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.

2 Dashboard	> _	Feature Visibility				
🔆 Security Fabric	>	Core Features		Security Features		
FortiView	>					
🕂 Network	>	C Advanced Routing	•	Feature Set: Full UTM		
System 1.	~	C IPv6	0	AntiVirus	0	
Administrators		Switch Controller		C Application Control	0	
Admin Profiles				Email Eilter		
Firmware		C VPN	•			
Settings		WAN Opt. & Cache		C Endpoint Control	0	
HA		NiEi Controllor		O DNS Filter	C	
SNMP Replacement Message		WIFI Controller		Explicit Proxy	0	
FortiGuard	5	Additional Features	3			
Feature Visibility	<mark>2.</mark> ☆	C Allow Unnamed Policies	0	Intrusion Prevention Detect and block network-based attack	s.	
Certificates				Set up IPS Sensors (under Security Prof	ile	
Policy & Objects	>			Security Policies. Requires a subscription		
Security Profiles	>	O DNS Database	0	to FortiGuard IPS.		

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.

Dashboard	> ^	3. 🛨 Create New 🖋 Edit 🔚 Clone 🍵	Delete Search Q
🔆 Security Fabric	>	Namo	Commonts A
🖿 FortiView	>	Name 🗸	Comments
🕂 Network	>	IPS all_default	All predefined signatures with default setting.
System	>	IPS all_default_pass	All predefined signatures with PASS action.
Policy & Objects	>	IPS default	Prevent critical attacks.
Security Profiles 1.	~	IPS high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities
AntiVirus		protect_client	Protect against client-side vulnerabilities.
Web Filter		protect_email_server	Protect against email server-side vulnerabilities.
DNS Filter		protect_http_server	Protect against HTTP server-side vulnerabilities.
Application Control			
Intrusion Prevention 2.	☆		
Email Filter			
SSL/SSH Inspection			
Web Rating Overrides			
Web Profile Overrides	1		
Custom Signatures			

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.

Name	Prueba						
Comments	Write a comme	Write a comment // 0/255					
Block malicious URLs							
IPS Signatures and Filt	ers						
+ Create New	🌛 Edit 🗎 🗎 De	lete					
Details	Exempt IPs	Action	Packet Logging				
SEV	3.	Monitor	Oisabled				
Botnet C&C							
Scan Outgoing Connections to Botnet Sites Disable Block Monitor							

Paso 5.

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

🚯 Dashboard	New Policy
🔆 Security Fabric	>
🖿 FortiView	> Inspection Mode Flow-based Proxy-based
+ Network	>
System	> Firewall / Network Options
Policy & Objects	VAT C
IPv4 Policy 1.	IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool
IPv6 Policy	Preserve Source Port 🔾
Authentication Rules	Protocol Options PRX default
Local In Policy	
IPv4 Access Control	Security Profiles
List	AntiVirus 🔿
IPv6 Access Control	Web Filter
List	DNS Filter
IPv4 DoS Policy	Application Control
IPv6 DoS Policy	2. IPS 💽 IPS Prueba 👻 🖋
Addresses	Email Filter
Internet Service Database	SSL Inspection sst certificate-inspection 🔹

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.

User & Device	>	Date/Time	Ø	Severity	Source	Protocol	User	Action	Count	Attack Name
WiFi & Switch Controller	>	2020/06/03 07:37:12			162.243.142.17	6		detected		ZGrab.Scanner
山 Log & Report	~	2020/06/03 07:37:11			162.243.142.17	6		detected		ZGrab.Scanner
Forward Traffic	- 1	2020/06/03 07:35:28			162.243.142.17	6		detected		ZGrab.Scanner
Local Traffic		2020/06/03 02:53:11			162.243.138.177	6		detected		ZGrab.Scanner
Sniffer Traffic		2020/06/03 02:53:08			162.243.138.177	6		detected		ZGrab.Scanner
Events		2020/06/03 02:53:06			162.243.138.177	6		detected		ZGrab.Scanner
AntiVirus		2020/06/03 02:51:15			162.243.138.177	6		detected		ZGrab.Scanner
Web Filter		2020/06/03 00:18:00			198.108.66.219	6		detected		ZGrab.Scanner
SSL		2020/06/02 23:21:53			198.108.66.252	6		detected		ZGrab.Scanner
DNS Query		2020/06/02 18:33:52			83.143.86.62	6		detected		ZGrab.Scanner
Application Control	_	2020/06/02 18:33:53			83.143.86.62	6		detected		ZGrab.Scanner
Intrusion Prevention	☆	2020/06/02 16:45:37			198.108.66.176	6		detected		ZGrab.Scanner
Anomaly		2020/06/02 16:45:37			198.108.66.176	6		detected		ZGrab.Scanner
Anti-Spam	-	2020/06/02 13:10:18			185.216.140.6	6		detected		ZGrab.Scanner
Log Settings Threat Weight		2020/06/02 12:18:17			185.216.140.6	6		detected		ZGrab.Scar 0% 154

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

Intrusions	Monitored
intrusions	women

#	Intrusion Name	Intrusion Type	Severity	Counts
1	Backdoor.DoublePuls ar	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.Co llection.InvokerTransfor mer.Code.Execution	OS Command Injection	Critical	13
7	Linear.eMerge.card_s can_decoder.php.Comm and.Injection		Critical	3
8	PHPUnit.Eval-stdin.P HP.Remote.Code.Executi on		Critical	1
9	Mirai.Botnet		High	7
10	MS.SMB.Server.Trans .Peeking.Data.Informatio n.Disclosure	Information Disclosure	Medium	214
11	TCP.Out.Of.Range.Ti mestamp	DoS	Low	3,258,711
12	TCP.Overlapping.Frag ments	Buffer Errors	Low	8,235
13	HTTP.Request.Smugg ling	Permission/Priviledge/Ac cess Control	Low	5,165
14	NBSS.Invalid.Fragme nt	Anomaly	Low	62
15	TCP.Bad.Option.Leng th	Anomaly	Low	30
16	TCP.Window.Size.Zer	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							
+ Create Nev	v 🖋 Edit 1	🗊 Delete					
Details	Exempt IPs	Action	Packet Logging				
SEV SEV		O Block	Oisabled				
SEV		Default	8 Disabled				
SEV				2			

Referencias

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

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

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