

## ISA 2004 Security Certification Checklist [Windows 2003 Server Edition Only]

### Operating System

- Verify Windows 2003 is patched and all service packs installed. If not, install all critical available. *NOTE: Make sure ISA 2004 is installed before Service Pack 1 is installed.*
- Install Security Configuration Wizard.
  - Select "Create a new Security Policy".
  - Enter the FQDN, IP, or DNS Name. Click "Next".
  - When viewing the "SCW Viewer", close it down.
  - Click "Next" on "Processing Security Configuration Database".
  - Make sure "Fileserver" and "Microsoft Internet Security and Acceleration Server 2004" are selected on the "Select Server Roles" page. Click "Next" on "Select Server Roles". *NOTE: Do not select "Remote access\VPN Server" if using VPN access through ISA server.*
  - On "Select Client Features" leave everything checked except "WINS Client" and "DNS Registration Client". Click "Next".
  - The "Select Administration and Other Options" page will now appear. Be sure to remove "Application Installation from Group Policy" from the options. Click "Next".
  - Now on the "Handling Unspecified Services" page, select "Do not change the startup mode of the service option". Click "Next".
  - The "Confirm Service Changes" page will show all the services enabled, disabled, and shut off completely. Review and click "Next".
  - On "Network Security", these features are unnecessary so select "Skip this Section" to continue on. Click "Next".
  - The "Registry Settings" box should now appear, click "Next".
  - Be sure on this next page to select both "All computers that connect to it satisfy the following minimum operating system requirements" and "It has surplus processor capacity that can be used to sign file and print traffic". Click "Next".
  - "Outbound Authentication Methods" has only two options that need to be selected that are "Domain Accounts" and "Local Accounts on the Remote Computers". "Click Next".
  - On "Outbound Authentication using Domain Accounts" make sure "Windows NT 4.0 Service Pack 6a or later Operating Systems" is selected.
  - Now, on "Registry Security Settings", everything should be selected appropriately – just click "Next".
  - "Audit Policy" should appear, click "Next".

- You should select “Audit successful and unsuccessful activities” on the “System Audit Policy” page, and then click “Next”.
- The next page that comes up is the “Audit Policy Summary”, here you will select “SCWAudit.inf”, click “Next”.
- Now, click “Next” on the “Save Security Policy”.
- Name the Security Policy “isasecpol” and click “Next”.
- Close the “SCW Viewer”.
- Choose “Apply Now”.
- Click “Next” on “Applying Security Policy” and on the next page click “Finish”.

## Hardware Settings

- Ensure two (2) network interface cards are installed.
- Configure the Internal NIC to use the Internal DNS Server. *NOTE: Make sure DNS is only setup on the Internal NIC for the Forwarding DNS Server.*
- Under “Network Connections”, choose “Advanced > Advanced Settings”. Make sure the Internal NIC is at the top of the list.
- Configure the External NIC to use the External Gateway.

## Internet Security and Acceleration 2004

- Install ISA 2004 after Windows 2003 Server is installed.
- Verify ISA 2004, Service Pack 1, is installed.
- Enable “Edge Firewall Policy” inside ISA Server.
  - On the “Welcome to the Network Template Wizard”, click “Next”.
  - On the “Export the ISA Server Configuration” page, click the “Export” button. Click “Next”. Select the appropriate name and destination per present policies and save the configuration files.
  - Place checks in both the “Export User Permission settings” and “Export Confidential Information (encryption will be used)” selection areas.
  - Now on the “Set Password” page, enter an appropriate strong password and save it. Click “Ok” on the export dialog box and then click “Next”.

On the Internal Addresses page, add the Internal Addresses for the network. These are the “PRIVATE” addressing scheme used. Click “Next”.

Choose “Restricted Web Access – ISP network services” and click “Next”.

Review the settings and finish the wizard.

I hereby accept this checklist as being complete and understand that failure to comply with any part specifically defined will result in termination of my position with NSF, Inc. Individuals must remit this document to ISSM before device is connected to the network for supervisor approval.

Employee: \_\_\_\_\_ Signature: \_\_\_\_\_

Supervisor: \_\_\_\_\_ Signature: \_\_\_\_\_

