



# Claró-cloud

## Manual de Usuario

Como conectarnos a nuestro  
Datacenter Virtual



Es simple



# Conexión a Datacenter Virtual Claro Cloud

## Primeros Pasos



Este manual cubre el procedimiento estándar para realizar una conexión a tus servidores virtuales contenidos en el Datacenter Virtual (DCV) Cloud contratado.

Podrás conectarte vía VPN (utilizando el programa *\*Cisco VPN Client*) o bien desde tu segmento público, mediante la carga de reglas de FW, configurado origen IP publica de tu ISP y destino un Servidor Virtual. Más adelante lo veremos con mayor detalle.

Como dato adicional le recordamos que es indispensable para establecer cualquier tipo de conexión crear las reglas en el firewall en su panel de control para que de esta manera se pueda acceder a los servidores.

No olvides consultar le Manual de **“Mejores Practicas Infraestructura como Servicio Claro.pdf”** donde en cual encontraras información muy útil para darle mayor robustez y seguridad a tus entornos de computación en la nube de Claro, accede al documento desde [aquí](#).

### VPN

El perfil VPN (archivo de perfil “.pcf”), segmento de red de tu VPN y credenciales de acceso para la conexión VPN las recibirás por mail previamente de parte del equipo de Activaciones Cloud.

**Importante:** recordar modificar la contraseña de acceso a tu Panel de Control Claro Cloud, luego de realizar el primer logueo.

\*Para verificar el proceso de instalación del Cisco VPN Client, haga clic [aquí](#).

**Claro<sup>o</sup>-cloud**

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS

[www.cloud.claro.com.ar](http://www.cloud.claro.com.ar)  
[sopORTEcloud@claro.com.ar](mailto:sopORTEcloud@claro.com.ar)



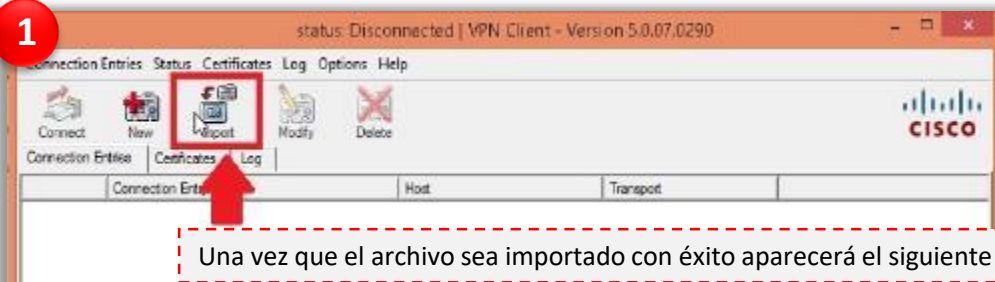
0800-12-CLOUD(25683)



## Establecer conexión VPN


En principio, debes establecer la conexión VPN con el Datacenter Cloud. Para esto tienes que abrir la aplicación “Cisco VPN Client” e importar (*import*) el archivo .pcf indicándole al programa la ruta donde guardo el archivo.

**1**

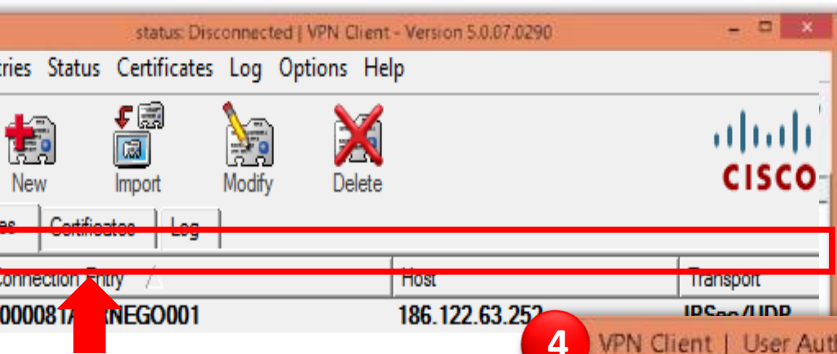


Una vez que el archivo sea importado con éxito aparecerá el siguiente mensaje.

**2**

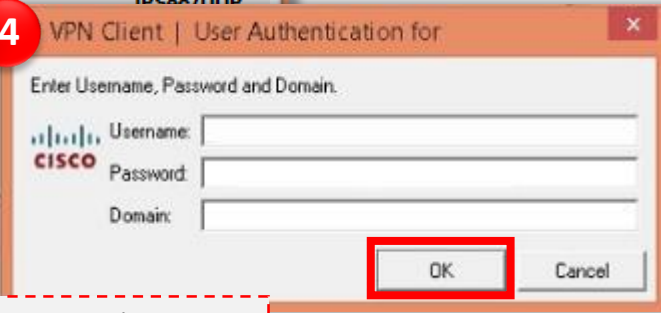


**3**




Al hacer un “doble click” sobre la conexión se le solicitará que ingrese las credenciales de acceso. Que le fueron provista vía email. No es necesario completar el campo “domain”

**4**



Quando nos conectemos aparecerá este mensaje, simplemente presionamos el botón “Continue”



POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS



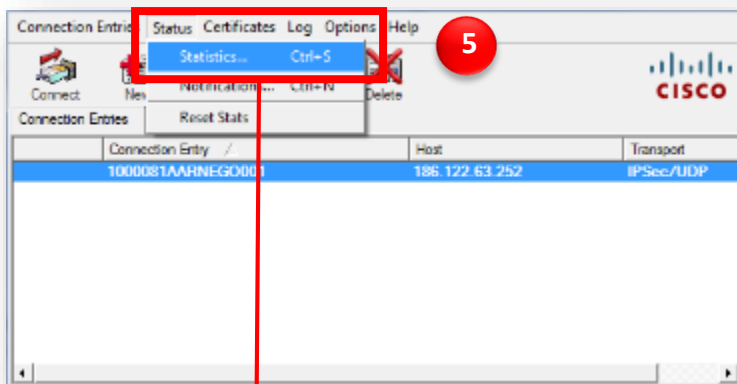


## Establecer conexión VPN

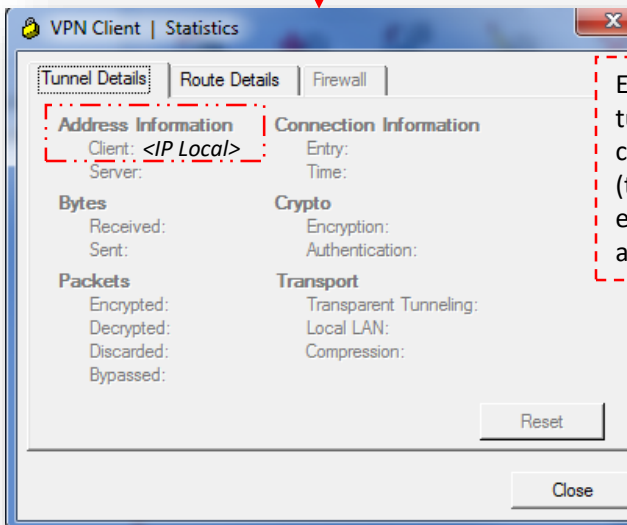


En este momento, ya estableciste la conexión VPN, ahora en menú de opciones, selecciona Status y del menú despegable selecciona *Statistics*.

Allí encontraras datos que serán útiles para para generar las reglas del firewall exitosamente. Ten en cuenta donde obtener estos datos luego.



De la ventana de Statistics, hay que observar las solapas "Tunnel Details"



En **Tunnel Details** veras la IP asignada a tu computadora. Ese dato lo usaras como "IP ORIGEN" en la regla de Firewall (también se especifica el rango completo en la planilla que se envía desde activaciones)

- Con esta IP podrás generar una regla con protocolo IP, la cual te permitirá todo el trafico desde tu red hasta el servidor en el que cargues la regla, mas adelante la veremos en detalle.

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS

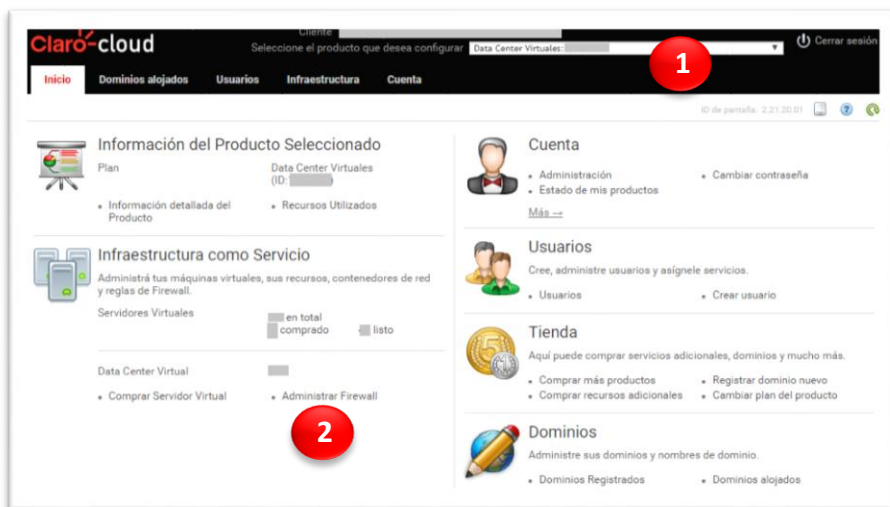




## Generación de reglas de Firewall Cloud



Para generar reglas en el Firewall Cloud tienes que dirigirte a tu panel de control Claro Cloud, seleccionar el producto Data Center Virtual y desde allí ingresar en la opción “Administrar Firewall”. Se abrirá el portal de gestión de reglas de FW, desde donde podrás hacer alta y baja de reglas.



### Repasemos algunas consideraciones, y terminologías, antes de ingresar a configurar tus reglas de firewall

- Cada regla se debe crear para cada servidor que la requiera, no se podrá generar una única regla para toda la red, sin embargo, lo que se puede hacer en particular para ingresar a administrar los servidores, es dar acceso a un servidor, y desde ese conectarse al resto (Jump de servidores)
- Veremos que según el tipo de DCV que hayamos contratado, cuando creamos las reglas, nos pedirá que elijamos sobre que Tarjeta de red aplicar la regla. Puede ser NIC0 o NIC1, en general las reglas deberán cargarse sobre la NIC0 que es la que red publica, prestar atención a la dirección de IP que el sistema mostrara por cada NIC en el 3er paso de la carga de reglas, serán las mismas que veras desde tu control panel , en la sección **Red** de cada uno de tus servidores virtuales.
- Una vez creada cada regla no podrán editarse, deberás eliminarla y crearla nuevamente si así lo deseas.

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Acceso a la administración de Reglas de Firewall Cloud



A continuación detallamos los primeros pasos que siempre deberemos realizar para agregar reglas de Firewall:

1

Desde este botón abrimos el *Administrador de las reglas de FW*

Si tuvieras más de un DCV, desde aquí lo podrías seleccionar para filtrar tus SV.

Servidor Virtual	Sistema Operativo	Fecha de Creación	Estado
00-NCTest-4	Linux	05/12/2016 09:01:21 p.m.	Running
Prueba-VPN-1	Windows Server 2008 R2	09/08/2017 05:20:58 p.m.	Running
OEBUSSINESM-1	Linux	17/11/2016 04:32:31 p.m.	Running

Abajo la lista de SV asociados a tu cuenta, deberás siempre seleccionar uno antes de ingresar al administrador.

2

Manage Network Paths

Network Interface:  Server: Opencode-1

Load Balancer Pool: \*

Network Paths

+ -

Aquí podrás seleccionar la tarjeta de red

Por ultimo desde aquí podrás sumar o eliminar una regla existente.

\* **Importante:** es posible que en este lugar veas la opción de "Load Balancer o Balanceador de Carga" si es así, tené en cuenta que no es una opción habilitada

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Configuración de la primer regla de Firewall Cloud



Para poder conectarse al DCV es indispensable generar al menos una regla, la cual permitirá el tráfico desde tu origen, ya sea desde la VPN o IP pública a tu DCV. Veamos un ejemplo:

**1** Create Network Path

**Server Context**

Server: [ ]

Network Interface: NICO

**Direction\*:**  Create Inbound Network Path  
 Create Outbound Network Path

Description: [ ]

Seleccionamos la opción "Create Inbound Network Path" y podemos agregar una descripción en la parte inferior para identificar la regla.

**2** Create Network Path

**Source Endpoint**

Type\*:  Server Network Interface  
 Network Endpoint

**Network Endpoint Details**

Name\*: [ ]

Address: [ ]

Network Mask: [ ]

Host Address\*:

Network Address\*:

Network Mask\*:

Llenamos los Detalles de red del "end point" de la siguiente manera:

**Segmento de Red:**

La dirección de IP que obtuvimos desde **Tunels Details**, al momento de configurar la VPN, que es la IP DE ORIGEN de tu red.

Si vas a conectarte con mas de un usuario, en este campo deberás ingresar **la IP del segmento de red de tu VPN**(este dato te fue entregado junto con el resto de la información al momento del alta)

**Mascara de red:** la mascara de la IP DE ORIGEN, será **255.255.255.240**

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Configuración de la primer regla de Firewall Cloud



Continuando:

3

### Destination Endpoint

Type\*:  
 Server Network Interface  
 Network Endpoint  
 Load Balancer Pool

#### Server Details

Service Offering Instance\*:   
Server\*:   
Network Interface\*: NIC0  
Address:

Visualizaremos los datos cargados previamente, a modo de resumen. En esta instancias no son datos editables (los datos cargados son solo ejemplos y no representan)

4

### Create Network Path

#### Path Constraints

Source:

Transport Protocol\*: TCP  
Application Protocol:   
 Port Range:

Enter either a single port or single port range. For example: 8884 - 8890

Allow Traffic:  Locked:   
Log:  Hidden:

Destination:

Como últimos pasos tendrás que seleccionar el tipo de protocolo de transporte, por ej TCP. Y protocolo de aplicación que si no lo dejamos especificado, aplicara a todos. También podrías ingresar acceso por rango de puertos.

Es importante, seleccionar la opción de "Permitir Trafico", para que la gestión sea exitosa. **las otras opciones no están disponibles, por lo tanto "FAVOR DE NO SELECCIONARLAS"**

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Conectarse al Datacenter Virtual sin VPN Client

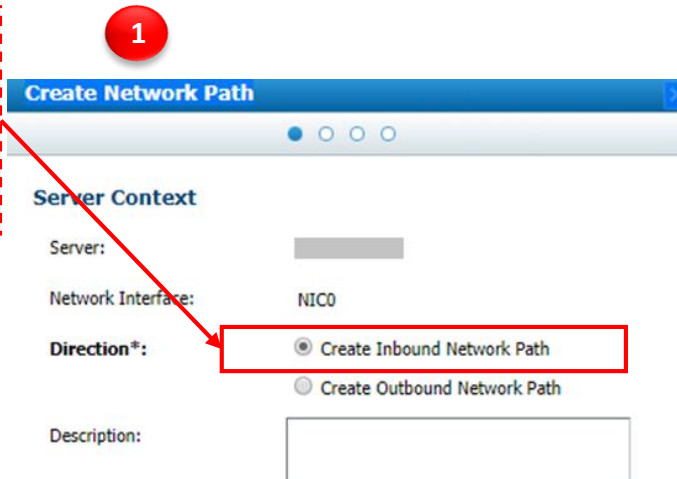


También podrás conectarte desde tu IP pública sin la necesidad de utilizar la conexión vía VPN, configurando la siguiente regla de FW sobre la interfaz de tu servidor del segmento público.

Seleccionar el contexto a donde aplicaremos la regla.

**Dirección:** Ruta de Red Interna

1



**Create Network Path**

Server Context

Server: [ ]

Network Interface: NICO

**Direction\*:**  Create Inbound Network Path  
 Create Outbound Network Path

Description: [ ]

2



**Create Network Path**

Source Endpoint

Type\*:  Server Network Interface  
 Network Endpoint

Network Endpoint Details

Name\*: [ ]

Address: [ ]

Network Mask: [ ]

**Host Address\*:** <IP pública de tu red >

Network Address\*: [ ]

Network Mask\*: [ ]

Help < Back Next > Cancel

Configurando la **IP que le asigna su proveedor de internet**, podrás obtener acceso al servidor seleccionado, desde la terminal que posee la IP indicada. Tener en cuenta que al no ser una IP estática, esta opción podría no ser la más aconsejable dado a los posibles cambios que efectúe su proveedor de internet.

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS



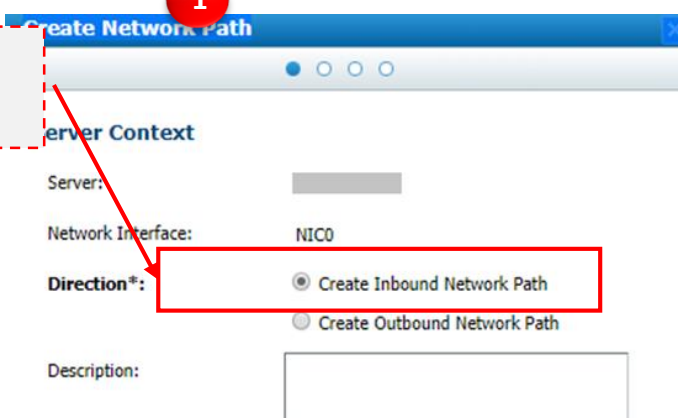


## Procedimiento para agregar ruta interna –Tipo regla Any (sin VPN)

De esta manera, podrás configurar permisos de acceso a tu DCV sin filtros o restricciones desde cualquier origen. **ESTA NO ES LA MEJOR PRACTICA, YA QUE DEJA EXPUESTA SU INFRAESTRUCTURA.**

1

Seleccionaremos en **Dirección:** ruta de red interna



**Create Network Path**

Server Context

Server: [ ]

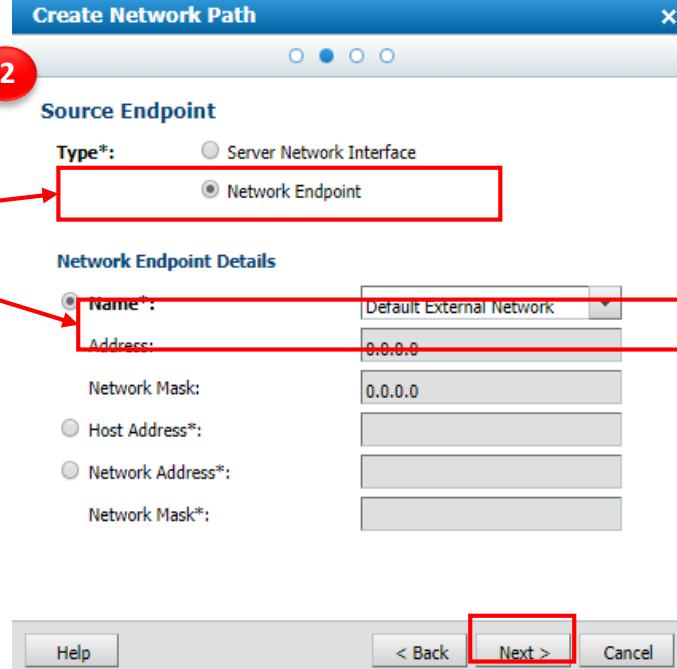
Network Interface: NIC0

**Direction\*:**  Create Inbound Network Path  
 Create Outbound Network Path

Description: [ ]

2

-En **Type** seleccionamos red de "Network Endpoint"  
-En **Name** seleccionamos "Default External Network" y  
-Finalizamos con **Next>**



**Create Network Path**

**Source Endpoint**

**Type\*:**  Server Network Interface  
 Network Endpoint

**Network Endpoint Details**

**Name\*:** Default External Network  
Address: 0.0.0.0  
Network Mask: 0.0.0.0

Host Address\*:  
 Network Address\*:  
Network Mask\*:

Help < Back **Next >** Cancel

De este modo, se completarán automáticamente los campos necesarios para habilitar el acceso desde todos los orígenes.

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





3 Nos mostrara punto de destino y detalles del servidor

### Destination Endpoint

Type\*:  Server Network Interface  
 Network Endpoint  
 Load Balancer Pool

### Server Details

Service Offering Instance\*:

Server\*:

Network Interface\*:

Address:

4 En Restricciones de ruta:  
-**Protocolo de transporte**: TCP, UDP o IP dependiendo el tipo de regla que se requiera.  
-**Protocolo de aplicación**: RDP O SSH, etc. (dependiendo el SO o puerto a habilitar)  
-Seleccionamos la casilla **Permitir Tráfico** y **“Guardar”** para aplicar los cambios.

### Create Network Path

Path Constraints

Source: Default External Network

**Transport Protocol\*:** TCP

Application Protocol:

Port Range:

Enter either a single port or single port range. For example: 8884 - 8890

**Allow Traffic:**  Locked:

Log:  Hidden:

Destination:  ->  -> NIC0

Help < Back **Save** Cancel

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Como ver si las reglas están creadas y gestionarlas

Una vez que finalizamos el proceso de creación / adición de reglas, el sistema regresara al portal general de administración.

Desde aquí podrás listar y administrar las reglas generadas. El portal podría demora unos minutos en reflejar las reglas configuradas.

1 de red gestion

Interfase de red: NICO      Servidor: RodoTestWin-2  
IP Address: 200.57.170.94

Ruta de red

1 entries returned

Enforced	Permitir tráfico	Oculto	Bloqu...	Log	Origen	Destino	Protocolo
Yes	Permit	No	No	No	External Network	SOI1730291-2->RodoTestWin-2->NICO	TCP

2

Actividad pendiente

Usuario	actividad	Avance (%)	Estatus	Tiempo de ini...	Hora de finali...	Error	Accion necesaria
tenant_admin10	Create Network: Path	100	Completed	31/08/2017 10:57	31/08/2017 11:00		

Desde aquí podrá visualizar las tareas pendientes que el gestor de configuración está procesando y el status de cada una de las modificaciones.

Ruta de red

3

1 entries returned

Enforced	Permitir tráfico	Oculto	Bloqu...	Log	Origen	Destino	Protocolo
Yes	Permit	No	No	No	External Network	SOI1730291-2->RodoTestWin-2->NICO	TCP

Intuitivamente, desde los símbolos +, podremos crear una nueva regla o desde el signo - eliminar una regla seleccionada previamente.

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS



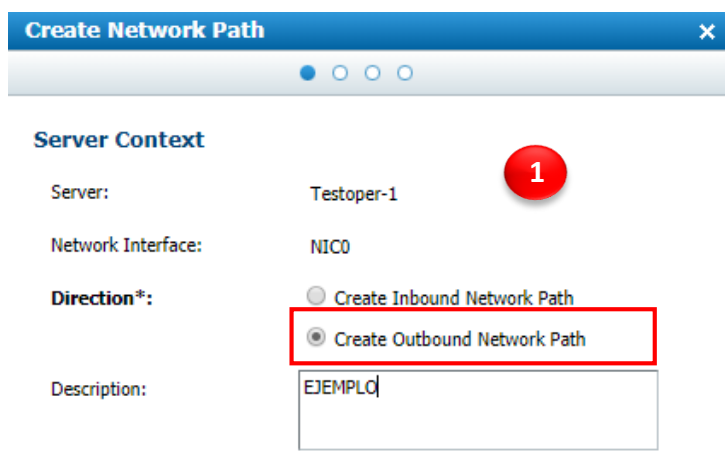


## D. Procedimiento para agregar una regla de salida (recomendamos no hacerlo a menos que tengan una política de tráfico muy estricto)

Del mismo modo que lo vimos en la pagina 6 , ingresamos al portal de administración de reglas de FW para agregar un regla. Elegimos el servidor deseado, y la tarjeta de red (NIC0 o NIC1)

IMPORTANTE: cada DCV tiene 2 reglas por Default, una bloquea todo el tráfico entrante y otra permite todo el tráfico saliente. Al cargar cualquier regla saliente, la regla implícita se borra y se bloquea el tráfico de todas las maquinas del DCV salvo lo permitido en la regla que acabamos de cargar para un SV en particular.

Habiendo seleccionado la tarjeta, por ejemplo NIC0. Seleccionamos en **Direction: Create Outbound Network Path**



**Create Network Path**

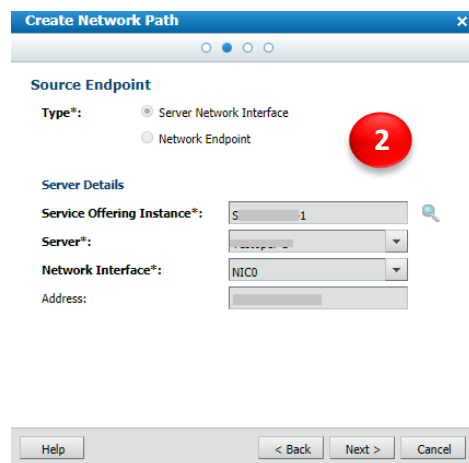
Server Context

Server: Testoper-1

Network Interface: NIC0

Direction\*:  
 Create Inbound Network Path  
 Create Outbound Network Path

Description: EJEMPL0



**Create Network Path**

Source Endpoint

Type\*:  
 Server Network Interface  
 Network Endpoint

Server Details

Service Offering Instance\*: S...1

Server\*: Testoper-1

Network Interface\*: NIC0

Address:

Help < Back Next > Cancel

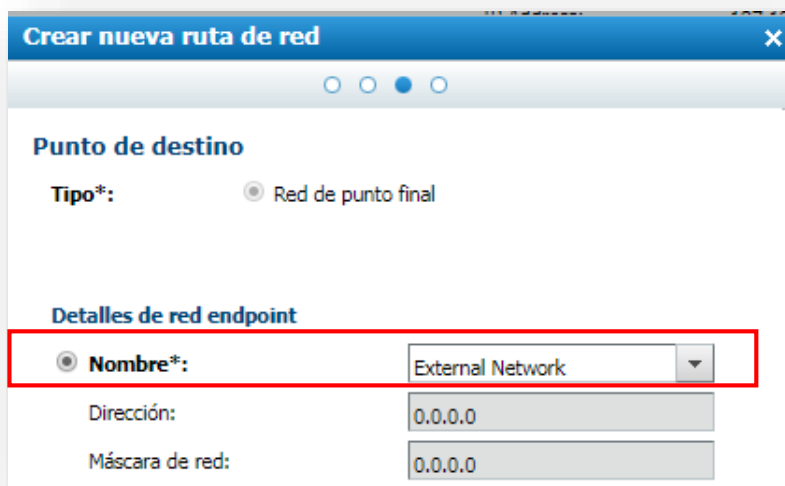
Nos muestra la configuración damos en **Next**

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





3 Se selecciona **External Network** y damos **continuar**

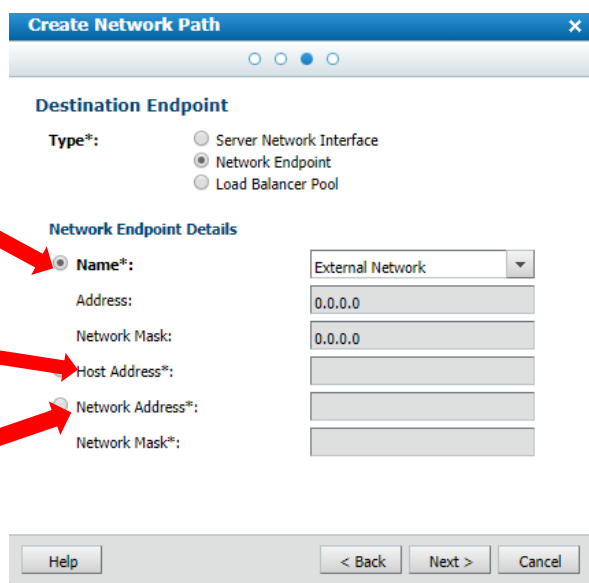


4 - Seleccionamos el destino entre:

1- **External Network** (any) hacia todo internet.

2- **Host Address** Hacia una Ip especifica

3- **Network Address** hacia un rango IP (VPN)



POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





- 5 Para finalizar elegimos el tipo de tráfico que queremos permitir entre las opciones de protocolo y aplicaciones o puertos.

**Create Network Path**

**Path Constraints**

Source: SOI1042450-1 -> [redacted] -> NIC0

Transport Protocol\*: IP

Application Protocol:  [redacted]  Port Range: [redacted]

Enter either a single port or single port range. For example: 8884 - 8890

Allow Traffic:  Locked:

Log:  Hidden:

Destination: External Network

Help < Back Save Cancel

Apretamos en Save y aguardamos unos minutos q la regla impacte en el Firewall y el resto de los equipos de red de la infraestructura.



## Personalización de uso de la VPN

Otra opción que puede ser útil, es la de configurar la VPN, de modo que quede siempre conectada y no pida validación de credenciales cada 2hs. Para esto se debe modificar el archivo de configuración.

El archivo de configuración de la conexión se encuentra en el directorio "Archivos de programa\Cisco Systems\VPN Client\Profiles" (o "Program files\Cisco Systems\VPN Client\Profiles") y su extensión es .pcf. Se trata de un archivo de texto plano, por lo que podemos abrirlo con el Notepad.

Las líneas a modificar son:

Donde dice:

```
Username=  
SaveUserPassword=0  
UserPassword=
```

```
ForceKeepAlives=0
```

Se completa con:

```
Username=nombre_de_usuario  
!SaveUserPassword=1  
!UserPassword=password
```

```
!ForceKeepAlives=1
```

Se suman las credenciales (usuario y contraseña) que te llegaron vía emails, pero el detalle mas importante es agregar el símbolo "!" los campos *SaveUserPassword*, *UserPassword* y *ForceKeepAlive*.

### Inicio de la conexión desde la línea de comandos

El cliente de VPN provee una forma de iniciar conexiones desde la línea de comandos. El comando a ejecutar se encuentra en el directorio "Archivos de programa\Cisco Systems\VPN Client" (o "Program files\Cisco Systems\VPN Client").

La sintaxis es la siguiente:

Para conectar la VPN: ***vpnclient connect nombre-conexion***

Para desconectar la VPN: ***vpnclient disconnect***

Una vez conectados, podemos ver el Status de la conexión, en VPN-Cient | Statistics, "Route Details"; se deben observar las IP address que constituyen el tráfico de encriptación (columna "Secured Routes"). Se puede entonces realizar tests de acceso a la solución correspondiente, realizando "pings".

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





## Instalación y configuración de Cisco VPN Client

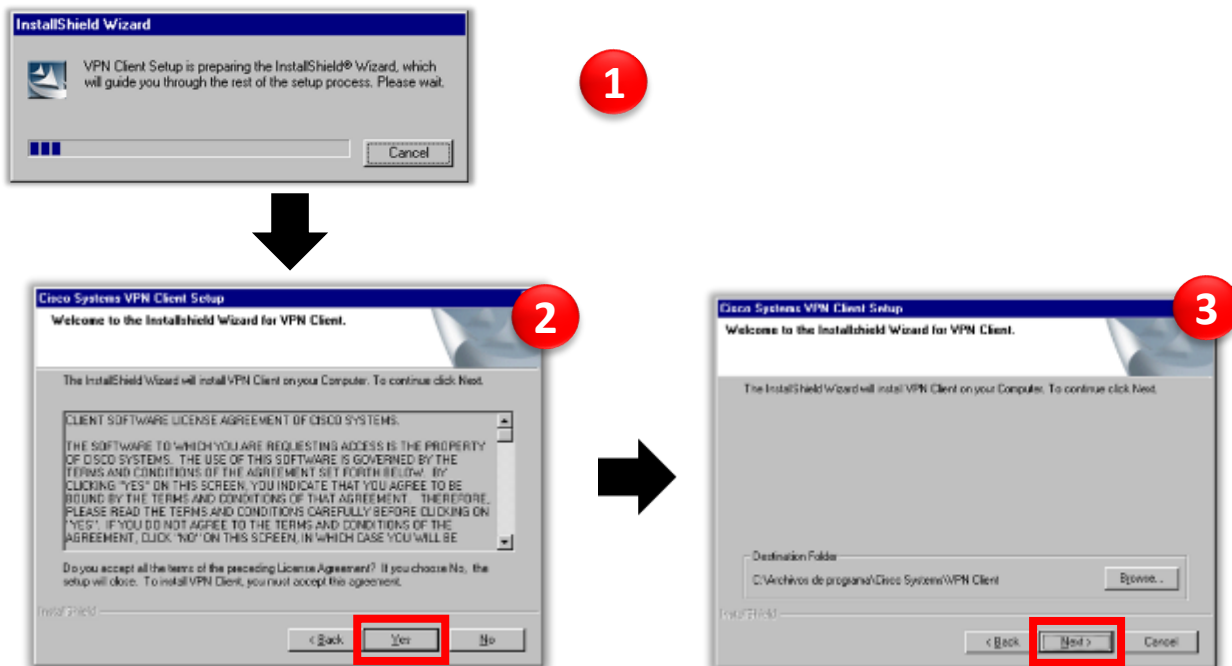
A continuación veremos los pasos a seguir para la instalación del cliente *Cisco VPN Client*<sup>1</sup> y su configuración para establecer una VPN contra el terminador del DCV Claro Cloud. El objetivo final es acceder a los servidores virtuales, para su administración.

Si no tienes aun la herramienta, puedes descargarla desde la pagina de oficial de Cisco o siguiendo este vinculo <http://200.69.128.10/vpnclient/> e ingresando las siguientes credenciales <USER: vpnclient y PASS: P1ntuR4#1>

### Instalación

\* El cliente no es compatible con Windows 10, para instalarlo es necesario un procedimiento no homologado del cual Claro no se hace responsable ni puede proveer. El mismo esta disponible en internet.

Para comenzar la instalación, ejecutar el archivo setup.exe descargado.



<sup>1</sup>La aplicación VPN Cisco Client, **no es compatible con Windows 10**, usted podrá modificar la configuración de su SO, bajo su control, en base a información e instrucciones de acceso publico en internet. Se muestran los snapshots para versión 3.6, el procedimiento es similar para la versión 5 (versión recomendada).

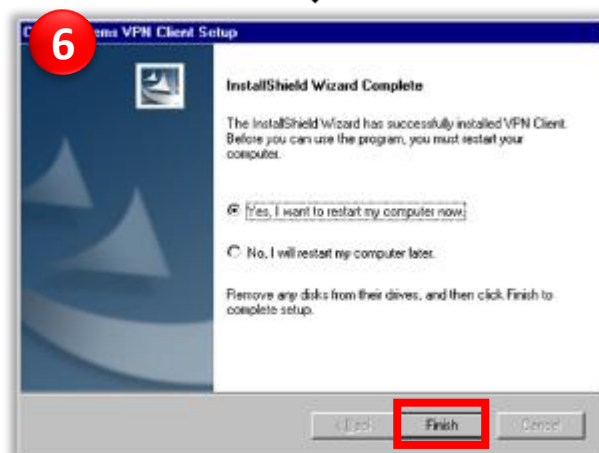
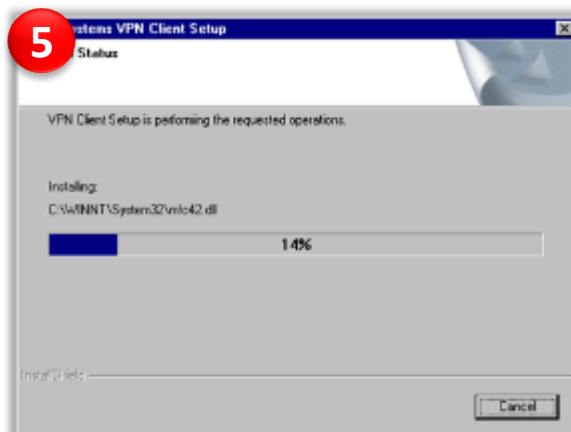
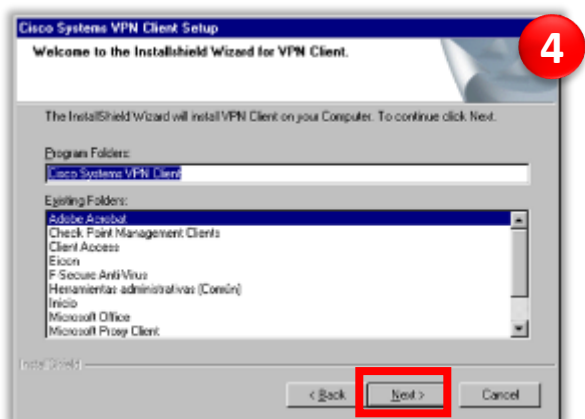
[Volver a inicio de la guía](#)

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS





Continuamos con los últimos pasos de la instalación. Luego del paso 6, al finalizar el proceso la Computadora se reiniciara.



[Volver a inicio de la guía](#)

No dudes en contactarte con nosotros antes cualquier duda o inquietud. Recordá también que si querés más información de nuestros productos y servicios Cloud, podés visitar nuestra pagina web <http://cloud.claro.com.ar/>

POR CUALQUIER CONSULTA NO DUDES EN COMUNICARTE CON NOSOTROS

