

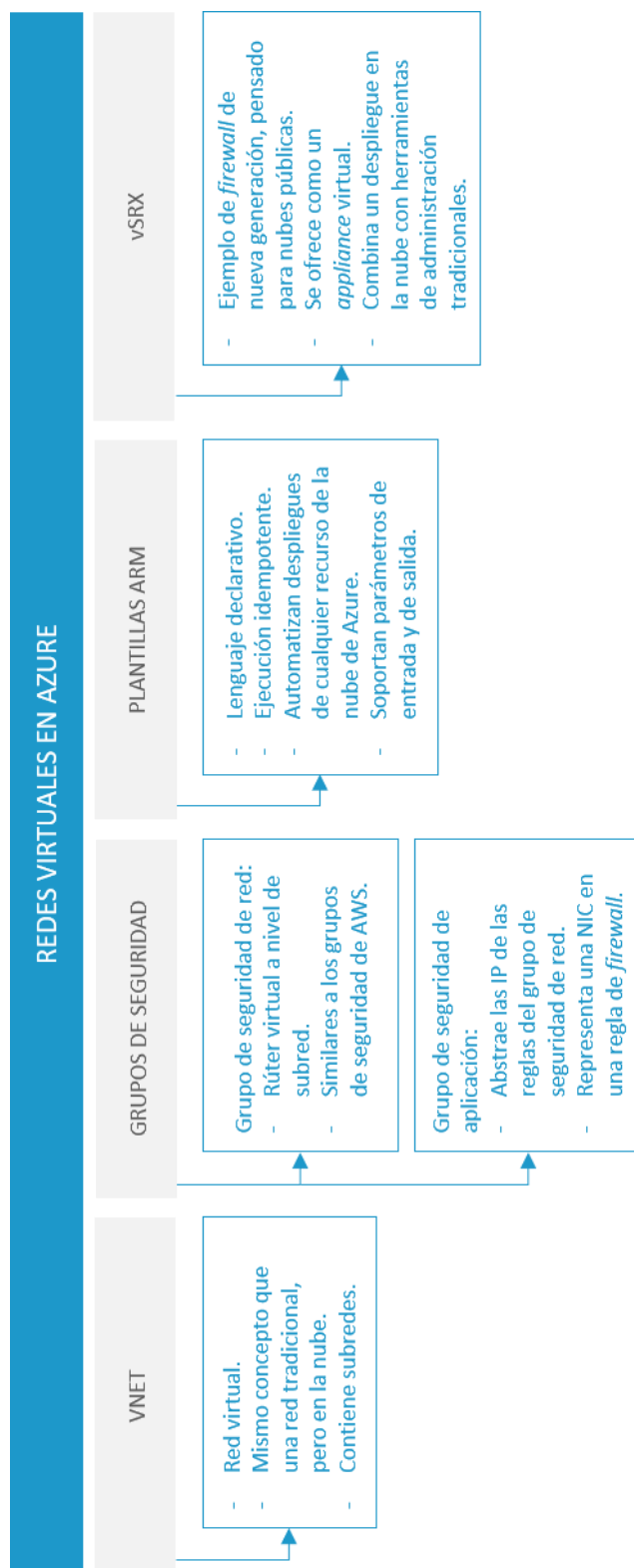
SecDevOps y Administración de Redes para Cloud

---

# Administración de redes en cloud

# Índice

Esquema	3
Ideas clave	4
6.1. Introducción y objetivos	4
6.2. Redes virtuales en Azure	5
6.3. Caso práctico: redes y grupos de seguridad en Azure	8
6.4. Caso práctico: <i>firewall</i> Juniper	17
6.5. Caso práctico: VPN en AWS	33
6.6. Referencias bibliográficas	45
A fondo	46
Test	48



## 6.1. Introducción y objetivos

Los **recursos de computación** pueden ser la cara visible de la oferta de los **proveedores de nube**, pero los servicios de red no son solo un **elemento auxiliar**:

- ▶ Son tan automatizables como cualquier otro elemento, a través de plantillas de configuración, llamadas de API o SDKs.
- ▶ Tienen suficiente funcionalidad como para poder usarlos por sí mismos en entornos híbridos.

Las **herramientas de administración de redes virtuales** en la nube difieren mucho de las herramientas tradicionales. Los proveedores han diseñado nuevos conceptos y entidades, y los fabricantes de productos de red tradicionales han saltado al tren de la **virtualización** con soluciones integradas con la nube.

Este tema presentará los servicios de red de **Azure** y un ejemplo de integración de una herramienta de otro fabricante, **Juniper**, también en la nube de Azure. Además, se mostrará un caso práctico adicional, con los pasos para **configurar una VPN** de cliente en AWS.

Los **objetivos** que se pretenden conseguir en este tema son:

- ▶ Practicar con interfaces de proveedores de nube.
- ▶ Conocer los conceptos de red nativos de un proveedor de nube.
- ▶ Aprender a automatizar despliegues completos.
- ▶ Tomar contacto con soluciones de terceros, integradas en la infraestructura de nube pública.

## 6.2. Redes virtuales en Azure

Los **servicios de red** de Azure proporcionan la base para construir **soluciones de nube nativas e híbridas**. Azure Virtual Network es la pieza principal que permite conectar, de forma segura, los recursos nativos y la infraestructura de nube a los **centros de datos físicos**.

### Azure Virtual Network

Azure Virtual Network (denominada también VNet) es una de las **piezas esenciales** para la infraestructura de red privada en Azure (Tullock, 2013). VNet permite que muchos tipos de recursos de Azure, como las **máquinas virtuales**, se comuniquen de manera segura entre sí, con Internet y con las redes locales **on-premise**. VNet es similar a la red tradicional de un centro de datos, pero tiene **beneficios adicionales** de la infraestructura nativa de nube, como la **escalabilidad y alta disponibilidad**.

### Conceptos de VNet

Algunos de los **conceptos esenciales** de VNet son:

- ▶ **Espacio de direcciones:** al crear una red virtual, es necesario especificar un espacio de direcciones IP privadas. Azure asigna IP de este espacio a los recursos conectados a la red virtual. Por ejemplo, una VM desplegada en una red virtual con espacio de direcciones 10.0.0.0/16 recibirá una IP privada dentro de esa subred, por ejemplo, 10.0.0.4.
- ▶ **Subredes:** las subredes permiten segmentar la red virtual en una o más redes, y asignar una parte del espacio de direcciones de la red virtual a cada subred. Los recursos podrán desplegarse en la subred necesaria, de acuerdo con las necesidades de la arquitectura de los sistemas. Al igual que en una red tradicional, la segmentación de las subredes mejora la eficiencia de asignación de direcciones.

Además, los recursos dentro de las subredes se pueden proteger utilizando grupos de seguridad de red.

- ▶ **Regiones:** una región es un conjunto de centros de datos, implementados dentro de un perímetro con una latencia definida y conectados a través de una red regional dedicada de baja latencia. Una VNet tiene un alcance para una sola región de Azure; sin embargo, se pueden conectar varias redes virtuales de diferentes regiones mediante el emparejamiento de redes virtuales.
- ▶ **Suscripción:** una suscripción de Azure está vinculada a una sola cuenta, la que se utilizó para crear la suscripción y se utiliza para fines de facturación (es un concepto similar al de cuenta en AWS). Los recursos se provisionan dentro de una suscripción. Una VNet tiene un alcance de una suscripción, y una suscripción puede tener tantas VNets como sean necesarias.

## Mejores prácticas

Al conocimiento técnico tienen que acompañarle **recomendaciones** de uso, como las siguientes:

- ▶ Hay que asegurar que los espacios de direcciones no estén superpuestos. Además, tampoco deben solaparse con los rangos de red de la organización.
- ▶ Las subredes no deben cubrir todo el espacio de direcciones de la red virtual. Hay que planificar con anticipación y reservar un espacio de direcciones para el futuro.
- ▶ Es recomendable tener menos VNets, pero más grandes que muchas redes virtuales pequeñas, para reducir los esfuerzos de administración.
- ▶ Las redes virtuales deben estar protegidas con grupos de seguridad de red.

## Conexión con Internet

De manera predeterminada, todos los recursos en una red virtual pueden iniciar **comunicación saliente** hacia Internet. En sentido contrario, sin embargo, los recursos son accesibles desde Internet si se les asigna una **dirección IP pública**, o un **balanceador de carga**, y el tráfico está permitido con un grupo de seguridad de red.

## Conexión con otros recursos de Azure

Los recursos de Azure se **comunican de forma segura** entre sí de una de las siguientes maneras:

<b>A través de una red virtual</b>	Además de las máquinas virtuales, otros servicios, como Azure Kubernetes Service o los grupos de autoescalado Scale Sets, pueden conectarse a una VNet.
<b>Mediante emparejamiento de redes virtuales, o VNet peering</b>	Es posible interconectar redes virtuales y enrutar tráfico entre ellas, permitiendo que los recursos en cualquiera de las redes virtuales se comuniquen entre sí.

Tabla 1. Comunicación segura de los recursos de Azure. Fuente: elaboración propia.

## Conexión con recursos locales

Los recursos locales y las redes virtuales en la nube se pueden **conectar** mediante cualquier **combinación** de las siguientes opciones:

- **Red privada virtual (VPN) de punto a sitio (*point-to-site*):** en este caso, cada equipo de la red local que necesite conectarse a recursos de Azure puede establecer una VPN. También se pueden denominar VPN de cliente.

- ▶ **VPN de sitio a sitio (*site-to-site*):** en este caso, un dispositivo VPN específico en la red local establece una conexión VPN con un Azure VPN *Gateway*. Este dispositivo VPN enruta el tráfico de las máquinas de la red local a la red virtual de Azure.
- ▶ **Azure ExpressRoute:** esta solución establece una conexión a través de un colaborador de Azure. Al estilo de un servicio MPLS, este tráfico no se envía por Internet.

### Seguridad de red

Es posible filtrar el tráfico de red entre subredes de grupos de seguridad.

## 6.3. Caso práctico: redes y grupos de seguridad en Azure

Este apartado mostrará cómo **desplegar** una red virtual en Azure y cómo **configurar** los grupos de seguridad para limitar el tráfico (Microsoft, 2021). Los pasos se mostrarán en el portal de Azure, pero podrían **automatizarse** a base de llamadas de API o con plantillas ARM.

El objetivo es **desplegar un servidor web**, al que se podrá acceder desde Internet solo por HTTP, y un servidor de salto, o *jump host*, al que se podrá acceder por RDP. Los administradores usan habitualmente **máquinas de salto** como punto intermedio para poder conectarse a otros servidores.



## Red virtual

El primer paso consiste en **crear una red virtual**. El asistente solicita la subscripción (equivalente al concepto de cuenta en otros proveedores), un grupo de recursos, o *resource group*, y una región (Figura 1). Los **grupos de recursos** son contenedores de otros objetos y actúan como límite de delegación de permisos.

All services > Virtual networks > Create virtual network

### Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

**Project details**

Subscription \* ⓘ Free Trial

Resource group \* ⓘ CustomRG  
[Create new](#)

**Instance details**

Name \* CustomVNet ✓

Region \* (Europe) France Central

Figura 1. Selección de grupo de seguridad y región. Fuente: elaboración propia.

El siguiente paso solicita el **espacio de direcciones** de la red virtual y las subredes. Se pueden definir más subredes una vez creada la VNet y, como se ha comentado previamente, es recomendable mantener un **espacio de direcciones amplio y segmentado** para poder ampliar las subredes en el futuro. La Figura 2 muestra cómo el espacio 10.0.0.0/16, con capacidad para 256 subredes de clase C, se ha segmentado en 2. Para el caso práctico se usará una de ellas.

All services > Virtual networks > Create virtual network

### Create virtual network

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

**IPv4 address space**

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+ Add subnet](#) [Remove subnet](#)

Subnet name	Subnet address range
<input type="checkbox"/> subnet1	10.0.1.0/24
<input type="checkbox"/> subnet2	10.0.0.0/24

Figura 2. Espacio de direcciones y subredes. Fuente: elaboración propia.

Aunque es posible definir un **Azure Firewall** durante la creación de la VNet, en este caso práctico se demostrará el uso de **grupos de seguridad**. Por lo tanto, el resto de los campos del asistente se pueden dejar con la **configuración por defecto**.

## Grupos de seguridad de aplicación

Los grupos de seguridad de aplicación de Azure, o *application security groups*, permiten **agrupar máquinas virtuales e interfaces** de red en **grupos lógicos**, que pueden usarse en grupos de seguridad de red. Esto los convierte en una **extensión natural** de la estructura de la aplicación, ya que las reglas de los grupos de seguridad de red se pueden definir en base a objetos de la nube y no a IP específicas.

Para crear un **grupo de seguridad de aplicación** no hay más que seleccionar el tipo de recurso en el portal de Azure e introducir el nombre. No tiene configuraciones adicionales. Para este caso práctico son necesarios dos grupos, **webASG** y **adminASG**, ambos en el mismo grupo de recursos que la red virtual.

## Grupos de seguridad de red

Los grupos de seguridad de red, o *network security groups*, funcionan como **firewalls virtuales** a nivel de interfaz de máquina virtual y de subred. Contienen listas de reglas definidas a partir del protocolo, rango de IP y puertos de origen y rango de IP y puertos de destino. Un mismo grupo de seguridad de red puede estar **asociado** a más de una interfaz y subred.

El asistente de creación del grupo de seguridad solo solicita el **nombre**. Una vez creado, es posible añadir las **configuraciones necesarias**. En primer lugar, es necesario **asociar** el grupo de seguridad a la subred en la que se desplegarán las máquinas virtuales. Para ello, hay que abrir los **detalles del grupo de seguridad**, hacer clic en **Subnets** y en **Associate** y, finalmente, seleccionar la red virtual que contiene la subred y la propia subred, tal como muestra la Figura 3.

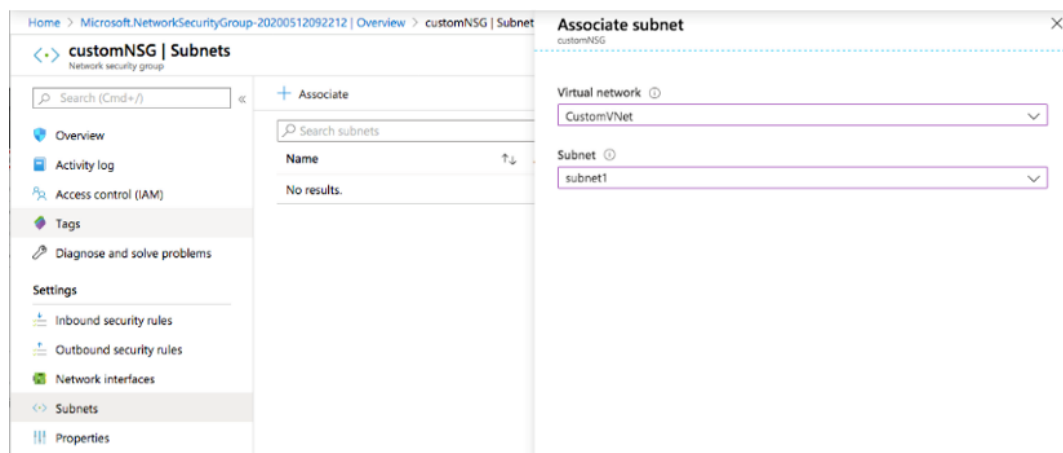


Figura 3. Asociación de grupo de seguridad de red a una subred. Fuente: elaboración propia.

El grupo de seguridad necesita **dos reglas**: una para permitir el **tráfico** HTTP a los servidores web y otra para permitir el **acceso** a administradores al equipo de salto.

**Add inbound security rule** customNSG

Basic

Source \* ⓘ  
Any

Source port ranges \* ⓘ  
\*

Destination \* ⓘ  
Application security group

Destination application security group \* ⓘ  
webASG

Destination port ranges \* ⓘ  
80,443 ✓

Protocol \*  
Any TCP UDP ICMP

Action \*  
Allow Deny

Priority \* ⓘ  
200 ✓

Name \*  
PublicWeb ✓

Figura 4. Regla para acceso a los servidores web. Fuente: elaboración propia.

La regla para el **acceso web** se muestra en la Figura 4. Como se puede observar, en el campo de destino no se ha especificado una IP, sino un **grupo de seguridad** de aplicación. Este grupo se asociará a las **máquinas virtuales** más adelante.

La segunda regla permite el tráfico a los **puertos 22 y 3389** (SSH para los equipos de salto Linux y RDP para los Windows). Además, el origen está **restringido** a una IP específica con el objetivo de evitar ataques de fuerza bruta. La Figura 5 muestra la lista de reglas definitiva. Los grupos de seguridad contienen **tres reglas** por defecto, que también aparecen en la imagen: dos de ellas permiten **todo el tráfico interno** en la red virtual y el tráfico desde un balanceador de red, mientras que la última **deniega** todo el tráfico.

Al igual que las reglas de *iptables*, el orden afecta, por lo que esta última regla actuará como **regla por defecto** para cualquier tráfico que no active alguna de las anteriores. El orden de las reglas no está definido por una posición, sino por una prioridad, por

lo que es habitual asignar prioridades no consecutivas para poder **intercalar reglas** nuevas más adelante, si fuera necesario.

Priority	Name	Port	Protocol	Source	Destination	Action
110	AdminAccess	22,3389	TCP	139.47.100.40	adminASG	Allow
200	PublicWeb	80,443	TCP	Any	webASG	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Figura 5. Reglas del grupo de seguridad. Fuente: elaboración propia.

## Despliegue de las máquinas virtuales

La creación de las **máquinas virtuales** no es parte de la administración de redes, pero sirve para **ilustrar la funcionalidad** que pueden ofrecer los administradores de red a los de sistemas o DevOps, si es que los roles están **diferenciados**. En este paso, se **crearán** dos máquinas virtuales, ambas con Windows Server 2019, en el mismo grupo de recursos, en la misma red virtual y en la misma subred. Los aspectos relevantes son:

- ▶ **No hay que seleccionar** un grupo de seguridad de red en la NIC, ya que esto se configurará más adelante con los grupos de seguridad de aplicación (Figura 6).
- ▶ **Tampoco hay que seleccionar puertos de entrada** (en el primer paso del asistente), por la misma razón.
- ▶ Las dos máquinas **deben tener una IP pública**. En un caso real, la IP pública estaría en un balanceador de carga que enviaría el tráfico al servidor web. En el caso del servidor de salto, se podría evitar la IP pública con la funcionalidad de Azure Bastion, o con una conexión VPN entre la VNet y la oficina remota.

Home > Virtual machines > Create a virtual machine

## Create a virtual machine

---

Basics   Disks   **Networking**   Management   Advanced   Tags   Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ CustomVNet ▼  
[Create new](#)

Subnet \* ⓘ subnet1 (10.0.1.0/24) ▼  
[Manage subnet configuration](#)

Public IP ⓘ (new) web-ip ▼  
[Create new](#)

NIC network security group ⓘ ☒ None ☐ Basic ☐ Advanced

**i** The selected subnet 'subnet1 (10.0.1.0/24)' is already associated to a network security group 'customNSG'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Figura 6. Configuración de red de la interfaz del servidor web. Fuente: elaboración propia.

Las **características** de la VM, como tamaño, región o disco, no son relevantes para este caso práctico, por lo que pueden usarse los valores por defecto. El nombre de usuario y contraseña se usarán más adelante.

## Configuración de grupos de seguridad

Al crear las máquinas, Azure crea también una **NIC virtual**. Es en esta NIC en la que hay que configurar el **grupo de seguridad de aplicación**. La Figura 7 muestra el cuadro de diálogo para configurarlo: una vez seleccionada la VM hay que ir a *Networking > Application security groups > Configure the application security groups* y seleccionar el grupo concreto. Cada VM debe tener su grupo correspondiente.

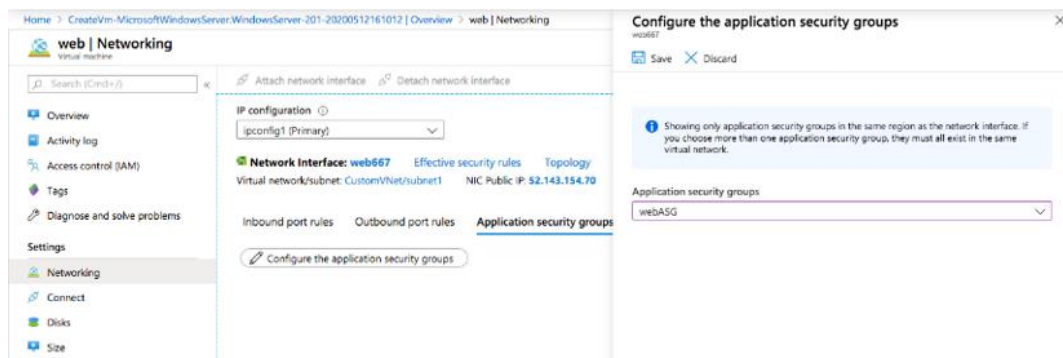


Figura 7. Grupo de seguridad de aplicación en el servidor web. Fuente: elaboración propia.

## Comprobación de la configuración

El **entorno** está **listo** para su uso. El siguiente paso es **conectarse** al servidor de salto. Para ello, basta con abrir el **cliente de escritorio remoto** e introducir la IP pública, disponible en la pestaña Overview de la máquina virtual. Azure ofrece también la opción de **descargar un fichero .rdp** con la configuración necesaria en la pestaña Connect. Si los pasos anteriores se han seguido correctamente, la sesión de escritorio remoto se abrirá con éxito.

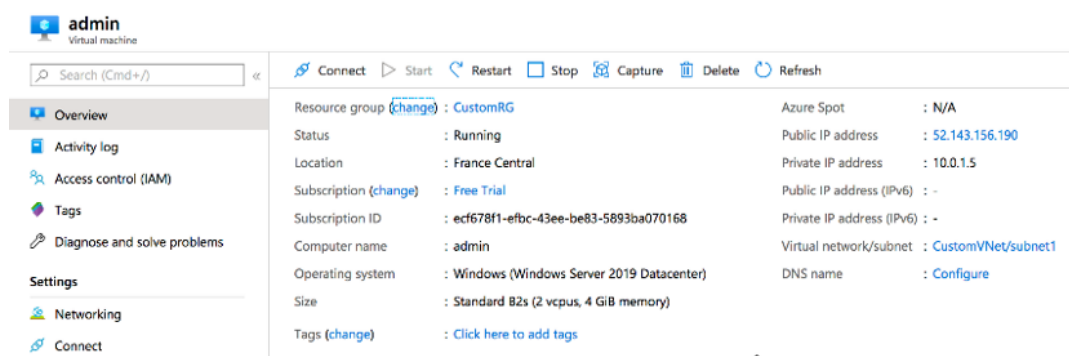


Figura 8. Detalles de la máquina virtual. Fuente: elaboración propia.

Sin embargo, los intentos de **abrir una conexión de escritorio remoto** contra el servidor web no serán posibles, ya que esa VM solo recibirá tráfico HTTP, no RDP, desde Internet, gracias a la configuración de los grupos de seguridad.

Para completar la prueba, el siguiente paso es **instalar el rol de servidor web** en la segunda máquina virtual.

Desde el propio servidor de salto es posible, valga la redundancia, **saltar al servidor web por RDP** (el comando `mstsc /v:web` sirve de atajo). Esta conexión es viable porque, por defecto, las máquinas virtuales de una misma red virtual pueden **comunicarse sin restricciones**. Una vez en la máquina de destino, tras esta doble conexión RDP, es posible activar el rol de servidor web con el comando de PowerShell `Install-WindowsFeature -name Web-Server -IncludeManagementTools` (Figura 9).

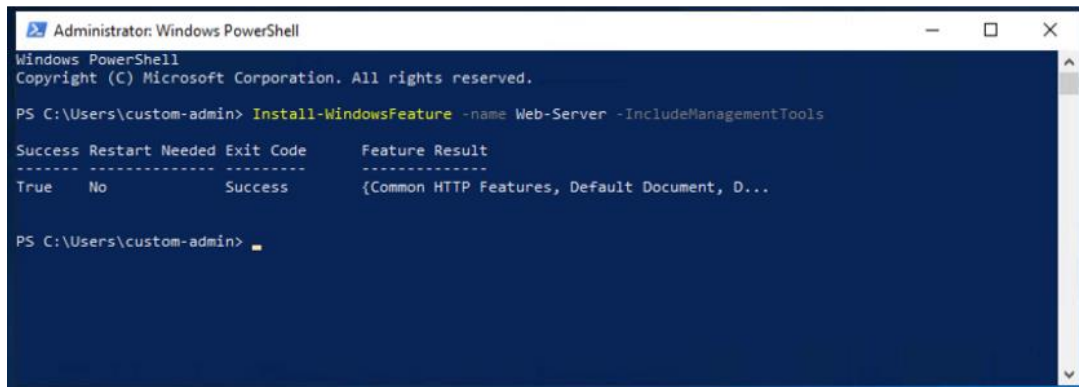


Figura 9. Instalación de servicio web. Fuente: elaboración propia.

El último paso consiste en **consultar la IP pública de la VM** con el servidor web y apuntar el navegador a `http://<ip_pública_web>`. La Figura 10 muestra la **vista de resumen de la VM**, con la IP pública; y el **navegador**, con la página por defecto del servidor web de Windows.

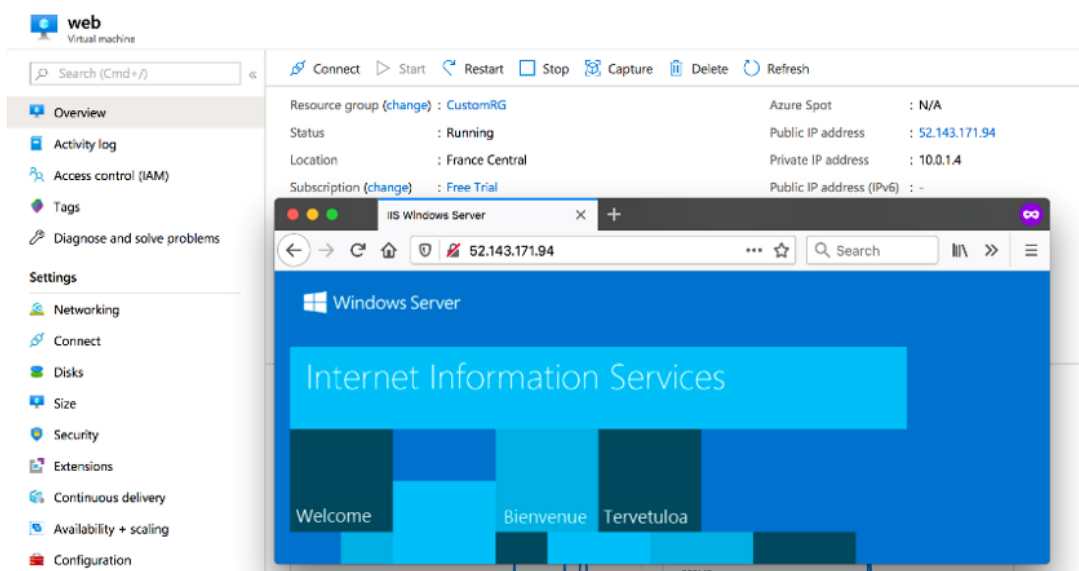


Figura 10. Acceso por HTTP al servidor web. Fuente: elaboración propia.



Esta conexión es posible, de nuevo, gracias a que el **tráfico HTTP** está permitido desde Internet a este equipo en los **grupos de seguridad**.

## Limpieza

Los **recursos de nube** incurren en gastos en cuanto entran en funcionamiento, por lo que hay que asegurarse de **borrar todos los recursos** una vez terminada las pruebas. Todos los elementos creados durante este caso se pueden borrar, rápidamente, eliminando el grupo de recursos al que se han añadido.

## 6.4. Caso práctico: *firewall* Juniper

El caso práctico anterior hacía uso de **servicios nativos de Azure**, exclusivamente. Sin embargo, muchos administradores de red están acostumbrados a usar soluciones de desarrolladores tradicionales como Cisco o Juniper. Estas compañías suelen ofrecer sus productos como **soluciones virtuales** que se pueden integrar en entornos de nube privada o pública.

Estas soluciones pueden ofrecerse como un **appliance** virtual o como parte de la tienda de aplicaciones. Los usuarios de los proveedores de nube pueden entonces aprovechar sus conocimientos para **administrar las redes virtuales** con las mismas herramientas que usan en las redes locales.

Un *appliance* se refiere a una máquina virtual que empaqueta el sistema operativo con un software específico. Se pueden distribuir como una imagen o plantilla lista para ser desplegada en un entorno de virtualización.

En el siguiente vídeo, titulado «**Redes en la nube**», puedes seguir la demostración del caso práctico que se está desarrollando.



Accede al vídeo

El escenario de este caso práctico consiste en una **red interna confiable**, una **red pública o DMZ** y una **red de administración** conectadas con un *firewall* Juniper vSRX (Figura 11).

El vSRX es un *appliance* virtual que ofrece **servicios de seguridad y de red** en entornos de nube pública o privada. Se conoce como **firewall de nueva generación**, o *next generation firewall*, porque no solo funciona como *firewall* avanzado (a nivel de paquetes y de aplicación), sino también como *rúter*, VPN, NAT o IPS (sistema de detección y prevención de intrusiones).

Juniper vSRX está basado en el sistema operativo Junos, por lo que cualquier administrador familiarizado con otros productos de Juniper puede aprender a configurar un vSRX con poco esfuerzo.

El despliegue de este escenario va a hacer uso de otra herramienta de Azure, las **plantillas de Azure Resource Manager (ARM)** (Microsoft, 2021). Estas plantillas permiten desplegar recursos usando un **lenguaje declarativo**, es decir, el **código de la plantilla** expresa el estado final de un conjunto de recursos, pero no indica cómo deben desplegarse, ni los pasos individuales que habría que dar para crear cada recurso.

La principal ventaja es la **automatización** que ofrecen: una plantilla se puede desplegar varias veces con parámetros diferentes, y cada despliegue tendrá, exactamente, la misma **topología**. Además, la ejecución es idempotente, por lo que si la configuración de un despliegue cambia (por ejemplo, por un error humano), la plantilla se puede ejecutar de nuevo para devolverlo a su estado original.

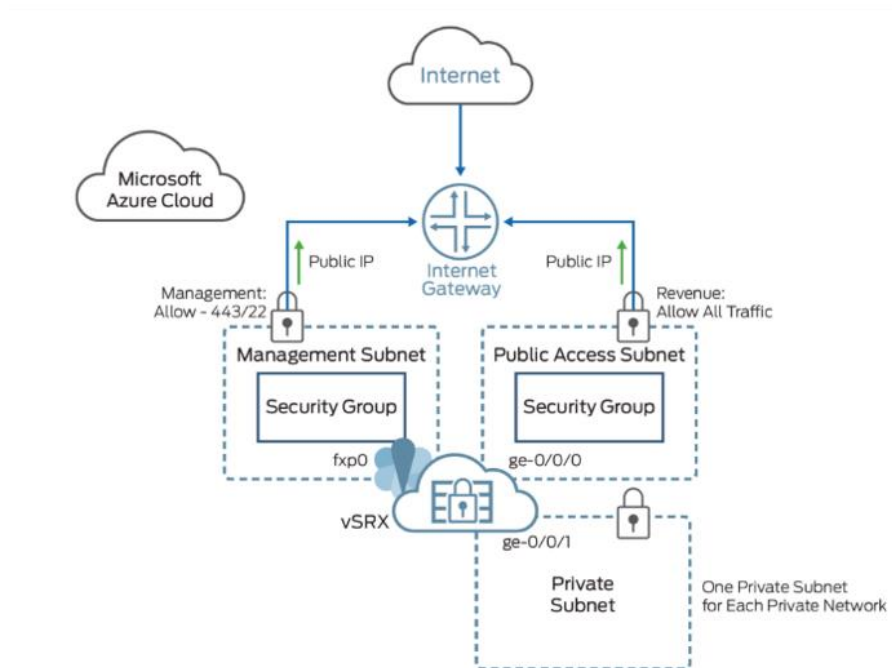


Figura 11. Diagrama de red del caso práctico. Fuente: Juniper, 2021.

## Descripción de la plantilla

Las plantillas se definen en **formato JSON**. Los campos relevantes son:

- ▶ La **sección de parámetros** define los datos configurables durante el despliegue, por ejemplo, los rangos de direcciones IP de la red virtual y de cada subred. Facilitan la reusabilidad de la plantilla.
- ▶ Las **variables** pueden definirse a partir de los valores de los parámetros para su uso en el resto de la plantilla. Por ejemplo, la imagen del *appliance* a desplegar depende del parámetro *payAsYouGo*, ya que Juniper ofrece una imagen de máquina virtual para cada tipo de licencia.
- ▶ La sección de **recursos** define cada objeto, siguiendo la sintaxis definida en la documentación (Microsoft, 2020).
- ▶ Las **variables de salida**, u **outputs**, permiten exponer campos de los objetos creados por la plantilla para un consumo fácil por parte del usuario, o de una llamada de API. Se usan especialmente para extraer valores no conocidos en el momento del despliegue como, por ejemplo, la IP pública asignada a una interfaz de red.

Microsoft ofrece [plantillas de ejemplo](#) para su despliegue inmediato, o como punto de partida, para escribir plantillas personalizadas. El portal de Azure ofrece, además, una funcionalidad muy útil para el desarrollo de plantillas. Los asistentes de creación de objetos ofrecen una opción en el último paso, *Download a template for automation*, que convierte los datos de entrada del asistente en una **plantilla de ARM**.

La plantilla puede tener más de un recurso. Por ejemplo, la Figura 12 muestra esta opción en un **asistente de creación de VM**. La lista de recursos contiene no solo la VM, sino también la **interfaz de red**, una **VNet** y un **grupo de seguridad** de red nuevos, entre otros. El **código** de estas plantillas se puede combinar para construir plantillas más complejas. También puede servir para, simplemente, comprobar la sintaxis con un ejemplo práctico, sin depender de la documentación.

The screenshot displays the 'Template' view in the Azure portal. The breadcrumb navigation at the top reads: Home > Virtual machines > Create a virtual machine > Template. Below the navigation bar, there are buttons for 'Download', 'Add to library (preview)', and 'Deploy'. A blue information banner states: 'Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resources and configurable input parameters and deploy with script or code. Learn more about template deployment.' Below this, there is a checkbox labeled 'Include parameters' which is checked. The main content area is divided into two panes. The left pane, titled 'Template', shows a tree view of the template's components. Under 'Parameters (21)', there are three 'Variables' (nsgId, vnetId, subnetRef) and six 'Resources' (networkInterfaces, networkSecurityGroups, virtualNetworks, publicIpAddresses, virtualMachines, and storageAccounts). The right pane shows the ARM template JSON code, which includes the schema, contentVersion, parameters, and resource definitions. The code is as follows:

```
1 {
2   "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "location": {
6       "type": "string"
7     },
8     "networkInterfaceName": {
9       "type": "string"
10    },
11    "networkSecurityGroupName": {
12      "type": "string"
13    },
14    "networkSecurityGroupRules": {
15      "type": "array"
16    },
17    "subnetName": {
18      "type": "string"
19    },
20    "virtualNetworkName": {
21      "type": "string"
22    },
23    "addressPrefixes": {
24      "type": "array"
```

Figura 12. Plantilla ARM automática a partir del asistente de creación de VM. Fuente: elaboración propia.

Las plantillas se crean como un **recurso** más en el **portal de Azure**. La plantilla que despliega el escenario se incluye a continuación; se puede copiar a la sección de **código de una plantilla nueva** (Figura 13) para empezar con el despliegue.

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "location": {
      "type": "string",
      "defaultValue": "westus",
      "metadata": {
        "description": "The region in which resources will be deployed"
      }
    },
    "payAsYouGo": {
      "type": "bool",
      "metadata": {
        "description": "License type as offered by Juniper: true for pay as you go, false for bring your own license."
      }
    },
    "virtualMachineSize": {
      "type": "string",
      "defaultValue": "Standard_DS3_v2",
      "metadata": {
        "description": "Virtual Machine Size"
      }
    },
    "deploymentName": {
      "type": "string",
      "metadata": {
        "description": "Deployment Name, for use in VM hostname, storage account and related resources."
      }
    },
    "vSRXAddressGE000": {
      "type": "string",
      "defaultValue": "10.4.1.4",
      "metadata": {
        "description": "IP de la interfaz ge-0/0/0 del vSRX"
      }
    },
    "vSRXAddressGE001": {
      "type": "string",
      "defaultValue": "10.4.2.4",
      "metadata": {
        "description": "IP de la interfaz ge-0/0/0 del vSRX"
      }
    }
  },
```

```

    "vsrxUsername": {
      "type": "string",
      "metadata": {
        "description": "Usuario administrador del vSRX"
      }
    },
    "vsrxPassword": {
      "type": "securestring",
      "metadata": {
        "description": "Contraseña del usuario del vSRX"
      }
    },
    "vnetPrefix": {
      "type": "string",
      "defaultValue": "10.4.0.0/16",
      "metadata": {
        "description": "Rango de direcciones de la VNet"
      }
    },
    "ManagementSubnetPrefix": {
      "type": "string",
      "defaultValue": "10.4.0.0/24",
      "metadata": {
        "description": "Management subnet prefix"
      }
    },
    "TrustedSubnetPrefix": {
      "type": "string",
      "defaultValue": "10.4.2.0/24",
      "metadata": {
        "description": "Trust subnet prefix"
      }
    },
    "UntrustedSubnetPrefix": {
      "type": "string",
      "defaultValue": "10.4.1.0/24",
      "metadata": {
        "description": "Untrust subnet prefix"
      }
    }
  },
  "variables": {
    "offer": "[if(parameters('payAsYouGo'), 'vsrx-next-generation-firewall-solution-template-payg', 'vsrx-next-generation-firewall-solution-template')]",
    "sku": "[if(parameters('payAsYouGo'), 'vsrx-payg-b1-azure-image-solution-template', 'vsrx-byol-azure-image-solution-template')]",
    "vsrxname": "[concat('vsrx-', parameters('deploymentName'))]",
    "storageAccountName": "[concat('vsrx', parameters('deploymentName'), 'sa')]",
    "vsrx-addr-fxp0": "[concat(variables('vsrxname'), '-fxp0')]",
    "vsrx-addr-ge000": "[concat(variables('vsrxname'), '-ge-0-0-0')]",
    "vnet-name": "[concat(variables('vsrxname'), '-vnet')]",
    "vnet-mgt-subnet-name": "[concat(variables('vnet-name'), '-management')]",
    "vnet-untrust-subnet-name": "[concat(variables('vnet-name'), '-untrust')]",
  }
}

```

```

"vnet-trust-subnet-name": "[concat(variables('vnet-name'), '-trust')]",
"rtt-untrust": "[concat('rtt-untrust-subnet-', variables('vnet-name'))]",
"rtt-trust": "[concat('rtt-trust-subnet-', variables('vnet-name'))]",
"vsrxVM": {
  "vmSize": "[parameters('virtualMachineSize')]",
  "vmName": "[variables('vsrxname')]",
  "pipNameFxp0": "[variables('vsrx-addr-fxp0')]",
  "pipNameGe000": "[variables('vsrx-addr-ge000')]",
  "mgtNicName": "[concat('if-', variables('vsrxname'), '-fxp0')]",
  "untrustNicName": "[concat('if-', variables('vsrxname'), '-ge-0-0-0')]",
  "untrustPrivateIP": "[parameters('vSRXAddressGE000')]",
  "trustNicName": "[concat('if-', variables('vsrxname'), '-ge-0-0-1')]",
  "trustPrivateIP": "[parameters('vSRXAddressGE001')]"
},
"vnet-id": "[resourceId('Microsoft.Network/virtualNetworks', variables('vnet-name'))]",
"vnet-untrust-subnet-id": "[concat(variables('vnet-id'), '/subnets/', variables('vnet-untrust-subnet-name'))]",
"vnet-trust-subnet-id": "[concat(variables('vnet-id'), '/subnets/', variables('vnet-trust-subnet-name'))]",
"vnet-mgt-subnet-id": "[concat(variables('vnet-id'), '/subnets/', variables('vnet-mgt-subnet-name'))]",
"vsrx-pip-fxp0-id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('vsrxVM').pipNameFxp0)]",
"vsrx-pip-ge000-id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('vsrxVM').pipNameGe000)]",
"storageContainerName": "vsrx",
"linuxConfigurationPassword": {
  "disablePasswordAuthentication": "false"
}
},
"resources": [
{
  "apiVersion": "2018-02-01",
  "name": "pid-7c99adcc-2917-4c23-abba-98cf108e3ba2",
  "type": "Microsoft.Resources/deployments",
  "properties": {
    "mode": "Incremental",
    "template": {
      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
      "contentVersion": "1.0.0.0",
      "resources": []
    }
  }
},
{
  "type": "Microsoft.Storage/storageAccounts",
  "name": "[variables('storageAccountName')]",
  "apiVersion": "2017-06-01",
  "location": "[parameters('location')]",
  "kind": "Storage",
  "sku": {
    "name": "Standard_LRS"
  }
}
]

```

```

    }
  },
  {
    "type": "Microsoft.Network/publicIPAddresses",
    "name": "[variables('vsrxVM').pipNameFxp0]",
    "apiVersion": "2016-03-30",
    "location": "[parameters('location')]",
    "properties": {
      "publicIPAllocationMethod": "Static",
      "dnsSettings": {
        "domainNameLabel": "[variables('vsrxVM').pipNameFxp0]"
      }
    }
  }
},
{
  "type": "Microsoft.Network/publicIPAddresses",
  "name": "[variables('vsrxVM').pipNameGe000]",
  "apiVersion": "2016-03-30",
  "location": "[parameters('location')]",
  "properties": {
    "publicIPAllocationMethod": "Static",
    "dnsSettings": {
      "domainNameLabel": "[variables('vsrxVM').pipNameGe000]"
    }
  }
}
},
{
  "apiVersion": "2016-03-30",
  "type": "Microsoft.Network/virtualNetworks",
  "name": "[variables('vnet-name')]",
  "location": "[parameters('location')]",
  "dependsOn": [
    "[concat('Microsoft.Network/routeTables/', variables('rtt-untrust'))]",
    "[concat('Microsoft.Network/routeTables/', variables('rtt-trust'))]"
  ],
  "properties": {
    "addressSpace": {
      "addressPrefixes": [
        "[parameters('vnetPrefix')]"
      ]
    },
    "subnets": [
      {
        "name": "[variables('vnet-mgt-subnet-name')]",
        "properties": {
          "addressPrefix": "[parameters('ManagementSubnetPrefix')]"
        }
      },
      {
        "name": "[variables('vnet-untrust-subnet-name')]",
        "properties": {
          "addressPrefix": "[parameters('UntrustedSubnetPrefix')]",
          "routeTable": {

```



```

        "id": "[resourceId('Microsoft.Network/routeTables', variables('rtt-untrust'))]"
    }
  },
  {
    "name": "[variables('vnet-trust-subnet-name')]",
    "properties": {
      "addressPrefix": "[parameters('TrustedSubnetPrefix')]",
      "routeTable": {
        "id": "[resourceId('Microsoft.Network/routeTables', variables('rtt-trust'))]"
      }
    }
  }
]
}
},
{
  "apiVersion": "2017-10-01",
  "type": "Microsoft.Network/routeTables",
  "name": "[variables('rtt-untrust')]",
  "location": "[parameters('location')]",
  "tags": {
    "displayName": "RTT - Untrust subnet"
  },
  "properties": {
    "routes": [
      {
        "name": "RouteToAny",
        "properties": {
          "addressPrefix": "0.0.0.0/0",
          "nextHopType": "Internet"
        }
      }
    ]
  }
},
{
  "apiVersion": "2017-10-01",
  "type": "Microsoft.Network/routeTables",
  "name": "[variables('rtt-trust')]",
  "location": "[parameters('location')]",
  "tags": {
    "displayName": "RTT - Trust subnet"
  },
  "properties": {
    "routes": [
      {
        "name": "RouteToAny",
        "properties": {
          "addressPrefix": "0.0.0.0/0",
          "nextHopType": "VirtualAppliance",

```

```

        "nextHopIpAddress": "[parameters('vSRXAddressGE001')]"
    }
}
]
}
},
{
    "apiVersion": "2016-03-30",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('vsrxVM').mgtNicName]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/', variables('vnet-name'))]",
        "[concat('Microsoft.Network/publicIPAddresses/', variables('vsrxVM').pipNameFxp0)]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Dynamic",
                    "publicIPAddress": {
                        "id": "[variables('vsrx-pip-fxp0-id')]"
                    },
                    "subnet": {
                        "id": "[variables('vnet-mgt-subnet-id')]"
                    }
                }
            }
        ]
    }
}
},
{
    "apiVersion": "2016-03-30",
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('vsrxVM').untrustNicName]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/', variables('vnet-name'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Static",
                    "privateIPAddress": "[variables('vsrxVM').untrustPrivateIP]",
                    "publicIPAddress": {
                        "id": "[variables('vsrx-pip-ge000-id')]"
                    },
                    "subnet": {
                        "id": "[variables('vnet-untrust-subnet-id')]"
                    }
                }
            }
        ]
    }
}
}
}

```

```

    }
  }
]
}
},
{
  "apiVersion": "2016-03-30",
  "type": "Microsoft.Network/networkInterfaces",
  "name": "[variables('vsrxVM').trustNicName]",
  "location": "[parameters('location')]",
  "dependsOn": [
    "[concat('Microsoft.Network/virtualNetworks/', variables('vnet-name'))]"
  ],
  "properties": {
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "privateIPAllocationMethod": "Static",
          "privateIPAddress": "[variables('vsrxVM').trustPrivateIP]",
          "subnet": {
            "id": "[variables('vnet-trust-subnet-id')]"
          }
        }
      }
    ],
    "enableIPForwarding": true
  }
},
{
  "apiVersion": "2016-03-30",
  "name": "[variables('vsrxVM').vmName]",
  "type": "Microsoft.Compute/virtualMachines",
  "location": "[parameters('location')]",
  "plan": {
    "name": "vsrx-byol-azure-image-solution-template",
    "publisher": "juniper-networks",
    "product": "vsrx-next-generation-firewall-solution-template"
  },
  "dependsOn": [
    "[concat('Microsoft.Network/networkInterfaces/', variables('vsrxVM').mgtNicName)]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vsrxVM').untrustNicName)]",
    "[concat('Microsoft.Network/networkInterfaces/', variables('vsrxVM').trustNicName)]",
    "[concat('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))]"
  ],
  "properties": {
    "hardwareProfile": {
      "vmSize": "[variables('vsrxVM').vmSize]"
    },
    "storageProfile": {
      "imageReference": {

```

```

        "publisher": "juniper-networks",
        "offer": "vsrx-next-generation-firewall-solution-template",
        "sku": "vsrx-byol-azure-image-solution-template",
        "version": "latest"
    },
    "osDisk": {
        "osType": "Linux",
        "name": "[concat(variables('vsrxVM').vmName, '-Disk')]",
        "vhd": {
            "uri": "[concat(reference(concat('Microsoft.Storage/storageAccounts/',
variables('storageAccountName')), '2017-06-01').primaryEndpoints.blob,
variables('storageContainerName'), '/', variables('vsrxVM').vmName,
uniquestring(resourceGroup().id), '.vhd'))]"
        },
        "caching": "ReadWrite",
        "createOption": "FromImage"
    }
},
"osProfile": {
    "computerName": "[variables('vsrxVM').vmName]",
    "adminUsername": "[parameters('vsrxUsername')]",
    "adminPassword": "[parameters('vsrxPassword')]",
    "linuxConfiguration": "[variables('linuxConfigurationPassword')]"
},
"networkProfile": {
    "networkInterfaces": [
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vsrxVM').mgtNicName)]",
            "properties": {
                "primary": true
            }
        },
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vsrxVM').untrustNicName)]",
            "properties": {
                "primary": false
            }
        },
        {
            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vsrxVM').trustNicName)]",
            "properties": {
                "primary": false
            }
        }
    ]
},
"diagnosticsProfile": {
    "bootDiagnostics": {
        "enabled": true,

```

```

        "storageUri": "[reference(concat('Microsoft.Storage/storageAccounts/',
variables('storageAccountName')), '2017-06-01').primaryEndpoints.blob]"
    }
}
}
},
"outputs": {
    "managementIP": {
        "value":
"[reference(resourceId('Microsoft.Network/publicIPAddresses',variables('vsrxVM').pipNameFxp0)).ipAd
dress]",
        "type": "string"
    },
    "hostname": {
        "value": "[variables('vsrxname')]",
        "type": "string"
    }
}
}
}

```

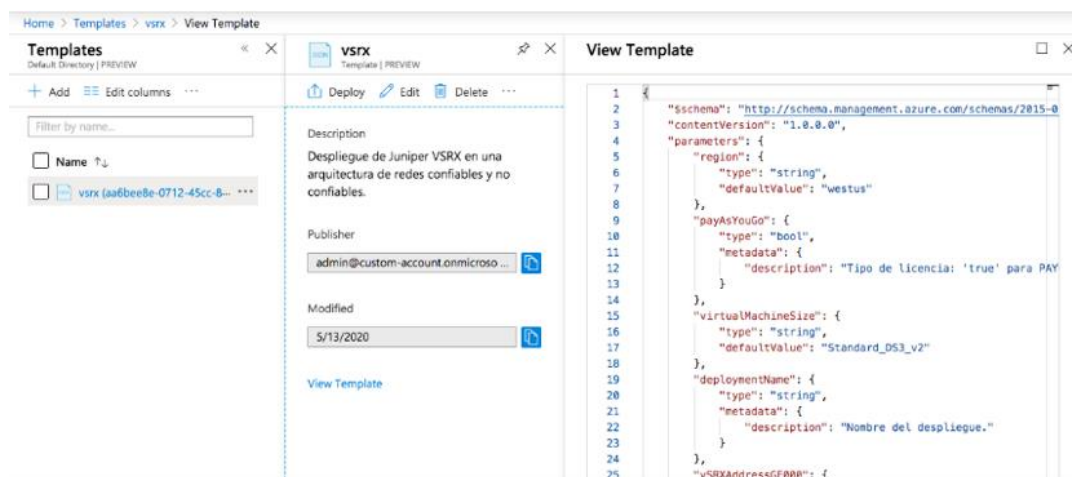


Figura 13. Creación de la plantilla. Fuente: elaboración propia.

El despliegue de la plantilla solicita los **parámetros de entrada** en una interfaz gráfica, tal como muestra la Figura 14. La plantilla se podría desplegar programáticamente y desde la línea de comandos. En esos casos, el despliegue se compone de **dos archivos**: un archivo que contiene el mismo documento JSON con el que se crea la plantilla en el portal de Azure, y un segundo archivo JSON con los valores de los parámetros.

[Home](#) > [Templates](#) > [vsrx](#) > Custom deployment

## Custom deployment

Deploy from a custom template

---

11 resources

[Edit template](#)
[Edit paramet...](#)
[Learn more](#)

### BASICS

Subscription \*

Free Trial

Resource group \*

vSRX-RG  
[Create new](#)

Location

(Europe) France Central

### SETTINGS

Region

francecentral

Pay As You Go \* ⓘ

false

Virtual Machine Size

Standard\_DS3\_v2

Deployment Name \* ⓘ

vsrxcustom ✓

Vsrx Address GE000 ⓘ

10.4.1.4

Vsrx Address GE001 ⓘ

10.4.2.4

Vsrx Username \* ⓘ

custom-admin ✓

Vsrx Password \* ⓘ

..... ✓

Figura 14. Parámetros en el despliegue de la plantilla. Fuente: elaboración propia.

Una vez **confirmado** el despliegue, el portal muestra el estado y los recursos a medida que estos se crean. Las plantillas usan un **lenguaje declarativo**, por lo que el orden en el que están definidos en la plantilla no tiene por qué ser el mismo en el que Azure los crea. El motor se encargará de decidir el orden en función de las **dependencias definidas** en la plantilla.

... Your deployment is underway

Deployment name: admin\_customaccount.onmicrosoft.com.vsrx      Start time: 5/13/2020, 8:56:06 AM  
Subscription: Free Trial      Correlation ID: 59d8ed6b-86ef-4864-abb5-dc62f7d52689  
Resource group: vsrx-RG

Deployment details (Download)

Resource	Type	Status
vsrx-vsrxcustom	Microsoft.Compute/virtualMachines	Created
vsrxvsrxcustomsa	Microsoft.Storage/storageAccounts	OK
if-vsrx-vsrxcustom-fxp0	Microsoft.Network/networkInterfaces	Created
if-vsrx-vsrxcustom-ge-0-0-0	Microsoft.Network/networkInterfaces	Created
if-vsrx-vsrxcustom-ge-0-0-1	Microsoft.Network/networkInterfaces	Created
vsrx-vsrxcustom-vnet	Microsoft.Network/virtualNetworks	OK
vsrxvsrxcustomsa	Microsoft.Storage/storageAccounts	OK
vsrx-vsrxcustom-fxp0	Microsoft.Network/publicIPAddresses	OK
vsrx-vsrxcustom-ge-0-0-0	Microsoft.Network/publicIPAddresses	OK
rtt-untrust-subnet-vsrx-vsrxcustom-vnet	Microsoft.Network/routeTables	OK
rtt-trust-subnet-vsrx-vsrxcustom-vnet	Microsoft.Network/routeTables	OK
pid-7c99adcc-2917-4c23-abba-98cf108e3ba2	Microsoft.Resources/deployments	OK

Figura 15. Despliegue de la plantilla en proceso. Fuente: elaboración propia.

La sección **Outputs** mostrará las dos **variables de salida** definidas en la plantilla (Figura 16). Estos valores no se podían determinar antes del despliegue, por lo que son cruciales para poder hacer uso de ellos en un **proceso automatizado**. En este caso práctico, la plantilla se ha desplegado a mano y, dado que todo se ha lanzado desde el portal, la IP de administración se podría consultar directamente en las **propiedades** de la **máquina virtual**.

Si el despliegue de la plantilla se lanza, por ejemplo, desde un trabajo de **Jenkins** para automatizar las pruebas de una nueva versión de una aplicación, la variable de salida se puede usar como **entrada** en un *script* que finalice la configuración del **vSRX** antes de continuar con las pruebas.

admin\_customaccount.onmicrosoft.com.vsrx | Outputs

Deployment

Search (Cmd+/)

«

Overview

Inputs

Outputs

Template

managementIP

52.143.183.77

hostname

vsrx-vsrxcustom

Figura 16. Parámetros de salida. Fuente: elaboración propia.

Este ejemplo no está tan **automatizado**, por lo que la configuración del vSRX se hará manualmente. El siguiente paso es usar la IP de administración para **abrir una sesión SSH** e introducir los comandos que muestra la Figura 17.



```
1. ssh
~ $ssh custom-admin@52.143.183.77
The authenticity of host '52.143.183.77 (52.143.183.77)' can't be established.
ECDSA key fingerprint is SHA256:zodd6YaKJN+ve8yd4Pg9DCnGDmxPHk1hWp2dWgJtdQw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.143.183.77' (ECDSA) to the list of known hosts.
Password:
Last login: Wed May 13 07:09:53 2020 from 139.47.100.40
--- JUNOS 15.1X49-D100.6 built 2017-06-28 07:33:31 UTC
custom-admin@vsrx-vsrxcustom> configure
Entering configuration mode

[edit]
custom-admin@vsrx-vsrxcustom# set system root-authentication plain-text-password
New password:
Retype new password:

[edit]
custom-admin@vsrx-vsrxcustom# set interfaces ge-0/0/0 unit 0 family inet address 10.4.1.4/24

[edit]
custom-admin@vsrx-vsrxcustom# set interfaces ge-0/0/1 unit 0 family inet address 10.4.2.4/24

[edit]
custom-admin@vsrx-vsrxcustom# set routing-instances vsrx-vr1 instance-type virtual-router

[edit]
custom-admin@vsrx-vsrxcustom# set routing-instances vsrx-vr1 interface ge-0/0/0.0

[edit]
custom-admin@vsrx-vsrxcustom# set routing-instances vsrx-vr1 interface ge-0/0/1.0

[edit]
custom-admin@vsrx-vsrxcustom# commit check
configuration check succeeds

[edit]
custom-admin@vsrx-vsrxcustom# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless confirmed
commit complete

# commit confirmed will be rolled back in 10 minutes
[edit]
custom-admin@vsrx-vsrxcustom# commit
commit complete

[edit]
custom-admin@vsrx-vsrxcustom#
```

Figura 17. Conexión remota por SSH y configuración inicial de Junas. Fuente: Juniper, 2021.

Esta configuración solo **inicializa** las interfaces y aísla el **tráfico de administración** del tráfico de datos. A partir de este punto, un administrador puede usar la **consola** o la **interfaz web**, a la que también se accede con la IP pública de administración (Figura 18), para configurar reglas de *firewall* entre las redes confiables y no confiables, así como cualquiera de los servicios disponibles en el *appliance* virtual.



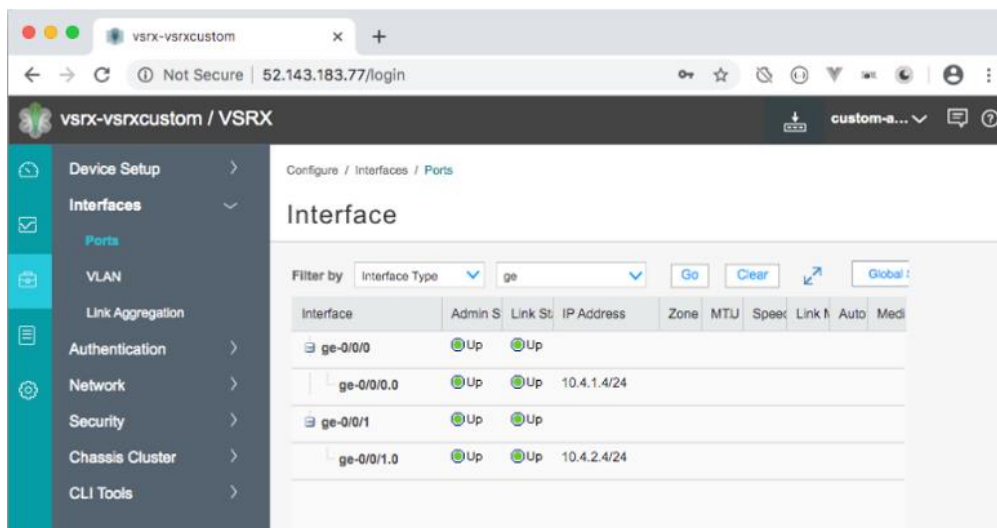


Figura 18. Interfaz web Junos. Fuente: elaboración propia.

La posibilidad de definir las **políticas de red**, con una herramienta ya conocida por los administradores, es muy relevante en entornos corporativos: permite aprovechar la experiencia y conocimientos de administradores de red acostumbrados a unas **herramientas concretas** en un entorno totalmente nuevo, aprovechando lo mejor de ambos mundos.

## Limpieza

Al igual que en el caso práctico anterior, todos los **recursos** se pueden borrar, simplemente, eliminando el grupo de recursos que los contiene.

## 6.5. Caso práctico: VPN en AWS

Al igual que en el caso práctico anterior, este une los dos temas principales de esta asignatura: **redes y seguridad**. En este caso, se explica paso a paso el procedimiento necesario para **configurar una VPN de cliente mediante OpenVPN en AWS** (Amazon Web Services, s. f.).

Las **VPN de cliente** sirven para dar acceso remoto a usuarios individuales. Son útiles, por ejemplo, para **usuarios itinerantes** que necesitan acceder a los recursos de su organización, o para **pequeñas oficinas** en las que no merece la pena la inversión en un dispositivo de VPN corporativo, y prefieren dar acceso individualmente a sus usuarios.

Las VPN **encapsulan el tráfico de la red** origen en otros paquetes, y lo *desencapsulan* en la red destino, depositando el tráfico como si ambas redes estuvieran **interconectadas** por un simple rúter.

En el caso de la **VPN de cliente**, no hay red origen como tal. El cliente de VPN crea una interfaz de red virtual en el equipo del usuario. Cuando se establece la conexión, el cliente de VPN recibe una IP de la red destino, mediante el **servidor DHCP** de la VPN, y la configura en la interfaz virtual. A partir de ese momento, el **tráfico** que los procesos del equipo del usuario envíen a esa interfaz atravesará el túnel de la VPN y llegará a la **red de destino**.

La **arquitectura** del caso práctico consiste, a alto nivel, de los elementos de la Figura 19:

- ▶ La VPC que aloja las subredes de aplicaciones y la subred de los clientes de VPN.
- ▶ La subred VPN, de cuyo rango de IP obtendrán las direcciones los clientes.
- ▶ El VPN *endpoint*, o punto de finalización de la VPN, al que se conectarán los clientes. Actúa como servidor de VPN.
- ▶ Un software de cliente instalado en el equipo.
- ▶ Un certificado de servidor en el servidor de VPN (no aparecen en el diagrama).

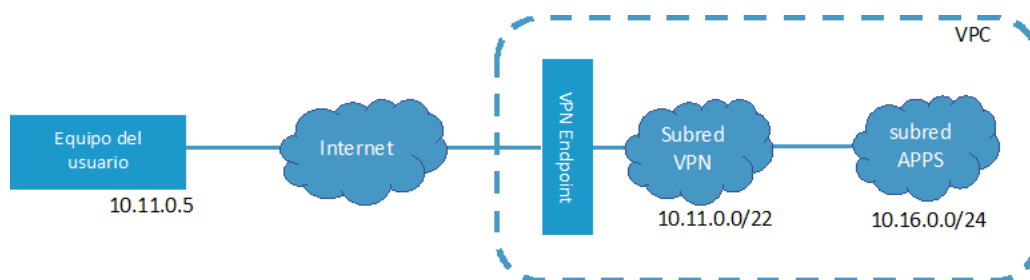


Figura 19. Arquitectura de la conexión con cliente de VPN. Fuente: elaboración propia.

Como requisito para crear un cliente de VPN, AWS requiere un **certificado válido**. Aunque es posible importar certificados existentes, el caso práctico hace uso de **AWS Certificate Manager**, uno de los servicios de nube de AWS que permite administrar autoridades de certificación y certificados. Se creará una CA nueva y un certificado de servidor.

En primer lugar, en la sección de **Certificate Manager** de la consola de AWS, se crea una CA raíz siguiendo el asistente. La Figura 20 muestra los campos del nombre distinguido del certificado.

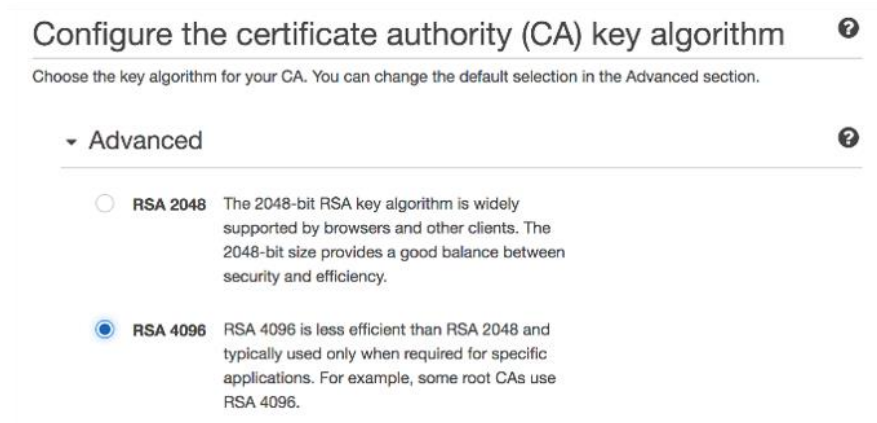
**Configure the certificate authority (CA) name** ?

Name your CA using the distinguished name (DN) format. The name is used as the subject in the CA certificate and as the issuer in certificates that the CA issues. These names cannot be changed later.

Subject distinguished name	Value
Organization (O)*	Custom <small>Company name. Max length of 64 characters.</small>
Organization Unit (OU)*	DemoDept <small>Company subdivision. Max length of 64 characters.</small>
Country name (C)*	Spain (ES) ▼ <small>Two letter country code</small>
State or province name*	Madrid <small>Full name. Max length of 128 characters</small>
Locality name*	Madrid <small>City. Max length of 128 characters.</small>
Common Name (CN)*	CustomCA <small>Certificate authority name. Max length of 64 characters.</small>

Figura 20. Opciones del certificado de la CA. Fuente: elaboración propia.

En el siguiente paso se configura el **tipo de algoritmo** que usarán las claves de la CA. El valor por defecto es **RSA 2048**, pero, para el caso práctico, se ha escogido una longitud de clave de 4096 bits.



**Configure the certificate authority (CA) key algorithm** ?

Choose the key algorithm for your CA. You can change the default selection in the Advanced section.

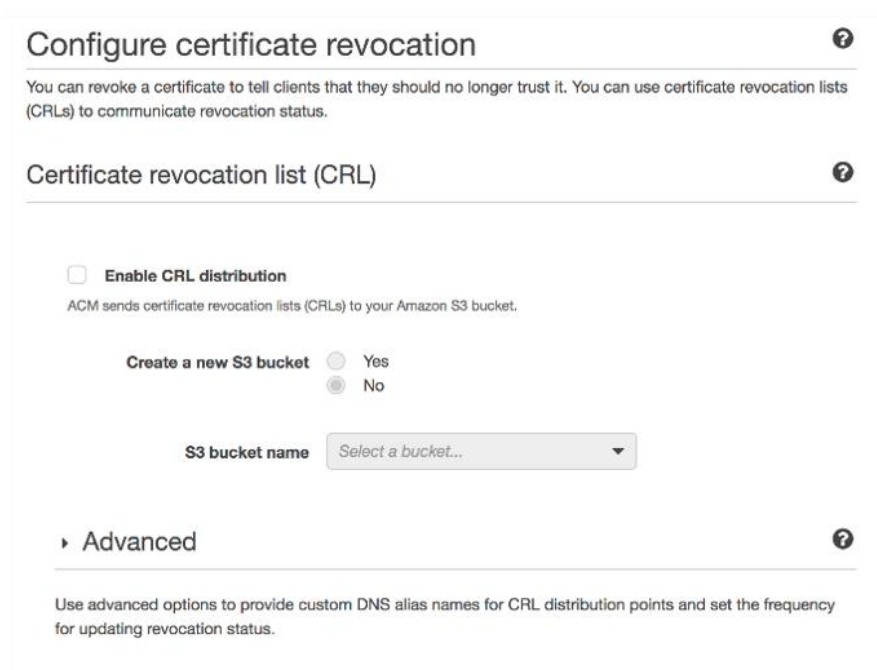
▼ **Advanced** ?

☐ **RSA 2048** The 2048-bit RSA key algorithm is widely supported by browsers and other clients. The 2048-bit size provides a good balance between security and efficiency.

☒ **RSA 4096** RSA 4096 is less efficient than RSA 2048 and typically used only when required for specific applications. For example, some root CAs use RSA 4096.

Figura 21. Elección de longitud clave. Fuente: elaboración propia.

*Certificate Manager* permite mantener una lista de **certificados revocados**. Para el ejemplo no es necesario, ya que la CA va a ser **borrada** inmediatamente. En caso de necesitarla, es tan fácil como indicar un **bucket de S3** donde se almacenará la información de los certificados revocados.



**Configure certificate revocation** ?

You can revoke a certificate to tell clients that they should no longer trust it. You can use certificate revocation lists (CRLs) to communicate revocation status.

**Certificate revocation list (CRL)** ?

☐ **Enable CRL distribution**  
ACM sends certificate revocation lists (CRLs) to your Amazon S3 bucket.

**Create a new S3 bucket** ☐ Yes ☒ No

**S3 bucket name**

► **Advanced** ?

Use advanced options to provide custom DNS alias names for CRL distribution points and set the frequency for updating revocation status.

Figura 22. Configuración de CRL. Fuente: elaboración propia.

El asistente termina ofreciendo la posibilidad de **crear el certificado autofirmado** de la CA raíz recién creada. Una vez creado, es posible descargar el certificado en formato PEM (Figura 24).

### Specify the root CA certificate parameters

We will activate this CA with a self-signed root CA certificate. You can always generate a new certificate later.

Validity

10

Years

Estimated expiration: 2030-05-25 18:32:34UTC

Signature algorithm

SHA256WIT...

Figura 23. Parámetros del certificado de la CA. Fuente: elaboración propia.

CA common name	Organization	OU	Type	Status
<input checked="" type="radio"/> CustomCA	Custom	DemoDept	Root	Active

Status

CA certificate

Revocation configuration

Tags

Permissions

Subject

Organization (O)

Custom

Organization Unit (OU)

DemoDept

Country name (C)

ES

State or province name

Madrid

Locality name

Madrid

Common Name (CN)

CustomCA

CA certificate validity

Not after

Expires in

2030-05-25 18:32:55UTC

3651 Days

Additional information

Signature algorithm

Serial number

SHA256WITHRSA

43917679296488423552875895988262157949

Certificate body

```
-----BEGIN CERTIFICATE-----
MIIFmDCCA4CgAwIBAgIQIQo8w+uotzjurKpPao4+fTANBgkqhkiG9w0BAQsF
ADBM
MQswCQYDVQQGEwJFUzEPMA0GA1UECgwGQ3VzdG9tMREwDwYDVQQLEAhEZW1v
RGVw
dDEPMA0GA1UECAwGTWFKcm1kMREwDwYDVQQDDAhDdXN0b21DQTEPMA0GA1UE
BwwG
TWFKcm1kMB4XDTEwMDUyNTE3MzI1NVoXDTMwMDUyNTE4MzI1NVowZjELMAkG
A1UE
BhMCRVMxZzANBgNVBAoMBkNlc3RvbTERMA8GA1UECwwIRGVtYDZAN
-----END CERTIFICATE-----
```


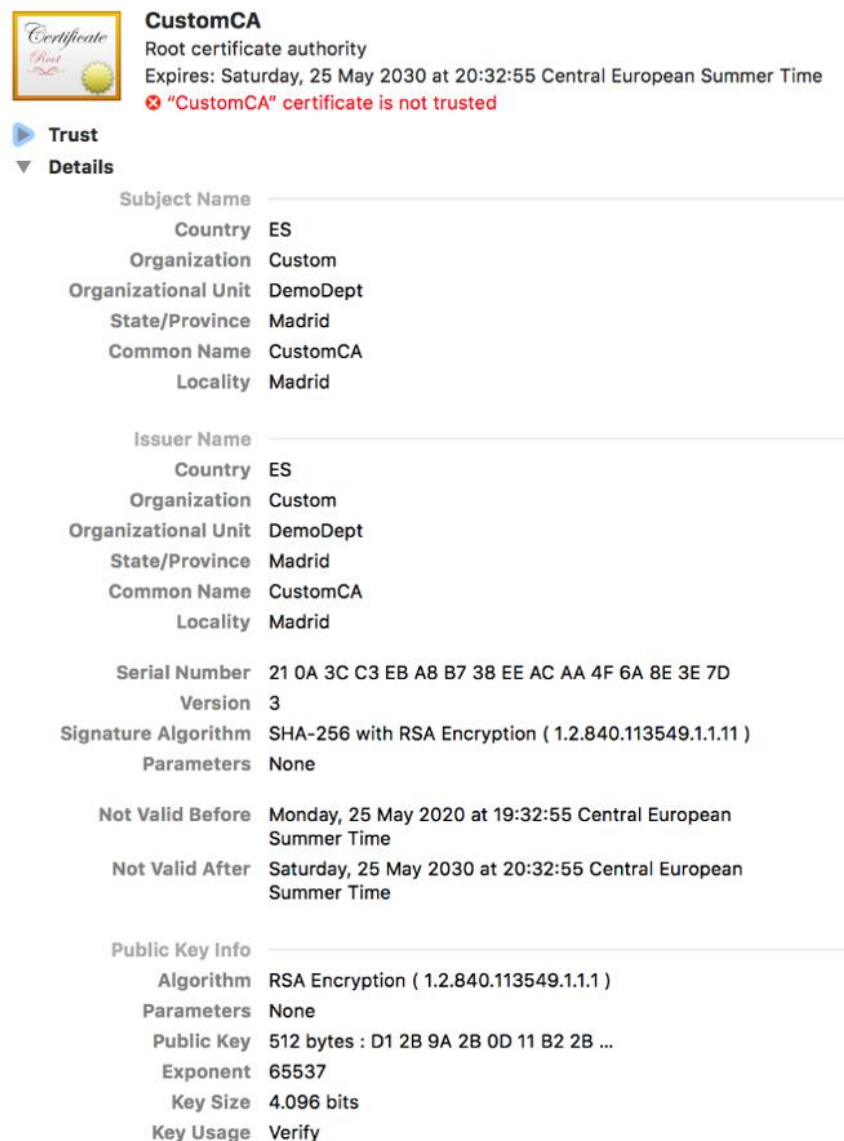
 Export Certificate body to a file

Figura 24. Configuración de la CA raíz. Fuente: elaboración propia.

Este certificado no ha sido emitido por una **autoridad reconocida**, por lo que el **sistema operativo** y los **navegadores** lo considerarían no confiable, como muestra la Figura 25. No obstante, es posible agregarlo al **almacén local** y habilitarlo como confiable. Este archivo se podría transferir a otros equipos de manera segura para que estos pudieran también confiar en la nueva CA.



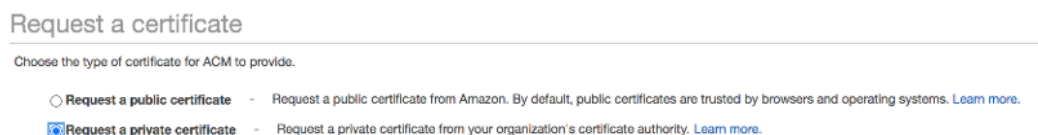
**CustomCA**  
 Root certificate authority  
 Expires: Saturday, 25 May 2030 at 20:32:55 Central European Summer Time  
 ❌ "CustomCA" certificate is not trusted

**Trust**  
 ▼ **Details**

Subject Name	
Country	ES
Organization	Custom
Organizational Unit	DemoDept
State/Province	Madrid
Common Name	CustomCA
Locality	Madrid
Issuer Name	
Country	ES
Organization	Custom
Organizational Unit	DemoDept
State/Province	Madrid
Common Name	CustomCA
Locality	Madrid
Serial Number	21 0A 3C C3 EB A8 B7 38 EE AC AA 4F 6A 8E 3E 7D
Version	3
Signature Algorithm	SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )
Parameters	None
Not Valid Before	Monday, 25 May 2020 at 19:32:55 Central European Summer Time
Not Valid After	Saturday, 25 May 2030 at 20:32:55 Central European Summer Time
Public Key Info	
Algorithm	RSA Encryption ( 1.2.840.113549.1.1.1 )
Parameters	None
Public Key	512 bytes : D1 2B 9A 2B 0D 11 B2 2B ...
Exponent	65537
Key Size	4.096 bits
Key Usage	Verify

Figura 25. Certificado de la CA. Fuente: elaboración propia.

En cualquier caso, el **certificado de la CA** no se puede usar como **certificado de servidor**. Para ello, hay que crear un **certificado privado** firmado por la CA. Se tratará de un certificado privado, ya que es para uso exclusivamente interno, y será emitido por esta CA.



Request a certificate

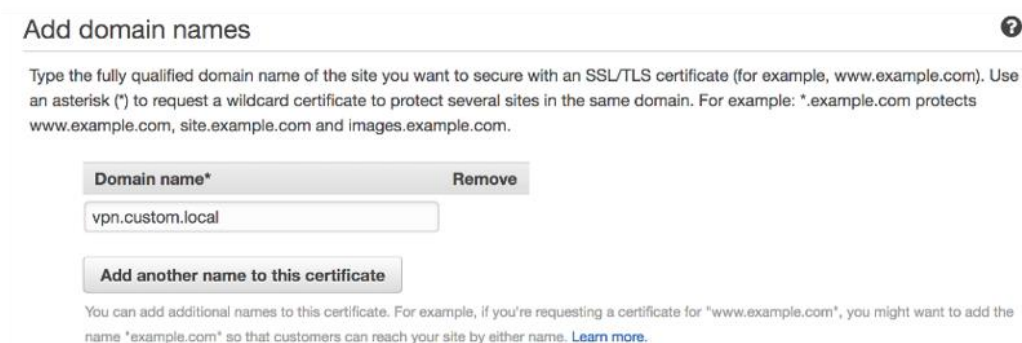
Choose the type of certificate for ACM to provide.

☐ Request a public certificate - Request a public certificate from Amazon. By default, public certificates are trusted by browsers and operating systems. [Learn more.](#)

☒ Request a private certificate - Request a private certificate from your organization's certificate authority. [Learn more.](#)

Figura 26. Creación de certificado privado. Fuente: elaboración propia.

Aunque no es relevante en este caso, es posible **añadir** un **nombre DNS** al certificado. En el caso de la Figura 27, este certificado podría usarse en un servidor web, que alojara la web, bajo el nombre de host `vpn.custom.local`.



Add domain names

Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, `www.example.com`). Use an asterisk (\*) to request a wildcard certificate to protect several sites in the same domain. For example: `*.example.com` protects `www.example.com`, `site.example.com` and `images.example.com`.

Domain name*	Remove
vpn.custom.local	

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for `"www.example.com"`, you might want to add the name `"example.com"` so that customers can reach your site by either name. [Learn more.](#)

Figura 27. Nombre DNS del certificado. Fuente: elaboración propia.

Figura 28. Certificado privado ya creado. Fuente: elaboración propia.

Una vez completado el asistente, la consola ofrece la opción de **descargar** tres archivos en formato PEM: el certificado, la cadena de certificados (que solo incluye el certificado de la CA) y la clave privada. La clave privada estará **protegida**, obligatoriamente, por una clave o *passphrase*. El certificado y la clave serán necesarios más adelante.

A continuación, hay que asegurarse de que hay una **VPC disponible**. La Figura 29 muestra los detalles de la VPC del ejemplo. La subred, de donde recibirán las IP los clientes VPN, deberá estar **contenida** en el rango de esta VPC, 10.10.0.0/16.

</

Figura 29. VPC del cliente VPN. Fuente: elaboración propia.



El siguiente paso es **crear el Client VPN**, como llama AWS a los **puntos de terminación** de VPN de cliente. El campo **Client IPv4 CIDR** es el rango del que recibirán IP los clientes VPN. También hay que especificar el **ARN** del certificado creado, anteriormente, en *Server certificate* ARN (el ARN es el identificador único de los recursos en AWS).

El cliente de servidor se puede usar también como **elemento de autenticación** de cliente, por lo que se especifica el mismo ARN en el campo *Client certificate* ARN. Si se crean **certificados específicos** para cada usuario con el procedimiento anterior, también se podrán usar con el cliente de VPN.

Create a new Client VPN endpoint to enable clients to access networks over a TLS VPN session

Name Tag: customVPN ⓘ

Description: ⓘ

Client IPv4 CIDR\*: 10.11.0.0/22 ⓘ

Authentication Information

Server certificate ARN\*: arn:aws:acm:eu-west-1:014641795089:certificate... ⓘ

Authentication Options: Choose one or more authentication methods from below ⓘ

☒ Use mutual authentication

☐ Use user-based authentication

Client certificate ARN\*: arn:aws:acm:eu-west-1:014641795089:certificate... ⓘ

Figura 30. Opciones de creación de Client VPN. Fuente: elaboración propia.

Para terminar, hay que **especificar los servidores DNS** que se configurarán en el cliente, la **VPC** a la que estarán asociadas las conexiones y un **grupo de seguridad**. Este grupo de seguridad controlará el tráfico desde y hacia las IP de los clientes conectados.

Other optional parameters

DNS Server 1 IP address

DNS Server 2 IP address

Transport Protocol ☐ TCP ☒ UDP

Enable split-tunnel ☐

VPC ID

Security Group IDs

Select security groups

< 1 to 1 of 1 >

Group ID	Group Name	VPC ID	Description
sg-057cf20bb1e73805f	-	vpc-0fa3e8831d4c0586	-

Close

VPN port

Figura 31. Opciones del cliente VPN. Fuente: elaboración propia.

Una vez creado el *client VPN*, hay que **asociarlo** a una **subred**. AWS configurará automáticamente una **tabla de rutas**, pero se pueden personalizar.

Client VPN Endpoint: cvpn-endpoint-0e0cc53d3f71f1eb9

Summary Associations Security Groups Authorization Route Table Connections Tags

Associate Disassociate

Filter by attributes or search by keyword < 1 to 1 of 1 >

Association ID	Network ID	Description	Endpoint ID	State	Security Groups
cvpn-assoc-06...	subnet-0b72d6...	-	cvpn-endpoint-...	Associating	sg-057cf20bb1e73805f

Figura 32. Asociación de subred al cliente VPN. Fuente: elaboración propia.

En este punto ya es posible **descargar** la **configuración del cliente**. Este archivo contiene la configuración de conexión, que pueden leer los clientes, compatible con **OpenVPN**. Estos archivos son de texto sencillo y se pueden editar manualmente.

**Download Client Configuration**

Download VPN client configuration file for the Client VPN Endpoint

Client VPN Endpoint ID cvpn-endpoint-0e0cc53d3f71f1eb9

Figura 33. Descarga de configuración de cliente. Fuente: elaboración propia.

El **archivo** del caso práctico será más o menos así:

```
client
dev tun
proto udp
remote          cvpn-endpoint-0e0cc53d3f71f1eb9.prod.clientvpn.eu-west-
1.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
verb 3
<ca>
-----BEGIN CERTIFICATE-----
MIIFmDCCA4CgAwIBAgIQIQo8w+uotzjurKpPao4+fTANBgkqhkiG9w0BAQsFADBm
MQswCQYDVQQGEwJFUzEPMA0GA1UECgwGQ3VzdG9tMREwDwYDVQQLEhEZW1vRGVw
...
70aXzkHei4WjHZtmL3arciml2XpX2oMVSXtdzhh+t+ppT50B2/d1+EFMo94=
-----END CERTIFICATE-----

</ca>
reneg-sec 0
```

No obstante, el **fichero de configuración** no se podrá conectar, ya que no contiene el certificado de cliente. Para ello, se usarán los **ficheros** descargados anteriormente. Si el certificado se ha guardado en el fichero `custom.crt`, y la clave en `custom.key`, habrá que añadir las dos siguientes líneas al fichero `.ovpn`.

```
cert custom.crt
key custom.key
```

Como cliente de **OpenVPN** se ha usado [Tunnelblick](#), que es un **cliente gratuito** y de **código abierto**. Tunnelblick puede abrir los archivos `.ovpn` directamente. Una vez añadida la configuración, es posible establecer el túnel a través del menú del programa.

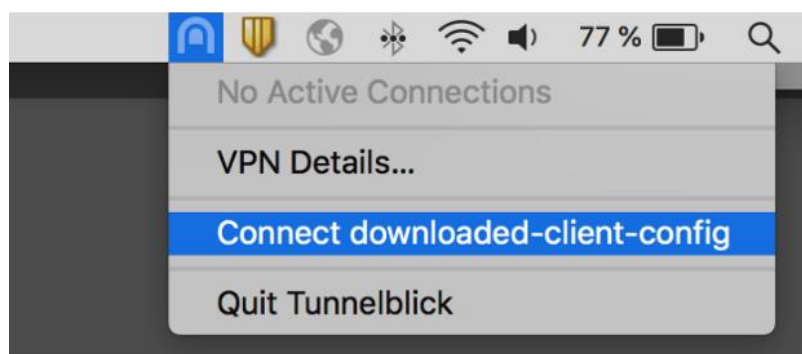


Figura 34. Conexión VPN con Tunnelblick. Fuente: elaboración propia.

Tunnelblick pedirá la **clave privada** al hacer clic en Connect. Esta *passphrase* se especificó al descargar el certificado de servidor. Si todo ha ido bien, aparecerá un mensaje de Tunnelblick parecido a la Figura 35.

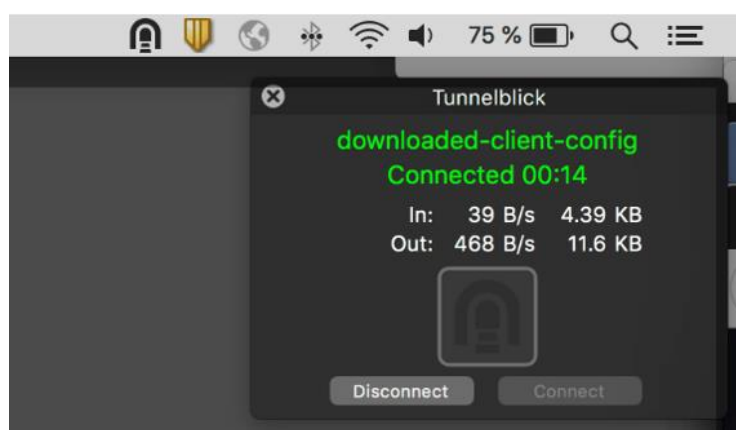


Figura 35. Conexión de Tunnelblick correcta. Fuente: elaboración propia.

El cliente habrá recibido una **IP de la subred de destino**. Aunque, en el ejemplo, no se configuraron servidores DNS, ya sería posible establecer conexiones SSH o RDP a instancias de la VPC, siempre y cuando el **grupo de seguridad** lo permitiera.

## 6.6. Referencias bibliográficas

Amazon Web Services. (S. f.). *Client VPN endpoints*.

<https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-working-endpoints.html>

Juniper. (2021, junio 7). *vSRX Deployment Guide for Private and Public Cloud Platforms*.

[https://www.juniper.net/documentation/en\\_US/vsrx/information-products/pathway-pages/security-vsrx-azure-guide-pwp.html](https://www.juniper.net/documentation/en_US/vsrx/information-products/pathway-pages/security-vsrx-azure-guide-pwp.html)

Microsoft. (2020, diciembre 21). *Define resources in ARM templates*.

<https://docs.microsoft.com/en-us/azure/templates/>

Microsoft. (2021, junio 3). *Tutorial: Filter network traffic with a network security group using the Azure portal*.

<https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic>

Microsoft. (2021, marzo 12). *What are ARM templates?*

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/overview>

Tullock, M. (2013). *Introducing Windows Azure for IT Professionals*. Microsoft Press.

## The Journey to Cloud Networking

Sciarrilli, N. (2020, abril 28). *The Journey to Cloud Networking*.  
<https://aws.amazon.com/es/blogs/architecture/the-journey-to-cloud-networking/>

Este pequeño artículo repasa algunas ideas que sirven para reflexionar sobre cómo afrontar un despliegue o una migración de redes a la nube. Es específico de AWS, pero las ideas que plantea aplican a cualquier proveedor.

## Despliegue de Cisco en AWS

Cisco Systems. (2019, junio 16). *Deploying Cisco Web Security and Security Management Virtual Appliances on Amazon. Elastic Compute Cloud on Amazon Web Services*.  
[https://www.cisco.com/c/dam/en/us/td/docs/security/content\\_security/virtual\\_appliances/Cisco\\_Content\\_Security\\_Virtual\\_Appliance\\_Install\\_Guide\\_AWS\\_EC2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide_AWS_EC2.pdf)

Esta guía paso a paso es parecida al segundo caso práctico, pero aplicada a un *appliance* virtual de Cisco en la nube de AWS. Es interesante comparar los tipos de recursos ofrecidos por uno y otro proveedor, y cómo los fabricantes de productos de seguridad y red se adaptan a ellos.

## Arquitectura con múltiples redes virtuales en AWS

Amazon Web Services. (2020). *Building a Scalable and Secure Multi-VPC AWS Network Infrastructure*. [https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf?did=wp\\_card&trk=wp\\_card](https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf?did=wp_card&trk=wp_card)

Esta guía presenta una arquitectura de red compleja para AWS. No es una guía paso a paso, sino una guía de referencia, en la que se explica brevemente los recursos que va a usar, qué papel juegan en esta arquitectura y cómo se integran entre ellos. Es más avanzada que los ejemplos presentados hasta ahora, pero, gracias a las descripciones de los recursos, es fácil de seguir, incluso con poca experiencia en AWS.

## Azure Quickstart Templates

Microsoft Azure. (<https://azure.microsoft.com/en-us/resources/templates/>).

Plantillas para despliegue inmediato, o como punto de partida para realizar plantillas personalizadas.

1. ¿Qué rango de IP puede tener una subred en Azure?
  - A. 10.0.1.0/24.
  - B. 10.0.0.0/16.
  - C. 192.168.0.0/24.
  - D. Cualquiera de los anteriores.
  
2. ¿Cómo es posible definir el destino concreto de una regla de entrada en un grupo de seguridad de red sin conocer la IP de destino?
  - A. Usando un grupo de seguridad de aplicación, y aplicando este grupo a la NIC de una máquina virtual.
  - B. Con un asterisco.
  - C. Con la dirección 0.0.0.0/0.
  - D. No se puede.
  
3. ¿Qué razones se pueden dar para usar una solución de red de otro fabricante en un proveedor de nube?
  - A. Para aprovechar la experiencia de los administradores.
  - B. Para disponer de más funcionalidades que las ofrecidas por los servicios nativos.
  - C. Todas las anteriores.
  - D. No se puede: en la nube solo se pueden usar servicios propios de cada proveedor.
  
4. ¿Qué tipos de recursos se pueden desplegar con una plantilla de ARM?
  - A. Máquinas virtuales.
  - B. Redes, subredes y grupos de seguridad.
  - C. Discos e interfaces de red.
  - D. Todos los anteriores.



5. ¿Qué significa que las plantillas ARM sean declarativas?
- A. Que el desarrollador declara las variables explícitamente.
  - B. Que la plantilla define el estado final deseado, sin expresar los pasos que hay que dar para llegar al él.
  - C. Que se pueden ejecutar varias veces y se conseguirá el mismo resultado.
  - D. Las plantillas ARM son imperativas, no declarativas.
6. ¿Qué significa que las plantillas ARM sean idempotentes?
- A. Que la plantilla define el estado final, no los pasos que hay que dar para llegar a él.
  - B. Que se pueden parametrizar.
  - C. Que tienen variables de salida.
  - D. Que una misma plantilla se puede ejecutar varias veces y el resultado será el mismo.
7. ¿Cómo afecta el orden de las reglas de un grupo de seguridad?
- A. Se evaluarán por orden creciente de prioridad. Si una regla se activa con un paquete, ya no se procesan más reglas.
  - B. El orden no afecta, todas las reglas se aplican a todos los paquetes.
  - C. Se evaluarán primero las que tengan una prioridad más alta.
  - D. Se evaluarán por orden creciente de puerto de destino.
8. ¿Qué IP recibe un cliente VPN al establecer la conexión?
- A. Una de la red privada local.
  - B. Una de la subred establecida en el servidor de VPN.
  - C. Ninguna, se enruta el tráfico con la IP de la red local.
  - D. Una de la subred de aplicaciones que se quiere administrar.