MANUAL DE CONFIGURACIÓN PARA LA IDENTIFICACIÓN DE FIRMAS PARA IMPLEMENTACIÓN EL IPS EN FORTINET

ANEXO

PRESENTADO POR:
DAVID ALEJANDRO TORRES RONCANCIO
JOSE FELIPE ZAMBRANO PEREZ

MODERNIZACION TECNOLÓGICA DE LA INFRAESTRUCTURA DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL PARA LA RED CORPORATIVA

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
[06/06/2020]

Sistema de prevención de intrusos IPS

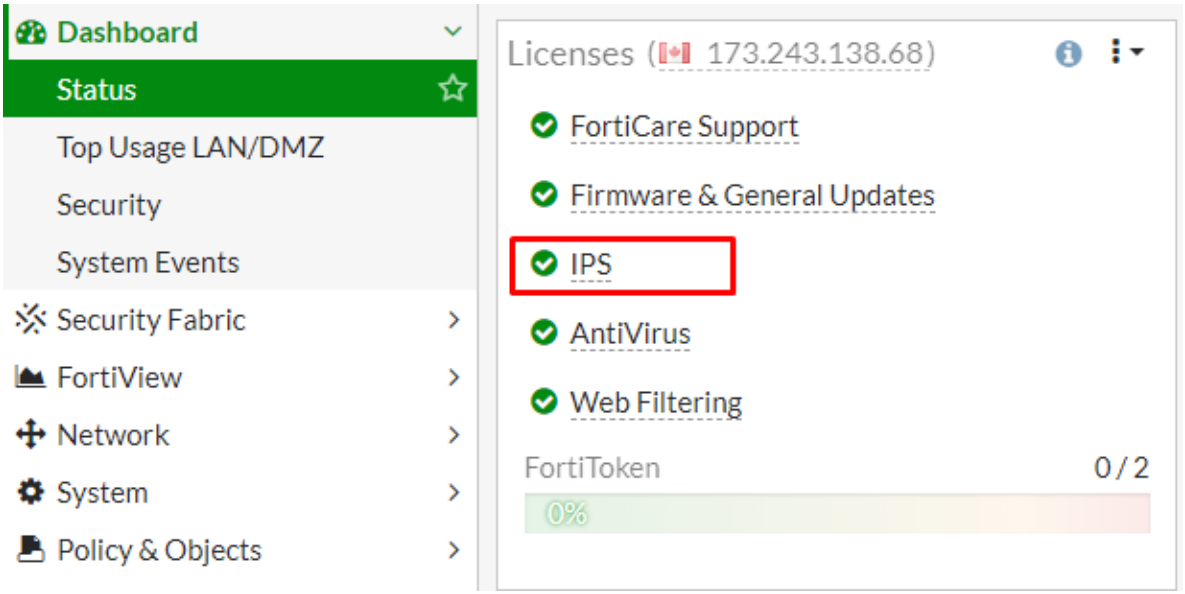
El sistema de previsión de intrusos es una funcionabilidad incorporada en la mayoría de los firewalls de Next- Generation Firewall (NGFW), Fortinet incorporo esta tecnología hace más de unos años atrás, este sistema protege contra ataques de malware y amenazas conocidas o de día cero con una más de 13362 firmas en su base de datos.

Para el correcto funcionamiento del IPS en Fortigate debe tener conexión a Fotiguard el cual proporciona las actualizaciones de las firmas de ataques o vulnerabilidades conocidas.

A continuación, se detallará el proceso de activación y configuración del perfil de seguridad IPS para el firmware 6.2

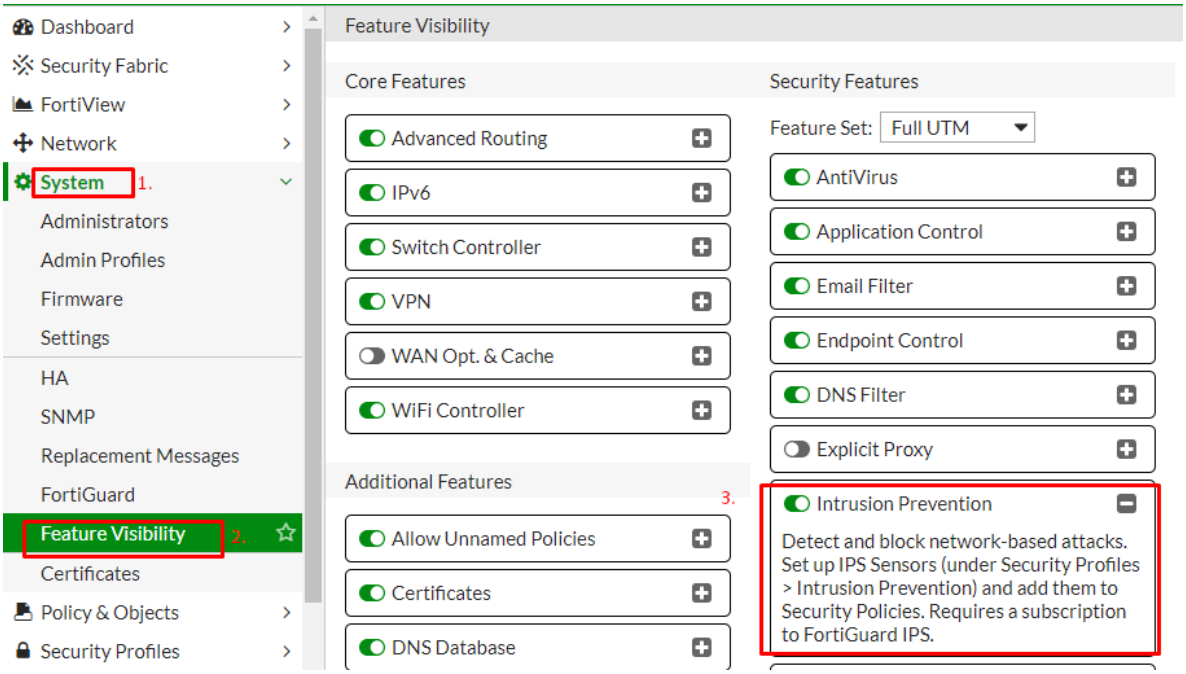
Paso 1.

El primer paso consiste en verificar en el firewall Fortigate el Dashborad > Status en la sección de licencias donde indica que servicios se tiene activos, debe tener activa la licencia de IPS, Fortinet por lo general incluye una licencia full UTM donde abarca antivirus, web filter e IPS.



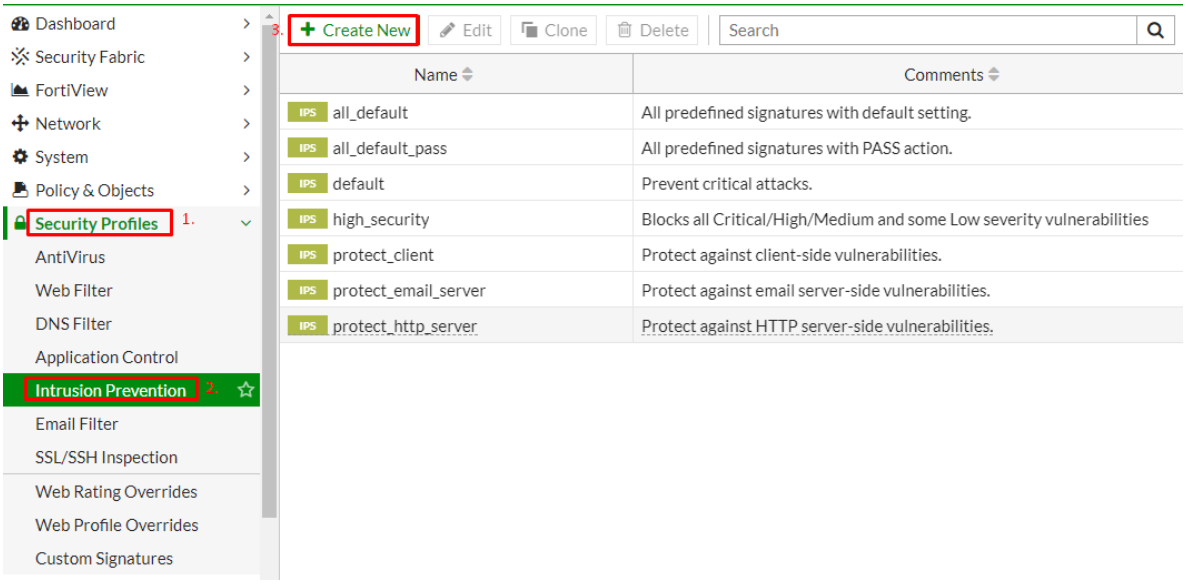
Paso 2.

En el Fortigate se procede a realizar la activación del modulo de seguridad IPS, seleccionamos System > Feature Visibility > Intrusión Prevention.



Paso 3.

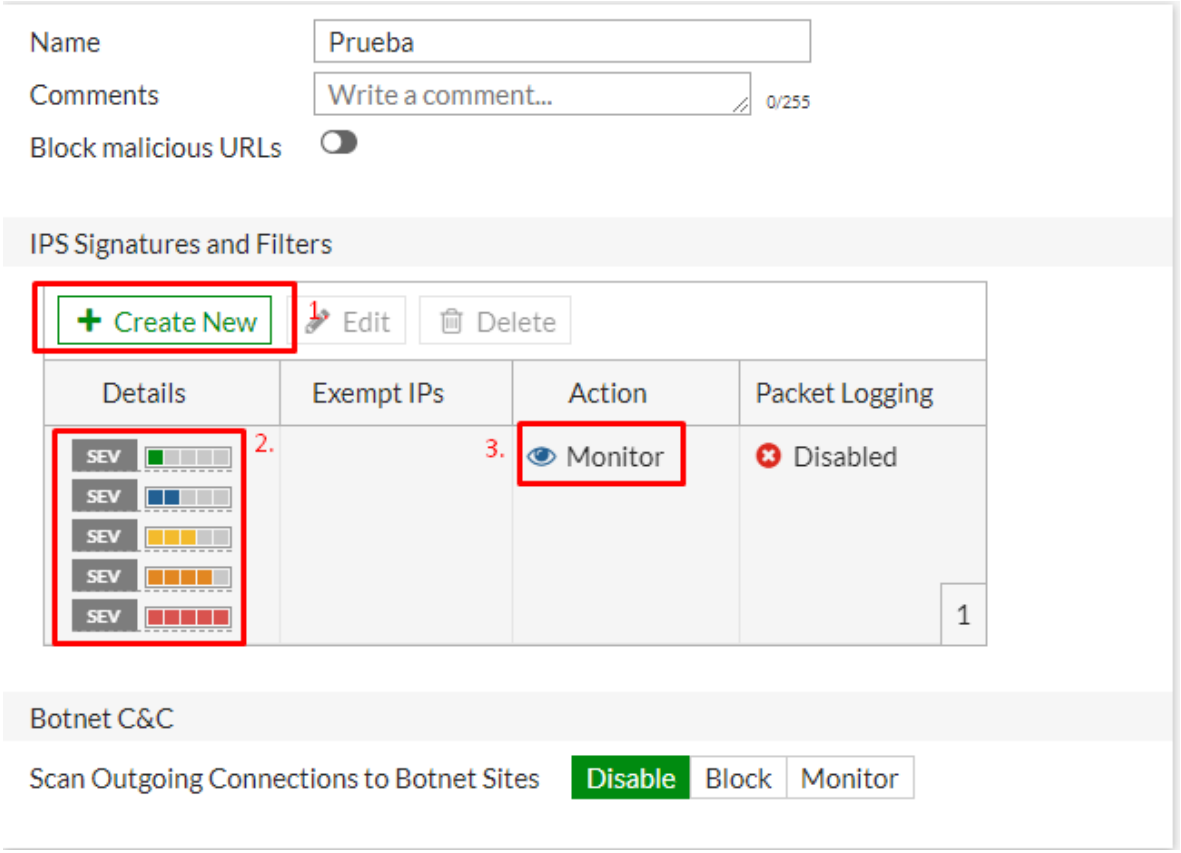
Una vez verificado la licencia y la conexión al Fortiguard se procede con la creación del perfil de seguridad IPS, seleccionamos Secuity Profiles > Intrusion Protection > create New.



Para la versión de firmware 6.2 Fortinet incluye unos perfiles de seguridad IPS por default.

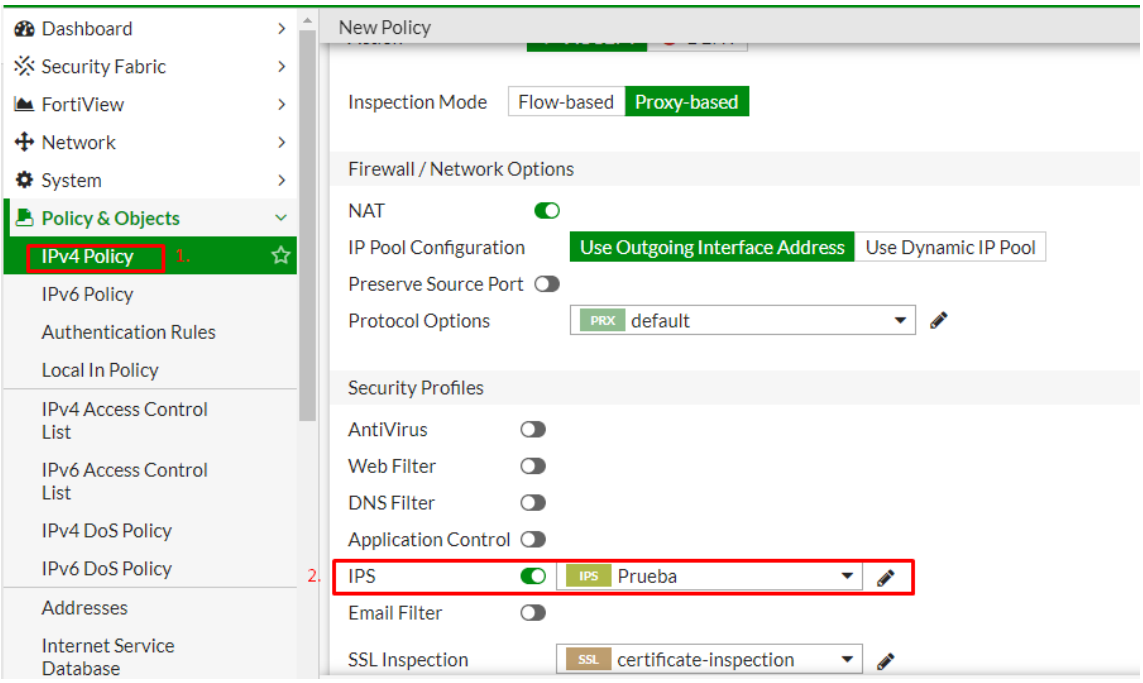
Paso 4.

Se procede a crear un perfil IDS (solo detección) con la acción de monitoreo filtrando las amenazas críticas, altas, medias, bajas e informativas para la identificación de firmas con el fin de perfilar el perfil de IPS definitivo para la organización determinada.



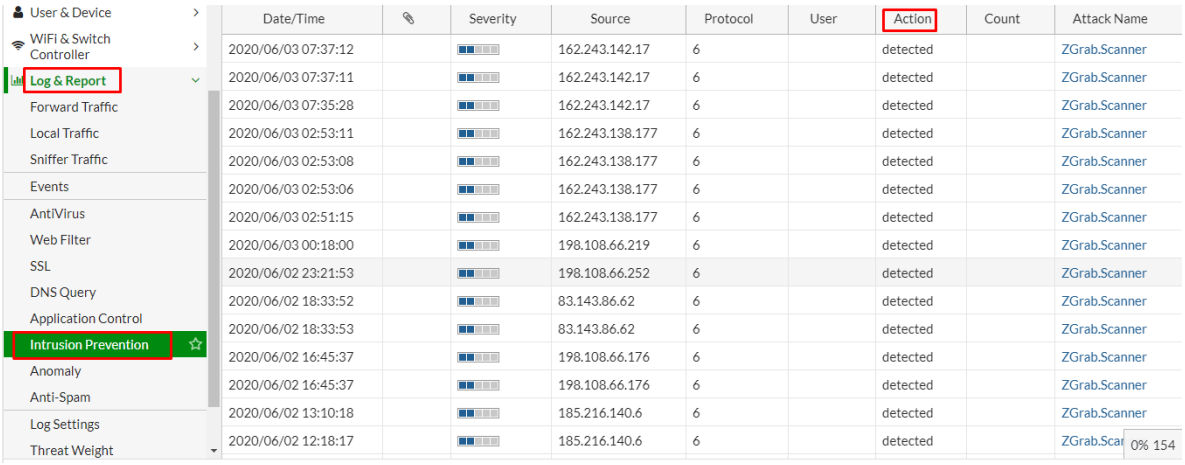
Paso 5.

Se debe realizar la activación del perfil de seguridad en la política correspondiente de acuerdo ala necesidad requerida (publicaciones, navegación).



Paso 6

Al activar el perfil de seguridad en la política procedemos a revisar los logs en el Fortigate o si se tiene implementado un FortiAnalyzer después de un tiempo determinado, para identificar las firmas y configurar el perfil de seguridad definitivo realizando los bloqueos pertinentes.



Para el FortiAnalyzer por defecto trae un reporte gerencial de IPS donde se visualiza la cantidad de ataques y de firmas encontradas.

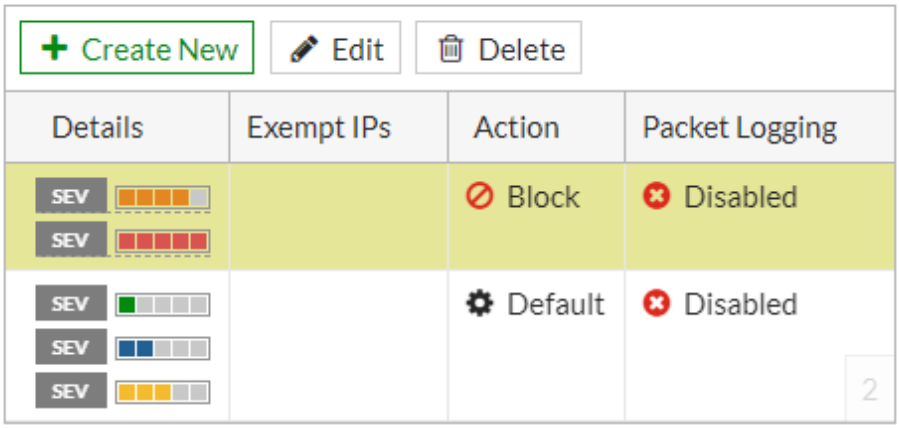
Intrusions Monitored

#	Intrusion Name	Intrusion Type	Severity	Counts
1	Backdoor.DoublePulsar	Malware	Critical	20,843
2	tcp_dst_session	Anomaly	Critical	2,896
3	ip_dst_session	Anomaly	Critical	2,883
4	H-worm.Botnet		Critical	207
5	tcp_syn_flood	Anomaly	Critical	27
6	Apache.Commons.Collection.InvokerTransformer.Code.Execution	OS Command Injection	Critical	13
7	Linear.eMerge.card_scan_decoder.php.Command.Injection		Critical	3
8	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution		Critical	1
9	Mirai.Botnet		High	7
10	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	Information Disclosure	Medium	214
11	TCP.Out.Of.Range.Timestamp	DoS	Low	3,258,711
12	TCP.Overlapping.Fragments	Buffer Errors	Low	8,235
13	HTTP.Request.Smuggling	Permission/Priviledge/Access Control	Low	5,165
14	NBSS.Invalid.Fragment	Anomaly	Low	62
15	TCP.Bad.Option.Length	Anomaly	Low	30
16	TCP.Window.Size.Zero.DoS	DoS	Low	8

Paso 7.

Al realizar el respectivo análisis de los logs correspondientes al perfil de seguridad activado en modo de monitoreo y de acuerdo al resultado, se debe realizar la configuración del perfil definitivo con acción de bloquear de acuerdo a las firmas encontradas y con el fin de mitigar las vulnerabilidades.

IPS Signatures and Filters



Referencias

https://www.fortinet.com/products/ips#services

https://ncora.com/fortigate-modulo-ips/

https://www.fortinet.com/products/ips