PRODUCTO 2

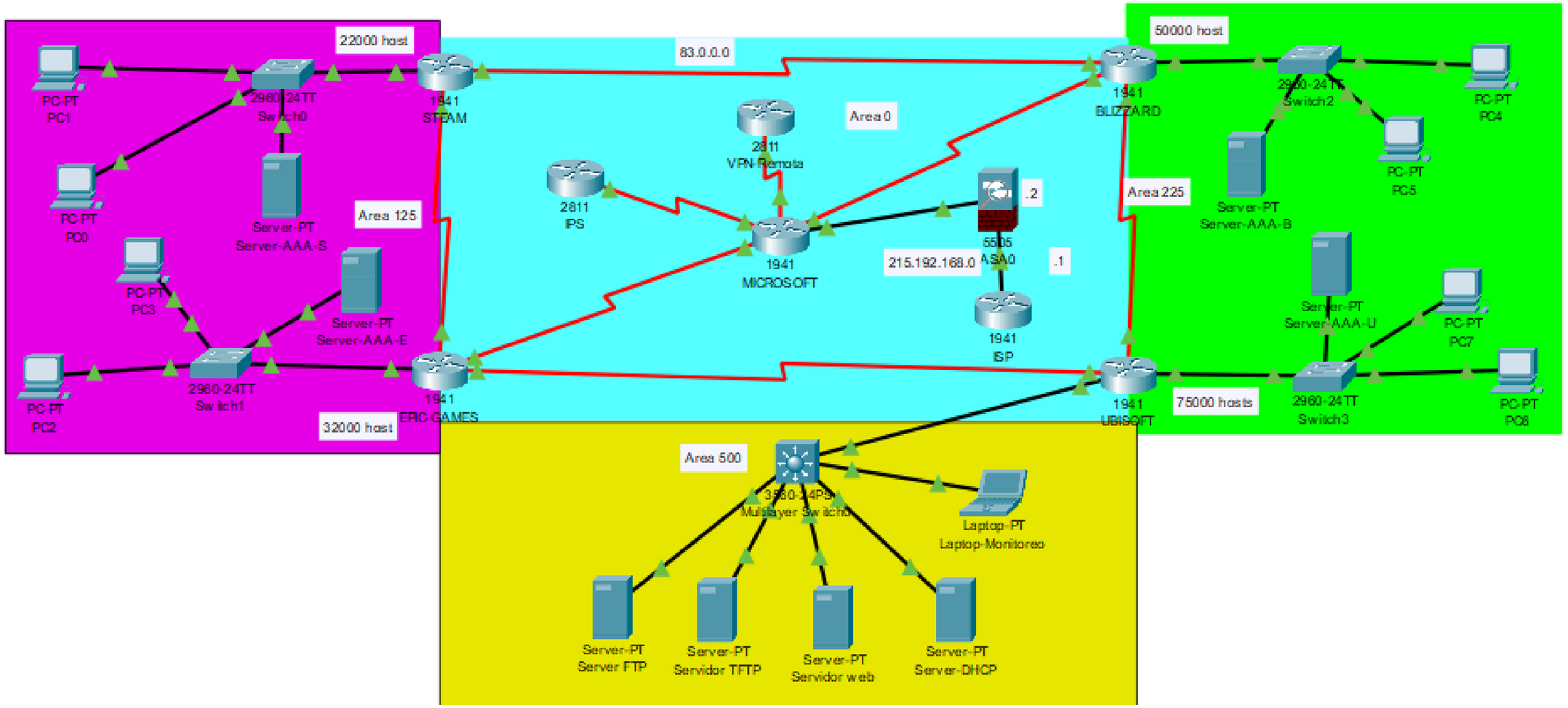
EQUIPO 1:
DE ALBA GARCÍA JESUS EDUARDO
GARCIA MARTINEZ LUIS DANIEL
SAINOS BONILLA CHRISTIAN ALEXIS
VAZQUEZ ROJAS FRANCISCO JAVIER

ÍNDICE DEL DOCUMENTO

1_ ESCENARIO

NUESTRA METODOLOGÍA

ESCENARIO


22000 host
PC-PT
PC1
2960-24TT
Switch0
1941
STEAM
PC-PT
PC0
Server-PT
Server-AAA-S
Area 125
PC-PT
PC3
Server-PT
Server-AAA-E
PC-PT
PC2
2960-24TT
Switch1
1941
EPIC-GAMES
32000 host
83.0.0.0
Area 0
2811
VPN-Remota
2811
IPS
1941
MICROSOFT
.2
5505
ASA0
215.192.168.0
.1
1941
ISP
1941
BLIZZARD
50000 host
2960-24TT
Switch2
PC-PT
PC4
PC-PT
PC5
Server-PT
Server-AAA-B
Area 225
Server-PT
Server-AAA-U
PC-PT
PC7
75000 hosts
2960-24TT
Switch3
PC-PT
PC8
1941
UBISOFT
Area 500
3560-24PS
Multilayer Switch0
Laptop-PT
Laptop-Monitoreo
Server-PT
Server FTP
Server-PT
Servidor TFTP
Server-PT
Servidor web
Server-PT
Server-DHCP

INTRODUCCIÓN

NUESTRO ESCENARIO

RECONOCIMIENTO

El escenario cuenta con routers, switches (capa 2 y 3), firewall, servidores y dispositivos finales.

ANÁLISIS

El escenario cuenta con redundancia y comunicación de toda la red, asi como también un router que simula la función de isp

PLANEACIÓN

Con base al escenario se busca mantener la confidencialidad, proporcionar seguridad y buena comunicación dentro de la red

EJECUCIÓN

Se implementaron diversos métodos de seguridad dentro de la red, asi como también estrategias tanto en routers como en switches

2 – POLITICAS IMPLEMENTADAS

POLITICAS DE SEGURIDAD

SE IMPLEMENTAN ACL

Esto para gantizar una mejor seguridad dentro de la red y mantener restricciones a ciertas acciones

Política 1

RED EPIC-GAMES:

Se configuró una ACL extendida en el router correspondiente que bloquea el tráfico HTTP y HTTPS hacia los servidores web alojados en el área 500.

Política 2

RED UBISOFT:

se implementó una ACL estándar en el router Steam que restringe el tráfico SSH proveniente de la red de Ubisoft.

Política 3

RED BLIZZARD:

Se estableció una ACL específica en el router Blizzard para evitar conexiones no autorizadas al servidor FTP ubicado en el área 500.

Política 4

ACL EN CISCO ASA

- access-list 100 permit icmp any any:
- access-list 100 deny icmp any any:
- access-group 100 in interface outside:.

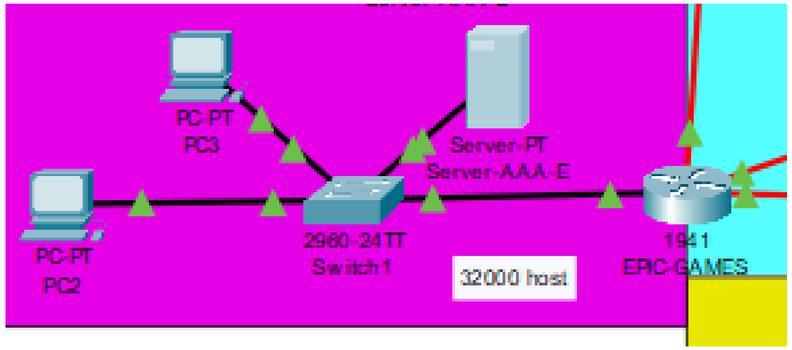
POLITICAS DE SEGURIDAD

IDENTIFICACION DE LUGARES

Aqui se puede ver donde se implementaron las acls anteriores

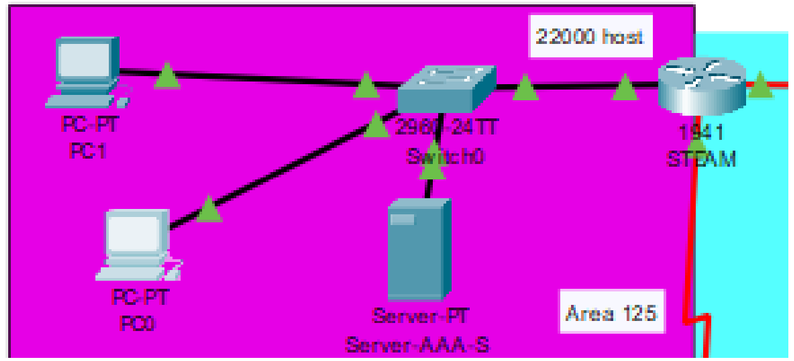
Política 1

RED EPIC-GAMES:



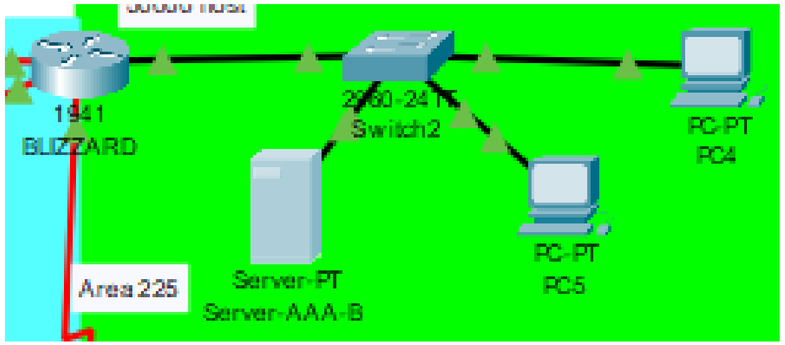
Política 2

RED UBISOFT:



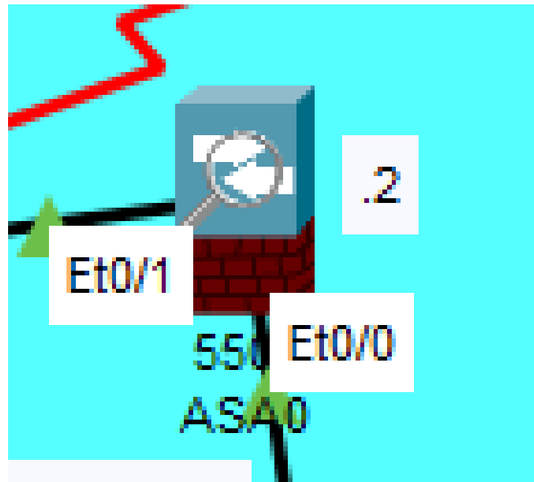
Política 3

RED BLIZZARD:



Política 4

ACL EN CISCO ASA



3 – IMPLEMENTACION AAA

AAA

¿QUÉ SE LLEVO A CABO?

PASO 1

AUTENTICACION

Se crearon diversos usuarios con los nombres de:

- **Employed**
- **Supervisor**
- **JR**
- **cisco**

PASO 2

AUTENTICACION

Se realizo una configuración dentro de los router para que cada usuario pueda acceder a sus respectivos perfiles, al mismo tiempo se agregaron servidores para dicho servicio.

```
)#aaa new-model
)#aaa authentication login Acceso_Ssh group
)#radius-server host 83.3.128.1 key psws
)#line vty 0 4
-line)#login authentication Acceso_Ssh
-line)#
```

PASO 3

AUTORIZACION

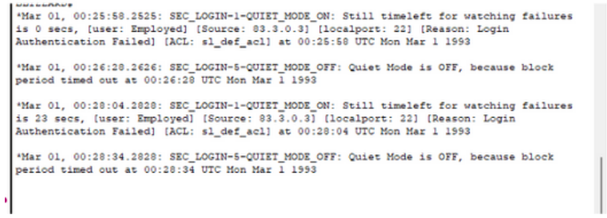
Para que cada usuario pueda accede a su perfil se les dio una contraseña única del perfil y un nivel privilegio, posteriormente se encriptó para mayor seguridad

```
Employed privilege 5 secret 5 $1$mE
JR privilege 11 secret 5 $1$mERr$84
Supervisor privilege 10 secret 5 $1
cisco privilege 15 secret 5 $1$mERr
```

PASO 4

AUTORIZACION

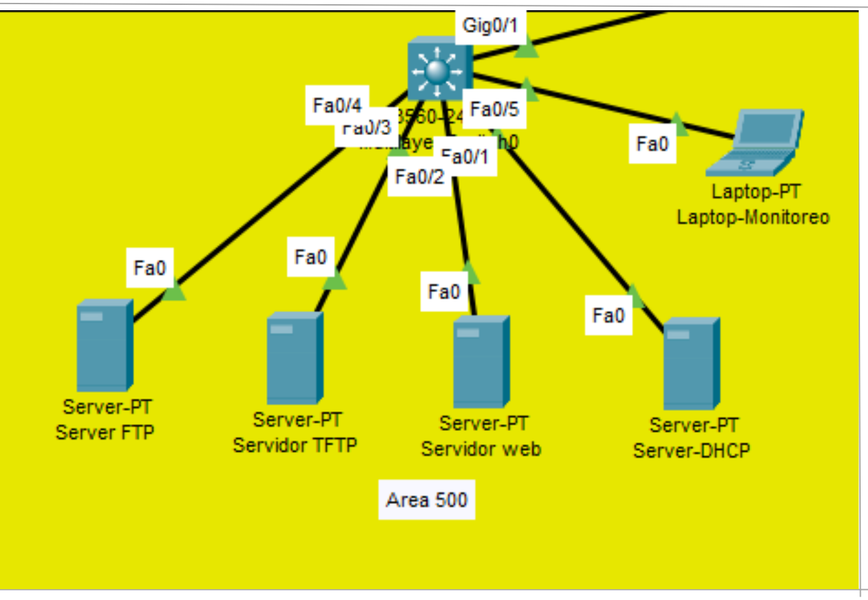
Dentro de los routers se configuro una verificación para alertar al usuario si hay un intento de inicio de sesión.



4 – MEDIDAS DE SEGURIDAD

IDENTIFICACION DE PUERTOS Y DMZ

NUESTRA DMZ



Ubicación

¿DONDE SE UBICO?

Nuestra DMZ se ubico en un switch de capa 3 el cual esta conectado a el router de la red de UBISOFT y este cuenta con seguridad en los puertos y negociacion para identificar el puerto

¿Porque?

SE DECIDIO HACER UNA DMZ

- Aqui se asegura la zona mas importante de nuestra infraestructura ya que esta cuenta con distintos servidores que cumplen con diversas funciones tales como: WEB, TFTP, FTP y DHCP. Ademas por seguridad esta solo cuenta con el acceso de un solo router

```
interface FastEthernet0/5
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/6
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/7
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/8
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/9
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/10
 switchport mode access
 switchport nonegotiate
 switchport port-security
!
interface FastEthernet0/11
 switchport mode access
```

5 – FIREWALL

FILTRADO DE PAQUETES

FIREWALL

FIREWALL ASA

5505

Se opto por utilizar este firewall conectado a los router del ISP y Microsoft esto gracias a que conectan la red LAN con la red WAN y proporcionan una mayor seguridad

FUNCIONALIDAD

CONFIGURACION

El firewall cumple con la función de NAT . para traducir direcciones IP privadas a publicas, se configuró una ruta estática para mantener conexión con la red y ACLS

```
object network LAN
 subnet 83.0.0.0 255.0.0.0
 nat (inside,outside) dynamic interface
```

```
access-list outbound extended permit ip any any
access-list 100 extended permit icmp any any
access-list 100 extended deny icmp any any
```

6 — IPS

BASADO EN RED

IPS BASADO EN RED

IPS

- El router tiene como función detectar y prevenir amenazas mediante la inspección del tráfico en tiempo real, utilizando firmas predefinidas.

- Además, se configuraron acciones para generar alertas y bloquear los paquetes maliciosos en el momento en que se detecta una amenaza.

- La firma de seguridad configurada (ID 2004) se activó correctamente y está lista para prevenir ataques específicos en la red.

```
%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [215.192.168.8 -> 83.4.64.29:0] RiskRating:25

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [215.192.168.9 -> 83.4.64.29:0] RiskRating:25

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [215.192.168.8 -> 83.4.64.29:0] RiskRating:25

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [215.192.168.9 -> 83.4.64.29:0] RiskRating:25

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [83.4.64.29 -> 83.4.64.10:0] RiskRating:25
```

7 – ALGORITMOS CRIPTOGRAFICOS

CRIPTOGRFIA

1 HASH

Se utilizo una enryptacion de hash cuando se creo la VPN de aaceso remoto

2 AES

Se utilizo una encryptacion de AES con 256 Bits para la configuracion de la VPN

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

CRIPTOGRFIA

3 RSA

Se utiliza un encryptamiento para llaves de 1024 cuando se configura el servicio de SSH

```
router(config)# ip domain-name CCNA-lab.com
router(config)# crypto key generate rsa
router(config)# ip ssh version 2
```

4 PASSWORD

Cuando se configura la contraseña uno de los pasos posteriores es aplicar el comando service password-encrption para mantener a contraseña encryptada

```
service password-encryption
security passwords min-length 10
```

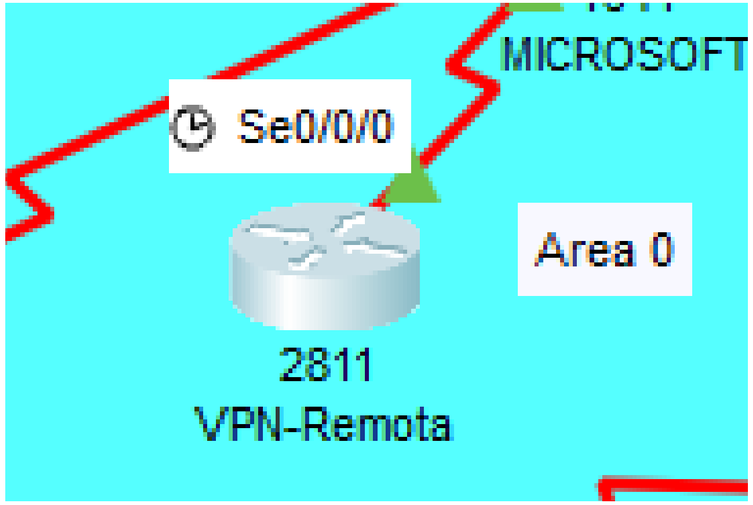
8 — VPN

ACCESO REMOTO

VPN DE ACCESO REMOTO

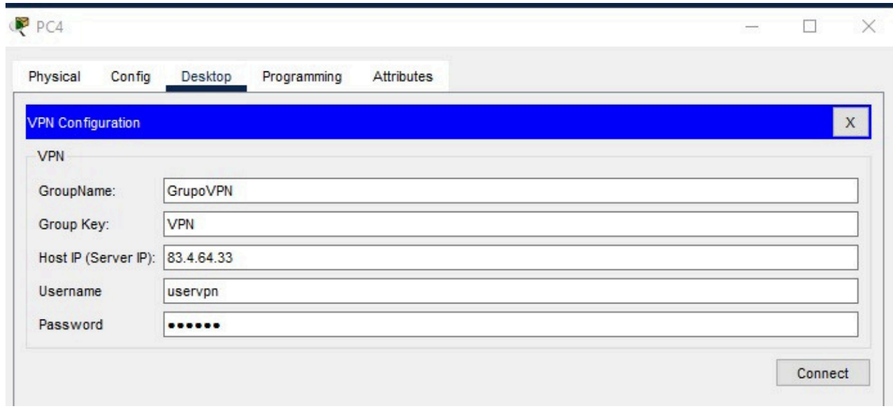
IMPLEMENTACION DE VPN

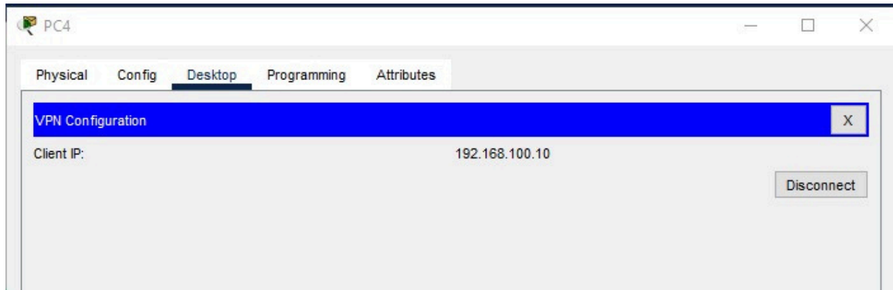
Brinda mas seguridad y confidencialidad dentro de os pquetes enviadoe en la red



Se coloco un router conectado a MICROSOFT que cumple con la función de una VPN de acceso remoto la cual permita los usuarios de la red que accedan a el y rinde un túnel seguro.

- Cada usuario tiene acceso a un canal privado remotamente, esto proporciona mayor seguridad para garantizar que las conexiones remotas sean seguras, confiables y eficientes.





GRACIAS POR SU ATENCIÓN