

REMEDDOS USAGE

Verificar e-mail

La primera vez que accedemos a la aplicación deberemos confirmar nuestra dirección de correo electrónico el cual ya habrá sido enviado al correo proporcionado.

Verifica tu dirección de correo electrónico

Hemos enviado un correo a la dirección que nos ha sido facilitada. Por favor verifica tu identidad a través de el link incluido en el email. Contacte con REDIMadrid en caso de haber algún problema o no haber recibido el email.

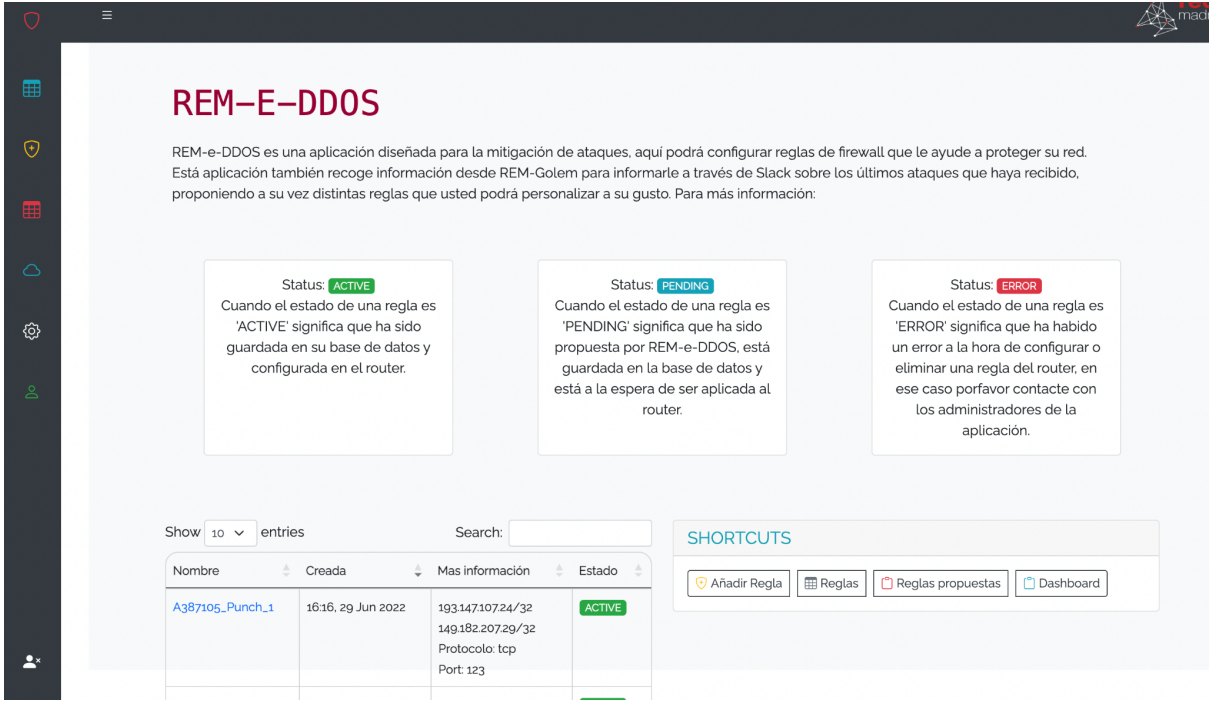
Una vez confirmada nuestra dirección de correo electrónico podremos acceder sin problemas a la aplicación.

En todas las ventanas de la aplicación también podremos encontrar la caja de 'shortcuts' donde poder acceder de manera rápida a las acciones más necesarias como la añadir una regla o ver tus reglas propuestas así como las activas.







SHORTCUTS

-  Añadir Regla
-  Reglas
-  Reglas propuestas
-  Dashboard

Tenemos una barra lateral izquierda en la que aparecerán todas las ventanas de la aplicación. El primer botón abre la ventana de Dashboard donde aparecerá información básica de la aplicación así como una tabla de reglas que estén activas en ese momento.



El segundo botón, nos lleva a todas las reglas que están o han estado activas en el router de nuestra organización.

Reglas de Firewall ⓘ									
Show 20 entries		ACTIVE PENDING ERROR DEACTIVATED			Search:				
Showing 1 to 6 of 6 entries					Previous 1 Next				
Nombre	Información	Acción	Estado	Pertenece a	Caduca	Respuesta	Otros		
A387105_Punch_1	Dst Addr Src Addr Ports Protocols	193.147.107.24 149.182.207.29 123 tcp	DESACTIVADA	David Rincón (null)	28 de julio de 2022	Regla caducada	Resincronizar		
anotherest_Punch	Dst Addr Src Addr TCP flag Protocols	1.1.1.1/32 2.2.2.2/32 push tcp	DESACTIVADA	redamin@redamin.com (CEU)	19 de julio de 2022	Regla caducada	 		
A386555_Punch_4	Dst Addr Src Addr Ports Protocols	193.147.107.37 162.144.240.39 123 tcp	DESACTIVADA	alicia.cardenosa@imdea.org (null)	16 de julio de 2022	Regla caducada	 		
A386555_Punch_2	Dst Addr Src Addr Ports Protocols	193.147.107.37 185.84.80.25 123 tcp	DESACTIVADA	alicia.cardenosa@imdea.org (null)	16 de julio de 2022	Regla caducada	 		

Añadir/eliminar/editar una regla de firewall

Hay varias formas de añadir una regla de firewall, las principales son a través del botón en la barra lateral o en el menú de shortcuts donde también aparece esta opción.

El procedimiento es el siguiente, se envía un mensaje a slack con un código de verificación para que sea introducido en la aplicación. Esta 'comprobación' dura 15 minutos. Durante estos 15 minutos podremos eliminar, añadir o editar tantas reglas como queramos, después se volverá a enviar un código para repetir el proceso.



Para eliminar o editar cualquier regla, se puede acceder a estas opciones a través de la ventana de mis reglas donde en cada regla aparecerá una opción para bien editar o eliminar la regla que se desee.

Golem Events

Accederemos a los eventos que REM-Golem ha detectado a través del cuarto botón en la barra lateral, el calendario rojo.


🔔 Ataques recibidos desde REM-GOLEM


Show 5 entries Search:


ID	Type	Received at	Institution	Important Data	Status	Max Value	Threshold	More Information	Actions
A387682	DDOS	13:08, 26 Jul 2022	Punch	Src Addr 191.202.168.171 Dest Addr 0.0.0.0 Port 123 Protocol tcp Tcpflag ----S-	Ongoing	320/Pps	100/Pps	REM-GOLEM	 


Showing 1 to 1 of 1 entries Previous 1 Next

Shortcuts

 Añadir Regla

 Reglas







 Reglas propuestas

 Dashboard





En esta página se encuentran todos los eventos que REM-Golem ha filtrado y enviado a la aplicación de REM-e-DDOS. Podremos ver los datos más importantes del evento así como acceder al link de rem-golem donde ver más información. Si pulsamos el ID veremos las reglas que la aplicación de REM-e-DDOS ha propuesto para mitigar el ataque.

Reglas propuestas para mitigar el ataque: **A387682**

← REM-Golem events

ID	Proposed	Dest Addr	Src Addr	More information	Status	Actions
A387682_Punch_1	13:08, 26 Jul 2022	193.147.107.24	191.202.168.171	Protocolo: tcp Port: 123	PENDING	  
A387682_Punch_2	13:12, 26 Jul 2022	193.147.107.24	125.251.122.131	Protocolo: tcp Port: 123	PENDING	  

Shortcuts

 Añadir Regla  Reglas  Reglas propuestas  Dashboard

Desde esta ventana podremos o bien hacer commit de la regla al router, eliminarla o editarla antes de hacer el commit. Para cualquiera de estas acciones también hay que verificar tu identidad como cuando se añade una regla, es decir introducir el código enviado a tu slack.

Mi perfil

En el último botón de la barra lateral tenemos el apartado de 'mi perfil' donde veremos la organización en la que estamos registrados así como nuestro nombre de usuario y una opción para poder cambiar la contraseña.

Mi perfil

Institución

Punch


1.1.1.1/32 193.145.15.29/32 2.2.2.2/32

Usuario

Username: acsnz

First name: alicia

Last name: snz

Email: 

[Cambiar contraseña](#)

Shortcuts

[Añadir Regla](#)[Reglas](#)[Reglas propuestas](#)[Dashboard](#)