



Serviço Público Federal  
Conselho Federal de Medicina Veterinária

INFORMAÇÃO 7/2025 - GETIC/SUPEX/DE/CFMV/SISTEMA

Em 23 de fevereiro de 2025.

Ao Senhor  
Pregoeiro do CFMV  
Vitor Hugo da Silva Ramos

Assunto: **Resposta à SOLICITAÇÃO 7/2025 - SELIC/GERAD/SUPEX/DE**

Senhor Pregoeiro,

1. Em resposta ao seu pedido de manifestação técnica enviado ao Setor de Infraestrutura e Segurança da Informação - SESEG/GETIC, referente à qualificação técnica da licitante e demais documentos necessários, conforme os requisitos exigidos no **Pregão Eletrônico nº 90012/2024**, do PA nº **0110044.0000049/2024-74**; informamos que foi analisada a documentação da empresa **GRG Tech Assessoria e Informática LTDA**.

2. Foram analisados os documentos enviados pela licitante em relação às Especificações Técnicas, Habilitação e Qualificação Técnica, quanto ao atendimento das condições previstas no edital, em especial, a:

2.1. QUALIFICAÇÃO TÉCNICA;

2.2. PROPOSTA COMERCIAL;

3. Identificou-se o seguinte:

a) A empresa licitante apresentou proposta **compatível** com as especificações do edital;

b) A empresa apresentou **5 (cinco) atestados** de capacidade técnica, dos quais **apenas 2 (dois) são compatíveis** com o objeto da licitação. Isso comprova o fornecimento de pontos de acesso no total de 50% (cinquenta) do montante solicitado neste certame, conforme item 9.31 do TR;

c) A licitante apresentou documento oficial do fabricante comprovando que a mesma faz parte do programa de parceria do fabricante, conforme item 9.32 do TR;

d) A licitante enviou o ANEXO G junto à proposta. Durante a análise da documentação foram realizadas diligências com a mesma para sanar as dúvidas encontradas pela equipe. Após as explicações, constatou-se que todas as funcionalidades da solução apresentada atendem às especificações do edital.

4. **DECISÃO**: Portanto, a empresa GRG Tech Assessoria e Informática LTDA **atende** aos requisitos do edital.

Atenciosamente,

Leonardo Stefan Barbosa de Oliveira  
Analista de Rede do Setor de Infraestrutura - SESEG  
Gerência de Tecnologia da Informação e Comunicação - GETIC

Documento assinado eletronicamente por:

- **Leonardo Stefan Barbosa de Oliveira, Empregado - CMSUP - SESEG**, em 23/02/2025 14:52:50.

Este documento foi emitido pelo SUAP em 23/02/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.cfmv.gov.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 411578

Código de Autenticação: 5da2dfd92d



**SISTEMA  
CFMV/CRMVs**  
Conselhos Federal e Regionais de Medicina Veterinária

SIA TRECHO 6 Lotes, 130/140, Setor de Indústria e Abastecimento, Brasília / DF,  
CEP 71205-60

## Marcia Fernanda de Macedo Marto

---

**De:** Rodrigo Monção <rodrigo@grgtech.io>  
**Enviado em:** terça-feira, 18 de fevereiro de 2025 18:35  
**Para:** Informática GETIC-CFMV  
**Cc:** licitacoes@grgtech.io; felipe@grgtech.io  
**Assunto:** Re: Diligência sobre Anexo G – Tabela de cumprimento dos Requisitos

Prezados, Boa tarde.

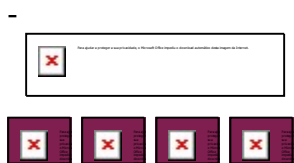
Abaixo, em azul, estão as respostas da diligência realizada. Em caso de dúvidas adicionais, estamos à disposição e certos que a solução classificada como líder pelo Gartner está aderente ao projeto do CFMV.

- **No item 1.4, foi anexado um link para um documento em PDF (ExtremeCloud-IQ), que entendemos ser uma controladora virtual. Está correto nosso entendimento?**
  - Prezados, o Extreme CloudIQ, conforme descrito no documento “26797-ExtremeCloud-IQ-DS-F.pdf”, é uma console de gerenciamento unificada. A licença ofertada permite o uso exclusivamente em nuvem, ou também utilizando servidor virtual local.
  - Na arquitetura proposta pela Extreme Networks, há uma diferença entre a palavra “controladora” e “gerenciamento”, uma vez que as funções de controle ficam distribuídas em todos os Pontos de Acesso. Portanto, em caso de falha do gerenciamento, a rede continua operando de forma contínua e sem parada.
  - Sendo assim, há um gerenciamento centralizado e único para toda a solução. Caso a equipe do CFMV entenda que a solução proposta é similar ao termo “controladora” descrito no edital, a solução faz uso e está ofertado.
- **Nos itens 2.2 a 2.5, sobre a necessidade de uma controladora, a sua resposta negativa. Entendemos, portanto, que sua solução não utiliza controladora. Está correto nosso entendimento?**
  - Prezados, para melhor explicar essa situação, devemos esclarecer os termos utilizados e que cada fabricante possui uma terminologia diferente.
  - De acordo com o prospecto técnico da solução de gerenciamento “26797-ExtremeCloud-IQ-DS-F.pdf”, o CloudIQ é uma console de gerenciamento unificada. A licença ofertada permite o uso exclusivamente em nuvem, ou também utilizando uma máquina virtual local.
  - Na arquitetura proposta pela Extreme Networks, há uma diferença entre a palavra “controladora” e “gerenciamento”, uma vez que as funções de controle ficam distribuídas em todos os Pontos de Acesso. Portanto, em caso de falha do gerenciamento, a rede continua operando de forma contínua e sem parada.
  - Conforme explicado no item 2.8, a arquitetura da Extreme Networks é distribuída, ou seja, os Pontos de Acesso têm todo o hardware necessário para realização de controle e as políticas são criadas na console de gerência. Após a criação destas políticas, essas são aplicadas nos Pontos de Acesso necessários.
  - Sendo assim, há um gerenciamento centralizado e único para toda a operação. Caso a equipe do CFMV entenda que isso é o termo “controladora”, a solução faz uso e está ofertado
- **Se sua solução não tem controladora, os APs são autogerenciados? E, se são autogerenciados, onde encontramos essa informação e documentação?**

- Prezados, conforme exemplificado anteriormente, a solução da Extreme Networks faz o uso de uma console de gerenciamento unificada, a qual pode ser apenas em nuvem ou também instalada local.
  - Conforme explicado no item 2.8, a arquitetura da Extreme Networks é distribuída, ou seja, os Pontos de Acesso têm todo o hardware necessário para realização de controle e as políticas são criadas na console de gerência. Após a criação destas políticas, essas são aplicadas nos Pontos de Acesso necessários. A partir da aplicação das políticas, os Pontos de acesso se auto gerenciam.
  - Sendo assim, há um gerenciamento centralizado e único para toda a operação. Caso a equipe do CFMV entenda que isso é o termo “controladora”, a solução faz uso e está ofertado.
  - Caso o CFMV requeira utilizar o Ponto de Acesso sozinho, há duas opções. A primeira é utilizar o sistema operacional IQ Engine e manter uso da gerência. A segunda é utilizando o sistema operacional WiNG ([Access Point System Reference Guide - WiNG Release 7.9.5.0 – Página 34](#)). Essa é a vantagem do Ponto de Acesso da Extreme, conforme detalhado na pergunta 5.
- **No item 2.6 não localizamos a informação correta sobre o funcionamento do AP em modo de redundância e alta disponibilidade, pois no documento foi anexado um pdf que faz referência ao ExtremeCloudIQ.**
    - O item 2.6 em questão solicita “Implementar mecanismo de funcionamento para trabalhar com controladores WLAN em redundância”.
    - Por entender que o objetivo do CFMV é garantir uma gerência centralizada redundante, utilizamos a informação que a solução de gerenciamento utilizada – Extreme CloudIQ – é redundante, conforme descrito no item “Reliability” do documento, o qual informa que é solução possui alta disponibilidade, conforme o trecho “High availability with disaster recovery and redundancy”.
    - Para a redundância do ambiente, independente da console de gerenciamento, conforme explanado no item 2.8, a arquitetura da Extreme Networks é distribuída, ou seja, os Pontos de Acesso têm todo o hardware necessário para realização de controle e as políticas são criadas na console de gerência. Após a criação destas políticas, essas são aplicadas nos Pontos de Acesso necessários. Dessa maneira, a queda de um Ponto de Acesso não impacta o ambiente como um todo.
    - Ou seja, a solução possui redundância e alta-disponibilidade tanto no gerenciamento, quanto na arquitetura dos Pontos de Acesso!
  - **No item 2.7 a resposta enviada faz referência a 2 (dois) sistemas operacionais para WI-Fi (IQ Engine ou WiNG Operating System). Poderia nos explicar qual a diferença entre eles?**
    - As soluções da Extreme Networks, tanto de Rede Cabeada (Switches), quanto de rede sem fio (Wireless), possuem equipamentos de hardware universal.
    - Hardware Universal – Nomenclatura utilizada pela Extreme Networks para informar que os equipamentos suportam mais de um sistema operacional. Portanto, os Pontos de Acesso ofertados podem ser utilizados em ambos os cenários.
    - Dessa forma, o CFMV pode alterar o sistema operacional do equipamento, uma vez que a aquisição do equipamento dá direito de uso dos dois sistemas operacionais ao cliente.

- WiNG é um sistema operacional advindo da Motorola/Zebra, que foi adquirido pela Extreme Networks em 2016, enquanto o IQ Engine é um projeto inicial da Aerohive, adquirida em 2019.
- Ambas são soluções de alta qualidade técnica e atualmente não existe discrepância técnica entre ambas. Entretanto, para clientes legados, os quais possuem uma estrutura toda com o WiNG, quando vão realizar a expansão do ambiente, optam por esse sistema operacional, para a correta realização de roaming entre eles. O mesmo acontece com clientes com o IQ Engine.
- Como a Extreme Networks tem evoluído e muito a solução de gerenciamento em nuvem, diversos clientes optaram pelo IQEngine. Atualmente, ambos os sistemas operacionais podem utilizar a gerência em nuvem.
- Como forma de ofertar uma solução única para todos os clientes, ou seja, as mesmas características de Hardware, a Extreme criou a política de único hardware para qualquer ambiente (Hardware Universal).

Atenciosamente,



### Rodrigo Monção

Diretor

Pré-vendas | Garage Tech

+55 61 3963-1776 | +55 61 99812-3588

[rodrigo@grgtech.io](mailto:rodrigo@grgtech.io)

[grgtech.io](http://grgtech.io)

SIG Quadra 2 Lote 420, Ed. City Offices, Brasília-DF, Brasil

Em ter., 18 de fev. de 2025 às 17:04, 'Informática GETIC-CFMV' via Licitacoes <[licitacoes@grgtech.io](mailto:licitacoes@grgtech.io)> escreveu:

Prezado sr. Felipe, boa tarde.

Ficamos com algumas dúvidas no conteúdo do documento enviado.

Seguirei com a numeração dos itens do ANEXO G.

- No item 1.4, foi anexado um link para um documento em PDF (ExtremeCloud-IQ), que entendemos ser uma controladora virtual. Está correto nosso entendimento?

- Nos itens 2.2 a 2.5, sobre a necessidade de uma controladora, a sua resposta negativa. Entendemos, portanto, que sua solução não utiliza controladora. Está correto nosso entendimento?
- Se sua solução não tem controladora, os APs são autogerenciados? E, se são autogerenciados, onde encontramos essa informação e documentação?
  
- No item 2.6 não localizamos a informação correta sobre o funcionamento do AP em modo de redundância e alta disponibilidade, pois no documento foi anexado um pdf que faz referência ao ExtremeCloudIQ.
  
- No item 2.7 a resposta enviada faz referência a 2 (dois) sistemas operacionais para WI-Fi (IQ Engine ou WiNG Operating System). Poderia nos explicar qual a diferença entre eles?

Solicito a resposta sobre estes questionamentos até **19/2/2025 às 12h** para que possamos dar prosseguimento à habilitação de sua empresa.

Aguardo retorno.

At.te



**Marcia Fernanda de Macedo Marto**  
Setor de Infraestrutura e segurança da Informação - SESEG  
Conselho Federal de Medicina Veterinária  
(61) 2106-0457

# Documento Digitalizado Público

## Troca email com a GRG Tech - Primeira Diligencia

**Assunto:** Troca email com a GRG Tech - Primeira Diligencia  
**Assinado por:** Marcia Marto  
**Tipo do Documento:** EMAIL  
**Situação:** Finalizado  
**Nível de Acesso:** Público  
**Tipo do Conferência:** Documento Original

Documento assinado eletronicamente por:

- **Márcia Fernanda de Macedo Marto, Empregado - CMSUP - SESEG**, em 23/02/2025 15:03:01.

Este documento foi armazenado no SUAP em 23/02/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.cfmv.gov.br/verificar-documento-externo/> e forneça os dados abaixo:

**Código Verificador:** 1002938

**Código de Autenticação:** 2262cd7638



## Marcia Fernanda de Macedo Marto

---

**De:** Rodrigo Monção <rodrigo@grgtech.io>  
**Enviado em:** sábado, 22 de fevereiro de 2025 21:41  
**Para:** Informática GETIC-CFMV  
**Cc:** licitacoes@grgtech.io; felipe@grgtech.io; Bruno Oliveira  
**Assunto:** Re: Diligência sobre Anexo G – Tabela de cumprimento dos Requisitos  
**Anexos:** Diligência - 2.1.pdf

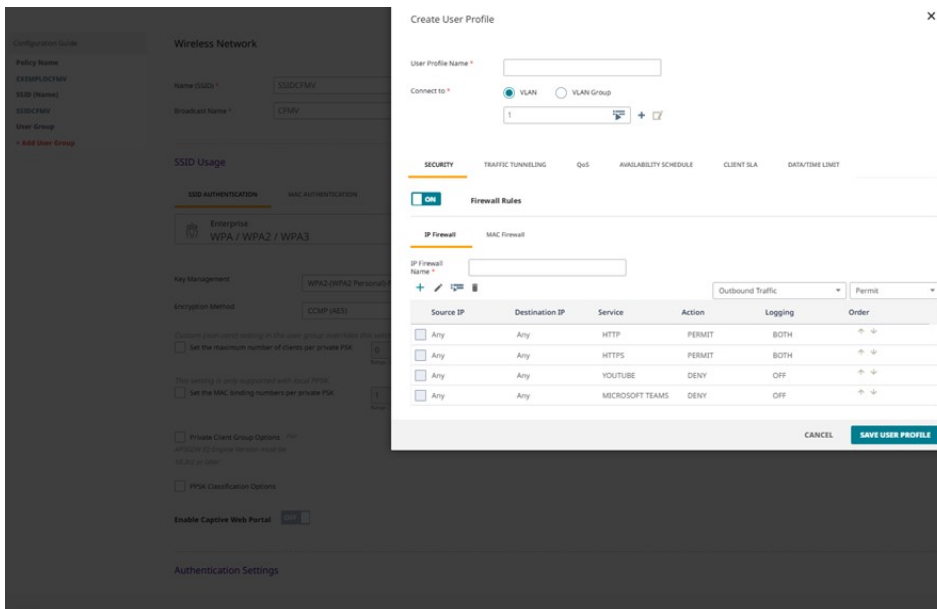
Prezados, Boa noite.

Obrigado pelo retorno. De forma tempestiva, com relação às perguntas realizadas, abaixo trazemos as devidas respostas em Azul e com imagens. Para evitar algum erro de formatação do e-mail, enviaremos também como anexo.

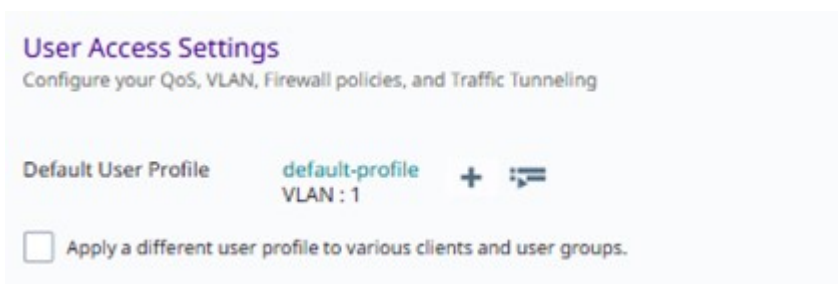
As novas soluções providas pela Extreme Networks são de extrema relevância e qualidade, sendo líder no quadrante do Gartner e é capaz de prover o mais alto nível de tecnologia. Considerando as respostas apresentadas, e conforme orientado, aguardamos o prosseguimento à habilitação.

1. No item 2.17, refere-se a: Permitir a criação de perfis de usuários a partir do qual se determinem parâmetros individuais de QoS, VLAN, políticas de firewall e criptografia de tráfego.
  - [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
  - Página 516/517
  - ExtremeIoT Essentials in ExtremeCloud IQ User Profiles
  - Durante a análise não identificamos referência na documentação indicada referente a existência de memória não volátil (NVRAM). Solicitamos o esclarecimento e indicação correta para comprovação deste item.
    - **RESPOSTA: Não identificamos, no item solicitado, nenhuma referência a memória não volátil (NVRAM). Com relação a esta característica, temos descrito pelo próprio fabricante, em carta apresentada durante a fase de habilitação, que a solução atente o requisito. Documento: “0005.2025\_ExtremeNetworks.pdf”, no subitem “Declaramos que”. Portanto, a solução ofertada possui memória não volátil (NVRAM)**
    - **Como não há associação com o item descrito, trazemos mais uma comprovação para o item em questão, para tentar sanar alguma dúvida possivelmente existente.**
  - **A solução da Extreme Networks possui uma gerência tão robusta, que é capaz de criar políticas que são únicas e podem ser associadas a diversos tipos de equipamentos. A solução atende ao item solicitado, conforme poder ser visualizado na imagem a seguir:**





- 
- Na imagem verificamos que é possível criar políticas de firewall em camada 7, ao adicionar Youtube e Teams como exemplos. Tais configurações podem ser associadas por tipo de usuários, conforme imagem a seguir e página 116 do manual:



- 
- A configuração desejada também pode ser confirmada nas páginas 237 e 238 do mesmo documento, com o trecho a seguir:

#### Add a User Profile

Use this task to create user profiles that define user traffic settings on APs. After a user associates with a device, the device assigns the user to a user profile. The device can make this assignment dynamically from attributes returned by a RADIUS authentication server or statically by using the default user profile set.

1. Go to **Configure > Common Objects > Policy > User Profiles**.
2. Select **+**.
3. Type a **Name** for the profile.
4. Select **VLAN** or **VLAN Group** for the profile.
5. Select a VLAN or VLAN group from the menu, or select **+**.  
See [Configure VLAN Settings](#) on page 115 for more information.
6. On the **Security** tab, apply IP or MAC firewall rules.  
For more information, see [Configure User Profile Security](#) on page 238.

- 
- Podemos verificar ainda na guia “User Profile Settings” (<https://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-user-profile-settings.htm?Highlight=user%20policy>) que é possível a criação de perfis onde podemos fazer a configuração de VLANs (Select either the default VLAN or VLAN group, or another VLAN or VLAN group from the drop-down list ()), or select to add a new VLAN or VLAN group. See "[Configure VLAN Settings](#)".), QoS (Configure QoS settings on the User Profile QoS tab. See "[User Profile QoS Settings](#)".), políticas de firewall (Configure firewall rules on the User Profile Security tab. See "[User Profile Security Settings](#)".). Quanto à criptografia de tráfego, O ExtremeCloud IQ exibe uma lista de perfis de usuário cujo tráfego pode ser encaminhado por meio do túnel VPN IPsec da Camada 2

ou encaminhado sem tunelamento

(<https://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/configuration/configuring-l2-ipsec-vpn-services.htm?Highlight=user%20encryption>).

○ Além disso, é possível adicionar outras funcionalidades ao perfil do usuário, como Tunelamento GRE (Enable traffic tunneling (GRE) on the User Profile Traffic Tunneling tab. See "GRE Traffic Tunneling"), URL Filtering (Configure URL filtering rules on the URL Filtering tab. See "User Profile URL Filtering".), SLA (Configure Client Service Level Assurance settings on the User Profile Client SLA tab. See "Client SLA Settings".), Limites de Tempo (Configure data usage and time limits for this user profile on the User Profile Data/Time Limit tab. See "Access Restriction Settings".)

2. No item 3.6, refere-se a: Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior;

○ <https://extr-p-001.sitecorecontenthub.cloud/api/public/content/7460a7c327ea455d8cc806fcbc9d07b7?v=43d958cf>

○ Durante a análise não identificamos referência na documentação indicada referente a existência de memória não volátil (NVRAM). Solicitamos o esclarecimento e indicação correta para comprovação deste item.

○ **RESPOSTA: Não identificamos, no item solicitado, nenhuma referência a memória não volátil (NVRAM). Com relação a esta característica, temos descrito pelo próprio fabricante, em carta apresentada durante a fase de habilitação, que a solução atente o requisito. Documento: "0005.2025\_ExtremeNetworks.pdf", no subitem "Declaramos que". Portanto, a solução ofertada possui memória não volátil (NVRAM).**

○ Além disso, o documento

**"[https://documentation.extremenetworks.com/wireless/AP\\_Guides/AP410C/downloads/AP410C\\_Installation\\_Guide.pdf](https://documentation.extremenetworks.com/wireless/AP_Guides/AP410C/downloads/AP410C_Installation_Guide.pdf)", sua página 11, no trecho "Reset button details", detalha que o equipamento mantém as configurações após o reboot.**

3. No item 3.8, refere-se a: Possibilitar Backup e Restore da configuração por meio da interface gráfica, onde no documento enviado por esta empresa contém a seguinte indicação:

○ [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)

○ Página 429

○ Device Management Servers

○ Durante a análise identificamos se tratar de configuração para switch e não wireless (AP). Tendo em vista ao final do bloco de configuração fazer alusão a configurações de switch (Related Topics Configure Switch Devices on page 427) e o bloco desta features e/ou configuração está agrupada dentro do gerenciamento de switches (Configure Switch Devices). Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- **RESPOSTA:** Verificando a análise realizada, temos que o Tópico “Device Management Servers” não está relacionado ao tópico superior. Entretanto, considerando a importância dessa funcionalidade, essa característica pode ser validada no mesmo manual, na página 158, no tópico “Configure AP Templates”. Uma vez que todas as configurações são realizadas através de políticas, as quais podem ser aplicadas a mais de 01 ponto de acesso de forma fácil e ágil, as configurações estão atreladas as políticas criadas (Conforme descrito na página 130 - Configure Device Templates). Sendo assim, é possível salvar as alterações das políticas e sempre que for preciso fazer uma restauração do equipamento, é simplesmente aplicar a política novamente.
- Além disso, todas as políticas podem ter o backup realizado, conforme página 43, no trecho “To perform a manual backup, select Backup Now”.

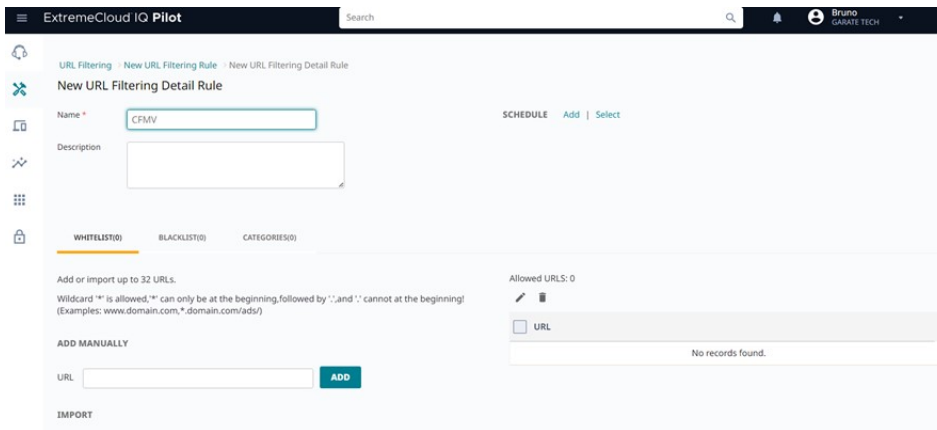
4. No item 3.28, refere-se a: Deverá suportar filtro de conteúdo;

- [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
- Página 141
- URL Filtering
- Durante a análise identificamos se tratar de configuração para routers. Solicitamos o esclarecimento e indicação correta para comprovação deste item.
- **RESPOSTA:** Considerando a análise realizada, podemos informar outro trecho do mesmo manual analisado. Na página 259, no tópico “IP Firewall Policies”, temos as políticas e filtros a serem criados. Como exemplo real, temos uma imagem da console, com um exemplo de filtro a ser aplicado:

The screenshot shows the configuration page for a firewall policy named 'FiltroDeConteudo'. It includes a form for Name and Description, and a table of rules. The table has columns for Source IP, Destination IP, Service, Action, Logging, and Order. The rules listed are:

Source IP	Destination IP	Service	Action	Logging	Order
<input type="checkbox"/> Any	Any	YOUTUBE	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	SYSLOG	DENY	OFF	↑ ↓
<input type="checkbox"/> Any	Any	VOIP-SVP	DENY	OFF	↑ ↓
<input type="checkbox"/> Any	Any	YMSG	DENY	OFF	↑ ↓
<input type="checkbox"/> Any	Any	AMAZON	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	BADOO	PERMIT	OFF	↑ ↓
<input type="checkbox"/> Any	Any	BANKECOM	PERMIT	OFF	↑ ↓

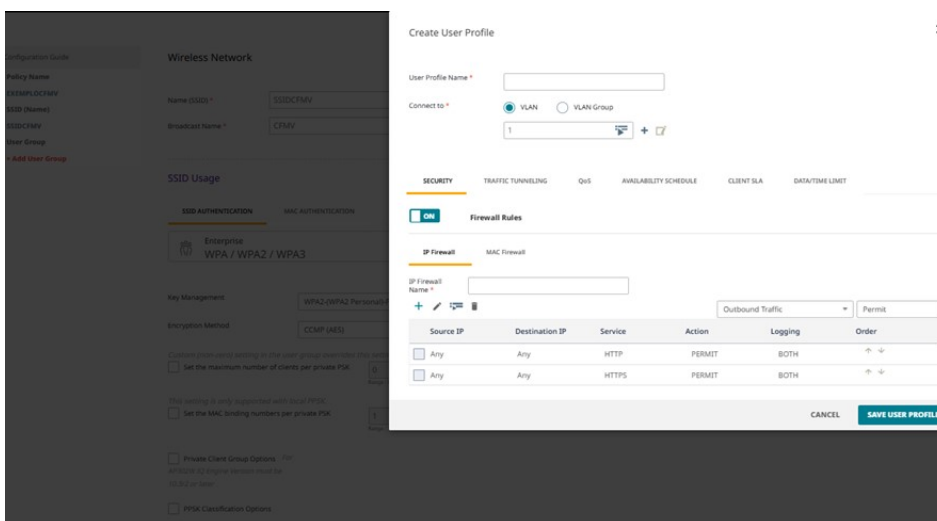
- Além disso, adicionamos novamente o tópico URL Filtering (Configure URL filtering rules on the URL Filtering tab. See "User Profile URL Filtering".)



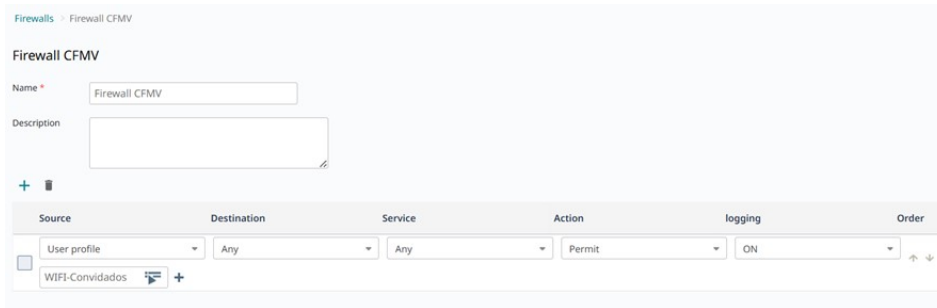
- 
- **As opções são vastas e o item é atendido.**

5. No item 3.29, refere-se a: Deverá implementar firewall com capacidade de rastreamento do estado da conexão (stateful firewall);

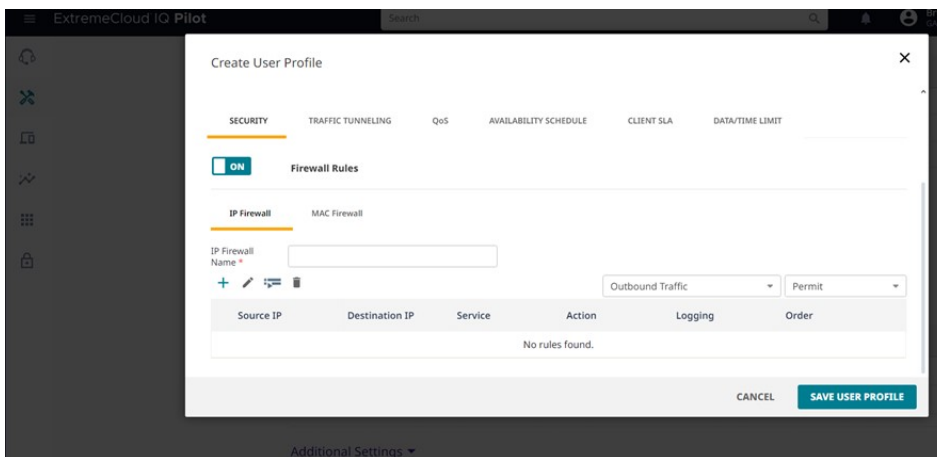
- [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
- Página 272
- Configure Classifier Map Services
- Durante a análise identificamos se tratar de configuração para roteadores relacionados a WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.
- **RESPOSTA: Considerando informações públicas, como o site do fabricante de firewall Fortinet <https://www.fortinet.com/br/resources/cyberglossary/stateful-firewall>, temos que a solução da Extreme ofertada atende completamente ao item em questão, pois é possível criar as regras de firewall stateful, conforme imagens a seguir:**



-



- 
- Na página 259 no manual detalha o “Add IP Firewall Policies”, comprovando o atendimento.
- É possível verificar ainda a opção Device Level WAN Stateful Firewall ([https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)) na página 438, comprovando de forma inequívoca o atendimento ao item e demonstrado na imagem abaixo:

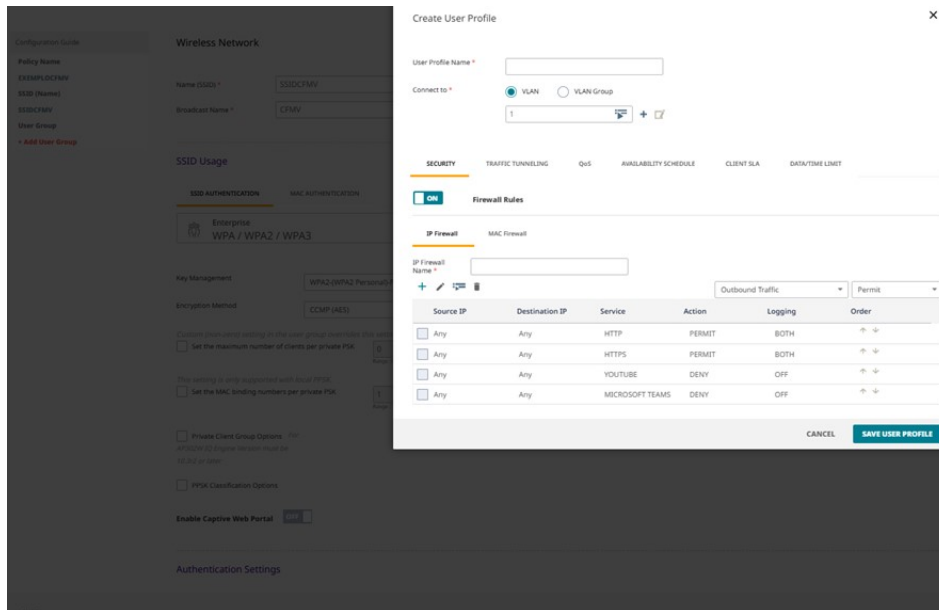


- 
- 

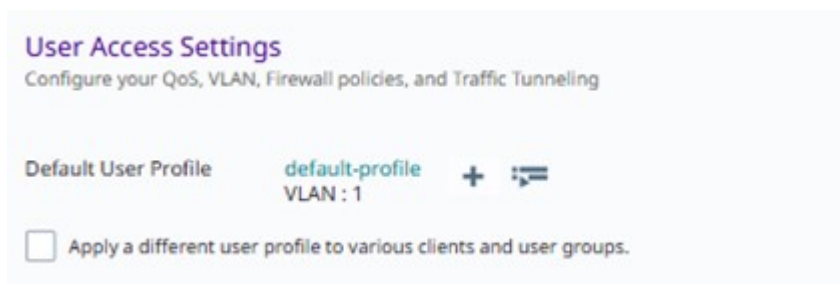
6. No item 3.30, refere-se a: Deverá permitir a criação de políticas de firewall em camada 7 e sua associação de forma dinâmica de acordo com a identidade do usuário autenticado com o ponto de acesso operando no modo autogerenciado ou gerenciado por Controladora WLAN;

- <https://extr-p-001.sitecorecontenthub.cloud/api/public/content/7460a7c327ea455d8cc806fcbc9d07b7?v=43d958cf>
- 7
- Security
- Durante a análise identificamos se tratar de configuração para routers relacionados a WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.
- **RESPOSTA: A solução da Extreme Networks possui uma gerência tão robusta, que é capaz de criar políticas que são únicas e podem ser associadas a diversos tipos de**

equipamentos. A solução atende ao item solicitado, conforme poder ser visualizado na imagem a seguir:



- 
- Na imagem verificamos que é possível criar políticas de firewall em camada 7, ao adicionar Youtube e Teams como exemplos. Tais configurações podem ser associadas por tipo de usuários, conforme imagem a seguir e página 116 do manual:

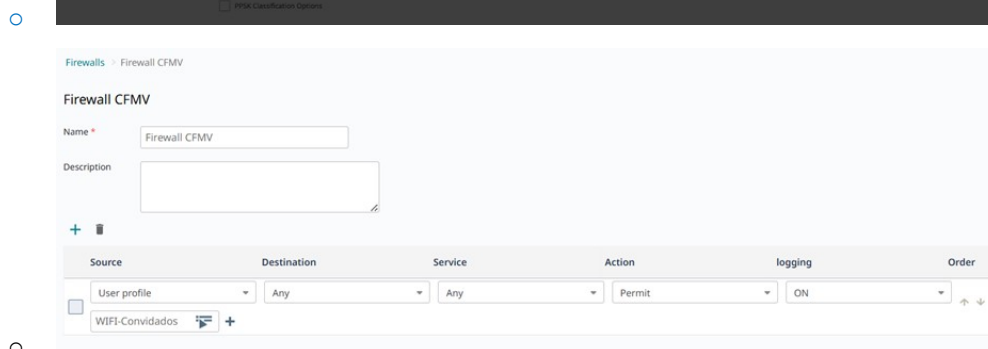
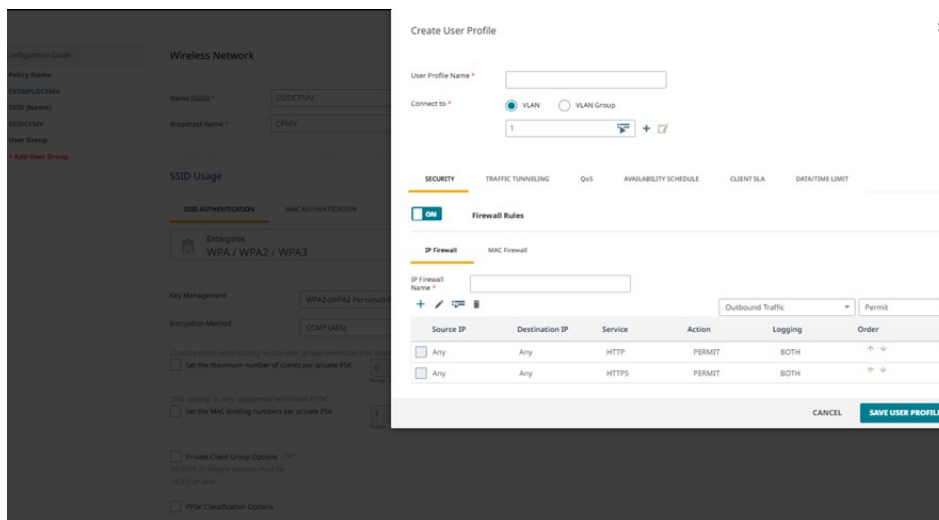


- 
- Nas páginas 237 e 238 é especificado “Add a User Profile”, o qual permite a criação de tal regra.

7. No item 3.31, refere-se a: Deverá implementar firewall com capacidade de rastreamento do estado da conexão (stateful firewall);

- [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
- Página 259
- Add IP Firewall Policies
- 26797-ExtremeCloud-IQ-DS-F.pdf
- Página 9
- Application, network, and MAC layer firewall policy rules

- Durante a análise identificamos se tratar de configuração para routers relacionados a SD-WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.
- **RESPOSTA: Considerando informações públicas, como o site do fabricante de firewall Fortinet <https://www.fortinet.com/br/resources/cyberglossary/stateful-firewall>, temos que a solução da Extreme ofertada atende completamente ao item em questão, pois é possível criar as regras de firewall stateful, conforme imagens a seguir:**



- **Na página 318 do manual também cita o “configure a firewall policy”, de forma a comprovar o item solicitado.**

8. No item 3.46, refere-se a: Deverá suportar sua própria autenticação com o controlador via certificado digital;

- [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
- Pagina 324/325
- Create a Certificate and Key
- Durante a análise identificamos se tratar de criação ou importação de certificados, mas não identificamos a integração para comunicação do software Extreme Cloud IQ e os dispositivos. Solicitamos o esclarecimento e indicação correta para comprovação deste item.
- **RESPOSTA: Além da capacidade de certificado já comprovada, o ponto de acesso possui uma conexão segura e com certificado da Extreme Networks, conforme o manual na página**

399, em “Configure Bootstrap CAPWAP settings”, conforme detalhado do trecho “security” da RFC4118 (RFC 4118 - Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)).

- Na página 412, em “Configure AP Devices”, fica evidente ao atendimento da segurança do ambiente, com possibilidade de alterações de “network administrator credentials and administrator assignments, and configure CAPWAP and Shared Key settings”.
- Conforme documentação da própria Extreme Networks, a qual adquiriu a solução da empresa **Aerohive** - [https://documentation.extremenetworks.com/xiq/legacy/Aerohive\\_Security\\_Guide.pdf](https://documentation.extremenetworks.com/xiq/legacy/Aerohive_Security_Guide.pdf) - na página 7 descreve a forma de comunicação, a qual atende ao requisito do item.
- Podemos ainda verificar na seção **CAPWAP Configuration** (<https://docs.aerohive.com/330000/docs/help/english/ng/Content/gui/devices/configuring-device-credentials.htm?Highlight=capwap>) que, por padrão, quando um dispositivo se conecta pela primeira vez ao ExtremeCloud IQ, ele usa uma senha de bootstrap predefinida combinada com vários outros valores para derivar uma chave compartilhada que os dispositivos usam para autenticar uns aos outros. A chave é exclusiva para cada relacionamento dispositivo-ExtremeCloud IQ. Então, depois que o dispositivo e o ExtremeCloud IQ se autenticam e concluem o handshake DTLS, eles geram outra chave para criptografar suas comunicações. Eles geram uma chave de criptografia diferente após cada handshake DTLS.
- Conforme a RFC 4347 (<https://www.rfc-editor.org/rfc/rfc4347.html#section-3.2>) e posteriores, o Datagram Transport Layer Security utiliza o mecanismo de troca de certificados no processo de handshake, conforme evidenciado abaixo:

#### 4.2.2. Handshake Message Format

In order to support message loss, reordering, and fragmentation, DTLS modifies the TLS 1.1 handshake header:

```
struct {
    HandshakeType msg_type;
    uint24 length;
    uint16 message_seq; // New field
    uint24 fragment_offset; // New field
    uint24 fragment_length; // New field
    select (HandshakeType) {
        case hello_request: HelloRequest;
        case client_hello: ClientHello;
```

Rescorla & Modadugu

Standards Track

[Page 13]

RFC 4347

Datagram Transport Layer Security

April 2006

```
case hello_verify_request: HelloVerifyRequest; // New type
case server_hello: ServerHello;
case certificate: Certificate;
case server_key_exchange: ServerKeyExchange;
case certificate_request: CertificateRequest;
case server_hello_done: ServerHelloDone;
case certificate_verify: CertificateVerify;
case client_key_exchange: ClientKeyExchange;
case finished: Finished;
} body;
} Handshake;
```

○



Atenciosamente,



**Rodrigo Monção**

Diretor

Pré-vendas | Garage Tech

+55 61 3963-1776 | +55 61 99812-3588

[rodrigo@grgtech.io](mailto:rodrigo@grgtech.io)

[grgtech.io](http://grgtech.io)

SIG Quadra 2 Lote 420, Ed. City Offices, Brasília-DF, Brasil

Em sex., 21 de fev. de 2025 às 16:01, Informática GETIC-CFMV <[informatica@cfmv.gov.br](mailto:informatica@cfmv.gov.br)> escreveu:  
Prezado sr. Rodrigo, boa tarde.

Ficamos com algumas dúvidas no conteúdo do documento enviado.

Seguirei com a numeração dos itens do ANEXO G.

- No item 2.17, refere-se a: Permitir a criação de perfis de usuários a partir do qual se determinem parâmetros individuais de QoS, VLAN, políticas de firewall e criptografia de tráfego.

- <https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/GUID-6EC7C11A-AF2D-4AC0-ADFC-8FDCA3DABD80.shtml>
- Página 516/517
- ExtremeIoT Essentials in ExtremeCloud IQ User Profiles

Durante a análise não identificamos referência na documentação indicada referente a existência de memória não volátil (NVRAM). Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.6, refere-se a: Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior;

- <https://extr-p-001.sitecorecontenthub.cloud/api/public/content/7460a7c327ea455d8cc806fcbc9d07b7?v=43d958cf>

Durante a análise não identificamos referência na documentação indicada referente a existência de memória não volátil (NVRAM). Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.8, refere-se a: Possibilitar Backup e Restore da configuração por meio da interface gráfica;, onde no documento enviado por esta empresa contém a seguinte indicação:
  - [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
  - Página 429
  - Device Management Servers

Durante a análise identificamos se tratar de configuração para switch e não wireless (AP). Tendo em vista ao final do bloco de configuração fazer alusão a configurações de switch (Related Topics Configure Switch Devices on page 427) e o bloco desta features e/ou configuração está agrupada dentro do gerenciamento de switches (Configure Switch Devices). Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.28, refere-se a: Deverá suportar filtro de conteúdo;
  - [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/ExtremeCloud_IQ_24_6_0_User_Guide.pdf)
  - Página 141
  - URL Filtering

Durante a análise identificamos se tratar de configuração para routers. Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.29, refere-se a: Deverá implementar firewall com capacidade de rastreamento do estado da conexão (stateful firewall);
  - [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme\\_Cloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme_Cloud_IQ_24_6_0_User_Guide.pdf)
  - Página 272
  - Configure Classifier Map Services

Durante a análise identificamos se tratar de configuração para routers relacionados a WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.30, refere-se a: Deverá permitir a criação de políticas de firewall em camada 7 e sua associação de forma dinâmica de acordo com a identidade do usuário autenticado com o ponto de acesso operando no modo autogerenciado ou gerenciado por Controladora WLAN;
  - <https://extr-p-001.sitecorecontenthub.cloud/api/public/content/7460a7c327ea455d8cc806fcb-c9d07b7?v=43d958cf>
  - 7
  - Security

Durante a análise identificamos se tratar de configuração para routers relacionados a WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.31, refere-se a: Deverá implementar firewall com capacidade de rastreamento do estado da conexão (stateful firewall);
  - [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme Cloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme%20Cloud_IQ_24_6_0_User_Guide.pdf)
  - Página 259
  - Add IP Firewall Policies
  
  - 26797-ExtremeCloud-IQ-DS-F.pdf
  - Página 9
  - Application, network, and MAC layer firewall policy rules

Durante a análise identificamos se tratar de configuração para routers relacionados a SD-WAN e não a wireless, WLAN ou AP. Solicitamos o esclarecimento e indicação correta para comprovação deste item.

- No item 3.46, refere-se a: Deverá suportar sua própria autenticação com o controlador via certificado digital;

- [https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme Cloud\\_IQ\\_24\\_6\\_0\\_User\\_Guide.pdf](https://documentation.extremenetworks.com/ExtremeCloud%20IQ%20v24.6.0%20User%20Guide/downloads/Extreme%20Cloud_IQ_24_6_0_User_Guide.pdf)
- Pagina 324/325
- Create a Certificate and Key

Durante a análise identificamos se tratar de criação ou importação de certificados, mas não identificamos a integração para comunicação do software Extreme Cloud IQ e os dispositivos. Solicitamos o esclarecimento e indicação correta para comprovação deste item.

Solicito a resposta sobre estes questionamentos até 22/2/2025 às 23h para que possamos dar prosseguimento à habilitação de sua empresa.

Aguardo retorno.

At.te

Leonardo Stefan  
CFMV / GETIC / SESEG

---

# Documento Digitalizado Público

## Troca email com a GRG Tech - Segunda Diligencia.

**Assunto:** Troca email com a GRG Tech - Segunda Diligencia.  
**Assinado por:** Marcia Marto  
**Tipo do Documento:** EMAIL  
**Situação:** Finalizado  
**Nível de Acesso:** Público  
**Tipo do Conferência:** Documento Original

Documento assinado eletronicamente por:

- **Márcia Fernanda de Macedo Marto, Empregado - CMSUP - SESEG**, em 23/02/2025 15:04:34.

Este documento foi armazenado no SUAP em 23/02/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.cfmv.gov.br/verificar-documento-externo/> e forneça os dados abaixo:

**Código Verificador:** 1002939

**Código de Autenticação:** c2ba18f30a

