

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 1 de 18
	31/05/2016	1	31/05/2016	


Guía de Homologación Fortigate 200D

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	31/05/2016	1	31/05/2016	Página 2 de 18

Nombre		Fecha	Unidad
Elaboró	Jonathan Vargas	31/05/2016	Dpto. Soporte Especializado
	Victor Nuñez		
Revisó	Claudio Perdic	31/05/016	Dpto. Soporte Especializado
Revisó			


Registro de Modificaciones				
Revisión		Emisor	Descripción De la Modificación	Aprobó
Nº	Fecha	Nombre Dpto. /		
1	31/05	V. Nuñez	Crea el documento.	C. Perdic
2				
3				
4				
5				
6				
7				
8				
9				
10				

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 3 de 18
	31/05/2016	1	31/05/2016	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 4 de 18
	31/05/2016	1	31/05/2016	

INDICE

1. OBJETIVOS.....	5
2. ALCANCES	5
3. ESQUEMA LABORATORIO DE HOMOLOGACIÓN	5
4. EQUIPO HOMOLOGADO 200D	6
5. RESULTADO DE HOMOLOGACIÓN	8
5.1. Rendimiento	8
5.2. Configuración.....	9
6. Conclusiones.....	18

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 5 de 18
	31/05/2016	1	31/05/2016	

1. **OBJETIVOS**

- Presentar los resultados de la homologación del equipo Fortigate 200D como CPE para los servicios de Claro.
- Configuraciones estándar de equipos Fortigate 200D.


2. **ALCANCES**

En el presente documento se ven los resultados y lista de configuraciones del equipo Fortigate 200D. Configuraciones con los servicios comúnmente utilizados en equipos CPE de clientes, tanto para sitios centrales como sucursales.

3. **ESQUEMA LABORATORIO DE HOMOLOGACIÓN**

El esquema del laboratorio para esta tarea está compuesto por 2 etapas:

- Rendimiento: Se conecta el equipo directamente al equipo IXIA, el cual nos proporciona la prueba de rendimiento de acuerdo al RFC 2544.
- Funcionalidades: Se conecta el equipo a una serie de equipos simulando una interred hacia la MPLS. Se verifican todas las funcionalidades que se entregan como Claro, entre las cuales se destacan seguridad centralizada, ruteo dinámico, DHCP, NAT, entre otras.


	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 6 de 18
	31/05/2016	1	31/05/2016	

4. EQUIPO HOMOLOGADO 200D

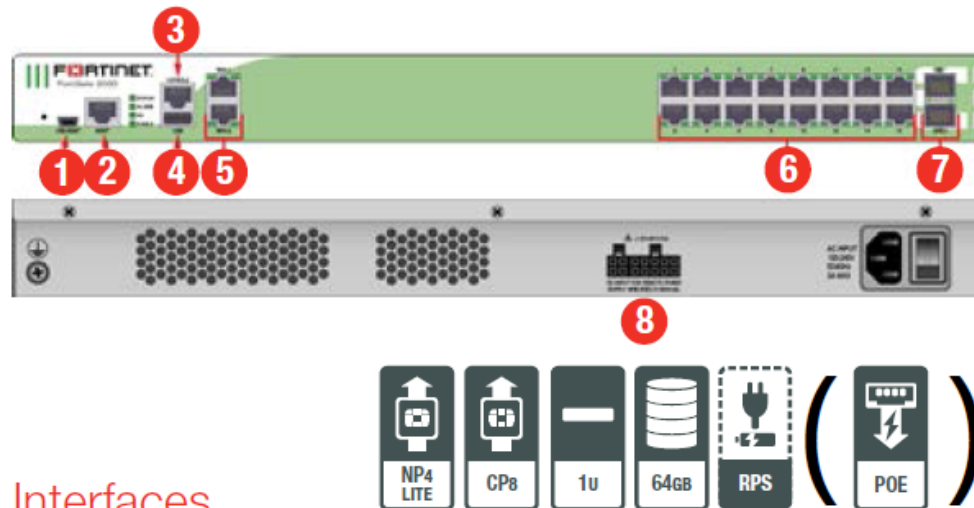
Equipo con capacidad de 2 puertas WAN 10/100/1000 Mbps, adicionalmente posee 16 interfaces LAN 10/100/1000 y 2 puertas Giga para uso con SFP. Posee 1 USB y conector consola estándar.

El sistema y especificaciones del equipo utilizado son:

Fortigate 200D
FG200D3915803104 # get system status Version: FortiGate-200D v5.2.4,build0688,150722 (GA) Virus-DB: 16.00560(2012-10-19 08:31) Extended DB: 1.00000(2012-10-17 15:46) IPS-DB: 5.00555(2014-10-07 01:21) IPS-ETDB: 0.00000(2001-01-01 00:00) Serial-Number: FG200D3915803104 Botnet DB: 1.00000(2012-05-28 22:51) BIOS version: 05000004 System Part-Number: P11534-06 Log hard disk: Available Internal Switch mode: interface Hostname: FG200D3915803104 Operation Mode: NAT Current virtual domain: root Max number of virtual domains: 10 Virtual domains status: 1 in NAT mode, 0 in TP mode Virtual domain configuration: disable FIPS-CC mode: disable Current HA mode: standalone Branch point: 688 Release Version Information: GA FortiOS x86-64: Yes System time: Mon May 23 08:16:00 2016


	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	31/05/2016	1	31/05/2016	Página 7 de 18

FortiGate 200D(-POE)



Interfaces

1. USB Management Port
2. Management Port
3. Console Port
4. USB Port
5. 2x GE RJ45 WAN Interfaces
6. 16x GE RJ45 LAN Interfaces / 8x GE RJ45 LAN and
8x GE RJ45 PoE Interfaces on POE Model
7. 2x GE SFP DMZ Interfaces
8. FRPS Connector (not available on FG-200D-POE)

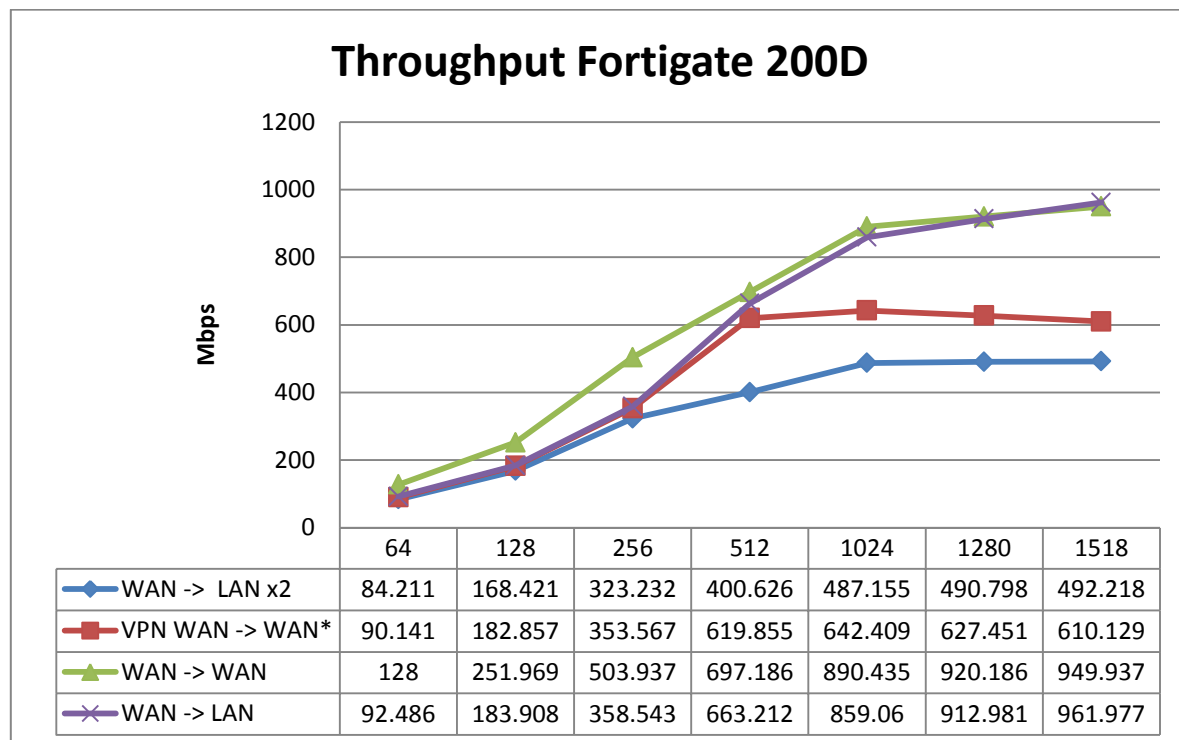
	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	31/05/2016	1	31/05/2016	Página 8 de 18


5. RESULTADO DE HOMOLOGACIÓN

5.1. *Rendimiento*

En la tabla siguiente se puede ver el rendimiento del equipo alcanzado de acuerdo al RFC 2544. Se diferencian 4 curvas:


- WAN -> LAN x2: Se utilizaron 4 interfaces del equipo, enviando tráfico desde las puertas WAN hacia las puertas LAN.
- WAN -> WAN: Se utilizaron solamente las puertas WAN y se envió tráfico entre ellas.
- WAN -> LAN: Se utilizaron una puerta WAN y una LAN y se envió tráfico entre ellas.
- VPN: Se establece una VPN IPSec Site to Site contra otro equipo 200D conectados por una puerta WAN y utilizando la otra puerta WAN.




	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 9 de 18
	31/05/2016	1	31/05/2016	

5.2. Configuración


Sección	Configuración	Comentarios
Configuración de interfaz física WAN	config system interface	
	edit "wan1"	Se define que puerta se modifica.
	set vdom "root"	
	set mode static	Se define como será el direccionamiento.
	set ip 192.168.1.2 255.255.255.252	
	set allowaccess ping snmp telnet	Se determina que servicios tendrá la puerta, se deben habilitar siempre PING, SNMP y TELNET
	set status up	Por defecto viene UP.
	set type physical	Se define que la puerta será L3
	set description ''	
	set speed auto	Se define la velocidad de la puerta.
	next end	
Configuración de interfaz loopback	config system interface edit "Loopback 0" set vdom "root" set ip 10.156.33.152 255.255.255.255 set allowaccess ping snmp telnet radius-acct set status up set type loopback set description '' next end	
Configuración de Sub-Interfaces	config system interface edit "DATOS" set vdom "root" set mode static set ip 10.1.1.20 255.255.255.0 set allowaccess ping snmp telnet set status up	
	set type vlan	Se define la puerta como Sub-Interfaz Vlan
	set interface "wan1"	Se define a que puerta física está ligada.
	set vlanid 201	Se define el tag de la VLAN a utilizar
	next end	
Configuración de IP secundaria	config system interface edit "lan4" set secondary-IP enable config secondaryip edit 1 set ip 10.10.10.2 255.255.255.252 next end next end	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial			Código Documento
	Guía de Homologación			
	Equipo Fortigate 200D			
	Fecha de Revisión 31/05/2016	Revisión N° 1	Fecha de Emisión 31/05/2016	Página 10 de 18


Sección	Configuración	Comentarios
Configuración de puertos switch	<pre> config system interface edit "lan" set vdom "root" set ip 192.168.1.99 255.255.255.0 set allowaccess ping https ssh http fgfm capwap set type hard-switch set listen-forticlient-connection enable set role lan set snmp-index 5 nextend </pre>	Se configure una puerta "internal", que define la IP que va a tener, simil a una interfaz vlan.
	<pre> config system virtual-switch </pre>	Se configuran las puertas switch del equipo
	<pre> edit "lan" </pre>	Se define un nombre que se asocie a la interfaz vlan.
	<pre> set physical-switch "sw0" </pre>	Se debe definir un nombre para el grupo a utilizar.
	<pre> config port </pre>	
	<pre> edit "port1" next </pre>	Se editan las puertas a utilizar, aca se puede definir speed y status.
	<pre> edit "port2" next edit "port3" next edit "port4" next edit "port5" next </pre>	Se agregan o editan el resto de las puertas.
	<pre> delete "port6" </pre>	Si se desea eliminar una puerta de la asocian, se utiliza delete y esta aparecera como interfaz fisica en el listado normal.
Configuración de VRRP – HSRP	<pre> end next end </pre>	
	<pre> config system interface edit "wan2" set vrrp-virtual-mac enable config vrrp edit 1 set vrip 10.1.1.100 set priority 120 set vrgrp 10 next end next end </pre>	
Rutas Estáticas	<pre> config router static edit 1 </pre>	
	<pre> set dst 10.3.35.0 255.255.255.0 </pre>	Se define la ruta.
	<pre> set gateway 10.3.30.1 </pre>	Se define el siguiente salto.
	<pre> set device "lan4" </pre>	Se debe definir por cual interfaz está el siguiente salto
	<pre> next end </pre>	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 11 de 18
	31/05/2016	1	31/05/2016	


Sección	Configuración	Comentarios
Ruteo Dinámico BGP	config router bgp	
	set as 64924	Se define el AS del equipo.
	set router-id 10.1.1.20	Se define el ID con que se levanta BGP.
	config neighbor	Se definen los diferentes vecinos que va a tener el servicio.
	edit "10.1.1.1"	
	set remote-as 64923	Se define el AS del vecino
	set route-map-in "Filtro_IN"	Se define si existe algún route-map asociado al vecino.
	next	
	end	
	config network	Se definen las redes a participar del proceso BGP.
	edit 1	
	set prefix 10.0.33.152 255.255.255.255	Se define una por un a las redes.
	next	
	edit 2	
	set prefix 192.168.2.0 255.255.255.0	
	next	
	end	
	config redistribute "connected"	
	set status enable/disable	Si es necesario se define si se redistribuyen las redes conectadas.
	set route-map "Filtro_OUT1"	
	end	
	config redistribute "static"	
	set status enable/disable	Si es necesario se define si se redistribuyen las rutas estáticas.
	set route-map "Filtro_OUT"	
	end	
	end	
ACL	config router access-list	
	edit "ACL_Filtro_IN"	Se definen ACL con Nombre, como objetos.
	config rule	
	edit 1	
	set action permit	Se definen las redes y acciones de la regla.
	set wildcard 10.1.5.0 0.0.0.255	
	next	
	edit 2	
	set action deny	Se definen las redes y acciones de la regla.
	set wildcard 10.1.5.0 0.0.0.255	
	next	
	edit 3	
	set action permit	Se definen las redes y acciones de la regla.
	set wildcard 10.1.5.0 0.0.0.255	
	next	
	end	
	next	
	end	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial			Código Documento
	Guía de Homologación			
	Equipo Fortigate 200D			
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 12 de 18
	31/05/2016	1	31/05/2016	


Sección	Configuración	Comentarios
Filtros Route-MAP	config router route-map	.
	edit "Filtro_IN"	Se define el Nombre del route-map
	config rule	
	edit 1	Se define qué tipo de acción tiene el route-map
	set match-ip-address "ACL_Filtro_IN"	Opcional
	set set-aspath-action prepend	Opcional
	set set-aspath "56000 56000 56000"	
Objetos de RED	next	
	end	
	next	
	end	
	config firewall address	
	edit "REDES_LAN"	Se define el Nombre del objeto de RED
	set associated-interface "lan2"	Se define la interfaz asociada al objeto.
	set type ipmask	Se define el tipo de objeto de red.
	set subnet 10.1.1.0 255.255.255.0	Se define la red.
	next	
	edit "LAN2"	
	set associated-interface "lan3"	Se define el Nombre del objeto de RED
	set type iprange	Se define la interfaz asociada al objeto.
Políticas de Trafico (Como el equipo es FW, es necesario definir políticas de trafico de acuerdo a lo configurado) ES IMPORTANTE EL ORDEN DE LAS REGLAS, YA QUE SE APLICAN SECUENCIAL	set end-ip 192.168.100.50	Se define la IP de inicio del rango
	set start-ip 192.168.100.20	Se define la IP de fin del rango
	next	
	end	
	config firewall policy	
	edit 1	Edita la primera regla.
	set srcintf "wan1"	Se define la interfaz de origen del tráfico.
	set dstintf "wan2"	Se define la interfaz de destino del tráfico.
	set srcaddr "all"	Se define las IP de origen (deben ser objetos de red asociado a la interfaz de origen) del tráfico.
	set dstaddr "all"	Se define las IP de destino (deben ser objetos de red asociado a la interfaz de destino) del tráfico.
	set action accept	Se define a la acción de la regla.
	set schedule "always"	
	set service "ALL"	Se define qué tipo de tráfico se desea aplicar (puede ser objeto de servicio).
	next	
	edit 2	Ejemplo de la regla reciproca a la anterior.
	set srcintf "wan2"	
	set dstintf "wan1"	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 13 de 18
	31/05/2016	1	31/05/2016	


	<pre> set srcaddr "all" set dstaddr "all" set action accept set schedule "always" set service "ALL" next end </pre>	
DHCP Server	<pre> config system dhcp server edit 1 </pre>	Se define el servidor a utilizar
	<pre> set dns-service default set default-gateway 192.168.2.1 </pre>	Se define el default Gateway que entrega el servidor.
	<pre> set netmask 255.255.255.0 </pre>	Se define la máscara de la red.
	<pre> set interface "lan2" </pre>	Se asocia el servidor a una interfaz.
	<pre> config ip-range edit 1 </pre>	Se define el rango de IP del servidor
	<pre> set start-ip 192.168.2.100 </pre>	Se define la ip de inicio del rango a entregar por el servidor.
	<pre> set end-ip 192.168.2.254 </pre>	Se define la ip de fin del rango a entregar por el servidor.
	<pre> next end next end </pre>	
NAT	<pre> config firewall ippool edit "Nat_Lan" </pre>	Se define un objeto de pool ip para el NAT.
	<pre> set startip 200.29.174.74 </pre>	Se define el inicio del rango de IP para el NAT.
	<pre> set endip 200.29.174.74 </pre>	Se define el fin del rango de IP para el NAT.
	<pre> set type overload </pre>	Se define de tipo Overload (PAT)
	<pre> next end </pre>	
	<pre> config firewall policy edit 4 </pre>	Se asocia el NAT a una política de acceso.
	<pre> set name "Lan2Internet" </pre>	Se define el nombre de la regla
	<pre> set srcintf "lan" set dstintf "Wan_Internet" set srcaddr "PC_jonathan" set dstaddr "all" set action accept set schedule "always" set service "ALL" </pre>	Se configure los mismos parámetros de la regla simple de acceso
	<pre> set nat enable </pre>	Se habilita el NAT en la regla.
	<pre> set ippool enable </pre>	Se define que se utilizara una IP diferente a la de la interfaz.
	<pre> set poolname "Nat_Lan" </pre>	Se define el objeto asociado a la IP a utilizar el

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 14 de 18
	31/05/2016	1	31/05/2016	


	next	NAT.
	end	
	config firewall policy	
	edit 4	
	set name "Lan2Internet"	
	set srcintf "lan" set dstintf "Wan_Internet" set srcaddr "PC_jonathan" set dstaddr "all" set action accept set schedule "always" set service "ALL"	
	set nat enable	
Configuración de los servidores de radius.	next	Solo se debe habilitar el NAT en la política y tomar la IP de la interfaz por defecto.
	end	
	config user radius	
	edit "Radius"	
	set server "200.27.95.3"	
	set secret telmex_secret	
	set nas-ip 10.156.33.152	
	set auth-type pap	
	set source-ip 10.156.33.152	
	set secondary-server "200.27.193.131" set secondary-secret telmex_secret	
Configuración de los esquemas de autenticación.	next	Se define un nombre para identificar los servidores. Se define el servidor primario. Se define la clave del servidor.
	end	
	config user group	
	edit "Remote_Radius"	
	set group-type firewall set member "Radius"	
Configuración de perfiles de acceso	next	Se define un grupo y se asocia al grupo de servidores antes configurado
	end	
	config system accprofile	
	edit "monitor"	
	set scope vdom	
	set comments ''	
	set mntgrp read	
	set admingrp read	
	set updategrp read	
	set authgrp read	
	set sysgrp read	
	set netgrp read	
	set loggrp read	
	set routegrp read	
	set fwgrp read	
	set vpngrp read	
	set utmgrp read	
	set endpoint-control-grp read	
	set wifi read	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial			Código Documento
	Guía de Homologación			
	Equipo Fortigate 200D			
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 15 de 18
	31/05/2016	1	31/05/2016	


	<pre> next edit "noaccess" set scope vdom set comments '' set mntgrp none set admingrp none set updategrp none set authgrp none set sysgrp none set netgrp none set loggrp none set routegrp none set fwgrp none set vpngrp none set utmgrp none set endpoint-control-grp none set wifi none next end </pre>	Se define el perfil de NoAccess, para la configuración de radius, todos quedan en "none".
Configuración de usuarios locales del equipo.	<pre> config system admin edit "wildcard" </pre>	Se crea un perfil "Wildcard" para la conexión desde RADIUS.
	<pre> set remote-auth enable </pre>	Se autoriza la autenticación remota.
	<pre> set accprofile "noaccess" </pre>	Se define que el perfil es "noaccess", ya que es el radius quien da los permisos.
	<pre> set vdom "root" set wildcard enable </pre>	Se asocia a la vdom native.
	<pre> set remote-group "Remote_Radius" </pre>	Se define tipo wildcard para que todos puedan ingresar.
	<pre> set accprofile-override enable next </pre>	Se asocia al grupo de Radius.
	<pre> edit "sfanor.." set remote-auth enable set accprofile "prof_admin" set vdom "root" set remote-group "Remote_Radius" set password ENC AK1nkyCLeQt+aRJ+uSbqzXVcM41G6Fp2QyN1MY2GV0HX0w= set accprofile-override enable next </pre>	Se autoriza que tome el perfil desde el ACS.
	<pre> edit "sfanor.." set remote-auth enable set accprofile "super_admin" set vdom "root" set remote-group "Remote_Radius" set password ENC AK1nLgKxCz3xVMIAWKeiPmhQw6M03ap4ZdHTzSHXxv1Ezc= set accprofile-override enable next end </pre>	Se define un usuario Local, con perfil de administrador, para en caso de que la conexión al servidor de Radius este abajo.
	<pre> edit "sfanor.." set remote-auth enable set accprofile "super_admin" set vdom "root" set remote-group "Remote_Radius" set password ENC AK1nLgKxCz3xVMIAWKeiPmhQw6M03ap4ZdHTzSHXxv1Ezc= set accprofile-override enable next end </pre>	Se define un usuario Local, con perfil de super administrador, para en caso de que la conexión al servidor de Radius este abajo.
	<pre> config router static edit 3 set dst 200.27.95.0 255.255.255.240 set gateway 10.3.30.1 set device "lan4" next </pre>	Si el equipo no posee rutas dinámicas con la MPLS, se deben definir rutas estáticas a las redes de la Red de Gestión.
	<pre> config router static edit 3 set dst 200.27.95.0 255.255.255.240 set gateway 10.3.30.1 set device "lan4" next </pre>	Si el equipo no posee rutas dinámicas con la MPLS, se deben definir rutas estáticas a las redes de la Red de Gestión.

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial			Código Documento
	Guía de Homologación			
	Equipo Fortigate 200D			
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 16 de 18
	31/05/2016	1	31/05/2016	

	<pre> edit 4 set dst 200.27.193.128 255.255.255.240 set gateway 10.3.30.1 set device "lan4" next end </pre>	
Configuración de Lista de acceso y aplicación en los usuarios.	<pre> config system admin edit "wildcard" </pre>	Se edita el usuario Wildcard, que asocia todos los accesos.
	<pre> set trusthost1 200.27.95.0 255.255.255.240 </pre>	Se autoriza las redes de Gestión
	<pre> set trusthost2 200.27.193.128 255.255.255.240 set trusthost3 192.168.0.0 255.255.255.0 </pre>	Se autoriza la Lan del equipo.
	<pre> next edit "sfanor." set trusthost1 200.27.95.0 255.255.255.240 set trusthost2 200.27.193.128 255.255.255.240 set trusthost3 192.168.0.0 255.255.255.0 </pre>	Se replican las redes para los 2 usuarios locales.
	<pre> next edit "sfanor.." set trusthost1 200.27.95.0 255.255.255.240 set trusthost2 200.27.193.128 255.255.255.240 set trusthost3 192.168.0.0 255.255.255.0 </pre>	Se replican las redes para los 2 usuarios locales.
	<pre> next end </pre>	
Configuración de NTP.	<pre> config system ntp set type custom config ntpserver edit 1 set server "200.27.95.5" </pre>	Se debe configurar NTP global.
	<pre> next end </pre>	Se define el servidor de NTP de la red de Gestión.
	<pre> set ntpsync enable </pre>	Se habilita la sincronización.
	<pre> set source-ip 10.156.33.152 </pre>	Se define la ip de origen de las consultas de NTP.
	<pre> set syncinterval 60 end </pre>	
SNMP	<pre> config system snmp sysinfo set status enable set description "snmp" set contact-info "jvargas@clarochile.cl" set location "fanor" end </pre>	Se habilita el SNMP
	<pre> config system snmp community edit 1 set name "fortinet" </pre>	Se define la comunidad.
		Se edita un grupo.
		Se define el nombre de la comunidad.
	<pre> config hosts edit 1 </pre>	
		Se configuran los host que pertenecen a la comunidad.
	<pre> set ip 190.208.24.128 255.255.255.128 </pre>	Se configura la IP o red de las consultas.
	<pre> set interface "Wan_Datos" </pre>	Se debe definir por cual interfaz es la consulta.
	<pre> next </pre>	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 17 de 18
	31/05/2016	1	31/05/2016	

	<pre> end next end </pre>	
QoS	<pre> config firewall shaper traffic-shaper edit Telefonía set guaranteed-bandwidth 10000 set maximum-bandwidth 10000 set diffserv enable set diffservcode 101110 next edit Video set maximum-bandwidth 60000 set diffserv enable set diffservcode 010010 set priority medium next edit Datos set maximum-bandwidth 30000 set diffserv enable set diffservcode 000000 set priority low next end </pre>	<p>Se deben definir los objetos que definen el BW de acuerdo al tipo de tráfico.</p> <p>En cada objeto se debe identificar que marca de QoS se debe aplicar.</p>
	<pre> config firewall policy edit 2 set uuid 69a78358-cff7-51e5-90ba-77a9ae3fbb74 set srcintf "lan1" set dstintf "wan1" set srcaddr "all" set dstaddr "all" set action accept set schedule "always" set service "ALL" set traffic-shaper "Telefonía" next end </pre>	<p>Cada objeto de QoS se debe agregar a una política específica, por lo que se deben definir los flujos específicos a los cuales agregar QoS.</p>
NetFlow	<pre> config system netflow set collector-ip 190.208.24.144 </pre>	Se define el servidor remoto del NETFLOW
	<pre> set collector-port 9996 </pre>	Se define el puerto de comunicación.
	<pre> set source-ip 10.156.33.152 end </pre>	Se define la ip de origen.
	<pre> config system interface edit "lan" set netflow-sampler both next </pre>	Se debe habilitar en cada puerta la necesidad de capturar el tráfico.
	<pre> edit "Wan_Datos" set netflow-sampler both next </pre>	
	<pre> edit "Wan_Internet" set netflow-sampler both next end </pre>	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 200D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 18 de 18
	31/05/2016	1	31/05/2016	

6. Conclusiones

El equipo homologado en esta guía cumple con las condiciones mínimas para operar como CPE pero con algunas restricciones importantes:

- Valido como **CPE para un solo servicio**, Datos o Internet, no se recomienda para operar con 2 o más servicios, ya que el equipo no está homologado para trabajar con múltiple VDOM.
 - o El símil indicado por proveedor es utilizar vdom, que es virtualizar N firewall en uno físico, pero las problemáticas de utilizar este esquema es que la administración se duplica ya que como se crean N firewall virtuales, estos tienen su propia administración, repitiendo las configuraciones N veces.
- Se válida para servicios de hasta **600 Mbps**.
 - o Si bien el equipo posee un mayor ancho de banda, cercano a 900 Mbps o mayor, se presentan diferentes escenarios y este ancho de banda es el recomendado para la operación óptima del equipo.
 - o Se presentan valores para el rendimiento utilizando **VPN IPSec**, es para tener en consideración que al utilizar esta característica **el BW recomendado es de 200 Mbps**.
- Como el equipo es un Firewall, **se deben configurar políticas de acceso para todos los flujos**.
 - o Dada la estructura de Firewall del equipo, posee una política de denegar todo tipo de tráfico si no se estipula lo contrario, por lo que como CPE, al tener funcionalidad de router, se debe especificar 2 políticas para cada flujo de tráfico que se tenga, por ejemplo para un servicio con 1 WAN y 2 LAN: Wan->Lan, Wan->Lan2, Lan->Wan, Lan->Lan2, Lan2 ->Lan, Lan2->Wan.
- En esta guía **no se validan las funcionalidades de UTM** del equipo (Antivirus, IPS, Filtro Web). Al habilitar estos servicios el rendimiento del equipo disminuye por lo que se debe evaluar caso a caso.
- Equipo no posee servicio de IP SLA, por lo que **no puede operar para servicios con Monitoreo Service Assurance**.
- **Equipo no recomendado para cliente BECH.**