Global Information Assurance Certification Paper

Table of Contents 1
Jean-Jacques_BARDOUIL_GSEC.doc 2

How to secure iSeries Navigator

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: BARDOUIL, Jean-Jacques
Location: Security Essentials Courses

Paper Abstract: The iSeries Navigator is a powerful tool for managing the iSeries. It install easily on windows computer and can be use by any user with an access on the iSeries. But this package could introduce information disclosure about the iSeries system and security configuration. This practical assignment will describe how to enforce security of this product.

January 28, 2004

Table of Contents

Introduction 1
Presentation of the iSeries security 1
System values 1
Network attribute 2
User profile 3
Object authority 3
TCP/IP Network security 4
Presentation of iSeries Navigator 4
How Client Access works 7
How to secure iSeries Navigator 9
Installation 9
OS400 integrated security 9
Using SSL with Client Access : 9
IP filtering 10
Exit program 10
Application Administration 11
Policy 13
Protection of the integrated file system group 13
Conclusion 13
References 15

List of Figures

Figure 1 iSeries network security capabilities at the various levels (IBM Corporation SG24-6227 p11) 4
Figure 2 Contextual menu on the File Systems view (IBM Corporation. SG24-6226 p 337) 6
Figure 3 Contextual menu for Disk 6
Figure 4 Establishing client/server communications (IBM Corporation. SC41-5740 figure 4-1) 7
Figure 5 Application Administration 12

List of Tables

Table 1 List of server available for Client Access and their description 8
Table 2 Function of Client Access and server needed 8
Table 3 example of exit point control 11

Introduction

Since the OS400 Version 4 (V4R2), IBM provided a new graphical interface to manage the iSeries server, the Operations Navigator or iSeries Navigator since V5R2. This product is a graphical application for Microsoft Windows computer connected to one or more iSeries on a TCP/IP network.
It presents an explorer view of the iSeries file system, hardware, configuration and allows contextual menu as well as drag and drop with the mouse.
End users can easily manage their print out, or display, send message and see all jobs they started and system administrator can fully control and monitor the iSeries configuration with this program. Some system operations can only be performed thru this interface like LPAR or cluster configuration.
"Those new to OS/400 can typically be "more productive sooner" getting to "know the system» through the Operations Navigator interface compared to learning the OS/400 command interface. » (IBM redbook SG24-6226, p 3.)
However, "Operations navigator is not designed for use by application users. Just like the MAIN menu from IBM gave users too much function, Operations Navigator also gives users too much function" (Wayne Evans)
And "iSeries was originally designed as a follow-on product for S/36 and S/38. Many iSeries installations were, at one time, S/36 installations or S/38 installations. To control what users could do, security administrators on those earlier systems often used a technique that is referred to as **menu security** or **menu access control"**…but…"computers and computer users have changed a great deal in the past few years. Many tools, such as query programs and spreadsheets, are available so that users can do some of their own programming to off-load IS departments." : IBM Corporation. SC41-5300 Chapter 6.
Currently many iSeries have security policies inherited from the menu security strategy.
This document will present the way to control the use of iSeries Navigator functions by end users.

Presentation of the iSeries security

Current iSeries security is based on authorities a user has on an object, authorization for a user to perform system operations, security auditing, and network security.

System values

These are the system policies of the iSeries. A group of security system values gives the system rule for password, security auditing, how many invalid access are allowed and the action when this number is reach.
The main securities values that control security of client server applications are :
QSECURITY : this value defines the level of security of the iSeries
Level 10 : no more supported since V4R3
Level 20 : security only by authentification

Level 30 : security by authentification and resources protection
Level 40 : security by authentification, resources protection, and OS400 integrity.
Level 50 : enforces OS400 protection of the level 40.
A minimum level of 40 is necessary in a client server environment. It ensures that the access to OS400 resources is granted according to IBM recommendation. Only documented system program or API can be used in user program, and this prevents to circumvent the OS400 integrated security.
QMAXSIGN and QMAXSGNACN : these values control the maximum number of invalid sign-ons, and the action when this maximum number of attempts is reached.
Recommended value for QMAXSIGN is 3 and recommended value for QMAXSGNACN is to disable the user profile and the device. Then after three errors on a identification, the PC cannot be used to try to connect to the server, and if the error is on password, the user id could not be used on another device without being primary reactivated.
QAUTOVRT : specifies if the telnet session is automatically configured (and how many can be configured). On iSeries, telnet session could be named and the telnet command (exactly the telnet 5250 command) could include the name of the session you want to use. If QAUTOVRT is set to 10, 10 sessions could be automatically created by OS400 with an internal name even if the telnet client does not provide a session name. If QAUTOVRT is set to 0, you have to manually create all session definitions you need for yours users, and then you can manage how many sessions are authorized for one client, and you can forbid a telnet session that does not provide the session name.
QRMTSIGN : specifies if the telnet session could bypass the signon screen. The user id used by Client Access could be used to automatically logon on the iSeries. This must be set to *FRCSIGNON to force the user to identify on telnet session.
Password system value : these system values begin with “QPWD” and controls the structure of the password and the lifetime of the password. IBM recommends a strong password policy with a lifetime of 90 days maximum.
AUDIT : these system values start with “QAUD”. They can start the security audit to log all security relevant actions. You can log access to object, save and restore events, action of user profile, modification of the iSeries security policies and modification of the iSeries configuration. You need the *AUDIT privilege to start, stop, view the security audit.
All records are stored in one or more journal receiver that you must protect and archive. You should monitor the audit journal to have intrusion detection, or to have information on security or configuration change.
More details on system value can be found in : IBM Corporation. SC41-5302 book.

Network attribute

Network attribute defines policies for SNA network.
Within the network attribute, there is a parameter for the security of Client

Access, but this concerns only the old DOS version of Client Access and not iSeries Navigator.

User profile

With the QSECURITY system value greater than 10 the iSeries requires all users to identify and authenticate before accessing to server applications.
The user profile definition in iSeries contains the user id and the password, the initial job parameters, one or more group profile, the initial menu and program, the possibility to limit the use of the command line and the “special authorities”.
Many parameters of the profile could have the value *SYSVAL which refers to system policies. Always monitor profiles that do not have not this value and document exceptions.
The initial menu, initial program and the possibility to limit the use of the command line are only active in a “green screen” or telnet application (menu se curity), and have no effect on iSeries Navigator or other client server products.
The group profiles are special user profiles that could give to a group of user the same authority to the iSeries resources. The user profile inherits the group profile authority, in addition to his authority. The group profile could also give special authority to the user profile, and be the owner objects newly created by the user.
Special authority controls the authorization of performing system operations on the iSeries. They are given at the user profile level or at group profile level.
List of special authorities:

- *ALLOBJ bypasses the object authority security.
- *AUDIT allows a user to manage, view the security auditing.
- *IOSYSCFG allows a user to manage configuration of the system and device connected.
- *JOBCTL allows a user to control jobs on the system.
- *SAVSYS allows a user to save and restore all objects on the iSeries.
- *SECADM allows a user to manage user profile and security policies.
- *SERVICE allows a user to have service system access.
- *SPLCTL allows user to manage all output print in the system.

These special authorities, also named privileges are part of the iSeries integrated security. They protect iSeries at command line level, but also at API and low-level instruction level at security level 40 (National Security Agency, p 217) and therefore are efficient in a client server environment.
User profile could need several privileges to perform system function. The management of the security policies needs *ALLOBJ, *AUDIT and *SECADM privileges for example. However, IBM recommends that end users have no special authorities.

Object authority

Each object on the iSeries has authority attribute at the object level and at the data level.
There is an authority for the owner of the object, a default authority, and possibly authorities for user profiles and group profiles.

This protection protects iSeries at command line level, but also at API and low-level instruction level at security level 40.
More detail on migrated from menu security to object authority security can be found in : IBM Corporation. SC41-5300 Chapter 6.

TCP/IP Network security

Currently, iSeries support the following TCP/IP security facilities : LT2P, RADIUS, IP packet filtering and NAT, VPN, SSL, Kerberos.

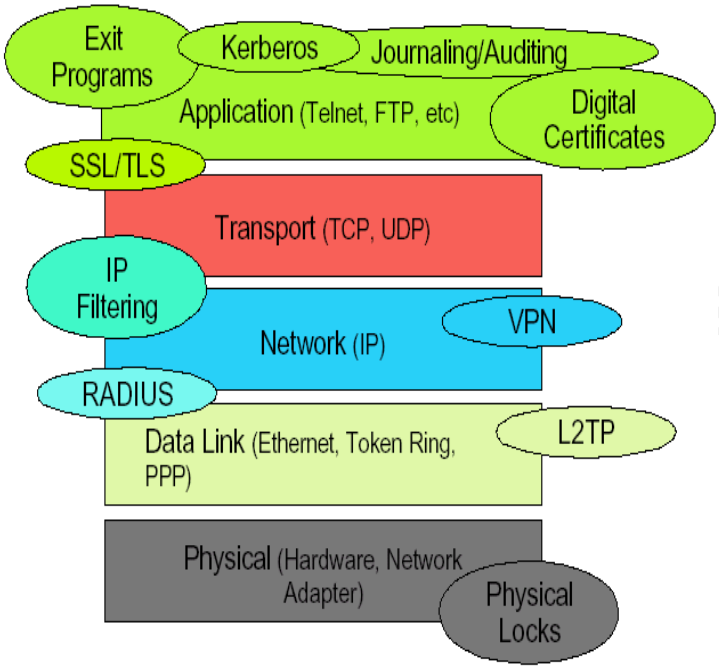

Figure 1 iSeries network security capabilities at the various levels (IBM Corporation SG24-6227 p11)

Presentation of iSeries Navigator

iSeries Navigator is part of the Client Access package. The other parts of the package are terminal and printer emulation, data transfer from and to the iSeries, remote command, ODBC and OLE drivers for iSeries.
It has been designed to allow new iSeries customers to easily manage the system. It also adds new functionalities that cannot be managed with the command line (IP filter for example).
iSeries Navigator components are presented by groups :

- **Basic Operation** group that contains the management of messages, printer output, and printer.
  The user may needs *SPLCTL and/or *JOBCTL privileges or authority to perform menu actions. Without privilege, users can manage their jobs and printouts.
- **Work Management** group to monitor and manage active job, server job,

job queue and memory.
User must have *JOBCTL privilege to change any job parameter.
Without privilege, user can only see his job. This group is not needed for basic user.

- **Configuration and Service** group that manage system policies, hardware, software, fixes, performance data.
  User must have nearly all privileges to use this group but without privileges, users can have a read access on all these data. This option must be protected so that only system administrator can use it.
- **Network** group for TCP/IP management and configuration (routes and interfaces configuration, VPN, NAP, IPTABLE, Remote access, DNS, TCP/IP Servers, HTTP Servers …).
  Users must have *IOSYSCFG privilege and authority on configuration file to change configuration of TCP/IP services. If user has not privilege, he can “only view” the parameter (confidentiality problem). This option must be protected so that only system administrator can use it.
- **Security** group to set up the system security policies.
  Users must have *ALLOBJ, *AUDIT, *SECADM privileges to change parameter in this group but without privileges user can have a read access on all these data. This option must be protected so that only system and security administrators can use it.
- **User and Group** group to manage user access.
  Users must have *SECADM, *AUDIT privileges and *ALLOBJ privilege or authority on user profile. If user has no privilege, he can “only view” the user profile on which he have authority (confidentiality problem). This option must be protected so that only system and security administrators can use it.
- **Database** group to manage database object using SQL terminology.
  User must have authority on the objects and data content. Only developer and system administrator need to use this option.
- **File systems** group to manage the file system of the iSeries with a hierarchy tree structure. It provides storage management methods similar to personal computer and UNIX operating system. One specific file system is the QSYS.LIB directory. It contents all the traditional iSeries objects like libraries, files or user profile.
  User will see all objects on which he has authority and can shred (delete) object if he has the *OBJEXIST authority on object. But it can be an easy way to transfer data from the iSeries to a personal computer by simply using the drag and drop function of iSeries Navigator.
- **Backup** to schedule simple backup
  User must have *JOBCTL and *SAVSYS privileges to change parameter in this group. . Only system administrator needs to use this option.
- **Application Development** to work with Unix development environment.
- **Commands** group to schedule the execution of program on iSeries.
  Only developer and system administrator need to use this option.

- **Package and product** group to package program like IBM does. User must have *ALLOBJ and *SECADM privileges to use these functions. Only developer and system administrator need to use this option.
- **Monitor** group to define graphical monitor of the system, the system alert message queue and jobs. Only system administrator needs to use this option.
- **AFP manager** group for printing facility. Only developer and system administrator need to use this option.
- **Application** group to restrict the use of iSeries Navigator. User needs *SECADM privilege to use this function. Only system administrator needs to use this option.
- **Optional** plug in for IBM or other optional interface. Only developer and system administrator need to use this option.

Some of these groups only exist since version 5 of OS400

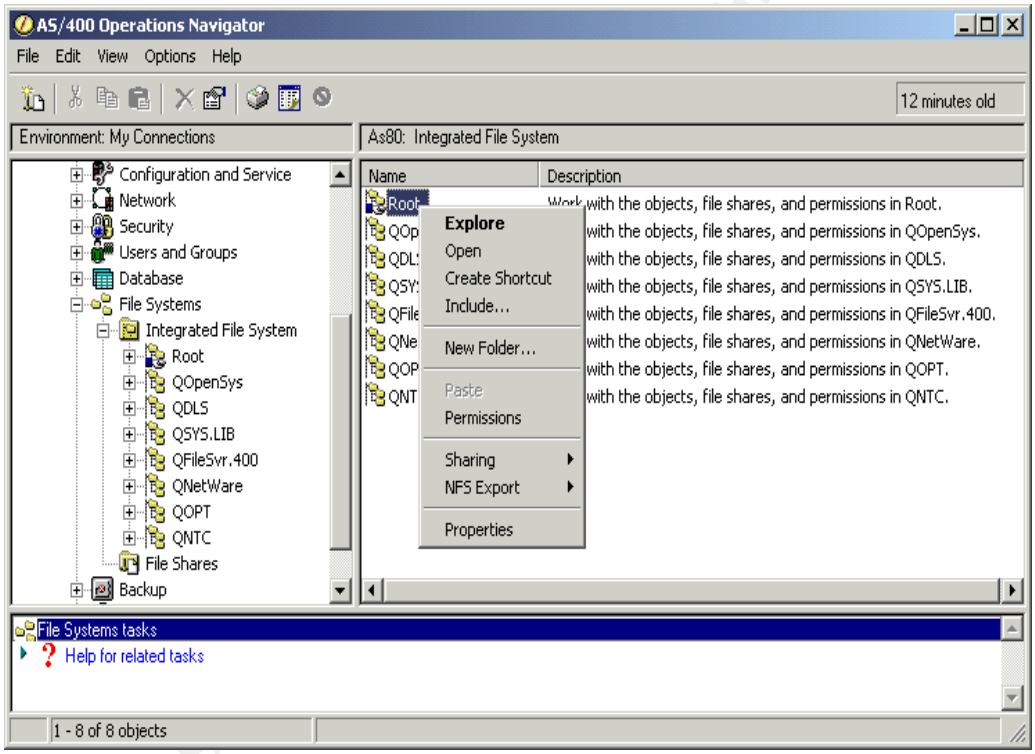

Figure 2 Contextual menu on the File Systems view (IBM Corporation. SG24-6226 p 337)

With iSeries Navigator we can verify a disk, or start job to monitor performance which could make a deny of service on the iSeries.

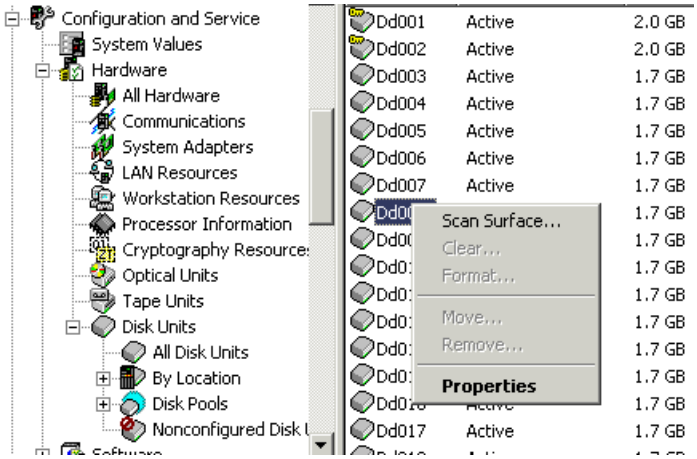

Figure 3 Contextual menu for Disk

You could also see or modify the security with just a click of mouse. iSeries Navigator displays too much configuration to end users even if they have no system privilege. From a security point of view, only few options must be accessible to all users of the iSeries.

How Client Access works

Client Access communicates with Daemons on the iSeries. These Daemons are named Host Server on the iSeries.
The Client connects to the Host Server on iSeries and asks for a server. If this server is started, then it starts a new server job to handle the communication with the client.
The client reconnects to this new job, communicates the user profile and the password. The server verifies the user profile and the password, and then changes the job to the user profile

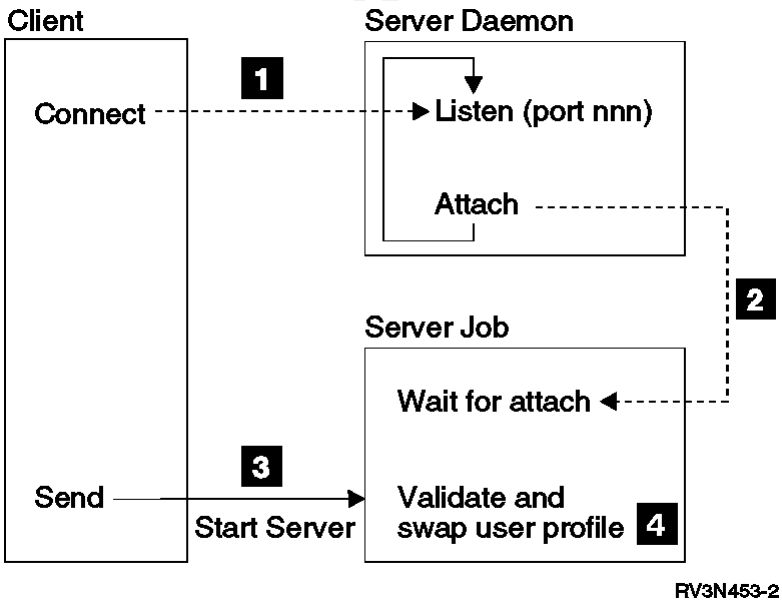

Figure 4 Establishing client/server communications (IBM Corporation. SC41-5740 figure 4-1)

By default, servers are not started. They could be started by the command STRHOSTSVR followed by the list of the servers we want to start or by the special value *ALL to start all servers.
I have noticed that many system administrators do not know which servers are needed for their application. Therefore they use the *ALL parameter.
To find which Host Server is necessary, you could use the command Netstat and look in the column “idle time”. If idle time corresponds to the start of the service, then the service is not used and you can stop it.
The table after shows for each function of Client Access the host servers we need to start.

Table 1 List of server available for Client Access and their description

Server	Port	SSL port	Description
Port Mapper	449	N/A	Returns the port number for the requested
Central	8470	9470	Used when a Client Access license is required, and also for downloading translation tables.
Database	8471	9471	Used for accessing the AS/400 database.
Data Queue	8472	9472	Allows access to the AS/400 data queues, used for passing data between applications.
File Server	8473	9473	Used for accessing any part of the AS/400 file system.
Print	8474	9474	Used to access printers known to the AS/400 system.
Remote Command	8475	9475	Used to send commands from a PC to an AS/400 system and for program calls.
Sign-on	8476	9476	Used for every Client Access connection to authenticate users and to change passwords.
Web Admin	2001	2010	Used to access Web applications served by the AS/400 system.
MAPI	5110		Used by the Mail APIs.
DDM	446	448	Used to access data via DRDA and for record level access.
Telnet	23	992	Used to access 5250 emulation.
USF	8480	N/A	Used for multimedia data.
LDAP	389	636	Provides network directory services.
Mgmt Central	5555	5566 5577	Used to manage multiple AS/400 systems in a network.
NetServer	137, 138, 139	N/A	Allows access to the AS/400 file system from Windows PCs.

Table 2 Function of Client Access and server needed

Function	sign-on	central	telnet	database	remote cmd	file	print	web adm	mgmt centr	usf	netserv	ldap	dataq	ddm
PC5250 Display & Printer Emulation	Y	Y	Y											
Data Transfer	Y	Y		Y										
Base Operations Navigator Support	Y				Y									

All Operations Navigator Functions	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
ODBC	Y			Y										
OLE db	Y			Y	Y								Y	Y
AFP Viewer	Y						Y							
Client Access Install											Y			
Fax Support	Y						Y							
Inconming Remote Command														

How to secure iSeries Navigator

Installation

You can choose not to install the product on the iSeries. However, iSeries functionalities that can be configured or started only by iSeries Navigator cannot be used. IP filter for example is one of these functionalities.
If iSeries Navigator is installed on server, then during the install on the client, you could choose a “basic install” that will install only the Basic Operation group. Then put the installation CD in a secure place, and protect the image of the CD in the \QIBM\ProdData\CA400\Express\Install\Image directory of the iSeries. However, I have verified, you could find the Client Access install CD on the Internet (search for “Client Access” on a Peer to Peer network for example) and this makes me think that iSeries Navigator could be used by anyone who wants to see the contents and the configuration of an iSeries.
“Not installing the product is security by ignorance -- and it is effective for 90+% of the population -- but do not be fooled, there will be some clever users that install the product.” Wayne Evans
The control of the installation could not be a way to enforce security of iSeries Navigator.

OS400 integrated security

If you have a strong security on your profiles and on your objects, then the only risk with Client Access is information disclosure.
If the users of the iSeries have no privilege in their user profile, they cannot modify the iSeries configuration, nor TCP/IP, or the security but he can look at these items.
If you have a strong security on objects that allows only access to data by program, then your user will not be able to modify objects or data with Navigator on your iSeries.
Therefore, you have to verify periodically than your security is always so strong.

Using SSL with Client Access :

To protect your iSeries authentication security in a network environment, SSL encryption must be used with Client Access.
The excellent documentation from Jose Guerrero (in the SANS InfoSec Reading Room) describe how to implement it. The IBM implementation guide is the SG24-6939 Red Book, chapter 4.5.
Use OS400 IP Filtering to log the non SSL Client Access port utilization in a first time. When you have ensured that all clients use SSL, you can restrict Client Access to use only SSL daemon.

IP filtering

iSeries Packet rules is accessible through iSeries Navigator (Group IP Policies). With IP filtering on the iSeries, you could control which IP address accesses the port on the server. Therefore, you could allow or deny specific or range of IP address to connect to specific Host server, for any request.
Control by IP filtering is at high level (Host server), based on IP address.
You have also the possibility to log all accesses in a log file (QIPFILTER in QUSRSYS library).
This is very useful to find which Host server is used when we use one function of iSeries Navigator. Just log all traffic between your IP address and the iSeries.

If you just want to log utilization of the host servers, then the last line must allow all protocols from all addresses and ports because the OS400 adds the rule "All traffic that is not permitted is automatically denied" at the IP filter rule.
If you forgot that line, then it is possible that iSeries Navigator cannot connect to server. Furthermore, you cannot have access to IP filter configuration.
Then, use the command RMVTCPTBL on a command line of the iSeries and the IP filter service will be stopped.

Example of logging utilization of Database and Data Queue Host Servers

```
INCLUDE   FILE = /QIBM/Services.i3p
# Statements to permit inbound CLIENTACCESS over ETHERNET
# ------------------------------------------------------
FILTER SET ISERIES_PERMIT   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = *   DSTADDR = *
SERVICE = CLIENTACCESS_8471_TCP_FS   JRN = FULL
FILTER SET ISERIES_PERMIT   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = *
SERVICE = CLIENTACCESS_8471_TCP_FC   JRN = FULL
FILTER SET ISERIES_PERMIT   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = *   DSTADDR = *
SERVICE = CLIENTACCESS_8475_TCP_FS   JRN = FULL
FILTER SET ISERIES_PERMIT   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = *
SERVICE = CLIENTACCESS_8475_TCP_FC   JRN = FULL
# ------------------------------------------------
# Statements to permit all Services over ETHERNET
# ------------------------------------------------
FILTER SET ISERIES_PERMIT   ACTION = PERMIT   DIRECTION = *   SRCADDR = *   DSTADDR = *   PROTOCOL = *
DSTPORT = *   SRCPORT = *   JRN = OFF
# ------------------------------------------------------
FILTER_INTERFACE   LINE = ETHERNET   SET = ISERIES_PERMIT
```

The implementation of the iSeries IP Filtering is described in the IBM Corporation. iSeries Networking Security Packet rules documentation.

Exit program

For each Host server, IBM provides one or more exit point to control the activity of the host server. You just have to register your own control program in the registration table to have an exit program.
The exit point passes to your program the user profile and the request done by Client Access.
With this solution, you can develop a user profile based security to allow specific user to specific operation only (traditional security for iSeries) and this

solution in not dependent on the client program. Any client program (IBM or not) must use the same API (at security level of 40) for accessing the iSeries contents and therefore can be controlled with the same exit program.
You could also log the access and the request with the same exit point.
On the market place, some good commercial products control security on iSeries with these exit points.
The list of the exit point and the way to use it is in Client Access Express Host Servers documentation SC41-5740 (Appendix A).

Table 3 example of exit point control

OS/400 servers	exit point	Control
File Server	QIBM_QPWFS_FILE_SERV	Change file attributes Create stream file or create directory Delete file or delete directory List file attributes Move Open stream file Rename Allocate conversation
Database Server	QIBM_QZDA_INIT	server initiation.
Database Server	QIBM_QZDA_NDB1	Create source physical file Create database file, based on existing file Add, clear, delete database file member Override database file Delete database file override Delete file Add library list
Database Server	QIBM_QZDA_SQL1	SQL request Prepare Open Execute Connect Create package Clear package Delete package Stream fetch Execute immediate Prepare and describe Prepare and execute or prepare and open Open and fetch Execute or open
Central Server	QIBM_QZSC_SM	system management requests
Central Server	QIBM_QZSC_NLS	conversion table requests
Remote Command	QIBM_QZRC_RMT	remote command or distributed program call requests

Application Administration

This option of iSeries Navigator controls if a user is authorized to view group or individual functions of iSeries Navigator.
This is not a security solution but more an application feature. For example, a user with the necessary privilege can be denied to manage the TCP/IP

configuration with iSeries Navigator, but he can always configure TCP/IP with OS400 command on “green screen”.
Authorization can be granted or revoked for :

- User with *ALLOBJ privilege (typically the system and security administrator).
- Default user.

Access can be allowed or denied to specific user profile or group profile.
This option is similar to the limit capability parameter of the user profile in the “green screen” environment and is the easiest way to limit access to system information with iSeries Navigator.
This option is not installed by default when installing the iSeries Navigator. You have to do a full or a selective install on the Windows computer in charge of managing this application.
After installation, the option is accessible with a right click of the mouse on the system name of the iSeries.
Then for all functions un-needed to all users, you have to uncheck default access and then give access to specific function to specific user or for example to the developer group profile.
With the function Management Central, several iSeries could be managed from one central point.

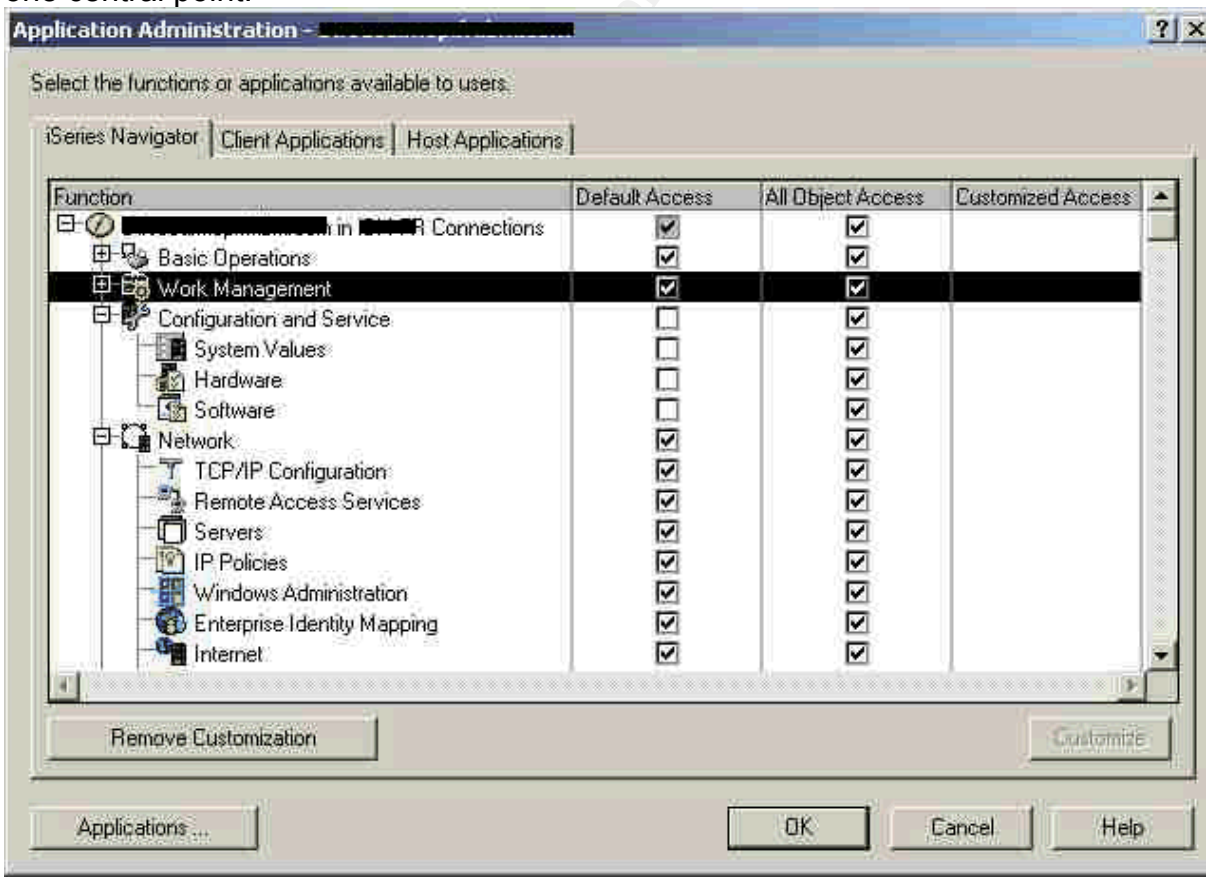

Figure 5 Application Administration

Policy

Client Access package contains windows policies to restrict user for certain actions or to protect configuration of the Client Access configuration on PC. Policies apply depending on the PC user profile.
You will need to configure a policy server, either on a Microsoft server, on the iSeries Netserver, or on a Netware Server and a primary logon server.
As for Application Administration, the policies act on application, and therefore are not really iSeries security but application customization.
The file template caerestr.adm restrict user to run Client Access function, and contain one policy to prevent use of iSeries Navigator.
This is some functions on the client computer that policy can control :

- prevent data transfer upload or download use
- prevent remote command use
- prevent remote program use
- require secure sockets
- prevent connections to systems not previously defined
- prevent all data transfer to an iSeries server
- prevent Excel add-in uploads
- Prevent usage of iSeries Navigator
- Maximum number of PC 5250 Sessions

Protection of the integrated file system group

You can control the access to the QSYS.LIB folder from the root directory (File systems group view) by using the QPWFSERVER authorization list. When a user as no authority on this object, then he cannot access to QSYS.LIB content from the root directory of the integrated file system (IFS). For an authority of *USE or greater authority the contents of the QSYS.LIB directory can access, according to object authority strategy.
The default authority value of the QPWFSERVER at the system ships is *USE and must be customize according to your security policy.
This authorization list does not secure other way of accessing the QSYS.LIB content like the client access transfer file, or ODBC driver.
Other protection can be implemented to protect other File System of IFS. There are documented in : IBM Corporation. SC41-5300 Chapter 15.
The security auditing can also be used on directory to monitor access to these objects.

Conclusion

By default, iSeries Navigator introduces possible information disclosure to end user.
To prevent this Application Administration can be easily used to deny the possibility of using system and security functionality of iSeries Navigator.
By default, Application Administration allows these options to all users. This must be changed as soon as possible.

If you are already using Microsoft policy then you can also use the Client Access Policy to control the usage of Client Access.
In a second time, you have to configure SSL on all computers who using client access. After that, use IP Filter, OS400 integrated security and exit point to secure the iSeries from all client server application that could be use with the iSeries server.
In a client-server application for iSeries, the integrated security of OS400 is the only way to ensure security. Good authority on object and less system privileges in user profile are the only way to secure these environments.

References

IBM Corporation. Managing OS/400 with Operations Navigator V5R1, Volume 1: Overview and More,SG24-6226
< http://www.redbooks.ibm.com/redbooks/SG246226.html>

Evans, Wayne O. New Security Features for the iSeries 400 Webcast on search400.com the 23 January 2001.
<http://search400.techtarget.com/webcastsTranscript/0,289691,sid3_gci508965,00.html>

IBM Corporation. Client Access Express Host Servers V4R4M0, SC41-5740
<http://publib.boulder.ibm.com/cgi-bin/bookmgr/BOOKS/QB3AUX03>

IBM Corporation. Managing OS/400 with Operations Navigator V5R1 Volume 2: Security, SG24-6227
< http://www.redbooks.ibm.com/redbooks/SG246227.html>

National Security Agency. Final Evaluation Report, International Business Machines Corporation AS/400 (Report CSC-FER-95/006)
<http://www.radium.ncsc.mil/tpep/library/fers/NCSC-FER-95-006.ps>

IBM Corporation. iSeries Networking Security Packet rules
< http://publib.boulder.ibm.com/html/ as400/v5r1/ic2924/info/rzajb/rzajb000.pdf>

IBM Corporation. iSeries Security Reference SC41-5302
<http://publib.boulder.ibm.com/iseries/v5r2/ic2924/books/c4153026.pdf>

IBM Corporation. Tips and tools for securing your iSeries server SC41-5300
<http://publib.boulder.ibm.com/iseries/v5r1/ic2924/books/c4153005.pdf>

IBM Corporation. iSeries Access for Windows V5R2 Hot Topics: Tailored Images, Application Administration, SSL, and Kerberos SG24-6939
<http://www.redbooks.ibm.com/redbooks/pdfs/sg246939.pdf>

Guerrero, Jose. Using SSL with Client Access Express for AS/400. SANS Institute 2001. October 9, 2001.
<http://www.sans.org/rr/whitepapers/vpns/745.php>