

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 provisionado, 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#
```

[illegible]

```
CCE-CORPOBOYACA ID#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

1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67
 68
 69
 70
 71
 72
 73
 74
 75
 76
 77
 78
 79
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
 100
 101
 102
 103
 104
 105
 106
 107
 108
 109
 110
 111
 112
 113
 114
 115
 116
 117
 118
 119
 120
 121
 122
 123
 124
 125
 126
 127
 128
 129
 130
 131
 132
 133
 134
 135
 136
 137
 138
 139
 140
 141
 142
 143
 144
 145
 146
 147
 148
 149
 150
 151
 152
 153
 154
 155
 156
 157
 158
 159
 160
 161
 162
 163
 164
 165
 166
 167
 168
 169
 170
 171
 172
 173
 174
 175
 176
 177
 178
 179
 180
 181
 182
 183
 184
 185
 186
 187
 188
 189
 190
 191
 192
 193
 194
 195
 196
 197
 198
 199
 200
 201
 202
 203
 204
 205
 206
 207
 208
 209
 210
 211
 212
 213
 214
 215
 216
 217
 218
 219
 220
 221
 222
 223
 224
 225
 226
 227
 228
 229
 230
 231
 232
 233
 234
 235
 236
 237
 238
 239
 240
 241
 242
 243
 244
 245
 246
 247
 248
 249
 250
 251
 252
 253
 254
 255
 256
 257
 258
 259
 260
 261
 262
 263
 264
 265
 266
 267
 268
 269
 270
 271
 272
 273
 274
 275
 276
 277
 278
 279
 280
 281
 282
 283
 284
 285
 286
 287
 288
 289
 290
 291
 292
 293
 294
 295
 296
 297
 298
 299
 300
 301
 302
 303
 304
 305
 306
 307
 308
 309
 310
 311
 312
 313
 314
 315
 316
 317
 318
 319
 320
 321
 322
 323
 324
 325
 326
 327
 328
 329
 330
 331
 332
 333
 334
 335
 336
 337
 338
 339
 340
 341
 342
 343
 344
 345
 346
 347
 348
 349
 350
 351
 352
 353
 354
 355
 356
 357
 358
 359
 360
 361
 362
 363
 364
 365
 366
 367
 368
 369
 370
 371
 372
 373
 374
 375
 376
 377
 378
 379
 380
 381
 382
 383
 384
 385
 386
 387
 388
 389
 390
 391
 392
 393
 394
 395
 396
 397
 398
 399
 400
 401
 402
 403
 404
 405
 406
 407
 408
 409
 410
 411
 412
 413
 414
 415
 416
 417
 418
 419
 420
 421
 422
 423
 424
 425
 426
 427
 428
 429
 430
 431
 432
 433
 434
 435
 436
 437
 438
 439
 440
 441
 442
 443
 444
 445
 446
 447
 448
 449
 450
 451
 452
 453
 454
 455
 456
 457
 458
 459
 460
 461
 462
 463
 464
 465
 466
 467
 468
 469
 470
 471
 472
 473
 474
 475
 476
 477
 478
 479
 480
 481
 482
 483
 484
 485
 486
 487
 488
 489
 490
 491
 492
 493
 494
 495
 496
 497
 498
 499
 500
 501
 502
 503
 504
 505
 506
 507
 508
 509
 510
 511
 512
 513
 514
 515
 516
 517
 518
 519
 520
 521
 522
 523
 524
 525

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



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

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

DESCRIPCIÓN DE LA SOLICITUD DE VISITA TÉCNICA

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

REPORTE DE ACTIVIDADES:

→ Visita técnica 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 SIN 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 el cliente y retiro de la sede.

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

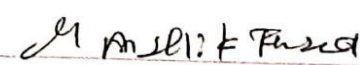
ESTADO DE LA NOVEDAD: SOLUCIONADA ☒ EN PROCESO PENDIENTE OTRA

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE


 Nombre: Alfredo Ojeda
 C.C.: 7.171.355
 N° TELEFONICO: 310 359 6302

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S


 Nombre: Angelica Fonseca
 C.C.: 1049640115
 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: 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
17859 2	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 provisionado, 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

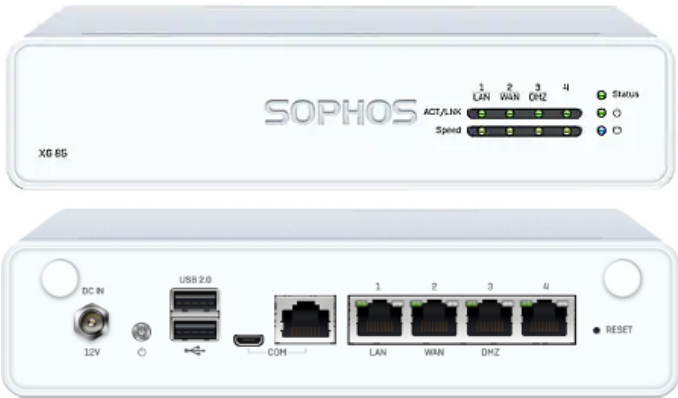
CCE-CORPOBOYACA_ID2#
```

[illegible]

Equipos instalados

Se relacionan los equipos adecuados para la prestación de los servicios

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

AllVLANREDAdd interface				
Interface		Status/Interface speed	IP address	Misc
 GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static		
 Port1 LAN Physical	Unplugged Auto-negotiated	172.16.16.16/255.255.255.0 Static		
 Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	181.225.70.237/255.255.255.254 Static		
 Port3 LAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	192.168.12.1/255.255.255.0 Static		
 Port4 Unbound Physical	Disabled Auto-negotiated	N/A		

☐ ENRUTAMIENTO

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

IPv4 gateway							
AddDelete							
☐	Name 	IP address	Interface	Health check	NAT policy	Status	Manage
☐	INTERNET_MC	181.225.70.236	Port2	On	MASQ		

❑ 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.

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters		
Name		Description					In use	Manage			
	Default Policy	A typical starter policy with options suitable for many organizations					0				
	Bloq_General						1				
	Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments					0				
	No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites					0				
	No Explicit Content	Deny access to sexually explicit sites					0				
	No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites					0				
	No Online Chat	Deny access to online chat sites					0				
	No Web Mail	Deny access to web mail sites					0				
	No Web Mail or Chat	Deny access to web mail and online chat sites					0				
	No web uploads	Restrict users from uploading content to any site					0				

❑ 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.

Application filter	Synchronized Application Control	Application list	Traffic shaping default
Name Default action	Description		
Allow All	Allow	Allow All Policy.	
<u>Block filter avoidance apps</u>	Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse internet by connecting to servers on the internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
<u>Block generally unwanted apps</u>	Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
<u>Block high risk (Risk Level 4 and 5) apps</u>	Allow	Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
<u>Block peer to peer (P2P) networking apps</u>	Allow	Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
<u>Block very high risk (Risk Level 5) apps</u>	Allow	Drops traffic that are classified under very high risk apps (Risk Level- 5).	
Deny All	Deny	Deny All Policy.	

☐ 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.

XG Firewall

MONITOR & ANALYZE

Control center

Current activities

Diagnostics

PROTECT

Firewall

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Advanced threat

Central synchronization

Firewall

How-to guides Log viewer Help admin ▾

Media Commerce Partners

IPv4 IPv6 Enable filter

+ Add firewall rule

ID	Name	Source	Destination	What	Action	Features
1	LAN to WAN	in 128.84 GB, out 16.55 GB				

☐ LICENCIA

Serial Number	Registered	Model
COA100R6MB6WVF2	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 solución de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

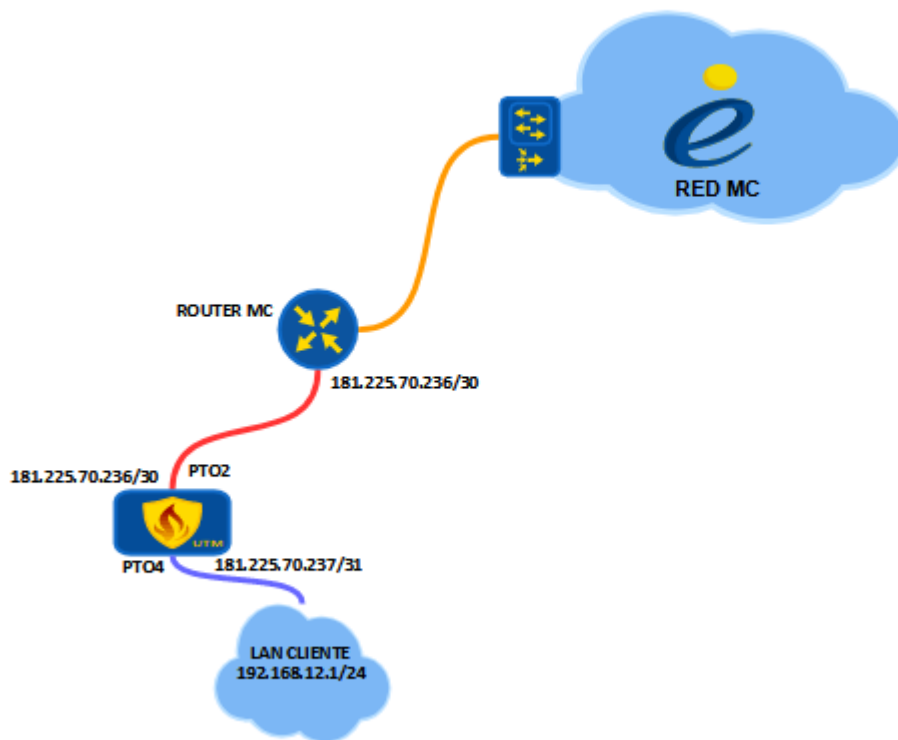
1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría "Malware Communication"
2. El motor AV habilitado nos ayuda a detectar el 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



CIUDAD: TUNJA FECHA: 05-03-21 HORA INICIAL: 16:10 HORA FINAL: 16:40
 CLIENTE: CORPORACION AUTONOMA D.B. 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 serie 1 COA 100R6MB6WVF2. 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 ☒ EN PROCESO ☐ PENDIENTE ☐ OTRA ☐

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE

Nombre:

C.C.:

N° TELEFONICO:

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S

Nombre:

C.C.:

N° TELEFONICO:

7 171-355

810 559 6362

Angelica Fonseca

Angelica Fonseca

1049640115

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

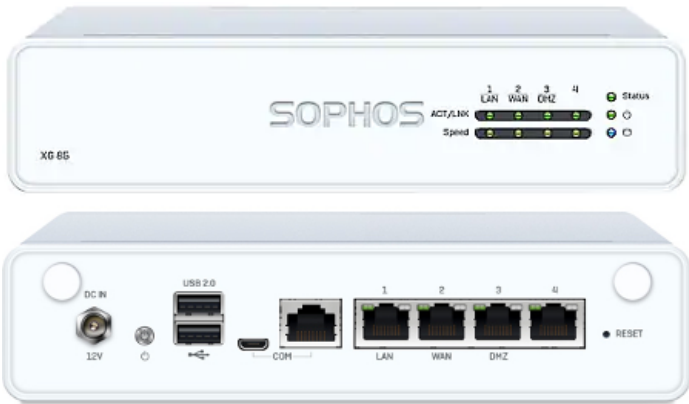
CCE-CORPOBOYACA_ID3#
```

[illegible]

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	C0A100VPG2P32E	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

Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement	Cellular WAN	IP tunnels	Neighbors (ARP-NDP)	Dynamic DNS
AllVLANRED Add interface									
Interface		Status/Interface speed	IP address		Misc				
	GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static						
	Port1 LAN Physical	Unplugged Auto-negotiated	172.16.16.16/255.255.255.0 Static						
	Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	190.121.140.105/255.255.255.0 Static						
	Port3 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.10.1/255.255.255.0 Static						
	Port4 Unbound Physical	Disabled Auto-negotiated	N/A						

□ ENRUTAMIENTO

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

Static routing	Policy routing	Gateways	BGP	OSPF	Information	Upstream proxy	Multicast (PIM-SM)	RIP
IPv4 gateway								
AddDelete								
☐	Name 	IP address	Interface	Health check	NAT policy	Status	Manage	
☐	INTERNET_MC	190.121.140.104	Port2	On	MASQ			

□ 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.

Policies

User activities

Categories

URL groups

Exceptions

General settings

File types

Surfing quotas

User notifications

Content filters

Policy test

Add policy

Name	Description	In use	Manage
+ Default Policy	A typical starter policy with options suitable for many organizations	0 ▲	+ ⌂ ✎ 🗑
+ Bloq_General	pornografía y juegos de azar, mintic	1	+ ⌂ ✎ 🗑
+ Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	0 ▲	+ ⌂ ✎ 🗑
+ No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites	0 ▲	+ ⌂ ✎ 🗑
+ No Explicit Content	Deny access to sexually explicit sites	0 ▲	+ ⌂ ✎ 🗑
+ No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites	0 ▲	+ ⌂ ✎ 🗑
+ No Online Chat	Deny access to online chat sites	0 ▲	+ ⌂ ✎ 🗑
+ No Web Mail	Deny access to web mail sites	0 ▲	+ ⌂ ✎ 🗑
+ No Web Mail or Chat	Deny access to web mail and online chat sites	0 ▲	+ ⌂ ✎ 🗑
+ No web uploads	Restrict users from uploading content to any site	0 ▲	+ ⌂ ✎ 🗑

□ 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.

Application filter	Synchronized Application Control	Application list	Traffic shaping default
☐ Name ☐ Default action			
☐ Allow All			
☐ Block filter avoidance apps			
☐ Block generally unwanted apps			
☐ Block high risk (Risk Level 4 and 5) apps			
☐ Block peer to peer (P2P) networking apps			
☐ Block very high risk (Risk Level 5) apps			
☐ Bloq_pornografía juegos			
☐ Deny All			

□ 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.

MONITOR & ANALYZE
Control center
Current activities
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless

Firewall

How-to guides Log viewer Help admin Media Commerce Partners

IPv4 IPv6 Enable filter Add firewall rule

ID	Name	Source	Destination	What	Action	Features
1	INTERNET GENERAL in 10.03 GB, out 558.54 MB	LAN, Any host	WAN, Any host	Any service	Accept	AV WEB APP QoS IHB RE NAT LOG IPS

□ LICENCIA

Serial Number	Registered	Model
COA100VPG2P32E	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 solución de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

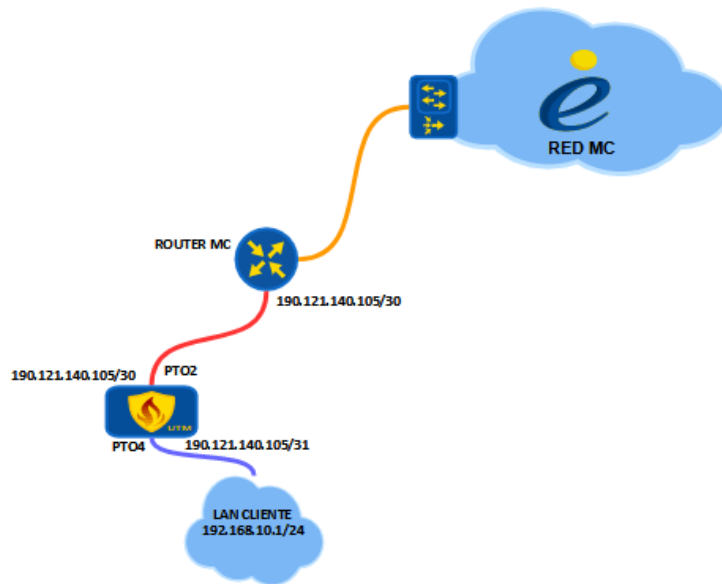
1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría "Malware Communication"
2. El motor AV habilitado nos ayuda a detectar el 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



	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-196
	FORMATO VISITA (SOPORTE)	Versión. 03
		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 Soplos XFA 86 SIN COA100UPFA2P32E. Se valida gestión y servicio, con el cliente conectando el PC directamente al UTM.
 → Se confirma servicio operativo con cliente y con Ing Herran,

ESTADO DE LA NOVEDAD: SOLUCIONADA X EN PROCESO PENDIENTE OTRA

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE

Nombre:

C.C.:

N° TELEFONICO:


 Alfredo Quijela Peña
 7 171 355
 310 559 6302

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S

Nombre:

C.C.:

N° TELEFONICO:


 Angelica Fonseca
 1049640115
 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
17874 6	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 provisionado, 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#
```

[illegible]

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	C0A100XFTBXXC5	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

MONITOR & ANALYZE Control center Current activities Diagnostics	Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDP) Dynamic DNS									
	All VLAN RED Add interface ▼									
PROTECT Firewall Intrusion prevention Web Applications Wireless Email Web server Advanced threat Central synchronization	Interface Status/Interface speed IP address Misc									
CONFIGURE VPN Network Routing Authentication System services										
SYSTEM Profiles Hosts and services Administration Backup & firmware Certificates										

□ ENRUTAMIENTO

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

MONITOR & ANALYZE Control center Current activities Diagnostics	Static routing Policy routing Gateways BGP OSPF Information Upstream proxy Multicast (PIM-SM) RIP								
	IPv4 gateway								
PROTECT Firewall Intrusion prevention Web Applications Wireless Email Web server Advanced threat Central synchronization									
CONFIGURE VPN Network Routing Authentication									

□ 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.

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

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters		
	Default Policy	A typical starter policy with options suitable for many organizations					1				
	Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments					0				
	No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites					0				
	No Explicit Content	Deny access to sexually explicit sites					0				
	No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites					0				
	No Online Chat	Deny access to online chat sites					0				
	No Web Mail	Deny access to web mail sites					0				
	No Web Mail or Chat	Deny access to web mail and online chat sites					0				
	No web uploads	Restrict users from uploading content to any site					0				

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.

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	Application filter		Synchronized Application Control		Application list		Traffic shaping default	

☐ 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.

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

IPv4 IPv6 Enable filter

+ Add firewall rule

ID	Name	Source	Destination	What	Action	Features
4	Internet General in 24.53 GB, out 1.99 GB	LAN, Any host	WAN, Any host	Any service	Accept	AV WEB APP IDS I H6 URL NAT LOG IPS

☐ LICENCIA

Serial Number	Registered	Model
COA100XFTBXXC5	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 solución de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

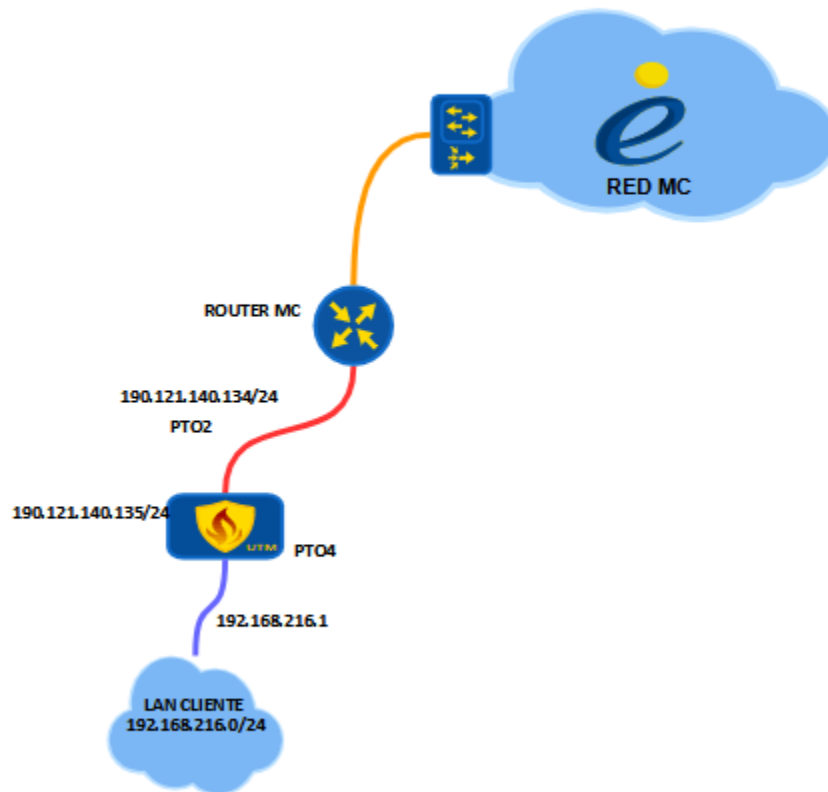
1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría "Malware Communication"
2. El motor AV habilitado nos ayuda a detectar el 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 CORPORACION AUTONOMA REGIONAL DE BOYACA ID_10



CIUDAD: SOCHA FECHA: 26-03-21 HORA INICIAL: 12:00 HORA FINAL: 14:00
 CLIENTE: CCE CORPOBOYACA SUBCLIENTE: N/A
 TICKET ACTIVIDAD: 01 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 técnica para instalación de equipo solicitud del área PEM.

REPORTE TECNICO: → Se realiza visita y se instala equipo UTM Sophos SIN COA100XFBXXXCS 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

Dayssy Santos

Nombre:

Dayssy Liliana Santos F.

C.C.:

1.056.552.432

N° TELEFONICO:

3214021334.

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S

Angelica Fonseca

Nombre:

Angelica Fonseca

C.C.:

1049640115

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
17874 7	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

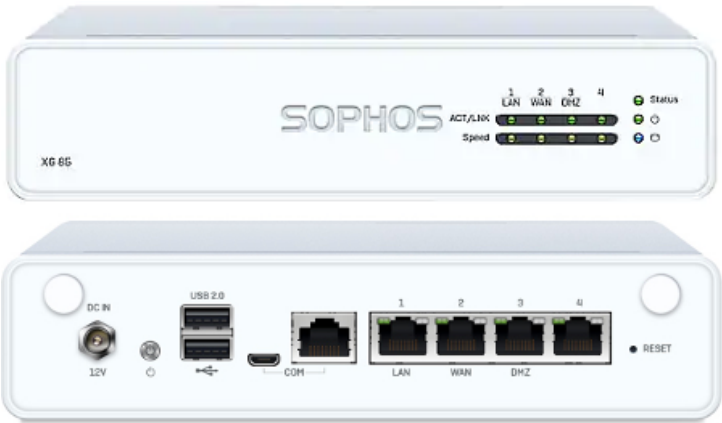
CCE_CORPOBOYACA_ID7#
```

[illegible]

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

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

Interfaces

Zones

WAN link manager

DNS

DHCP

IPv6 router advertisement

Cellular WAN

IP tunnels

Neighbors (ARP-NDP)

Dynamic DNS

All

VLAN

RED

Add interface

Interface	Status/Interface speed	IP address	Misc
 QuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
 Port1 LAN Physical	Unplugged Auto-negotiated	172.16.16.16/255.255.255.0 Static	
 Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	181.225.70.239/255.255.255.0 Static	
 Port3 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.100.1/255.255.255.0 Static	
 Port4 Unbound Physical	Disabled Auto-negotiated	N/A	

☐ ENRUTAMIENTO

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

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

Static routing

Policy routing

Gateways

BGP

OSPF

Information

Upstream proxy

Multicast (PIM-SM)

RIP

IPv4 gateway

Add

Delete

☐	Name	IP address	Interface	Health check	NAT policy	Status	Manage
☐	<u>Internet MC</u>	181.225.70.238	Port2	On	MASQ		

IPv6 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.

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

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters		
	Default Policy	A typical starter policy with options suitable for many organizations					1				
	Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments					0				
	No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites					0				
	No Explicit Content	Deny access to sexually explicit sites					0				
	No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites					0				
	No Online Chat	Deny access to online chat sites					0				
	No Web Mail	Deny access to web mail sites					0				
	No Web Mail or Chat	Deny access to web mail and online chat sites					0				
	No web uploads	Restrict users from uploading content to any site					0				

☐ 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.

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	Application filter		Synchronized Application Control	Application list	Traffic shaping default
	☐	Name	Default action	Description	Manage
	☐	Allow All	Allow	Allow All Policy.	
	☐	<u>Block filter avoidance apps</u>	Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
	☐	<u>Block generally unwanted apps</u>	Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
	☐	<u>Block high risk (Risk Level 4 and 5) apps</u>	Allow	Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
	☐	<u>Block peer to peer (P2P) networking apps</u>	Allow	Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
	☐	<u>Block very high risk (Risk Level 5) apps</u>	Allow	Drops traffic that are classified under very high risk apps (Risk Level- 5).	
	☐	Deny All	Deny	Deny All Policy.	

□ 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.

The screenshot shows the Palo Alto Networks firewall configuration interface. On the left is a sidebar with navigation options: MONITOR & ANALYZE (Control center, Current activities, Diagnostics) and PROTECT (Firewall, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced threat). The main area displays two firewall rules under the 'IPv4' tab.

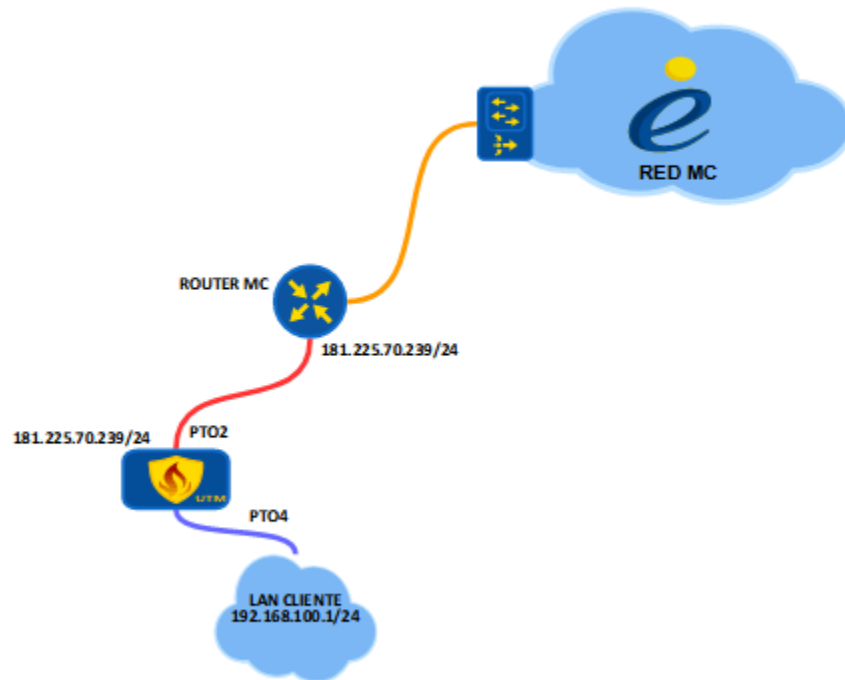
ID	Name	Source	Destination	What	Action	Features
1	LAN to WAN in 803.43 MB, out 303.49 MB					
4	Internet General in 803.43 MB, out 303.49 MB	LAN, Any host	WAN, Any host	Any service	Accept	AV, WEB, APP, DCS, HB, RL, NAT, LOG, IPS

□ LICENCIA

Serial Number	Registered	Model
COA100R8TF6M634	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	-



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

CIUDAD: COATEA FECHA: 23-03-21 HORA INICIAL: 12:00 HORA FINAL: 15:00
 CLIENTE: CCE CORPOBOYACIT SUBCLIENTE: NIA
 TICKET ACTIVIDAD: OT 179843 - 179844 DIRECCION: CL 11 # 4-45

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

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

REPORTE DE ACTIVIDADES:

➤ Visita técnica 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 COA100R8TF6H634, con 2 patch cord UTM, uno instalado a nivel LAN y otro a nivel WAN.

➤ Se presentan problemas de gestión por lo que se realizan descarte de primer nivel y se evidencia que es posible daño de POE o patch cord hacia la antena se reparte al área encargada para su validación.

➤ Se confirma visita e instalación de UTM con cliente y se informa a la compañera Yessica Gomez.

ESTADO DE LA NOVEDAD: SOLUCIONADA EN PROCESO ☒ 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 al incidente al centro de gestión y al Inq. Alfredo, Orjuela. quedamos a la espera de Asistente Técnico.

FIRMA FUNCIONARIO CLIENTE

Nombre: Nancy Milena Uelandia Leal
 C.C.: 40.039.613

N° TELEFONICO:
 3112328287

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S

Nombre: Angelica Fonseca
 C.C.: 1049640115

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

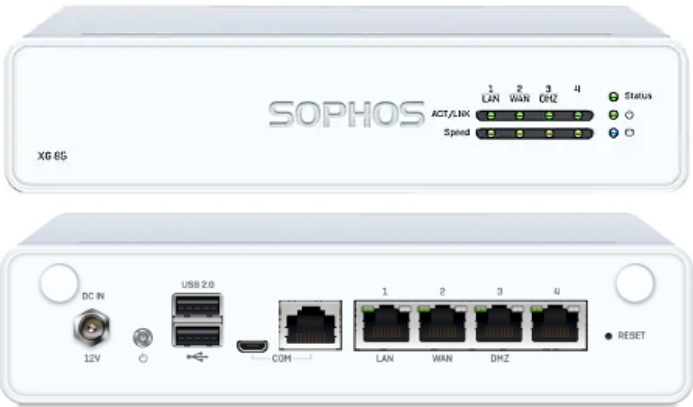
CCE_CORPOBOYACA#
```

[illegible]

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

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

Interfaces

Zones

WAN link manager

DNS

DHCP

IPv6 router advertisement

Cellular WAN

IP tunnels

Neighbors (ARP-NDP)

Dynamic DNS

All

VLAN

RED

Add interface

Interface	Status/Interface speed	IP address	Misc
 GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
 Port1 LAN Physical	Unplugged Auto-negotiated	172.16.16.16/255.255.255.0 Static	
 Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	190.121.140.109/255.255.255.0 Static	
 Port3 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated	192.168.100.1/255.255.255.0 Static	
 Port4 Unbound Physical	Disabled Auto-negotiated	N/A	

☐ ENRUTAMIENTO

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

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

Static routing

Policy routing

Gateways

BGP

OSPF

Information

Upstream proxy

Multicast (PIM-SM)

RIP

IPv4 gateway

Add

Delete

☐	Name	IP address	Interface	Health check	NAT policy	Status	Manage
☐	<u>WAN TO CISCO</u>	190.121.140.108	Port2	On	MASQ	●	

IPv6 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.

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

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters		
	Default Policy	A typical starter policy with options suitable for many organizations					0				
	Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments					0				
	No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites					0				
	No Explicit Content	Deny access to sexually explicit sites					0				
	No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites					0				
	No Online Chat	Deny access to online chat sites					0				
	No Web Mail	Deny access to web mail sites					0				
	No Web Mail or Chat	Deny access to web mail and online chat sites					0				
	No web uploads	Restrict users from uploading content to any site					0				

☐ 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.

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	Application filter		Synchronized Application Control	Application list	Traffic shaping default
	☐	Name	Default action	Description	Manage
	☐	Allow All	Allow	Allow All Policy.	
	☐	<u>Block filter avoidance apps</u>	Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
	☐	<u>Block generally unwanted apps</u>	Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
	☐	<u>Block high risk (Risk Level 4 and 5) apps</u>	Allow	Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
	☐	<u>Block peer to peer (P2P) networking apps</u>	Allow	Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
	☐	<u>Block very high risk (Risk Level 5) apps</u>	Allow	Drops traffic that are classified under very high risk apps (Risk Level- 5).	
	☐	Deny All	Deny	Deny All Policy.	

□ 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.

MONITOR & ANALYZE
Control center
Current activities
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server

IPv4 IPv6 Enable filter

Add firewall rule

ID	Name	Source	Destination	What	Action	Features
1	INTERNET_GENERAL in 2.19 GB, out 538.23 MB	LAN, Any host	WAN, Any host	Any service	Accept	AV WEB APP IPS NAT LOG

□ LICENCIA

Serial Number	Registered	Model
COA100VT26994AE	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 solución de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

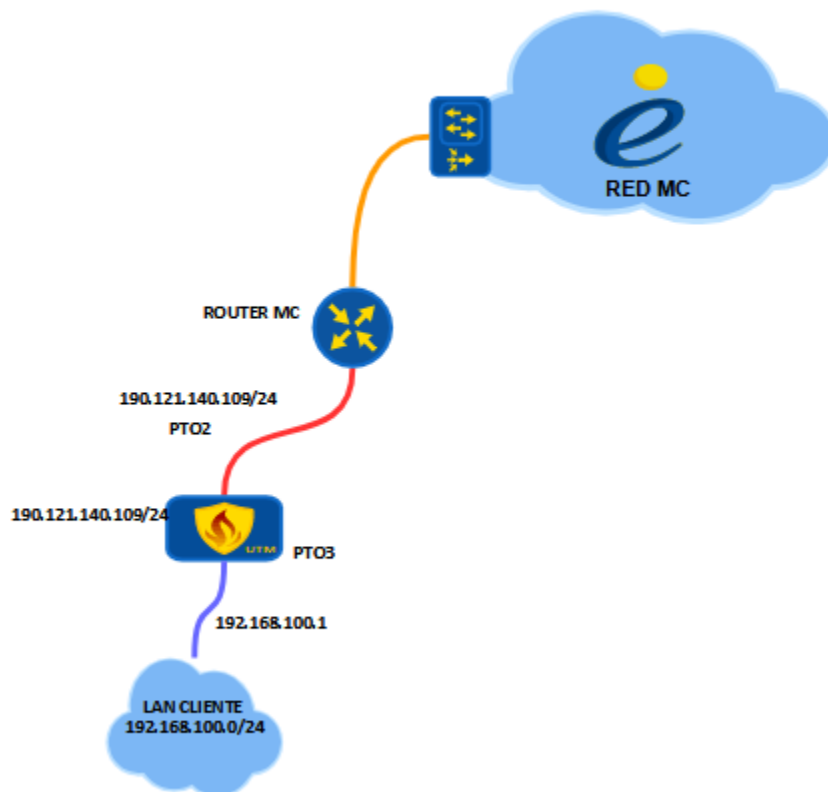
1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría "Malware Communication"
2. El motor AV habilitado nos ayuda a detectar el 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

Topologia CCE-CORPOBOYACA CORPORACIÓN AUTÓNOMA REGIONAL DE BOYACÁ ID_22



CIUDAD: PAUNA FECHA: 02-03-21 HORA INICIAL: 11:00 HORA FINAL: 14:00
 CLIENTE: CORPORACION AUTONOMA BY SUBCLIENTE: N/A
 TICKET ACTIVIDAD: OT 178596 DIRECCION: CIL 5 #05-05 P. 202

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

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

REPORTE DE ACTIVIDADES:

→ Visita tecnica para instalacion de equipos pbr solicitud del area de PEM.

REPORTE TECNICO: → Se realiza visita se procede a instalar equipo CISCO 1841 S/N FTX1030W0V1 y switches XA86 S/N COA100UT2699 9AE.

Se valida configuración con la Ing Leydy Guacheta, se instala 2 pto 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 ☒ EN PROCESO ☐ PENDIENTE ☐ OTRA ☐

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE

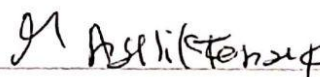


Nombre: WLP Cepeda A.

C.C.: 1053330684.

N° TELEFONICO: 3133874000

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S



Nombre: Angelica Fonseca

C.C.: 1049640115

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.

DHCP Server

IP Version:	☒ IPv4 ☐ IPv6
MAC Address:	60-32-B1-7D-8F-78
IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255.255.255.0 ▼
IGMP Snooping:	☒ Enable
Second IP:	☐ Enable
DHCP:	☒ Enable
	☒ DHCP Server ☐ DHCP Relay
IP Address Pool:	192 . 168 . 1 . 100 - 192 . 168 . 1 . 199
Address Lease Time:	1440 minutes. (1-2880. The default value is 1440.)
Default Gateway:	192 . 168 . 1 . 1 (Optional)
Default Domain:	(Optional)

PPP Secret <45884>

Name:	45884	OK
Password:	xxxxxx ▲	Cancel
Service:	pppoe ▼	Apply
Caller ID:	▼	Disable
Profile:	6 Mbps 1:1 ▼	Comment
Local Address:	▼	Copy
Remote Address:	▼	Remove
Routes:	▼	
Limit Bytes In:	▼	
Limit Bytes Out:	▼	
Last Logged Out:	Apr/05/2021 08:19:47	

enabled

Diagnostic Tools

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

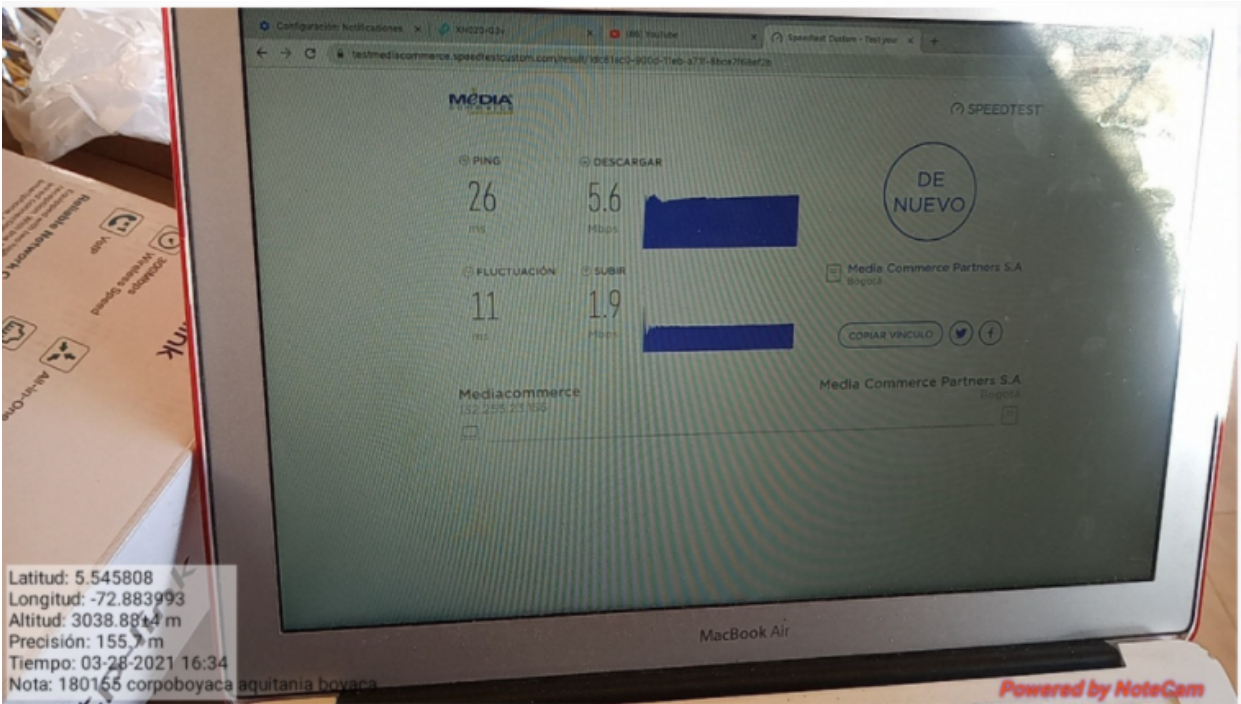
Diagnostic Type

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

[illegible]

Ping a CPE

```
64 bytes from 172.20.1.25: icmp_seq=501 ttl=60 time=9.61 ms
64 bytes from 172.20.1.25: icmp_seq=502 ttl=60 time=9.59 ms
64 bytes from 172.20.1.25: icmp_seq=503 ttl=60 time=9.61 ms
^C
--- 172.20.1.25 ping statistics ---
503 packets transmitted, 503 received, 0% packet loss, time 100916ms
rtt min/avg/max/mdev = 9.404/12.340/45.488/5.538 ms, ipg/ewma 201.028/9.701 ms
[ayazrce@LENOVO-LA0X1017 rconfig]#
```

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



	GESTIÓN OPERATIVA Y PROYECTOS	Código. GOP-F-198 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 -> DOMOSO		

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

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

REPORTE DE ACTIVIDADES:

➔ Visita técnica para instalación de equipo UTM solicitud área de TCM.

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 con COA100VQY99DOB con caja original y accesorios necesarios.

ESTADO DE LA NOVEDAD:	EN PROCESO	PENDIENTE	OTRA
-----------------------	------------	-----------	------

OBSERVACIONES DEL CLIENTE:

FIRMA FUNCIONARIO CLIENTE

Nadra A. Topia U.

Nombre: Nadia Alexandra Topia Uscategui

C.C.: 1.053.584.752

N° TELEFONICO: 3112963966.

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S



Nombre: Angelica Fonseca

C.C.: 1049640115

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.

DHCP Server

IP Version:	☒ IPv4 ☐ IPv6
MAC Address:	84-D8-1B-74-28-18
IP Address:	192 . 168 . 100 . 1
Subnet Mask:	255.255.255.0
IGMP Snooping:	☒ Enable
Second IP:	☐ Enable
DHCP:	☒ Enable
	☒ DHCP Server ☐ DHCP Relay
IP Address Pool:	192 . 168 . 100 . 100 - 192 . 168 . 100 . 199
Address Lease Time:	1440 minutes. (1-2880. The default value is 1440.)
Default Gateway:	192 . 168 . 100 . 1 (Optional)

PPP Secret <48171>

Name:	48171	OK
Password:	xxxxxx	Cancel
Service:	pppoe	Apply
Caller ID:		Disable
Profile:	22_Downlink_22_Uplink	Comment
Local Address:		Copy
Remote Address:		Remove
Routes:		
Limit Bytes In:		
Limit Bytes Out:		
Last Logged Out:	Mar/06/2021 20:47:09	
enabled		

Diagnostic Tools

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

Diagnostic Type

Test Internet surfing

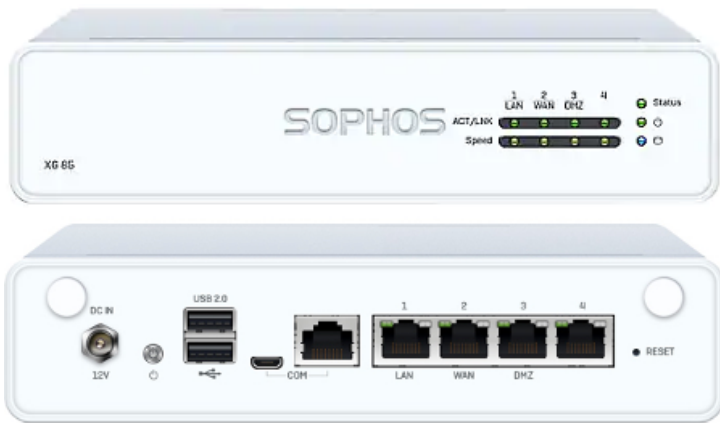
Start

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	C0A100VFPFG2P32E	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

Interfaces		Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement	Cellular WAN	IP tunnels	Neighbors (ARP-NDP)	Dynamic DNS
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		GuestAP WiFi Wireless protection	Unplugged Auto-negotiated		10.255.0.1/255.255.255.0 Static					
		Port1 LAN Physical	Unplugged Auto-negotiated		172.16.16.16/255.255.255.0 Static					
		Port2 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated		10.20.30.1/255.255.255.252 Static					
		Port2.251 WAN VLAN	N/A N/A		190.121.140.107/255.255.255.254 Static					
		Port3 LAN Physical	Connected 1000 Mbps - Full Duplex Auto-negotiated		192.168.100.1/255.255.255.0 Static					
		Port4 Unbound Physical	Disabled Auto-negotiated		N/A					

☐ ENRUTAMIENTO

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

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

Static routing

Policy routing

Gateways

BGP

OSPF

Information

Upstream proxy

Multicast (PIM-SM)

RIP

IPv4 gateway

Name

IP address

Interface

Health check

NAT policy

Status

Manage

Internet MC

190.121.140.106

Port2.251

On

MASQ

IPv6 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.

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

Policies	User activities	Categories	URL groups	Exceptions	General settings	File types	Surfing quotas	User notifications	Content filters		
	Default Policy	A typical starter policy with options suitable for many organizations					0				
	Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments					0				
	No Ads or Explicit Content	Deny access to advertisements and sexually explicit sites					0				
	No Explicit Content	Deny access to sexually explicit sites					0				
	No Games Ads or Explicit Content	Deny access to games, advertisements, and sexually explicit sites					0				
	No Online Chat	Deny access to online chat sites					0				
	No Web Mail	Deny access to web mail sites					0				
	No Web Mail or Chat	Deny access to web mail and online chat sites					0				
	No web uploads	Restrict users from uploading content to any site					0				

☐ 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.

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	Application filter		Synchronized Application Control		Application list		Traffic shaping default	
	☐							
	☐		Name		Default action		Description	
	☐		Allow All		Allow		Allow All Policy.	
	☐		<u>Block filter avoidance apps</u>		Allow		Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
	☐		<u>Block generally unwanted apps</u>		Allow		Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
	☐		<u>Block high risk (Risk Level 4 and 5) apps</u>		Allow		Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
	☐		<u>Block peer to peer (P2P) networking apps</u>		Allow		Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
	☐		<u>Block very high risk (Risk Level 5) apps</u>		Allow		Drops traffic that are classified under very high risk apps (Risk Level- 5).	
	☐		Deny All		Deny		Deny All Policy.	

☐ 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.

MONITOR & ANALYZE
Control center
 Current activities
 Diagnostics
 PROTECT
Firewall
 Intrusion prevention
 Web
 Applications
 Wireless
 Email
 Web server
 Advanced threat
 Central synchronization

IPv4
 IPv6
 Enable filter

+ Add firewall rule

ID	Name	Source	Destination	What	Action	Features
1	LAN to WAN in 3.81 GB, out 348.86 MB					
4	Internet General in 3.81 GB, out 348.86 MB	LAN, Any host	WAN, Any host	Any service	Accept	[AV] [WEB] [APP] [QoS] [H3] [RT] [NAT] [LOG] [IPS]

☐ 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 solución de UTM se ha configurado según los estándares recomendados por el fabricante para prevenir en lo posible estos tipos de ataque

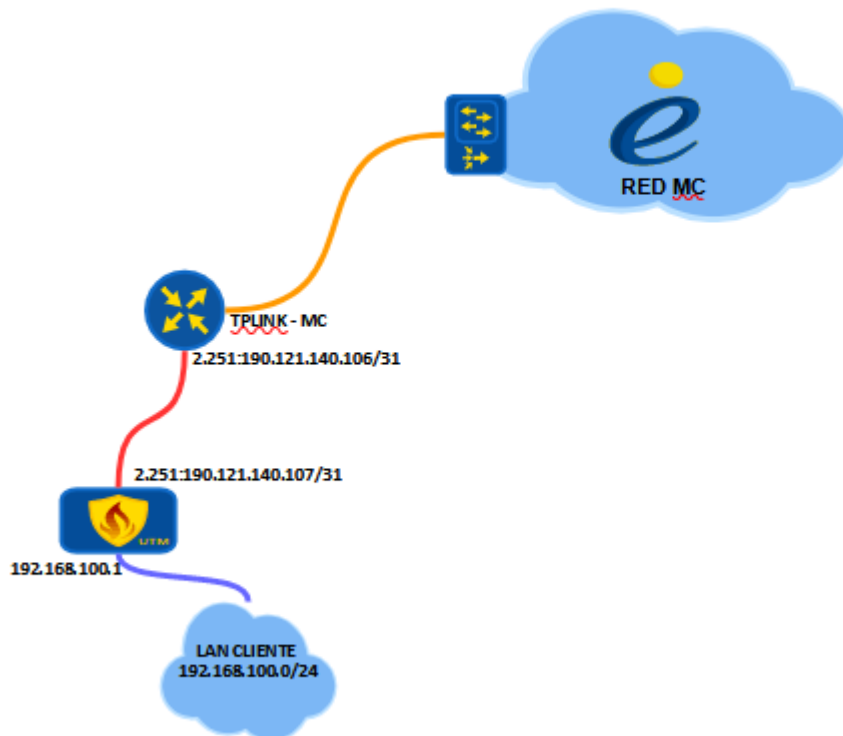
1. Con el motor IPS habilitado estamos conectando el exploit y detectando el comportamiento malicioso, se aplica el perfil sugerido para conexiones entrantes de WAN a LAN y de LAN a WAN enfatizando principalmente en la categoría "Malware Communication"
2. El motor AV habilitado nos ayuda a detectar el 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 BOYACA ID_20



CIUDAD: MIRAFLORES FECHA: 25-03-21 HORA INICIAL: 12:00 HORA FINAL: 14:20.
 CLIENTE: CCE CARPOBOYACA SUBCLIENTE: PIA
 TICKET ACTIVIDAD: 0179907 179906 DIRECCION: CRA 12 # 2-05

DESCRIPCION DE LA SOLICITUD DE VISITA TECNICA

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

REPORTE DE ACTIVIDADES:

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

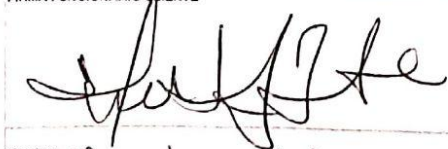
REPORTE TECNICO: Se realiza visita y se procede a instalar equipo
 UTM Sophos XF86 SIN COA100VF4YBJX14 con patch cord UTM conectado
 al puerto WAN (2) y conectando red LAN pto (3). Se informa a
 compañera Yessica para que realiza las respectivas configuraciones
 en conjunto con la Ing Leydy Guacheta, 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

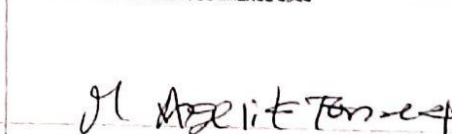


Nombre: Magaly Molina

C.C.: 1057411840

N° TELEFONICO: 315266 1779

FIRMA FUNCIONARIO MEDIA COMMERCE S.A.S



Nombre: Angelica Fonseca

C.C.: 1049640115

N° TELEFONICO: 320 6888987