Documentação API REST

para integração do GSM

Rua: Alexandre Dumas, 1711 - Birmann 11, térreo
Santo Amaro, São Paulo - SP 04717-911 - Brasil
Telefone: + 55 11 2165-8888
www.blockbit.com

ÍNDICE

1. API RESTful do GSM

O GSM utiliza uma *API RESTful (Representational State Transfer)* que consiste em um sistema de constrições arquiteturais de comunicação, que permite a troca de informações entre diferentes sistemas, de maneira segura pela rede. Conta com uma arquitetura orientada a serviços (SOA – *Service Oriented Architecture)* que permite escalabilidade, flexibilidade e facilidade de uso, tendo como principais características:

- ***Uma interface simples;***
- ***Escalabilidade:*** especialmente ao ser combinada com conceitos de micro serviços SOA;
- ***Sustentabilidade:*** enquanto o código da aplicação pode mudar sob a API, sua definição pode permanecer intacta;
- ***Performance:*** interações componentes dominam a performance percebida pelo usuário e a eficiência da API garante acesso aos dados primários disponíveis do sistema central, que também são consumidos para interações de front-end.

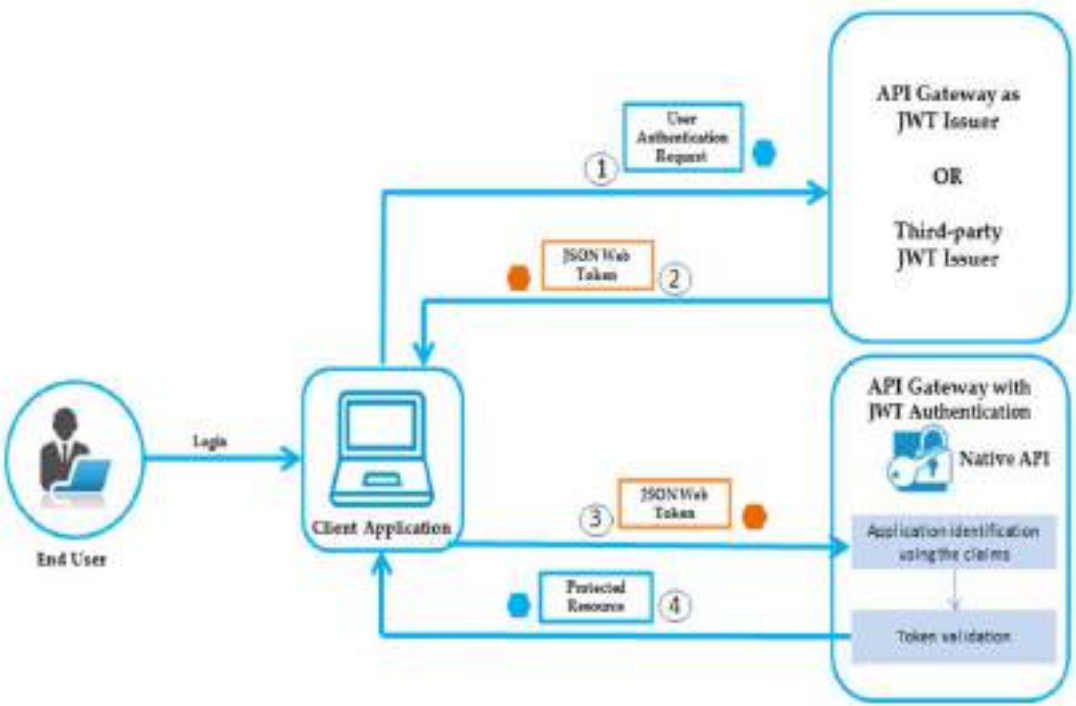
2. Autenticação

Os dados são coletados pela *API REST* em formato JSON. Todas as respostas incluem um código do tipo HTTP response, indicando sucesso ou falha das operações de requisição de dados. Estas requisições são autenticadas por JWT.

As opções são autenticadas por credenciais do tipo *user/password* com a armazenagem de um *token (Session ID)*. Há expiração do token por *aging* (envelhecimento). Isso quer dizer que o token, é um "passe" temporário para uso. Depois de o tempo de *aging* o usuário perde a conexão, pois é feito um *logoff* automático.

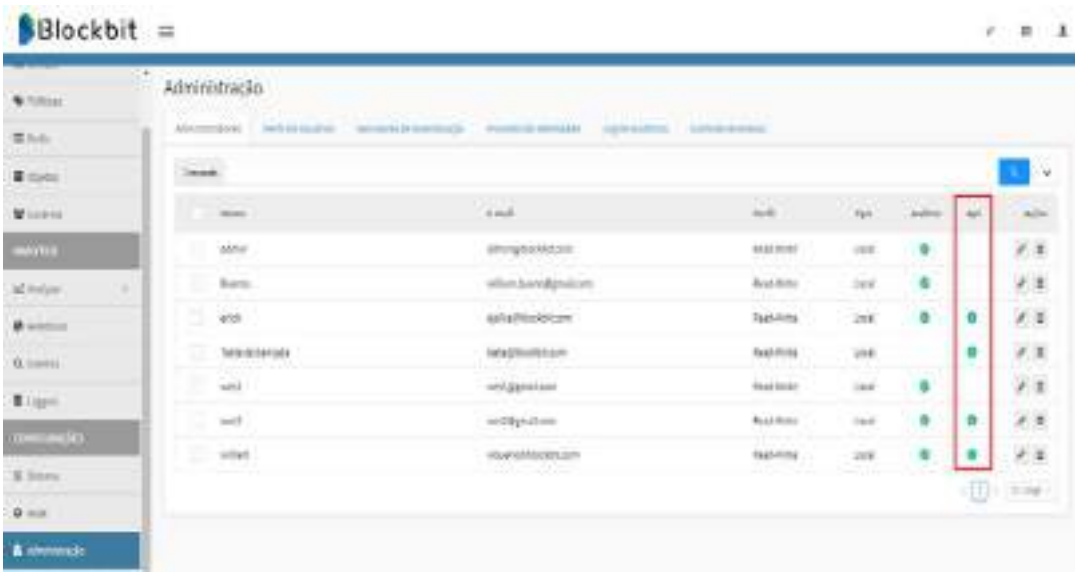
2.1. Fluxo de autorização JWT

O fluxo de solicitações e respostas de autorização entre o usuário final, aplicação cliente, *JWT issuer* e servidor de recursos ocorre conforme a imagem abaixo:

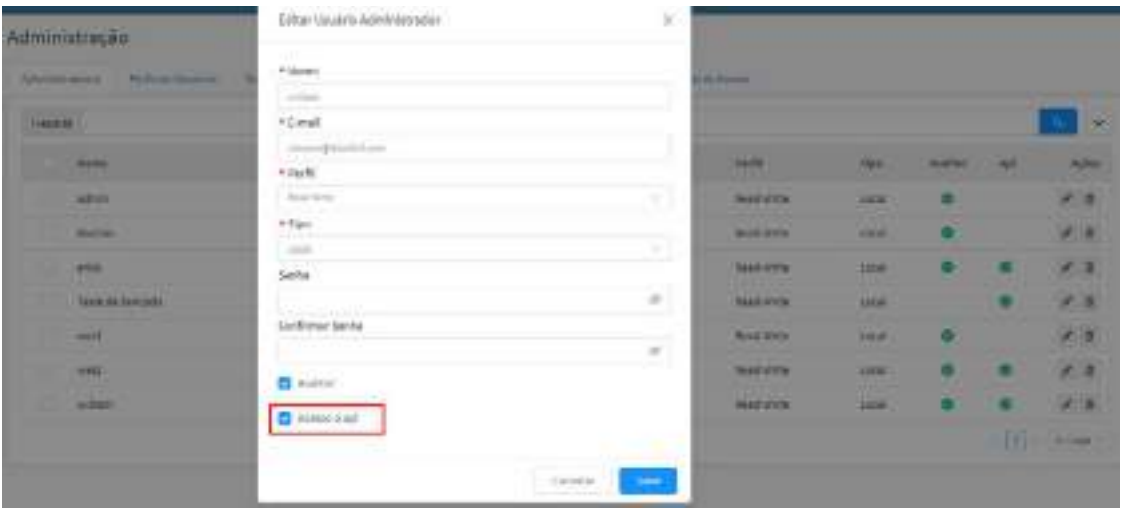


3. Ativação

Em Administração > Administradores encontramos a coluna “API” com a sinalização [ ] para usuários do tipo administrador com a API habilitada.



Para habilitar, basta editar um usuário administrador já existente ou criar um, e marcar a opção “API” conforme a imagem abaixo:



- ***Nome:*** Entre com o nome de usuário do GSM.
- ***E-mail:*** Insira o e-mail do usuário utilizado no login.
- ***Perfil:*** Escolha entre READ-ONLY e READ-WRITE, para moderar a permissão do usuário entre apenas leitura, ou leitura e edição das informações obtidas.
- ***Tipo:*** Escolha entre acesso Local e Remoto (se criado no próprio GSM é local).
- ***Senha:*** Utilize a senha da sessão.
- ***Auditor:*** Usuário administrador com acesso total. Se selecionado limitado, as alterações feitas em sistema por este usuário, passam por um processo de auditoria.
- ***Acesso API:*** Marque esta opção para habilitar a API do GSM, possibilitando assim a acessibilidade a dados de NGFWs.

4. Endpoints

Endpoints são os endereços (URL) que serão acessados pelo sistema nos quais serão realizadas as operações a partir de sua plataforma, por meio da API, com base em "*Requests*" e "*Responses*", diretamente em um terceiro sistema (operando pela porta 3002 do GSM).

Os métodos HTTP suportados pela API do GSM são os seguintes: *GET [Read]*, *POST [Create]* (somente utilizado na autenticação).

Para efeito de testes, exemplificação e ilustração foi utilizada a aplicação "Postman".

4.1. POST (Login)

Para acessar o GSM, é necessário realizar o login. Realize o "POST", na API por meio do request "*auth/login*" e utilize o e-mail e a senha de acesso do GSM para que seja gerado o "*auth token*", e iniciada a sessão.

Request

Tipo	**URL**
POST	auth/login

Parâmetros de Body

Parâmetro	**Tipo**	**Obrigatório**	**Descrição**
email	String	Sim	Admin user email
password	String	Sim	Admin user password

Exemplo de Request

URL

```
POST /auth/login
```

Exemplo de Body de um Request

JSON

```
{
  "email": "user@email.com",
  "password":"abc1234"
}
```

Responses

Sucesso

Parâmetro	Tipo	Descrição
Access_token	String	Um token JWT válido
refresh_token	String	Um refresh token JWT válido
token_type	String	Tipo de Token

Exemplo de Request com sucesso

JSON

```
{
  "access_token": "eyJhbGciOiJIUz...",
  "refresh_token": "eyJhbGciOiJI...",
  "token_type": "bearer"
}
```

Response de erro

Exemplo de Response de erro – 401 Unauthorized (Não autorizado)

JSON

```
{
  "code": 401,
```

```
  "message": "sql: no rows in result set"
}
```

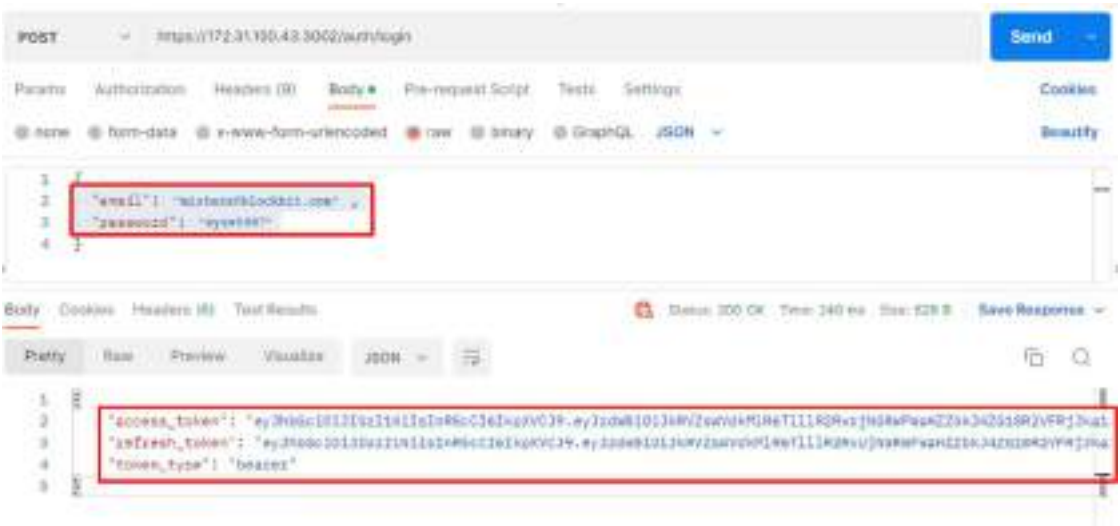
Response de erro – 400 Bad Request (Solicitação Inválida)

JSON

```
{
  "code": 400,
  "message": "Unprocessable Entity"
}
```

Abaixo podemos ver um exemplo de autenticação feita com sucesso, em uma plataforma escolhida para este guia:

Identificação do Login no GSM



Token gerado pelo sistema

4.2. GET (Appliance)

Este *Endpoint* envia uma solicitação com fluxo de "*Request*" / "*Response*" para obter informações acerca dos dispositivos Blockbit NGFW.

Request

Tipo	URL
GET	/api/appliances/list

Header

Chave	Tipo de Token	Valor[1]
Authorization	Bearer	Bearer eyjhbGciOiJIUz...

Exemplo de Request

[1] Este valor corresponde ao token do tipo "bearer" gerado para autenticação, suprimido em nosso exemplo por questões de espaço e paginação, porém presente na imagem anterior a esta tabela.

URL

```
GET /api/appliances/list
```

Filtros

Chave	Tipo	Obrigatório	Descrição
name	String	Não	Nome do dispositivo
Model	String	Não	Nome do modelo do dispositivo

Exemplo de filtros

URL

```
GET /api/appliances/list?name=yourstring&model=yourmodel
```

Paginação

Chave	Tipo	Obrigatório	Descrição
perPage	Int	Não	Linhas por página
page	Int	Não	Página atual

Exemplo de Request de paginação

URL

```
GET /api/appliances/list?page=1&perpage=10
```

Responses

Sucesso

Parâmetro	Tipo	Descrição
Total	Int	Total de dispositivos
perPage	Int	Linhas por página
page	Int	Página atual
items	Items <array>	Variedade de itens

Objetos do tipo item

Estes parâmetros servem para filtrar a pesquisa, permitindo trazer as informações por Id, nome, modelo e mais.

Parâmetro	Tipo	Descrição
id	Int	id do dispositivo
name	String	Nome do dispositivo
model	String	Nome do modelo do dispositivo
license status	String	Status da licença do dispositivo
version	String	Versão do dispositivo
status	String	Status do dispositivo

Exemplo de Response de sucesso – 200 Ok

JSON


```
{
   "data": {
      "total": 0,
      "perPage": 10,
      "page": 1,
      "items": [
         {
            "id": 14,
            "name": "NGFW_2.4.0_192.168.1.18",
            "model": "-",
            "licenseStatus": "true",
            "version": "BLOCKBIT UTM 2.4.0 build 22092212",
            "status": "-1"
         },
         {
            "id": 15,
            "name": "NGFW_2.4.0_172.31.150.48",
            "model": "BBv-10",
            "licenseStatus": "true",
            "version": "BLOCKBIT UTM 2.4.0 build 22092212",
            "status": "1"
         }
      ]
   }
}
```


Responses de Erro

Exemplos de response de erro – 401 Invalid Signature (Assinatura inválida)

JSON

```
{
   "error": true,
   "msg": "signature is invalid"
}
```

Problema com o token – 401 Invalid Token (Token Inválido)

JSON

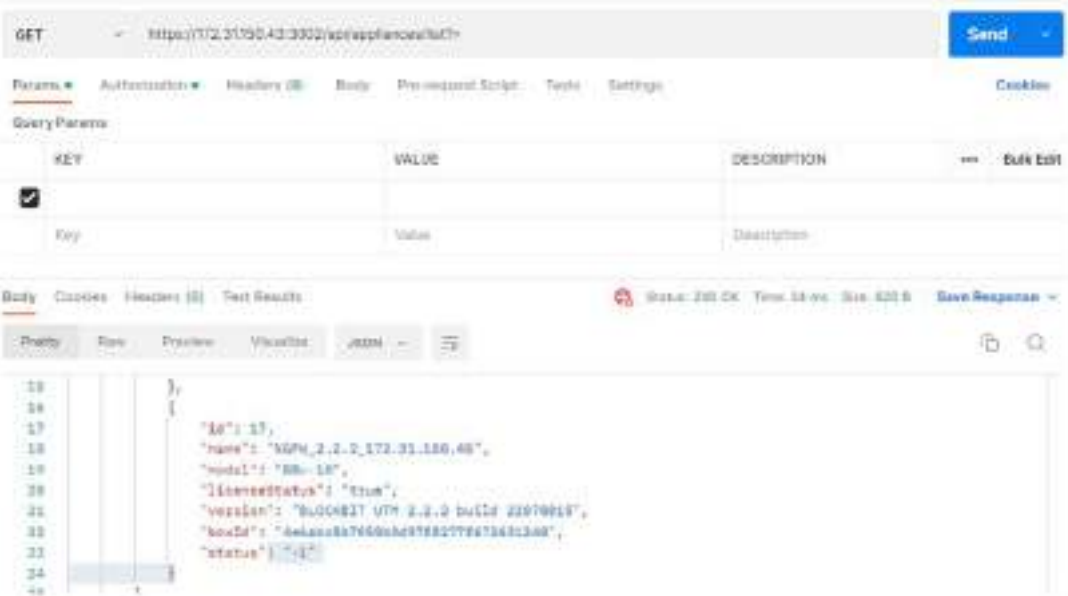
```
{
   "error": true,
   "msg": "token contains an invalid number of segments"
}
```

Token faltando – 400 Token Missing

JSON

```
{
   "error": true,
   "msg": "Missing or malformed JWT"
}
```

A tela a seguir ilustra uma pesquisa contendo as informações de *appliance*:



GET – Appliance query

4.3. GET (Policies)

Este *Endpoint* traz informações como total de tráfego, número de Políticas aplicadas, total de usuários por Política, entre outras, acerca dos Pacotes de Políticas de um Blockbit NGFW por meio do fluxo de Requests e Responses.

Request

Tipo	URL
GET	/api/policies/groups

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhGciOiJIUz...

Exemplo de Request

URL

```
GET /api/policies/groups
```

Filtros

Chave	Tipo	Obrigatório	Descrição
Name	String	Não	Nome do dispositivo

Exemplo de Request de filtro

URL

```
GET /api/policies/groups?name=yourstring
```

Paginação

Chave	Tipo	Obrigatório	Descrição
Perpage	Int	Não	Linhas por página
Page	Int	Não	Página atual

Exemplo de Request de paginação

URL

```
GET /api/policies/groups?page=1&perpage=10
```

Responses

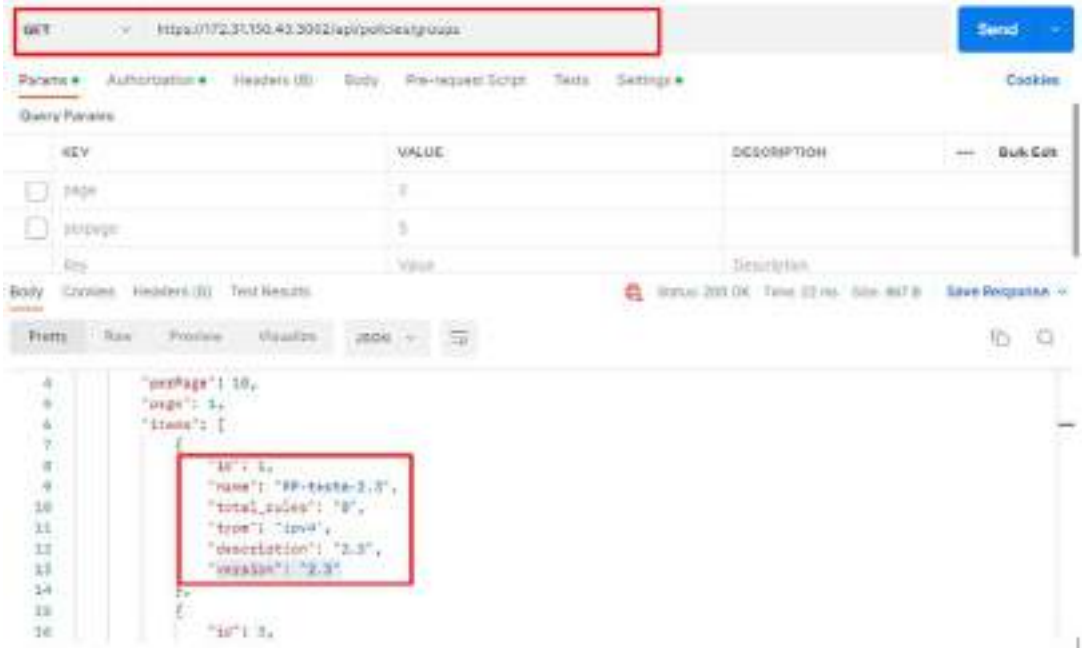
Response de sucesso

Parâmetro	Tipo	Descrição
Total	Int	Total de dispositivos
perPage	Int	Linhas por página
Page	Int	Página atual
items	Items <array>	Variedade de itens

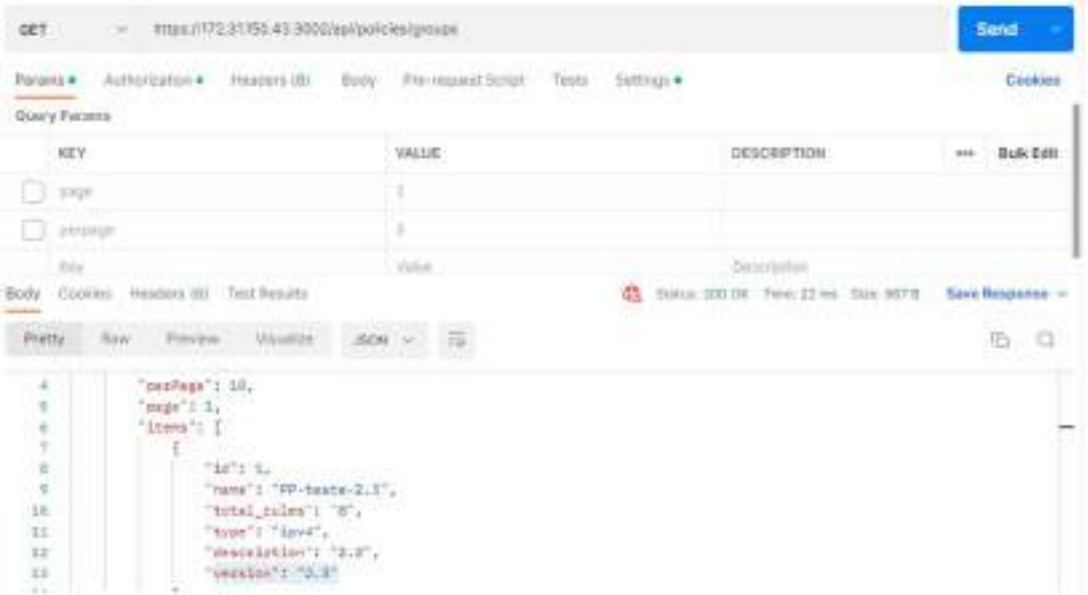
Objetos do tipo item

Parâmetro	Tipo	Descrição
id	Int	Id do dispositivo
name	String	Nome de pacote de Políticas
total_rules	Int	Total de Pacote de Políticas
type	String	Tipo IPv4 ou IPv6
description	String	Descrição do Pacote
version	String	Versão da Política

Seguem algumas imagens de resultado de pesquisa:



Request - Pacote de Políticas

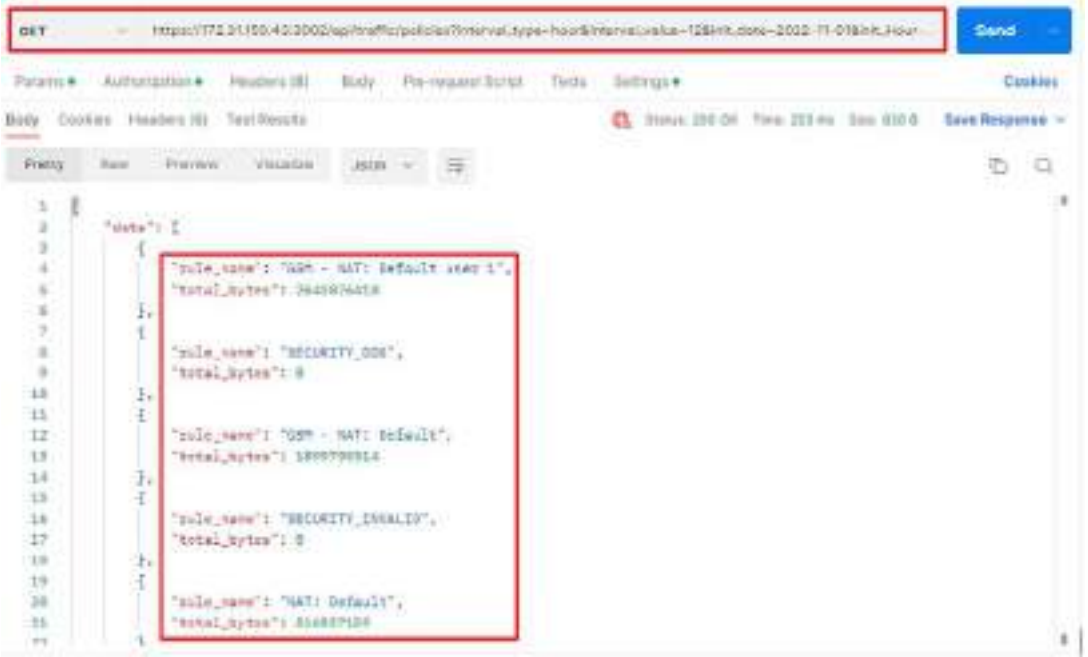


Response – Pacotes de Políticas

Request – Tráfego por usuário

Response - Tráfego por usuário

Request – Tráfego por Política



Response – Tráfego por Política

4.4. GET (Firewall)

Utilize este *Endpoint* para buscar informações acerca do Firewall, tais como serviços ativos, usuários e portas.

Requests

Requests (firewall getFWUsersCount)

Método	URL	Descrição	Argumentos	Saída
GET	/firewall	Lista o número de usuários registrados	getFWUsersCount, utm_index, startdate, enddate, period	tamanho

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getFWUsersCount	String	Sim	Comando
utm_index	Int	Sim	UTM index
startdate	String	Não	Data inicial
stopdate	String	Não	Data final
period	String	Não	Os últimos <6m, 3m, 1m,7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
size	Int	Número de conexões

Request para obtenção de número de conexões (firewall getFWConnectionCount)

Método	URL	Descrição	Argumentos	Saída
GET	/firewall	Lista o número de conexões ativas	getFWConnectionCount, getFWUsersCount, utm_index, startdate, enddate, period	tamanho

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getFWUsersCount	String	Sim	Comando
utm_index	Int	Sim	UTM index
startdate	String	Não	Data inicial
stopdate	String	Não	Data final
period	String	Não	Os últimos <6m, 3m, 1m, 7d, 3d, 24h, 12h>

Saída

Parâmetro	tipo	Descrição
size	Int	O número de usuários

Request para obtenção de status do Firewall (getFWStatus)

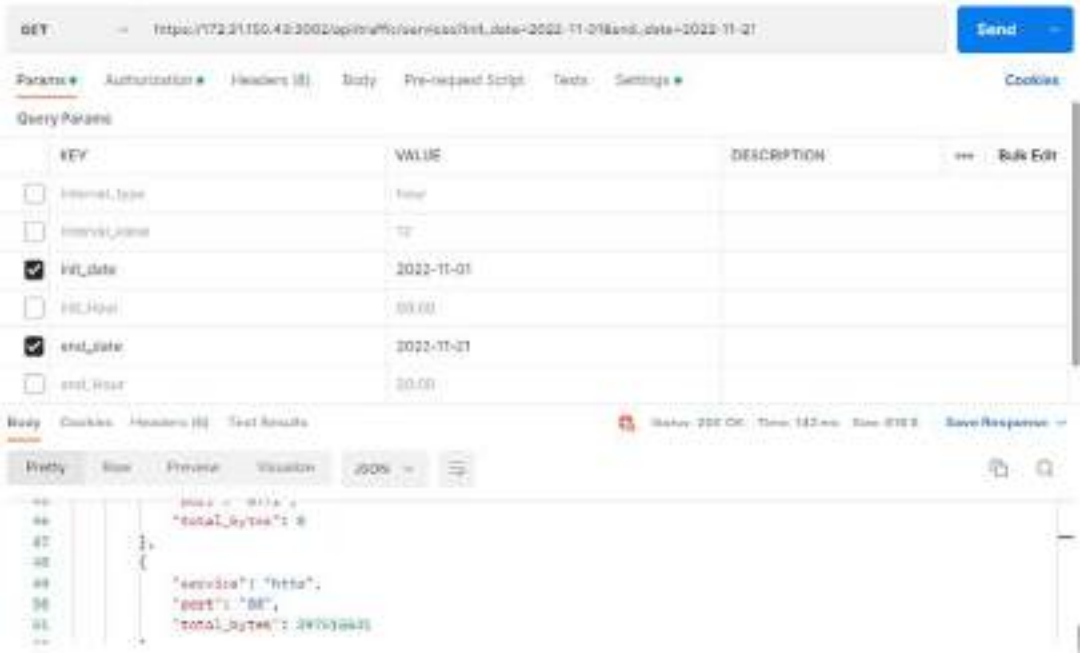
Método	URL	Descrição	Argumentos	Saída
GET	/firewall	Exibe o status geral do Firewall	utmIndex	Uso de CPU, Uso de memória, uso de disco

Argumentos (JSON payload)

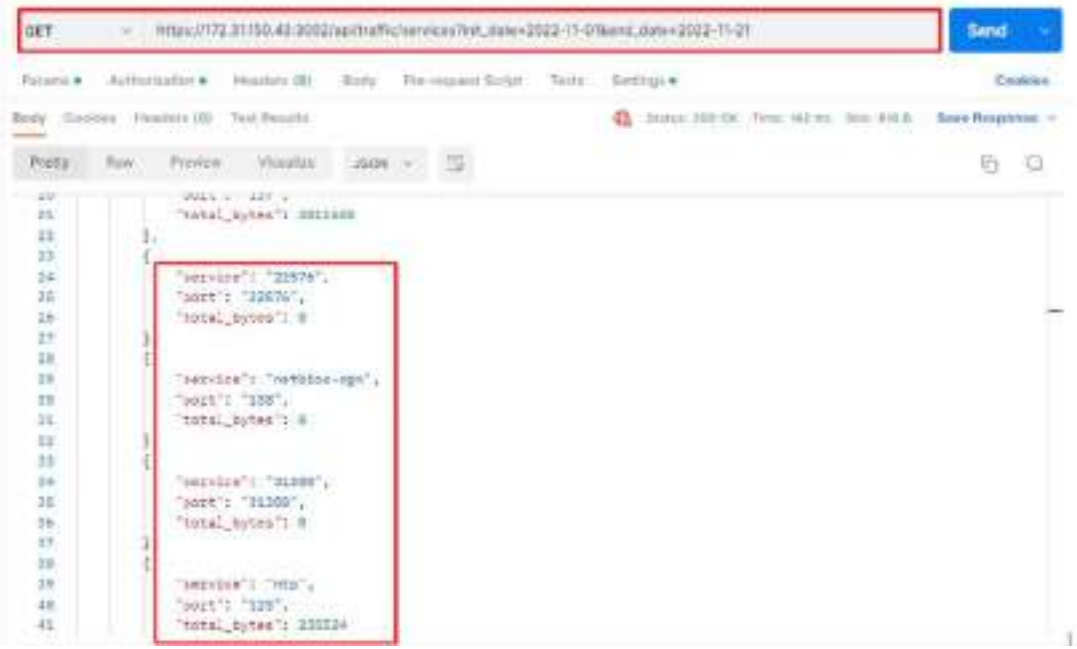
Parâmetro	Tipo	Obrigatório	Descrição
getUtmList	String	Sim	Comando

Saída

Parâmetro	Tipo	Descrição
cpuUsage	String	Uso de CPU pelo Firewall
memoryUsage	String or Long	Uso de memória pelo Firewall
diskUsage	String or Long	Uso de disco pelo Firewall



Request – Serviços, porta e total de tráfego por data



Response – Serviços, porta e total de tráfego por data

4.5. GET (IPS/IDS)

Este *Endpoint* é utilizado para buscar informações acerca do sistema de prevenção de intrusos, tais como total de alertas, endereços bloqueados, entre outros.

Requests

Request: ips getAttacksCount

Método	URL	Descrição	Argumentos	Saída
GET	/ips	Exibe o número de ataques identificados	getAttacksCount, utm_index, stardate, enddate, period	tamanho

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getAttacksCount	String	Sim	Comando
utm_index	Int	Sim	UTM index
Stardate	String	Não	Data de início
stopdate	String	Não	Data de fim
period	String	Não	Os últimos <6m, 3m, 1m, 7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
size	Int	Número de ataques identificados

Request: Ips getTotalAlertBlocked

Método	URL	Descrição	Argumentos	Saída
GET	/ips	Exibe o total de Alertas e de Bloqueados	getTotalAlertBlocked, utm_index, startdate, enddate, period	Total de alertas, total de bloqueados

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getTotalAlertBlocked	String	Sim	Comando
utm_index	Int	Sim	UTM index
Startdate	String	Não	Data inicial
Stopdate	String	Não	Data final
Period	String	Não	Os últimos <6m, 3m, 1m, 7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
totalAlert	Int	O total de alertas pelo IDS/IPS
totalBlocked	Int	O total de bloqueados pelo IDS/IPS

Request: ips getTopTenSignatures

Método	URL	Descrição	Argumentos	Saída
GET	/ips	Exibe as dez principais de assinaturas (TOP 10)	getTopTenSignatures, utm_index, startdate, enddate, period	*json_list{ }*

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getTopTenSignature	String	Sim	Comando
utm_index	Int	Sim	UTM index
startdate	String	Não	Filtro de data início
stopdate	String	Não	Filtro de data fim
period	String	Não	Os últimos <6m, 3m 1m 7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
json_list{string}	{string}	Listas de assinaturas

Request: Ips get TopCathegories

Método	URL	Descrição	Argumentos	Saída
GET	/ips	Exibe as dez principais categorias	getTopCategories, utm_index, startdate, enddate, period	*json_list{}*

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getTopCategories	String	Sim	Comando
utm_index	Int	Sim	UTM index
startdate	String	Não	Filtro de data início
stopdate	String	Não	Filtro de data fim
period	String	Não	Os últimos <6m, 3m 1m 7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
json_list{string}	{string}	Lista de categorias

Request: Ips getTopRisks

Método	URL	Descrição	Argumentos	Saída
GET	/ips	Exibe os principais riscos	getTopRisks, utm_index, startdate, enddate, period	*json_list{}*

Argumentos (JSON payload)

Parâmetro	Tipo	Obrigatório	Descrição
getTopRisks	String	Sim	Comando
utm_index	Int	Sim	UTM index
startdate	String	Não	Filtro de data início
stopdate	String	Não	Filtro de data fim
period	String	Não	Os últimos <6m, 3m 1m 7d, 3d, 24h, 12h>

Saída

Parâmetro	Tipo	Descrição
json_list{string}	{string}	Lista de riscos

4.5.1. IPS: Listar Top Source IPs

Request

Tipo	URL
GET	/api/ips/listTopSourceIP

Header

Chave	Tipo de token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET
/api/ips/listTopSourceIPS?interval_value=60&device_type=device
&device_id=1&interval_type=d
```

Filtros

É necessário inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Sim	id do dispositivo	1
device_type	String	Sim	Tipo do dispositivo	Dispositivo
interval_value	String	Relativo	Valor do intervalo	12
interval_type	String	Relativo	Tipo do intervalo	Horas
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Horário inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Horário final	20:00

Importante:

Caso sejam enviados initDate e end_date, os campos interval_type se tornam opcionais.

Caso sejam enviados interval_type e interval_value, os campos initDate e end_date se tornam opcionais.

Caso não sejam inseridos, os campos init_Hour e end_Hour assumem automaticamente os valores de 0:00 e 23:59, respectivamente.

Tipos de Intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de Request de filtro

URL

```
GET
/api/ips/listTopSourceIPS?interval_value=60&device_type=device
&device_id=1&interval_type=d
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
Error	String	Mensagem de erro
Items	Data<Array>	Variedade de dados de objeto

Objetos do tipo item

Parâmetro	Tipo	Descrição
key	String	identificação de impacto
doc_count	Int	Tráfego total por usuário
identifier	String	Descrição do identificador
hour	Date	Data do impacto

Exemplo de Response de sucesso

JSON


```
{
   "data": {
      "Items": [
         {
            "key": null,
            "doc_count": 144,
            "identifier": "histogram",
            "hour": "2022-10-27"
         },
         {
            "key": null,
            "doc_count": 3539,
            "identifier": "histogram",
            "hour": "2022-10-28"
         },
         {
            "key": null,
            "doc_count": 9,
            "identifier": "histogram",
            "hour": "2022-10-29"
         },
         {
            "key": null,
            "doc_count": 482,
            "identifier": "histogram",
            "hour": "2022-10-30"
         },
         {
            "key": null,
```

```
            "doc_count": 1656,
            "identifier": "histogram",
            "hour": "2022-10-31"
         },
         {
            "key": "186.220.197.72",
            "doc_count": 4709,
            "identifier": "top_hits",
            "hour": null
         },
         {
            "key": "177.183.0.125",
            "doc_count": 1121,
            "identifier": "top_hits",
            "hour": null
         }
      ],
      "Error": ""
   }
}
```

Response de erro

Exemplo de response de falha – 401 Invalid Signature (Assinatura Inválida)

JSON

```
{
   "error": true,
   "msg": "signature is invalid"
}
```

Problema com o Token - 401 Invalid Token (Token inválido)

JSON

```
{
   "error": true,
   "msg": "token contains an invalid number of segments"
}
```

Token faltando – 400 Token Missing

JSON

```
{
   "error": true,
   "msg": "Missing or malformed JWT"
}
```

4.5.2. IPS: Listar Top Categorias

Request

Tipo	URL
GET	/api/ips/listTopCategories

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET
/api/ips/listTopCategories?interval_value=60&device_type=device
&device_id=1&interval_type=d
```

Filtros

É possível inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Sim	Id de dispositivo	1
device_type	String	Sim	Tipo de dispositivo	Dispositivo
interval_value	String	Relativo	Valor de intervalo	12
interval_type	String	Relativo	Tipo de intervalo	hour
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Horário inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Horátio final	20:00

Importante:

Caso sejam enviados initDate e end_date, os campos interval_type e interval_value se tornam opcionais.

Caso sejam enviados interval_type e interval_value, os campos initDate e end_date se tornam opcionais

Caso os campos init_Hour e end_Hour caso não sejam passados assumem automaticamente os valores de 0:00 e 23:59, respectivamente.

Tipos de intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de Request de filtro

URL

```
GET
/api/ips/listTopCategories?interval_value=60&device_type=device
&device_id=1&interval_type=d
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
Error	String	Mensagem de erro
Items	Data<Array>	Variedade de dados de objeto

```
{
   "data": {
      "Items": [
         {
            "key": null,
            "doc_count": 144,
            "identifier": "histogram",
            "hour": "2022-10-27"
         },
         {
            "key": null,
            "doc_count": 3539,
            "identifier": "histogram",
            "hour": "2022-10-28"
         },
         {
            "key": null,
            "doc_count": 9,
            "identifier": "histogram",
            "hour": "2022-10-29"
         },
         {
            "key": null,
            "doc_count": 482,
            "identifier": "histogram",
            "hour": "2022-10-30"
         },
         {
            "key": null,
            "doc_count": 1656,
            "identifier": "histogram",
```

```
            "hour": "2022-10-31"
         },
         {
            "key": "TROJAN",
            "doc_count": 5830,
            "identifier": "top_hits",
            "hour": null
         }
      ],
      "Error": ""
   }
}
```


Objetos do tipo item

Parâmetro	Tipo	Descrição
key	String	Identificação de impacto
doc_count	Int	Tráfego total por usuário
identifier	String	Descrição do identificador
hour	Data	Data do impacto

4.5.3. IPS: Lista de impactos

Request

Tipo	URL
GET	/api/ips/listImpact

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET/api/ips/listImpact?interval_value=60&device_type=device&device_id=1&interval_type=d&nameImpact=low
```

Filtros

É necessário inserir ao menos uma data ou valor de intervalos (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Sim	Id do dispositivo	1
device_type	String	Sim	Tipo do dispositivo	Dispositivo
interval_value	String	Relativo	Valor de intervalo	12
interval_type	String	Relativo	Tipo de intervalo	Hora
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Horário inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Horário final	20:00
nameImpact	String	Sim	Horário final	Baixo

Importante:

Caso sejam enviados initDate e end_date, os campos interval_type e interval_value se tornam opcionais.

Caso sejam enviados interval_type e interval_value, os campos initDate e end_date se tornam opcionais.

Caso não sejam inseridos campos init_Hour e end_Hour, estes assumem automaticamente os valores de 00:00 e 23:59, respectivamente.

O campo nameImpact deverá ser inserido com um dos seguintes valores: low, medium, high.

Tipos de intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de Request de filtro

URL

```
GET
/api/ips/listImpact?interval_value=60&device_type=device&device
_id=1&interval_type=d&nameImpact=low
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
Error	String	Mensagem de erro
Items	Data<Array>	Variedade de dados do tipo objeto

```
{
  "data": {
    "Items": [
      {
        "key": null,
        "doc_count": 144,
        "identifier": "histogram",
        "hour": "2022-10-27"
      },
      {
        "key": null,
        "doc_count": 3539,
        "identifier": "histogram",
        "hour": "2022-10-28"
      },
      {
        "key": null,
        "doc_count": 9,
        "identifier": "histogram",
        "hour": "2022-10-29"
      },
      {
        "key": null,
        "doc_count": 482,
        "identifier": "histogram",
        "hour": "2022-10-30"
      },
      {
        "key": null,
        "doc_count": 1656,
        "identifier": "histogram",
        "hour": "2022-10-31"
      },
```

```
        {
          "key": "Possible KEYPLUG/Downadup/Conficker-C P2P encrypted
traffic UDP Ping Packet (bit value 5)",
          "doc_count": 1579,
          "identifier": "top_hits",
          "hour": null
        },
        {
          "key": "Possible KEYPLUG/Downadup/Conficker-C P2P encrypted
traffic UDP Ping Packet (bit value 4)",
          "doc_count": 1516,
          "identifier": "top_hits",
          "hour": null
        },
        {
          "key": "Possible Downadup/Conficker-C P2P encrypted traffic
UDP Ping Packet (bit value 16)",
          "doc_count": 1515,
          "identifier": "top_hits",
          "hour": null
        },
        {
          "key": "Possible KEYPLUG/Downadup/Conficker-C P2P encrypted
traffic UDP Ping Packet (bit value 1)",
          "doc_count": 1220,
          "identifier": "top_hits",
          "hour": null
        }
      ],
      "Error": ""
    }
}
```

Objetos do tipo item

Parâmetros	Tipo	Descrição
key	String	Identificação de impacto
doc_count	Int	Tráfego total por usuário
identifier	String	Descrição do identificador
hour	Data	Data do impacto

4.5.4. IPS: Lista de alertas de IP

Request

Tipo	URL
GET	/api/ips/listIpsAlert

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET
/api/ips/listIpsAlert?interval_value=60&device_type=device&device_id=1&interval_type=d
```

Filtros

É necessário inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Sim	Id do dispositivo	1
device_type	String	Sim	Tipo do dispositivo	Dispositivo
interval_value	String	Relativo	Valor do intervalo	12
interval_type	String	Relativo	Tipo de intervalo	Hora
init_date	String	Relativo	Data de início	2022-11-01
init_Hour	String	Relativo	Hora de início	08:00
end_date	String	Relativo	Data de final	2022-11-04
end_Hour	String	Relativo	Horário de final	20:00

Tipos de intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de Request de filtro

URL

```
GET
/api/ips/listIpsAlert?interval_value=60&device_type=device&device_id=1&interval_type=d
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
Allowed	Date	Data inicial
Blocked	Date	Data final
Items	Data<Array>	Variedade de dados de objeto do tipo dados


```
{
   "data": {
      "Allowed": 5830,
      "Blocked": 0,
      "Items": [
         {
            "Allowed": 144,
            "Blocked": 0,
            "KeyAsString": "2022-10-27"
         },
         {
```

```
            "Allowed": 3539,
            "Blocked": 0,
            "KeyAsString": "2022-10-28"
         },
         {
            "Allowed": 9,
            "Blocked": 0,
            "KeyAsString": "2022-10-29"
         },
         {
            "Allowed": 482,
            "Blocked": 0,
            "KeyAsString": "2022-10-30"
         },
         {
            "Allowed": 1656,
            "Blocked": 0,
            "KeyAsString": "2022-10-31"
         }
      ],
      "Error": ""
   }
}
```


Objetos do tipo item

Parâmetros	Tipo	Descrição
Allowed	Int	Nome da Política
Blocked	Int	Tráfego total por usuário
KeyAsString	Data	Total de dados por usuário

4.6. GET (Traffic)

Este *Endpoint* é destinado a levantar as informações sobre o tráfego total de informações por usuário, Pacote de Políticas ou Firewall.

4.6.1. Tráfego por Usuário

Request

Tipo	URL
GET	/api/traffic/users/:device_id

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET /api/traffic/users/:device_id
```

Filtros

É necessário inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Não	Id do dispositivo	1
interval_value	String	Relativo	Valor do intervalo	12
interval_type	String	Relativo	Tipo do intervalo	Hora
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Hora inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Hora final	20:00

Tipos de intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de filtro de Request

URL

```
GET /api/traffic/users/:device_id?interval_type=hour&interval_value=12&init_date=2022-11-01&init_Hour=08:00&end_date=2022-11-04&end_Hour=20:00
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
ini-date	Date	Data inicial
end-date	Date	Data final
data	Data<Array>	Variedade de dados de objeto

Objeto dados

Parâmetro	Tipo	Descrição
user	String	Usuário
Ips	Ips<Array>	Variedade de dados por IP
Macs	Macs<Array>	Variedade de dados por endereço Mac
total_bytes	Int	Tráfego total por usuário

Objeto IP

Parâmetro	Tipo	Descrição
ip	String	Endereço IP
total_bytes	Int	Tráfego total por usuário

Objeto Mac

Parâmetro	Tipo	Descrição
mac	String	String
total_bytes	Int	Tráfego total por usuário

Exemplo de Response de sucesso - 200

JSON


```
{
    "data": [
        {
            "user": "user@interno.com",
            "Ips": [
                {
                    "ip": "177.76.43.140",
                    "total_bytes": 123456
                }
            ],
            "Macs": [
                {
                    "Mac": "d4:6d:50:b6:48:c0",
                    "total_bytes": 123456
                }
            ],
            "total_bytes": 123456789
        }
    ],
    "date_end": "2022-11-04T20:00",
    "date_start": "2022-11-01T08:00"
}
```


Response de erro

Exemplo de Response de falha - 401 Invalid Signature (Assinatura Inválida)

JSON


```
{
    "error": true,
```

```
    "msg": "signature is invalid"
}
```

Problema de token - 401 Invalid Token (Token Inválido)

JSON

```
{
    "error": true,
    "msg": "token contains an invalid number of segments"
}
```

Token faltando - 400 Missing Token

JSON

```
{
    "error": true,
    "msg": "Missing or malformed JWT"
}
```

4.6.2. Tráfego por Serviço

Request

Tipo	URL
GET	/api/traffic/services/:device_id

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET /api/traffic/services/:device_id
```

Filtros

É necessário inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Não	Id do dispositivo	1
interval_value	String	Relativo	Valor do intervalo	12

interval_type	String	Relativo	Tipo de intervalo	Hora
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Horário inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Horário final	20:00

Tipos de intervalo

Chave	**Tipo**	**Descrição**
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de filtro de Request

URL

```
GET
/api/traffic/services?interval_type=hour&interval_value=12&init_date=2022-11-01&init_Hour=08:00&end_date=2022-11-04&end_Hour=20:00
```

Responses

Response de Sucesso

Parâmetro	Tipo	Descrição
ini-date	Date	Data inicial
end-date	Date	Data final
data	Dados<array>	Variedade de objetos do tipo dados

Objeto Dados

Parâmetro	Tipo	Descrição
services	String	Nome do serviço
port	Int	Porta do serviço
total_bytes	Int	Tráfego total por usuário

Exemplo de Response de sucesso – 200 Ok

JSON


```
{
    "data": [
        {
            "service": "domain",
            "port": "53",
            "total_bytes": 370553564
        },
        {
            "service": "https",
            "port": "443",
            "total_bytes": 95058654608
        },
        {
            "service": "utm-admin",
            "port": "98",
            "total_bytes": 5710212096
        },
        {
            "service": "ssh",
            "port": "22",
            "total_bytes": 4272399773
        },
        {
            "service": "netbios-ns",
            "port": "137",
            "total_bytes": 12437100
        },
        {
            "service": "ntp",
            "port": "123",
            "total_bytes": 14527924
        },
        {
            "service": "epmap",
            "port": "135",
            "total_bytes": 244077213
        },
        {
```

```
            "service": "snpp",
            "port": "444",
            "total_bytes": 376793171
        },
        {
            "service": "ldap",
            "port": "389",
            "total_bytes": 212349310
        },
        {
            "service": "ftp",
            "port": "21",
            "total_bytes": 39146745
        }
    ],
    "date_end": "2022-11-04T20:00",
    "date_start": "2022-11-01T08:00"
}
```


Responses de erro

Exemplo de Response de falha – 401 Invalid Signature (Assinatura inválida)

JSON


```
{
    "error": true,
    "msg": "signature is invalid"
}
```

Problema de Token – 401 Invalid Token (Token Inválido)

JSON

```
{
    "error": true,
    "msg": "token contains an invalid number of segments"
}
```

Token faltando – 400 Missing Token

JSON

```
{
    "error": true,
    "msg": "Missing or malformed JWT"
}
```

4.6.3. Tráfego por Política

Request

Tipo	URL
GET	/api/traffic/policies/:device_i

Header

Chave	Tipo de Token	Valor
Authorization	Bearer	Bearer eyJhbGciOiJIUz...

Exemplo de Request

URL

```
GET /api/traffic/policies/:device_id
```

Filtros

É necessário inserir ao menos uma data ou valores de intervalo (campos relativos).

Chave	Tipo	Obrigatório	Descrição	Exemplo
device_id	String	Não	Id do dispositivo	1
interval_value	String	Relativo	Valor do intervalo	12
interval_type	String	Relativo	Tipo do intervalo	Hora
init_date	String	Relativo	Data inicial	2022-11-01
init_Hour	String	Relativo	Hora inicial	08:00
end_date	String	Relativo	Data final	2022-11-04
end_Hour	String	Relativo	Hora final	20:00

Tipos de intervalo

Chave	Tipo	Descrição
hour	String	Hora
min	String	Minuto
d	String	Dia
m	String	Mês
y	String	Ano

Exemplo de Request de filtro

```
GET
/api/traffic/policies?interval_type=hour&interval_value=12&init_date
=2022-11-01&init_Hour=08:00&end_date=2022-11-
04&end_Hour=20:00
```

Response

Response de sucesso

Parâmetro	Tipo	Descrição
ini-date	Date	Data inicial
end-date	Date	Data final
data	Dados<Array>	Variedade de objetos do tipo dados

Objetos do tipo dados

Parâmetro	Tipo	Descrição
rule_name	String	Nome da regra
total_bytes	Int	Total de tráfego por usuário

Exemplo de Response de sucesso – 200

JSON


```
{
    "data": [
        {
            "rule_name": "FWD - LAN - Blockbit",
            "total_bytes": 219586888130
        },
        {
            "rule_name": "NAT - Saída - Full ",
            "total_bytes": 67418008773
        },
        {
            "rule_name": "Administração",
            "total_bytes": 0
        },
        {
            "rule_name": "NAT - Aplicativos Office",
            "total_bytes": 1920686939
        },
        {
            "rule_name": "NAT - Saída - ADM",
            "total_bytes": 5546072
        },
        {
            "rule_name": "WEB (Bancos e Gov)",
            "total_bytes": 12058064
        },
        {
            "rule_name": "Windows Rapise",
            "total_bytes": 430033526
        },
        {
            "rule_name": "DNS",
            "total_bytes": 0
        },
        {
            "rule_name": "VPN NG",
            "total_bytes": 0
        },
```

```
        {
            "rule_name": "IPsec",
            "total_bytes": 0
        }
    ],
    "date_end": "2022-11-04T20:00",
    "date_start": "2022-11-01T08:00"
}
```


Response de erro

Exemplo de Response de falha – 401 Invalid Signature (Assinatura Inválida)

JSON


```
{
    "error": true,
    "msg": "signature is invalid"
}
```


Problema de Token – 401 Invalid Token (Token inválido)

JSON


```
{
    "error": true,
    "msg": "token contains an invalid number of segments"
}
```

Token faltando – 400 Missing Token

JSON

```
{
    "error": true,
    "msg": "Missing or malformed JWT"
}
```

Canais de Atendimento:

Telefone:
+55 (11) 2165-8888

Suporte:
suporte@blockbit.com

Sugestões e reclamações:
ouvidoria@blockbit.com

Rua: Alexandre Dumas, 1711 - Birmann 11, térreo
Santo Amaro, São Paulo - SP 04717-911 - Brasil
Telefone: + 55 11 2165-8888
www.blockbit.com