

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	15/03/2016	1.2	14/01/2016	Página 1 de 16

Guía de Homologación Fortigate 80D

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			<i>Código Documento</i>
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	15/03/2016	1.2	14/01/2016	Página 2 de 16


Nombre		Fecha	Unidad
Elaboró	Jonathan Vargas	14/01/2016	Dpto. Soporte Especializado
	Victor Nuñez		
Revisó	Claudio Perdic	14/01/016	Dpto. Soporte Especializado
Revisó			

Registro de Modificaciones				
Revisión		Emisor	Descripción De la Modificación	Aprobó
Nº	Fecha	Nombre Dpto.		
1	14/01	V. Nuñez	Crea el documento.	C. Perdic
2	15/03	V. Nuñez	Agregan configuraciones de QoS	C. Perdic
3				
4				
5				
6				
7				
8				
9				
10				

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 3 de 16
	15/03/2016	1.2	14/01/2016	

INDICE

1. OBJETIVOS.....	4
2. ALCANCES	4
3. ESQUEMA LABORATORIO DE HOMOLOGACIÓN	4
4. EQUIPO HOMOLOGADO 80D	5
5. RESULTADO DE HOMOLOGACIÓN	6
5.1. Rendimiento	6
5.2. Configuración.....	7
6. Conclusiones.....	16

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 4 de 16
	15/03/2016	1.2	14/01/2016	

1. **OBJETIVOS**

- Presentar los resultados de la homologación del equipo Fortigate 80D como CPE para los servicios de Claro.
- Configuraciones estándar de equipos Fortigate 80D.


2. **ALCANCES**

En el presente documento se ven los resultados y lista de configuraciones del equipo Fortigate 80D. 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 80D			Código Documento
	Fecha de Revisión 15/03/2016	Revisión N° 1.2	Fecha de Emisión 14/01/2016	Página 5 de 16

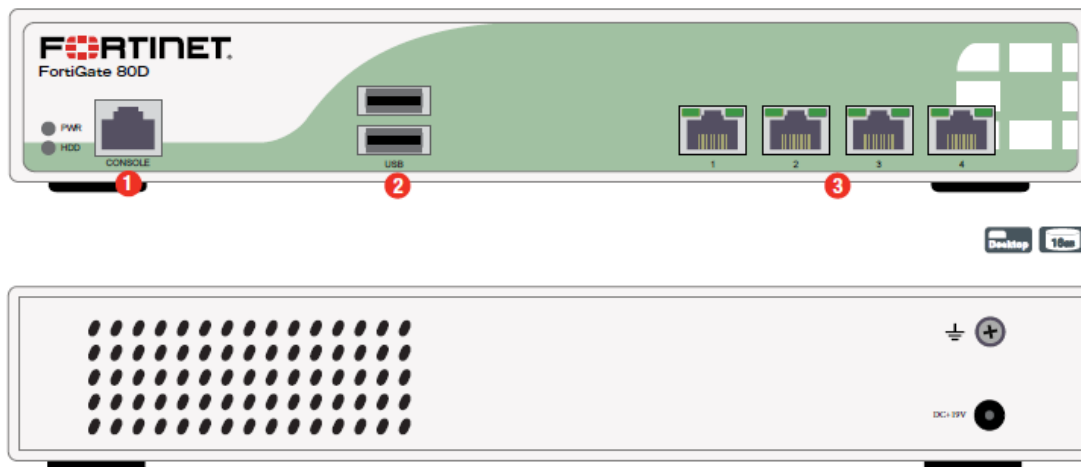
4. EQUIPO HOMOLOGADO 80D

Equipo con capacidad de 4 puertos 10/100/1000Mbps, adicionalmente posee 2 USB y conector consola estándar.

El sistema y especificaciones del equipo utilizado son:


Fortigate 80D FG080D3915001145 # get system status Version: FortiGate-80D v5.2.4,build0688,150814 (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: FG080D3915001145 Botnet DB: 1.00000(2012-05-28 22:51) BIOS version: 00010003 System Part-Number: P16202-01 Log hard disk: Available Hostname: FG080D3915001145 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 Jan 11 06:22:46 2016
--

FortiGate 80D



Interfaces

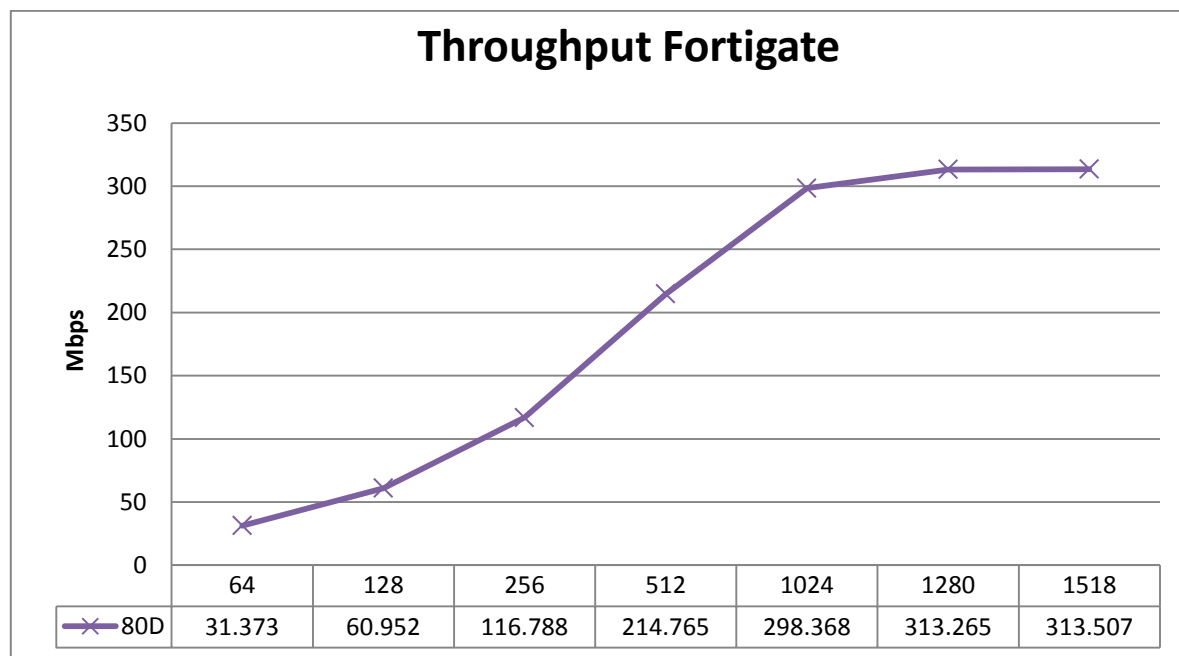
1. Console Port
2. 2x USB Ports
3. 4x GE RJ45 Ports


	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	
	15/03/2016	1.2	14/01/2016	Página 6 de 16

5. RESULTADO DE HOMOLOGACIÓN

5.1. Rendimiento


En la tabla siguiente se puede ver el rendimiento del equipo alcanzado de acuerdo al RFC 2544. Utilizando las 4 interfaces para pasar tráfico.




	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 7 de 16
	15/03/2016	1.2	14/01/2016	

5.2. Configuración


Sección	Configuración	Comentarios
Configuración de interfaz física WAN	config system interface	
	edit "port1"	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.
Configuración de interfaz loopback	next	
	end	
	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 ''	
Configuración de Interfaces VLAN	next	
	end	
	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
Configuración de IP secundaria	set interface "port1"	Se define a que puerta física está ligada.
	set vlanid 201	Se define el tag de la VLAN a utilizar
	next	
	end	
	config system interface	
	edit "port4"	
	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 Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 8 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
Configuración de VRRP – HSRP	<pre> config system interface edit "port1" set vrrp-virtual-mac enable config vrrp edit 1 set vrip 10.1.1.100 set priority 120 next end next end </pre>	
Rutas Estáticas	<pre> config router static edit 1 set dst 10.3.35.0 255.255.255.0 set gateway 10.3.30.1 set device "port4" next end </pre>	Se define la ruta.
		Se define el siguiente salto.
		Se debe definir por cual interfaz está el siguiente salto
Ruteo Dinámico BGP	<pre> config router bgp set as 64924 set router-id 10.1.1.20 </pre>	Se define el AS del equipo.
		Se define el ID con que se levanta BGP.
	<pre> config neighbor </pre>	Se definen los diferentes vecinos que va a tener el servicio.
	<pre> edit "10.1.1.1" set remote-as 64923 </pre>	Se define el AS del vecino
	<pre> set route-map-in "Filtro_IN" next end </pre>	Se define si existe algún route-map asociado al vecino.
	<pre> config network </pre>	Se definen las redes a participar del proceso BGP.
	<pre> edit 1 set prefix 10.0.33.152 255.255.255.255 next edit 2 set prefix 192.168.2.0 255.255.255.0 next end </pre>	Se define una por una las redes.
	<pre> config redistribute "connected" set status enable/disable set route-map "Filtro_OUT1" end </pre>	Si es necesario se define si se redistribuyen las redes conectadas.
	<pre> config redistribute "static" set status enable/disable set route-map "Filtro_OUT" end </pre>	Si es necesario se define si se redistribuyen las rutas estáticas.
	end	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 9 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
ACL	config router access-list edit "ACL_Filtro_IN"	Se definen ACL con Nombre, como objetos.
	config rule	
	edit 1 set action permit set wildcard 10.1.5.0 0.0.0.255 next	Se definen las redes y acciones de la regla.
	edit 2 set action deny set wildcard 10.1.5.0 0.0.0.255 next	Se definen las redes y acciones de la regla.
	edit 3 set action permit set wildcard 10.1.5.0 0.0.0.255 next	Se definen las redes y acciones de la regla.
	end next end	
Filtros Route-MAP	config router route-map	
	edit "Filtro_IN"	Se define el Nombre del route-map
	config rule	
	edit 1 set match-ip-address "ACL_Filtro_IN"	Se define qué tipo de acción tiene el route-map
	set set-aspath-action prepend	Opcional
	set set-aspath "56000 56000 56000"	Opcional
Objetos de RED	next end next end	
	config firewall address	
	edit "REDES_LAN"	Se define el Nombre del objeto de RED
	set associated-interface "port2"	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 "port3"	Se define el Nombre del objeto de RED
	set type iprange	Se define la interfaz asociada al objeto.
	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	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 10 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
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	<code>config firewall policy</code>	
	<code>edit 1</code>	Edita la primera regla.
	<code>set srcintf "port1"</code>	Se define la interfaz de origen del tráfico.
	<code>set dstintf "port2"</code>	Se define la interfaz de destino del tráfico.
	<code>set srcaddr "all"</code>	Se define las IP de origen (deben ser objetos de red asociado a la interfaz de origen) del tráfico.
	<code>set dstaddr "all"</code>	Se define las IP de destino (deben ser objetos de red asociado a la interfaz de destino) del tráfico.
	<code>set action accept</code>	Se define a la acción de la regla.
	<code>set schedule "always"</code>	
	<code>set service "ALL"</code>	Se define qué tipo de tráfico se desea aplicar (puede ser objeto de servicio).
	<code>next</code>	
DHCP Server	<code>edit 2</code>	Ejemplo de la regla reciproca a la anterior.
	<code>set srcintf "port2"</code>	
	<code>set dstintf "port1"</code>	
	<code>set srcaddr "all"</code>	
	<code>set dstaddr "all"</code>	
	<code>set action accept</code>	
	<code>set schedule "always"</code>	
	<code>set service "ALL"</code>	
	<code>next</code>	
	<code>end</code>	
	<code>config system dhcp server</code>	
	<code>edit 1</code>	Se define el servidor a utilizar
	<code>set dns-service default</code>	Se define el default Gateway que entrega el servidor.
	<code>set default-gateway 192.168.2.1</code>	
	<code>set netmask 255.255.255.0</code>	Se define la máscara de la red.
	<code>set interface "port2"</code>	Se asocia el servidor a una interfaz.
	<code>config ip-range</code>	
	<code>edit 1</code>	Se define el rango de IP del servidor
	<code>set start-ip 192.168.2.100</code>	Se define la ip de inicio del rango a entregar por el servidor.
	<code>set end-ip 192.168.2.254</code>	Se define la ip de fin del rango a entregar por el servidor.
	<code>next</code>	
	<code>end</code>	
	<code>next</code>	
	<code>end</code>	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 11 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
NAT	config firewall ippool	Se define un objeto de pool ip para el NAT.
	edit "Nat_Lan"	
	set startip 200.29.174.74	Se define el inicio del rango de IP para el NAT.
	set endip 200.29.174.74	Se define el fin del rango de IP para el NAT.
	set type overload	Se define de tipo Overload (PAT)
	next	
	end	
	config firewall policy	Se asocia el NAT a una política de acceso.
	edit 4	
	set name "Lan2Internet"	Se define el nombre de la regla
	set srcintf "lan" set dstintf "Wan_Internet" set srcaddr "PC_jonathan" set dstaddr "all" set action accept set schedule "always" set service "ALL"	Se configure los mismos parámetros de la regla simple de acceso
	set nat enable	Se habilita el NAT en la regla.
	set ippool enable	Se define que se utilizara una IP diferente a la de la interfaz.
	set poolname "Nat_Lan"	Se define el objeto asociado a la IP a utilizar el NAT.
	next	
	end	
	config firewall policy	Si se quiere utilizar la IP de la interfaz como NAT.
	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	Solo se debe habilitar el NAT en la política y tomara la IP de la interfaz por defecto.
	next	
	end	

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 12 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
Configuración de los servidores de radius.	<code>config user radius</code>	
	<code>edit "Radius"</code>	Se define un nombre para identificar los servidores.
	<code>set server "200.27.95.3"</code>	Se define el servidor primario.
	<code>set secret telmex_secret</code>	Se define la clave del servidor.
	<code>set nas-ip 10.156.33.152</code>	
	<code>set auth-type pap</code>	
	<code>set source-ip 10.156.33.152</code>	
	<code>set secondary-server "200.27.193.131"</code> <code>set secondary-secret telmex_secret</code>	
Configuración de los esquemas de autenticación.	<code>next</code> <code>end</code>	
	<code>config user group</code>	Se define un grupo y se asocia al grupo de servidores antes configurado
	<code>edit "Remote Radius"</code>	
	<code>set group-type firewall</code> <code>set member "Radius"</code>	
	<code>next</code> <code>end</code>	
Configuración de perfiles de acceso	<code>config system accprofile</code> <code>edit "monitor"</code> <code>set scope vdom</code> <code>set comments ''</code> <code>set mntgrp read</code> <code>set admingrp read</code> <code>set updategrp read</code> <code>set authgrp read</code> <code>set sysgrp read</code> <code>set netgrp read</code> <code>set loggrp read</code> <code>set routegrp read</code> <code>set fwgrp read</code> <code>set vpngrp read</code> <code>set utmgrp read</code> <code>set endpoint-control-grp read</code> <code>set wifi read</code> <code>next</code>	Se define el perfil de Monitoreo, todos los accesos solo en modo read.
	<code>edit "noaccess"</code> <code>set scope vdom</code> <code>set comments ''</code> <code>set mntgrp none</code> <code>set admingrp none</code> <code>set updategrp none</code> <code>set authgrp none</code> <code>set sysgrp none</code> <code>set netgrp none</code> <code>set loggrp none</code> <code>set routegrp none</code> <code>set fwgrp none</code> <code>set vpngrp none</code> <code>set utmgrp none</code> <code>set endpoint-control-grp none</code> <code>set wifi none</code> <code>next</code> <code>end</code>	Se define el perfil de NoAccess, para la configuración de radius, todos quedan en "none".

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 13 de 16
	15/03/2016	1.2	14/01/2016	


Sección	Configuración	Comentarios
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" </pre>	Se asocia a la vdom native.
	<pre> set wildcard enable </pre>	Se define tipo wildcard para que todos puedan ingresar.
	<pre> set remote-group "Remote_Radius" </pre>	Se asocia al grupo de Radius.
	<pre> set accprofile-override enable </pre>	Se autoriza que tome el perfil desde el ACS.
	<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 </pre>	Se define un usuario Local, con perfil de administrador, para en caso de que la conexión al servidor de Radius este abajo.
	<pre> next </pre>	
	<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 </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> next end </pre>	
Configuración de rutas estáticas a los servidores	<pre> config router static edit 3 set dst 200.27.95.0 255.255.255.240 set gateway 10.3.30.1 set device "port4" next edit 4 set dst 200.27.193.128 255.255.255.240 set gateway 10.3.30.1 set device "port4" next end </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 Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 14 de 16
	15/03/2016	1.2	14/01/2016	

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

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión N°	Fecha de Emisión	Página 15 de 16
	15/03/2016	1.2	14/01/2016	

Sección	Configuración	Comentarios
NetFlow	<code>config system netflow</code>	
	<code>set collector-ip 190.208.24.144</code>	Se define el servidor remoto del NETFLOW
	<code>set collector-port 9996</code>	Se define el puerto de comunicación.
	<code>set source-ip 10.156.33.152</code>	Se define la ip de origen.
	<code>end</code>	
	<code>config system interface</code>	
	<code>edit "lan"</code> <code>set netflow-sampler both</code> <code>next</code>	Se debe habilitar en cada puerta la necesidad de capturar el tráfico.
	<code>edit "Wan_Datos"</code> <code>set netflow-sampler both</code> <code>next</code>	
	<code>edit "Wan_Internet"</code> <code>set netflow-sampler both</code> <code>next</code>	
	<code>End</code>	
QoS	<code>config firewall shaper traffic-shaper</code> <code>edit Telefonía</code> <code>set guaranteed-bandwidth 10000</code> <code>set maximum-bandwidth 10000</code> <code>set diffserv enable</code> <code>set diffservcode 101110</code> <code>next</code> <code>edit Video</code> <code>set maximum-bandwidth 60000</code> <code>set diffserv enable</code> <code>set diffservcode 010010</code> <code>set priority medium</code> <code>next</code> <code>edit Datos</code> <code>set maximum-bandwidth 30000</code> <code>set diffserv enable</code> <code>set diffservcode 000000</code> <code>set priority low</code> <code>next</code> <code>end</code>	Se deben definir los objetos que definen el BW de acuerdo al tipo de trafico. En cada objeto se debe identificar que marca de QoS se debe aplicar.
	<code>config firewall policy</code> <code>edit 2</code> <code>set uuid 69a78358-cff7-51e5-90ba-77a9ae3fbb74</code> <code>set srcintf "port1"</code> <code>set dstintf "wan1"</code> <code>set srcaddr "all"</code> <code>set dstaddr "all"</code> <code>set action accept</code> <code>set schedule "always"</code> <code>set service "ALL"</code> <code>set traffic-shaper "Telefonía"</code> <code>next</code> <code>end</code>	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.

	Depto. Soporte Especializado/ Gerencia Corporativa Mercado Empresarial Guía de Homologación Equipo Fortigate 80D			Código Documento
	Fecha de Revisión	Revisión Nº	Fecha de Emisión	Página 16 de 16
	15/03/2016	1.2	14/01/2016	

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 posee vrf-lite.
 - 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 **100 Mbps**.
 - o Si bien el equipo posee un mayor ancho de banda, cercano a 300 Mbps, la curva es demasiado pronunciada para paquetes pequeños, por lo que un valor adecuado de operación viene dado por paquetes de 256 bytes.
- 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 trafico 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.**