fortigate, validación, directorio activo, ad

## Integración del Fortigate con el AD

Lo primero que hay que revisar es que tengamos los DNS bien configurados. System $\rightarrow$  Networks  $\rightarrow$  DNS y ponemos los valores correspondientes a nuestros DNS

System		DNS Settings
Obshboard     Status     Top Sources     Top Destinations     Top Applications     Traffic History     Threat History     Interface     ONS     Explicit Proxy     Packet Capture     Config     Config     Config     Config     Config     Config     Config     Config     Config     Monitor	DNS Settings Use FortiGuard Servers  Secondary DNS Server Local Domain Name	Αρρίγ

Una vez configurado el DNS, definimos el servidor de con el que nos vamos a conectar para validar usuarios. Para ello vamos a la pestaña User & Device  $\rightarrow$  Authentication  $\rightarrow$  LDAP Server y piulsamos sobre **Create New** 

System			New LDAP Server
Router	Name	mi AD	
Policy	Server Name/IP	miservidor.local	
Firewall Objects	Server Port	389	
Security Profiles	Common Name Identifier	sAMAaccountName	
VPN	Distinguished Name	DC-midominio,DC-loce	
User & Device	Bind Type	◎ Simple ◎ Anonymous ⑧ Regular	
User     User Definition     User Group     Guest Management	User DN Password Secure Connection	CN-usuario, CN-Users,	
Device     Vice Definition     Vice Group     Endpoint Profile     Authentication			OK Cancel
<ul> <li>Single Sign-On</li> <li>DAR Sequer</li> </ul>			

Rellenamos los campos teniendo en cuenta que para la validación con el directorio activo usamos **sAMAccountName** como Common Name Identifier

- En Distinguised Name ponemos el nombre del dominio→DC=midominio,DC=local
- User DN→ CN=usuario, CN=Users, DC=midominio, DC=local (nombre distinguido del usuario que vamos a usar para la validación)

Una vez creada la conexión con el servidor/es del directorio activo vamos a crear un grupo para la validación remota de los usuarios del mismo. Vamos a User & Device  $\rightarrow$  User  $\rightarrow$  User Group.

System	New User Group						
Router	Name acceso remoto	1					
Policy	Type # Freneal @ Fortinet Single Sign-On (FSSO) @ Guest @ RADDUS Single Sign-On (RSSO)						
Firewall Objects	- Local Users -	+ Decal Users -	-				
Security Profiles		- Pici Livere -					
VPN		9					
User & Device	- PKI Users -						
e 🚮 User • User Definition	=	i.,					
Over Group     Guest Hanagement	Remote authenticetion servers Add						
# 🕡 Device	Remote Server	- 24-	Group Name	Delete			
Authentication			Any * Specify CN=grpremoto, CN=Users, DC=mic	1			
Tiro-factor Authentication		•	Any # Specify (ON-graremoto, ON-Users, DC-mid)	12			
<ul> <li>Wurnerability Scan</li> <li>Monitor</li> </ul>			OK Cencel				

Creamos un nuevo grupo y le añadimos los servidores de directorio activo de nuestra organización y como cadena de conexión ponemos el nombre distinguido del grupo que queremos usar, en nuestro caso CN=grpremoto,CN=Users,DC=midominio,DC=local

Ahora podemos usar ese grupo para validar usuarios remotos en la VPN . Podemos editar la la fase1 de nuestra vpn y en el apartado XAUTH  $\rightarrow$  marcar Enable as Server. y en UserGroup elegir el grupo que hemos creado.

También podemos crear otro grupo y usarlo para la validación de los administradores . System $\rightarrow$  Admin $\rightarrow$  Administrators  $\rightarrow$  creamos un administrador nuevo  $\rightarrow$  type= remote y en user Group ponemos el grupo creado en el apartado anterior.

From: https://intrusos.info/ - **LCWIKI** 

Permanent link: https://intrusos.info/doku.php?id=hardware:fortigate:ad



Last update: 2023/01/18 14:36