Para el desarrollo de esta actividad se plantea una empresa financiera; para ello se plantea la siguiente infraestructura de red:

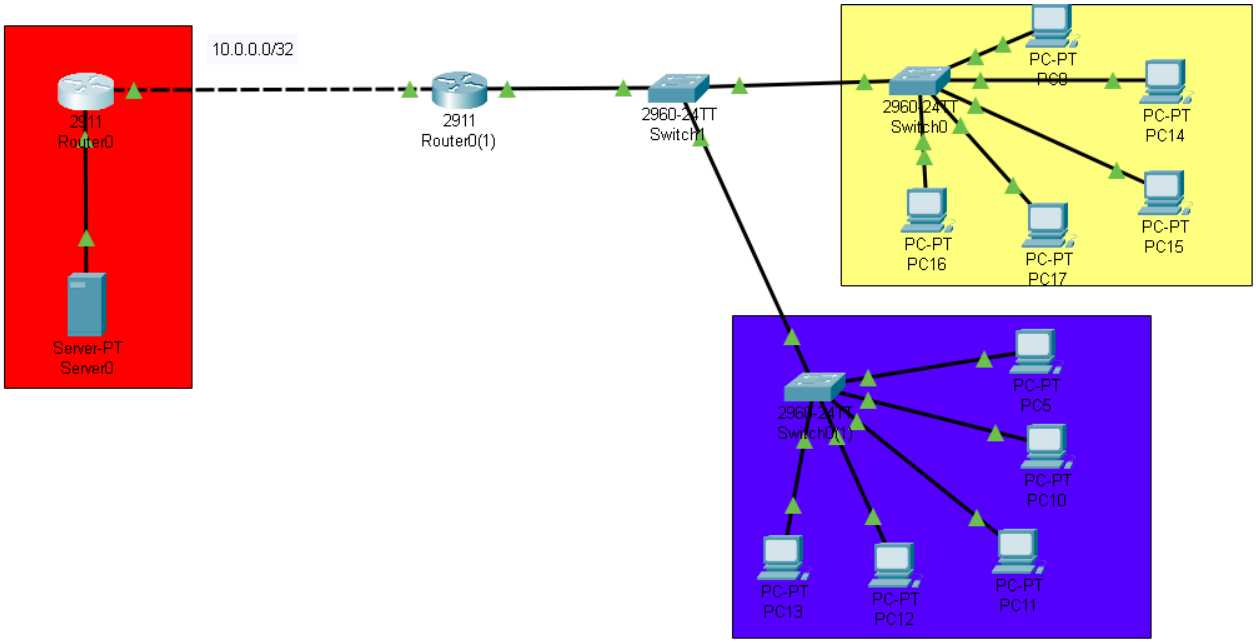

Ilustración 1. infraestructura de red.

En la ilustración 1, se tiene dos segmentos de red con vlan 10 en el área de color amarillo asignado a contabilidad y vlan 20 en el área de color azul asignado para administrativos y se configuro un servidor de HTTTP en el área de color rojo.

Para poder configurar estas vlans en el router, se establece una segmentación de red donde se tiene direcciones ip 192.168.0.0/25 con mascara de red 255.255.255.128; para el área de contabilidad se tiene direcciones ip desde la 192.168.1.0 hasta 192.168.1.127; donde se tiene la dirección de red 192.168.1.0, broadcast 192.168.1.127 y vlan10.

Para el área administrativos se tiene la dirección de red 192.168.1.128, broadcast 192.168.1.255 y vlan20.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.0.0.2        YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  up                    up
GigabitEthernet0/1.10  192.168.1.1     YES manual up                    up
GigabitEthernet0/1.20  192.168.1.129   YES manual up                    up
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Ilustración 2. Asignación de direcciones ip y vlans

Luego de tener la segmentación y vlan configurados en el router, se debe indicar a los switchs que vlan se habilitara para el trafico en la red además de poner el habilitar el modo troncal para un único enlace físico de transporte de tráfico de múltiples VLANs a través de una red.

```
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk allowed vlan 20
 switchport mode trunk
```

Ilustración 3.Configuración de switch para tráfico de red conforme las vlan configuradas.

Para este caso como del router viene la configuración de la vlan 10 y 20, esas ingresan al switch por el puerto FastEthernet0/1, luego se configura la vlan para cada switch en el puerto FastEthernet0/2 y FastEthernet0/3 como se observa en la ilustración 3.

```
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/2
 switchport trunk allowed vlan 20
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
```

Ilustración 4. Configuración de troncal de vlan 20.

Luego nos ubicamos en el switch que esta ubicado en cada área, que para esta explicación es el área administrativos, para este caso se tiene que habilitar el modo troncal de la vlan 20 en el puerto FastEthernet0/2 que está conectado al switch que divide las troncales de las vlan como se observa en la ilustración 4.

Para habilitar cada puerto de ese switch y conectar un punto final, se realiza el siguiente comando:

switchport access vlan 20

switchport mode access

con estas dos líneas de comando; lo que le indicamos al switch es que habilite el modo de acceso a la troncal de vlan 20, este comando se pone para cada punto final que se desee instalar; y este mismo proceso se realiza para el área de contabilidad, pero solo cambia la vlan de 20 a 10.

Luego se configura el servidor con la dirección ip 192.168.2.3; el router que conecta a ese servidor es 10.0.0.1 con direccionamiento a las direcciones ip 192.168.2.0/25; y del router donde se configuro las vlan con dirección 10.0.0.2 con direccionamiento a las ip 192.168.1.0/24.

Firewall:

Para este caso se establece las siguientes reglas en el router donde se configuro las vlan:

```
Extended IP access list FIREWALL
    10 deny ip 192.168.1.0 0.0.0.127 192.168.1.128 0.0.0.127 (4 match(es))
    20 permit ip any any
    30 permit ip 192.168.1.0 0.0.0.255 any
    40 deny ip any any
    50 permit tcp 192.168.1.128 0.0.0.127 192.168.1.0 0.0.0.127 eq www
Extended IP access list IDS_RULES
    10 permit tcp any host 192.168.2.3 eq www
    20 permit ip any any
    30 permit tcp 192.168.1.128 0.0.0.127 192.168.1.0 0.0.0.127 eq 443
Extended IP access list IPS_RULES
    10 deny tcp any host 192.168.2.3 eq telnet
    20 permit ip any any
```

Ilustración 5.configuración de reglas basicas de firewall.

Como se observa en la ilustración, se plantea una regla principal que es la denegación de conectividad entre el área administrativa y contabilidad, se coloca además unas reglas de IDS en el puerto 80 y 443 e IPS en el puerto de 23 de TCP.

Acceso remoto IPSEC:

Para este caso se usa el modelo de router 2911; una característica es que estos router no tienen habilitado el modo securityk9, que permite configurar el protocolo de acceso remoto IPSEC. Para ello se utiliza el siguiente comando desde la terminal:

License boot module C2900 tecnhology package securityk9

Luego de estar activado verificamos que este el enabled en yes como se observa en la ilustración 6:

Feature name	Enforcement	Evaluation	Subscription	Enabled	RightToUse
ipbasek9	no	no	no	yes	no
securityk9	yes	yes	no	yes	yes
datak9	yes	no	no	no	yes
uck9	yes	yes	no	no	yes

Ilustración 6.Habilitar el securityk9.

Luego se procede a configurar el IPSEC en el router que conecta al server, asignando una política 10 de isakmp, un grupo llamado Grupovpn con contraseña compartida key123$ y creando los siguientes usuarios con encriptación aes de 256bits.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
```

Ilustración 7. configuración de la encriptación

Luego se crea los usuarios y contraseñas encriptadas, y se crea el mapa estático de autenticación, autorización y configuración:

```
username admin privilege 15 secret 5 $1$mERr$AFX/pZT1Lh7NP3Dp3P/qq/
username admin1 secret 5 $1$mERr$DVT3wFEJ5lyHdllIg1ht60
username admin2 secret 5 $1$mERr$DVT3wFEJ5lyHdllIg1ht60
username cont1 secret 5 $1$mERr$DVT3wFEJ5lyHdllIg1ht60
username cont2 secret 5 $1$mERr$DVT3wFEJ5lyHdllIg1ht60
!
!
license udi pid CISCO2911/K9 sn FTX1524BT24-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
!
!
crypto isakmp client configuration group GrupoVPN
 key vpn123$
 pool POOLVPN
!
!
crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
!
crypto dynamic-map DinamicoVPN 10
 set transform-set SetVPN
 reverse-route
!
crypto map MapaEstatico client authentication list UsuarioVPN
crypto map MapaEstatico isakmp authorization list GrupoVPN
crypto map MapaEstatico client configuration address respond
crypto map MapaEstatico 20 ipsec-isakmp dynamic DinamicoVPN
```

Ilustración 8. configuración del VPN IPSEC.

Finalmente se realiza pruebas de conexión tanto del área de administrativos como de contabilidad:

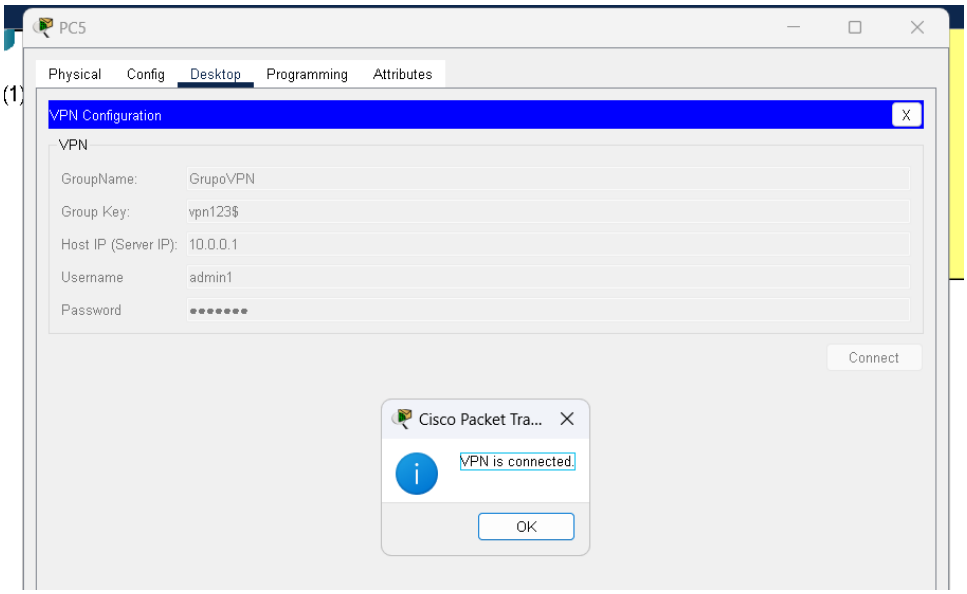

Ilustración 9. Conectividad VPN desde administrativos.

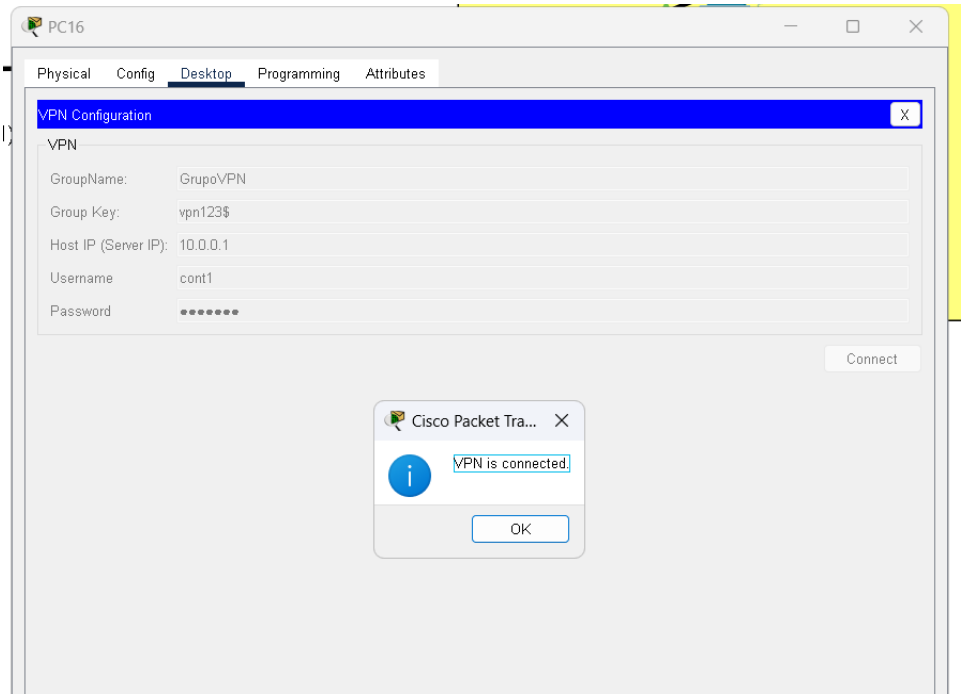

Ilustración 10.Conectividad VPN desde contabilidad.

HTTP:

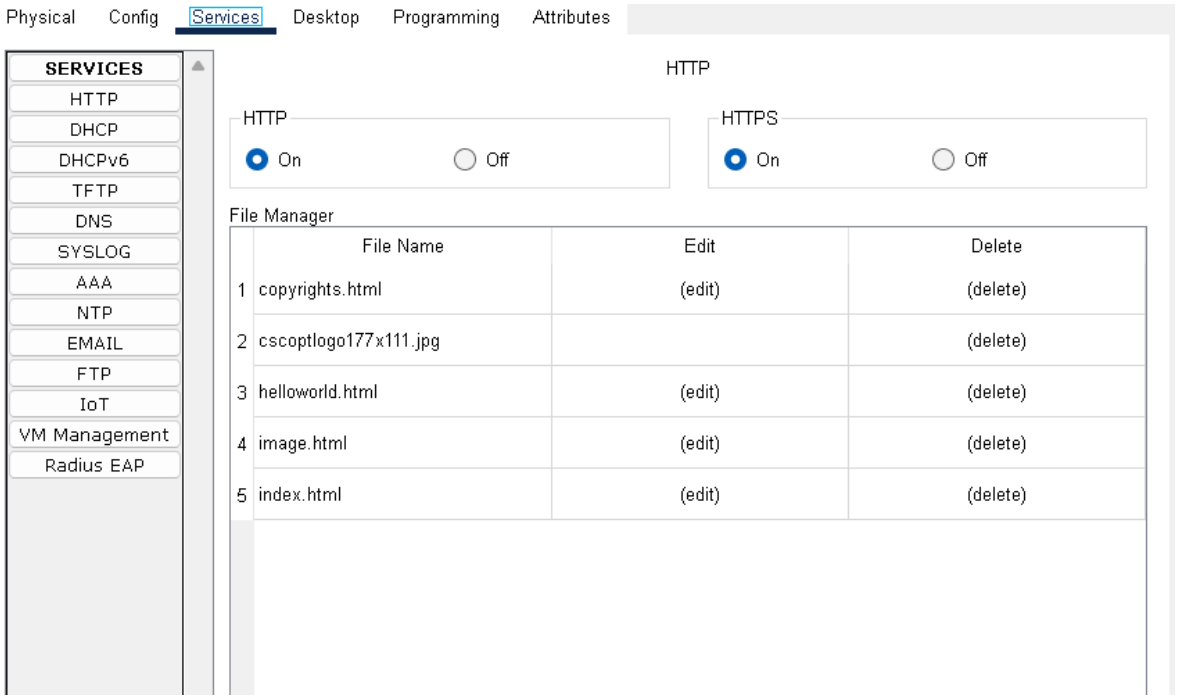

Ilustración 11. Servicios de HTTP en el server.

En la ilustración 11 se observa la activación de servicio HTTP y HTTPS, se observan archivos html en donde se modifica el diseño de index.html para visualizar mejor el menú de redirecciones a los demás archivos de copyrights, cscptlogo, helloworld e image. Para validar conexión al servicio se conecta desde un pc de administrativos el acceso a HTTP y HTTPS:

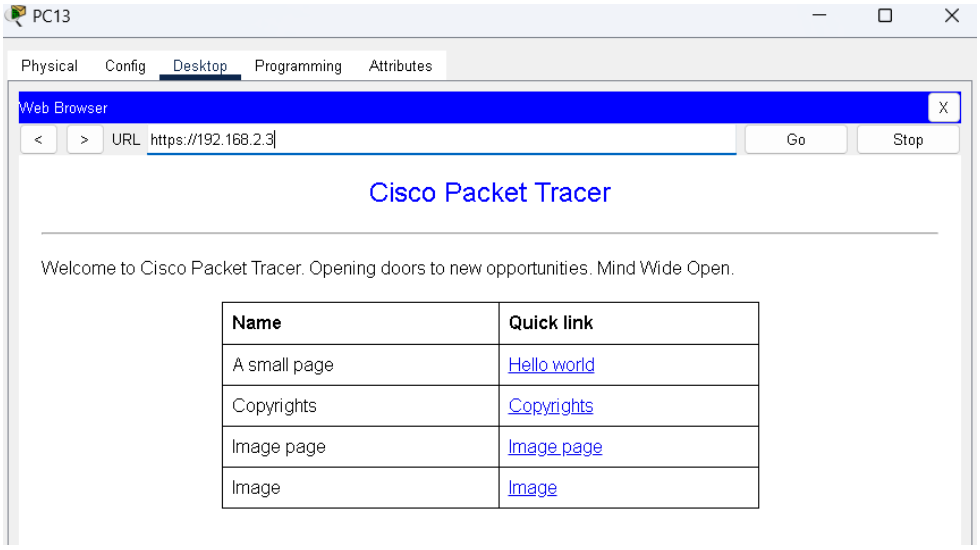

Ilustración 12. Acceso a HTTPS desde un pc de administrativos

Ilustración 13. Acceso a HTTP desde un pc de administrativos

Para este caso no tenemos acceso a paginas con protocolo http; lo que nos indica que el firewall si está filtrando. Y esto se valida con la siguiente ilustración 14.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.2.3 443
Trying 192.168.2.3 ...Open

[Connection to 192.168.2.3 closed by foreign host]
C:\>telnet 192.168.2.3 80
Trying 192.168.2.3 ...
% Connection timed out; remote host not responding
C:\>
```

Ilustración 14. Validación de conexión al puerto 80 y 443.