

# **SGSI SISTESEG ESTANDAR DE CONFIGURACION FIREWALL**

**DOCUMENTO GUIA**

## ***INDICE***

<i><b>1 INTRODUCCIÓN.....</b></i>	<i><b>3</b></i>
<i><b>2 ALCANCE.....</b></i>	<i><b>3</b></i>
<i><b>3 DETALLE DEL ESTANDAR.....</b></i>	<i><b>3</b></i>
<i><b>3.1 CONFIGURACION.....</b></i>	<i><b>4</b></i>

## **1 Introducción**

Este documento describe el estándar de configuración del firewall que debe ser utilizado por SISTESEG con el fin de mantener una red más segura, lo anterior con el fin de prevenir interrupciones al servicio producidos por amenazas de tipo accidental o intencional que pueda ingresar al perímetro de la red o a los sistemas de información. Este estándar es parte integral del modelo SGSI.

## **2 Alcance**

El alcance de este estándar de configuración cubre los firewalls que protegen el perímetro de la red local.

## **3 Detalle del estándar**

El objetivo del estándar de configuración de firewall es poder prevenir, detectar y corregir los eventos ocasionados por la presencia de código malicioso en el perímetro de la red.

### **Responsables de la configuración**

Oficial de seguridad.  
Gerente de sistemas  
Administrador IT  
Comité de Seguridad

### 3.1 CONFIGURACION ESTANDAR DE CONFIGURACION FIREWALL

ITEMS	ESTANDAR DE SEGURIDAD
<b>1. Recomendaciones generales para la configuración del firewall.</b>	<ol style="list-style-type: none"><li>1. No se recomienda la conexión remota al firewall. En caso de necesitarse, se debe implementar un protocolo seguro como IPSEC, utilizando 3DES o AES.</li><li>2. Se debe configurar el firewall como "fail closed", es decir en caso de que se produzca algún error, el firewall automáticamente cerrará todas las conexiones.</li><li>3. Se deben utilizar rutas estáticas en lugar de protocolos dinámicos como RIPv1, RIPv2 u OSPF.</li><li>4. El sistema operativo debe estar actualizado con las últimas versiones recomendadas por el fabricante (Ver estándares de configuración para el sistema operativo) con el fin de garantizar la seguridad en la plataforma y así evitar vulnerabilidades a diferentes tipos de ataques.</li><li>5. La aplicación del firewall debe estar con las últimas actualizaciones disponibles.</li><li>6. Se recomienda tener la última versión de la aplicación.</li><li>7. En caso de envío de información confidencial, esta debe pasar por el firewall en forma encriptada, usando algoritmos como: 3DES o AES.</li><li>8. Se recomienda implementar un mecanismo de contraseña única para los administradores del firewall.<ol style="list-style-type: none"><li>1. Complejidad contraseñas<ul style="list-style-type: none"><li>• Debe tener números, letras y caracteres especiales</li><li>• De conocimiento del administrador IT y su asistente</li></ul></li></ol></li><li>1. El sistema operativo donde esté funcionando el firewall deberá estar configurado en forma segura. (ver estándares de configuración del sistema operativo) y en lo posible durante su puesta en marcha, sólo instalar los servicios estrictamente requeridos.</li></ol>
<b>2. Parámetros de Seguridad</b>	<ol style="list-style-type: none"><li>1. Se deben deshabilitar puertos físicos no utilizados, si existiesen.</li><li>2. Se deberán deshabilitar todos los puertos lógicos que no se estén utilizando.</li><li>3. No se debe usar o habilitar los servicios de Telnet o FTP.</li><li>4. Se deben utilizar todas las posibles herramientas que posea el firewall para evitar ataques de negación de servicio. (DOS)<ol style="list-style-type: none"><li>a. Habilitar función de detección de intrusos</li></ol></li><li>5. Se deberán bloquear los accesos de JavaScript, VBScript, Applets y ActiveX a la red interna.</li><li>6. En caso de no necesitarse enrutamiento, se debe habilitar la función de stealth, para que el firewall no sea visible a posibles intrusos, y evitar así un ataque de negación de servicio.</li><li>7. Siempre se deberán utilizar reglas donde quede bien claro que máquina se</li></ol>

puede conectar con otra y tratar de no utilizar reglas genéricas Source=ANY, Destination=ANY.

8. Se deberá configurar el TCP Session Timeout en 800 segundos, para reducir el riesgo de recibir una negación de servicio.(DOS)
9. Se recomienda la inspección profunda en el paquete (Deep Packet Inspection) con el fin de evitar que ciertos virus o gusanos penetren en la red y causen pérdida de productividad o disponibilidad.
10. Las comunicaciones de terceros, contratistas u oficinas remotas, deben usar tecnología VPN, conjugando el uso de protocolos de encriptación y de autenticación. Además deben pasar por el firewall encriptadas o terminar en él.
11. Habilitar HTTP para navegar la Internet
12. Habilitar SMTP para el correo electrónico
13. Habilitar DNS
14. Habilitar SMTPS
15. Habilitar IKE client

### **3. Administración**

1. Deshabilitar todo servicio relacionado con la administración que no se esté usando.
2. Cualquier actividad de modificación de una regla del firewall o configuración, debe estar soportada por un procedimiento formal y su respectiva autorización por parte del oficial de seguridad, además de documentarse amplia y detalladamente todas estas actividades.
3. Se debe utilizar alguna herramienta que permita monitorear o administrar los eventos ocurridos en el firewall, tales como intentos de violación en el acceso o de las reglas y esto se debe hacer semanalmente o cuando algún suceso así lo amerite.

### **4. Auditoría**

1. Se deberá habilitar el servicio de registro de eventos, con su correspondiente huella de tiempo, además de definir el tamaño de la memoria a utilizar.
2. Se debe utilizar un servidor de registros (syslog).
3. En el servidor de registros; habilitar huella de tiempo (Timestamps) para facilitar la correlación de eventos a futuro.
4. Se deben hacer respaldo de los registros generados semanalmente.
5. Se deben hacer periódicamente pruebas de penetración sobre el firewall, para estimar su efectividad ante posibles nuevos ataques.

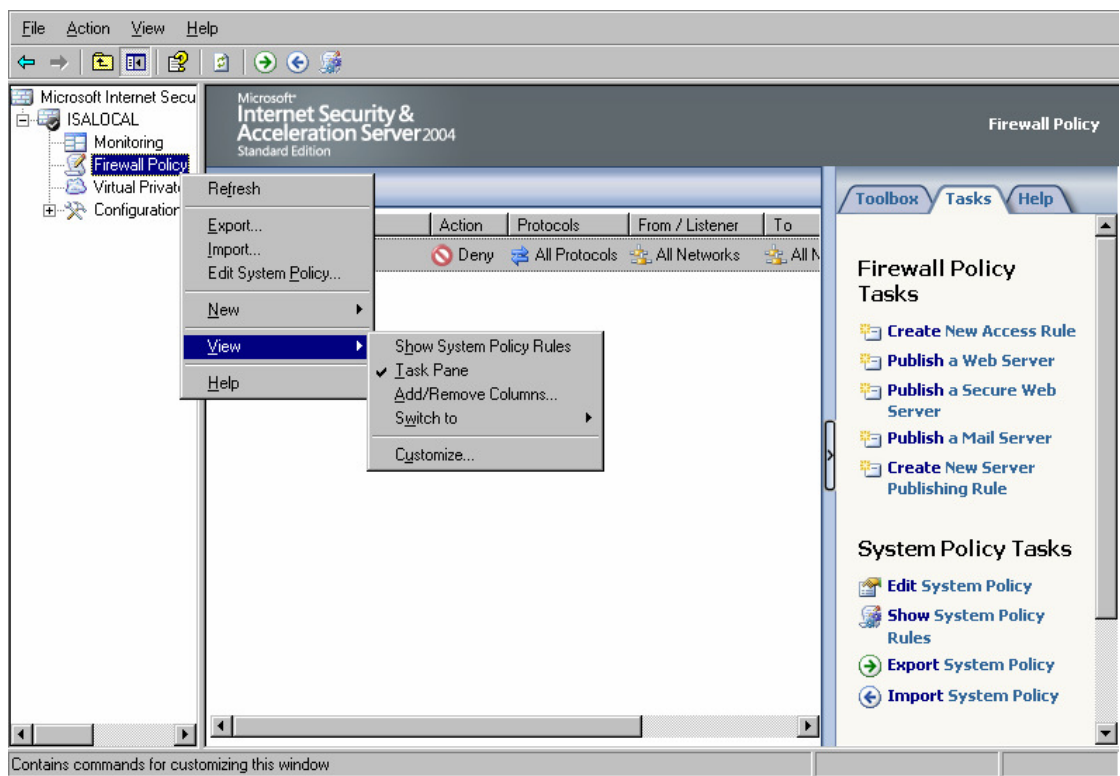


Figura 1. Ventana de control del firewall

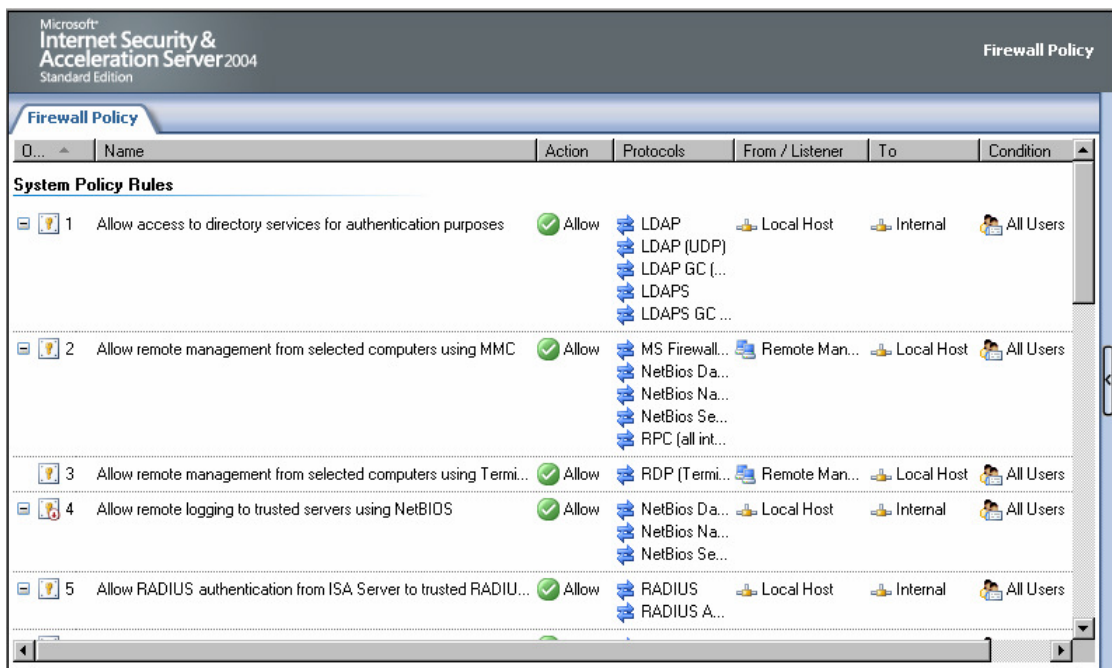


Figura 2. Reglas de firewall.

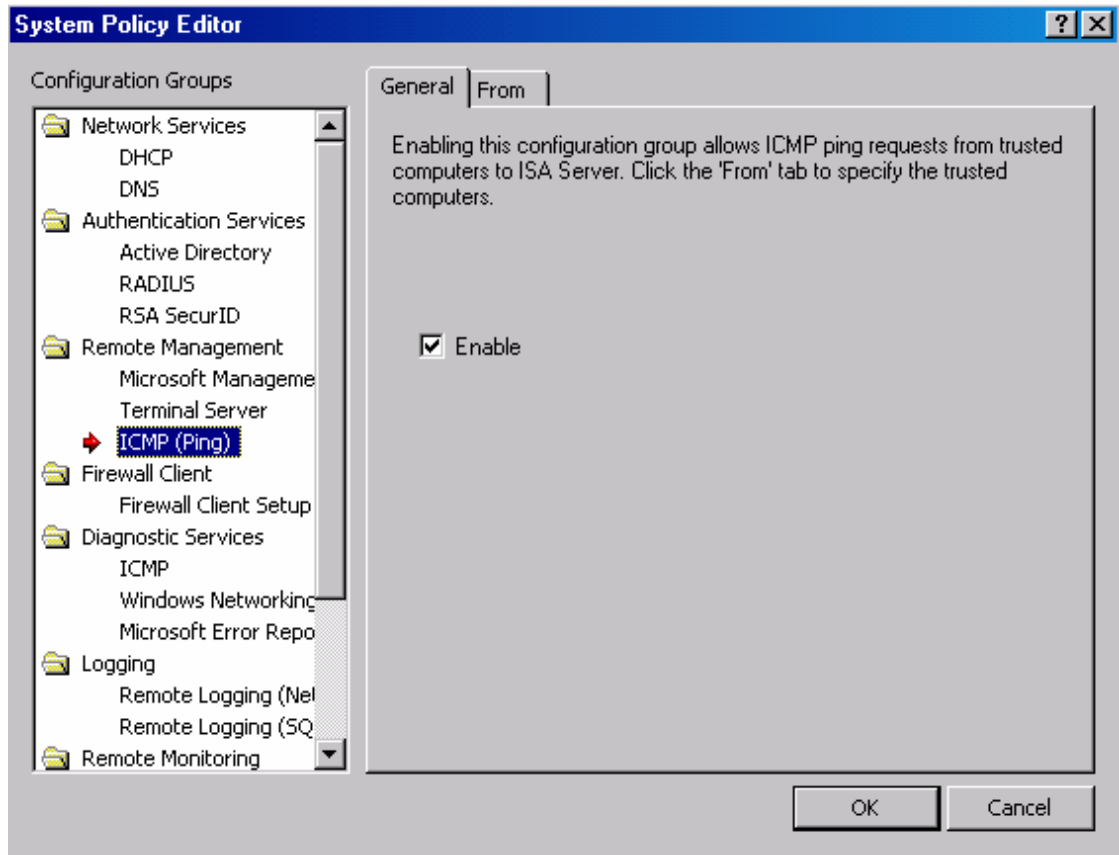


Figura 3. System policy editor



Order	Name	Action	Protocols	From	To	Condition
1	Allow access to directory services for authentication purposes	Allow	LDAP LDAP(GC) LDAP(UDP) LDAPS LDAPS(GC)	Local Host	Internal	All Users
2	Allow Remote Management using MMC	Allow	Microsoft Firewall Control RPC(all interfaces) NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Remote Management Computers	Local Host	All Users
3	Allow Remote Management using Terminal Server	Allow	RDP(Terminal Services)	Remote Management Computers	Local Host	All Users
4	Allow remote logging to trusted servers using NetBIOS	Allow	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Local Host	Internal	All Users
5	Allow RADIUS authentication from ISA Server to trusted RADIUS servers	Allow	RADIUS RADIUS Accounting	Local Host	Internal	All Users
6	Allow Kerberos authentication from ISA Server to trusted servers	Allow	Kerberos-Sec(TCP) Kerberos-Sec(UDP)	Local Host	Internal	All Users
7	Allow DNS from ISA Server to selected servers	Allow	DNS	Local Host	All Networks	All Users
8	Allow DHCP requests from ISA Server to all networks	Allow	DHCP(request)	Local Host	Anywhere	All Users
9	Allow DHCP replies from DHCP servers to ISA Server	Allow	DHCP(reply)	Anywhere	Local Host	All Users
10	Allow ICMP (PING) requests from selected computers to ISA Server	Allow	Ping	Remote Management Computers	Local Host	All Users
11	Allow ICMP requests from ISA Server to selected servers	Allow	ICMP Information Request ICMP Timestamp Ping	Local Host	All Networks	All Users
12 <sup>1</sup>	Allow VPN client traffic to ISA Server	Allow	PPTP	External	Local Host	All Users
13 <sup>2</sup>	Allow VPN site-to-site to ISA Server	Allow		External IPSec Remote Gateways	Local Host	All Users
14 <sup>2</sup>	Allow VPN site-to-site from ISA Server	Allow		Local Host	External IPSec Remote Gateways	All Users
15	Allow Microsoft CIFS protocol from ISA Server to trusted servers	Allow	Microsoft CIFS(TCP) Microsoft CIFS(UDP)	Local Host	Internal	All Users
16 <sup>7</sup>	Allow Remote logging using	Allow	Microsoft SQL(TCP)	Local Host	Internal	All Users

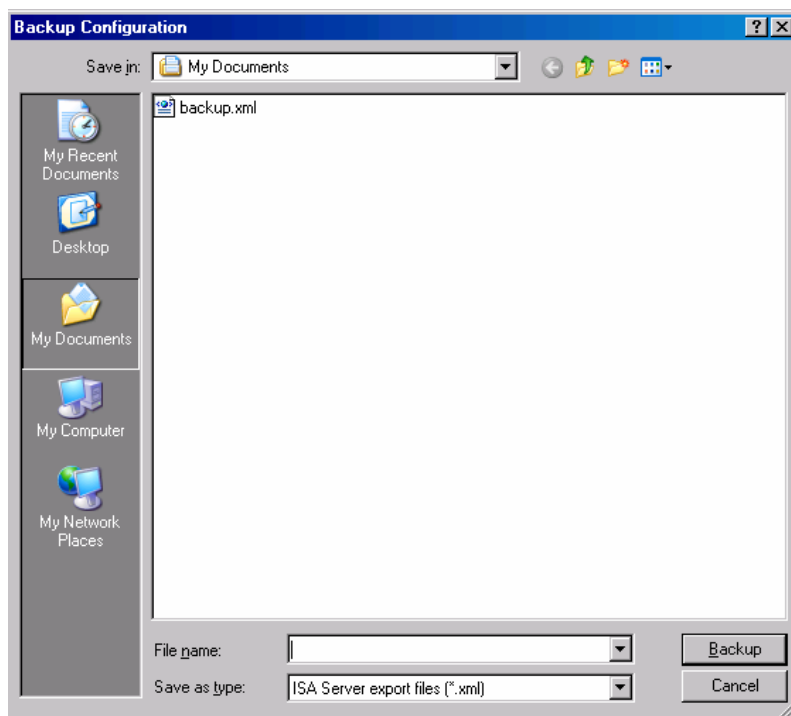
Order	Name	Action	Protocols	From	To	Condition
	Microsoft SQL protocol from firewall to trusted servers		Microsoft SQL(UDP)			
17	Allow HTTP/HTTPS requests from ISA Server to specified sites	Allow	HTTP HTTPS	Local Host	System Policy Allowed Sites	All Users
18 <sup>3</sup>	Allow HTTP/HTTPS requests from ISA Server to selected servers for HTTP connectivity verifiers	Allow	HTTP HTTPS	Local Host	All Networks	All Users
19 <sup>8</sup>	Allow access from trusted computers to the Firewall Client installation share on ISA Server	Allow	Microsoft CIFS(TCP) Microsoft CIFS(UDP) NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Internal	Local Host	All Users
20 <sup>9</sup>	Allow remote performance monitoring of ISA Server from trusted servers	Allow	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Remote Management Computers	Local Host	All Users
21	Allow NetBIOS from ISA Server to trusted servers	Allow	NetBIOS Datagram NetBIOS Name Service NetBIOS Session	Local Host	Internal	All Users
22	Allow RPC from ISA Server to trusted servers	Allow	RPC(all interfaces)	Local Host	Internal	All Users
23	Allow HTTP/HTTPS from ISA Server to specified Microsoft Error Reporting sites	Allow	HTTP HTTPS	Local Host	Microsoft Error Reporting sites	All Users
24 <sup>4</sup>	Allow SecurID protocol from ISA Server to trusted servers	Allow	SecurID	Local Host	Internal	All Users
25 <sup>5</sup>	Allow remote monitoring from ISA Server to trusted servers, using Microsoft Operations Manager (MOM) Agent	Allow	Microsoft Operations Manager Agent	Local Host	Internal	All Users
26 <sup>6</sup>	Allow HTTP from ISA Server to all networks for CRL downloads	Allow	HTTP	Local Host	All Networks	All Users
27	Allow NTP from ISA Server to trusted NTP servers	Allow	NTP(UDP)	Local Host	Internal	All Users
28	Allow SMTP from ISA Server to trusted servers	Allow	SMTP	Local Host	Internal	All Users
29	Allow HTTP from ISA Server to selected computers for Content Download Jobs	Allow	HTTP	Local Host	All Networks	System and Network Service

**Tabla 1.** Reglas existentes en el ISA SERVER 2004

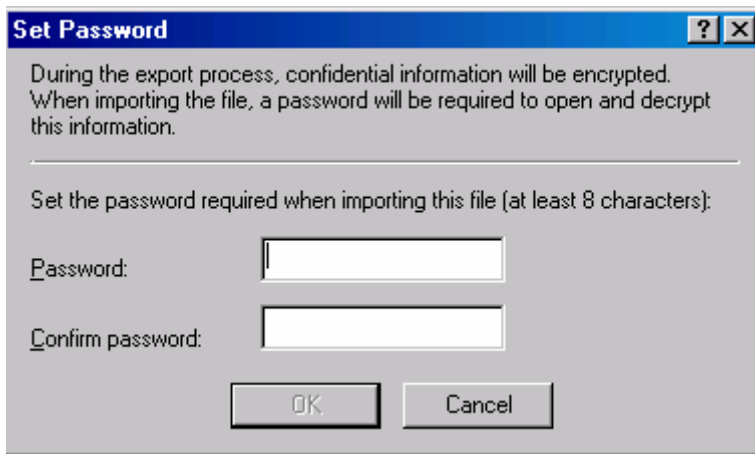
## Backing Up the Post-Installation Configuration

Perform the following steps to back up the post installation configuration:

1. Open the **Microsoft Internet Security and Acceleration Server 2004** management console and right-click the server name in the left pane of the console. Click the **Back Up** command.
2. In the **Backup Configuration** dialog box, enter a name for the backup file in the **File name** text box. Be sure to note where you are saving the file by checking the entry in the **Save in** drop-down list. In this example we will call the backup file **backup1**. Click the **Backup** button.



3. In the **Set Password** dialog box, enter a password and confirm the password in the **Password** and **Confirm password** text boxes. The information in the backup file is encrypted because it can potentially contain passwords and other confidential information that you do not want others to access. Click **OK**.



4. Click **OK** in the **Exporting** dialog box when you see the **The configuration was successfully backed up** message.

Make sure to copy the backup file to another location on the network after the backup is complete. The backup file should be stored offline on media that supported NTFS formatting so that you can encrypt the file