O|G|P

Hon. Sila M. Calderón
Gobernadora

Lcda. Melba Acosta
Directora
acostamelba@ogp.gobierno.pr

28 de agosto de 2003

MEMORANDO GENERAL NUM. 338-04

SECRETARIOS, JEFES DE AGENCIAS, DEPENDENCIAS Y CORPORACIONES PUBLICAS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

Melba Acosta
Directora

FUNCIONAMIENTO DE LOS PROGRAMAS ANTIVIRUS

Luego del reciente incidente de ataques de virus a través de la Red, nos vemos precisados a enfatizar en aspectos importantes de la seguridad de nuestros sistemas. La Oficina de Gerencia y Presupuesto, por conducto de la División de Tecnologías de Información Gubernamentales, continuamente envía a cada agencia copia de los avisos de seguridad relacionados a la protección de los sistemas de información que poseen las agencias. Adicionalmente, ofrecemos el producto de Antivirus y el servicio de actualización del mismo. Este servicio, de carácter proactivo, tiene la finalidad de mantener a las agencias protegidas de cualquier incidente que pueda amenazar y causar pérdidas significativas, tanto a sus sistemas de información como a los de las agencias que comparten la red interagencial.

A raíz del reciente ataque, hemos confirmado que el producto de Antivirus no está siendo actualizado como debe hacerse. Es imperativo que el personal de sistemas de cada agencia se mantenga informado a través de los avisos y ponga a funcionar debidamente el mecanismo de antivirus dentro de los próximos siete días naturales. De lo contrario, nos veremos obligados a interrumpir el servicio de Internet a las agencias que no cumplan con el propósito de proteger a la red interagencial. La falta de cooperación de alguna agencia individual pone en riesgo a los sistemas generales compartidos.

De necesitar ayuda técnica para cumplir con este aviso, favor de comunicarse con el Centro de Servicios vía teléfono al 787-729-0125, 0126, 0129 ó 0130, o vía correo electrónico (servicecenter@ogp.gobierno.pr), quienes estarán en la mejor disposición de cooperar con ustedes. Apreciamos y agradecemos su compromiso con la protección de nuestra red interagencial.

Anejo: Procedimiento para conectar antivirus.

I. Norton AntiVirus Server:

1. Caso: Cuando el servidor de AntiVirus reside en la misma máquina donde el ISA Server reside.

A. **ISA Management**:
Access Policy
IP Packets Filters
Create a Packet Filter
**deben de escribir la siguiente información:
IP packet filter name: **Norton (esto es estético, puede ser cualquier nombre, solo es para identificar el packet filter)**
Filter mode: **Allow packet transmission**
Filter type: **Custom**
Filter settings
IP protocol: **UDP**
Direction: **Both**
Local ports:**2967**
Remote ports: **All ports**
Local computer: **Default IP address for each external interface on the ISA server computer**
Remote Computer
Only this remote computer: **64.185.222.63**

B. **ISA Management**:
Access Policy
IP Packets Filters
Create a Packet Filter
**deben de escribir la siguiente información:
IP packet filter name: **Norton (esto es estético, puede ser cualquier nombre, solo es para identificar el packet filter)**
Filter mode: **Allow packet transmission**
Filter type: **Custom**
Filter settings
IP protocol: **UDP**
Direction: **Both**
Local ports:**38293**
Remote ports: **All ports**
Local computer: **Default IP address for each external interface on the ISA server computer**
Remote Computer
Only this remote computer: **64.185.222.63**

**este puerto es el que me permite ver que el servidor de Norton de cada agencia esté "up to date" en los dat's files.
**deben de repetir todos los pasos para el protocolo 38293

2. Caso: Cuando el servidor de AntiVirus reside detras de el ISA Server.

ISA Management:

1. Definir los "IP Packets Filters":
Access Policy
IP Packets Filters
Create a Packet Filter

**deben de escribir la siguiente información:
IP packet filter name: **Norton port 2967 (esto es estético, puede ser cualquier nombre, solo es para identificar el packet filter)**
Filter mode: **Allow packet transmission**
Filter type: **Custom**
Filter settings
IP protocol: **UDP**
Direction: **Both**
Local ports:**2967**
Remote ports: **All ports**
Local computer: **Default IP address for each external interface on the ISA server computer**
Remote Computer
Only this remote computer: **64.185.222.63**
Finish

2. Definir los "Protocols Definitions":
Policy Elements
Protocols Definitions
Create a Protocol Definition
**deben de escribir la siguiente información:
Protocol Definition Name: **NAV port 2967 (esto es estético, puede ser cualquier nombre, solo es para identificar el protocol definition)**
Primary Connetion Information
Port Number: **2967**
Protocol Type: **UDP**
Direction: **Received/Send**
Secondary Connetions: **Next**
Finish

2a. Editar el "Protocol Definition" creado:
Double-Click al protocolo creado
Ir al tab de **"Parameters"**
Darle **"Add"**
Port Range
From: **2967**
To: **2967**
Protocol Type: **UDP**
Direction: **Send/Received**
OK
repetir el paso **2a pero en **Direction** escribir **Received/Send**

3. Crear un "Client Address Set"
Policy Elements
Client Address Set
Create a Client Set
**deben de escribir la siguiente información:
Name: **NAV Server (esto es estético, puede ser cualquier nombre, solo es para identificar el client address set)**
Darle **"Add"**
Client Set IP Address
From: IP del servidor de Norton AntiVirus
To: IP del servidor de Norton AntiVirus
OK
OK

4. Pubilcar el servidor

Publishing

Server Publishing Rule

Publish a Server

**deben de escribir la siguiente información

Server Publishing Rule Name: **NAV Server 2967 (esto es estético, puede ser cualquier nombre, solo es para identificar el servidor)**

Address Mapping

IP address of the internal server: **IP del servidor de Norton AntiVirus**

External IP address on ISA Server: **IP válido del ISA Server**

Protocols Settings

Apply the rule to this protocol: **buscar el "protocol definition" creado**

Client Type

Apply the rule to requests from: **Specified computers (client address sets)**

Client Sets

Add

Buscar el "client address set" creado

Add

OK

Next

Finish

****deben de repetir todos los pasos exepto el #3 para el protocolo 38293**