



## Protección en Publicaciones IPv6 – DC CAN

Cada publicación por IPv6 además de la restricción de puerto correspondiente, tiene un perfil de Antivirus aplicado y un perfil de IPS que tiene como objetivo bloquear las firmas categorizadas como Críticas, Altas y Medias.

From	To	Source	Destination Address	Schedule	Service	Action	NAT	Security Profiles
WAN	LAN	all	all	always	ALL	DENY		
WAN	DMZ_VIP	all	2801:1e2:1:1026::167	always	HTTP HTTPS	ACCEPT	Disabled	AV default IPS IPS_WINDOWS_IIS SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::155	always	HTTP HTTPS	ACCEPT	Enabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::113	31_12_2020	HTTP HTTPS ALL_ICMP	ACCEPT	Enabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::31	always	HTTP HTTPS ALL_ICMP6	ACCEPT	Disabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::103	always	HTTP HTTPS TCP_8380	ACCEPT	Enabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::101	always	HTTP HTTPS	ACCEPT	Enabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection
WAN	DMZ_VIP	all	2801:1e2:1:1026::19	always	HTTP HTTPS	ACCEPT	Enabled	AV default IPS Block_Critical_High_Medium SSL certificate-inspection

Sin embargo, sobre el Datacenter CAN no se tiene logs de firmas bloqueadas por IPv6 durante los últimos 30 días.

Log View							ADOM: CAN
FortiGate	All Devices	Last N Days	N 30	Feb 02 To Mar 04			
Traffic	Destination IP = "2801*" Add Filter						
Security	#	Date/Time	Device ID	Severity	Source	Destination IP	Action
Antivirus	No entry found.						
Intrusion Prevention							



## Protección en Publicaciones IPv6 – DC CAN

Cada publicación por IPv6 además de la restricción de puerto correspondiente, tiene un perfil de Antivirus aplicado y un perfil de IPS que tiene como objetivo bloquear las firmas categorizadas como Críticas, Altas y Medias y relacionadas con la capa media con el cual se despliega la aplicación.

From	To	Source	Destination Address	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
WAN	DMZ	all	2801:1e2:5:8104::143 2801:1e2:5:8104::221	always	HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	1.78 TB
WAN	DMZ	all	2801:1e2:5:8103::82	always	HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	24.96 GB
WAN	DMZ	all	2801:1e2:5:8103::161	always	ALL_ICMP6 TCP_8080 TCP_8380	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	11.01 GB
WAN	DMZ	all	2801:1e2:5:8106::85	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Enabled	AV_MEN2 SERVER_WINDOWS_APACHE certificate-inspection	All	124.36 MB
WAN	DMZ	all	2801:1e2:5:8103::188 2801:1e2:5:4200::188 2801:1e2:5:8106::188	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 SERVER_WINDOWS_IIS certificate-inspection	All	41.44 GB
WAN	DMZ	all	2801:1e2:5:8104::133	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	586.55 MB
WAN	DMZ	all	2801:1e2:5:8281::19	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	99.60 MB
WAN	DMZ	all	2801:1e2:5:8103::71	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 SERVER_WINDOWS_IIS certificate-inspection	All	9.92 GB
WAN	DMZ	all	2801:1e2:5:8106::230	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 SERVER_WINDOWS_IIS certificate-inspection	All	168.25 MB
WAN	DMZ	all	2801:1e2:5:8103::81	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	44.66 GB
WAN	DMZ	all	2801:1e2:5:8103::93	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 SERVER_WINDOWS_APACHE certificate-inspection	All	3.23 MB
WAN	DMZ	all	2801:1e2:5:4116::93	always	ALL_ICMP6 HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 SERVER_WINDOWS_APACHE certificate-inspection	All	0 B
WAN	DMZ	all	2801:1e2:5:8104::111	always	HTTP HTTPS ALL_ICMP6	ACCEPT	Enabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	64.87 MB
WAN	DMZ	all	2801:1e2:5:8101::126	always	HTTP HTTPS ALL_ICMP6	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	885.48 MB
WAN	DMZ	all	2801:1e2:5:8101::127	always	HTTP HTTPS	ACCEPT	Disabled	AV_MEN2 IPS-LINUX_APACHE_TOMCAT_JBOSS certificate-inspection	All	0 B

A nivel de logs sobre las publicaciones en el datacenter externo si ha habido eventos en los últimos 30 días.



La educación  
es de todos

Mineducación

Log View

ADOM: TITANIUM

FortiGate

Traffic

Security

Antivirus

Intrusion Prevention

Application Control

Web Filter

DNS

SSL

Event

FortiWeb

FortiDDoS

Syslog

Custom View

Log Browse

Log Group

FW-TIT-01M\_MEN\_CO

Last N Days

N 30

Feb 02 To Mar 04

Custom View

Destination IP = "2801"

Add Filter

#	Date/Time	Device ID	Severity	Source	Destination IP	Action	Service
1	15:15:09	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:7292:7800:20a...	dropped	HTTP
2	15:15:08	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:7292:7800:20a...	dropped	HTTP
3	12:43:28	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:e910:e8a1:f031...	dropped	HTTP
4	12:43:28	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:e910:e8a1:f031...	dropped	HTTP
5	10:52:49	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:a54e:92fb:6694...	dropped	HTTP
6	10:52:49	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101:a54e:92fb:6694...	dropped	HTTP
7	03-02 17:17	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101::127	dropped	HTTP
8	03-02 17:17	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8101::127	dropped	HTTP
9	03-02 17:17	FG36E1TB19900...	critical	2001:4ca0:108:42:0:443:6:9	2801:1e2:5:8101::127	dropped	HTTPS
10	03-02 17:17	FG36E1TB19900...	critical	2001:4ca0:108:42:0:443:6:9	2801:1e2:5:8101::127	dropped	HTTPS
11	03-02 17:08	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8281::19	dropped	HTTP
12	03-02 17:08	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8281::19	dropped	HTTP
13	03-02 17:08	FG36E1TB19900...	critical	2001:4ca0:108:42:0:443:6:9	2801:1e2:5:8281::19	dropped	HTTPS
14	03-02 17:08	FG36E1TB19900...	critical	2001:4ca0:108:42:0:443:6:9	2801:1e2:5:8281::19	dropped	HTTPS
15	03-02 17:00	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8104::133	dropped	HTTP
16	03-02 17:00	FG36E1TB19900...	critical	2001:4ca0:108:42:0:80:6:9	2801:1e2:5:8104::133	dropped	HTTP
17	03-02 17:00	FG36E1TB19900...	critical	2001:4ca0:108:42:0:443:6:9	2801:1e2:5:8104::133	dropped	HTTPS