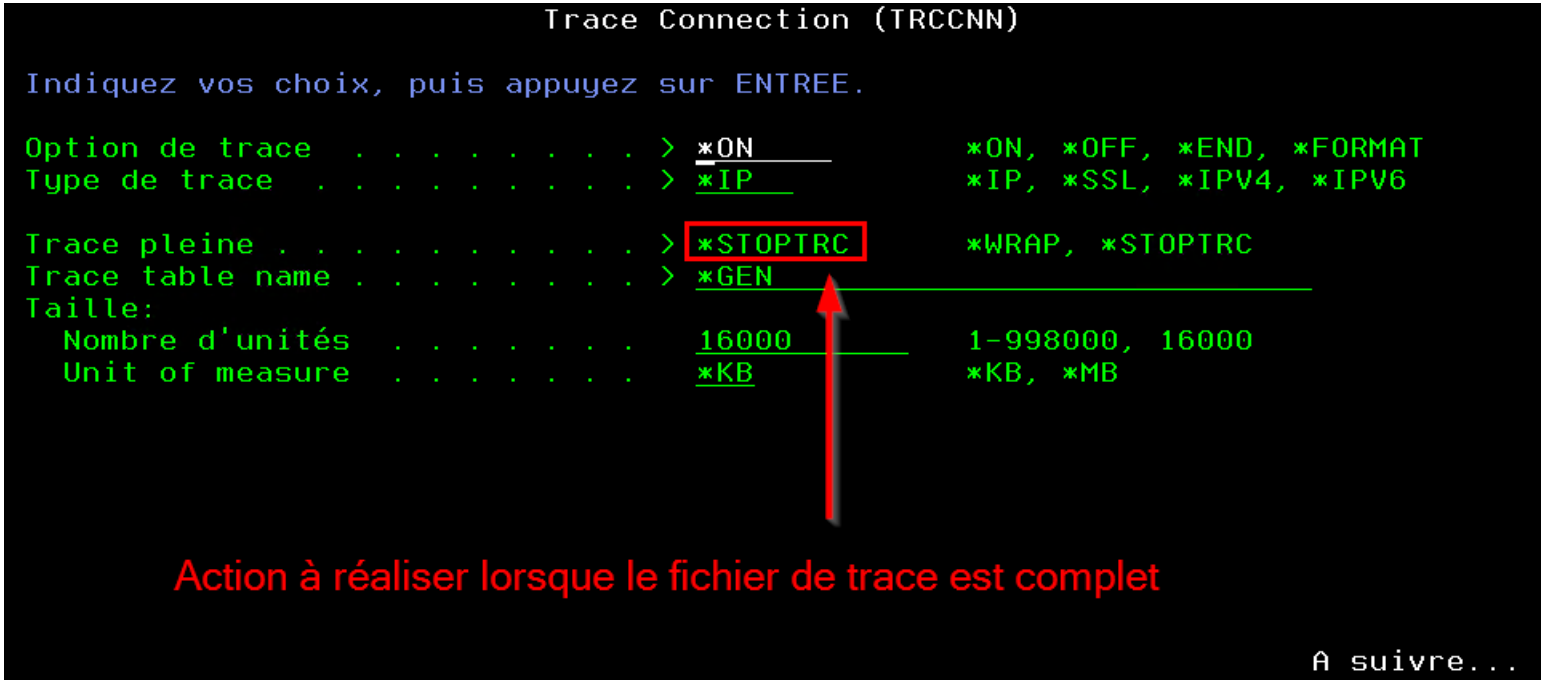
Liens vers les documentations officielles :

How To Use TRCCNN : https://www.ibm.com/support/pages/how-use-trccnn

Trace Connection (TRCCNN) : https://www.ibm.com/docs/en/i/7.3.0?topic=ssw_ibm_i_73/cl/trccnn.htm

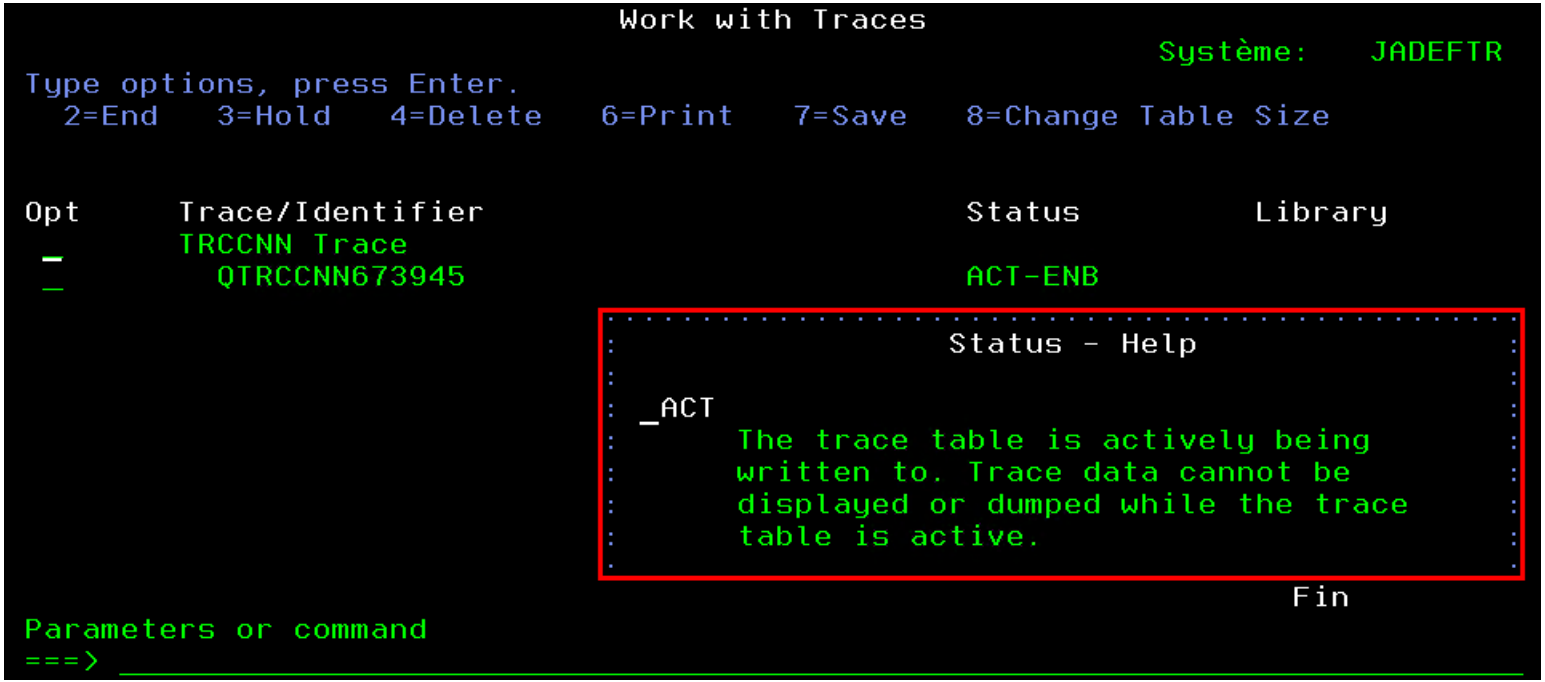
TRCCNN – Lancement d'une trace

TRCCNN SET(*ON) TRCTYPE(*IP) TRCFULL(*STOPTRC) TRCTBL(*GEN)



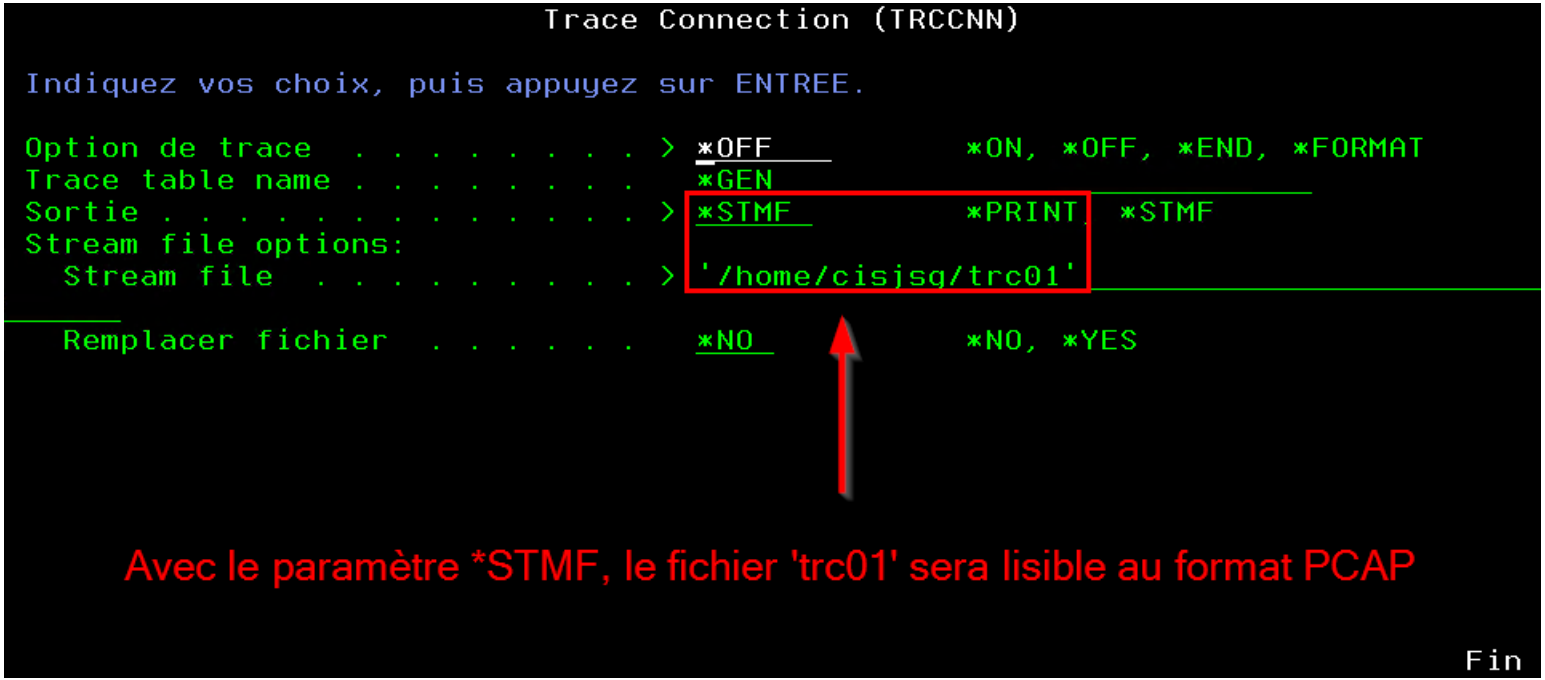
TRCCNN – Gestion des traces

WRKTRC *LIC

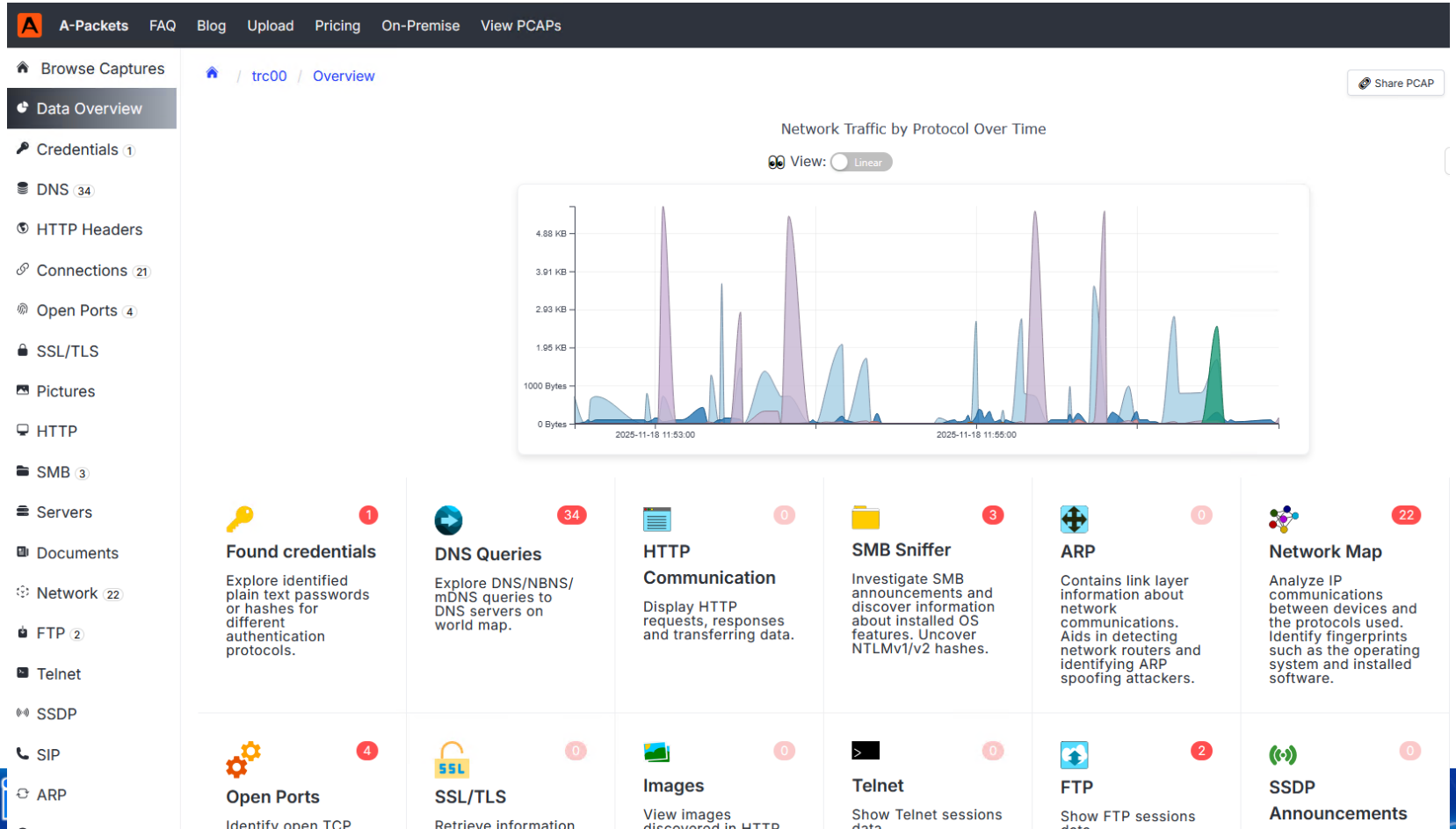


TRCCNN – Arrêt d'une trace avec génération PCAP

TRCCNN SET(*OFF) OUTPUT(*STMF) TOSTMF('/home/cisjsg/trc01')



TRCCNN – Analyse du fichier PCAP généré

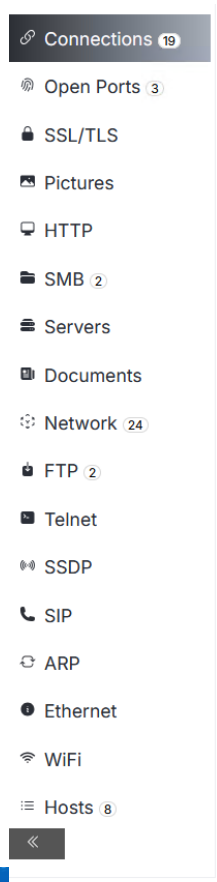


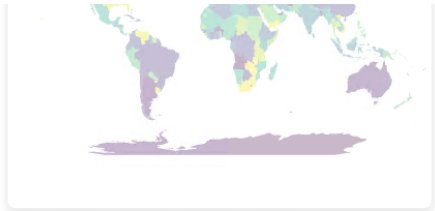
TRCCNN – Analyse du fichier PCAP généré

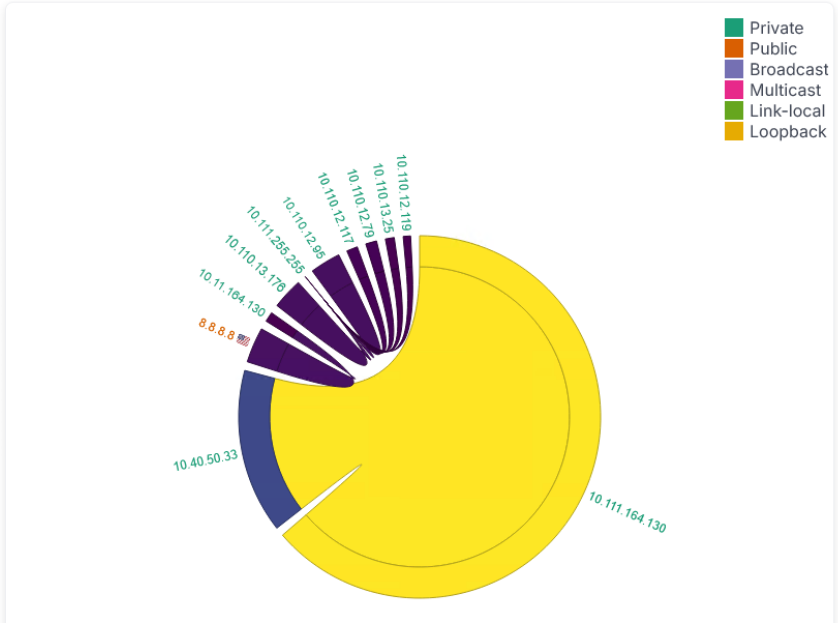
- Data Overview
- Credentials 1
- DNS 25
- HTTP Headers
- Connections 19
- Open Ports 3
- SSL/TLS
- Pictures
- HTTP
- SMB 2
- Servers
- Documents
- Network 24
- FTP 2
- Telnet
- SSDP

From	To	Type	Login	Password
10.40.50.33	10.111.164.130:21	FTP	jeanseb	pWeek25

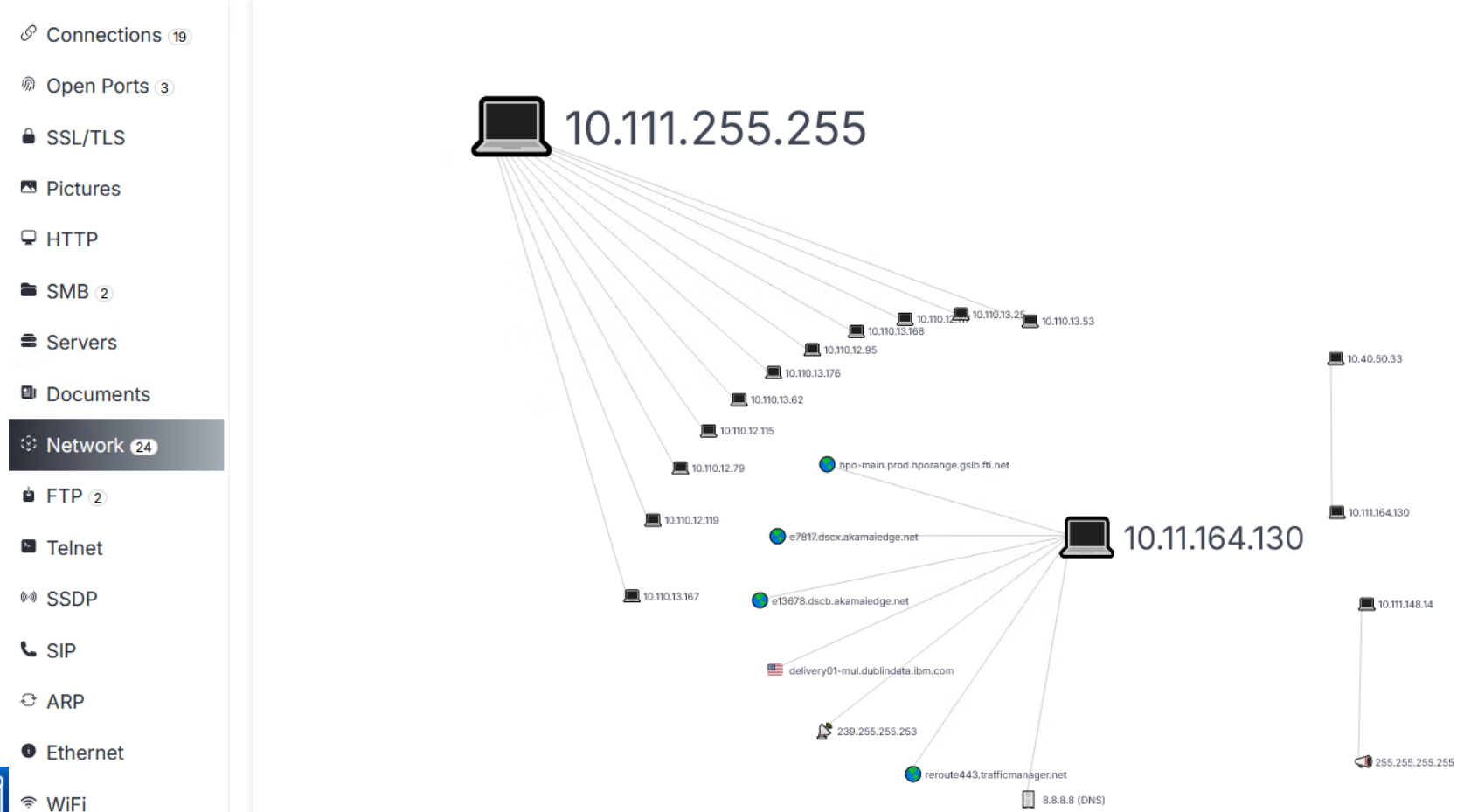
TRCCNN – Analyse du fichier PCAP généré



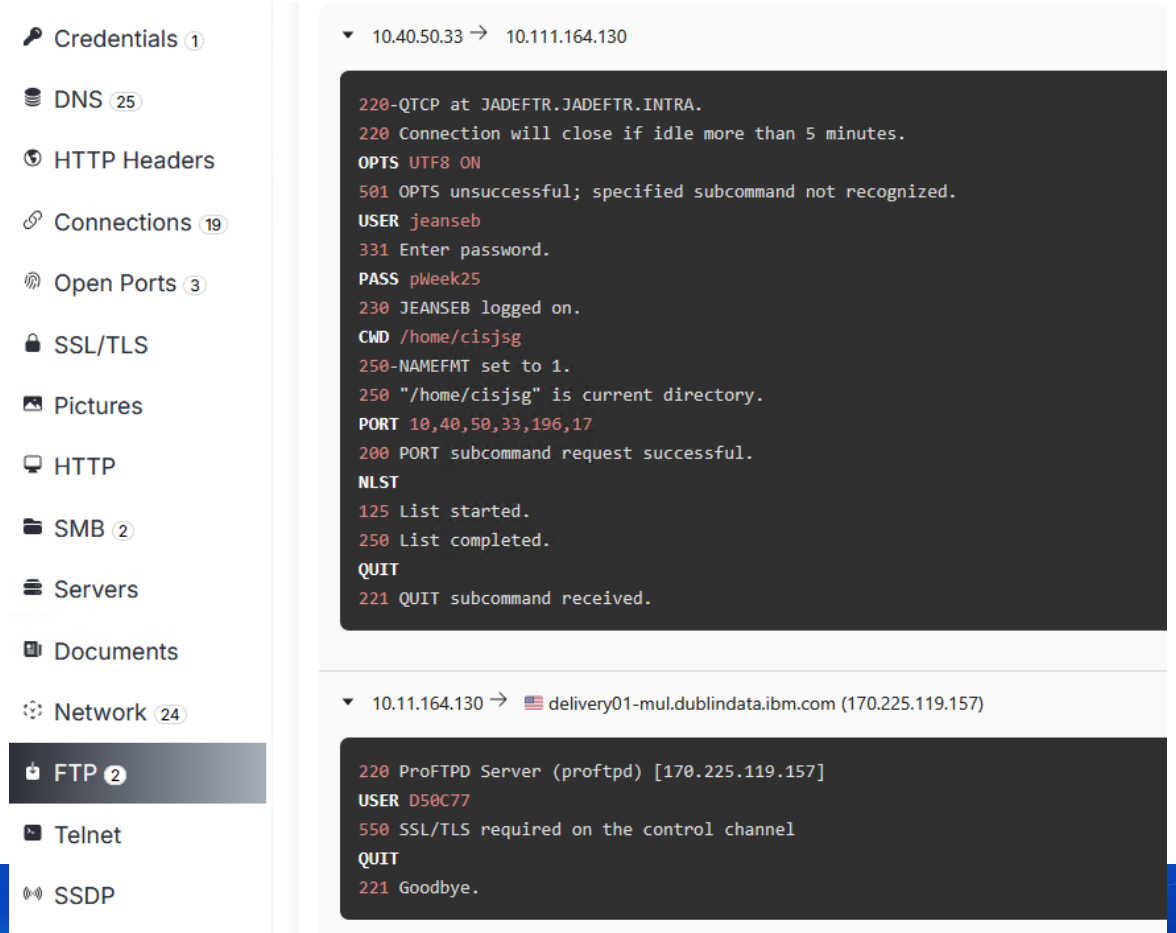




TRCCNN – Analyse du fichier PCAP généré

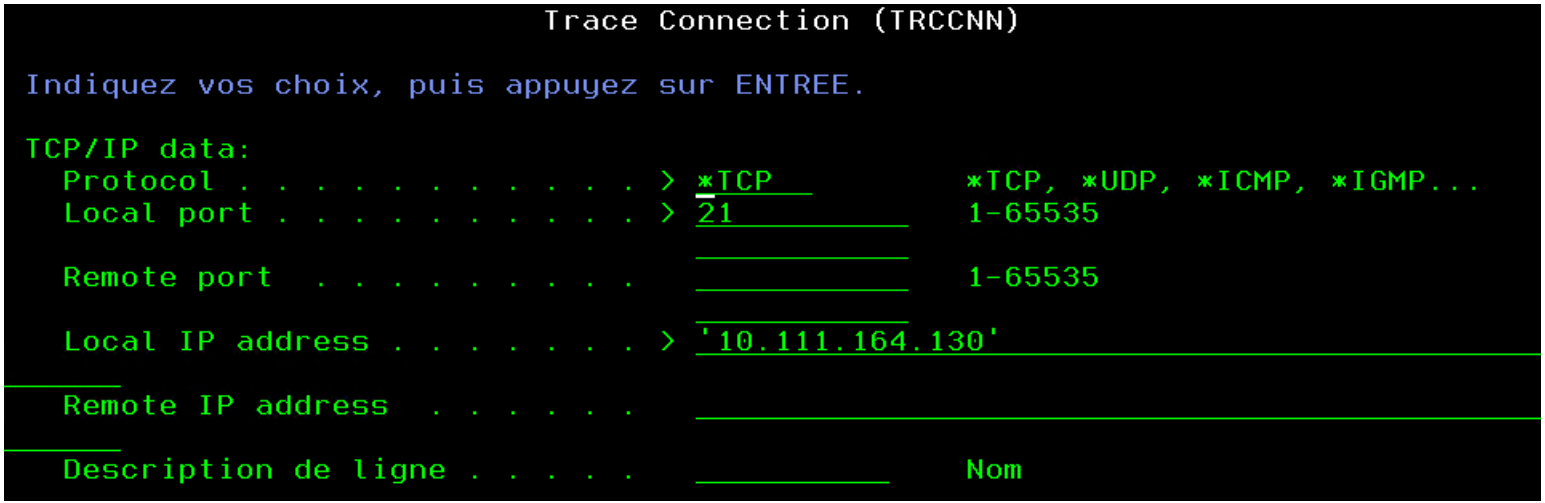


TRCCNN – Analyse du fichier PCAP généré



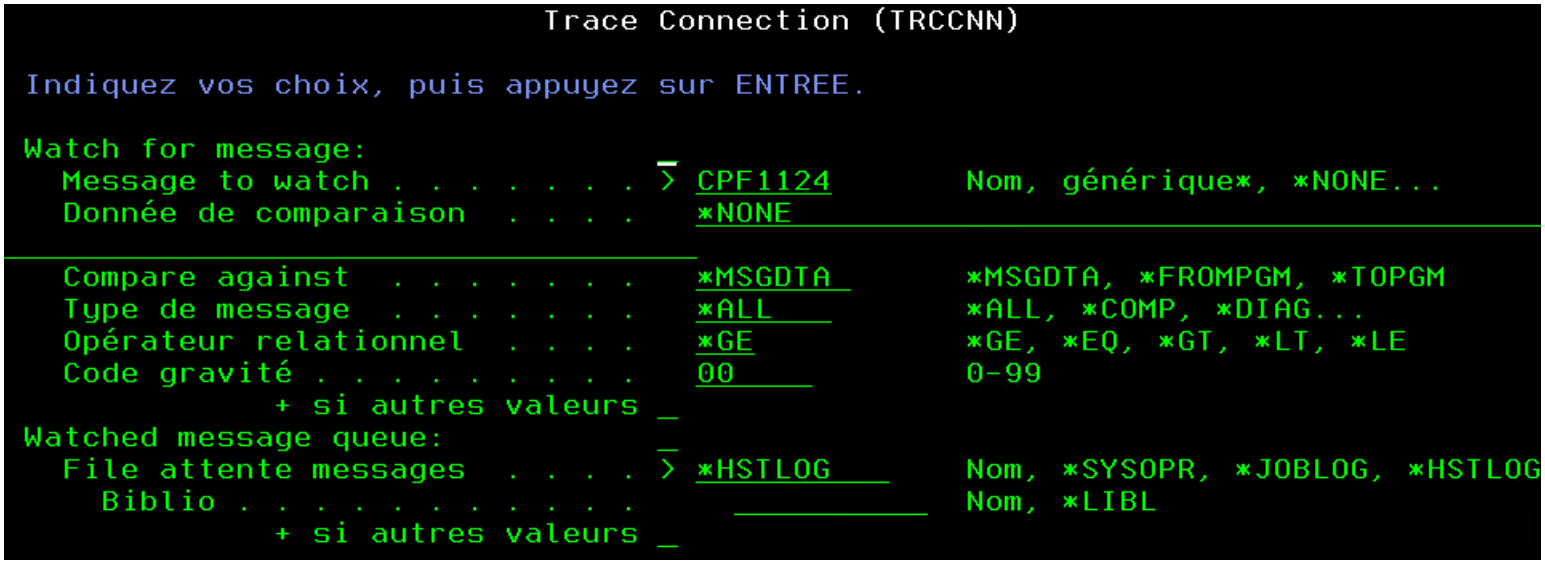
TRCCNN – Options de filtrage

TRCCNN SET(*ON) TRCTYPE(*IP) TRCTBL(*GEN) SIZE(64000) TCPDTA(*TCP (21) () '10.111.164.130') WCHMSG((CPF1124)) WCHMSGQ((*HSTLOG))



TRCCNN – Options d’arrêt

TRCCNN SET(*ON) TRCTYPE(*IP) TRCTBL(*GEN) SIZE(64000) TCPDTA(*TCP (21) () '10.111.164.130') WCHMSG((CPF1124)) WCHMSGQ((*HSTLOG))



TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

WRKWCH *ALL

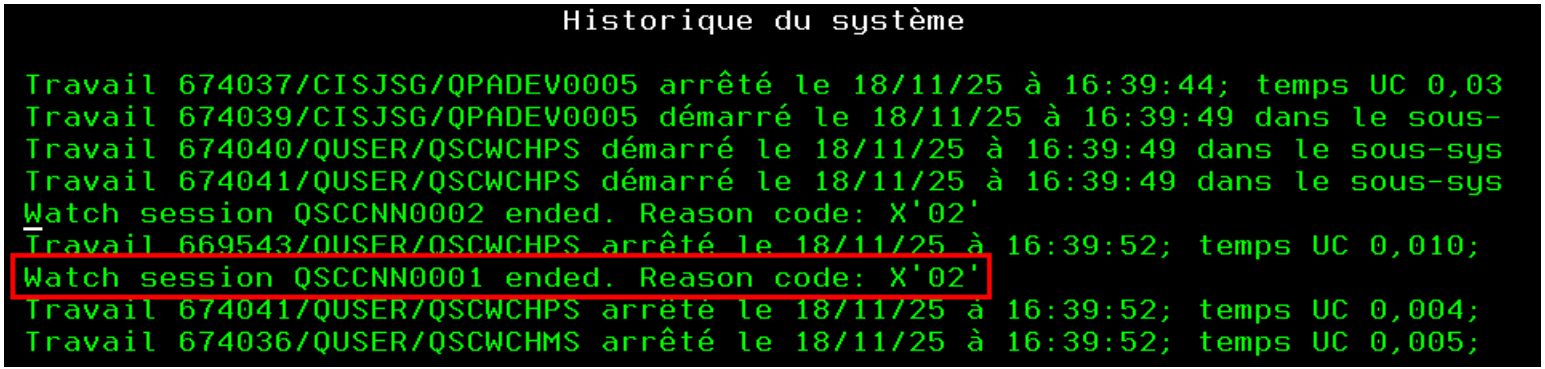
```
                              Work with Watches
                                                          Système:    JADEFTR
Type options, press Enter.
  1=Start    2=End    5=Display

Opt     Type/Session                        Origin        User          Status
 _      ___________________________
 _      Trace
 5        QSCCNN0001                        TRCCNN        CISJSG        ACTIVE
```

```
                                Display Watch
                                                          Système:    JADEFTR
Session ID . . . . . :   QSCCNN0001      Started:
Started by:                                 Date . . . . . :   18/11/25
  Travail  . . . . . :   QPADEV0005         Time . . . . . :   16:51:15
  Utilisat . . . . . :   CISJSG           Length of time to
  Numéro . . . . . :   674039               watch  . . . . . :   *NOMAX
Watch program  . . . :   *NONE            Intervalle . . . . . :   0
  Biblio . . . . . :
Origin . . . . . :   TRCCNN
Run priority . . . . :   25
          Type
          de            File attente messages   -------------Job--------------
Message   message       Name          Library     Name         Utilisat     Numéro
CPF1124   *ALL          QHST          QSYS
```

TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

DSPLOG



TRCCNN – Les ‘watches’ (ou triggers de l’IBM i)

DSPLOG + F1

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Une autre manière d'identifier les flux, c'est d'activer le pare-feu du système (disponible à partir de la 7.1) et de mettre en place des règles qui laissent tout passer mais enregistrent les flux dans un journal local DB2, ensuite requêtable en SQL.

PACKET RULES

Exemple de filtre permettant de tracer tous les flux entrant sur le système :

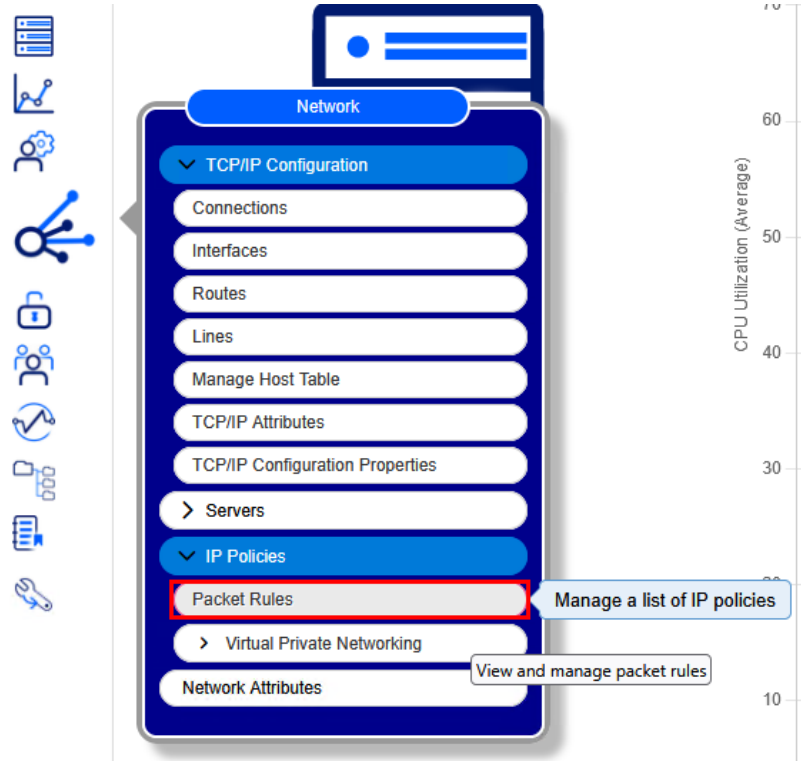
FILTER SET LogConnections ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = * **JRN = FULL**

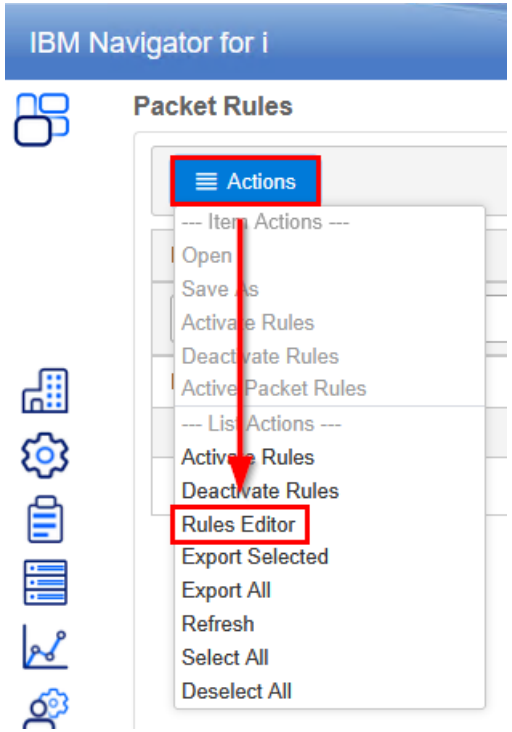
FILTER SET LogConnections ACTION = PERMIT DIRECTION = * SRCADDR = * DSTADDR = * PROTOCOL = * DSTPORT = * SRCPORT = * JRN = OFF

FILTER_INTERFACE LINE = ETHADMIN SET = LogConnections

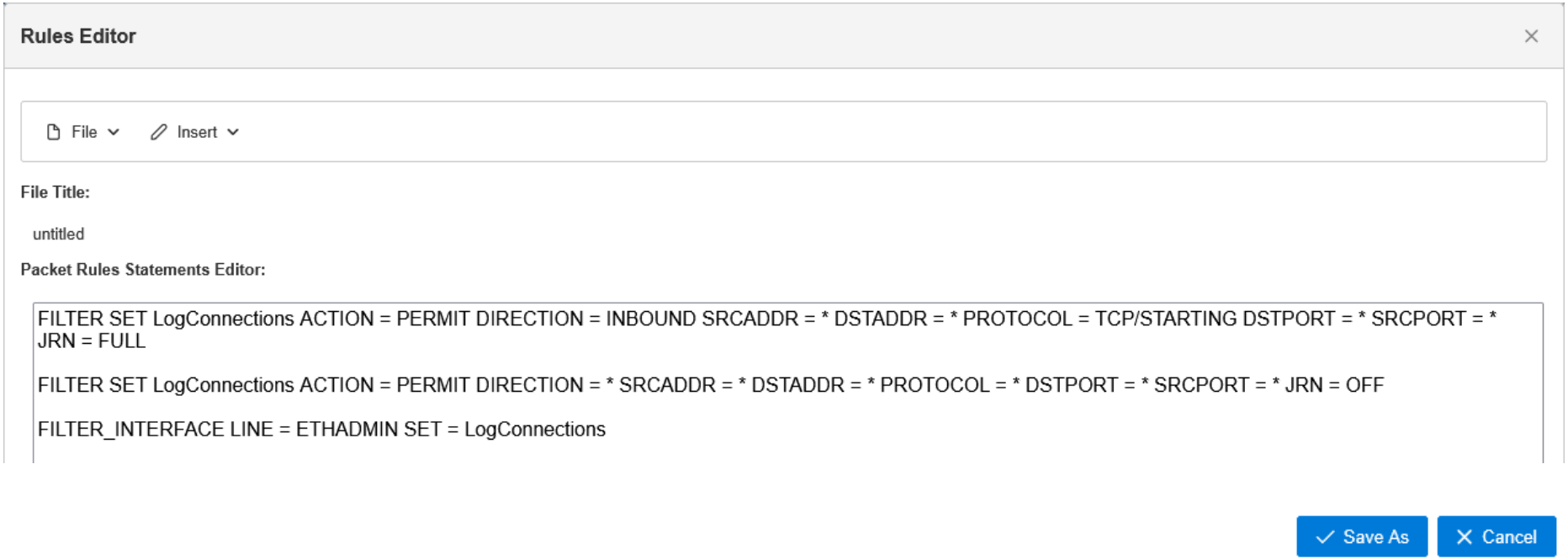
La seconde règle où "DIRECTION = *" est très importante car elle permet de dire qu'il faut laisser passer tout le reste du trafic entrant mais également tous les paquets sortant en retour !!!

PACKET RULES – Définition et mise en place de filtres

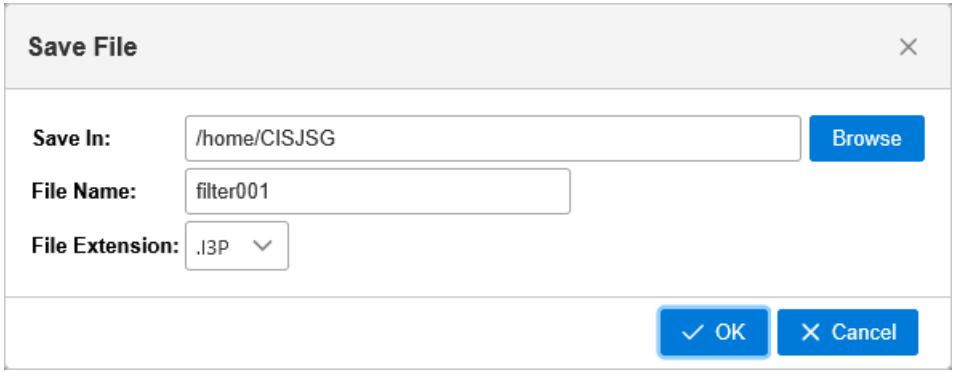




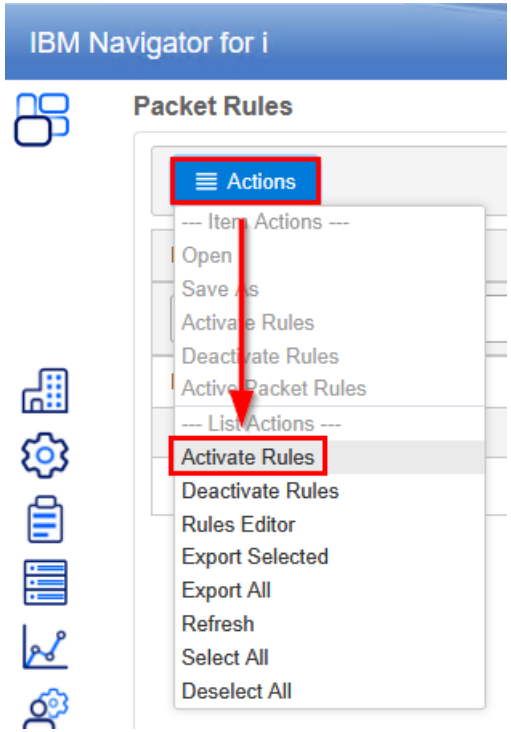
PACKET RULES – Définition et mise en place de filtres

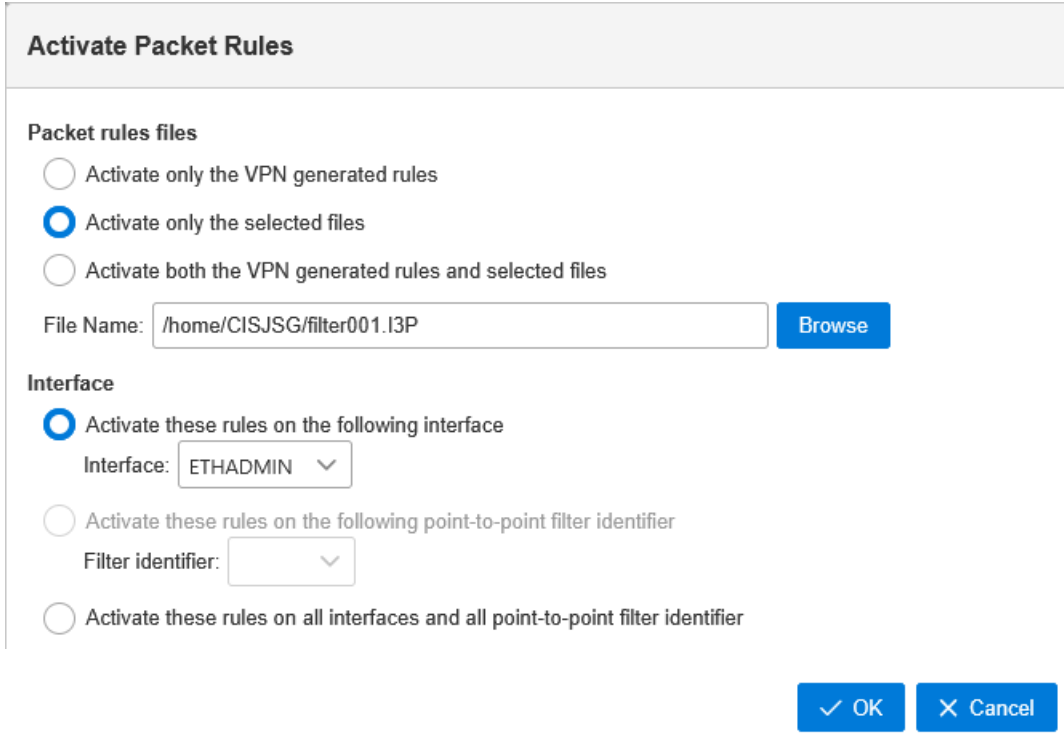


PACKET RULES – Définition et mise en place de filtres

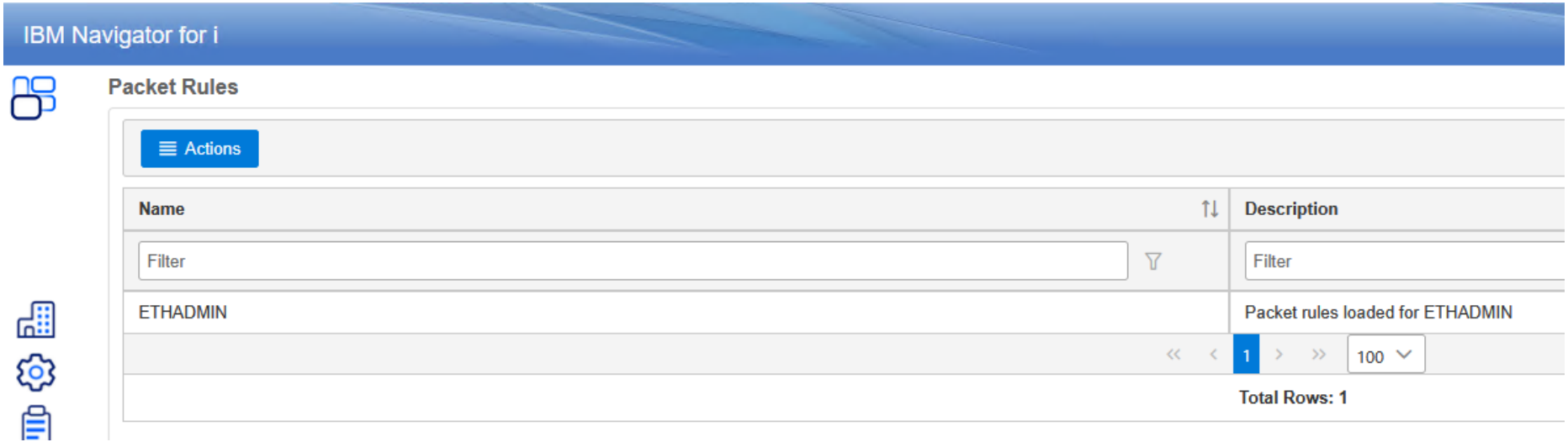


PACKET RULES – Définition et mise en place de filtres





PACKET RULES – Définition et mise en place de filtres



PACKET RULES – Contrôle des règles en place

Active Packet Rules

Filters

Address Translation

Inbound:

Properties

Action	Source	Destination	Source Port	Destination Port	Protocol	Origin	Journaling	Fragments
Permit	*	*	*	*	TCP/STARTING	Manual	Full	*
Permit	*	*	*	*	*	Manual	Off	*
Deny	*	*	*	*	*	Automatic	Off	*

Total Rows: 3

Outbound:

Properties | Security Associations

Action	Source	Destination	Source Port	Destination Port	Protocol	Connection Name	Origin	Journaling	Fragments
Permit	*	*	*	*	*		Manual	Off	*
Deny	*	*	*	*	*		Automatic	Off	*

Total Rows: 2

PACKET RULES – Commandes associées

- **La commande RMVTCPTBL peut être utilisée pour désactiver tous les filtres de règles sur le système => très pratique pour se débloquer si on s'est trompé dans les règles et qu'on s'est coupé l'accès à la machine !**

- Un filtre de règles peut être activé ou désactivé par programme via la commande LODIPFTR.

- Les entrées du journal des filtres de règles peuvent être affichées avec la commande DSPJRN JRN(QIPFILTER).

PACKET RULES – Consulter les paquets capturés

DSPJRN JRN(QIPFILTER)

```
                              Postes de journal

Journal  . . . . . :   QIPFILTER       Bibliothèque . . . . :   QUSRSYS
N° séquence le plus élevé à l'écran  . . . . . :    00000000000000000012
Indiquez vos options, puis appuyez sur ENTREE.
  5=Poste entier

Opt    Séquence    Code    Type    Objet    Bibliothèque    Travail    Heure
 _             1     J      PR                              QTOFJRN      12:36:52
 _             2     M      TF                              QTOFJRN      12:54:22
 _             3     M      TF                              QTOFJRN      12:55:32
 5             4     M      TF                              QTOFJRN      12:55:47
 _             5     M      TF                              QTOFJRN      12:55:47
 _             6     M      TF                              QTOFJRN      12:55:48
 _             7     M      TF                              QTOFJRN      12:55:48
 _             8     M      TF                              QTOFJRN      12:55:50
 _             9     M      TF                              QTOFJRN      12:55:50
 _            10     M      TF                              QTOFJRN      12:55:54
```

PACKET RULES – Consulter les paquets capturés

DSPJRN JRN(QIPFILTER)

```
                              Poste de journal

Objet . . . . . :                    Bibliothèque . . . . :
Membre . . . . . :
Données incomplètes  :   Non          Donn poste réduites  :   *NONE
Séquence . . . . . :   4
Code . . . . . :   M  - Données de gestion de réseau
Type . . . . . :   TF - Actions relatives aux règles de filtre IP

            Données spécifiques du poste
Colonne     *...+....1....+....2....+....3....+....4....+....5
 00001     'ETHADMIN  A I    2PERMIT   610.40.50.33    4992210'
 00051     '.111.164.130  2002                                 '
 00101     '        410.40.50.33                               '
 00151     '     410.111.164.130                               '
 00201     '                                                   '
 00251     '          '

                                                            Fin
```

PACKET RULES – Consulter les paquets capturés

SQL

*Sans titre 1

```sql
WITH filterlog AS (
        SELECT CAST(ENTRY_DATA AS VARCHAR(1000)) AS entry
            FROM TABLE (
                    QSYS2.DISPLAY_JOURNAL('QUSRSYS', 'QIPFILTER', JOURNAL_ENTRY_TYPES => 'TF')
                )
    )
    SELECT DISTINCT SUBSTR(entry, 1, 10) AS line,
           SUBSTR(entry, 29, 15) AS Srcip,
           SUBSTR(entry, 44, 5) AS Srcport,
           SUBSTR(entry, 49, 15) AS DestIP,
           SUBSTR(entry, 64, 5) AS DestPort
        FROM filterlog;
```

LINE	SRCIP	SRCPORT	DESTIP	DESTPORT
*ALL				
ETHADMIN				
ETHADMIN	10.40.50.33	49922	10.111.164.130	2002
ETHADMIN	10.40.50.33	49923	10.111.164.130	2002
ETHADMIN	10.40.50.33	49925	10.111.164.130	23
ETHADMIN	10.40.50.33	49935	10.111.164.130	23
ETHADMIN	10.40.50.33	49943	10.111.164.130	23
ETHADMIN	10.40.50.33	49946	10.111.164.130	23
ETHADMIN	10.40.50.33	49980	10.111.164.130	23
ETHADMIN	10.40.50.33	49992	10.111.164.130	23
ETHADMIN	10.40.50.33	50003	10.111.164.130	23
ETHADMIN	10.40.50.33	50013	10.111.164.130	23
ETHADMIN	10.40.50.33	50093	10.111.164.130	23
ETHADMIN	10.40.50.33	55317	10.111.164.130	2002
ETHADMIN	10.40.50.33	55321	10.111.164.130	2002
ETHADMIN	10.40.50.33	55322	10.111.164.130	2002
ETHADMIN	10.40.50.33	55323	10.111.164.130	2002
ETHADMIN	10.40.50.33	55324	10.111.164.130	2002
ETHADMIN	10.40.50.33	55325	10.111.164.130	21
ETHADMIN	10.40.50.33	55350	10.111.164.130	8476
ETHADMIN	10.40.50.33	55351	10.111.164.130	8475
ETHADMIN	10.40.50.33	55352	10.111.164.130	8476
ETHADMIN	10.40.50.33	55353	10.111.164.130	8471
ETHADMIN	10.40.50.33	55354	10.111.164.130	8475
ETHADMIN	10.40.50.33	55683	10.111.164.130	2002

AUTRES SOURCES – QHST (HISTORY LOG)

Accessible via SQL depuis la 7.1 au travers de la table HISTORY_LOG_INFO.

Compatible avec les formats SYSLOG RFC3164 et RFC5424.

[History of connections to IBM i]

```
create table qtemp.qhst as
(select * from table(qsys2.history_log_info(current timestamp -1 day)) x) with data;

select count(*) as "Count",
substring(trim(message_tokens), 65) as "IP Address",
substring(from_job, locate('/', substring(from_job, 8))+8) as "Job",
from_user as "Current User"
from qtemp.qhst where message_id = 'CPIAD09'
group by substring(trim(message_tokens), 65), substring(from_job,
locate('/', substring(from_job, 8))+8), from_user
order by 1 desc;
```

Count	IP Address	Job	Current User
7	127.0.0.1	QZDASOINIT	CISJSG
5	10.40.50.33	QZRCSRVS	CISJSG
4	127.0.0.1	QZRCSRVS	CISJSG
4	127.0.0.1	QPWFSERVSO	CISJSG
2	10.40.50.33	QZDASOINIT	CISJSG

AUTRES SOURCES – AUDIT JOURNAL

Pour auditer toutes les connexions TCP et UDP entrantes et sortantes du système, indiquez *NETSCK, *NETUDP et *NETTELSVR.

Les enregistrements d'audit SK-A/SK-C (en TCP) et SK-I/SK-O (en UDP) contiennent les informations suivantes :

- ✓ Famille d'adresses (IPv4 ou IPv6)
- ✓ Adresse IP locale
- ✓ Port local
- ✓ Adresse IP éloignée
- ✓ Port éloigné

Extension de niveau d'audit (QAUDLVL2) - Documentation IBM

AUTRES SOURCES – IDS, EXIT PGM, …

Principalement orienté sur la tâche de détection d'intrusion, la fonctionnalité **IDS** peut aussi permettre d'identifier des connexions entrantes ou sortantes en fonction des politiques mises en place.

Concepts de détection d'intrusion - Documentation IBM

L'implémentation de **programmes d'exit** est aussi une piste pour tracer les connexions.

Utilisation des programmes d'exit - Documentation IBM

S107 - TCP/IP est-il trop ouvert sur votre IBM i ?

Q&A ?


MERCI