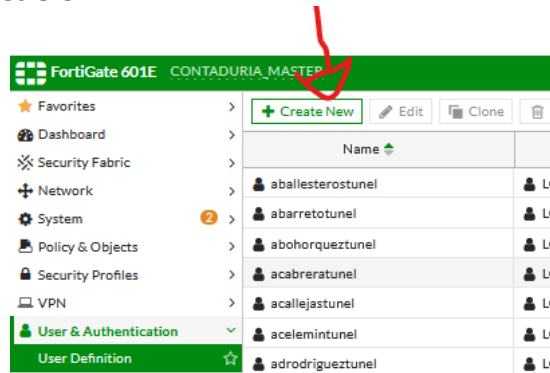


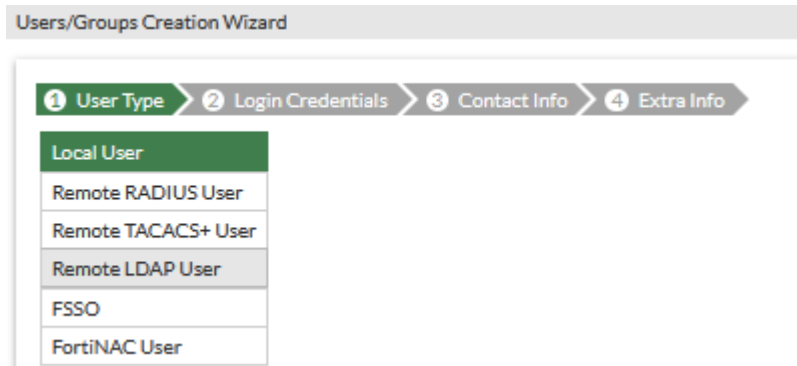
CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	1 de 10

CREACION USUARIO ACCESO VPN

1. User & Authentication

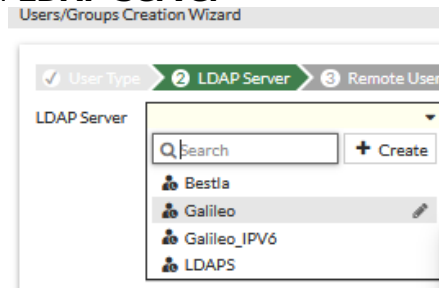


Ingresar en **Create New** y selecciones **Remote LDAP User**.



Click en Next

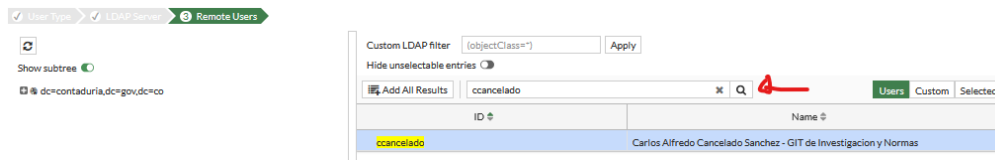
1.1 Seleccione **Galileo** en **LDAP Server**



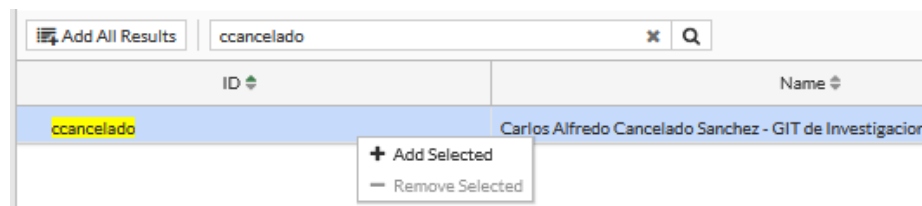
CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	2 de 10

Click en Next

1.2Escriba el nombre del usuario y de click en **Buscar** (Lupa)

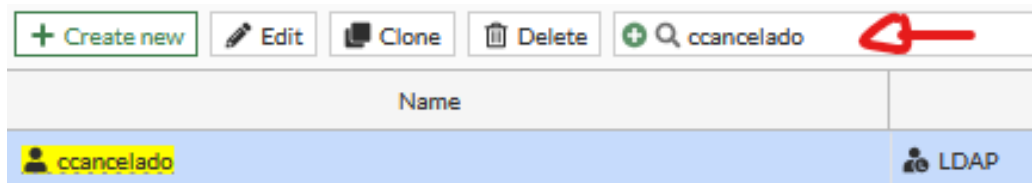


Seleccione el usuario y de click Derecho en el Mouse y selección **Add Selected**



Y de click en **Submit**.

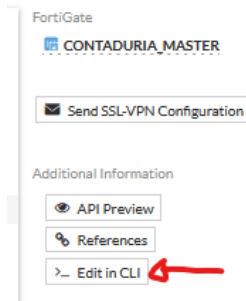
2. En **Search** ingrese el nombre del usuario y de Enter



Seleccione el usuario y de click en **Edit**

2.1. En **Additional Information** de click en **Edit in CLI**

CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	3 de 10



2.2. Escriba en su orden los siguientes comandos: en cada uno finalice con **Enter**

```
set two-factor email
set email-to 'correo-institucional-usuario'
end
```

```

CLI Console (2)
CONTADURIA_MASTER # config user local
CONTADURIA_MASTER (local) # edit "ccancelado"
CONTADURIA_MASTER (ccancelado) # show
config user local
  edit "ccancelado"
    set type ldap
    set ldap-server "Galileo"
  next
end
CONTADURIA_MASTER (ccancelado) # set two-factor email
CONTADURIA_MASTER (ccancelado) # set email-to 'ccancelado@contaduria.gov.co'
CONTADURIA_MASTER (ccancelado) # end
  
```

Cierre la ventana de CLI.

2.3. De click en **OK**

Edit User

Username

ccancelado

User Account Status

Enabled

Disabled

User Type

Remote LDAP User

LDAP Server

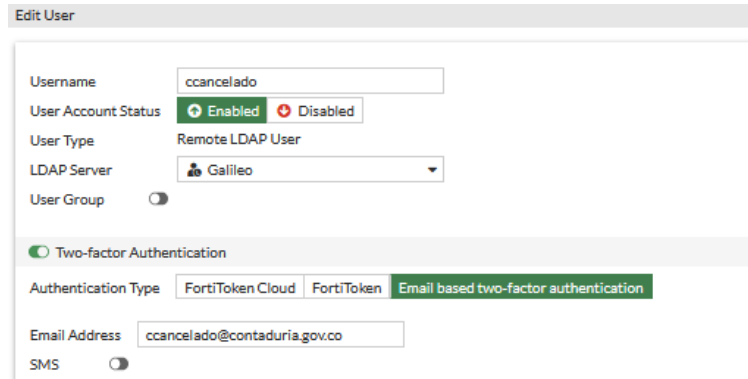
Galileo

User Group

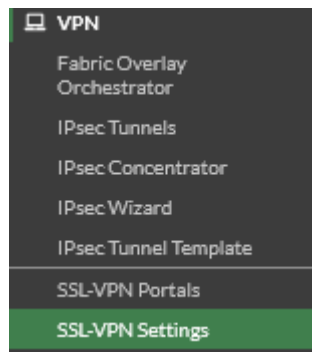
Two-factor Authentication

CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	4 de 10

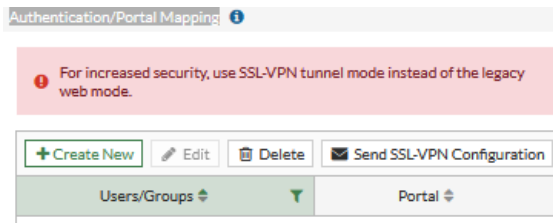
Si realiza la búsqueda nuevamente del usuario y edita la información le debe aparecer de esta forma:



3. En el menú seleccione **VPN** y seleccione **SSL-VPN Settings**



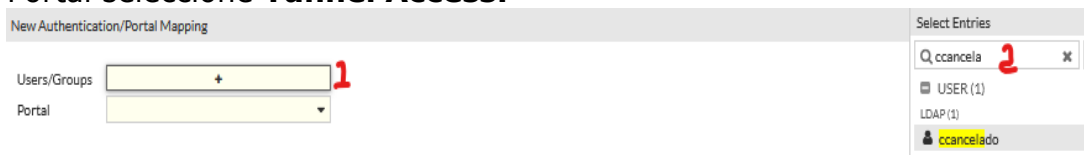
3.1 En **Authentication/Portal Mapping** de Click en Create New



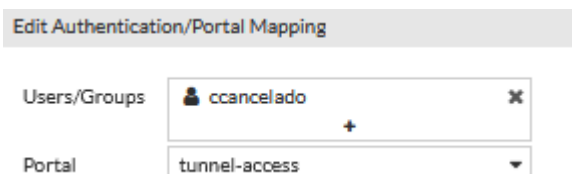
CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	5 de 10

3.2 De click en **Users/Groups (1)** y busque el nombre del usuario, de click sobre el nombre del usuario (2).

En Portal seleccione **Tunnel Access**.



De click en **OK**



De click en **Apply**

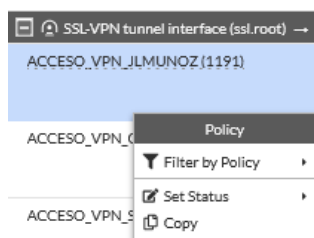
CREACION DE LAS POLÍTICAS VPN

4. En el menú seleccione **Policy & Objects** Seleccione **Firewall Policy**

4.1. Si es para conexión a **RDP (Escritorio Remoto)**, busque la siguiente sección:

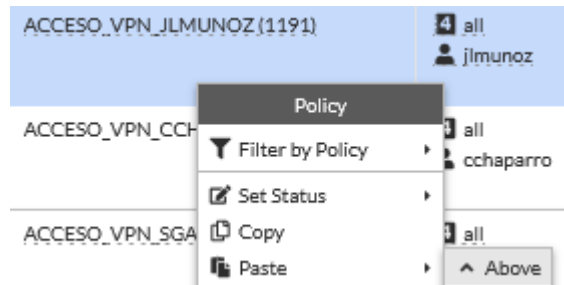


4.2. Seleccione la Primera política, de click Derecho y click en **Copy**



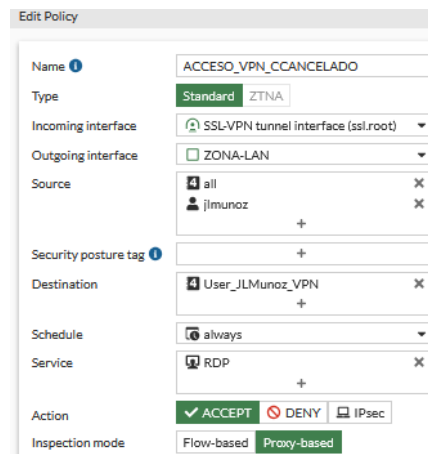
CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	6 de 10

Sobre esa misma política de click derecho y click en Paste/Above

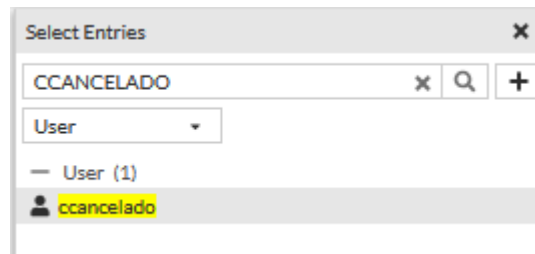


4.3. De doble click sobre la política pegada

De click en la sección de Source



En **Search** escriba el nombre del usuario y Seleccione **User**



CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	7 de 10

De click sobre el usuario y le debe aparecer agregado en **Source**

Name i

Type Standard ZTNA

Incoming interface SSL-VPN tunnel interface (ssl.root)

Outgoing interface ZONA-LAN

Source

all
✕

jimuno
✕

ccancelado
✕

+

Select Entries

CCANCELADO

User

— User (1)

ccancelado

Elimine el usuario adicional dando click sobre la **x**

4.4. De click en la sección **Destination**

De click en el signo **+** y Selecciones **Address**

Select Entries

Q
+

Address

— Address

FABRIC_DEVICE

FIREWALL_AUTH_PORTAL_ADDRESS

SSLVPN_TUNNEL_ADDR1

Cree el nuevo Objeto de Usuario ingresando el Nombre y la dirección **IP/Netmask** del equipo de oficina asignado.

New Address

Name

Color Change

Interface any

Type Subnet

IP/Netmask

Static route configuration ☐

Comments 0/255

De click en **OK** y en **OK**

Elimine el usuario adicional dando click en la **X**

CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	8 de 10

Security posture tag  +

Destination

4 User_JLMunoz_VPN
×

4 User_CCancelado_VPN
×

+

Schedule
 always

Service

 RDP
×

+

Y al final todo debe quedar así:

Edit Policy

Name  ACCESO_VPN_CCANCELADO

Type Standard ZTNA

Incoming interface
 SSL-VPN tunnel interface (ssl.root)

Outgoing interface
 ZONA-LAN

Source

4 all
×

 ccancelado
×

+

Security posture tag  +

Destination

4 User_CCancelado_VPN
×

+

Schedule
 always

Service

 RDP
×

+

Action
✓ ACCEPT
✗ DENY
IPsec

Inspection mode
Flow-based
Proxy-based

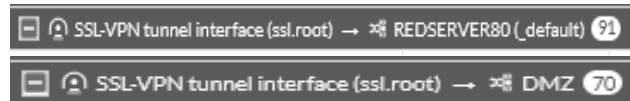
4.5. Habilite la política (Enable this Policy) y de click en **OK**

Enable this policy 

OK

CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	9 de 10

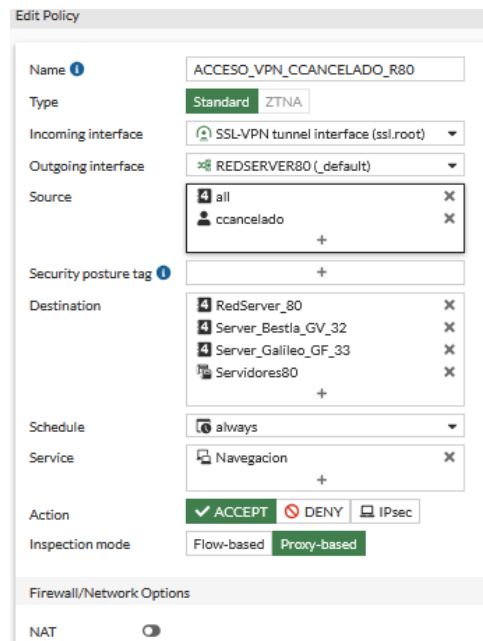
5. Si es conexión a VPN Directa entonces se deben crear las políticas sobre las secciones de REDSERVER80 Y DMZ



Siga los mismos pasos indicados en los ítems 4.2 y 4.3

Al final debe quedar algo así:

En el nombre de la política finalícelo con R80 para este caso.



Para la sección de Destination déjelos tal cual sin hacer ningún cambio al menos que se necesite agregar un puerto o protocolo si lo requiere para acceder a alguna aplicación.

Habilite la política y de **OK**.

CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
21/07/2026	GTI05-INS04	2	10 de 10

Enable this policy ☒

OK

6. Creación de la política de VPN Directa sobre la DMZ.

Edit Policy

Name ⓘ

ACCESO_VPN_CCANCELADO_DMZ

Type

Standard
ZTNA

Incoming interface

SSL-VPN tunnel interface (ssl.root)

Outgoing interface

DMZ

Source

all

ccancelado

Security posture tag ⓘ

Destination

Red_DMZ

Schedule

always

Service

Navegacion

Action

ACCEPT
DENY
IPsec

Inspection mode

Flow-based
Proxy-based

Firewall/Network Options

NAT

Enable this policy ☒

OK

7. Enviar el correo electrónico al usuario con el instructivo de VPN y el de Pathfinder sobre VPN.