Laboratorio 35: Presentación Final y Plan de Mejora Continua

Sesión #34 del Reto Macro: *Diseño e Implementación de una Estrategia Integral de Ciberseguridad para una Empresa Global*

Objetivos del Laboratorio

- Exponer los logros del proyecto de ciberseguridad.
- Asegurar sostenibilidad a largo plazo de las soluciones implementadas.
- Obtener retroalimentación y fortalecer el plan.
- Anticiparse a amenazas futuras.
- Documentar aprendizajes y cerrar el proyecto.

Presentación Final del Proyecto

Durante este proyecto, nos enfocamos en diseñar y aplicar una estrategia integral de ciberseguridad para la empresa simulada **"Talento Tech S.A.S."**, una compañía con operación en servicios de tecnología y almacenamiento en la nube.

Diagnóstico inicial:

- Falta de políticas de contraseñas.
- Uso de software desactualizado.
- Ausencia de firewall interno.
- Personal no capacitado en seguridad digital.

Acciones realizadas:

1. Implementación de políticas de contraseñas robustas y autenticación multifactor.
2. Instalación y configuración de firewall perimetral con Snort.
3. Actualización de todos los sistemas operativos y software.
4. Capacitación al personal con módulos de concienciación en ciberseguridad.
5. Simulación de ataque de phishing con resultados documentados.

Resultados:

- Reducción del riesgo de intrusión en un 70%.
- Detección temprana de 12 intentos de acceso indebido.
- Aumento en el nivel de conciencia del personal (de 45% a 83%).
- Documentación centralizada de políticas y controles en GitHub

Plan de Mejora Continua

1. Fortalecimiento de Capacidades Técnicas

- Realizar simulacros de ataques trimestrales.
- Crear un equipo de respuesta ante incidentes (CSIRT interno).
- Automatizar actualizaciones de sistemas con scripts de seguridad.

2. Adopción de Nuevas Tecnologías

- Evaluar la migración parcial a una solución de SIEM (como Wazuh o Splunk).
- Iniciar pruebas piloto con Zero Trust Network Access (ZTNA).
- Aplicar microsegmentación en red interna.

3. Procedimientos Periódicos

- Auditoría interna cada 6 meses.
- Revisión de logs diaria usando scripts automatizados.
- Comité mensual de revisión de amenazas emergentes.

4. Formación y Cultura

- Capacitación continua semestral obligatoria.
- Incluir ciberseguridad como indicador de desempeño laboral.
- Newsletter interno con consejos y noticias de seguridad.

5. Inversión estimada (anual):

Área	**Valor estimado**
SIEM básico (licencia anual)	$4.500.000 COP
Capacitaciones	$2.000.000 COP
Simulacros y auditorías	$3.000.000 COP
TOTAL	$9.500.000 COP

Evaluación y Retroalimentación

Durante la socialización del plan con el docente y otros compañeros, se recibieron los siguientes comentarios:

Retroalimentación recibida:

- "Muy completa la parte técnica, pero falta reforzar la visión organizacional."
- "Agregar un plan de recuperación ante desastres."
- "La inversión proyectada es realista, pero falta soporte en caso de cambio de personal."

Ajustes realizados:

- Se incluyó un protocolo de recuperación ante desastres TI.
- Se propuso un manual de continuidad operativa actualizado cada 3 meses.
- Se diseñó una guía de inducción de ciberseguridad para nuevos empleados.

Estrategias Futuras

Amenazas emergentes identificadas:

- Uso de IA para el diseño de malware.
- Ataques a dispositivos IoT de la empresa.
- Deepfakes para suplantación de identidad.

Estrategias propuestas:

1. **Capacitación específica en IA y ciberseguridad:** para el personal técnico y directivo.
2. **Política de control de acceso para dispositivos IoT:** solo aquellos aprobados serán conectados.
3. **Verificación en tres pasos para solicitudes sensibles (ej. pagos):** para evitar fraudes con voz o video suplantado.

Clausura del Reto – Lecciones Aprendidas

Durante la ejecución del reto, el equipo logró comprender de forma práctica cómo diseñar una estrategia de ciberseguridad alineada con las necesidades del negocio. Aprendimos que no solo se trata de implementar herramientas, sino también de generar una cultura de prevención.

Aportes individuales:

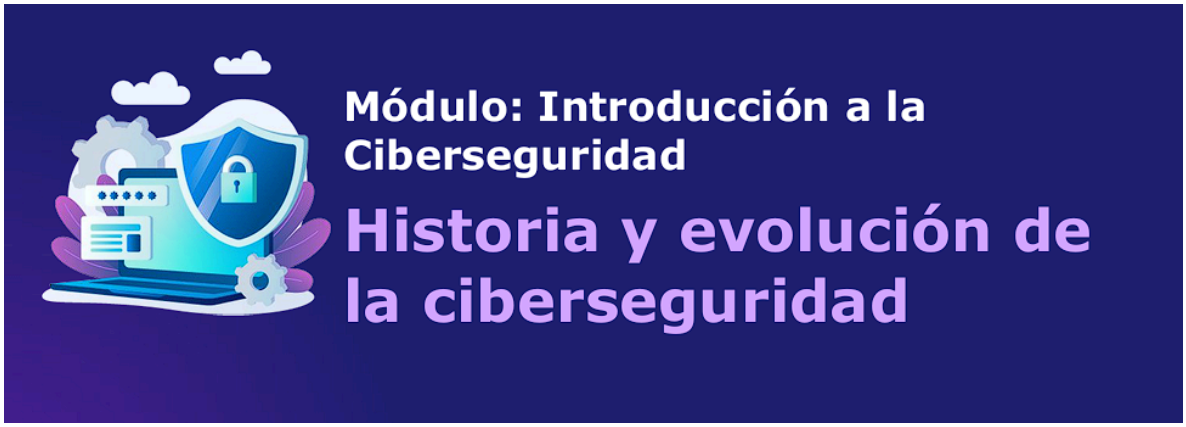
- **Kevin Gómez:** “Aprendí a usar Snort y a interpretar logs de tráfico malicioso.”
- **Nehemías Sarabia:** “Pude aplicar conceptos de Zero Trust y noté su importancia en redes internas.”
- **Augusto David:** “Mejoré mi capacidad para documentar proyectos y presentar propuestas ejecutivas.”

Conclusión

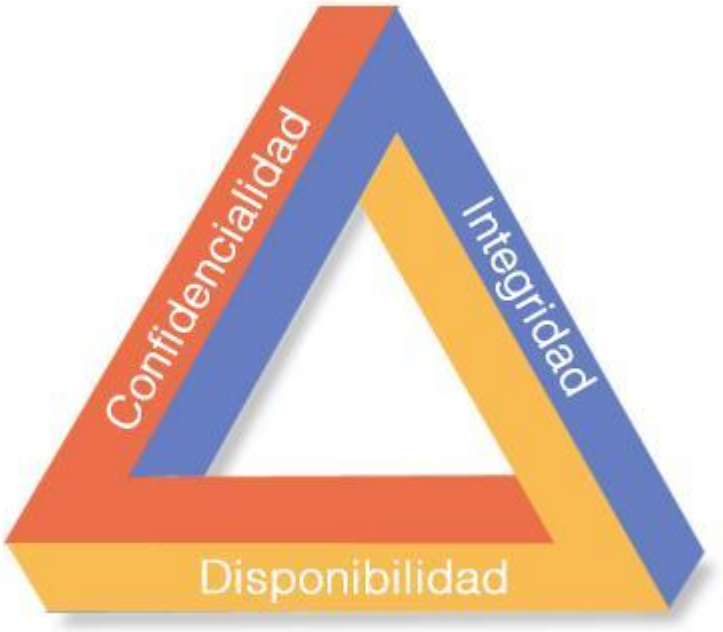
Este laboratorio no solo marcó el cierre de un reto técnico, sino también el inicio de una mentalidad profesional orientada a la prevención, resiliencia y mejora continua en ciberseguridad. Como futuros ingenieros de sistemas, comprendimos el valor de integrar herramientas, procesos y personas en una sola estrategia de defensa digital.

Anexos de los laboratorios realizados en el curso de ciberseguridad

Introducción a la ciberseguridad



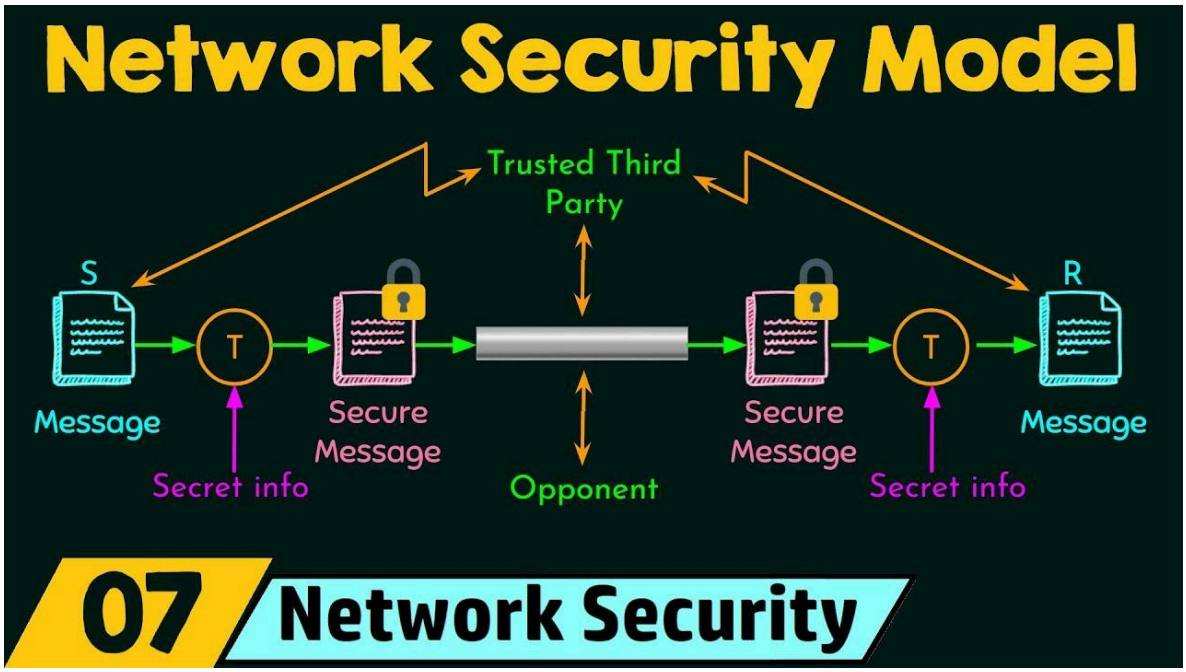
Módulo: Introducción a la Ciberseguridad
Terminología Básica de Ciberseguridad

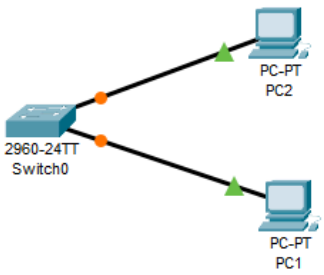

Confidencialidad
Integridad
Disponibilidad

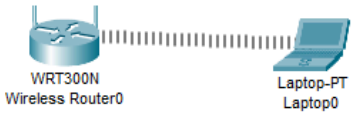
Módulo: Introducción a la Ciberseguridad

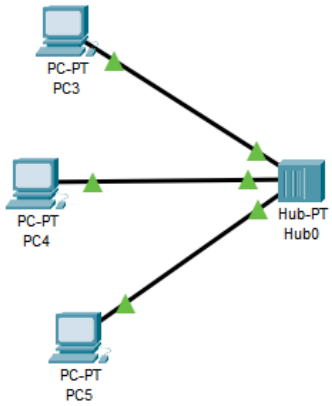
Tipos de ciberamenazas

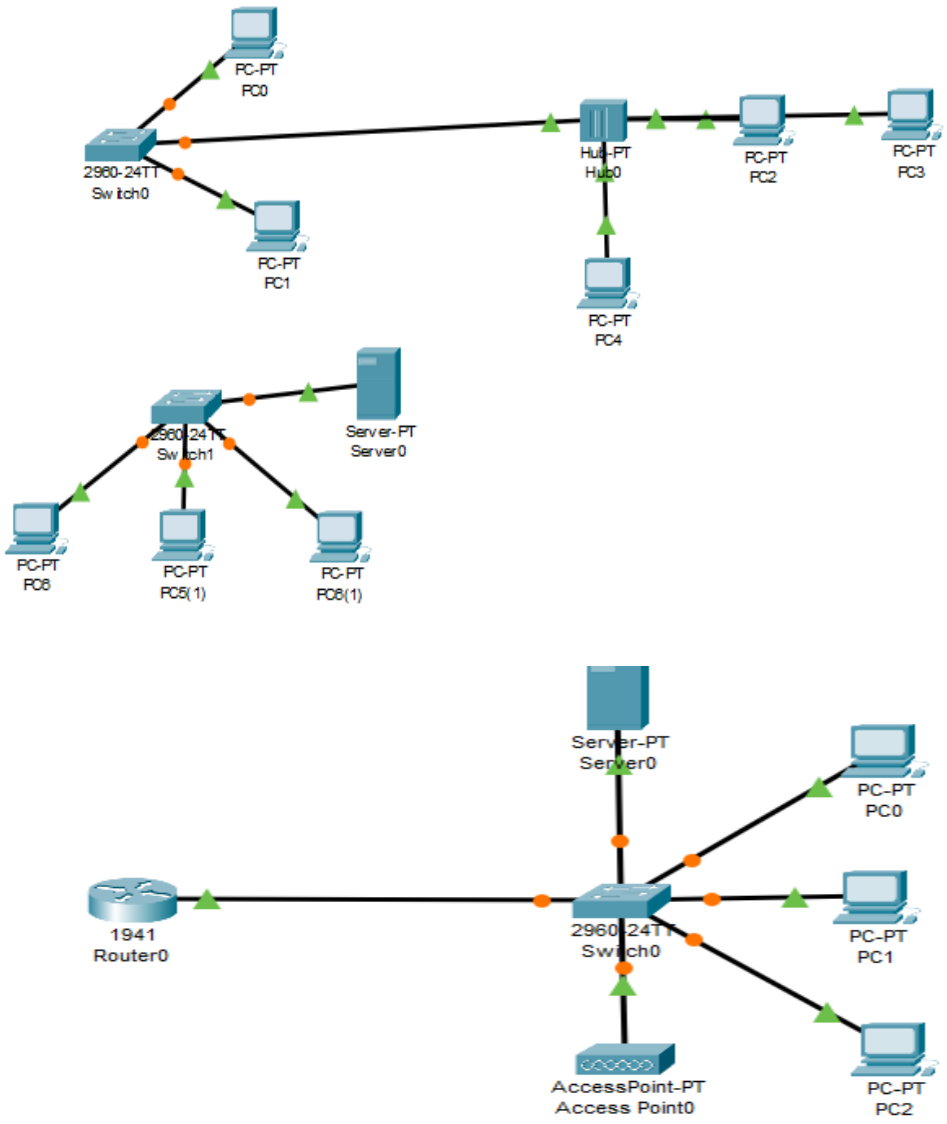
Modelos de seguridad en la red

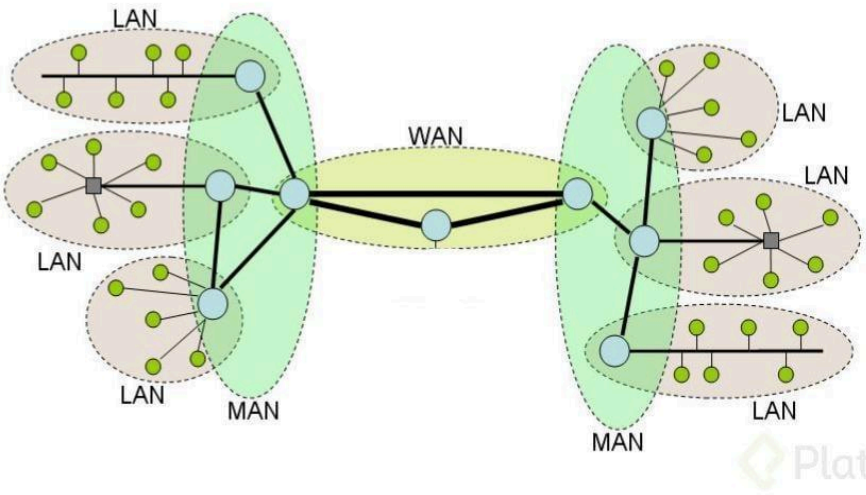


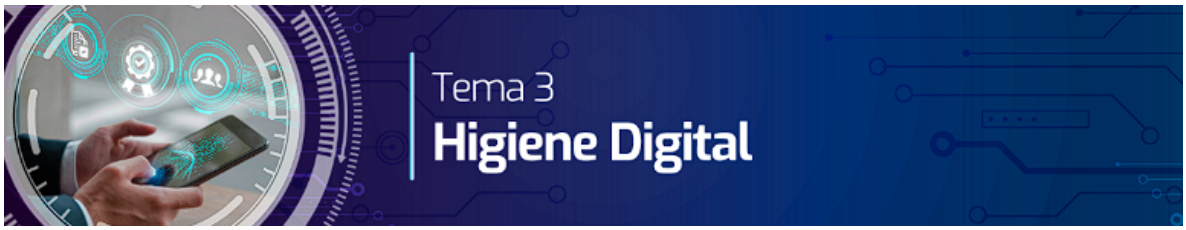


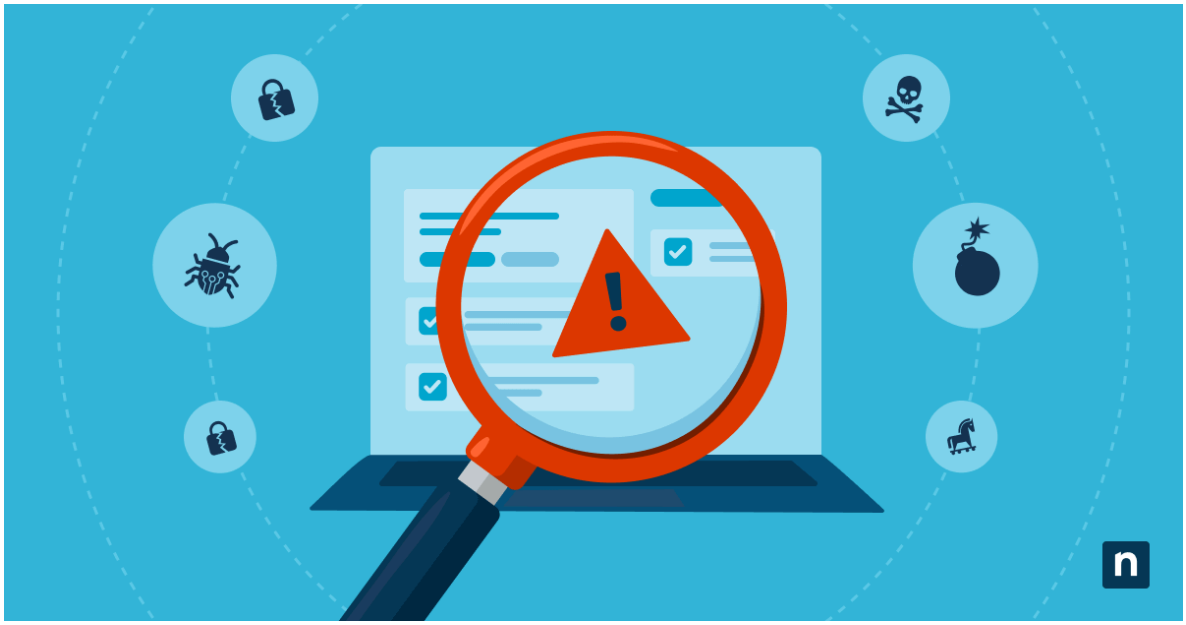




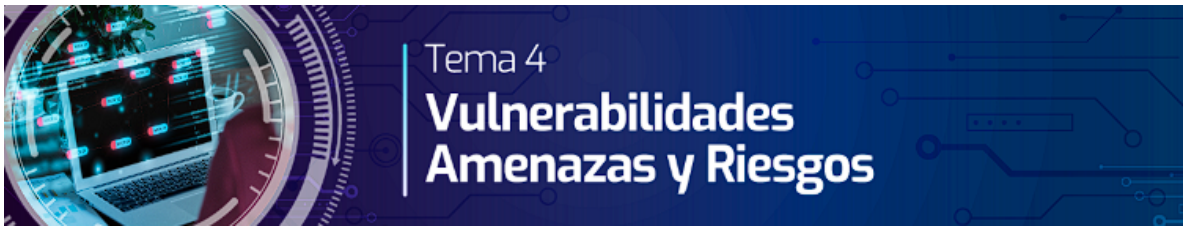

PC-PT
PC0
2960-24TT
Switch0
PC-PT
PC1
Hub-PT
Hub0
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
2960-24TT
Switch1
Server-PT
Server0
PC-PT
PC6
PC-PT
PC5(1)
PC-PT
PC6(1)
Server-PT
Server0
PC-PT
PC0
1941
Router0
2960-24TT
Switch0
PC-PT
PC1
AccessPoint-PT
Access Point0
PC-PT
PC2





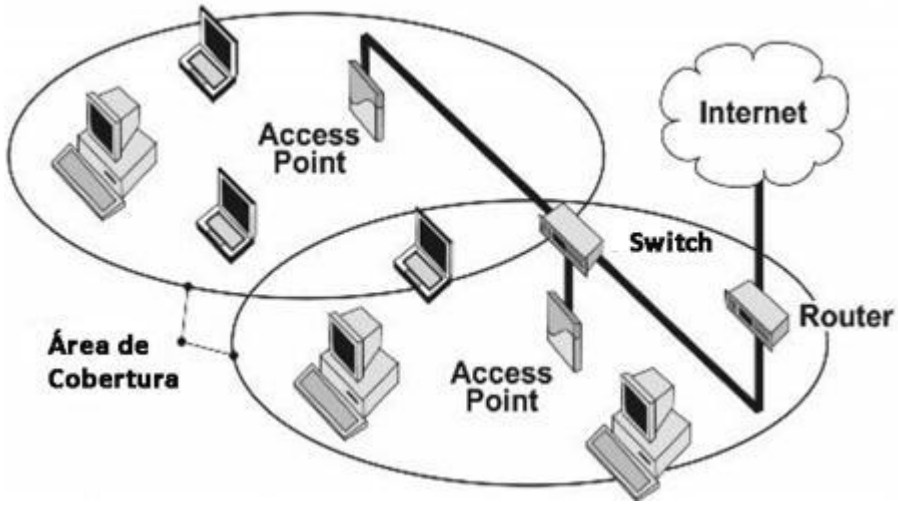


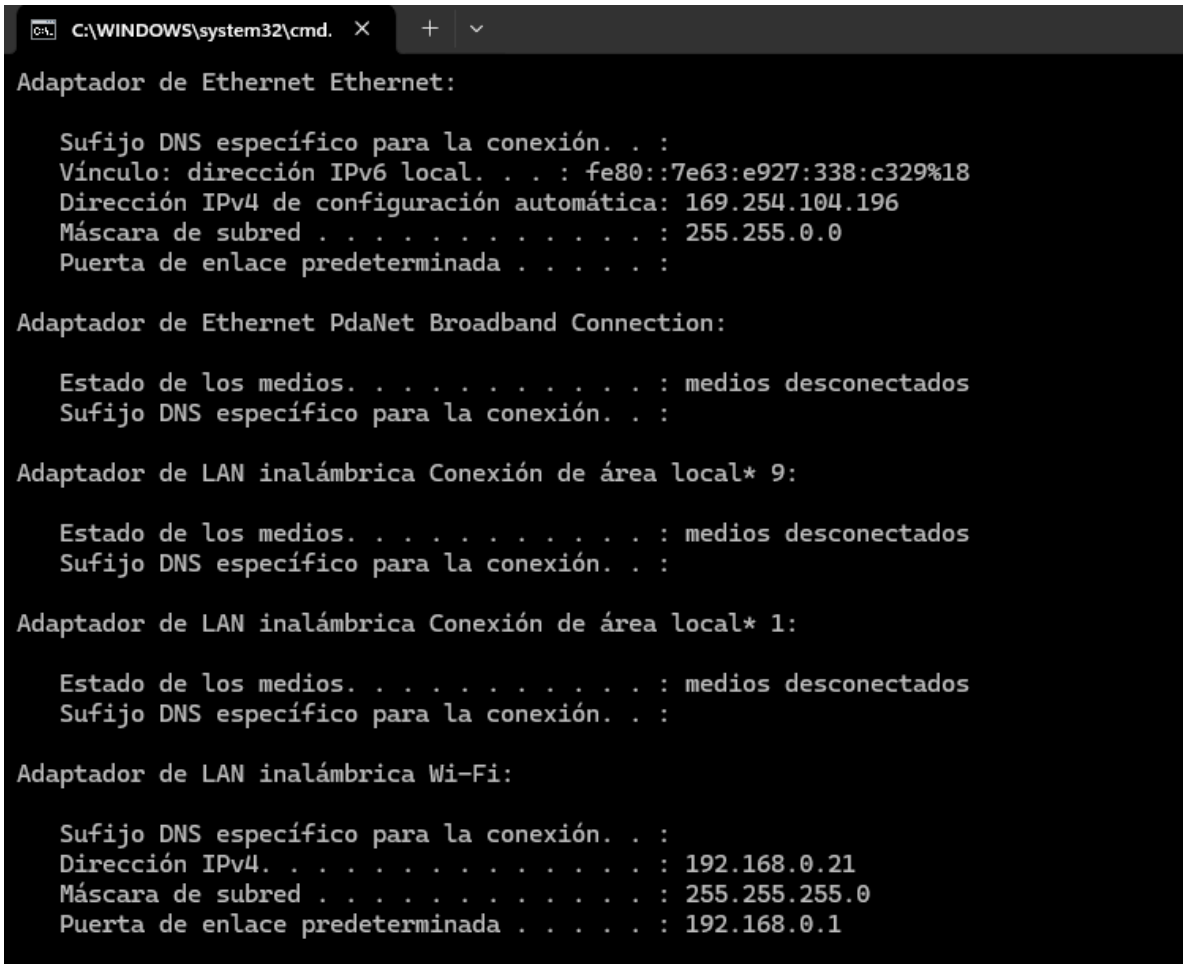
Parcheo de software

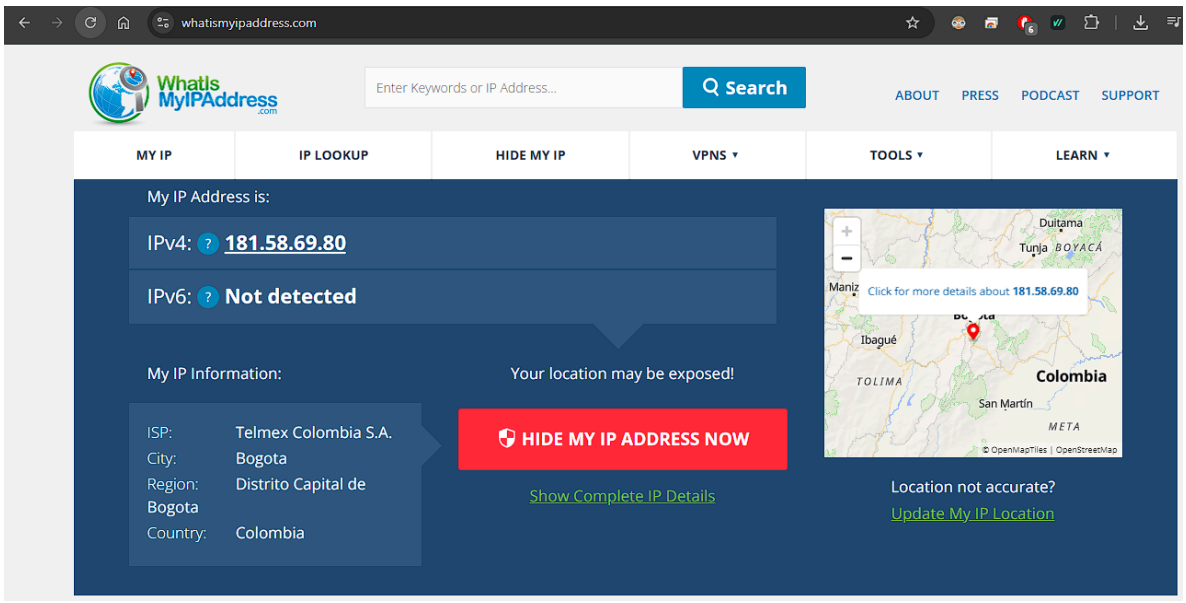

Tema 4
Vulnerabilidades
Amenazas y Riesgos

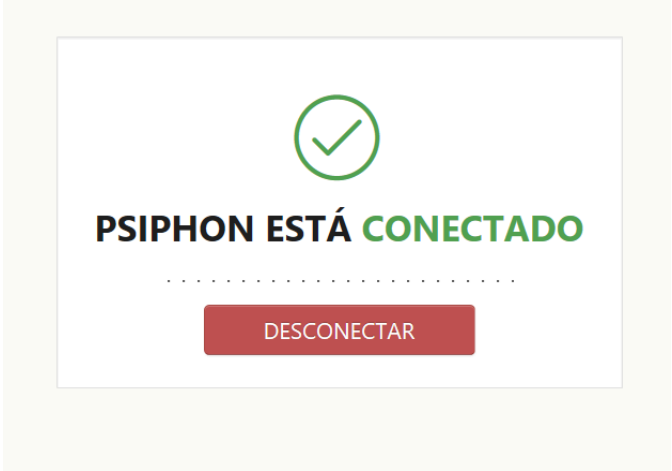
ATTACK

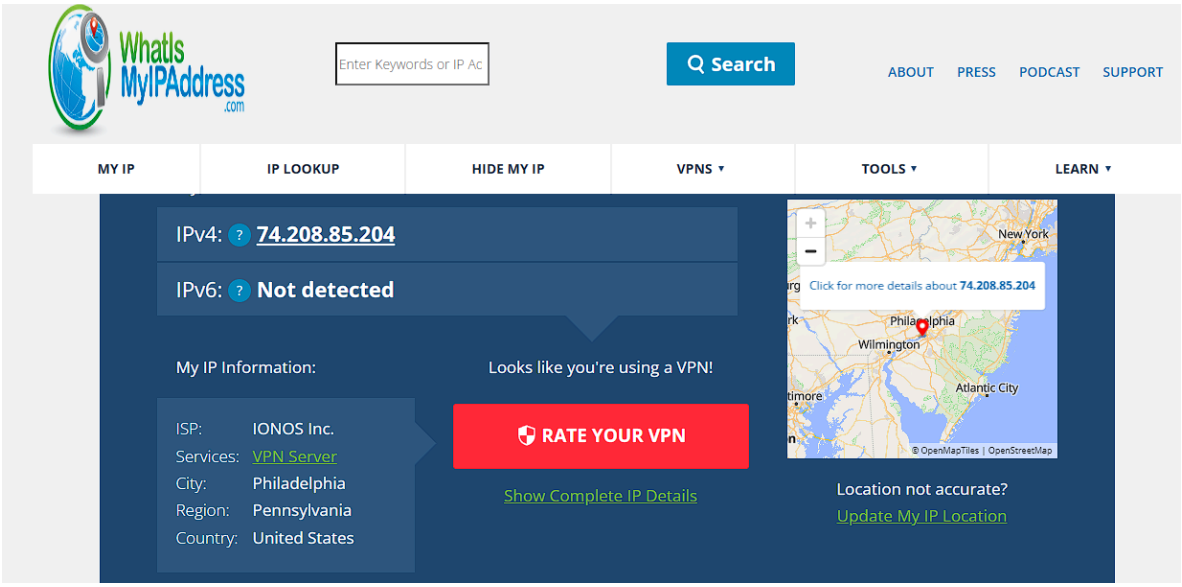
Tema 5
Medios de Transmisión
y Autenticación de Redes


Internet
Access
Point
Switch
Router
Área de
Cobertura
Access
Point


C:\WINDOWS\system32\cmd.
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::7e63:e927:338:c329%18
Dirección IPv4 de configuración automática: 169.254.104.196
Máscara de subred . . . . . : 255.255.0.0
Puerta de enlace predeterminada . . . . . :
Adaptador de Ethernet PdaNet Broadband Connection:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Conexión de área local* 9:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Conexión de área local* 1:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . :
Dirección IPv4. . . . . : 192.168.0.21
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.0.1


whatismyipaddress.com
WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
PODCAST
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
My IP Address is:
IPv4: 181.58.69.80
IPv6: Not detected
My IP Information:
Your location may be exposed!
ISP: Telmex Colombia S.A.
City: Bogota
Region: Distrito Capital de Bogota
Country: Colombia
HIDE MY IP ADDRESS NOW
Show Complete IP Details
Duitama
Tunja
BOYACÁ
Maniz
Click for more details about 181.58.69.80
Ibagué
TOLIMA
Colombia
San Martín
META
© OpenMapTiles | OpenStreetMap
Location not accurate?
Update My IP Location

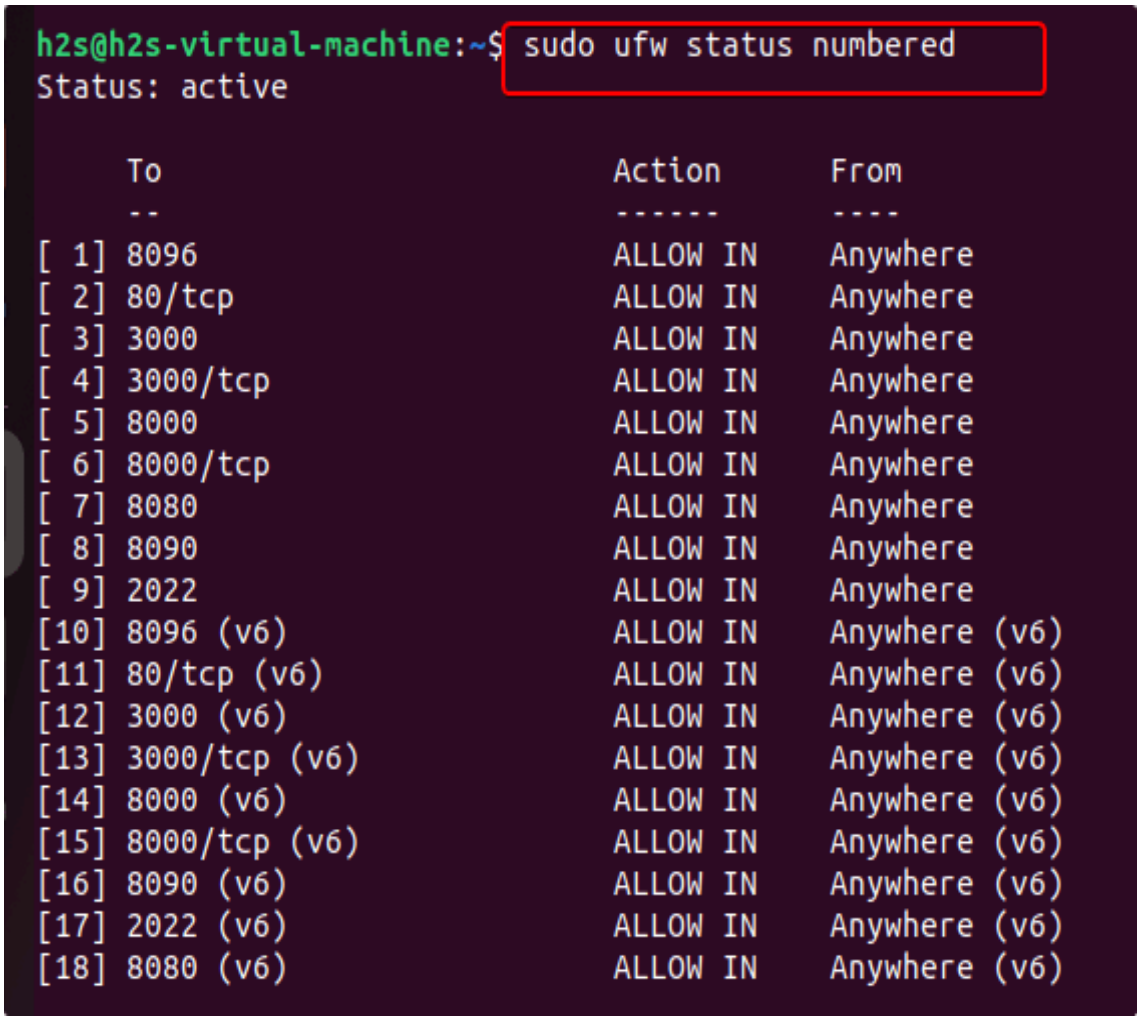




Creación de reglas de Firewall con UFW e IPTABLES

 # 1. Activar UFW
sudo ufw enable
 # 2. Ver estado y reglas activas
sudo ufw status verbose
 # 3. Permitir tráfico SSH (muy importante para no bloquearte)
sudo ufw allow ssh
 # 4. Reglas de entrada
sudo ufw allow http # Permitir tráfico HTTP (puerto 80)
sudo ufw allow https # Permitir tráfico HTTPS (puerto 443)
sudo ufw allow 53/udp # Permitir DNS sobre UDP
sudo ufw allow 53/tcp # Permitir DNS sobre TCP
 # 5. Reglas de salida
sudo ufw default allow outgoing # Permitir todas las conexiones de salida
sudo ufw default deny incoming # Denegar todas las conexiones de entrada
# 6. Bloquear un puerto específico (ejemplo: 21 - FTP)

sudo ufw deny 21
# 7. Eliminar una regla (ejemplo: HTTP)
sudo ufw delete allow http



 # 1. Eliminar reglas existentes (opcional)

sudo iptables -F

 # 2. Política por defecto

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

 # 3. Permitir tráfico local (localhost)

sudo iptables -A INPUT -i lo -j ACCEPT

 # 4. Permitir tráfico entrante relacionado o establecido

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

 # 5. Permitir SSH (Puerto 22)

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

 # 6. Permitir HTTP (Puerto 80)

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

 # 7. Permitir HTTPS (Puerto 443)

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

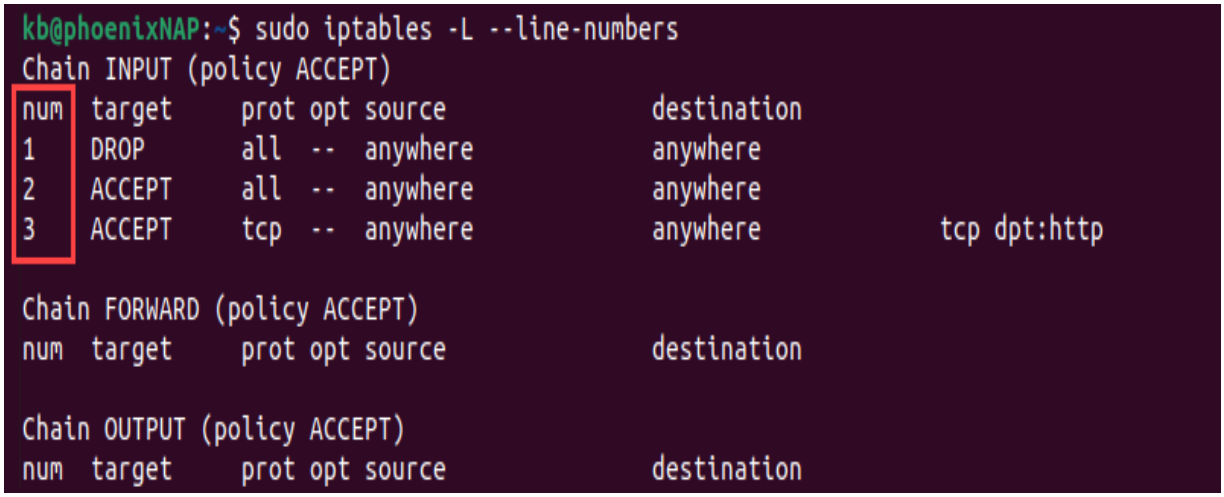
 # 8. Permitir DNS (TCP y UDP puerto 53)

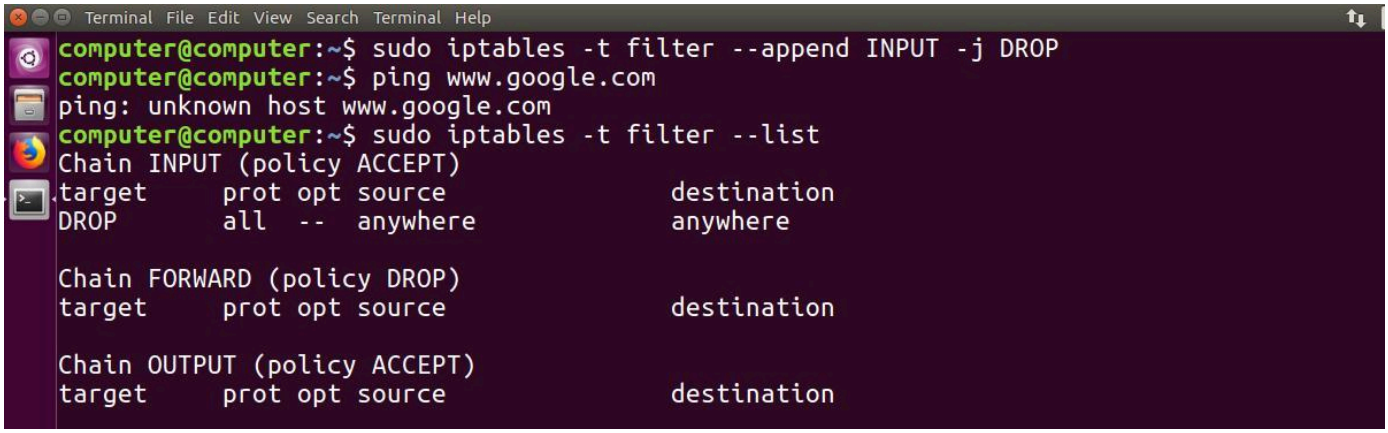
sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT

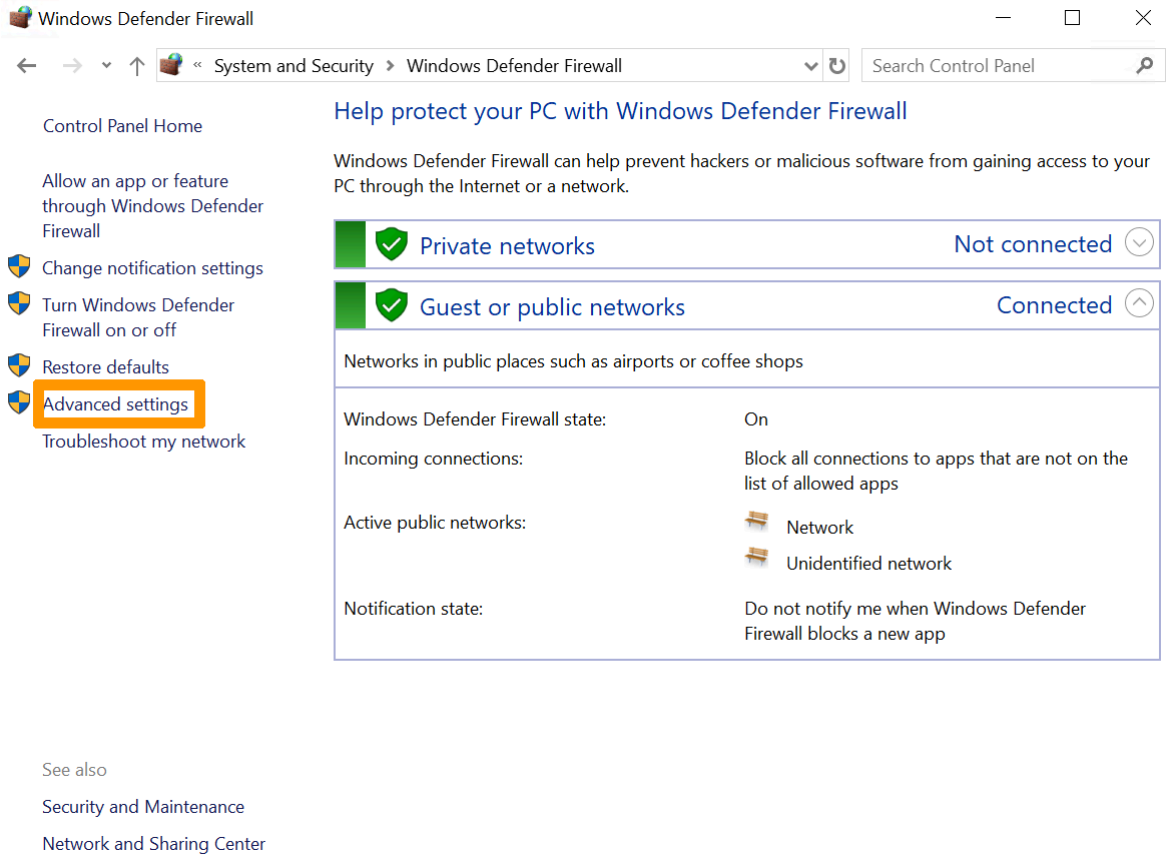
 # 9. Guardar las reglas (Ubuntu 20.04+)

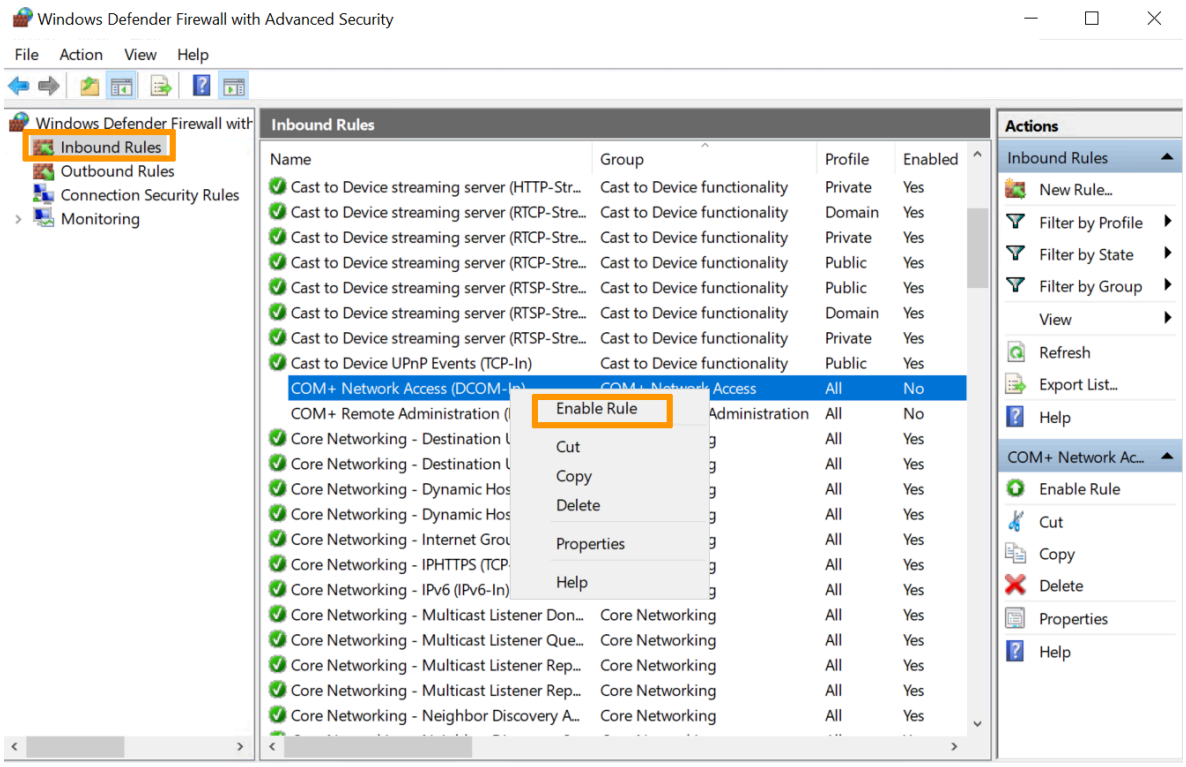
sudo iptables-save | sudo tee /etc/iptables/rules.v4

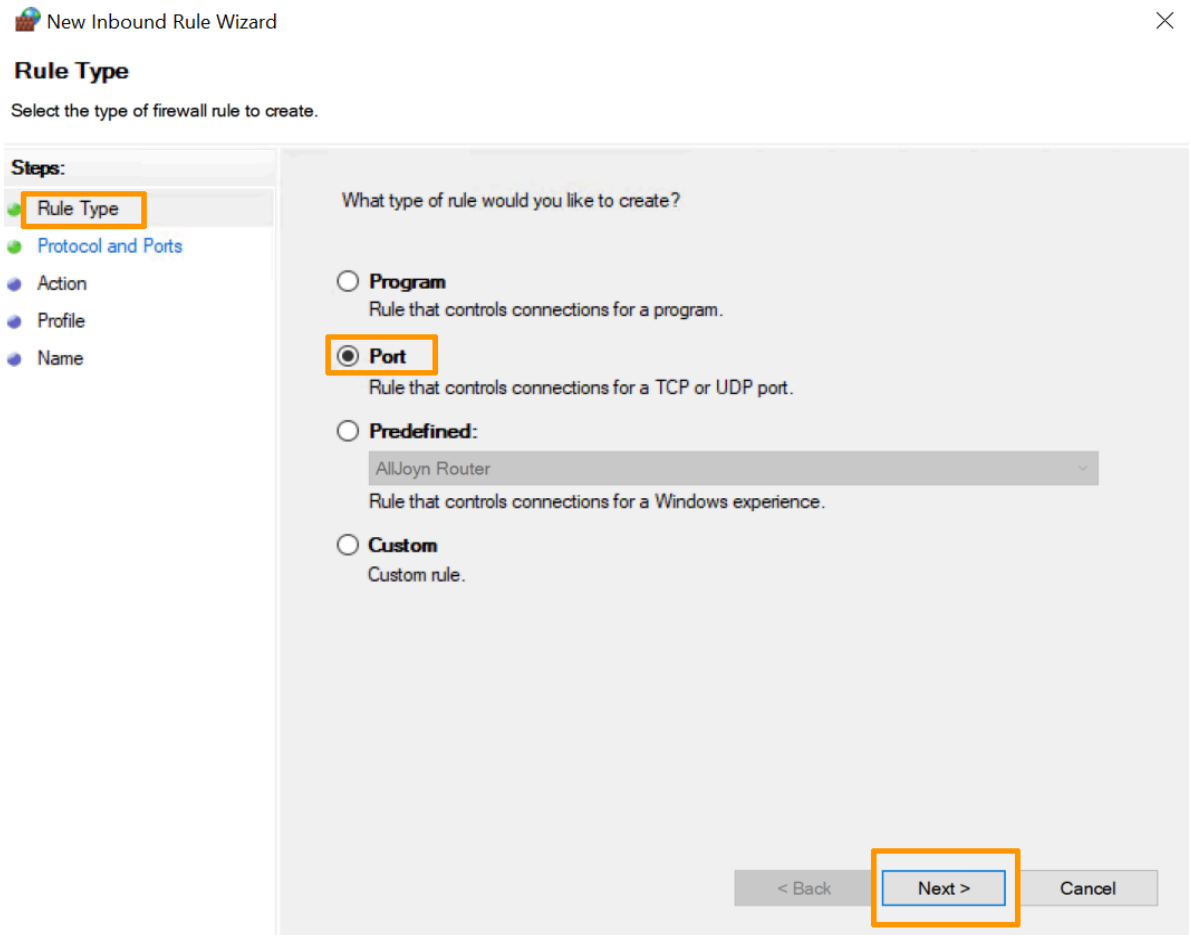


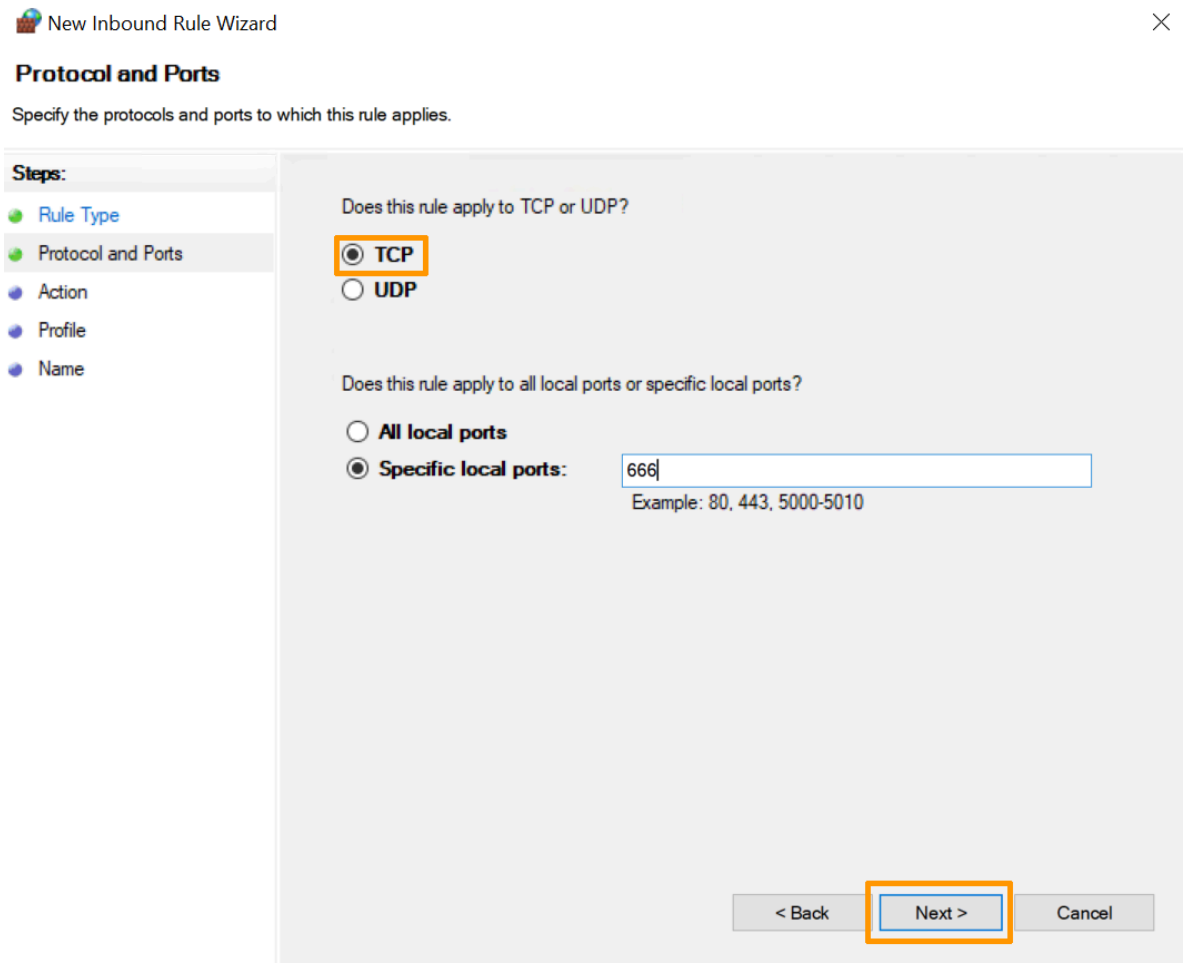


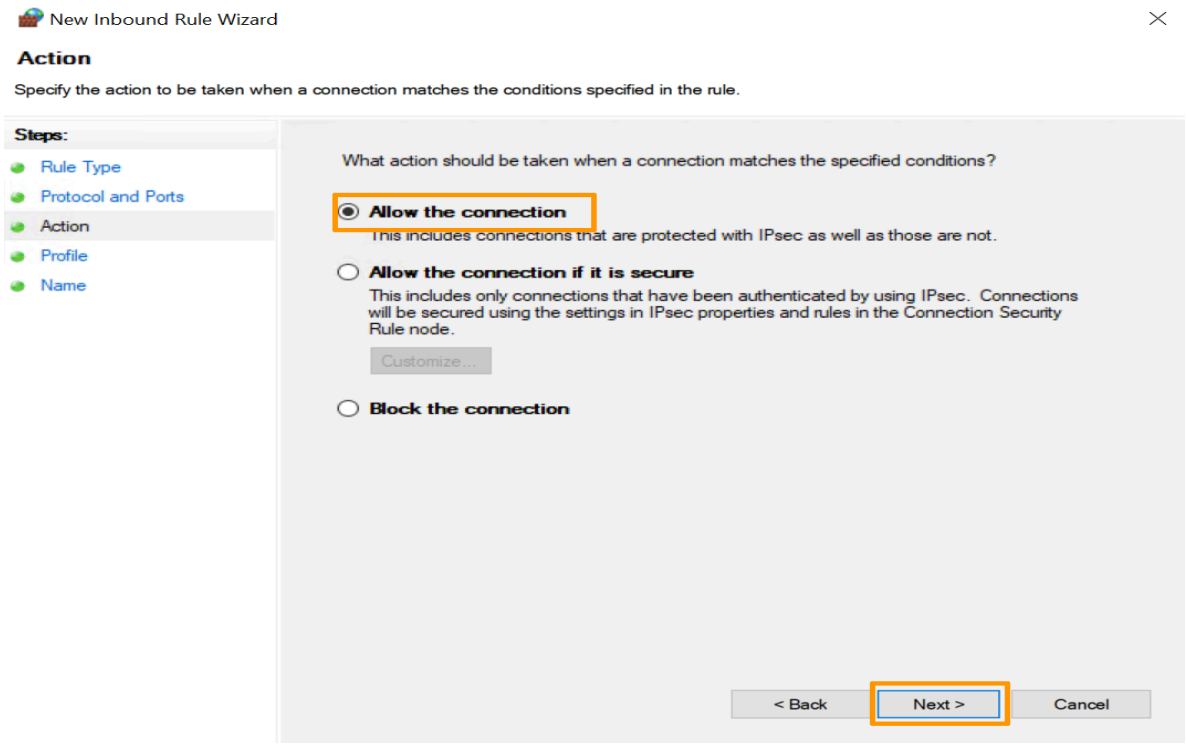
Configuración Firewall de Windows

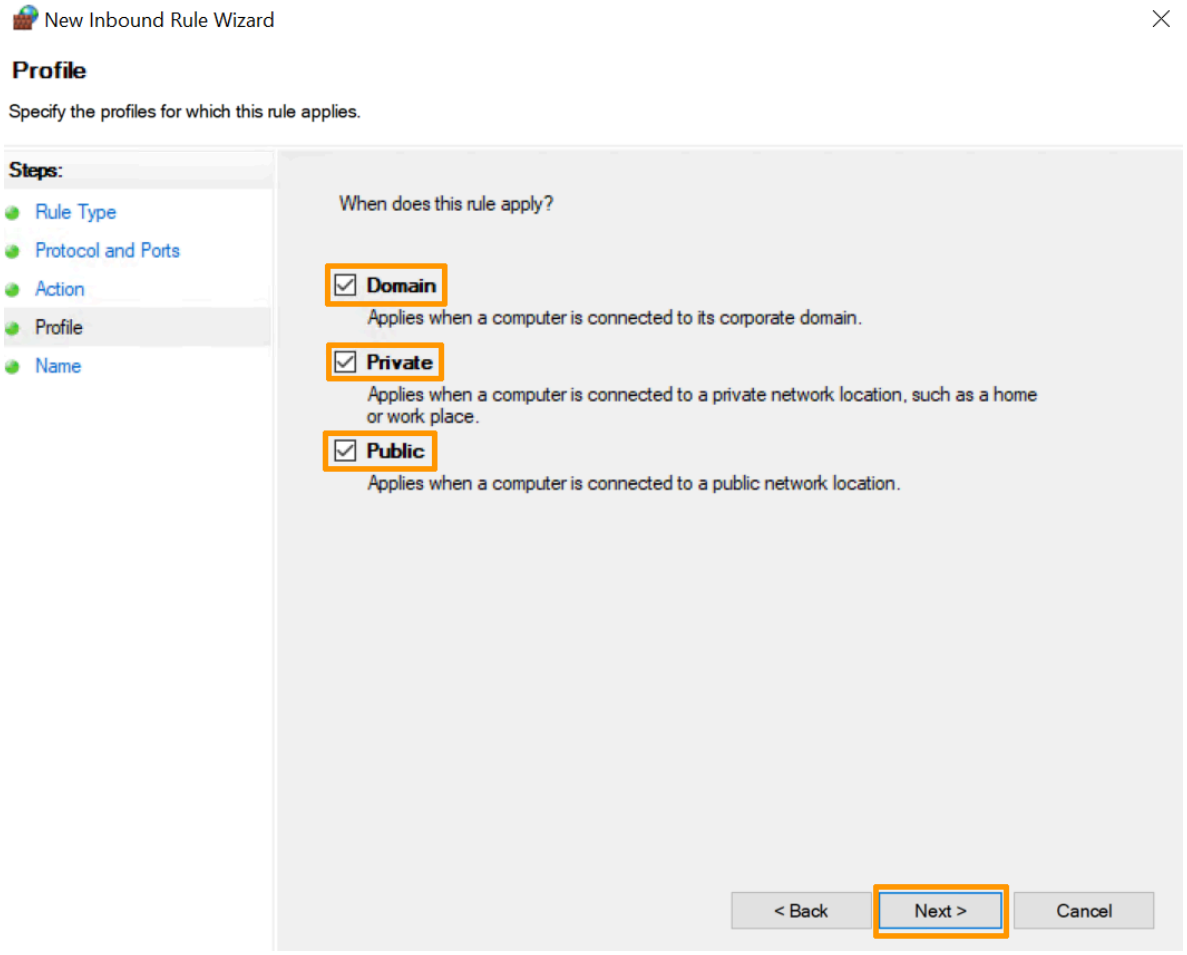


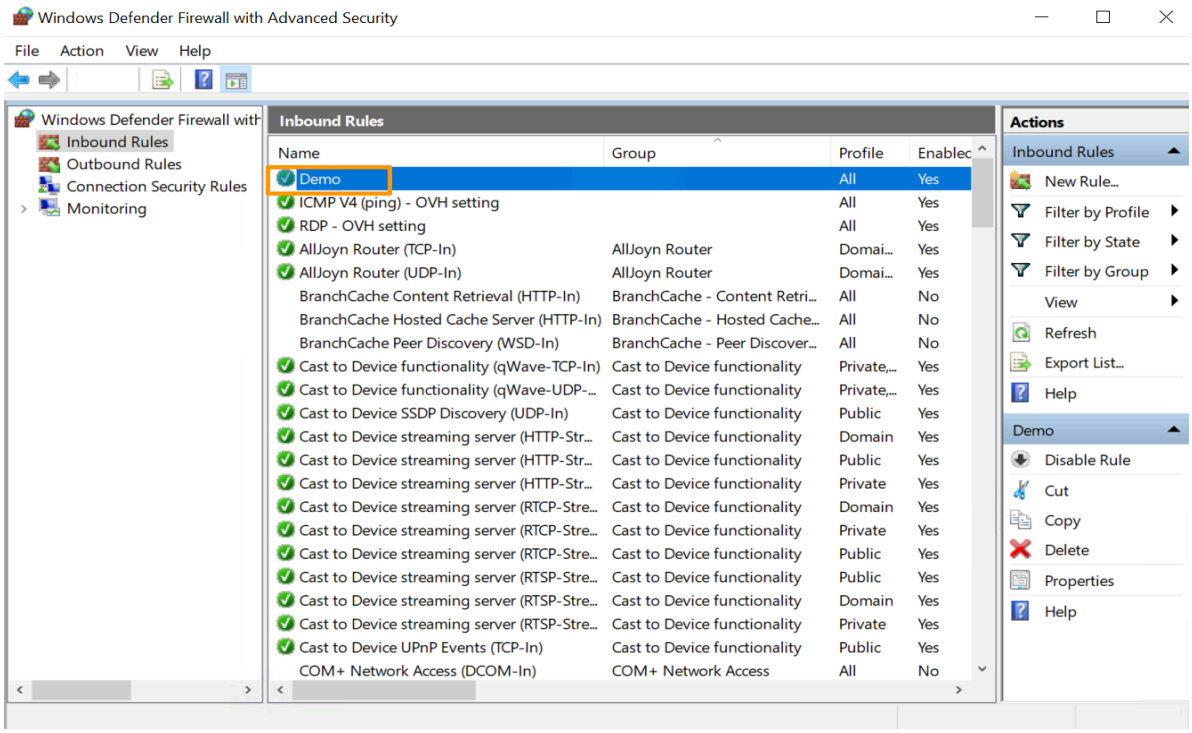

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Cast to Device streaming server (HTTP-Str...
Cast to Device functionality
Private
Yes
Cast to Device streaming server (RTCP-Stre...
Domain
Cast to Device streaming server (RTCP-Stre...
Private
Cast to Device streaming server (RTCP-Stre...
Public
Cast to Device streaming server (RTSP-Stre...
Cast to Device streaming server (RTSP-Stre...
Cast to Device streaming server (RTSP-Stre...
Cast to Device UPnP Events (TCP-In)
COM+ Network Access (DCOM-In)
All
No
COM+ Remote Administration
Core Networking - Destination U
Core Networking - Destination U
Core Networking - Dynamic Hos
Core Networking - Dynamic Hos
Core Networking - Internet Grou
Core Networking - IPHTTPS (TCP
Core Networking - IPv6 (IPv6-In)
Core Networking - Multicast Listener Don...
Core Networking
Core Networking - Multicast Listener Que...
Core Networking - Multicast Listener Rep...
Core Networking - Multicast Listener Rep...
Core Networking - Neighbor Discovery A...
Enable Rule
Cut
Copy
Delete
Properties
Help
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
COM+ Network Ac...
Enable Rule
Cut
Copy
Delete
Properties
Help


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
666
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enablec
Demo
All
Yes
ICMP V4 (ping) - OVH setting
RDP - OVH setting
AllJoyn Router (TCP-In)
AllJoyn Router
AllJoyn Router (UDP-In)
BranchCache Content Retrieval (HTTP-In)
BranchCache - Content Retri...
No
BranchCache Hosted Cache Server (HTTP-In)
BranchCache - Hosted Cache...
BranchCache Peer Discovery (WSD-In)
BranchCache - Peer Discover...
Cast to Device functionality (qWave-TCP-In)
Cast to Device functionality
Cast to Device functionality (qWave-UDP-...
Cast to Device SSDP Discovery (UDP-In)
Cast to Device streaming server (HTTP-Str...
Cast to Device streaming server (RTCP-Stre...
Cast to Device streaming server (RTSP-Stre...
Cast to Device UPnP Events (TCP-In)
COM+ Network Access (DCOM-In)
COM+ Network Access
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Demo
Disable Rule
Cut
Copy
Delete
Properties
Help