COMPANHIA DE PROCESSAMENTO DE DADOS DE PORTO ALEGRE – PROCEMPA
PREGÃO ELETRÔNICO PE N 006/2025
PROCESSO SEI 24.12.000001330-3

OBJETO: Contratação de empresa para fornecimento de solução de Segurança de E-mail (Secure E-mail Gateway - inbound e outbound), que contemple a instalação e a configuração da solução e das políticas de proteção, que seja entregue em appliance de máquina virtual, com a solução embarcada, a ser instalado em ambiente virtualizado próprio da PROCEMPA, com garantia e suporte de 12 meses, renováveis por mais 48 meses, com possibilidade de consumo de serviços técnicos especializados, sob demanda, para aplicação de melhores práticas de operação, conforme necessidades da PROCEMPA.

INTEGRASUL SOLUÇÕES EM INFORMÁTICA LTDA, pessoa jurídica de direito privado, inscrita no CNPJ sob nº 106.249.471/0001-14, com endereço em Rua Alagoas, 99 Bairro Jardim América, Caxias do Sul - RS, neste ato representado pelo seu representante legal MARCELO TRAVI PACHECO, vem respeitosamente, perante V. Sa., da Lei nº13.303/16, interpor as CONTRARRAZÕES ao recurso interposto pela empresa SCUNNA S/A, sociedade empresária de direito privado, com sede em Porto Alegre/RS, na Avenida Borges de Medeiros, 2233, sala 1302, CEP 90.110-910, inscrita no CNPJ/MF sob o nº 91.797.498/0001-10

4.67. A solução deve possibilitar quarentena automática de anexos criptografados

Contra-argumentos:

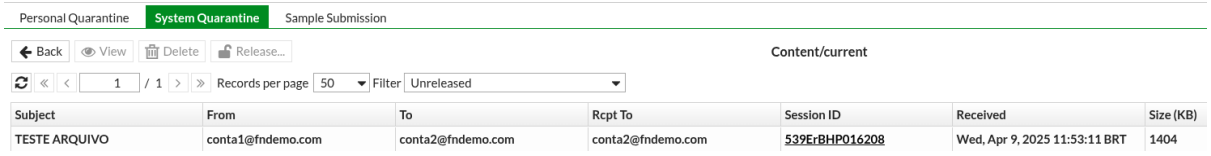
Usando o item Profile > Content  através de “Handling Archive” com “Action” em política para “Quarentena”, todo e qualquer anexo criptografado será quarentenado.
https://docs.fortinet.com/document/fortimail/7.6.2/administration-guide/921588/configuring-content-profiles-and-contentaction-profiles

Abaixo log de bloqueio:

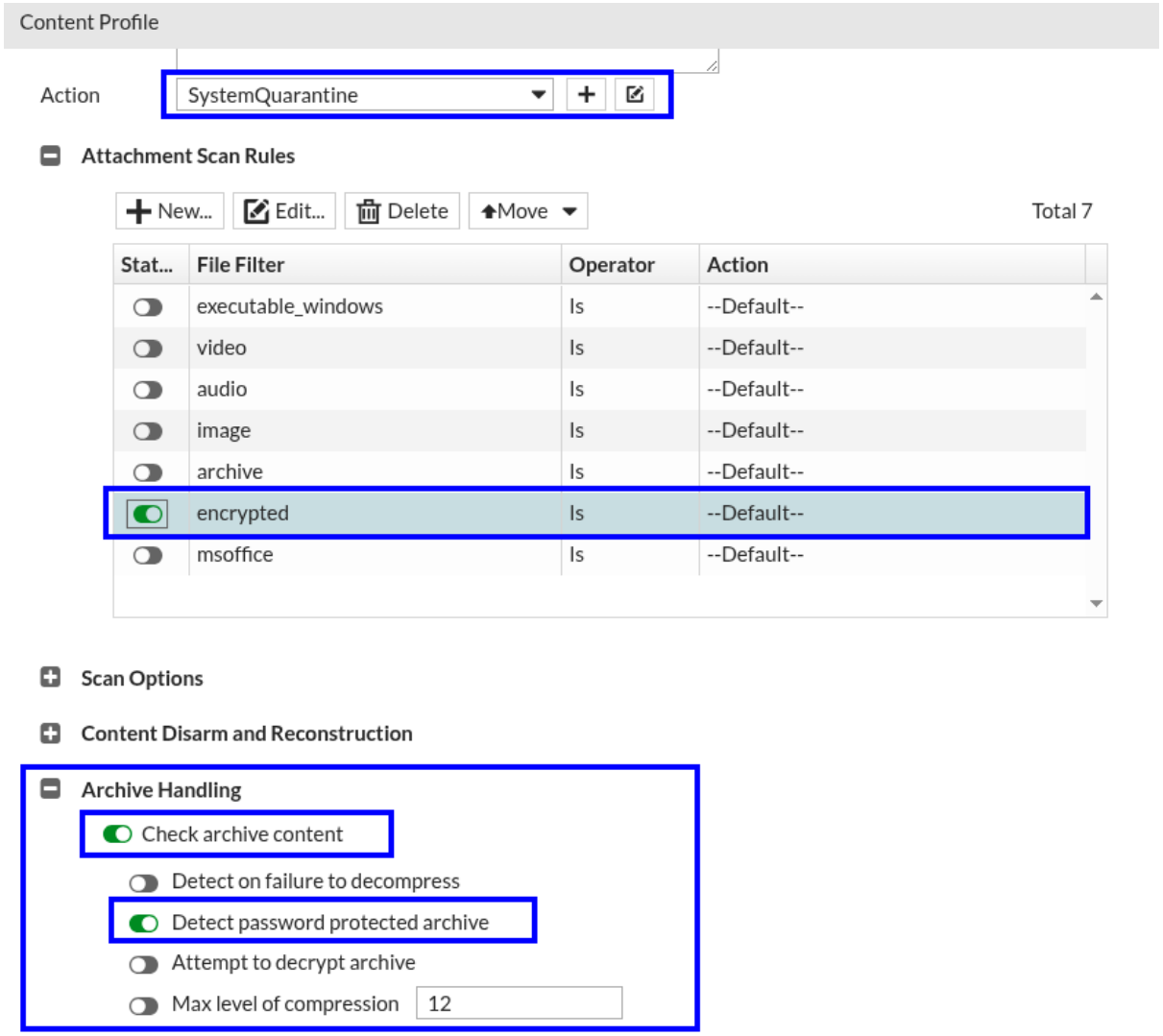
Log Details: 0300016209

| Column | Content |
|---|---|
| Date | 2025-04-09 |
| Time | 11:53:11.946 |
| Message | File name: arquivo.zip, detected by Content Filter, filetype application/openssl-encrypted-data, attachment scan rule: encrypted |
| Session ID | 539ErBHO016208-539ErBHP016208 |
| From | conta1@fndemo.com |
| To | conta2@fndemo.com |
| Subject | TESTE ARQUIVO |

Item na quarentena:




Perfil com ações definidas:



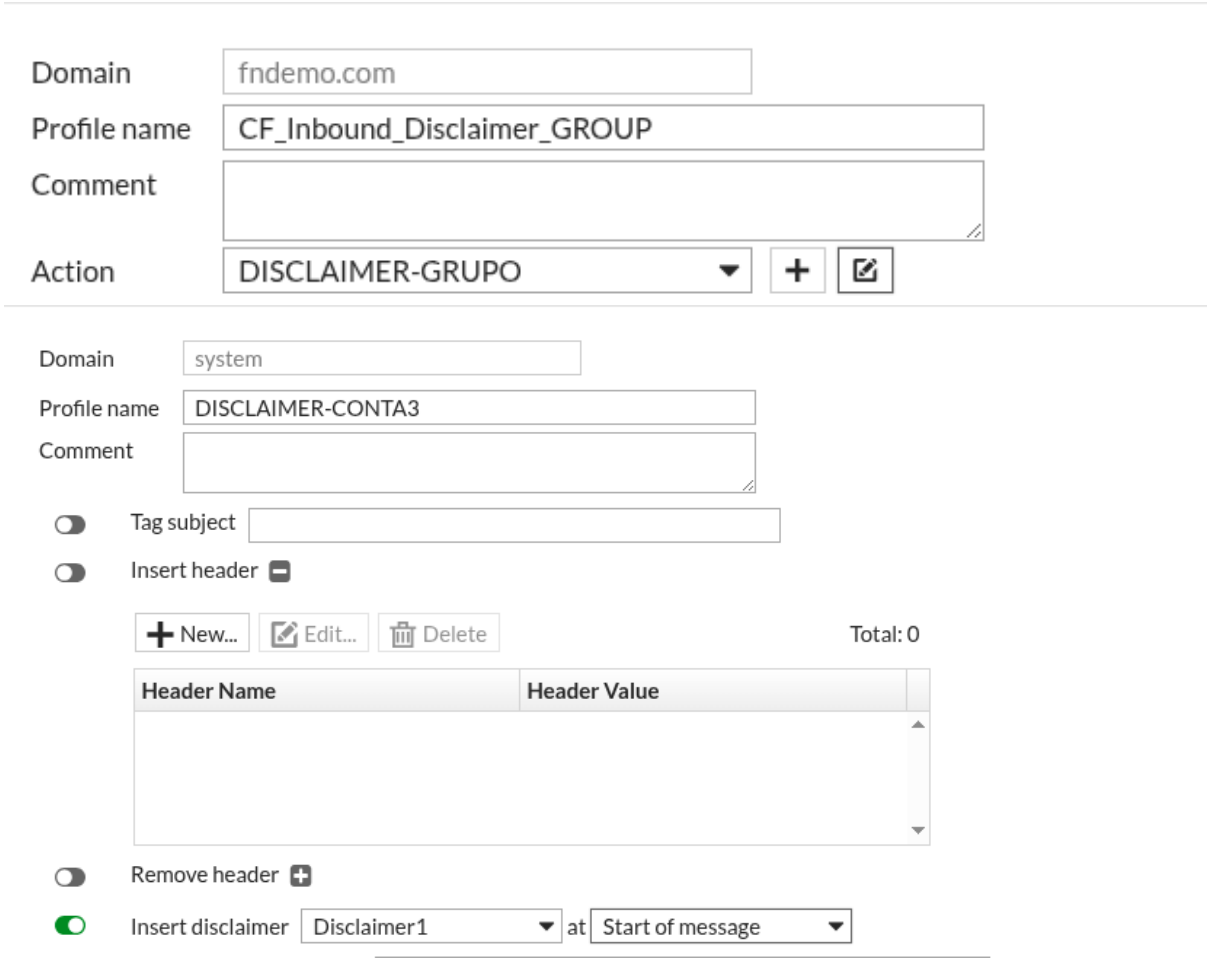
4.80. Deve suportar aplicação de “disclaimers” personalizados para usuários e grupos diferentes

Contra-argumentos:
Fortimail poderá ter um “disclaimer” para usuários, grupos de usuários ou domínio, definido por **Profile**, adicionando em **Content**.

Abaixo imagem de como ficaria aplicado em políticas:

| Stat... | ID | Domain Name | Sender Pattern | Recipient Pattern | AntiSpam | AntiVirus | Content |
|---|---|---|---|---|---|---|---|
| | 4 | system | *@* | conta3@fndemo.com | | | CF_Inbound_Disclaimer_Conta3 |
| | 3 | system | *@* | conta2@fndemo.com | | | CF_Inbound |
| | 1 | system | *@* | *@* | | | CF_Inbound |
| | 2 | fndemo.com | *@* | *@fndemo.com | | | CF_Inbound_Disclaimer_GROUP |
| | 1 | fndemo.com | *@* | GROUP | | | CF_Inbound_Disclaimer_GROUP |

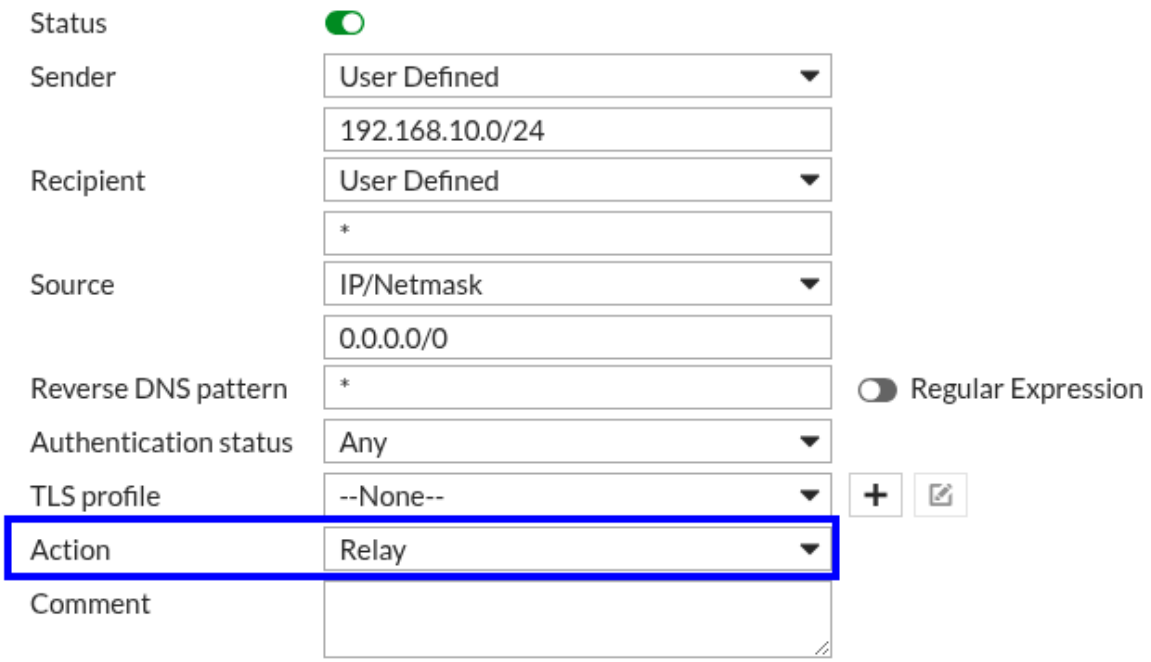
E abaixo a inserção ou não de “disclaimers”:



4.9. Deve permitir a autorização de quantidade ilimitada de endereços IPs no ambiente para envio de mensagens (função de relay).

Contra-argumentos:

Entende-se que o item define que o Gateway de e-mail possa atuar como relay sem restrição de origens. Dessa forma, com a aplicação de policies indicando quais IPs podem utilizar o serviço como relay ou open relay sem limites de IPs no ambiente.

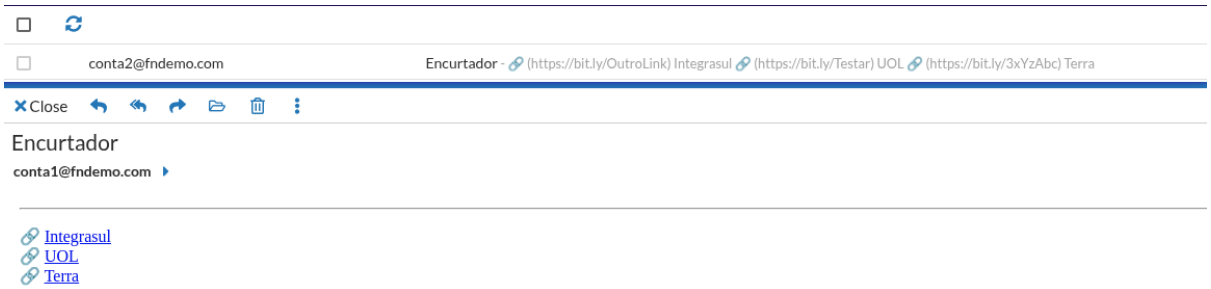


4.104.2. Assegurar que links de URLs suspeitas sejam dinamicamente reescritas antes que o e-mail seja entregue ao destinatário. Cada vez que um usuário clica em um destes links esteja ele na empresa ou em um local remoto, deverá ser exibido uma notificação de bloqueio. A análise deve abranger URLs encurtadas;

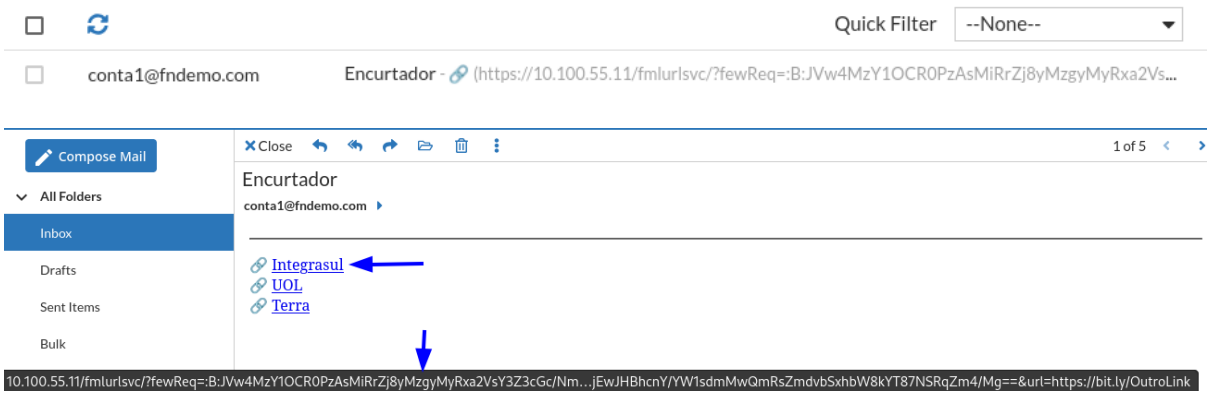
Contra-argumentos

A solução FortiMail contempla a sobrescrita de URL mesmo sendo encurtadas.

Abaixo temos screenshot de como o e-mail é enviado, apresentando a URL encurtada:




E abaixo temos o e-mail recebido no destino já com a URL reescrita:



4.106. Caso o processo de análise dinâmico seja realizado em infraestrutura em nuvem do fabricante, este deve explicar como a privacidade das informações é mantida;

Contra-argumentos:

Arquivos e URLs suspeitos são automaticamente submetidos do FortiMail para a FortiSandbox Cloud por meio de conexão segura (HTTPS/TLS), garantindo a confidencialidade dos dados em trânsito.

Os artefatos analisados são mantidos apenas durante o ciclo de inspeção comportamental e eliminados após o processamento, sem persistência em armazenamento permanente.

A Fortinet não retém dados pessoais identificáveis (PII) sem consentimento explícito. As amostras são anonimizadas, sempre que aplicável, e utilizadas exclusivamente para detecção de ameaças.

A solução está em conformidade com o GDPR e demais regulamentações de proteção de dados aplicáveis (https://trust.fortinet.com/product/default/gdpr-eu-us-dpf).

Abaixo link com todas as certificações de privacidade e dados da Fortinet:
https://trust.fortinet.com/

4.115. A proteção de URL deverá identificar se URL é maliciosa e redirecionar o usuário para uma página com uma notificação de bloqueio e ter a opção para descartar o e-mail 4.118. Se após a análise for constatado site malicioso, o sistema deverá exibir mensagem de alerta e o site será substituído por página de bloqueio criada e disponibilizada através da solução.

Contra-argumentos:

**ITENS 4.115 e 4.118**
É possivel mostrar para usuário tela de bloqueio, e o sistema tem a opção de rejeitar, conforme imagens abaixo:

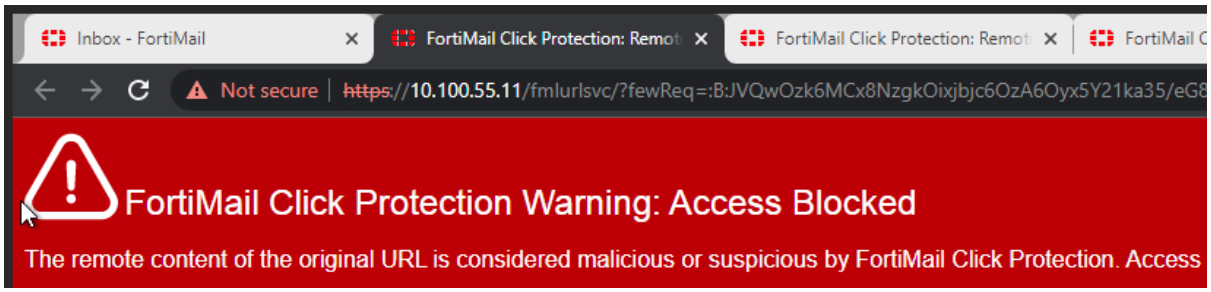
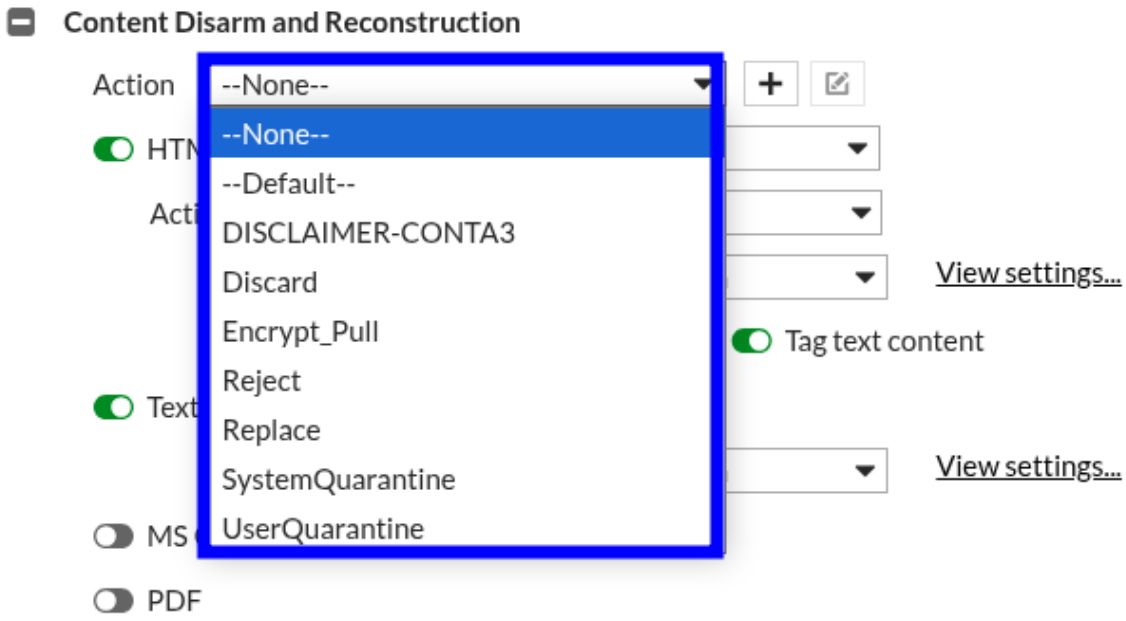


Imagem abaixo com opções de descarte:




4.121. A proteção de URL deverá reescrever links para os protocolos HTTP, HTTPS e FTP, URLs que comecem com “www” independente do protocolo.

Contra-argumentos:

Conforme documentação disposta em documentação Fortinet pode-se identificar (também imagens abaixo), que URLs absolutas com esquema no nome (protocolo) como: HTTPS, HTTP e **FTP**. Então pode ser concluído, que sim, a ferramenta FortiMail contempla protocolo FTP.

| | | |
|---|---|---|
| url-checking {aggressive \| extreme \| strict} | If you enable a FortiGuard scan or SURBL scan in an antispam profile, then FortiMail scans for blocklisted URLs in the email message body.<br>Types of URLs that URL filtering can scan include:<br>• **Absolute URLs** — URL syntax with scheme name (protocol), such as `http`, `https`, and `ftp`. They often only include a domain name. Example: `http://www.example.com`<br>• **Reference URLs** — No scheme name. Example: `example.com`<br>URLs in email can also be written in plain text instead of as clickable HTML links. While not technically a URL, the domain name of the sender can also be inspected.<br>By default, FortiMail scans for absolute URLs only. If you need to improve the spam catch rate or reduce false positives, you can change this. Select which to scan for.<br>• `strict`: Absolute URLs only.<br>**Note:** Websites without "http" or "https" but starting with "www" are also treated as absolute URLs. Example: `www.example.com`<br>• `aggressive`: Like `strict`, but also inspect reference URLs. Also check the domain name of the sender in the SMTP envelope (`MAIL FROM:`) and message header (`From:` and `Reply-To:`).<br>• `extreme`: Like `aggressive`, but also inspect URLs in plain text format. | strict |

### URL types

There are two types of URLs:

- Absolute URLs strictly follow the URL syntax and include the URL scheme names, such as "http", "https", and "ftp". For instance, http://www.example.com.
- Reference URLs do not contain the scheme names. For instance, example.com.

By default, FortiMail scans for absolute URLs.

You can use the following CLI command to change the default setting:

```
config antispam settings
  set uri-checking {aggressive | strict}
end
```

- `aggressive`: Choose this option to scan for both the absolute and reference URLs.
- `strict`: Choose this option to scan for absolute URLs only. Note that web sites without "http" or "https" but starting with "www" are also treated as absolute URLs. For instance, www.example.com.

For more information about this command, see FortiMail CLI Reference.

Face a todo exposto e com fundamento nas contrarazões arguidas, assim como nos princípios da motivação, eficiência, legalidade e formalismo moderado, considerando o interesse público, representando não só pela viabilidade de manutenção do presente certame, assim como ampliação do rol de concorrentes e garantia de fornecedor validado com expertise comprovada com muitos anos de mercado e atendimento a rigor à inúmeros órgãos públicos, solicitamos a manutenção do resultado final do certame onde a empresa Integrasul Soluções em Informática foi declarada vencedora.

Caxias do Sul, 09 de Abril de 2025.

Marcelo Travi Pacheco
Diretor Comercial

gov.br
Documento assinado digitalmente
MARCELO TRAVI PACHECO
Data: 09/04/2025 14:24:41-0300
Verifique em https://validar.iti.gov.br