CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 19 DE FEBRERO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178591	1	Tunja	CARRERA 2ª ESTE NO.53-70	50 Mbps	168.90.15.184/29 2800:490:4001:3a00::/56	168.90.15.185 2800:490:4001:3a00::1	168.90.15.186-168.90.15.190	Gi0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interface del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE-CORPOBOYACA_ID1# show running-config interface gigabitEthernet 0/1
Building configuration...

Current configuration : 364 bytes
!
interface GigabitEthernet0/1
 description ###To_Lan####
 ip address 168.90.15.185 255.255.255.248
 rate-limit input 52424000 9830400 19660800 conform-action transmit exceed-action drop
 rate-limit output 52424000 9830400 19660800 conform-action transmit exceed-action drop
 duplex auto
 speed auto
 media-type rj45
 ipv6 address 2800:490:4001:3A00::1/56
 !
end

CCE-CORPOBOYACA_ID1#
```

```
CCE-CORPOBOYACA_ID1#ping 8.8.8.8 source gigabitEthernet 0/1 repeat 1000 size 1448

Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 168.90.15.185
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/3/12 ms
CCE-CORPOBOYACA_ID1#
```

```
CCE-CORPOBOYACA_ID1#ping 2001:4860:4860::8888 source 2800:490:4001:3a00::1 rep
CCE-CORPOBOYACA_ID1#ping 2001:4860:4860::8888 source 2800:490:4001:3a00::1 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
Packet sent with a source address of 2800:490:4001:3A00::1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 0/3/12 ms
CCE-CORPOBOYACA_ID1#
```

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 3825	FTX1033A0BU	CARRERA 2ª ESTE NO.53-70

MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD: TUNJA	FECHA: 05-03-21	HORA INICIAL: 14:00	HORA FINAL: 14:40
CLIENTE: COORPORACION AUTONOMA BY		SUBCLIENTE: N/A	
TICKET ACTIVIDAD: OT 179848		DIRECCION: CRA 2A 53-70	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

☐ SOPORTE	☐ ASEGURAMIENTO	☐ NODOS INALAMBRICOS
☒ APROVISIONAMIENTO	☐ PROYECTOS INALAMBRICOS	☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

→ Visita tecnica para instalación de equipo UTM, por solicitud del área de PEM.

REPORTE TECNICO: → se realiza visita y se entrega equipo al Ing Alfredo se entrega UTM S/N COA100XT47H9X9B con cable de poder. El cliente no lo deja conectado debido a que tiene instalado 2 equipos UTM. y estos tienen filtrado.

→ Se confirma entrega con él cliente y retiro de la sede.

→ se deja instalada a la sede 8 licencias de cada uno de los equipos asignados para el proyecto.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	X	EN PROCESO		PENDIENTE		OTRA	

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nombre: Alfredo Ojuela	Nombre: Angelica Fonseca
C.C.: 7.171.355	C.C.: 1049640115
N° TELEFONICO: 310 559 6352	N° TELEFONICO: 320 6886987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 19 DE FEBRERO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Direccionamiento IP WAN: 181.225.70.237/31
Direccionamiento IP LAN: 192.168.12.1/24
Acceso al equipo: https://181.225.70.237:4445
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178592	2	Tunja	Carrera 6 NO. 55A-33, piso 3,barrio Santa Rita-Norte	20Mbps	181.225.70.236/31	181.225.70.237	181.225.70.238	Fa0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interface del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE-CORPOBOYACA_ID2# show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 301 bytes
!
interface FastEthernet0/1
 description ###To_Lan####
 ip address 181.225.70.236 255.255.255.254
 rate-limit input 20968000 3932160 7864320 conform-action transmit exceed-action drop
 rate-limit output 20968000 3932160 7864320 conform-action transmit exceed-action drop
 duplex auto
 speed auto
end

CCE-CORPOBOYACA_ID2#
```

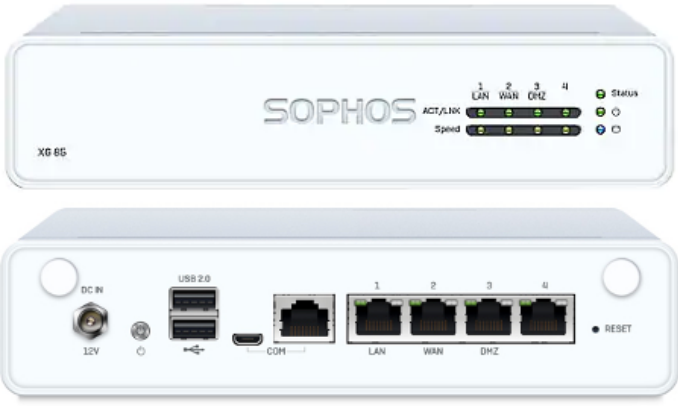
```
CCE-CORPOBOYACA_ID2#ping 8.8.8.8 source 181.225.70.236 repeat 1000 size 1448

Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 181.225.70.236
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/4/8 ms
CCE-CORPOBOYACA_ID2#
```

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

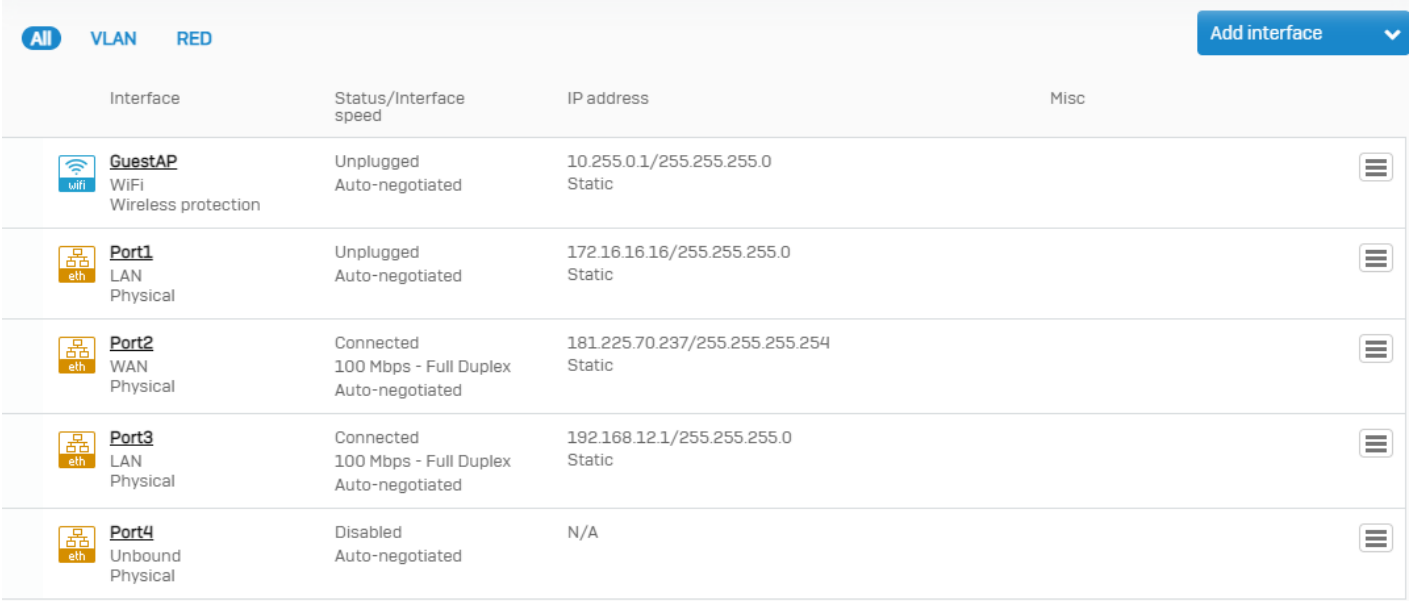
Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 1841	FHK133773C6	Edificion del Fondo Nacional del Ahorro: Carrera 6 NO. 55ª-33, piso 3,barrio Santa Rita-Norte
1	Sophos XG XG86	C0A100R6MB6WVF2	Edificion del Fondo Nacional del Ahorro: Carrera 6 NO. 55ª-33, piso 3,barrio Santa Rita-Norte



DETALLES DE LA CONFIGURACIÓN

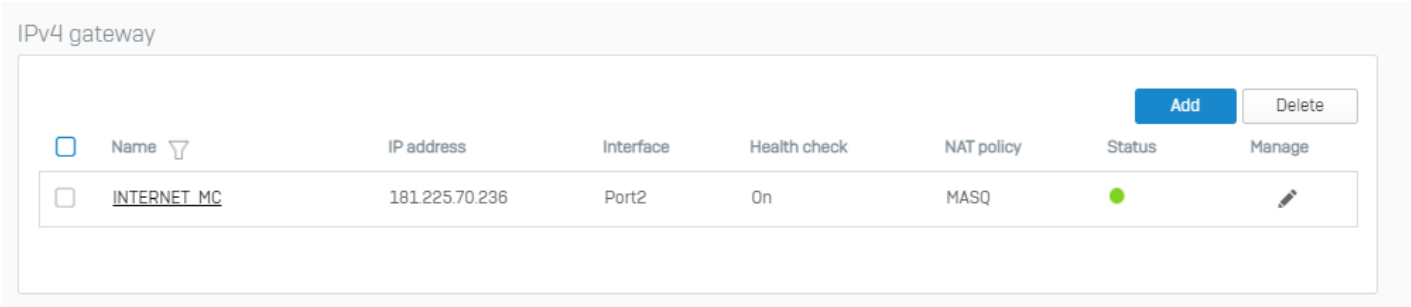
DIRECCIONAMIENTO IP E INTERFACES

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



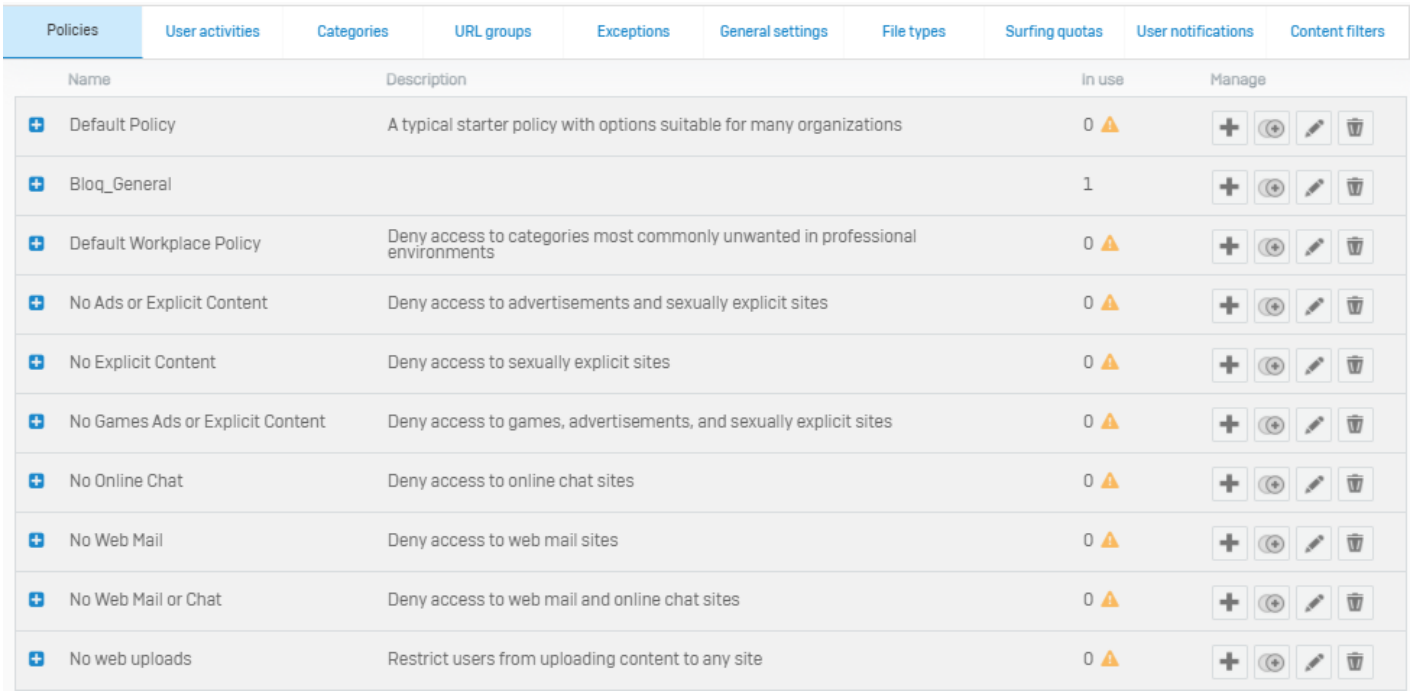
ENRUTAMIENTO

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



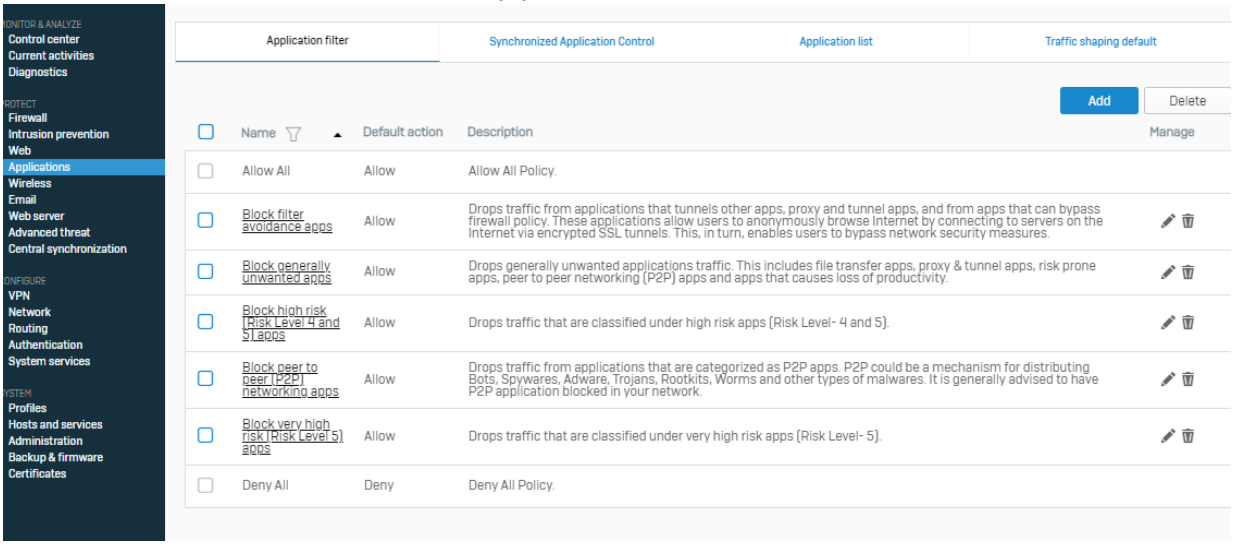
- **FILTRO WEB**

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet.



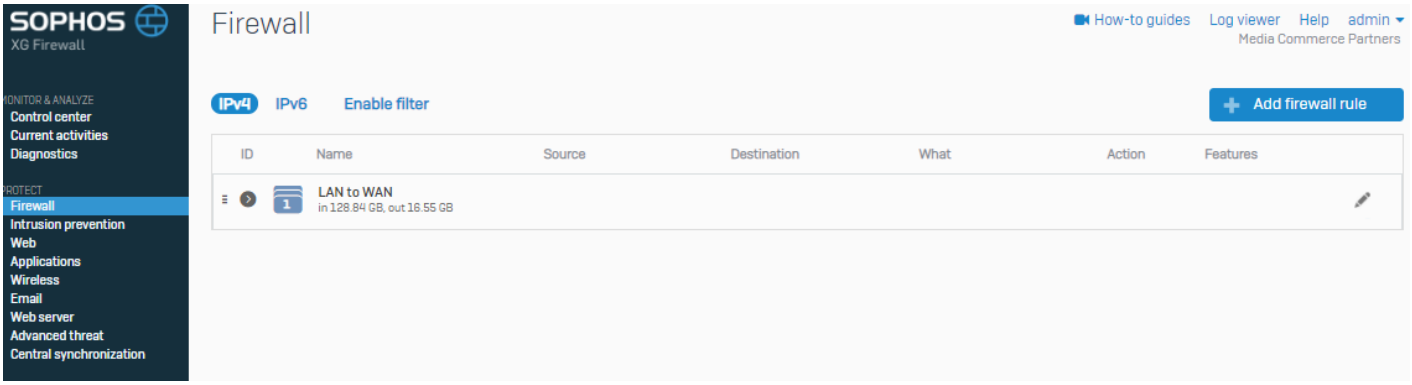
- **CONTROL DE APLICACIONES**

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



- **POLÍTICAS DE FIREWALL**

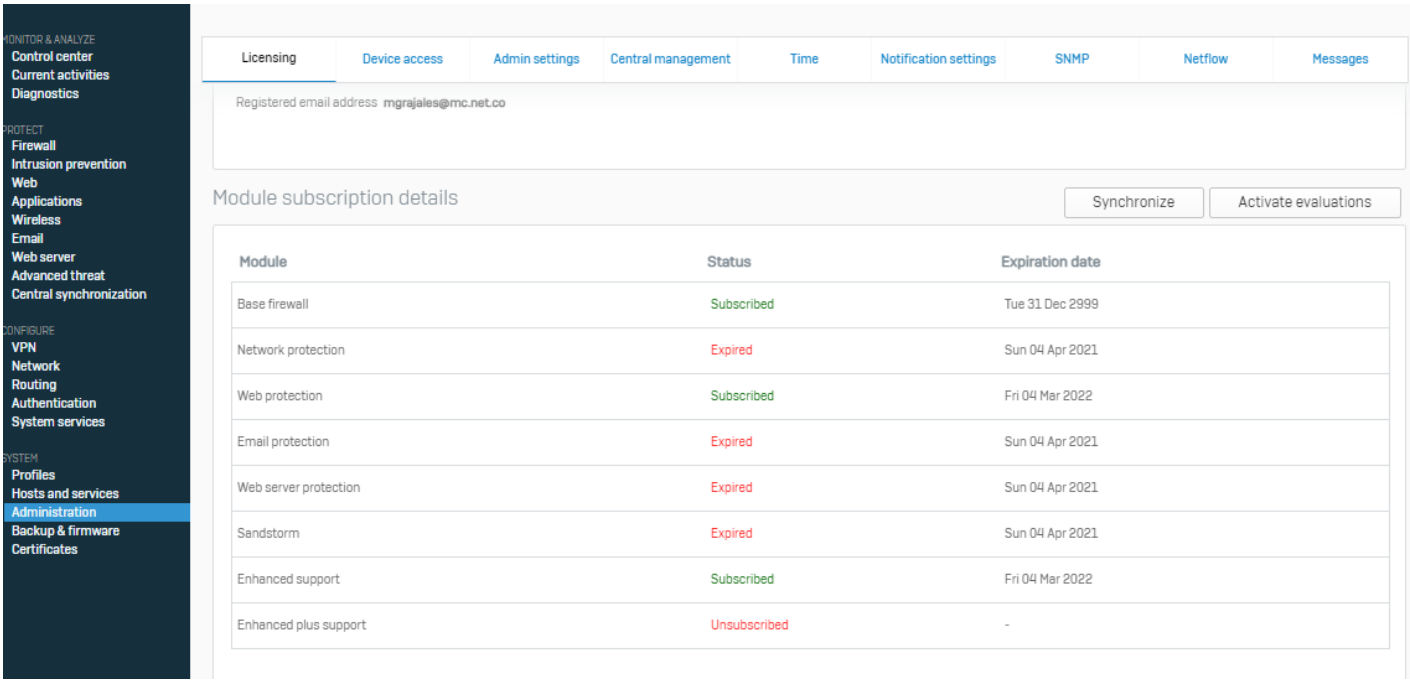
A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



- **LICENCIA**

Serial Number	Registered	Model
C0A100R6MB6WVF2	04 March 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate
Network Protection	Expired	Network Protection	04 Apr 2021	
Web Protection	Subscribed	L0012055845 / Web Protection	04 Mar 2022	
Email Protection	Expired	Email Protection	04 Apr 2021	
Web Server Protection	Expired	Webserver Protection	04 Apr 2021	
Zero-Day Protection	Expired	Zero-Day Protection	04 Apr 2021	
Enhanced Support	Subscribed	L0012055844 / Enhanced Support	04 Mar 2022	
Enhanced Plus Support Upgrade				


MONITOR & ANALYZE
Control center
Current activities
Diagnostics
PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization
CONFIGURE
VPN
Network
Routing
Authentication
System services
SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates
Licensing
Device access
Admin settings
Central management
Time
Notification settings
SNMP
Netflow
Messages
Registered email address mgrajales@mc.net.co
Module subscription details
Synchronize
Activate evaluations
Module
Status
Expiration date
Base firewall
Subscribed
Tue 31 Dec 2999
Network protection
Expired
Sun 04 Apr 2021
Web protection
Subscribed
Fri 04 Mar 2022
Email protection
Expired
Sun 04 Apr 2021
Web server protection
Expired
Sun 04 Apr 2021
Sandstorm
Expired
Sun 04 Apr 2021
Enhanced support
Subscribed
Fri 04 Mar 2022
Enhanced plus support
Unsubscribed
-

POLÍTICA DE SEGURIDAD

El equipo está actualmente configurado para la protección IPS contra todo tipo de amenazas externas, principalmente el ransomware, este malware encripta documentos, archivos personales, críticos y solicita transferir a otros fondos, dinero pero en moneda BitCoin para que la víctima desbloquee sus archivos. El comportamiento similar a un gusano exhibido por este malware se debe a una sonda activa para el puerto 445 (***ya bloqueado en su UTM***) del servidor SMBv1 en la LAN local que busca la presencia de Backdoor.Double.Pulsar. Si la puerta trasera está presente, la carga útil se entrega y se ejecuta a través de este canal. De lo contrario, se toma una ruta de explotación ligeramente menos confiable.

Por lo anterior es importante señalar que esta solucion de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría “Malware Communication”
2. El motor AV habilitado nos ayuda a detectar el malware junto con las variantes
3. El filtro web se habilitó a todos los usuarios sin excepción para bloquear los sitios web que se han identificado como atacantes potenciales
    - Anonymizers
    - Command & Control
    - Phishing & Fraud
    - Spam URLs

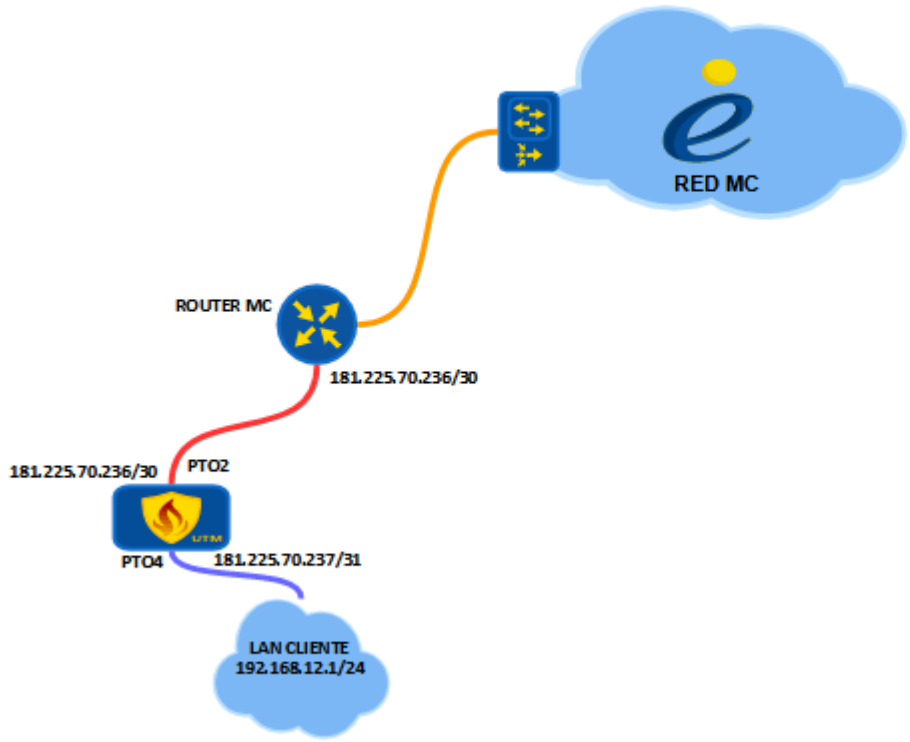
4. Con el control de aplicaciones estamos bloqueando igualmente para todos los usuarios el software Proxy and Tunnel principalmente para cortar cualquier tipo de gestión para la red TOR que es el protocolo de comunicación de los ataques ransomware.

de igual forma ninguna solución es 100% segura y solo estamos protegiendo el perímetro, no tenemos control sobre los dispositivos de almacenamiento que ingresen los usuarios en su computadora, por esto recomendamos en lo posible contar con una buena plataforma de antivirus y software adicionales que permitan controlar estos ataques que están en constante cambio. Si desea asesoría sobre cómo obtener protección adicional para su red LAN con un excelente antivirus o software adicional que le garantice no tener inconvenientes con el secuestro de datos importantes para su compañía puede consultar a nuestro asesor comercial.

Con el usuario y contraseña que le hemos entregado para la administración del equipo puede observar todas las políticas anteriormente mencionadas, le solicitamos por favor validar que la información registrada en este documento sea copia exacta de la configuración entregada en el UTM, si nota alguna anomalía por favor reportarse de inmediato.

ESQUEMA DE SOLUCIÓN, TOPOLOGÍA

Topología CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD: TUNJA	FECHA: 05-03-21	HORA INICIAL: 16:10	HORA FINAL: 16:40
CLIENTE: CORPORACION AUTONOMA D BY		SUBCLIENTE: N/A	
TICKET ACTIVIDAD: OT 179850		DIRECCION: CRA 6 # 65A-33 piso 3.	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

- ☐ SOPORTE
- ☐ ASEGURAMIENTO
- ☐ NODOS INALAMBRICOS
- ☒ APROVISIONAMIENTO
- ☐ PROYECTOS INALAMBRICOS
- ☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

→ Se realiza visita técnica para instalación de UTM solicitud area PEM.

REPORTE TECNICO:

→ Se realiza visita, se instala equipo UTM Sophos XG 86 serial COA100R6MB6WVF2, se valida gestión y servicio con cliente e Ing Herman Cano.

→ Se confirma servicio operativo con cliente. e Ing Herman.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	X	EN PROCESO		PENDIENTE		OTRA	

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nombre:	Nombre: Angelica Fonseca
C.C.: 7.171.355	C.C.: 1049640115
N° TELEFONICO: 3105596362	N° TELEFONICO: 320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 19 DE FEBRERO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Direccionamiento IP WAN: 190.121.140.105/31
Direccionamiento IP LAN: 192.168.10.1/24
Acceso al equipo: https://190.121.140.105:4445
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178593	3	Tunja	Carrera 3 NO.57-45, 2 piso, barrio santa ana	10Mbps	190.121.140.104/31	190.121.140.104	190.121.140.105	Fa0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interfaz del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE-CORPOBOYACA_ID3#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 300 bytes
!
interface FastEthernet0/1
 description ###To_Lan####
 ip address 190.121.140.104 255.255.255.0
 rate-limit input 10480000 1966080 3932160 conform-action transmit exceed-action drop
 rate-limit output 10480000 1966080 3932160 conform-action transmit exceed-action drop
 duplex auto
 speed auto
end

CCE-CORPOBOYACA_ID3#
```

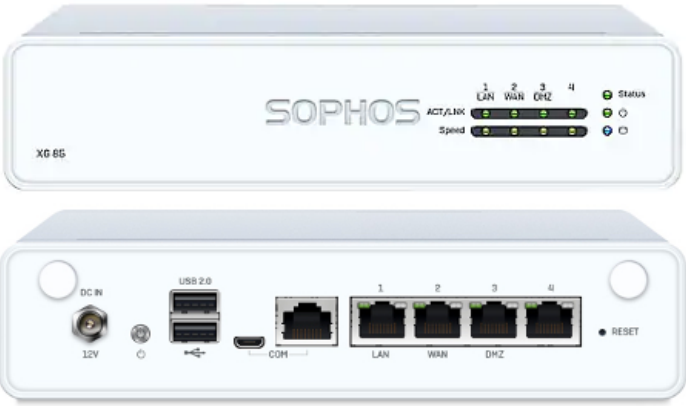
```
CCE-CORPOBOYACA_ID3#ping 8.8.8.8 source fastEthernet 0/1  repeat 1000 size 1448

Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 190.121.140.104
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/4/8 ms
CCE-CORPOBOYACA_ID3#
```

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

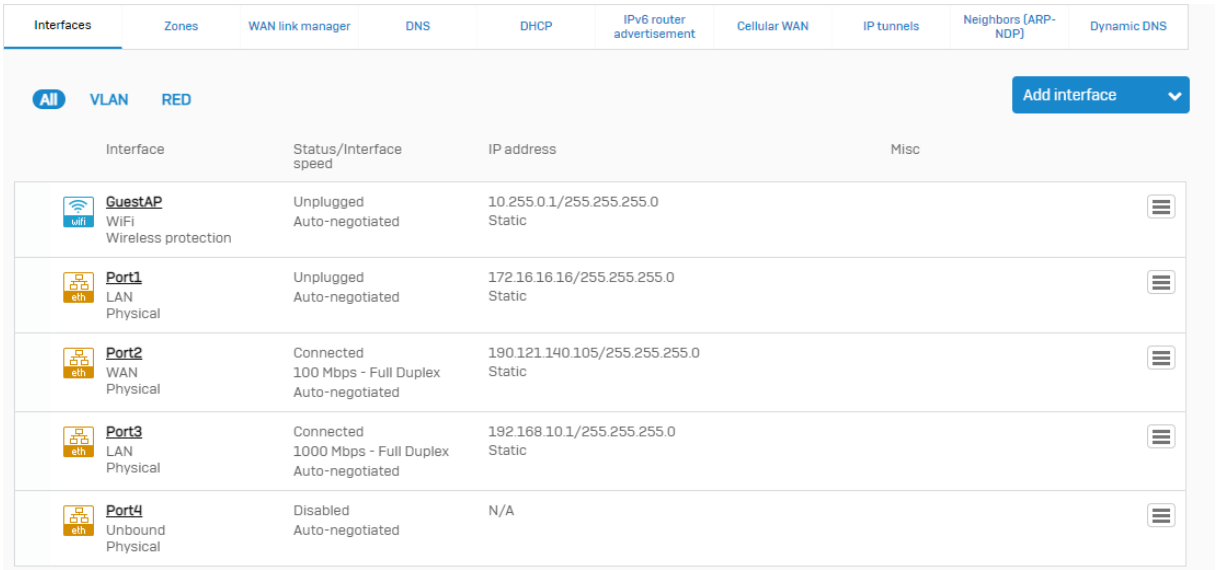
Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 1841	FTX1222Y25X	CARRERA 3 NO.57-45, 2 PISO, BARRIO SANTA ANA - SEDE CENTRO DOCUMENTAL
1	Sophos XG XG86	C0A100VPFG2P32E	CARRERA 3 NO.57-45, 2 PISO, BARRIO SANTA ANA - SEDE CENTRO DOCUMENTAL



DETALLES DE LA CONFIGURACIÓN

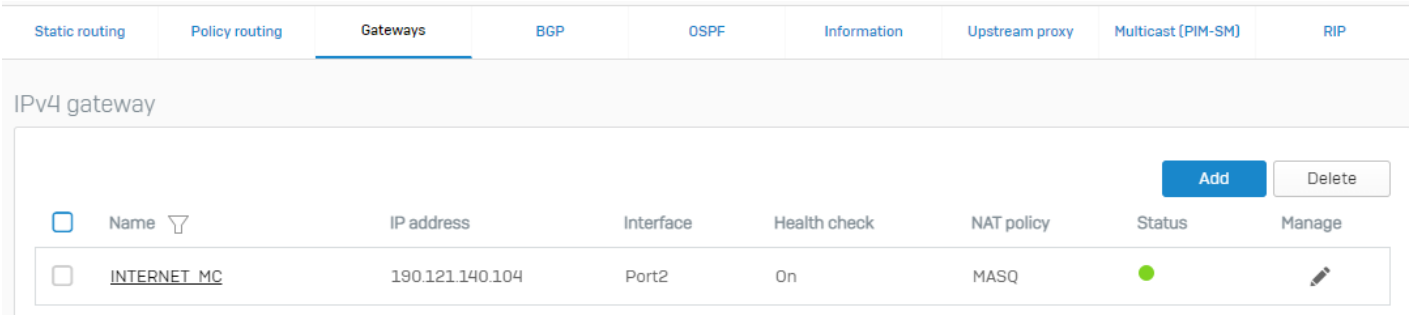
DIRECCIONAMIENTO IP E INTERFACES

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



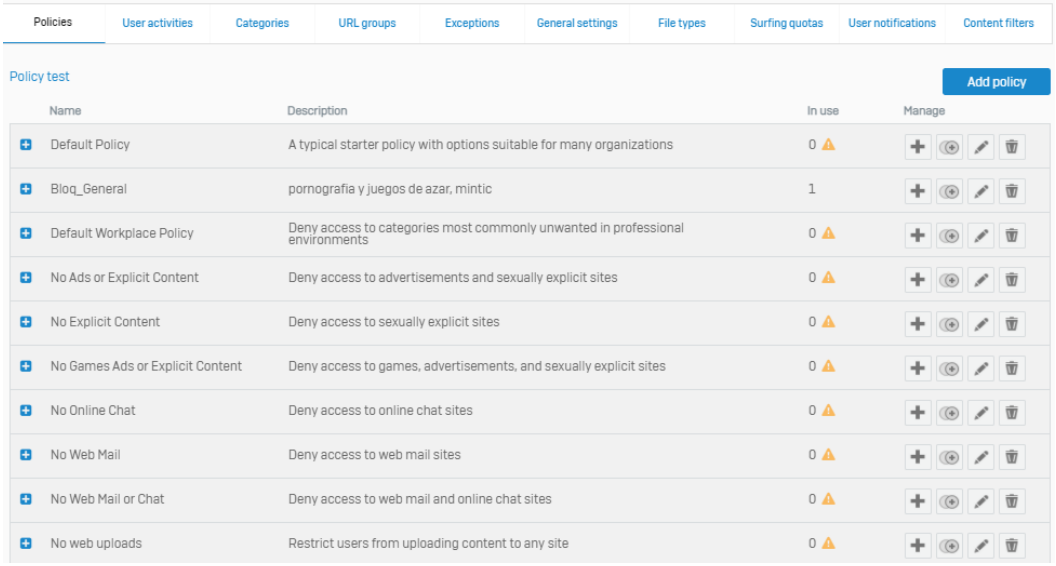
ENRUTAMIENTO

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



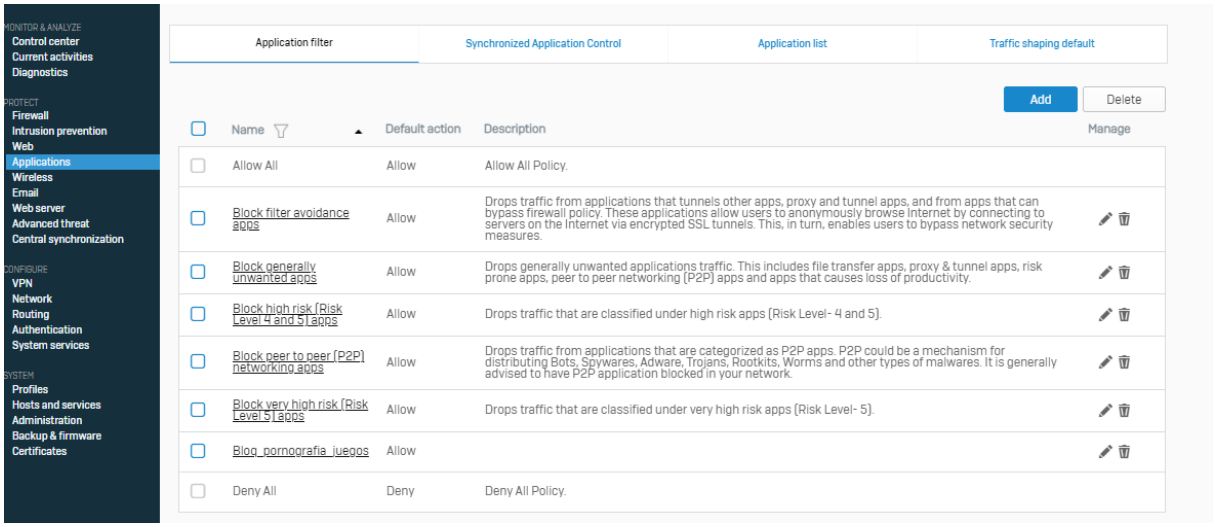
FILTRO WEB

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet**.**



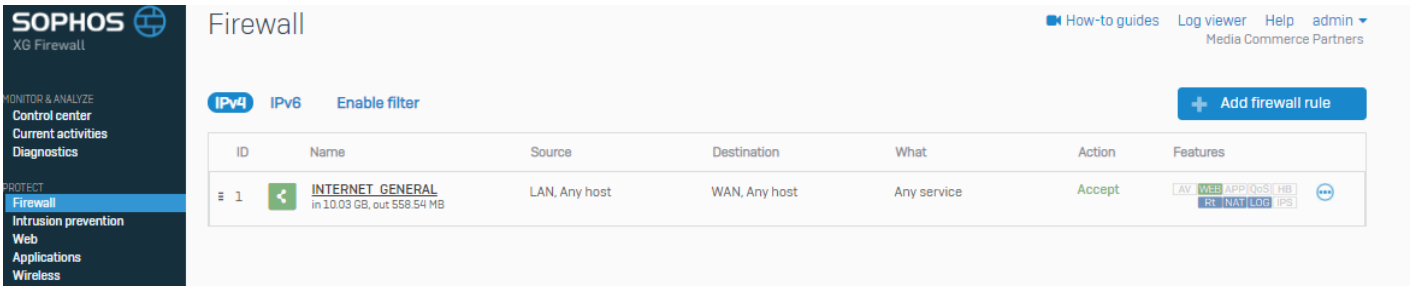
CONTROL DE APLICACIONES

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



POLÍTICAS DE FIREWALL

A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



LICENCIA

Serial Number	Registered	Model
C0A100VPFG2P32E	04 March 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate
Network Protection	Expired	Network Protection	04 Apr 2021	
Web Protection	Subscribed	L0012055762 / Web Protection	04 Mar 2022	
Email Protection	Expired	Email Protection	04 Apr 2021	
Web Server Protection	Expired	Webserver Protection	04 Apr 2021	
Zero-Day Protection	Expired	Zero-Day Protection	04 Apr 2021	
Enhanced Support	Subscribed	L0012055759 / Enhanced Support	04 Mar 2022	
Enhanced Plus Support Upgrade				

Module subscription details

Synchronize | Activate evaluations

Module	Status	Expiration date
Base firewall	Subscribed	Tue 31 Dec 2999
Network protection	Expired	Sun 04 Apr 2021
Web protection	Subscribed	Fri 04 Mar 2022
Email protection	Expired	Sun 04 Apr 2021
Web server protection	Expired	Sun 04 Apr 2021
Sandstorm	Expired	Sun 04 Apr 2021
Enhanced support	Subscribed	Fri 04 Mar 2022
Enhanced plus support	Unsubscribed	-

POLÍTICA DE SEGURIDAD

El equipo está actualmente configurado para la protección IPS contra todo tipo de amenazas externas, principalmente el ransomware, este malware encripta documentos, archivos personales, críticos y solicita transferir a otros fondos, dinero pero en moneda BitCoin para que la víctima desbloquee sus archivos. El comportamiento similar a un gusano exhibido por este malware se debe a una sonda activa para el puerto 445 (***ya bloqueado en su UTM***) del servidor SMBv1 en la LAN local que busca la presencia de Backdoor.Double.Pulsar. Si la puerta trasera está presente, la carga útil se entrega y se ejecuta a través de este canal. De lo contrario, se toma una ruta de explotación ligeramente menos confiable.

Por lo anterior es importante señalar que esta solucion de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría “Malware Communication”
2. El motor AV habilitado nos ayuda a detectar el malware junto con las variantes
3. El filtro web se habilitó a todos los usuarios sin excepción para bloquear los sitios web que se han identificado como atacantes potenciales
    - Anonymizers
    - Command & Control
    - Phishing & Fraud
    - Spam URLs

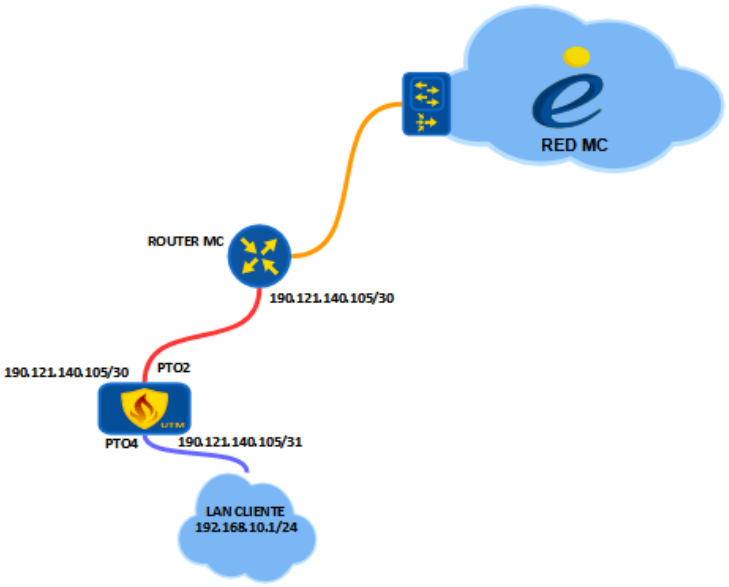
4. Con el control de aplicaciones estamos bloqueando igualmente para todos los usuarios el software Proxy and Tunnel principalmente para cortar cualquier tipo de gestión para la red TOR que es el protocolo de comunicación de los ataques ransomware.

de igual forma ninguna solución es 100% segura y solo estamos protegiendo el perímetro, no tenemos control sobre los dispositivos de almacenamiento que ingresen los usuarios en su computadora, por esto recomendamos en lo posible contar con una buena plataforma de antivirus y software adicionales que permitan controlar estos ataques que están en constante cambio. Si desea asesoría sobre cómo obtener protección adicional para su red LAN con un excelente antivirus o software adicional que le garantice no tener inconvenientes con el secuestro de datos importantes para su compañía puede consultar a nuestro asesor comercial.

Con el usuario y contraseña que le hemos entregado para la administración del equipo puede observar todas las políticas anteriormente mencionadas, le solicitamos por favor validar que la información registrada en este documento sea copia exacta de la configuración entregada en el UTM, si nota alguna anomalía por favor reportarse de inmediato.

ESQUEMA DE SOLUCIÓN, TOPOLOGÍA

Topología CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ ID_16



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD:	TUNJA	FECHA: 05-03-21	HORA INICIAL:	15:10	HORA FINAL: 15:50 .
CLIENTE:	CORPORACION AUTONOMA D		SUBCLIENTE:	N/A	
TICKET ACTIVIDAD:	OT 179852		DIRECCION:	CRA 3 # 67-45 piso 2.	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

☐ SOPORTE	☐ ASEGURAMIENTO	☐ NODOS INALAMBRICOS
☒ APROVISIONAMIENTO	☐ PROYECTOS INALAMBRICOS	☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

Visita tecnica para instalacion de equipo por solicitud del area de PEM..

REPORTE TECNICO:

- Se realiza visita tecnica, se instala equipo UTM Sophos XG 86 SN C0A100UPFG2P82E. Se valida gestión y servicio, con el cliente conectando el PC directamente al UTM.
- Se confirma servicio operativo con cliente y con Ing Hernan.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	X	EN PROCESO		PENDIENTE		OTRA	

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE		FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S	
Nombre:	Alfredo Ojuela Peña	Nombre:	Angelica Fonseca
C.C.:	7'171.355	C.C.:	1049640115
N° TELEFONICO:	310 559 6302	N° TELEFONICO:	320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 23 DE FEBRERO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet 20 Mbps

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Direccionamiento IP WAN: 190.121.140.135/31
Direccionamiento IP LAN: 192.168.216.381/24
Acceso al equipo: https://190.121.140.135:4445
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178746	6	SOCHA	CARRERA 10 NO. 3-57 - SOCHA (BOYACÁ)	20 Mbps	190.121.140.134/31	192.168.100.1/24	Se realiza nat.	Fa0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interface del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE-CORPOBOYACA_ID6#show run int fa0/1
Building configuration...

Current configuration : 367 bytes
!
interface FastEthernet0/1
 description ###To_Lan####
 ip address 190.121.140.134 255.255.255.254
 ip virtual-reassembly in
 rate-limit input 20968000 3932160 7864320 conform-action transmit exceed-action drop
 rate-limit output 20968000 3932160 7864320 conform-action transmit exceed-action drop
 duplex auto
 speed auto
 ipv6 address 2800:490:4000:6C00::1/56
end

CCE-CORPOBOYACA_ID6#
```

```
CCE-CORPOBOYACA_ID6#ping 8.8.8.8 source fastEthernet 0/1 rep 1000 size 1448
Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 190.121.140.134
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 24/35/184 ms
CCE-CORPOBOYACA_ID6#
```

Equipos instalados

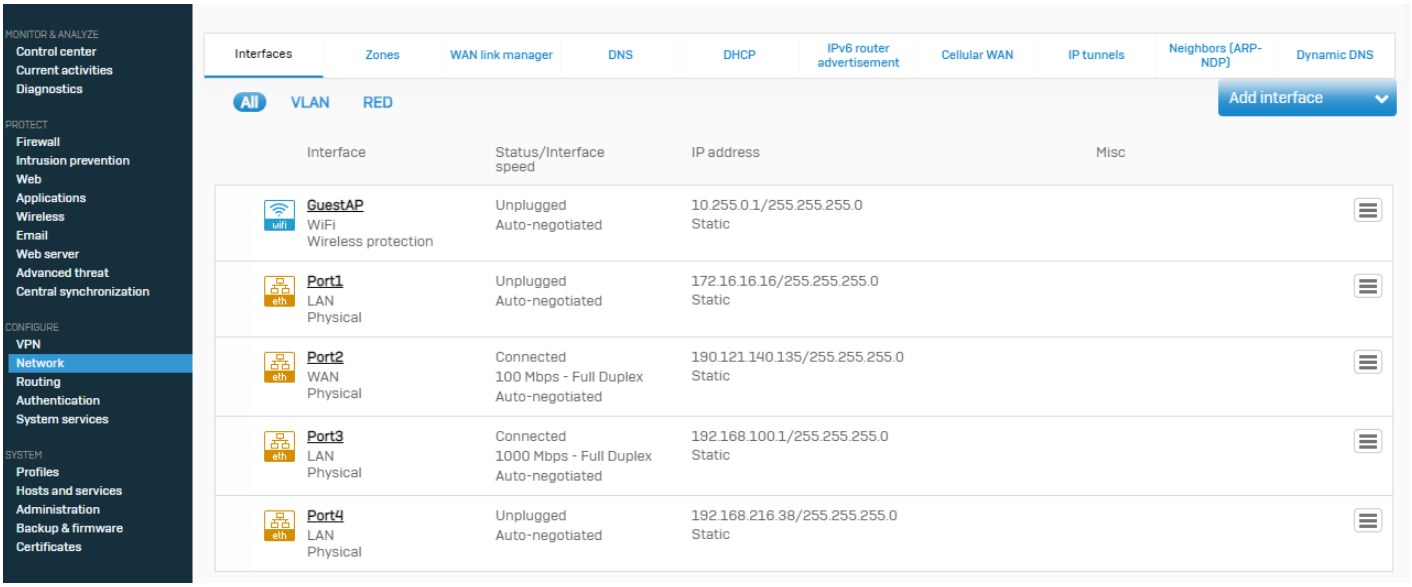
Se relacionan los equipos adecuados para la prestación de los servicios

Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 1841	FCZ10291269	Carrera 10 NO. 3-57 - Socha (Boyacá)
1	Sophos XG86	C0A100XFTBXXXC5	Carrera 10 NO. 3-57 - Socha (Boyacá)

DETALLES DE LA CONFIGURACIÓN

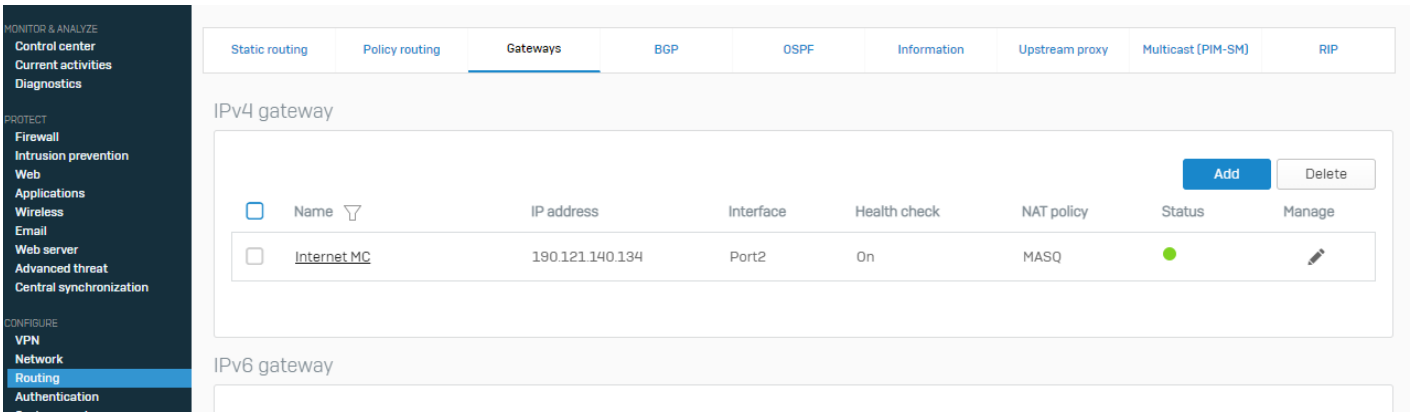
- **DIRECCIONAMIENTO IP E INTERFACES**

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



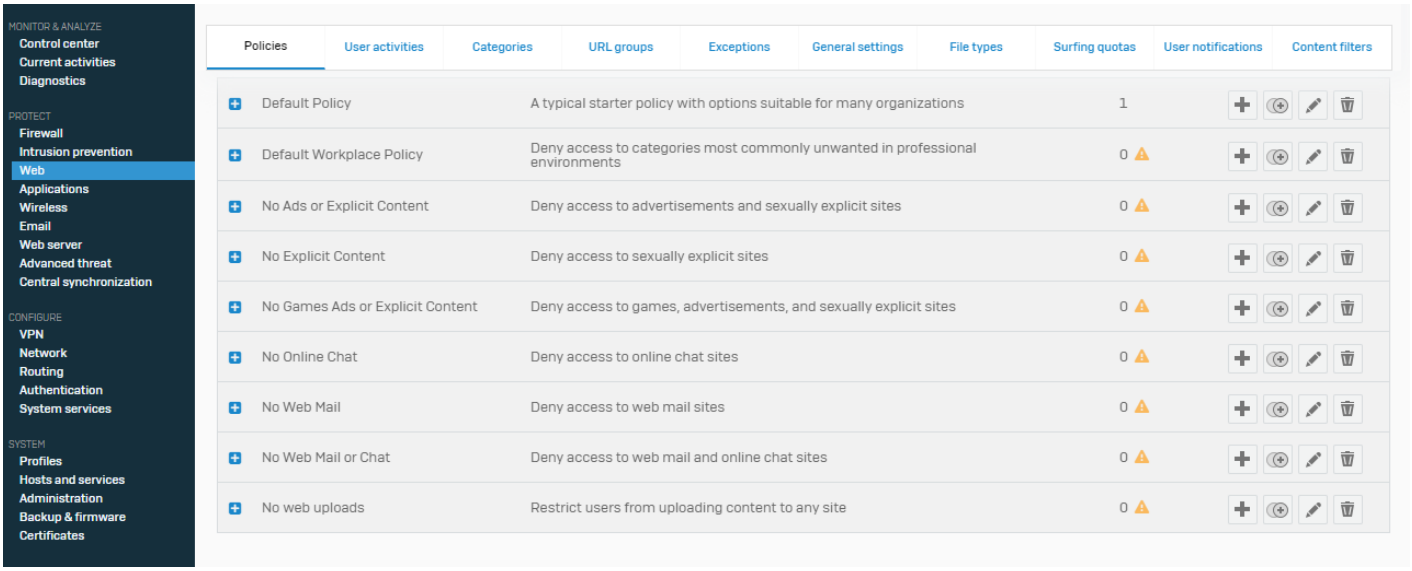
- **ENRUTAMIENTO**

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



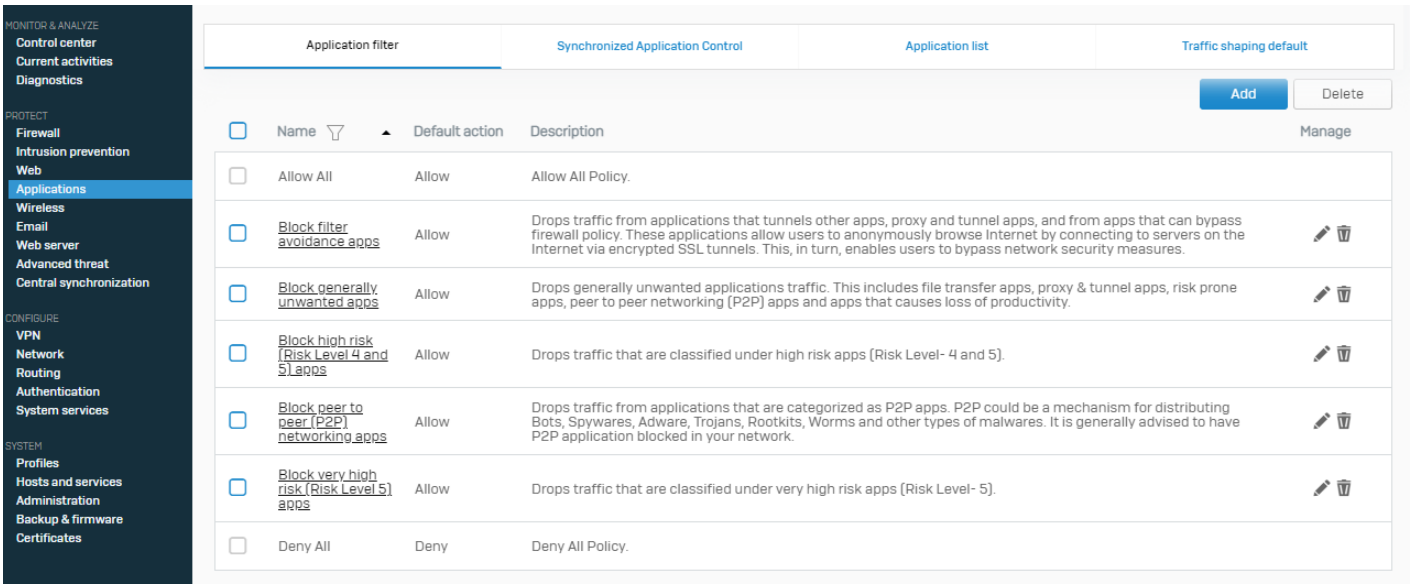
- **FILTRO WEB**

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet.



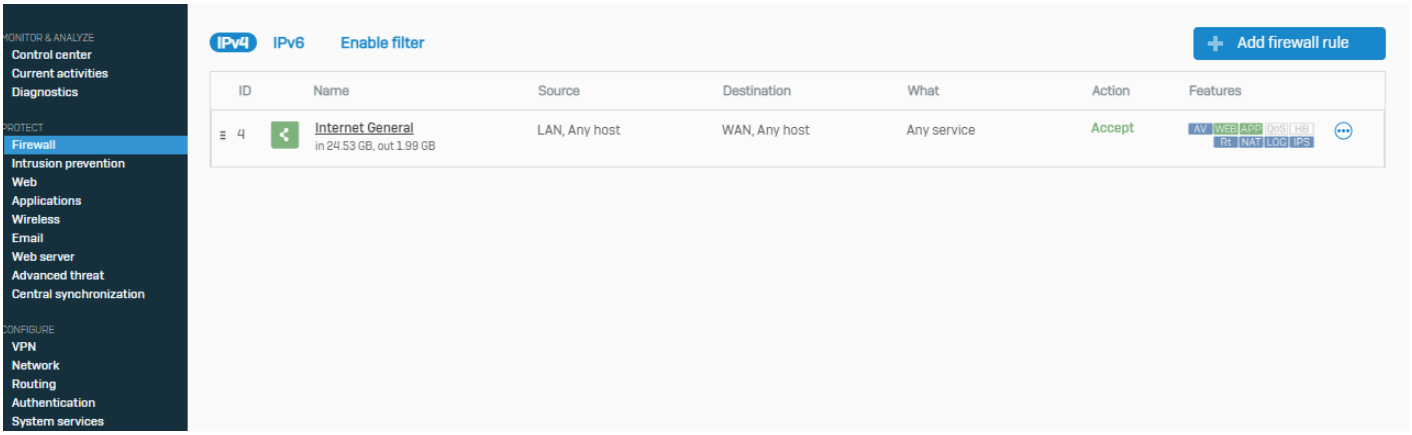
CONTROL DE APLICACIONES

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



POLÍTICAS DE FIREWALL

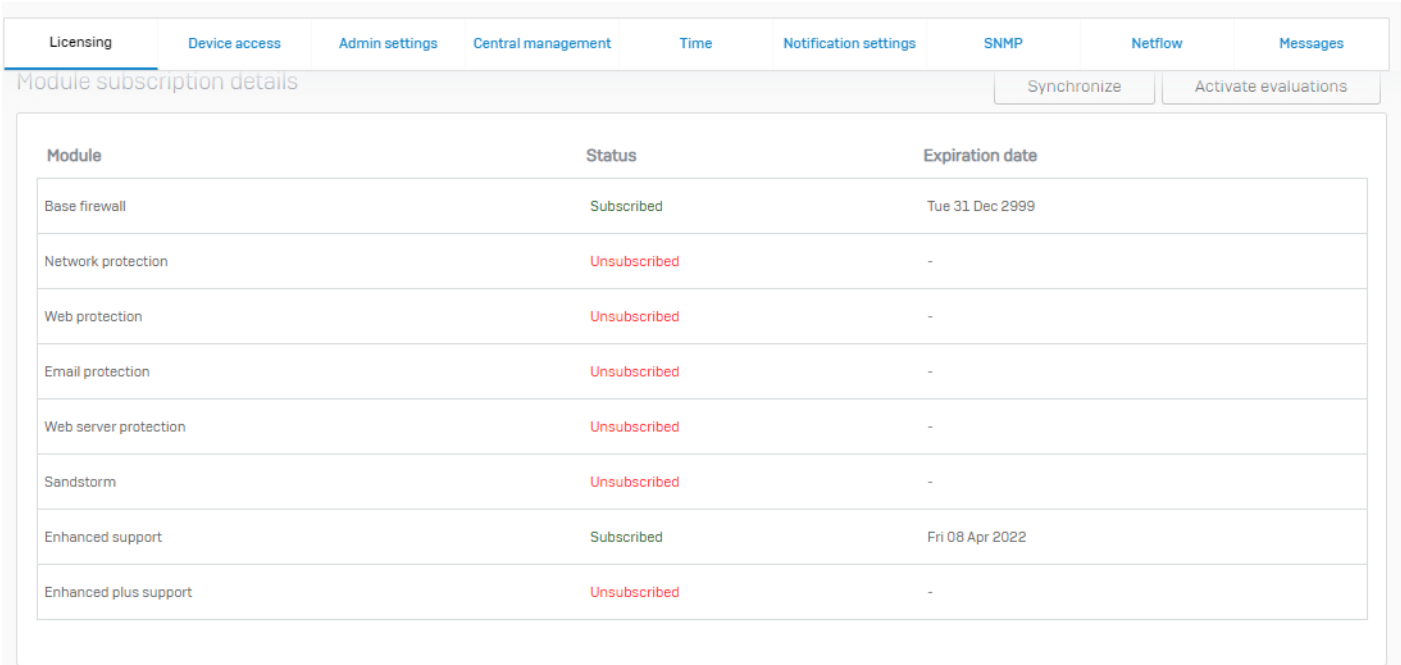
A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



LICENCIA

Serial Number	Registered	Model
C0A100XFTBXXXC5	09 April 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate ☐
Network Protection				☐
Web Protection				☐
Email Protection				☐
Web Server Protection				☐
Zero-Day Protection				☐
Enhanced Support	Subscribed	L0012226033 / Enhanced Support	08 Apr 2022	
Enhanced Plus Support Upgrade				


Licensing
Device access
Admin settings
Central management
Time
Notification settings
SNMP
Netflow
Messages
Module subscription details
Synchronize
Activate evaluations
Module
Status
Expiration date
Base firewall
Subscribed
Tue 31 Dec 2999
Network protection
Unsubscribed
-
Web protection
Unsubscribed
-
Email protection
Unsubscribed
-
Web server protection
Unsubscribed
-
Sandstorm
Unsubscribed
-
Enhanced support
Subscribed
Fri 08 Apr 2022
Enhanced plus support
Unsubscribed
-

POLÍTICA DE SEGURIDAD

El equipo está actualmente configurado para la protección IPS contra todo tipo de amenazas externas, principalmente el ransomware, este malware encripta documentos, archivos personales, críticos y solicita transferir a otros fondos, dinero pero en moneda BitCoin para que la víctima desbloquee sus archivos. El comportamiento similar a un gusano exhibido por este malware se debe a una sonda activa para el puerto 445 (***ya bloqueado en su UTM***) del servidor SMBv1 en la LAN local que busca la presencia de Backdoor.Double.Pulsar. Si la puerta trasera está presente, la carga útil se entrega y se ejecuta a través de este canal. De lo contrario, se toma una ruta de explotación ligeramente menos confiable.

Por lo anterior es importante señalar que esta solucion de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría “Malware Communication”
2. El motor AV habilitado nos ayuda a detectar el malware junto con las variantes
3. El filtro web se habilitó a todos los usuarios sin excepción para bloquear los sitios web que se han identificado como atacantes potenciales
    - Anonymizers
    - Command & Control
    - Phishing & Fraud
    - Spam URLs

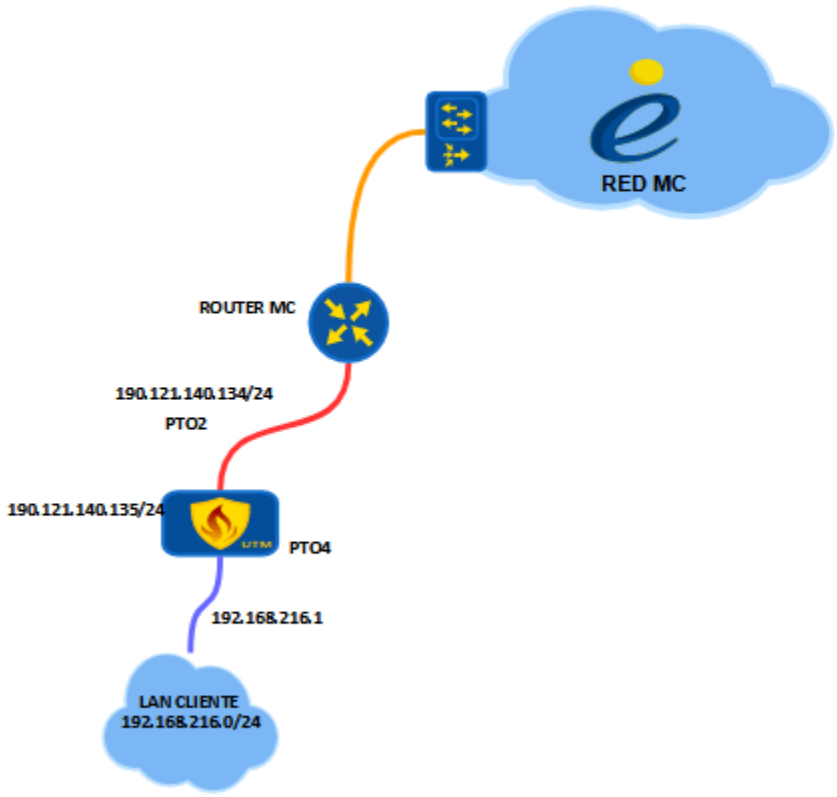
4. Con el control de aplicaciones estamos bloqueando igualmente para todos los usuarios el software Proxy and Tunnel principalmente para cortar cualquier tipo de gestión para la red TOR que es el protocolo de comunicación de los ataques ransomware.

de igual forma ninguna solución es 100% segura y solo estamos protegiendo el perímetro, no tenemos control sobre los dispositivos de almacenamiento que ingresen los usuarios en su computadora, por esto recomendamos en lo posible contar con una buena plataforma de antivirus y software adicionales que permitan controlar estos ataques que están en constante cambio. Si desea asesoría sobre cómo obtener protección adicional para su red LAN con un excelente antivirus o software adicional que le garantice no tener inconvenientes con el secuestro de datos importantes para su compañía puede consultar a nuestro asesor comercial.

Con el usuario y contraseña que le hemos entregado para la administración del equipo puede observar todas las políticas anteriormente mencionadas, le solicitamos por favor validar que la información registrada en este documento sea copia exacta de la configuración entregada en el UTM, si nota alguna anomalía por favor reportarse de inmediato.

ESQUEMA DE SOLUCIÓN, TOPOLOGÍA

Topología CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ ID_10



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD: SOCHA	FECHA: 26-03-21	HORA INICIAL: 12:00	HORA FINAL: 14:00
CLIENTE: CCE CORPOBOYACA		SUBCLIENTE: N/A	
TICKET ACTIVIDAD: OT 179845		DIRECCION: CRA 10 # 3-57	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

☐ SOPORTE	☐ ASEGURAMIENTO	☐ NODOS INALAMBRICOS
☒ APROVISIONAMIENTO	☐ PROYECTOS INALAMBRICOS	☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

→ Visita tecnica para instalación de equipo solicitud del area PEM.

REPORTE TECNICO: → Se realiza visita y se instala equipo UTM Sophos S/N C0A100XFBXXXCS con patch cord UTP y se realizan conexiones según indicaciones de la compañera Yessica Gomez.

→ Se confirma servicio operativo y la instalación de equipo con cliente. y compañera Yessica Gomez

ESTADO DE LA NOVEDAD:	EN PROCESO	PENDIENTE	OTRA

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Daysy Santos.	
Nombre: Daysy Liana Santos F.	Nombre: Angelica Fonseca
C.C.: 1.056.552.432	C.C.: 1049640115
N° TELEFONICO: 3214021334.	N° TELEFONICO: 320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 01 DE MARZO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet 20 Mbps

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Direccionamiento IP WAN: 181.225.70.239/31
Direccionamiento IP LAN: 192.168.100.1/24
Acceso al equipo: https://181.225.70.239:4445/
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178747	7	Soata	Calle 11 NO. 4-45	20 Mbps	181.225.70.238/31	192.168.100.1/24	Se realiza nat.	Fa0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interface del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE_CORPOBOYACA_ID7# show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 336 bytes
!
interface FastEthernet0/1
 description ###To_Lan####
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 rate-limit input 20968000 3932160 7864320 conform-action transmit exceed-action drop
 rate-limit output 20968000 3932160 7864320 conform-action transmit exceed-action drop
 duplex auto
 speed auto
end

CCE_CORPOBOYACA_ID7#
```

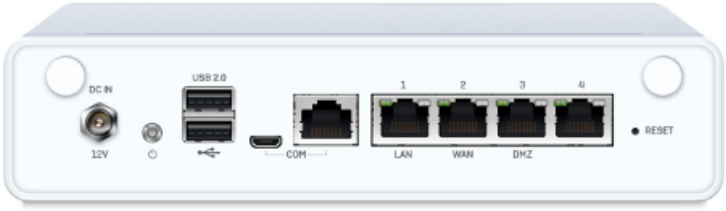
```
CCE_CORPOBOYACA_ID7# ping 8.8.8.8 source fastEthernet 0/1 repeat 1000 size 1448

Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 28/38/160 ms
CCE_CORPOBOYACA_ID7#
```

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

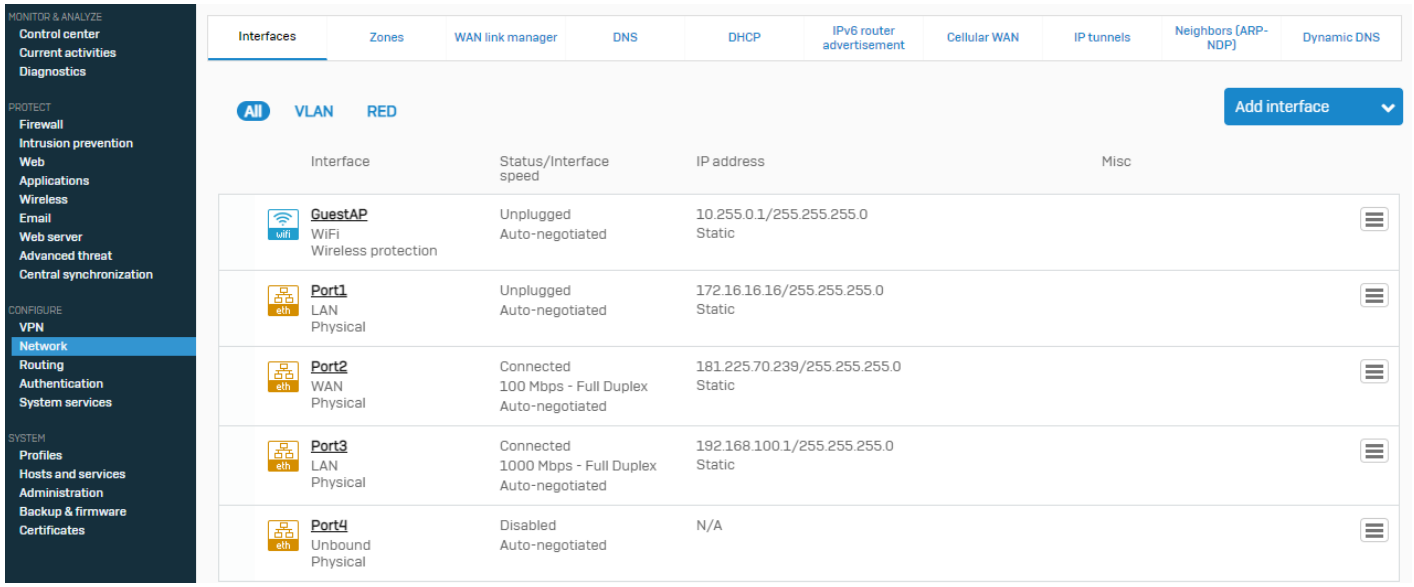
Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 1841	FTX1033W0X1	Calle 11 NO. 4-45 - Sede Soatá (Boyacá)
1	Sophos XG86	C0A100R8TF6M634	Calle 11 NO. 4-45 - Sede Soatá (Boyacá)



DETALLES DE LA CONFIGURACIÓN

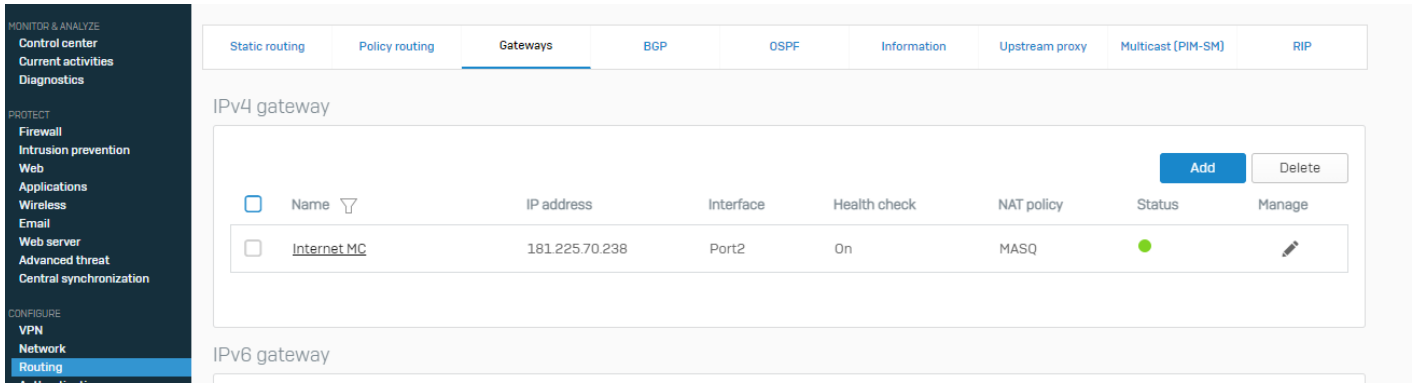
DIRECCIONAMIENTO IP E INTERFACES

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



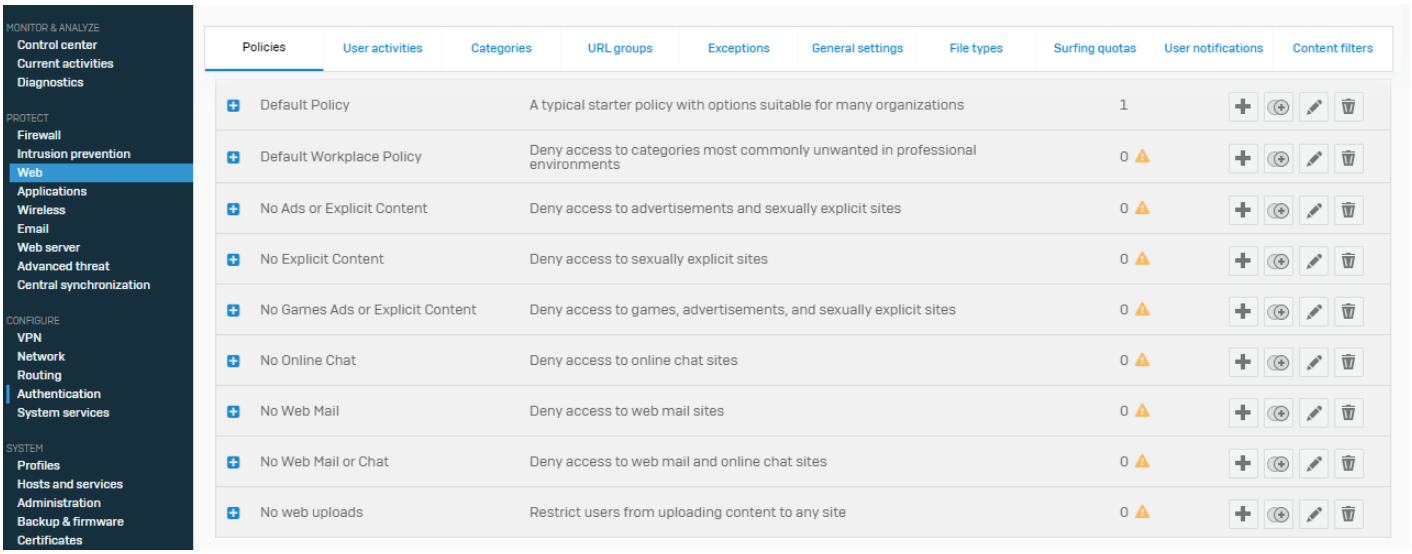
ENRUTAMIENTO

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



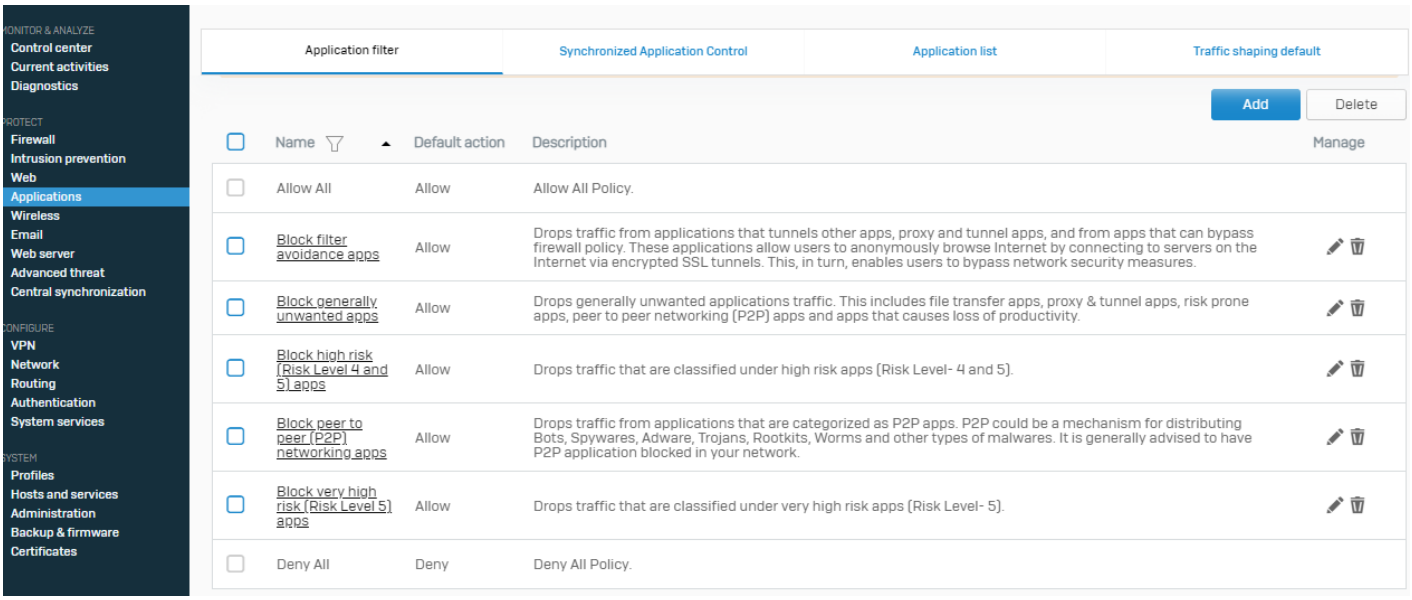
FILTRO WEB

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet.



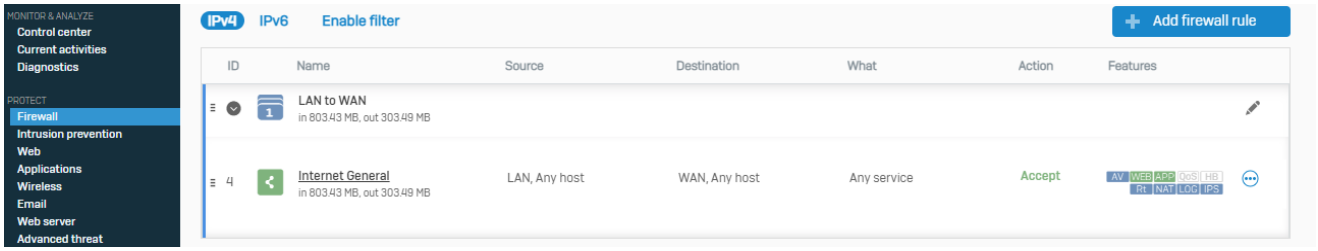
CONTROL DE APLICACIONES

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



POLÍTICAS DE FIREWALL

A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



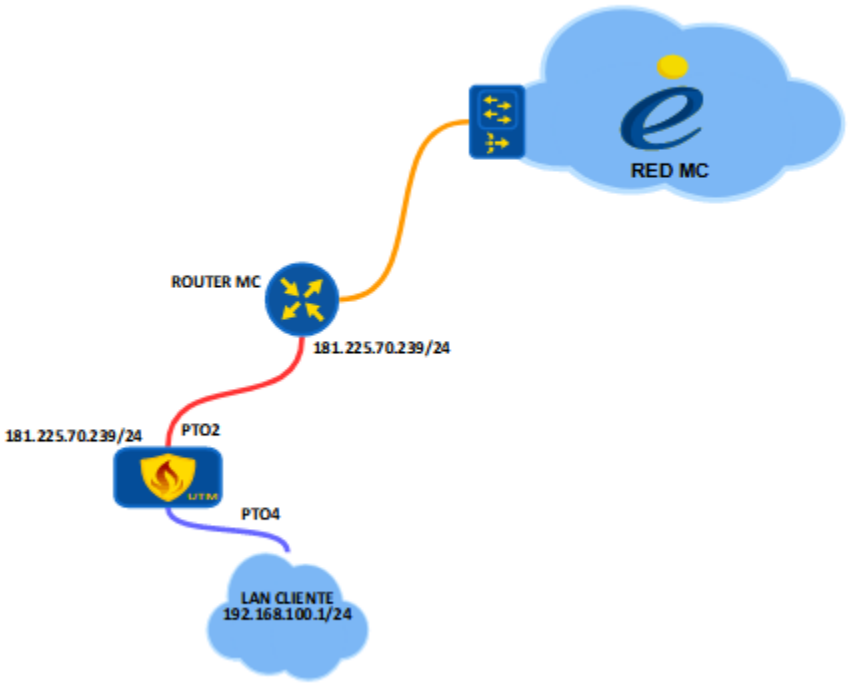
LICENCIA

Serial Number	Registered	Model
C0A100R8TF6M634	19 April 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate
Network Protection				☐
Web Protection	Subscribed	L0012274739 / Web Protection	18 Apr 2022	
Email Protection				☐
Web Server Protection				☐
Zero-Day Protection				☐
Enhanced Support	Subscribed	L0012274732 / Enhanced Support	18 Apr 2022	
Enhanced Plus Support Upgrade				
Central Orchestration				☐

Module	Status	Expiration date
Base firewall	Subscribed	Tue 31 Dec 2999
Network protection	Unsubscribed	-
Web protection	Subscribed	Mon 18 Apr 2022
Email protection	Unsubscribed	-
Web server protection	Unsubscribed	-
Sandstorm	Unsubscribed	-
Enhanced support	Subscribed	Mon 18 Apr 2022
Enhanced plus support	Unsubscribed	-

Topología CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ ID_7



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD: SOATA	FECHA: 23-03-21	HORA INICIAL: 12:00	HORA FINAL: 15:00 .		
CLIENTE: CCE CORPOBOYACA		SUBCLIENTE: NIA			
TICKET ACTIVIDAD: OT 179843 - 179847		DIRECCION: CLL 11 # 4-45			

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

☐ SOPORTE	☐ ASEGURAMIENTO	☐ NODOS INALAMBRICOS
☒ APROVISIONAMIENTO	☐ PROYECTOS INALAMBRICOS	☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

- Visita tecnica para instalación de equipo UTM por solicitud del area de PEM.

REPORTE TECNICO:

- Se realiza visita y se procede a instalar equipo UTM Sophos XG86 S/N C0A100R8TF6M634, con 2 patch cord UTM, uno instalado a Nivel LAN y otro a nivel WAN.
- Se presentan problemas de gestion por lo que se realizen descartes de primer nivel y se evidencia que es posible daño de POE o patch cord hacia la antena se reporta al área encargada para su validación.
- Se confirma visita e instalación de UTM con diente y se informa a la compañera Yesica Gomez.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	EN PROCESO X	PENDIENTE	OTRA

OBSERVACIONES DEL CLIENTE:

Se verifica la instalación del equipo sophos Referencia XG 86, pero no queda habilitado el servicio, se me informa que ya fue reportado el incidente al centro de gestión y al Ing. Alfredo, Orjuela. quedamos a la espera de Asistente Técnico.

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nombre: Nancy Milena Uclandia Leal	Nombre: Angelica Fonseca
C.C.: 40.039.613	C.C.: 1049640115
N° TELEFONICO: 3112328287	N° TELEFONICO: 320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 05 DE MARZO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet 20 Mbps - Activación de servicio Seguridad UTM.

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Información requerimiento:

Direccionamiento IP WAN: 190.121.140.109/31
Direccionamiento IP LAN: 192.168.100.1/24
Acceso al equipo: https://190.121.140.109:4445/
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
178596	5	Pauna	Calle 5 #5-05 Piso 2 - Sede Pauna (Boyacá)	20 Mbps	190.121.140.108/31	190.121.140.108	190.121.140.109	Fa0/1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interfaz del CPE, al igual que las pruebas de conectividad a los DNS de Google.

```
CCE_CORPOBOYACA#show running-config interface fastEthernet 0/1
Building configuration...

Current configuration : 317 bytes
!
interface FastEthernet0/1
 description ###To_LAN####
 ip address 190.121.140.108 255.255.255.254
 rate-limit input 20968000 3932160 7864320 conform-action transmit exceed-action drop
 rate-limit output 20968000 3932160 7864320 conform-action transmit exceed-action drop
 duplex auto
 speed auto
 no keepalive
end

CCE_CORPOBOYACA#
```

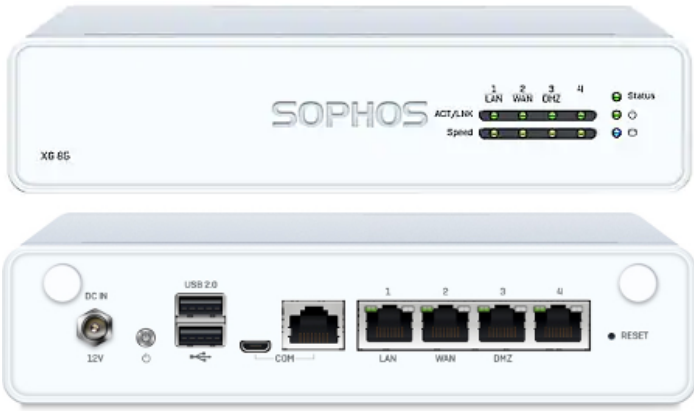
```
CCE_CORPOBOYACA#ping 8.8.8.8 repeat 1000 size 1448 source fastEthernet 0/1

Type escape sequence to abort.
Sending 1000, 1448-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 190.121.140.108
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/6/8 ms
CCE_CORPOBOYACA#
```

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

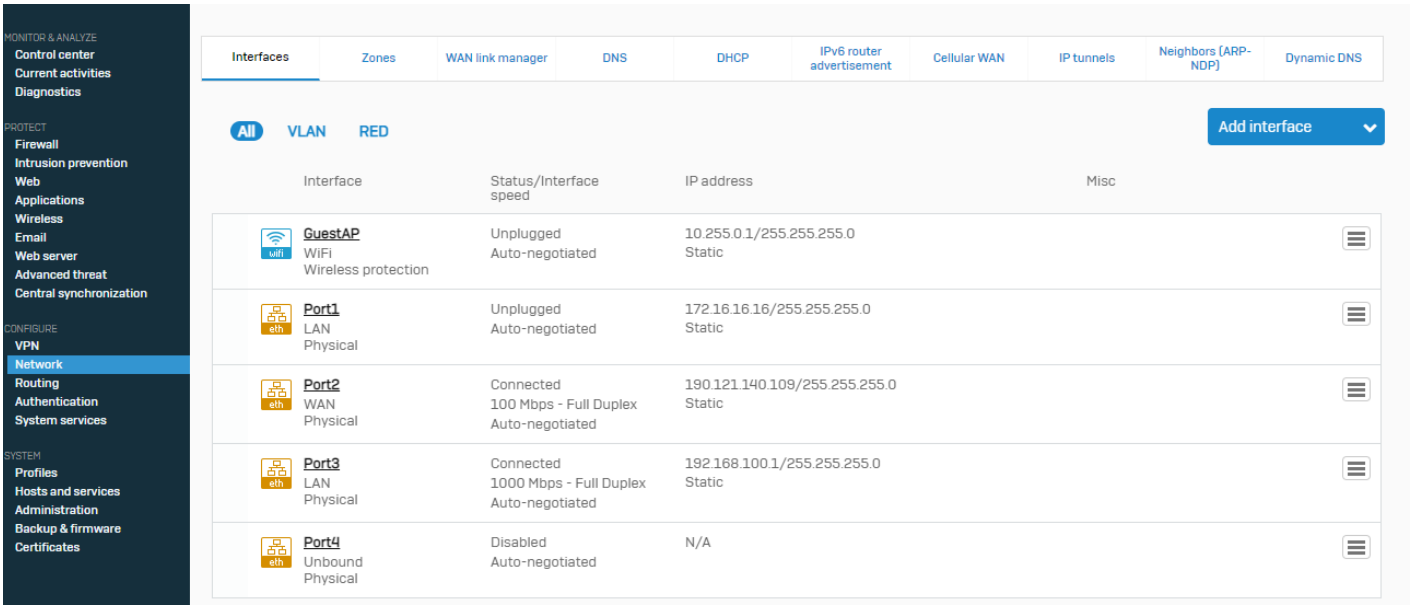
Cantidad	Enrutador Marca	Serial	Sede
1	Cisco 1841	FTX1030W0V1	Calle 5 #5-05 Piso 2 - Sede Pauna (Boyacá)
1	SOPHOS XG XG86	C0A100VT26994AE	Calle 5 #5-05 Piso 2 - Sede Pauna (Boyacá)



DETALLES DE LA CONFIGURACIÓN

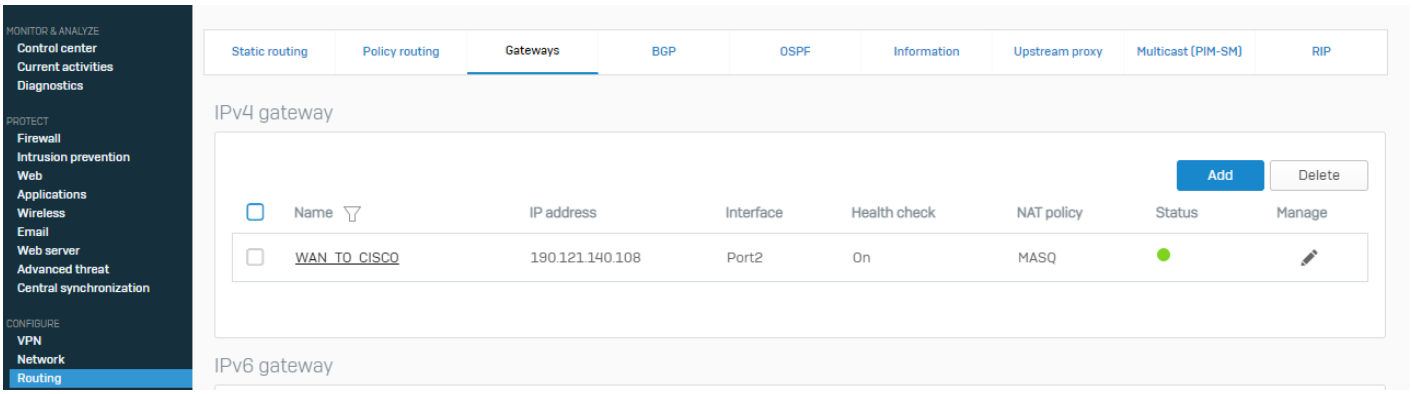
DIRECCIONAMIENTO IP E INTERFACES

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



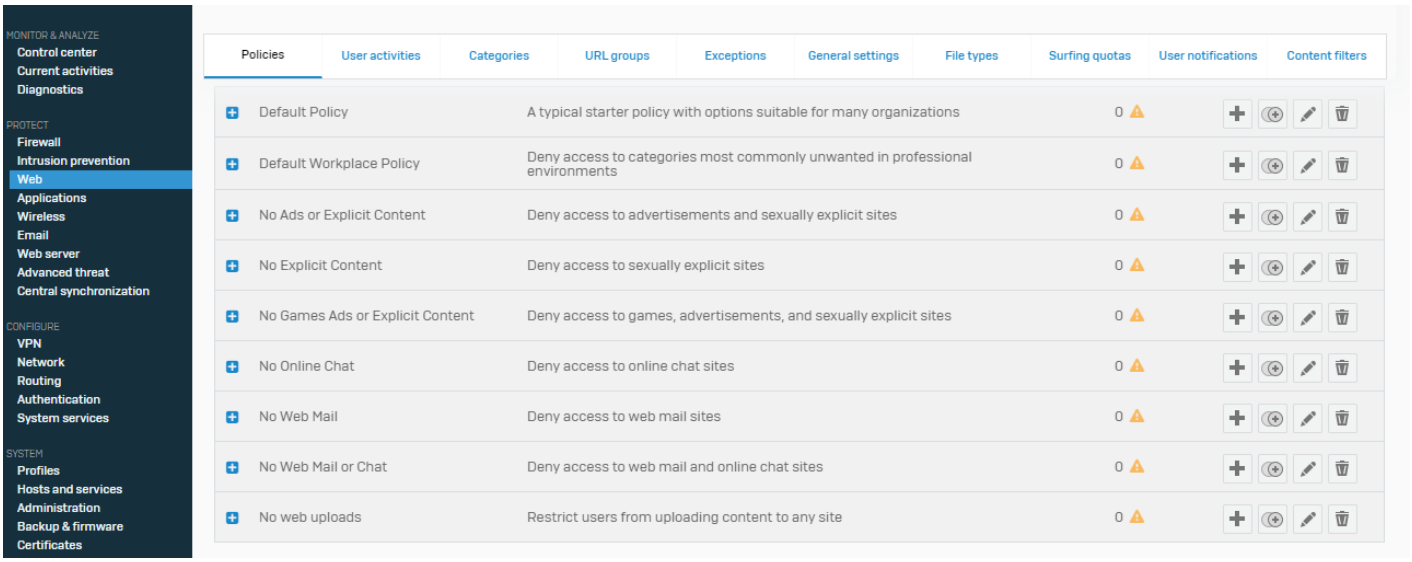
ENRUTAMIENTO

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



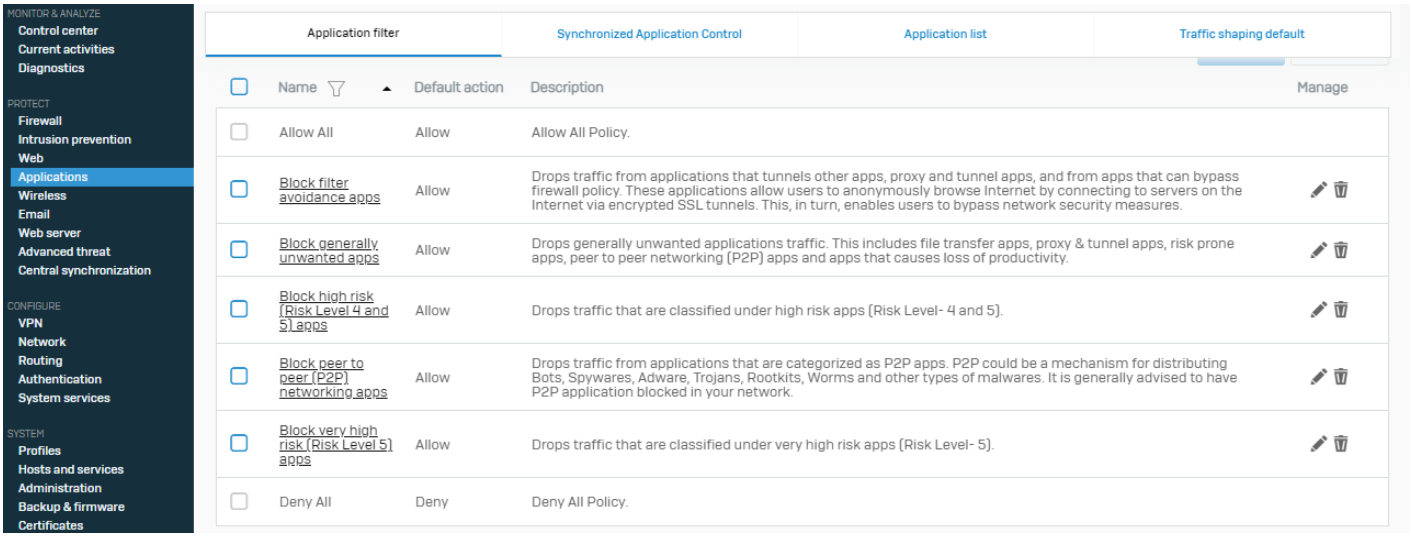
FILTRO WEB

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet.



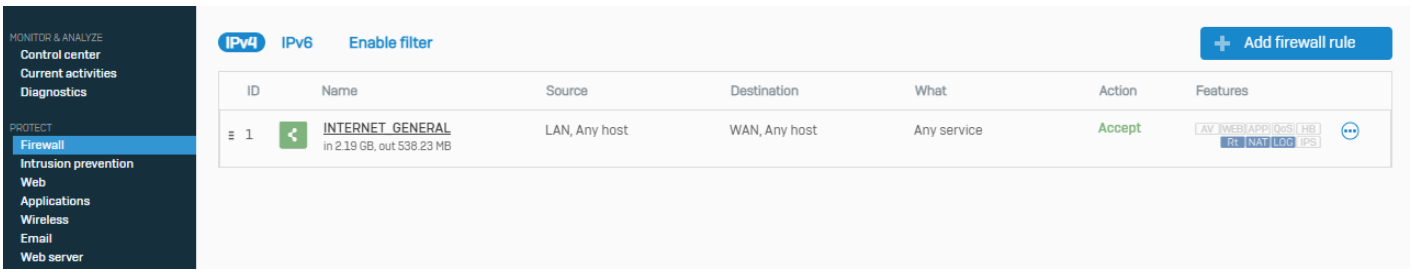
CONTROL DE APLICACIONES

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



POLÍTICAS DE FIREWALL

A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



LICENCIA

Serial Number	Registered	Model
C0A100VT26994AE	02 March 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate
Network Protection				☐
Web Protection				☐
Email Protection				☐
Web Server Protection				☐
Zero-Day Protection				☐
Enhanced Support	Subscribed	L0012233976 / Enhanced Support	11 Apr 2022	
Enhanced Plus Support Upgrade				

Module subscription details

Synchronize | Activate evaluations

Module	Status	Expiration date
Base firewall	Subscribed	Tue 31 Dec 2999
Network protection	Unsubscribed	-
Web protection	Unsubscribed	-
Email protection	Unsubscribed	-
Web server protection	Unsubscribed	-
Sandstorm	Unsubscribed	-
Enhanced support	Subscribed	Mon 11 Apr 2022
Enhanced plus support	Unsubscribed	-

POLÍTICA DE SEGURIDAD

El equipo está actualmente configurado para la protección IPS contra todo tipo de amenazas externas, principalmente el ransomware, este malware encripta documentos, archivos personales, críticos y solicita transferir a otros fondos, dinero pero en moneda BitCoin para que la víctima desbloquee sus archivos. El comportamiento similar a un gusano exhibido por este malware se debe a una sonda activa para el puerto 445 (***ya bloqueado en su UTM***) del servidor SMBv1 en la LAN local que busca la presencia de Backdoor.Double.Pulsar. Si la puerta trasera está presente, la carga útil se entrega y se ejecuta a través de este canal. De lo contrario, se toma una ruta de explotación ligeramente menos confiable.

Por lo anterior es importante señalar que esta solucion de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría “Malware Communication”
2. El motor AV habilitado nos ayuda a detectar el malware junto con las variantes
3. El filtro web se habilitó a todos los usuarios sin excepción para bloquear los sitios web que se han identificado como atacantes potenciales
    - Anonymizers
    - Command & Control
    - Phishing & Fraud
    - Spam URLs

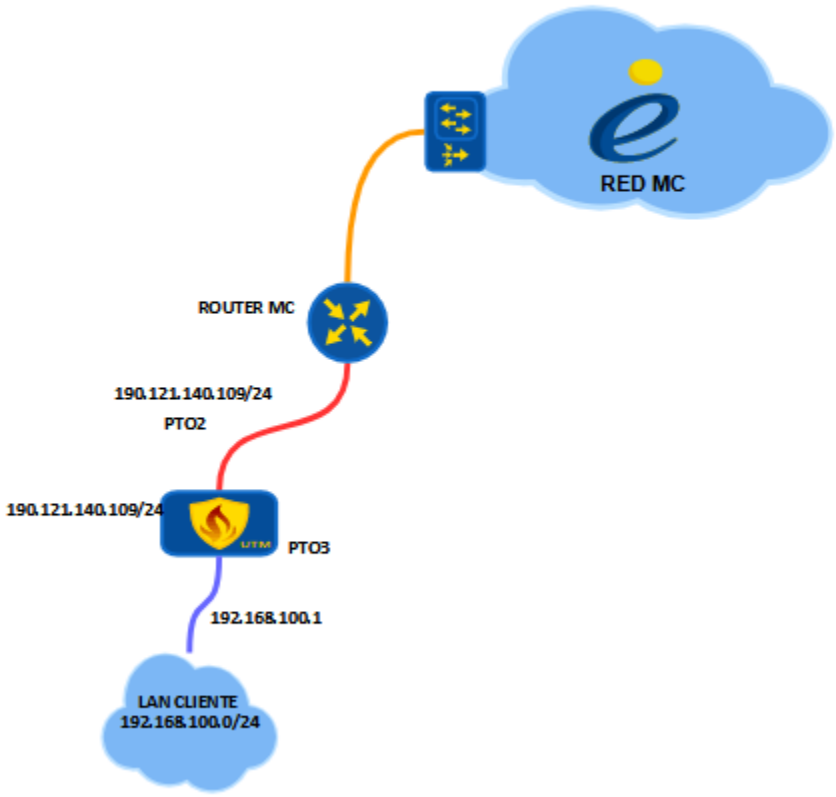
4. Con el control de aplicaciones estamos bloqueando igualmente para todos los usuarios el software Proxy and Tunnel principalmente para cortar cualquier tipo de gestión para la red TOR que es el protocolo de comunicación de los ataques ransomware.

de igual forma ninguna solución es 100% segura y solo estamos protegiendo el perímetro, no tenemos control sobre los dispositivos de almacenamiento que ingresen los usuarios en su computadora, por esto recomendamos en lo posible contar con una buena plataforma de antivirus y software adicionales que permitan controlar estos ataques que están en constante cambio. Si desea asesoría sobre cómo obtener protección adicional para su red LAN con un excelente antivirus o software adicional que le garantice no tener inconvenientes con el secuestro de datos importantes para su compañía puede consultar a nuestro asesor comercial.

Con el usuario y contraseña que le hemos entregado para la administración del equipo puede observar todas las políticas anteriormente mencionadas, le solicitamos por favor validar que la información registrada en este documento sea copia exacta de la configuración entregada en el UTM, si nota alguna anomalía por favor reportarse de inmediato.

ESQUEMA DE SOLUCIÓN, TOPOLOGÍA

Topología CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ ID_22



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD:	PAUNA	FECHA:	02-03-21	HORA INICIAL:	11:00 HORA FINAL: 14:00
CLIENTE:	CORPORACION AUTONOMA RY	SUBCLIENTE:	N/A		
TICKET ACTIVIDAD:	OT 178596	DIRECCION:	CLL 5 #05-05 Piso 2		

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

- ☐ SOPORTE
- ☐ ASEGURAMIENTO
- ☐ NODOS INALAMBRICOS
- ☒ APROVISIONAMIENTO
- ☐ PROYECTOS INALAMBRICOS
- ☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

→ Visita tecnica para instalación de equipos por solicitud del área de PEM.

REPORTE TECNICO: → Se realiza visita se procede a instalar equipo CISCO 1841 S/N FTX1030W0VL y sophos XA86 S/N C0A100UT2699FAE. Se valida configuración con la Ing Leydy Guacheta, se instala 2 patc cord UTP. y un herraje 1841.

→ Se conecta red LAN, se confirma capacidad de 20Megas.

→ Se confirma servicio operativo con el cliente y la Ing Leydy Guacheta quienes confirman retiro de la sede.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	X	EN PROCESO		PENDIENTE		OTRA	

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nombre: Yulp Cepeda A.	Nombre: Angelica Fonseca
C.C.: 1053330684.	C.C.: 1049640115
N° TELEFONICO: 3133874000	N° TELEFONICO: 320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 31 DE MARZO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet 6 Mbps

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
180155	258	Aquitania	KM 3 VÍA AQUITANIA A SOGAMOSO, SECTOR SANTA INÉS, VEREDA CAJÓN	6 Mbps		192.168.100.1/24	Se realiza nat.	Lan1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

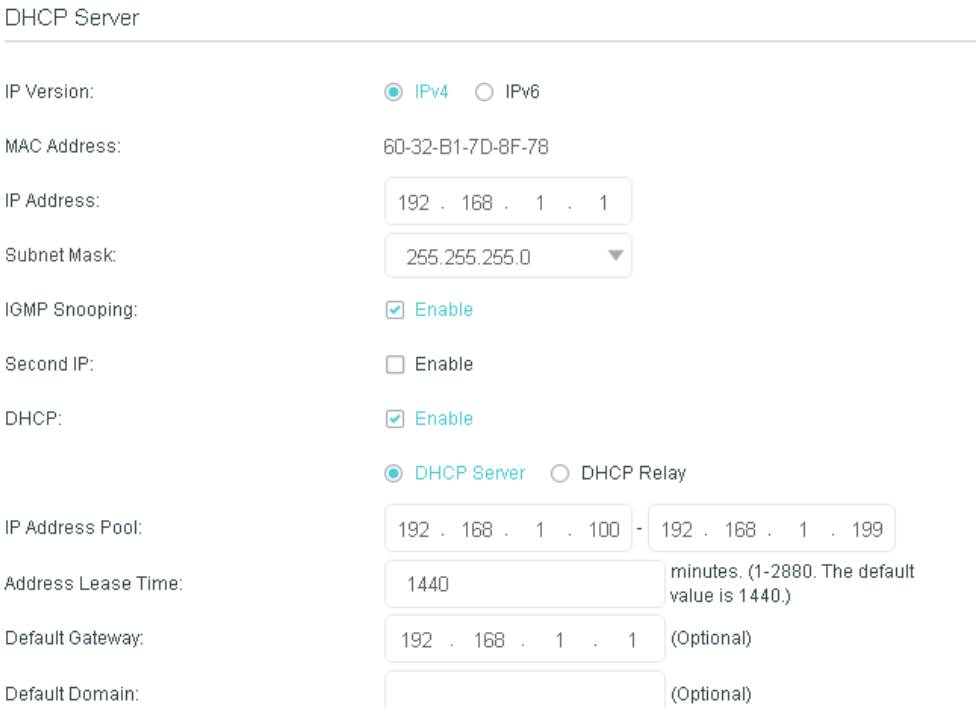
Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

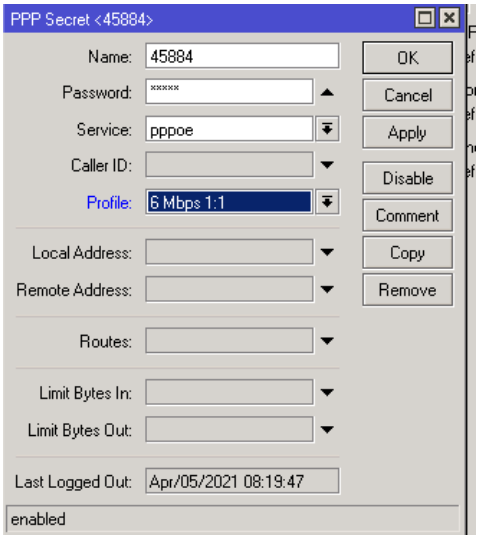
Cordialmente,

Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interfaz del CPE, al igual que las pruebas de conectividad a los DNS de Google.





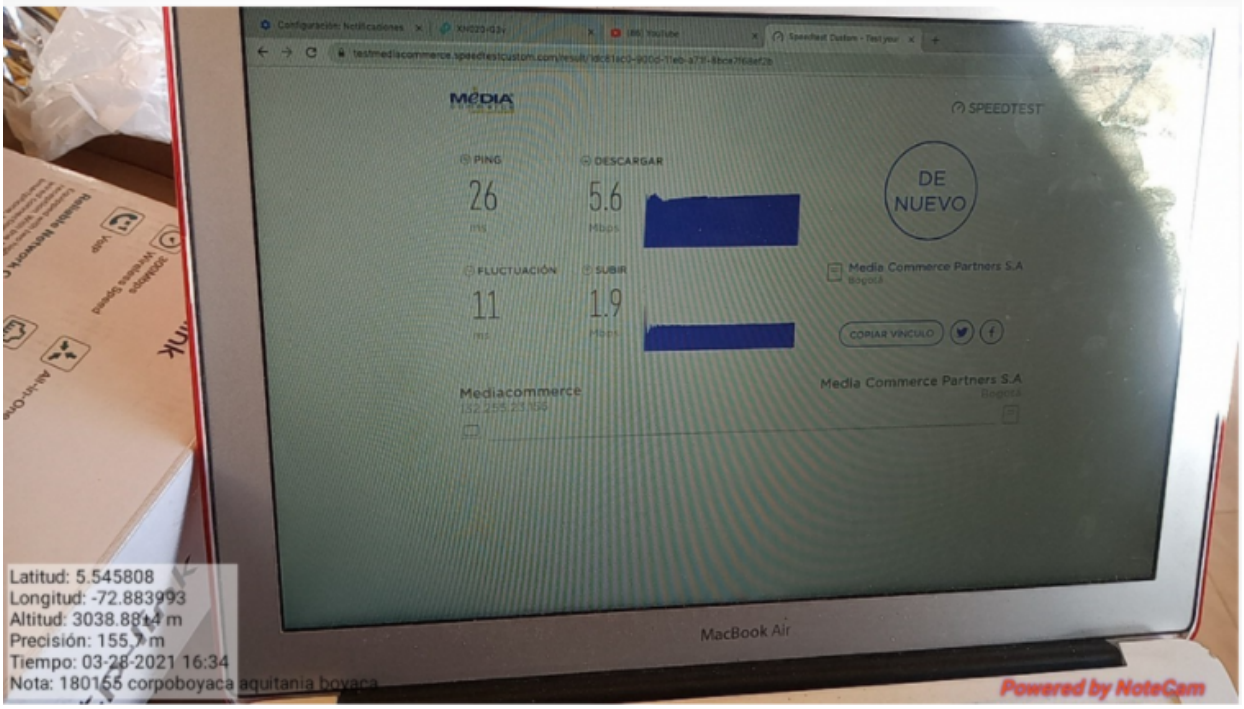
Diagnostic Tools

Click the Start button to test the Internet connection of the router.

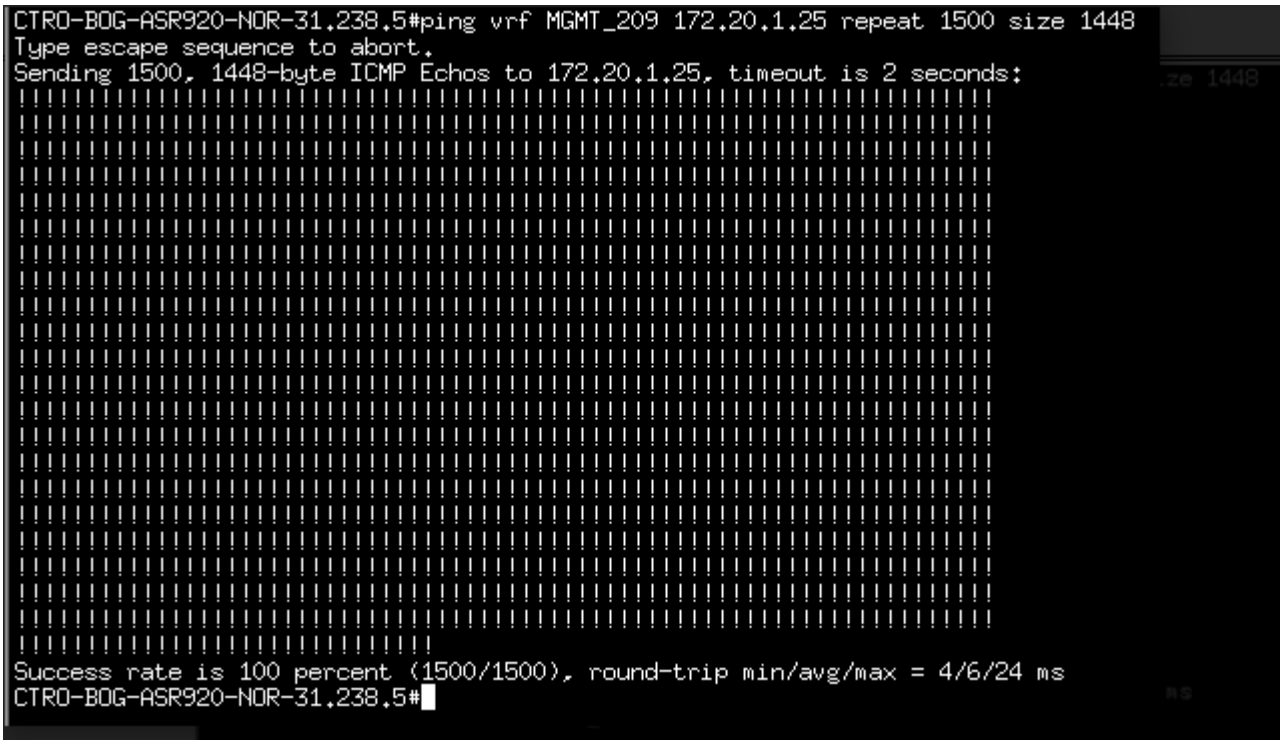
Diagnostic Type: Test Internet surfing — Start

Pon Register status	O5 (LOID: Init.)
VID[Priority]	250[0]
Bind port	Not bind
Test PPP Server connection	Pass
Test authentication with ISP	Pass
Test assigned IP address	Pass
Ping default gateway	Pass
Ping primary Domain Name Server	Pass

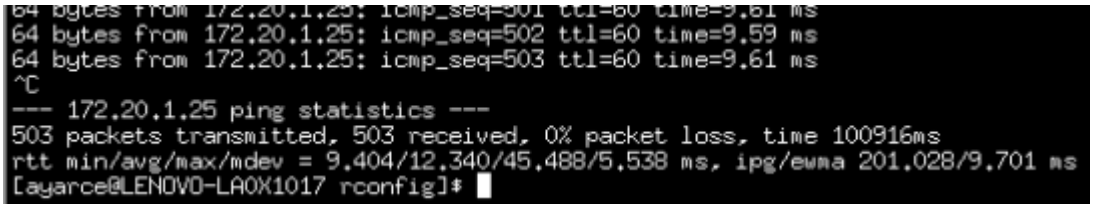
Test de velocidad



Calidad de enlace



Ping a CPE



Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios.

Equipo SOPHOS XG 86 se deja en las instalaciones del cliente pero este no queda funcionando dado que el cliente no permite realizar las conexiones. La señora Nadra Alexandra Topía firma el recibido, se adjunta acta.

Cantidad	Enrutador Marca	Serial	Sede
1	TPLINK	54504C47B17D8F78	KM 3 VÍA AQUITANIA A SOGAMOSO, SECTOR SANTA INÉS, VEREDA CAJÓN
1	SOPHOS XG 86	C0A100VQ7Y99D08	KM 3 VÍA AQUITANIA A SOGAMOSO, SECTOR SANTA INÉS, VEREDA CAJÓN

TOPOLOGÍA DE RED

MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2016

CIUDAD: AQUITANIA	FECHA: 05-04-21	HORA INICIAL: 13:00	HORA FINAL: 13:30.
CLIENTE: CCE CORPOBOYACA		SUBCLIENTE: N/A	
TICKET ACTIVIDAD: OT 179905		DIRECCION: K3 VIA AQUITANI -> SOGAMOSO	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

- ☐ SOPORTE
- ☐ ASEGURAMIENTO
- ☐ NODOS INALAMBRICOS
- ☒ APROVISIONAMIENTO
- ☐ PROYECTOS INALAMBRICOS
- ☐ NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

Visita tecnica para instalación de equipo UTM solicitud área de TEM.

REPORTE TECNICO: Se realiza visita y se procede a validar espacio para instalación de UTM, se identifica que no hay rack y la red LAN es totalmente WIFI, por lo que se informa a la implementadora y al cliente la novedad, quien informa que la red es temporalmente WIFI y no se puede dejar instalado UTM a la red local. Se deja equipo en custodia del cliente en sede para que sea instalado a futuro y se informa la novedad con el área correspondiente.

Se confirma visita con cliente y equipo UTM Sophos XG 86 SN: C0A1DOUQY99D08 con caja original y accesorios necesarios.

ESTADO DE LA NOVEDAD:	EN PROCESO	PENDIENTE	OTRA

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nadra A. Topia U.	
Nombre: Nadia Alexandra Topia Uscátegui	Nombre: Angelica Fonseca
C.C.: 1.053.584.752	C.C.: 1049640115
N° TELEFONICO: 3112963966.	N° TELEFONICO: 320 6888987

CCE-CORPOBOYACA CORPORACION
AUTONOMA REGIONAL DE BOYACA

Ingeniero. Pedro Vela.

Leydy Guachetá
Implementador de Servicios especiales.

PEREIRA, 09 DE MARZO DEL 2021

SEÑORES**:**

CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA

Ref. Activación canales de internet 20 Mbps

Para **MEDIA COMMERCE PARTNERS**, es muy grato poder saber que **CCE-CORPOBOYACA CORPORACION AUTONOMA REGIONAL DE BOYACA** ha depositado su confianza para permitirnos ser su proveedor de servicios de telecomunicaciones, lo que nos compromete día a día en prestar un excelente servicio con la calidad por ustedes esperada, que redundará en beneficios para la prestación de sus servicios de Telecomunicaciones.

Por esto nos permitimos dar inicio con la activación del servicio contratado. A continuación, referenciaremos los datos correspondientes de acuerdo con los requerimientos técnicos expuestos e implementados para el funcionamiento de este servicio:

Código referencia identificación MC: 48171

Direccionamiento IP WAN: 190.121.140.107/31
Direccionamiento IP LAN: 192.168.102.1/24
Acceso al equipo: https://190.121.140.107:4445/
Usuario cliente: corpoboyaca
Password: C0rp0b0y4c42021*

Información requerimiento:

OT	Enlace	Ciudad	Dirección	Capacidad	RED	GATEWAY (ROUTER MC)	IP DISPONIBLES	PTO LAN SERVICIO
179962	24	Miraflores	CRA 12 NO. 2-05 - Miraflores (Boyacá)	20 Mbps		192.168.100.1/24	Se realiza nat.	Lan1

Recuerde que cualquier evento sobre el servicio prestado lo puede reportar a nuestro Centro de gestión el cual tiene operación 7 x 24 x 365, por medio de las siguientes opciones de contacto:

NIVELES DE ESCALAMIENTO GESTIÓN DE FALLAS OPERATIVAS						
NIVEL	**TIEMPO DE ESCALAMIENTO**	**PUNTO DE ESCALAMIENTO**	**NOMBRE**	**TELEFONO FIJO**	**TELEFONO CELULAR**	**CORREO ELECTRONICO**
1	Inmediato	Centro de Gestión Gobierno	Agente en Turno	018000180166		soporte.estatal@mc.net.co soporte.cce@mc.net.co
2	1 hora	Coordinador de Centro de Gestión	Andrés Felipe Corrales	(6)3112700 Extensión 15001	3206777501	Andres.corrales@mc.net.co
3	2 horas	Subdirector de Soporte y Aseguramiento	Lilia Constanza Franco Ospina	(6)3112700 Extensión 15722	3206777517	constanza.franco@mc.net.co
4	4 horas	Director de Redes y Tecnología	Geovany Gallego	(6)3112700 Extensión 15701	3206770387	geovanny.gallego@mc.net.co

Solicitamos comedidamente confirmar vía email, el visto bueno y recepción a satisfacción del servicio aprovisionado, de no recibir ninguna notificación en las próximas 48 horas sucesivas a esta notificación se dará por entendido que el servicio ha sido recibido a satisfacción.

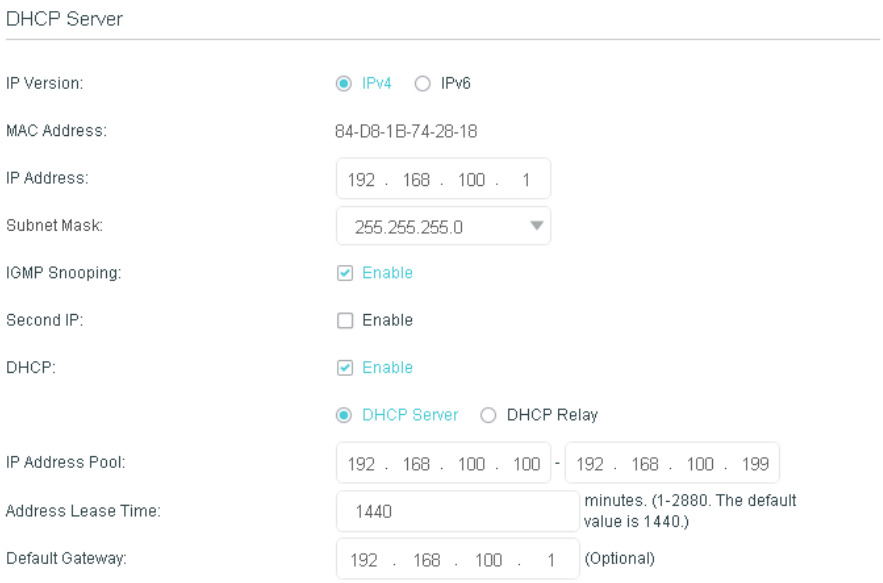
Los equipos que MEDIA COMMERCE entrega para la prestación del servicio son en comodato, los cuales son de propiedad de MEDIA COMMERCE. En caso de daño total que no provenga del deterioro natural, de hurto o extravío del (o los) equipo(s) el usuario que haya recibido equipos en comodato o arrendamiento deberá pagar a MEDIA COMMERCE el valor de reposición

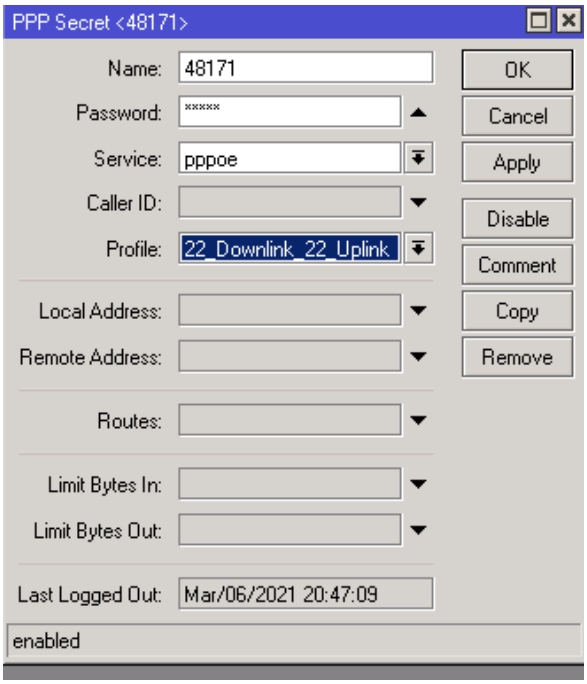
Cordialmente,

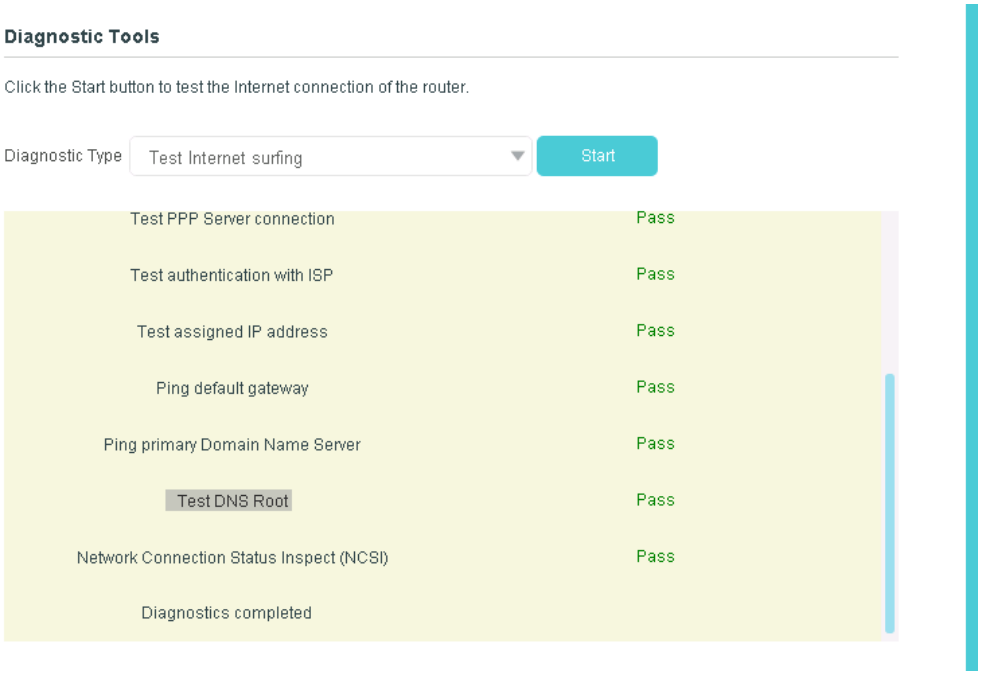
Leydy Guachetá
Implementador de Servicios Especiales
Línea Nacional 01 8000 11 2862 opción 2 – 01 8000 18 9878

ANEXOS

A continuación, se observa la configuración de BW en la interface del CPE, al igual que las pruebas de conectividad a los DNS de Google.



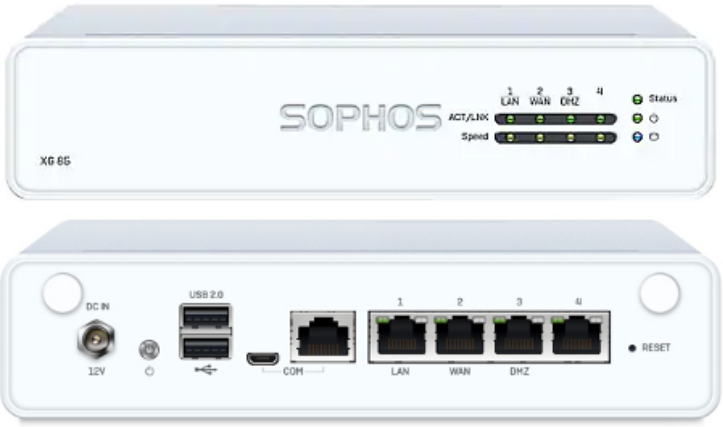



Diagnostic Tools
Click the Start button to test the Internet connection of the router.
Diagnostic Type
Test Internet surfing
Start
Test PPP Server connection
Pass
Test authentication with ISP
Pass
Test assigned IP address
Pass
Ping default gateway
Pass
Ping primary Domain Name Server
Pass
Test DNS Root
Pass
Network Connection Status Inspect (NCSI)
Pass
Diagnostics completed

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

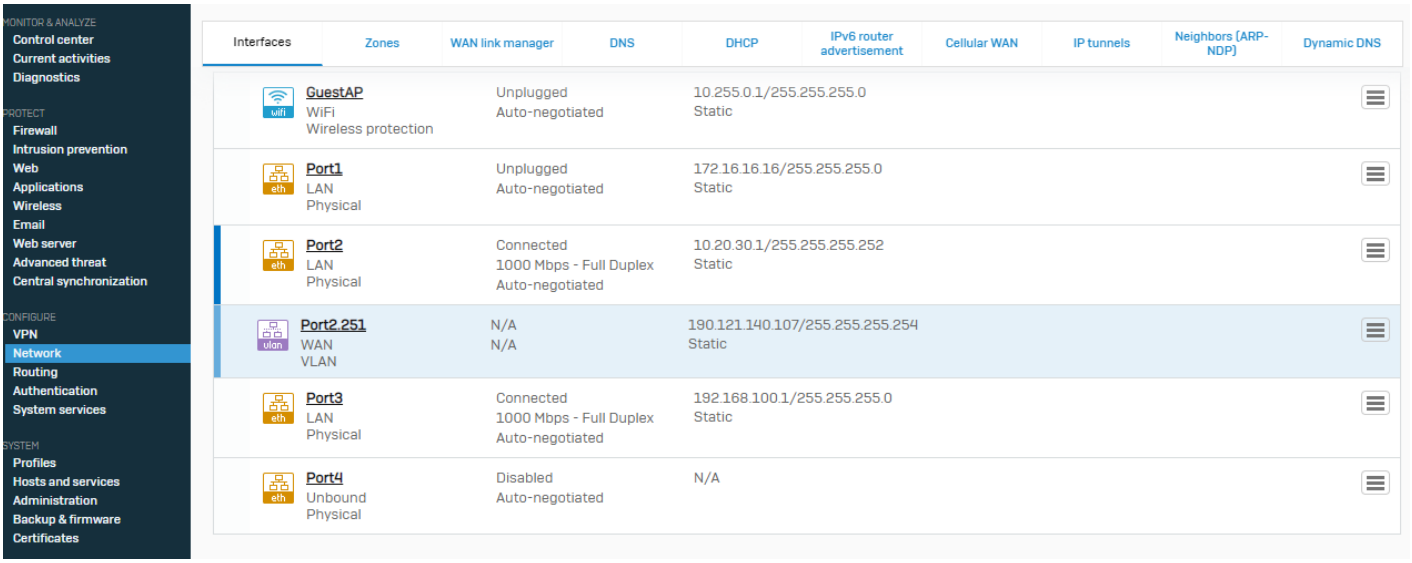
Cantidad	Enrutador Marca	Serial	Sede
1	TPLINK	54504C471B742818	CRA 12 NO. 2-05 - Miraflores (Boyacá)
1	Sophos XG XG86	C0A100VPFG2P32E	CRA 12 NO. 2-05 - Miraflores (Boyacá)



DETALLES DE LA CONFIGURACIÓN

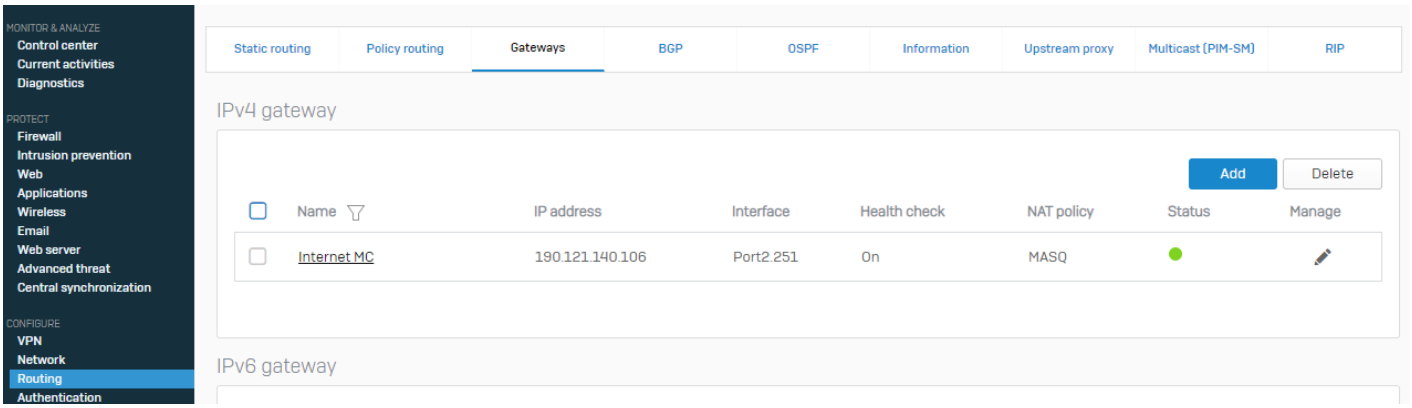
DIRECCIONAMIENTO IP E INTERFACES

A continuación, puede observar todo el direccionamiento IP que se configuró en cada una de las interfaces del dispositivo



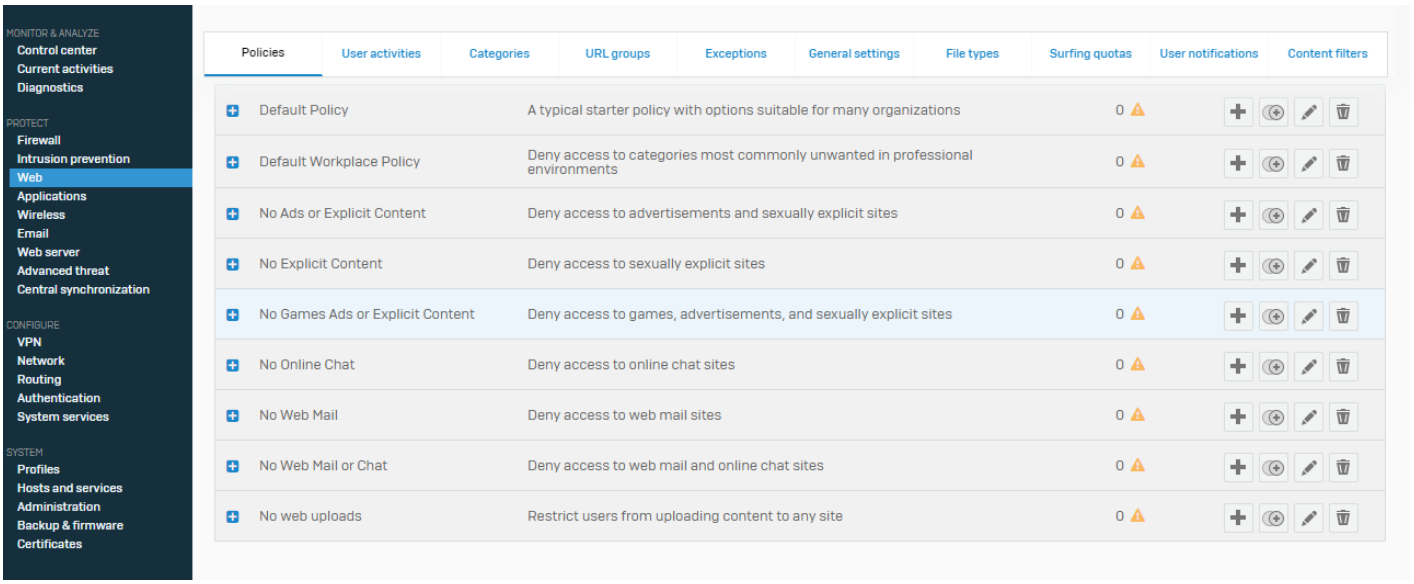
ENRUTAMIENTO

En la siguiente gráfica se muestran los enrutamientos realizados, red destino, interface y Gateway.



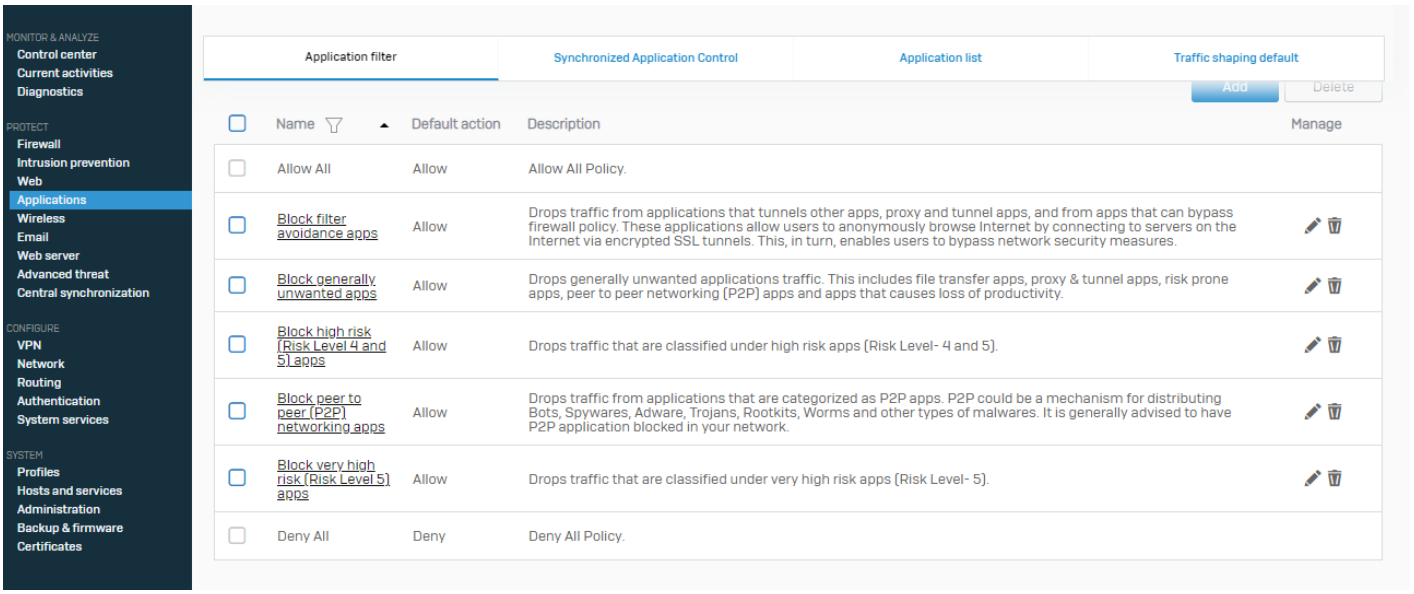
FILTRO WEB

A continuación, se observan los perfiles de filtrado web creados, estos son aplicados a las políticas de firewall dependiendo si el usuario es restringido o de libre acceso a internet.



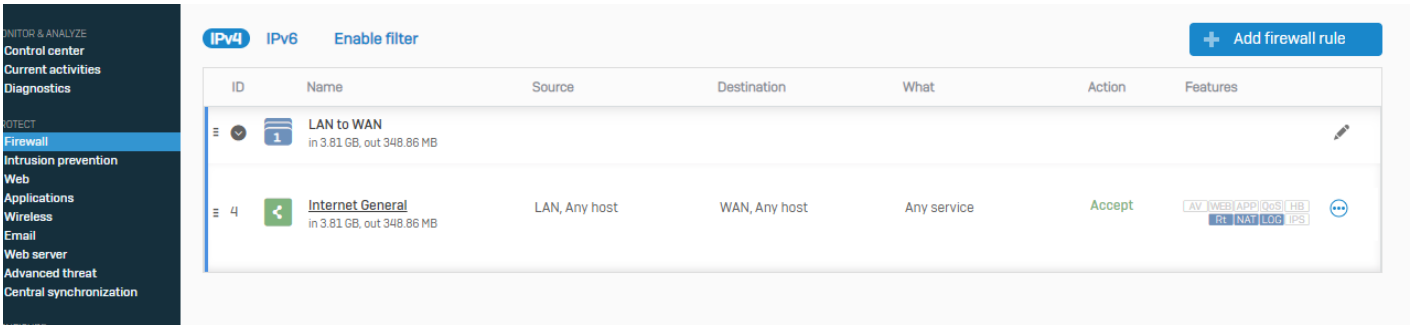
CONTROL DE APLICACIONES

Con el control de aplicaciones se bloqueó el software no productivo instalado en los equipos de cómputo y dispositivos móviles según su requerimiento, por motivos de seguridad se aplica restricción a todos los usuarios sin excepción del software tipo proxy y túnel.



POLÍTICAS DE FIREWALL

A continuación, se observan las políticas de firewall configuradas, en todas las políticas se aplicó el respectivo control IPS, filtro WEB y de aplicaciones para la seguridad perimetral contra el Ransomware y otros ataques que afectan algún tipo de vulnerabilidad de la red.



LICENCIA

Serial Number	Registered	Model
C0A100VF4YBJX14	09 April 2021	XG86

Subscription	Status	License Number/Product	Expiry Date	Evaluate
Network Protection	Evaluating	Network Protection	09 May 2021	
Web Protection	Evaluating	Web Protection	09 May 2021	
Email Protection	Evaluating	Email Protection	09 May 2021	
Web Server Protection	Evaluating	Webserver Protection	09 May 2021	
Zero-Day Protection	Evaluating	Zero-Day Protection	09 May 2021	
Enhanced Support	Subscribed	L0012239246 / Enhanced Support	12 Apr 2022	
Enhanced Plus Support Upgrade				

POLÍTICA DE SEGURIDAD

El equipo está actualmente configurado para la protección IPS contra todo tipo de amenazas externas, principalmente el ransomware, este malware encripta documentos, archivos personales, críticos y solicita transferir a otros fondos, dinero pero en moneda BitCoin para que la víctima desbloquee sus archivos. El comportamiento similar a un gusano exhibido por este malware se debe a una sonda activa para el puerto 445 (***ya bloqueado en su UTM***) del servidor SMBv1 en la LAN local que busca la presencia de Backdoor.Double.Pulsar. Si la puerta trasera está presente, la carga útil se entrega y se ejecuta a través de este canal. De lo contrario, se toma una ruta de explotación ligeramente menos confiable.

Por lo anterior es importante señalar que esta solucion de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría “Malware Communication”
2. El motor AV habilitado nos ayuda a detectar el malware junto con las variantes
3. El filtro web se habilitó a todos los usuarios sin excepción para bloquear los sitios web que se han identificado como atacantes potenciales
    - Anonymizers
    - Command & Control
    - Phishing & Fraud
    - Spam URLs

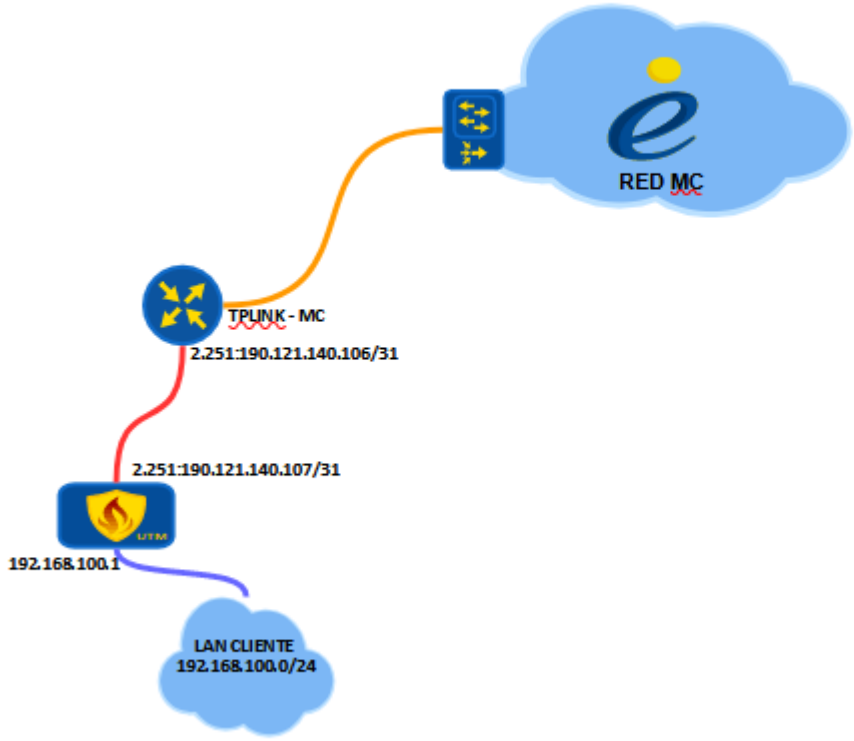
4. Con el control de aplicaciones estamos bloqueando igualmente para todos los usuarios el software Proxy and Tunnel principalmente para cortar cualquier tipo de gestión para la red TOR que es el protocolo de comunicación de los ataques ransomware.

de igual forma ninguna solución es 100% segura y solo estamos protegiendo el perímetro, no tenemos control sobre los dispositivos de almacenamiento que ingresen los usuarios en su computadora, por esto recomendamos en lo posible contar con una buena plataforma de antivirus y software adicionales que permitan controlar estos ataques que están en constante cambio. Si desea asesoría sobre cómo obtener protección adicional para su red LAN con un excelente antivirus o software adicional que le garantice no tener inconvenientes con el secuestro de datos importantes para su compañía puede consultar a nuestro asesor comercial.

Con el usuario y contraseña que le hemos entregado para la administración del equipo puede observar todas las políticas anteriormente mencionadas, le solicitamos por favor validar que la información registrada en este documento sea copia exacta de la configuración entregada en el UTM, si nota alguna anomalía por favor reportarse de inmediato.

ESQUEMA DE SOLUCIÓN, TOPOLOGÍA

Topología CCE-CORPOBOYACA CORPORACIÒN AUTÒNOMA REGIONAL DE BOYACÀ ID_20



MEDIA commerce	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196 Versión. 03
	FORMATO VISITA (SOPORTE)	Página. 1 de 1 Vigencia. Agosto de 2018

CIUDAD:	MIRAFLORES	FECHA: 25-03-21	HORA INICIAL:	12:00	HORA FINAL: 14:20.
CLIENTE:	CCE CORPOBOYACA		SUBCLIENTE:	PIA	
TICKET ACTIVIDAD:	OT 179907 179906		DIRECCION:	CRA 12 # 2-05	

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

[X] SOPORTE	[ ] ASEGURAMIENTO	[ ] NODOS INALAMBRICOS
[ ] APROVISIONAMIENTO	[ ] PROYECTOS INALAMBRICOS	[ ] NODOS INTERCONEXION

REPORTE DE ACTIVIDADES:

Visita técnica para instalación de equipo UTM Solicitud área de PEM.

REPORTE TECNICO: Se realiza visita y se procede a instalar Equipo UTM Sophos XG 86 SN C0A100VF4YBJX14. con patch cord UTM conetado al puerto WAN (2) y conectando red LAN pto (3). Se informa a compañera Yessica para que realiza las respectivas Configuraciones en conjunto con la Ing Leydy Guacheta. y el Ing Alfredo. (cliente.)

Se confirma visita y servicio operativo con cliente, se deja canal activo wifi activo por solicitud del cliente y con autorización del Ing Jimmy Baena.

ESTADO DE LA NOVEDAD:	SOLUCIONADA	X	EN PROCESO		PENDIENTE		OTRA	

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE	FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S
Nombre: Magaly Molina	Nombre: Angelica Fonseca
C.C.: 1'057411840	C.C.: 1049640115
N° TELEFONICO: 3152661779	N° TELEFONICO: 320 6888987