ILUSTRÍSSIMO SENHOR PREGOEIRO DA PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S.A

Ref.: Pregão Eletrônico nº 10/2024

OI SOLUÇÕES S/A, inscrita no CNPJ nº 09.719.875/0001-12, sediada na Av Roque Petroni Junior, 999 – Conj 82 – Vila Gertrudes, São Paulo, SP, CEP: 04.707-910, doravante denominada simplesmente "Oi", vem, tempestivamente, por seus representantes legais, com fulcro no art. 59, § 1º da Lei 13303/2016, interpor

RECURSO ADMINISTRATIVO

em face da decisão do I. Pregoeiro da PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S.A, que desclassificou a sua proposta, pelas razões que passa a expor.

Caso este r. Pregoeiro entenda por indeferir o presente recurso, requer a remessa deste à digna autoridade superior, na forma de **RECURSO HIERÁRQUICO**, com fundamento no princípio constitucional do Duplo Grau de Jurisdição.

Nestes termos,

Pede deferimento.

Manaus - AM, 01 de novembro de 2024

Rubrica

DS

I - TEMPESTIVIDADE

O presente Recurso Administrativo tem por finalidade a reforma da decisão que desclassificou a Oi neste certame, por estar eivada de vícios de legalidade.

Para tanto, cumpre observar que o prazo decadencial é de **3 (TRÊS) DIAS ÚTEIS**, **CONTADOS DA LAVRATURA DA ATA, CONFORME SE DEPREENDE DO ITEM 4.3.1 DO EDITAL**.

No caso em tela, a intenção de recurso foi registrada no dia **30 DE OUTUBRO DE 2024 (QUARTA-FEIRA)**, sendo este, portanto, o marco inicial para contagem do prazo. Logo, o término para apresentação do Recurso Administrativo dar-se-á no dia **04 DE NOVEMBRO DE 2024 (SEGUNDA-FEIRA).**

Ademais, insta registrar que a contagem do prazo no procedimento licitatório obedecerá aos ditames da Lei n.º 14.133/2021, juntamente com as regras processuais comuns (Código de Processo Civil Brasileiro), **EXCLUINDO-SE O DIA DE INÍCIO E INCLUINDO-SE O DO VENCIMENTO** (artigo 183, Lei nº 14.133/2021 e artigo 184, *caput*, Código de Processo Civil).

Conclui-se, portanto, pela **TEMPESTIVIDADE** deste Recurso Administrativo.

II – BREVE SÍNTESE DOS FATOS

O objeto do presente certame consiste na contratação de empresa especializada para eventual Aquisição de Serviços Gerenciados de Segurança da Informação destinado a proteção das redes computacionais dos clientes da PRODAM compreendendo a alocação de equipamentos Firewall de Próxima Geração (Next Generation Firewall-NGFW), operação e monitoramento remoto em regime 24x7, software para o gerenciamento centralizado e emissão de relatórios, prestação de serviços para instalação e configuração da solução, suporte técnico do fabricante para o hardware com garantia da solução e licenciamento do software para atualização pelo período de 36 meses, treinamento oficial do fabricante e transferência de conhecimento da solução para a equipe da PRODAM.

Rubrica FHL DS MCFM

Assim, aberta a sessão em 10.10.2024, se credenciaram diversas empresas, dentre elas, a Oi Soluções S.A, conforme descrito na ata do pregão.

Após a etapa de lances, a Oi foi classificada em 1º lugar, tendo sido convocada para apresentar documentos de habilitação e proposta. Contudo, teve sua proposta desclassificada por supostamente não atender a diversos itens do Edital e Anexos.

Ocorre que a Comissão Julgadora cometeu um equívoco ao analisar a proposta enviada pela Oi, pois esta atendeu plenamente todos os requisitos e exigências contidas no instrumento convocatório.

É, pois, contra tal decisão que se insurge a Recorrente, eis que neste particular, não foi proferida em perfeita consonância com as normas e princípios norteadores dos atos da Administração Pública, senão vejamos.

III – MÉRITO

III.1- DA EQUIVOCADA DESCLASSIFICAÇÃO DA PROPOSTA DA OI SOLUÇÕES S.A

A OI Soluções S/A, foi declarada ARREMATANTE por apresentar o melhor preço de R$ 21.144.999,96, para a Administração pública, onde o valor estimado para contratação seria de R$ 32.244.384,26, ou seja, uma redução de 34,42%.

Após as análises da proposta e documentação técnica enviadas, fomos desclassificados por não atender cerca de 30 (trinta) itens, de acordo com a mensagem do Sr. Pregoeiro disponibilizada no chat do Comprasnet:

> ***Mensagem do Pregoeiro***
>
> *Informamos que a proposta da OI SOLUÇÕES S/A, classificada em primeiro lugar, não atende aos itens 2.1.4.15; 2.1.4.16; 2.1.8.5; 2.2.4.15; 2.2.4.16; 2.2.8.5; 2.3.4.15; 2.3.4.16; 2.3.8.5; 2.5.4.36; 2.5.4.37; 2.5.8.9; 2.5.8.16; 2.5.8.17; 2.5.8.18; 2.5.8.19; 2.5.8.20; 2.6.2.10; 2.6.4.36; 2.6.4.37; 2.6.8.9; 2.6.8.16; 2.6.8.17; 2.6.8.18; 2.6.8.19 e 2.6.8.20, referentes às exigências de qualificação técnica do Anexo 1-A – Especificações Técnicas.*
>
> ***Enviada em 17/10/2024 às 14:59:38h***

De acordo com as exigências do edital a empresa arrematante deveria comprovar o atendimento a todos os itens mediante envio de um ponto a ponto onde demonstrasse o pelo atendimento daquele item com a referência evidenciada juntamente com o link para esta comprovação e assim foi feito.

O ponto a ponto foi elaborado em parceria com o fabricante da solução ofertada que ratifica atender 100% das exigências técnicas do edital.

Além do ponto a ponto foi enviado juntamente com a proposta os arquivos do Datasheet onde consta todas as características e especificações de todos os equipamentos que serão fornecidos à PRODAM.

Ocorre que não foi dado a oportunidade da OI Soluções se defender/esclarecer, através de diligências, previstas em Lei e no próprio edital para sanar qualquer dúvida apontada nesta desclassificação.

Vejamos o que diz o Edital:

> *20.6 É facultado ao Pregoeiro, ou à Autoridade Superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.*

É fato que o edital torna facultativo, porém a Oi Soluções S/A não teve a oportunidade de esclarecer todos os questionamentos, sendo a mesma desclassificada e com isso chamou-se o segundo colocado e seguiu-se com o processo licitatório.

Sobre este tema, podemos esclarecer que as Diligências nas licitações são um ato administrativo que o órgão público utiliza para solicitar o detalhamento de informações sobre os licitantes, sejam as condições para execução, habilitações ou qualquer outra informação pertinente para o processo licitatório.

Um exemplo de como a diligência pode ocorrer em uma licitação seria a solicitação de que informações sobre uma habilitação técnica apresentadas por um participante sejam mais detalhadas.

A diligência também é muito usada para sanear dúvidas em relação às informações dos atestados de capacidade técnica, especialmente porque são

documentos produzidos por terceiros, os quais muitas vezes já possuem um padrão de texto para emissão desses documentos.

O desafio do gestor público é, portanto, estabelecer uma relação de equilíbrio e compatibilidade entre os princípios citados no parágrafo precedente e os do formalismo moderado e da supremacia do interesse público, sobretudo porque no ambiente concorrencial haverá quase sempre insatisfação por parte dos perdedores com o resultado da disputa, o que obriga o pregoeiro ou a comissão de licitação a assumirem a responsabilidade por decidir em cada caso concreto sobre a pertinência ou não da diligência.

Em linhas gerais, portanto, a diligência funciona como um recurso indispensável para a comissão de licitação ou o pregoeiro aproveitarem boas propostas para a administração pública desde que os erros, falhas ou omissões identificadas em planilhas ou documentos apresentados possam ser sanados ou esclarecidos sem violação ao princípio da isonomia entre os licitantes.

Por fim, não se trata de uma simples faculdade ou direito da administração, mas de verdadeiro poder-dever do gestor público, posto que não há discricionariedade para decidir fazer ou não a diligência, quando esta se mostrar cabível, sob pena de descartar uma boa proposta e, consequentemente, acarretar prejuízo econômico para o órgão/entidade contratante.

E neste sentido a OI Soluções não teve a oportunidade de ter esta diligência para sanar as dúvidas, com isso, esclarecemos abaixo todos os Itens apontados no parecer técnico sinalizados como não atendidos.

A OI Soluções, trabalha com um leque de parceiros/fabricantes que apoiam nas avaliações para definição dos equipamentos, onde são feitas analises minuciosas pelos engenheiros do fabricante afim de escolher o equipamento que atende a todas as especificações exigidas no edital.

Neste sentido, segue as respostas e esclarecimentos/justificativas comprovando o pleno atendimento de todos os itens que geraram nossa desclassificação e comprovados no ponto a ponto fornecido no momento do pregão.

1. 2.1 SERVIÇO DE PROTEÇÃO DE PERÍMETRO PEQUENO PORTE

1.1. Subitem 2.1.4.15

2.1.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

Referência/URL

"Enabling antivirus in a policy

Note: detalhe para a imagem demonstrando os diversos perfis de segurança que podem ser habilitados numa mesma policy."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/767732/enabling-antivirus-in-a-policy

Rubrica FHL DS MCFM

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Há luz do edital, nota-se que o referido item, é flexibilizado, informando que pode e não que deve. Independente do desejado por esta instituição, o FortiGate permite plenamente o uso compartilhado das funcionalidades de segurança em uma mesma regra de segurança.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, conforme Datasheet, tem como base seu sistema operacional, chamado FortiOS.

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Estas políticas de segurança são efetivas na proteção do ambiente rede, fazendo a inspeção localmente no appliance, da camada de rede até a aplicação de todo o tráfego passante (em linha), tomando as ações configuradas sem nenhuma dependência de comunicação ou integração de agente com os hosts de rede.

Ao acessar o link disponibilizado podemos perceber na imagem que, quando criamos uma política de segurança é possível habilitar diversos perfis de segurança dentro desta, como: Antivirus, Web Filter, DNS Filter, Application Control, IPS e outros.

Afim de não restar duvidas, será fornecido de forma complementar mais duas referências com mais informações:

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/583477/configuring-an-ips-sensor

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/254346/external-malware-block-list

Podemos observar de forma mais detalhada sobre os mecanismos de proteção que estão inclusos nos perfis de segurança que podem ser combinados para a criação da política.

Conforme documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/836396/antivirus e seus sublinks, é abordado explicações e orientações de como ativar o filtro de antivirus/antimalware.

Segundo documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/605868/dns-filter e seus sublinks, é abordado explicações e orientações de como ativar o perfil “DNS

Rubrica

DS

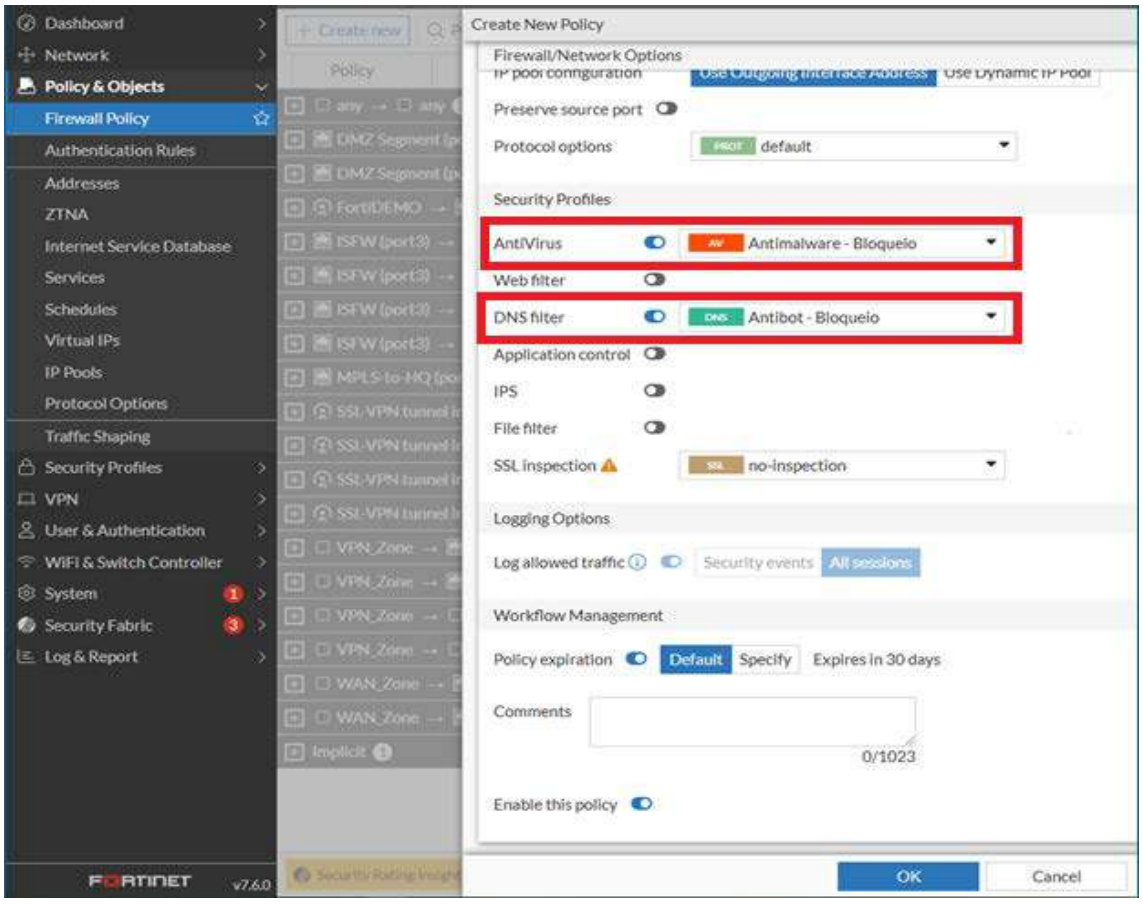
Filter” o qual tem a capacidade de identificar e bloquear comunicação de Botnets e tráfego de Comando e Controle (C&C).

O licenciamento do appliance FortiGate, ofertado para este certame, é o Bundle UTP, composto pelas seguintes funcionalidades destacadas pelos quadrados em vermelho:

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [2], AI-based Heuristic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [2] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [2]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		included with FortiCare Subscription		

Visando melhor explicar, segue uma imagem extraída da console com o objetivo de demonstrar a ativação dos perfis de segurança “Antimalware” e “DNS Filter”.

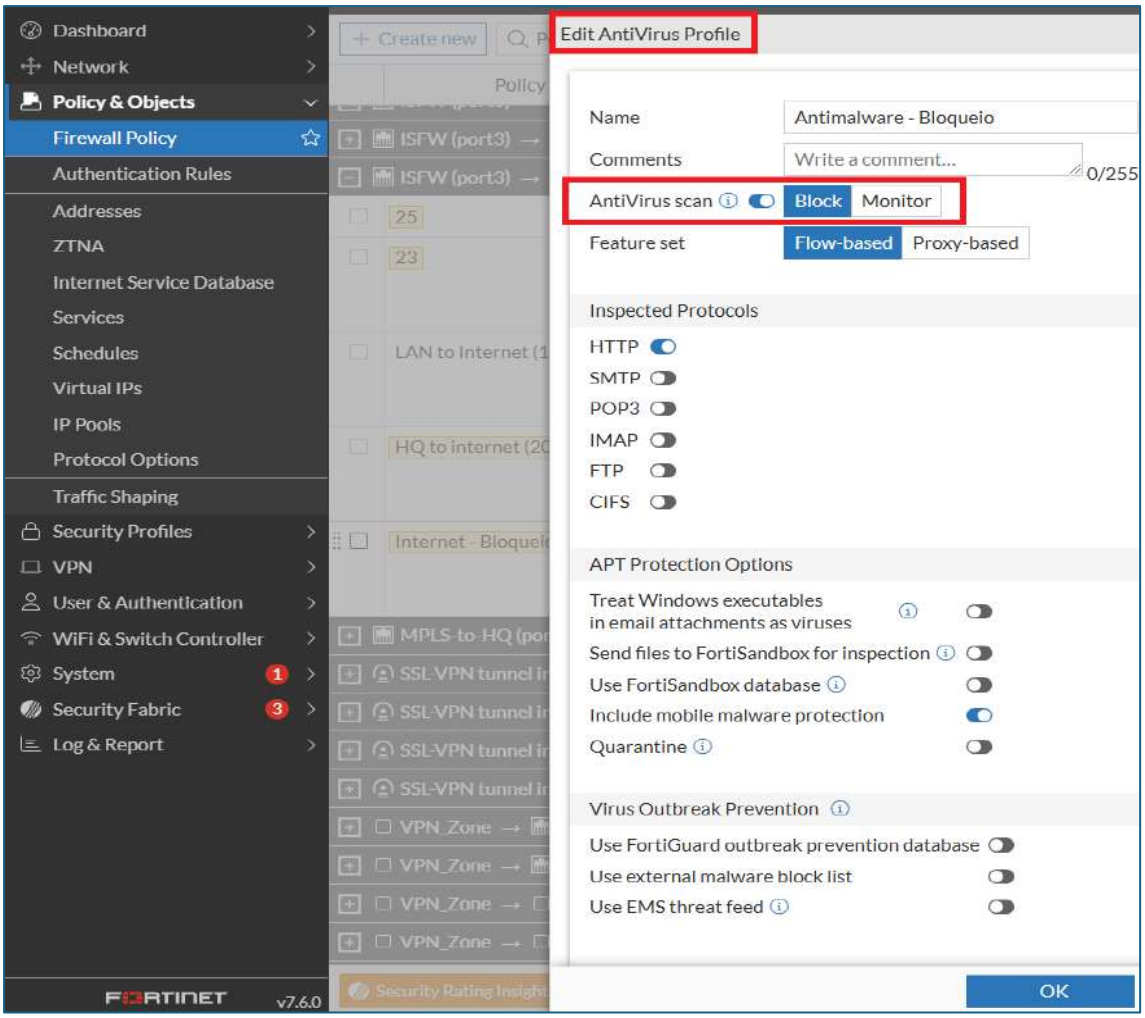


Note que nesta Imagem a criação da política de segurança, as chaves “AntiVirus” e “DNS Filter” ativas na mesma regras durante edição desta política.

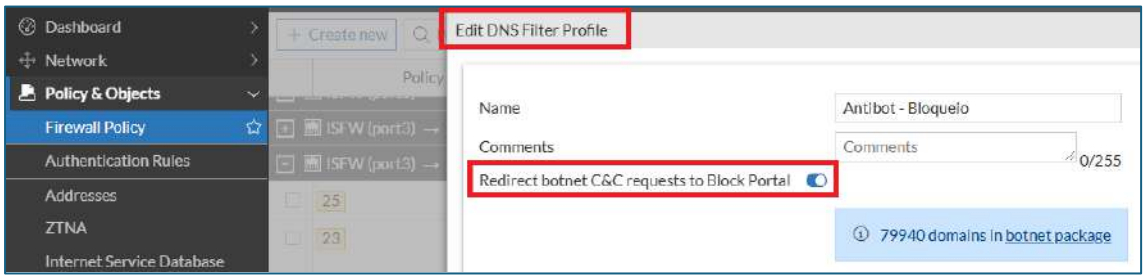
Rubrica

DS

Segue edição do perfil de segurança de “Antivirus”, com a ação de scan marcado para bloquear.



Segue edição do perfil de segurança de “DNS Filter”, com a ação de scan marcado para redirecionar as requisições de botnet para o portal de bloqueio da respectiva requisição.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

Rubrica

DS

1.2. Subitem 2.1.4.16

> *2.1.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;*

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

> ***Referência/URL***
>
> *Ordering the policy table*
>
> *Nota: para atender este item, pode-se clonar a policy existente, ajustar os perfis de segurança para monitorar/não bloquear e posicionar a nova policy acima da existente.*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/508696/ordering-the-policy-table.*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

O mecanismo de clonagem de uma política de segurança permite que as regras originais ou já criadas e homologadas sejam duplicadas sem que ocorra alterações na configuração original.

A partir disso é possível fazer modificações no que foi duplicada para se ajustar a uma nova necessidade. Para priorizar a nova política em relação as políticas operacionais do equipamento, é possível que ela seja posicionada antes da original para que seja acionada antes das outras que já estavam em operação.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, tem como base seu sistema operacional, chamado FortiOS.

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Para o pleno atendimento do requisito supra citado, basta configurar quatro perfis de segurança, sendo dois de “Antimalware” e dois de “DNS Filter”, onde para cada perfil, teremos um com ação de bloqueio e o outro com ação de monitoração.

Uma vez definido os perfis de segurança, basta criar duas regras de segurança, sendo uma contendo os perfils de monitoração e outra regra com contendo os perfis de bloqueio.

De forma complementar podemos observar conforme consta na url https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-policy-order-works-on-FortiGate/ta-p/207381 , nota-se conforme trecho: “The policies are consulted from top to bottom. The first rule that matches is applied and subsequent rules are not evaluated.”, que a execução das políticas de segurança são de cima para baixo (top/down), onde se fizer o match ou encontro da regra, a busca cessará nesta regra encontrada.

Trazendo o entendimento conforme respectivo requisito, quando esta instituição desejar ativar o modo de monitoração, teremos a política de monitoração com seus

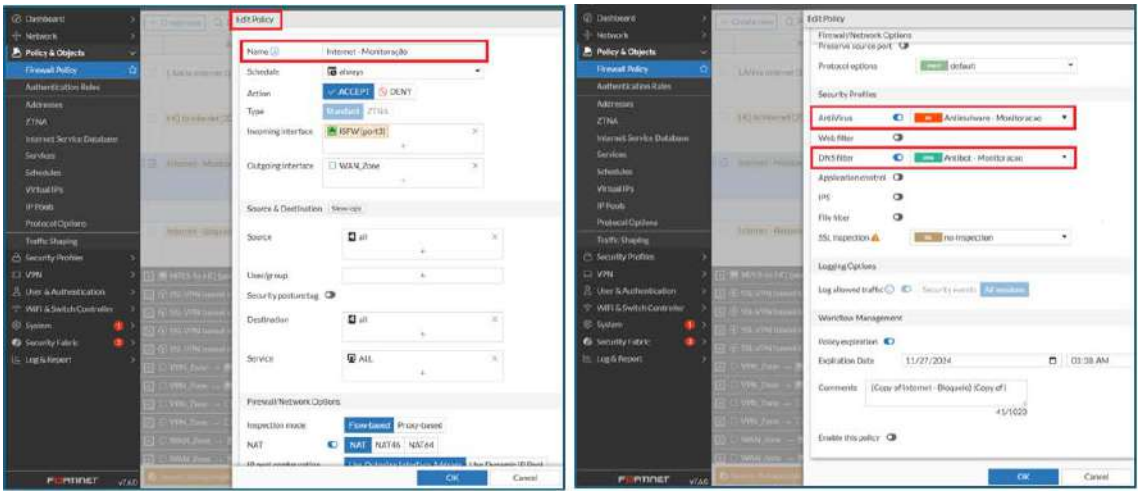
respectivos perfis já em modo de monitoração (sem nenhuma associação ou uso dos outros perfis já em uso) conforme nomes distintos, sendo ativada quando necessário e quando desejar voltar ao modo normal de operação, basta novamente desativar esta política de firewall.

Visando elucidar a dinâmica explicada, seguem imagens extraídas da console para melhor entendimento:

Nesta Imagem da base de políticas, com destaque em vermelho, duas políticas de firewall, seguidas de seus respectivos perfis nomes específicos e especificidades:

- Internet – Monitoração, sombreada em vermelho por estar com o status desabilitada, tendo os perfis de segurança “Antibot-Monitoração” e “Antimalware-Monitoração”;
- Internet – Bloqueio, tendo os perfis de segurança “Antibot-Bloqueio” e “Antimalware-Bloqueio”.

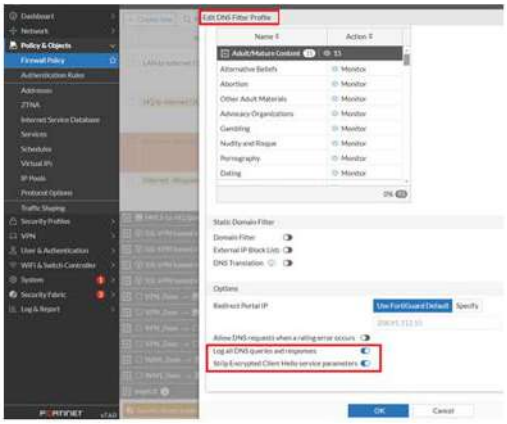
Segue imagem da política de segurança de nome “Internet - Monitoração”, com seus respecitvos perfis de monitoração de “Antimalware” e “DNS Filter” (Antibot).



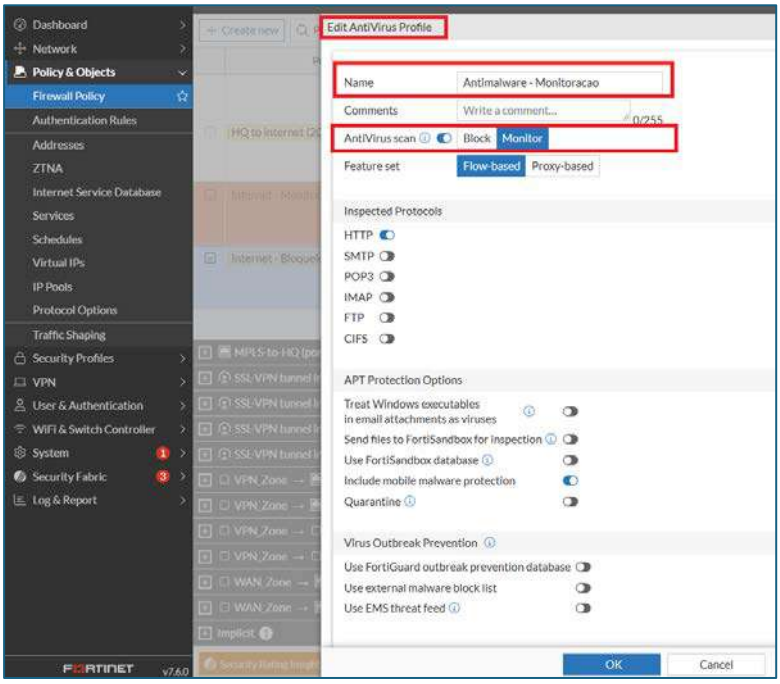
Rubrica

DS

Segue trecho do perfil de “DNS Filter”, de nome “Antibot - Monitoracao” (antibot) em monitoração com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas.



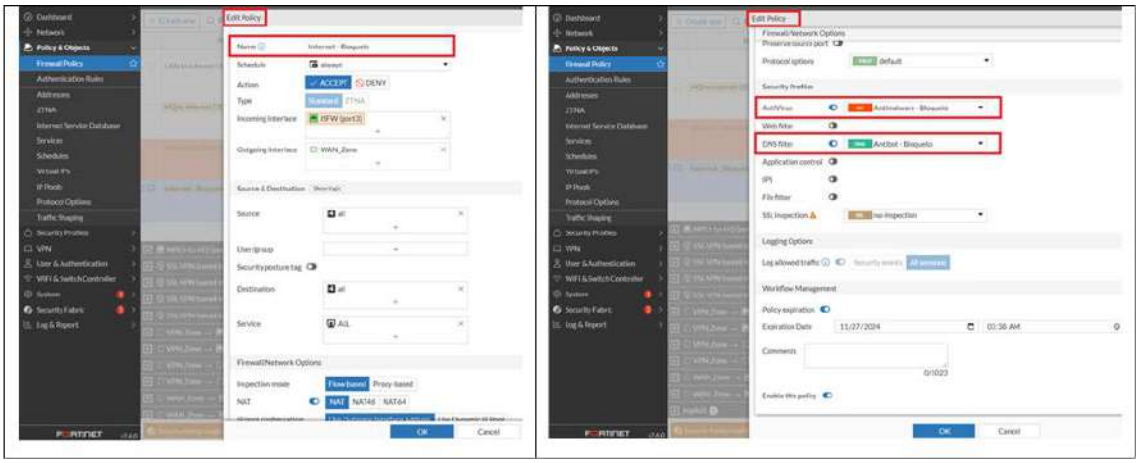
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Monitoracao” com a ação “Antivirus Scan” em “Monitor”.



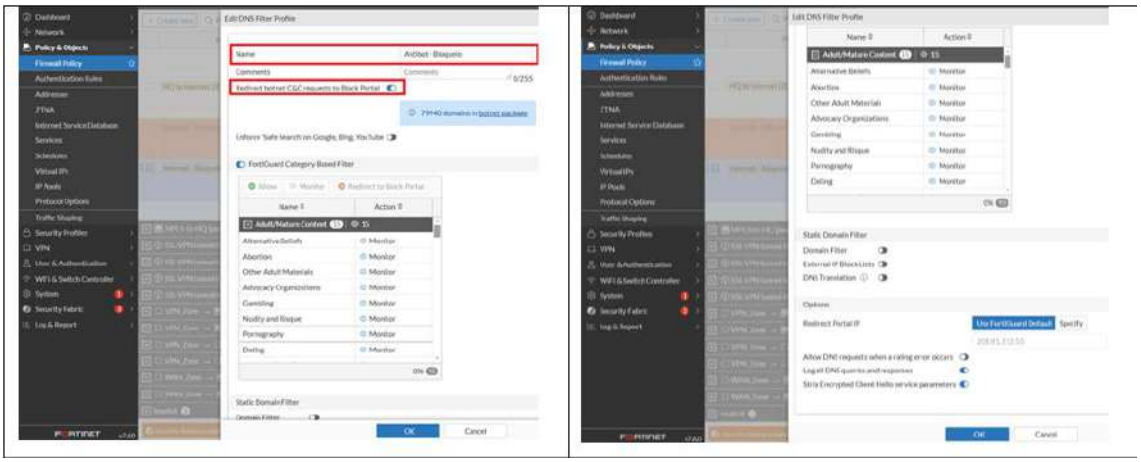
Rubrica

DS

Segue imagem da política de segurança de nome “Internet - Bloqueio”, com seus respecitvos perfis de bloqueio de “Antimalware” e “DNS Filter” (Antibot).



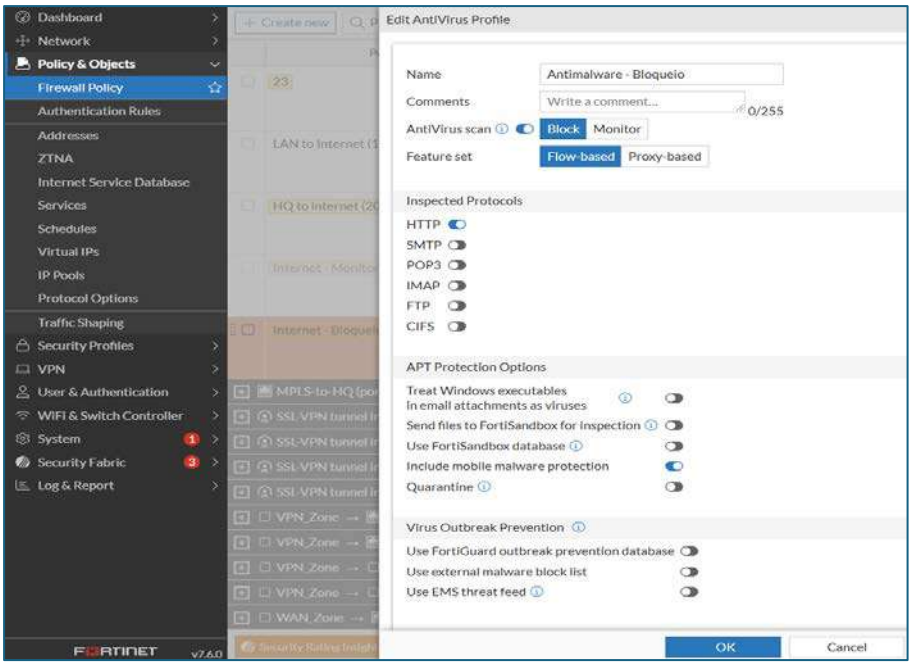
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas



Rubrica

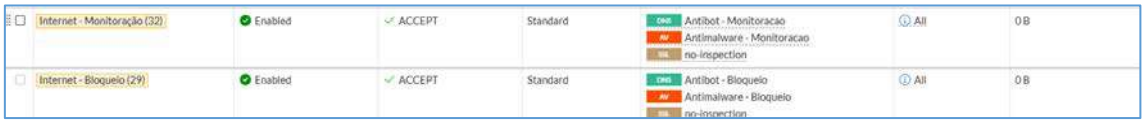
DS

Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a ação “Antivirus Scan” em “Block”.



Segue políticas de segurança em produção com a política de bloqueio ativada e a de monitoração desativada.

Segue políticas de segurança em produção com a política de monitoração ativada, como firewall analisa top/down, apenas a regra “Internet-Monitoração” processará o tráfego.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

1.3. <u>Subitem 2.1.8.5</u>

2.1.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

<u>Referência/URL</u>

"Phase 1 configuration (...)

Monitor tunnel for failover

Rubrica

DS

Monitor a site-to-site tunnel to guarantee operational continuity if the primary tunnel fails. Configure the secondary phase 1 interface to monitor the primary interface."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/790613/phase-1-configuration

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A comprovação utilizada nesse item foi apenas da funcionalidade de estabelecimento do túnel.

É necessário complementar a comprovação da funcionalidade de monitoramento do túnel remoto mencionando funcionalidade de health check que o equipamento também possui sem a necessidade de licenças adicionais.

A funcionalidade *Performance SLA link health monitoring* mede a integridade dos links conectados às interfaces dos membros SD-WAN enviando sinais de sondagem por meio de cada link para um servidor ou usando informações da sessão capturadas nas políticas de firewall e medindo a qualidade do link com base na latência, no jitter e na perda de pacotes.

Se um link falhar em todas as verificações de integridade, as rotas desse link serão removidas do grupo de balanceamento de carga de links SD-WAN e o tráfego será roteado por outros links.

Quando o link estiver funcionando novamente, as rotas serão restabelecidas automaticamente. Isso evita que o tráfego seja enviado para um link quebrado e se perca.

De forma complementar segue mais um link onde conseguimos comprovar o atendimento ao referido item:

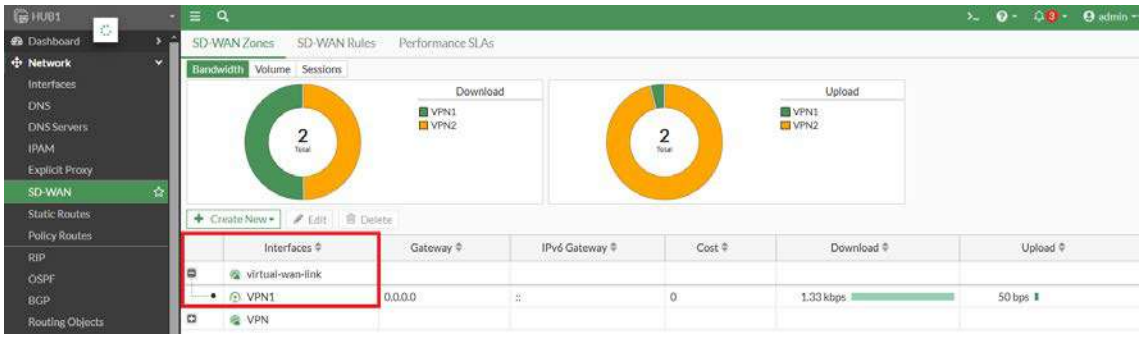
https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/580649/link-health-monitor

Em busca de melhor esclarecer os entendimentos sugeridos, a abordagem do SD-Wan normalmente refere-se ao conceito de vários links, conforme url https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/218559/configuring-the-sd-wan-interface , no trecho “The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others).

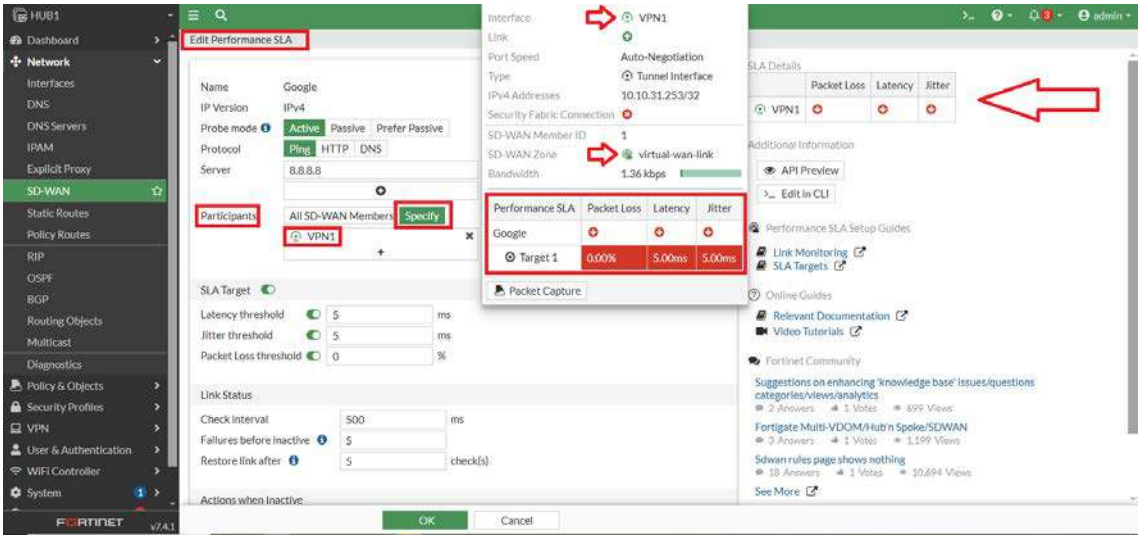
Rubrica FHL

DS

Isso não significa que para a monitoração de link funcionar necessite de vários links, ou de um link secundário, note a interface de nome “VPN1” associada a interface SD-Wan de nome “virtual-wan-link”:



Note o “Performance SLA”tendo como integrante apenas a interface lógica “VPN1”. É nítido conforme imagem anterior e esta, que apenas a interface “virtual-wan-link” com apenas um link ora o “VPN1”, permitindo ver em tempo real a monitoração do link com tempo de resposta por fator de monitoração e saúde (Packet Loss, Latency e Jitter).



Concluindo assim que o FortiGate é capaz de monitorar a saúde do túnel através da performance SLA utilizando um endereço IP que faça parte to túnel remoto com apenas uma interface ou link em uso.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

2. 2.2 SERVIÇO DE PROTEÇÃO DE PERÍMETRO MÉDIO PORTE

2.1. Subitem 2.2.4.15

2.2.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

Referência/URL

Rubrica

DS

"Enabling antivirus in a policy

Note: detalhe para a imagem demonstrando os diversos perfis de segurança que podem ser habilitados numa mesma policy."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/767732/enabling-antivirus-in-a-policy

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Há luz do edital, nota-se que o referido item, é flexibilizado, informando que pode e não que deve. Independente do desejado por esta instituição, o FortiGate permite plenamente o uso compartilhado das funcionalidades de segurança em uma mesma regra de segurança.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, conforme Datasheet, tem como base seu sistema operacional, chamado FortiOS.

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Estas políticas de segurança são efetivas na proteção do ambiente rede, fazendo a inspeção localmente no appliance, da camada de rede até a aplicação de todo o tráfego passante (em linha), tomando as ações configuradas sem nenhuma dependência de comunicação ou integração de agente com os hosts de rede.

Ao acessar o link disponibilizado podemos perceber na imagem que, quando criamos uma política de segurança é possível habilitar diversos perfis de segurança dentro desta, como: Antivirus, Web Filter, DNS Filter, Application Control, IPS e outros.

Afim de não restar duvidas, será fornecido de forma complementar mais duas referências com mais informações:

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/583477/configuring-an-ips-sensor

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/254346/external-malware-block-list

Podemos observar de forma mais detalhada sobre os mecanismos de proteção que estão inclusos nos perfis de segurança que podem ser combinados para a criação da política.

Conforme documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/836396/antivirus

e seus sublinks, é abordado explicações e orientações de como ativar o filtro de antivirus/antimalware.

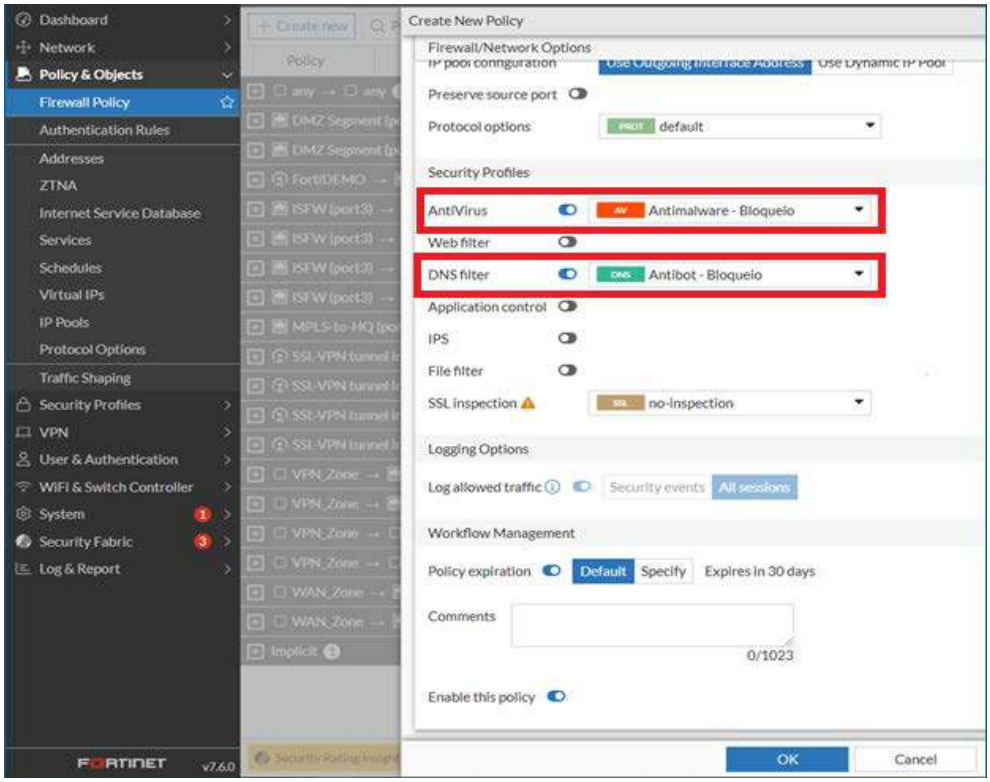
Segundo documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/605868/dns-filter e seus sublinks, é abordado explicações e orientações de como ativar o perfil “DNS Filter” o qual tem a capacidade de identificar e bloquear comunicação de Botnets e tráfego de Comando e Controle (C&C).

O licenciamento do appliance FortiGate, ofertado para este certame, é o Bundle UTP, composto pelas seguintes funcionalidades destacadas pelos quadrados em vermelho:

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		included with FortiCare Subscription		

Visando melhor explicar, segue uma imagem extraída da console com o objetivo de demonstrar a ativação dos perfis de segurança “Antimalware” e “DNS Filter”.

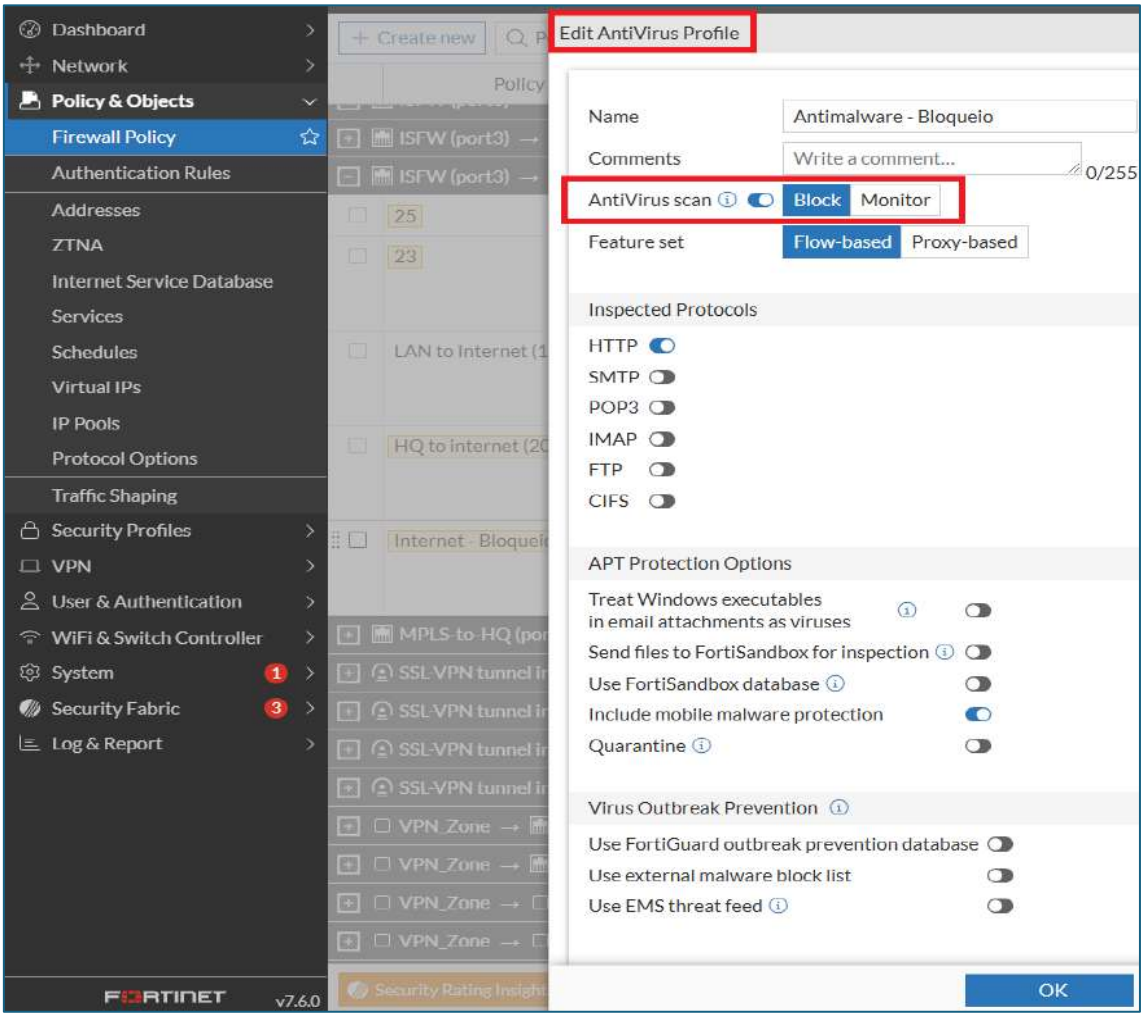


Rubrica

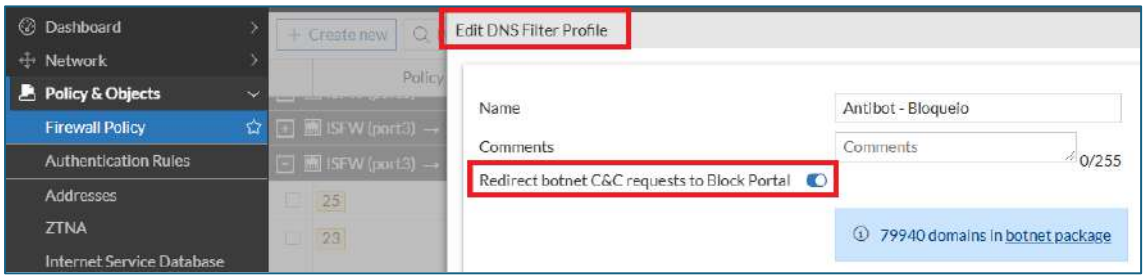
DS

Note que nesta Imagem a criação da política de segurança, as chaves “AntiVirus” e “DNS Filter” ativas na mesma regras durante edição desta política.

Segue edição do perfil de segurança de “Antivirus”, com a ação de scan marcado para bloquear.



Segue edição do perfil de segurança de “DNS Filter”, com a ação de scan marcado para redirecionar as requisições de botnet para o portal de bloqueio da respectiva requisição.



Rubrica

DS

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

2.2. Subitem 2.2.4.16

> *2.2.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;*

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

> ***Referência/URL***
>
> *Ordering the policy table*
>
> *Nota: para atender este item, pode-se clonar a policy existente, ajustar os perfis de segurança para monitorar/não bloquear e posicionar a nova policy acima da existente.*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/508696/ordering-the-policy-table*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

O mecanismo de clonagem de uma política de segurança permite que as regras originais ou já criadas e homologadas sejam duplicadas sem que ocorra alterações na configuração original.

A partir disso é possível fazer modificações no que foi duplicada para se ajustar a uma nova necessidade. Para priorizar a nova política em relação as políticas operacionais do equipamento, é possível que ela seja posicionada antes da original para que seja acionada antes das outras que já estavam em operação.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, tem como base seu sistema operacional, chamado FortiOS.

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Para o pleno atendimento do requisito supra citado, basta configurar quatro perfis de segurança, sendo dois de “Antimalware” e dois de “DNS Filter”, onde para cada perfil, teremos um com ação de bloqueio e o outro com ação de monitoração.

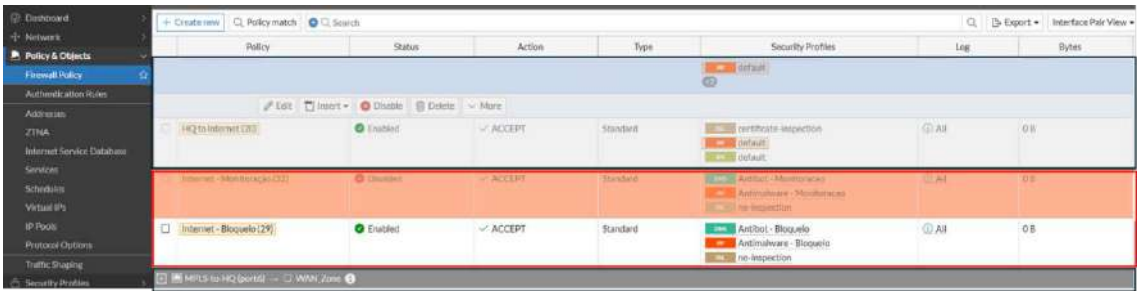
Uma vez definido os perfis de segurança, basta criar duas regras de segurança, sendo uma contendo os perfils de monitoração e outra regra com contendo os perfis de bloqueio.

De forma complementar podemos observar conforme consta na url https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-policy-order-works-on-FortiGate/ta-p/207381 , nota-se conforme trecho: “The policies are consulted from top

to bottom. The first rule that matches is applied and subsequent rules are not evaluated.", que a execução das políticas de segurança são de cima para baixo (top/down), onde se fizer o match ou encontro da regra, a busca cessará nesta regra encontrada.

Trazendo o entendimento conforme respectivo requisito, quando esta instituição desejar ativar o modo de monitoração, teremos a política de monitoração com seus respectivos perfis já em modo de monitoração (sem nenhuma associação ou uso dos outros perfis já em uso) conforme nomes distintos, sendo ativada quando necessário e quando desejar voltar ao modo normal de operação, basta novamente desativar esta política de firewall.

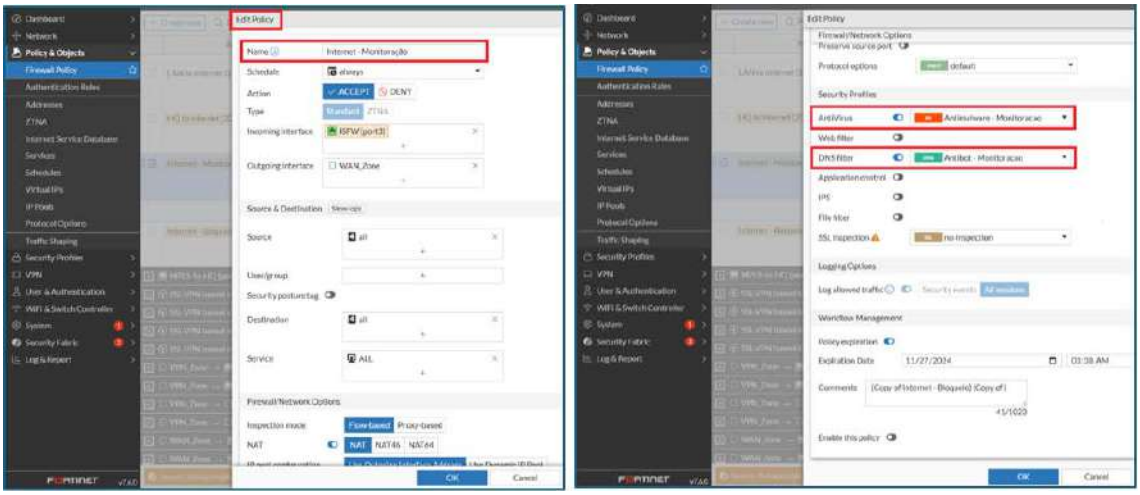
Visando elucidar a dinâmica explicada, seguem imagens extraídas da console para melhor entendimento:



Nesta Imagem da base de políticas, com destaque em vermelho, duas políticas de firewall, seguidas de seus respectivos perfis nomes específicos e especificidades:

- Internet – Monitoração, sombreada em vermelho por estar com o status desabilitada, tendo os perfis de segurança "Antibot-Monitoração" e "Antimalware-Monitoração";
- Internet – Bloqueio, tendo os perfis de segurança "Antibot-Bloqueio" e "Antimalware-Bloqueio".

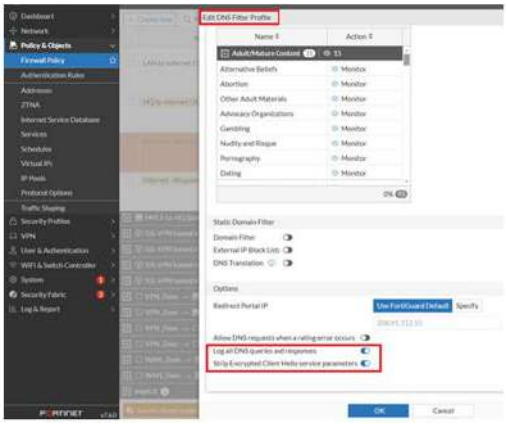
Segue imagem da política de segurança de nome "Internet - Monitoração", com seus respecitvos perfis de monitoração de "Antimalware" e "DNS Filter" (Antibot).



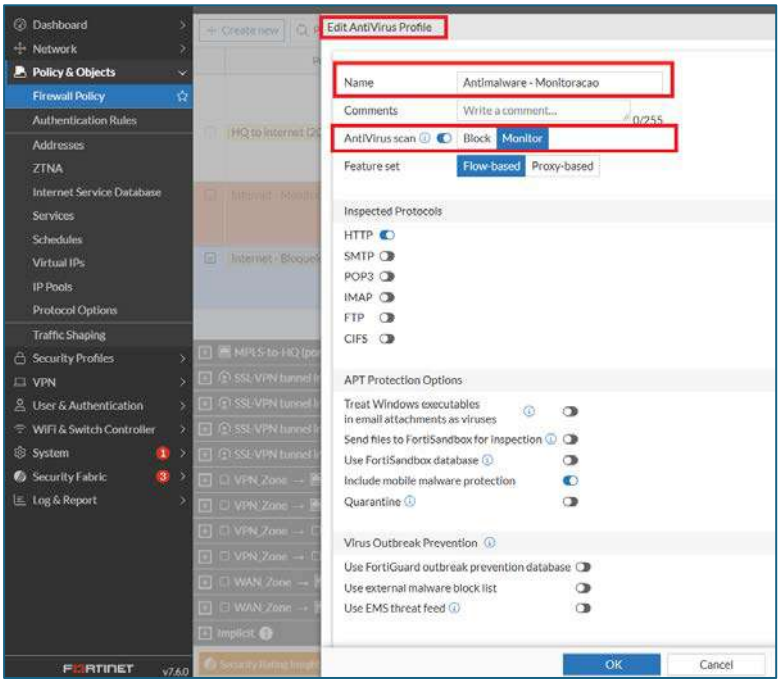
Rubrica

DS

Segue trecho do perfil de “DNS Filter”, de nome “Antibot - Monitoracao” (antibot) em monitoração com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas.



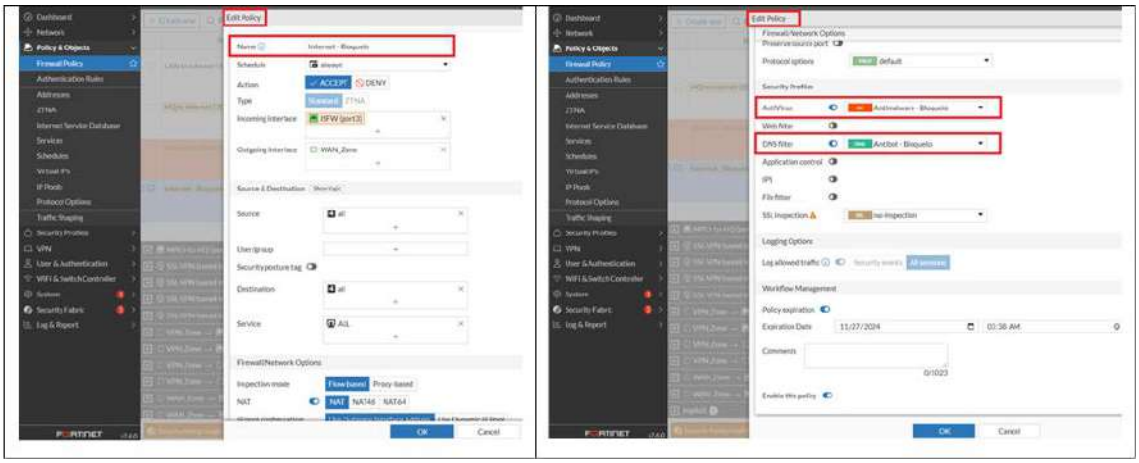
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Monitoracao” com a ação “Antivirus Scan” em “Monitor”.



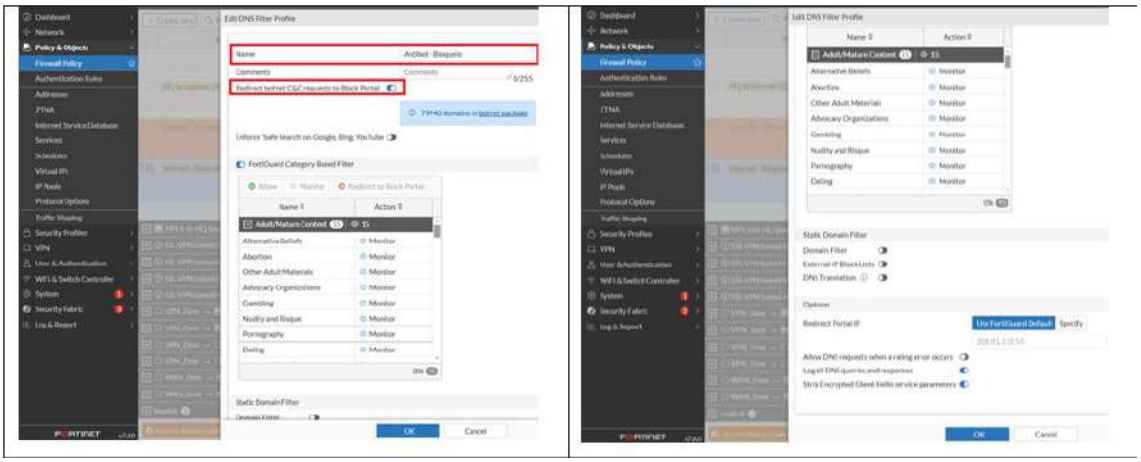
Rubrica

DS

Segue imagem da política de segurança de nome “Internet - Bloqueio”, com seus respecitvos perfis de bloqueio de “Antimalware” e “DNS Filter” (Antibot).



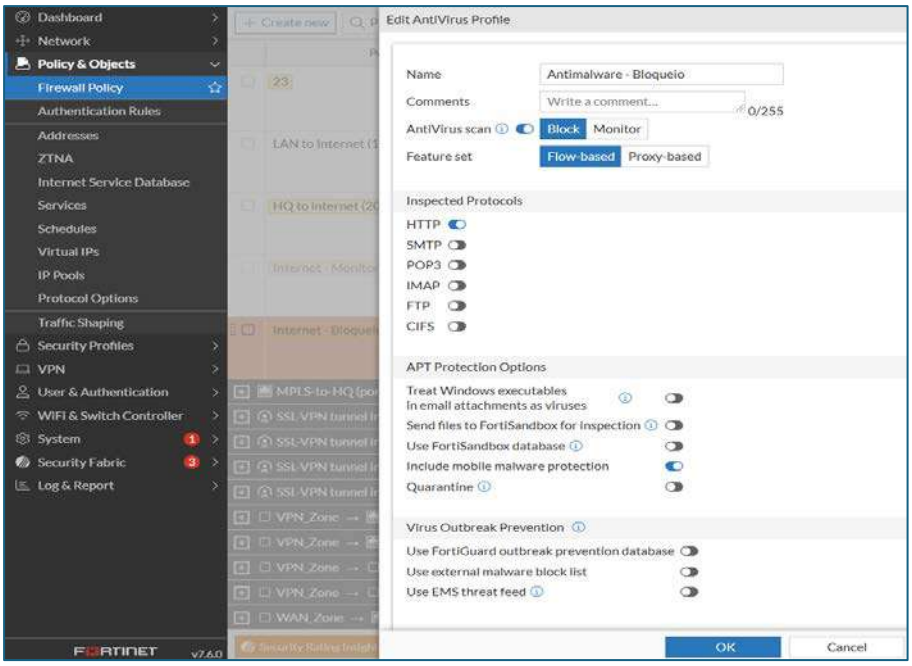
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas



Rubrica

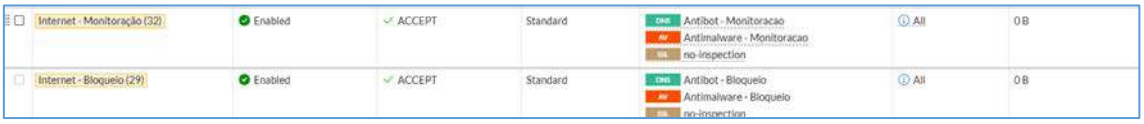
DS

Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a ação “Antivirus Scan” em “Block”.



Segue políticas de segurança em produção com a política de bloqueio ativada e a de monitoração desativada.

Segue políticas de segurança em produção com a política de monitoração ativada, como firewall analisa top/down, apenas a regra “Internet-Monitoração” processará o tráfego.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

2.3. <u>Subitem 2.2.8.5</u>

2.2.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

<u>Referência/URL</u>

"Phase 1 configuration (...)

Monitor tunnel for failover

Rubrica

DS

Monitor a site-to-site tunnel to guarantee operational continuity if the primary tunnel fails. Configure the secondary phase 1 interface to monitor the primary interface."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/790613/phase-1-configuration

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A comprovação utilizada nesse item foi apenas da funcionalidade de estabelecimento do túnel.

É necessário complementar a comprovação da funcionalidade de monitoramento do túnel remoto mencionando funcionalidade de health check que o equipamento também possui sem a necessidade de licenças adicionais.

A funcionalidade *Performance SLA link health monitoring* mede a integridade dos links conectados às interfaces dos membros SD-WAN enviando sinais de sondagem por meio de cada link para um servidor ou usando informações da sessão capturadas nas políticas de firewall e medindo a qualidade do link com base na latência, no jitter e na perda de pacotes.

Se um link falhar em todas as verificações de integridade, as rotas desse link serão removidas do grupo de balanceamento de carga de links SD-WAN e o tráfego será roteado por outros links.

Quando o link estiver funcionando novamente, as rotas serão restabelecidas automaticamente. Isso evita que o tráfego seja enviado para um link quebrado e se perca.

De forma complementar segue mais um link onde conseguimos comprovar o atendimento ao referido item:

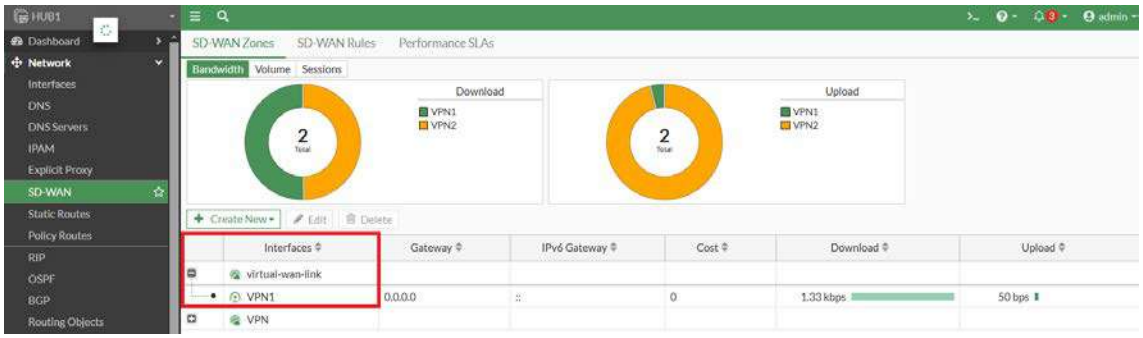
https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/580649/link-health-monitor

Em busca de melhor esclarecer os entendimentos sugeridos, a abordagem do SD-Wan normalmente refere-se ao conceito de vários links, conforme url https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/218559/configuring-the-sd-wan-interface , no trecho “The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others).

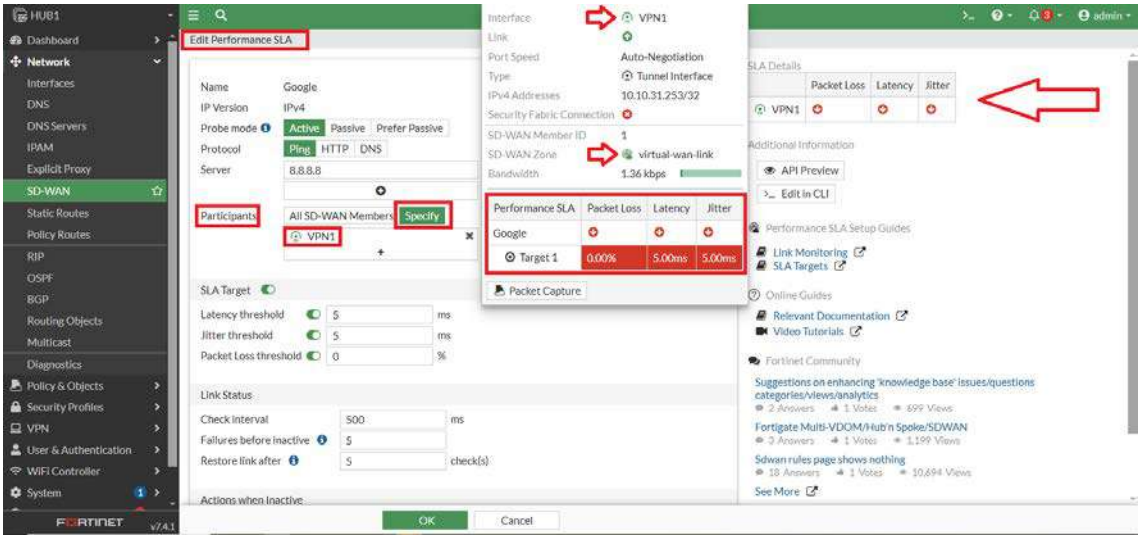
Rubrica FHL

DS MCFM

Isso não significa que para a monitoração de link funcionar necessite de vários links, ou de um link secundário, note a interface de nome “VPN1” associada a interface SD-Wan de nome “virtual-wan-link”:



Note o “Performance SLA”tendo como integrante apenas a interface lógica “VPN1”. É nítido conforme imagem anterior e esta, que apenas a interface “virtual-wan-link” com apenas um link ora o “VPN1”, permitindo ver em tempo real a monitoração do link com tempo de resposta por fator de monitoração e saúde (Packet Loss, Latency e Jitter).



Concluindo assim que o FortiGate é capaz de monitorar a saúde do túnel através da performance SLA utilizando um endereço IP que faça parte to túnel remoto com apenas uma interface ou link em uso.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

Rubrica

DS

3. 2.3 SERVIÇO DE PROTEÇÃO DE PERÍMETRO GRANDE PORTE

3.1. Subitem 2.3.4.15

2.3.4.15. A solução de proteção contra malware e bot podem compartilhar a mesma política para facilitar o gerenciamento.

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

Referência/URL

"Enabling antivirus in a policy

Note: detalhe para a imagem demonstrando os diversos perfis de segurança que podem ser habilitados numa mesma policy."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/767732/enabling-antivirus-in-a-policy

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Há luz do edital, nota-se que o referido item, é flexibilizado, informando que pode e não que deve. Independente do desejado por esta instituição, o FortiGate permite plenamente o uso compartilhado das funcionalidades de segurança em uma mesma regra de segurança.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, conforme Datasheet, tem como base seu sistema operacional, chamado FortiOS.

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Estas políticas de segurança são efetivas na proteção do ambiente rede, fazendo a inspeção localmente no appliance, da camada de rede até a aplicação de todo o tráfego passante (em linha), tomando as ações configuradas sem nenhuma dependência de comunicação ou integração de agente com os hosts de rede.

Ao acessar o link disponibilizado podemos perceber na imagem que, quando criamos uma política de segurança é possível habilitar diversos perfis de segurança dentro desta, como: Antivirus, Web Filter, DNS Filter, Application Control, IPS e outros.

Afim de não restar duvidas, será fornecido de forma complementar mais duas referências com mais informações:

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/583477/configuring-an-ips-sensor

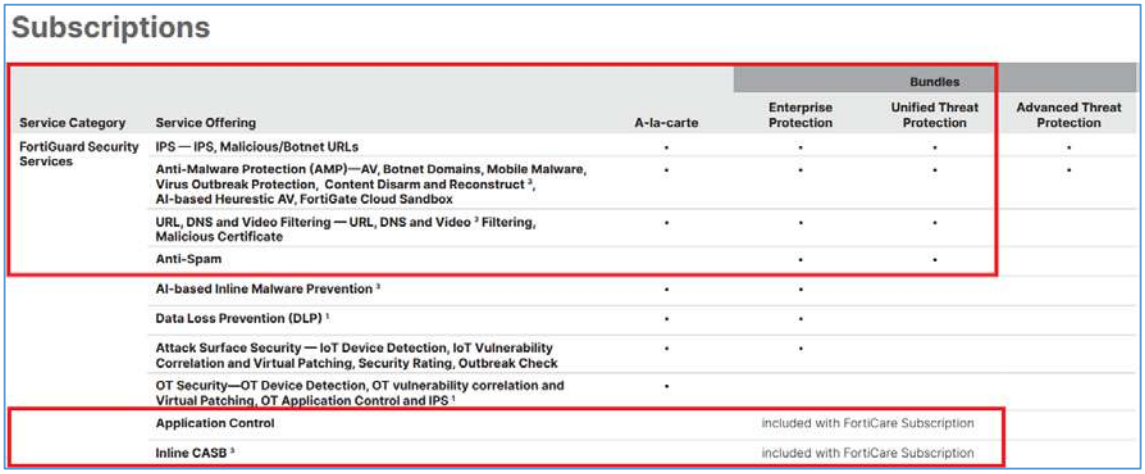
https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/254346/external-malware-block-list

Podemos observar de forma mais detalhada sobre os mecanismos de proteção que estão inclusos nos perfis de segurança que podem ser combinados para a criação da política.

Conforme documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/836396/antivirus e seus sublinks, é abordado explicações e orientações de como ativar o filtro de antivirus/antimalware.

Segundo documentação pública, nas urls: https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/605868/dns-filter e seus sublinks, é abordado explicações e orientações de como ativar o perfil “DNS Filter” o qual tem a capacidade de identificar e bloquear comunicação de Botnets e tráfego de Comando e Controle (C&C).

O licenciamento do appliance FortiGate, ofertado para este certame, é o Bundle UTP, composto pelas seguintes funcionalidades destacadas pelos quadrados em vermelho:



Subscriptions

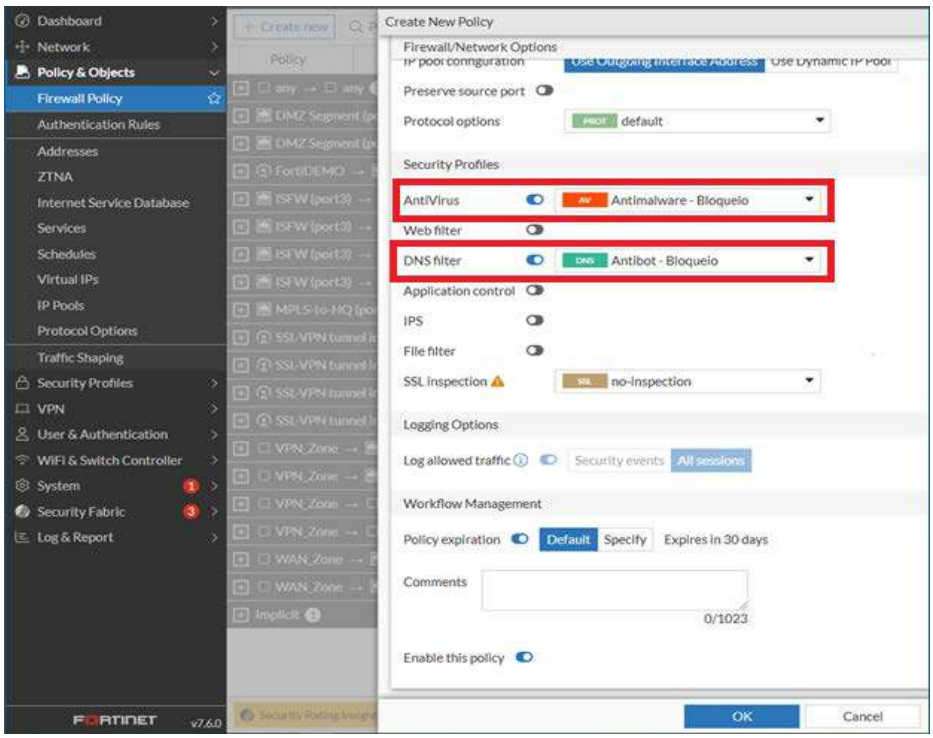
			Bundles		
Service Category	Service Offering	A-la-carte	Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [2], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [2] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		included with FortiCare Subscription		

Visando melhor explicar, segue uma imagem extraída da console com o objetivo de demonstrar a ativação dos perfis de segurança “Antimalware” e “DNS Filter”.

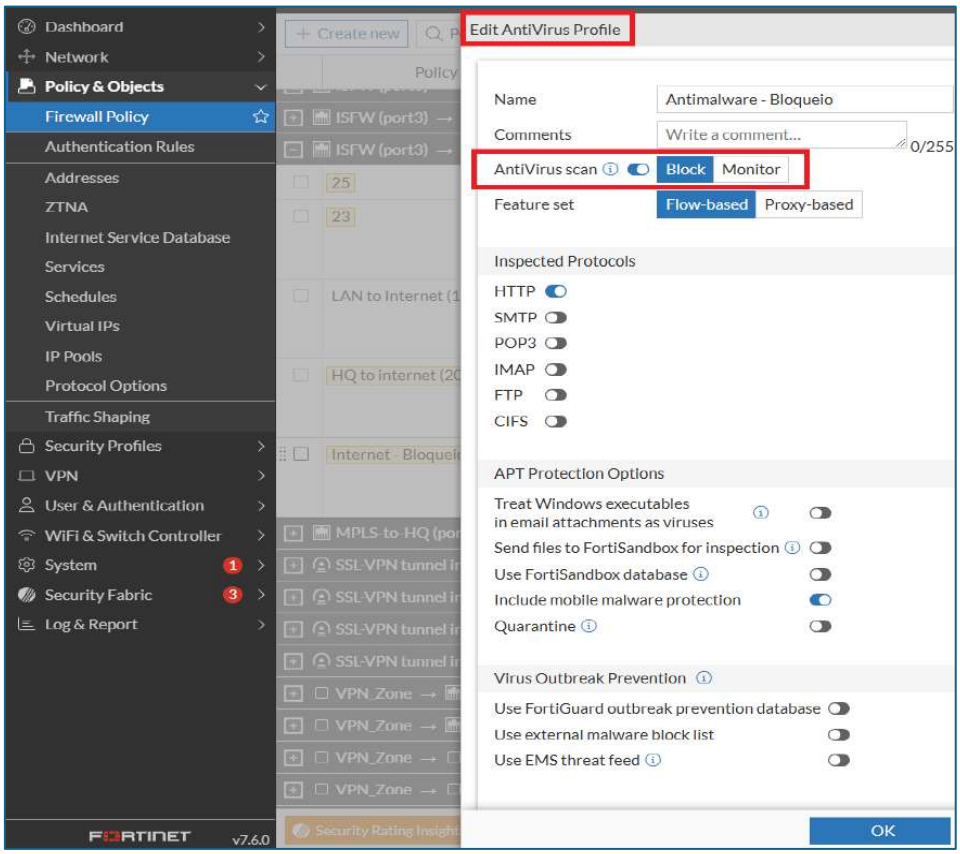
Note que nesta Imagem a criação da política de segurança, as chaves “AntiVirus” e “DNS Filter” ativas na mesma regras durante edição desta política.

Rubrica

DS



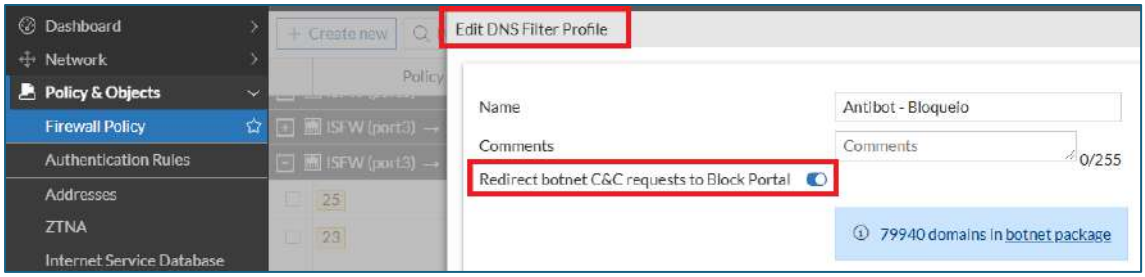
Segue edição do perfil de segurança de “Antivirus”, com a ação de scan marcado para bloquear.



Rubrica

DS

Segue edição do perfil de segurança de “DNS Filter”, com a ação de scan marcado para redirecionar as requisições de botnet para o portal de bloqueio da respectiva requisição.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

3.2. Subitem 2.3.4.16

> *2.3.4.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;*

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

> ***Referência/URL***
>
> *Ordering the policy table*
>
> *Nota: para atender este item, pode-se clonar a policy existente, ajustar os perfis de segurança para monitorar/não bloquear e posicionar a nova policy acima da existente.*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/508696/ordering-the-policy-table*

O mecanismo de clonagem de uma política de segurança permite que as regras originais ou já criadas e homologadas sejam duplicadas sem que ocorra alterações na configuração original.

A partir disso é possível fazer modificações no que foi duplicada para se ajustar a uma nova necessidade. Para priorizar a nova política em relação as políticas operacionais do equipamento, é possível que ela seja posicionada antes da original para que seja acionada antes das outras que já estavam em operação.

O appliance NGFW FortiGate, líder no Gartner nos segmentos de Firewall Empresarial (NGFW), SD-Wan e Rede Empresarial Cabeada e Wlan, tem como base seu sistema operacional, chamado FortiOS.

Rubrica DS

Por ser um NGFW, ele permite a criação das políticas de segurança de forma granular no tocante as funcionalidades desejadas, chamadas de Perfil de Segurança.

Para o pleno atendimento do requisito supra citado, basta configurar quatro perfis de segurança, sendo dois de “Antimalware” e dois de “DNS Filter”, onde para cada perfil, teremos um com ação de bloqueio e o outro com ação de monitoração.

Uma vez definido os perfis de segurança, basta criar duas regras de segurança, sendo uma contendo os perfils de monitoração e outra regra com contendo os perfis de bloqueio.

De forma complementar podemos observar conforme consta na url https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-policy-order-works-on-FortiGate/ta-p/207381 , nota-se conforme trecho: “The policies are consulted from top to bottom. The first rule that matches is applied and subsequent rules are not evaluated.”, que a execução das políticas de segurança são de cima para baixo (top/down), onde se fizer o match ou encontro da regra, a busca cessará nesta regra encontrada.

Trazendo o entendimento conforme respectivo requisito, quando esta instituição desejar ativar o modo de monitoração, teremos a política de monitoração com seus respectivos perfis já em modo de monitoração (sem nenhuma associação ou uso dos outros perfis já em uso) conforme nomes distintos, sendo ativada quando necessário e quando desejar voltar ao modo normal de operação, basta novamente desativar esta política de firewall.

Visando elucidar a dinâmica explicada, seguem imagens extraídas da console para melhor entendimento:

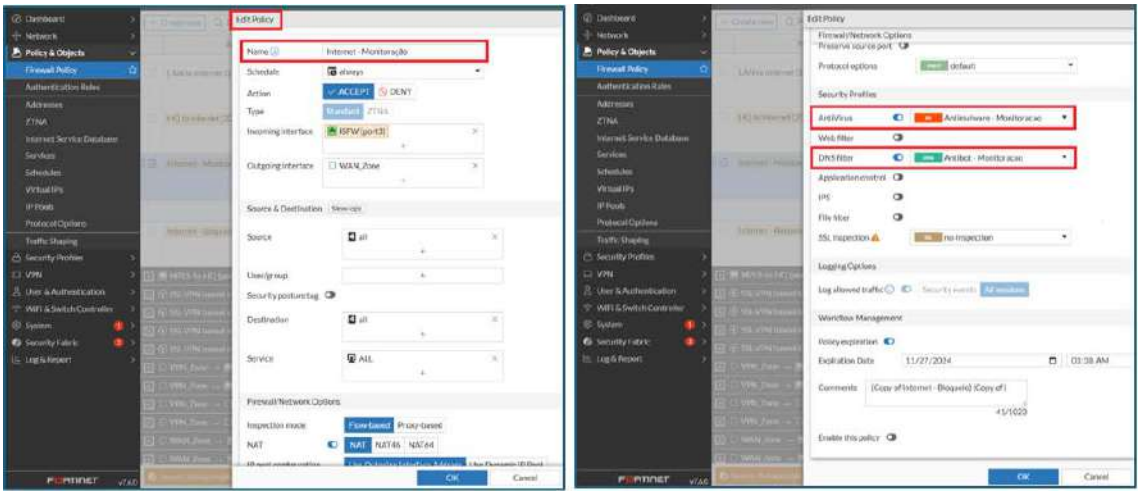
Nesta Imagem da base de políticas, com destaque em vermelho, duas políticas de firewall, seguidas de seus respectivos perfis nomes específicos e especificidades:

- Internet – Monitoração, sombreada em vermelho por estar com o status desabilitada, tendo os perfis de segurança “Antibot-Monitoração” e “Antimalware-Monitoração”;
- Internet – Bloqueio, tendo os perfis de segurança “Antibot-Bloqueio” e “Antimalware-Bloqueio”.

Rubrica

DS

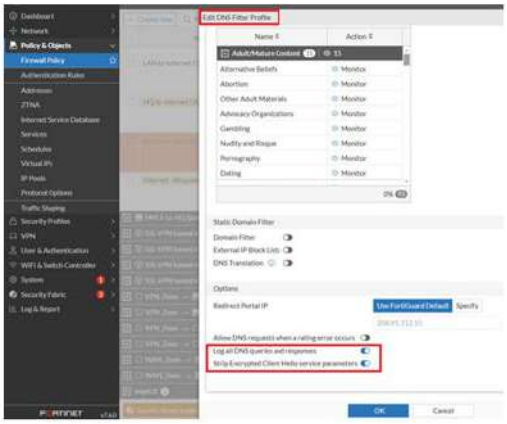
Segue imagem da política de segurança de nome “Internet - Monitoração”, com seus respecitvos perfis de monitoração de “Antimalware” e “DNS Filter” (Antibot).



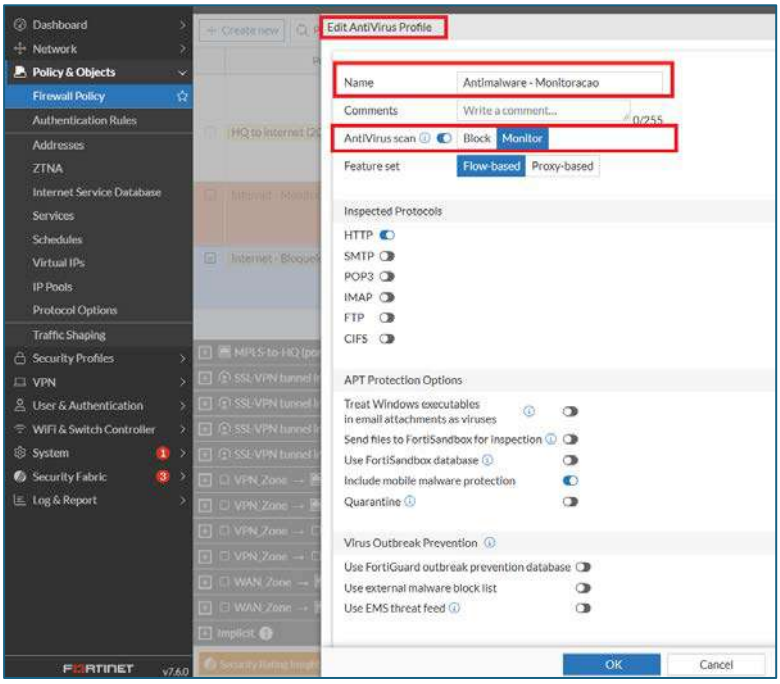
Rubrica

DS

Segue trecho do perfil de “DNS Filter”, de nome “Antibot - Monitoracao” (antibot) em monitoração com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas.



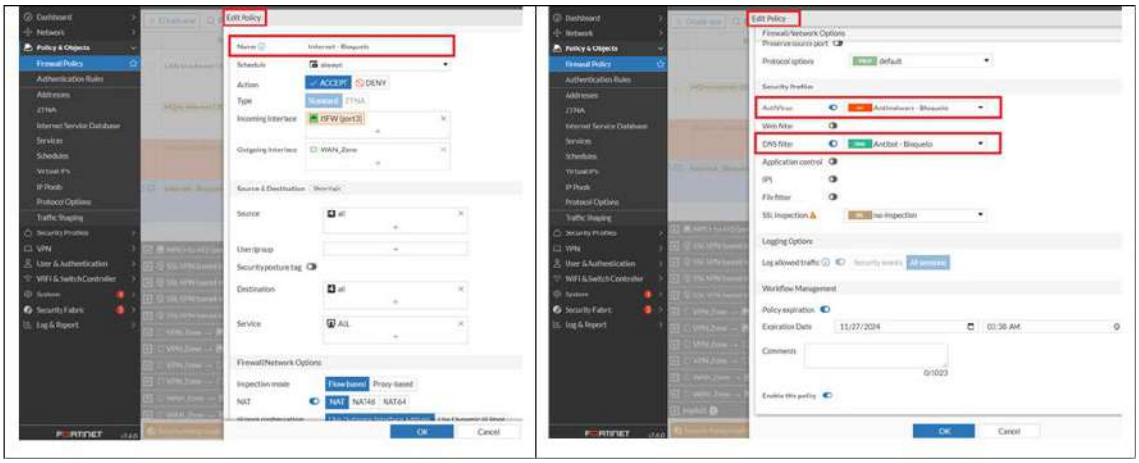
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Monitoracao” com a ação “Antivirus Scan” em “Monitor”.



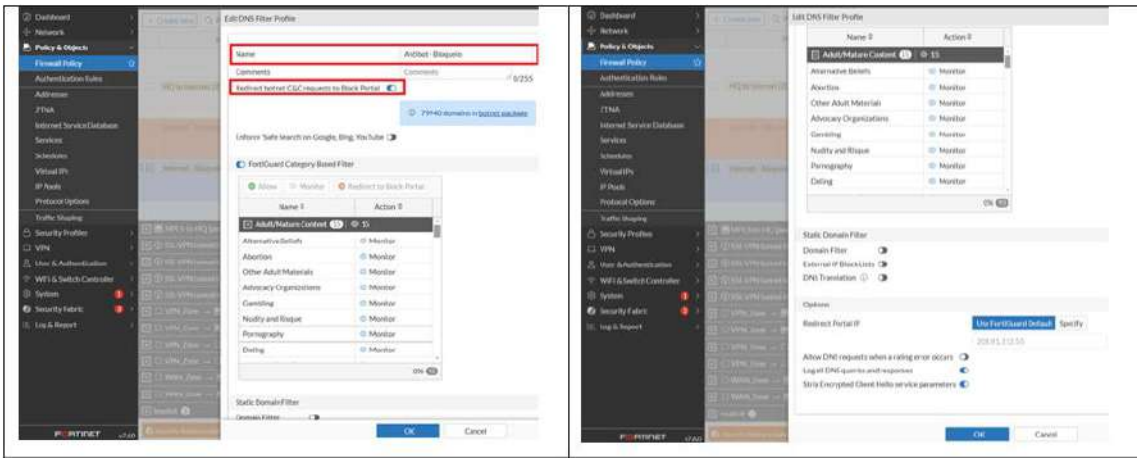
Rubrica

DS

Segue imagem da política de segurança de nome “Internet - Bloqueio”, com seus respecitvos perfis de bloqueio de “Antimalware” e “DNS Filter” (Antibot).



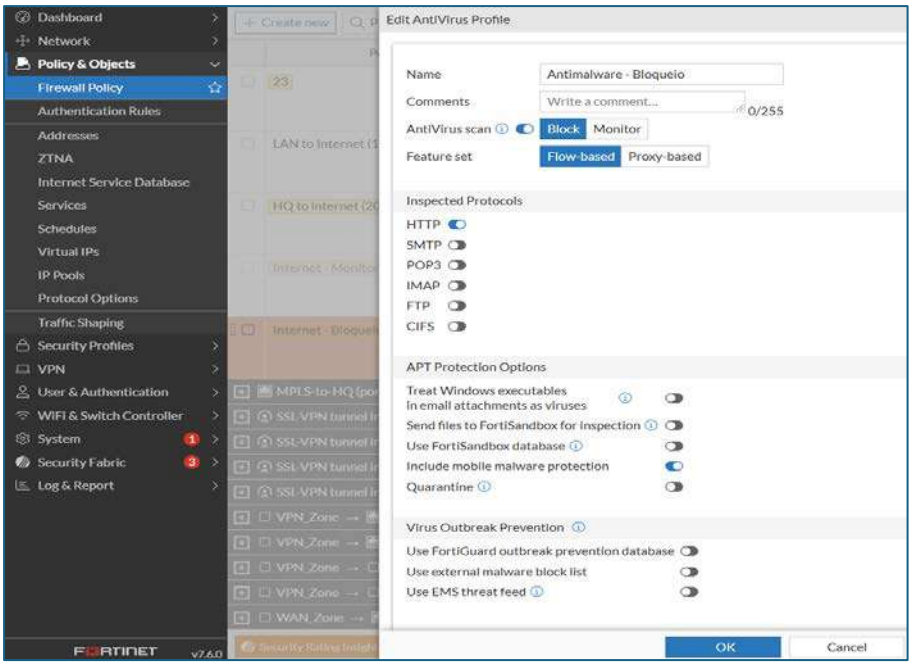
Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a opção de redirecionamento da comunicação botnet desativada, ou seja: permitindo a passagem sem bloqueio com registro de todas as requisições de pesquisas e respostas



Rubrica

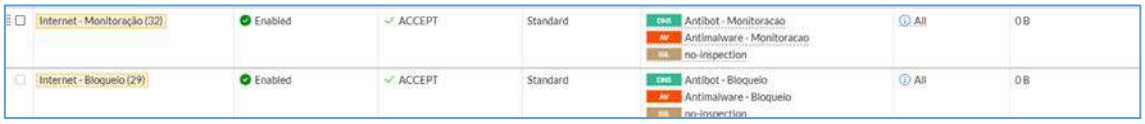
DS

Segue trecho do perfil de “Antimalware” de nome “Antimalware - Bloqueio” com a ação “Antivirus Scan” em “Block”.



Segue políticas de segurança em produção com a política de bloqueio ativada e a de monitoração desativada.

Segue políticas de segurança em produção com a política de monitoração ativada, como firewall analisa top/down, apenas a regra “Internet-Monitoração” processará o tráfego.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

3.3. <u>Subitem 2.3.8.5</u>

> *2.3.8.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;*

Foi evidenciado no ponto a ponto o atendimento deste item conforme segue:

> ***<u>Referência/URL</u>***
>
> *"Phase 1 configuration (...)*
>
> *Monitor tunnel for failover*

Rubrica

DS

Monitor a site-to-site tunnel to guarantee operational continuity if the primary tunnel fails. Configure the secondary phase 1 interface to monitor the primary interface."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/790613/phase-1-configuration

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A comprovação utilizada nesse item foi apenas da funcionalidade de estabelecimento do túnel.

É necessário complementar a comprovação da funcionalidade de monitoramento do túnel remoto mencionando funcionalidade de health check que o equipamento também possui sem a necessidade de licenças adicionais.

A funcionalidade *Performance SLA link health monitoring* mede a integridade dos links conectados às interfaces dos membros SD-WAN enviando sinais de sondagem por meio de cada link para um servidor ou usando informações da sessão capturadas nas políticas de firewall e medindo a qualidade do link com base na latência, no jitter e na perda de pacotes.

Se um link falhar em todas as verificações de integridade, as rotas desse link serão removidas do grupo de balanceamento de carga de links SD-WAN e o tráfego será roteado por outros links.

Quando o link estiver funcionando novamente, as rotas serão restabelecidas automaticamente. Isso evita que o tráfego seja enviado para um link quebrado e se perca.

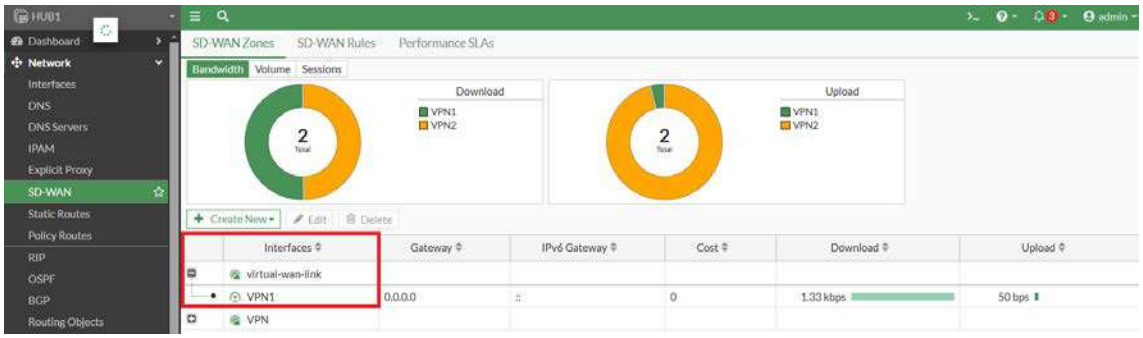
De forma complementar segue mais um link onde conseguimos comprovar o atendimento ao referido item:

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/580649/link-health-monitor

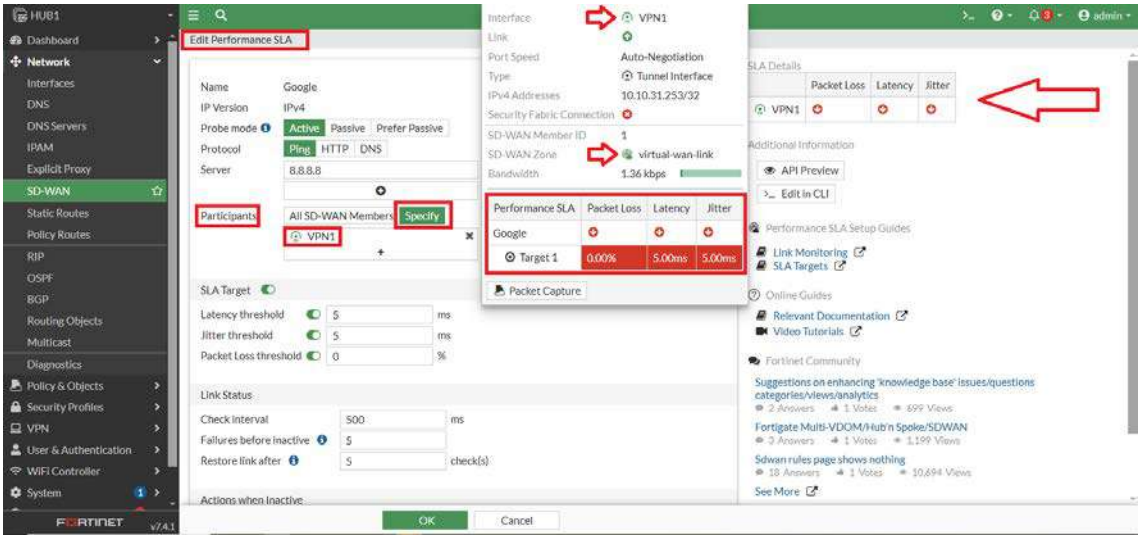
Em busca de melhor esclarecer os entendimentos sugeridos, a abordagem do SD-Wan normalmente refere-se ao conceito de vários links, conforme url https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/218559/configuring-the-sd-wan-interface , no trecho “The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others).

Rubrica DS

Isso não significa que para a monitoração de link funcionar necessite de vários links, ou de um link secundário, note a interface de nome “VPN1” associada a interface SD-Wan de nome “virtual-wan-link”:



Note o “Performance SLA”tendo como integrante apenas a interface lógica “VPN1”. É nítido conforme imagem anterior e esta, que apenas a interface “virtual-wan-link” com apenas um link ora o “VPN1”, permitindo ver em tempo real a monitoração do link com tempo de resposta por fator de monitoração e saúde (Packet Loss, Latency e Jitter).



Concluindo assim que o FortiGate é capaz de monitorar a saúde do túnel através da performance SLA utilizando um endereço IP que faça parte to túnel remoto com apenas uma interface ou link em uso.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4. 2.5. SERVIÇO DE PROTEÇÃO DE DATACENTER MÉDIO PORTE

4.1. Subitem 2.5.4.36.

2.5.4.36. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

Referência/URL

Rubrica

DS

"Data loss prevention

The FortiGate data loss prevention (DLP) system prevents sensitive data from leaving or entering your network by scanning for various patterns while inspecting traffic passing through the FortiGate. Data that matches defined sensitive data patterns is blocked, logged, allowed, or quarantined when it passes through the FortiGate."

Comprovação/Link

https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/153498/data-loss-prevention

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A página WEB disponibilizada no ponto a ponto, descreve a funcionalidade como um todo e abre subpáginas dependentes a esta com detalhes e particularidades referente ao item em questão.

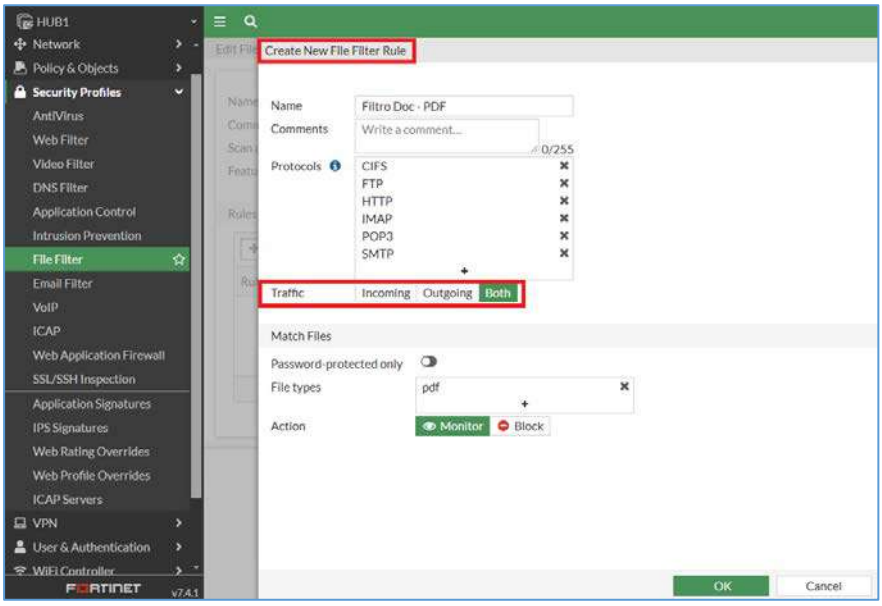
Ao navegar no portal, indo até o final da página mencionada, encontramos um hiperlink *"DLP examples"*, que ao acessar, abre-se uma nova página com os exemplos de criação de regras / políticas que fazem controle do tráfego nos sentidos upload, download e ambos.

De forma complementar e afim de facilitar a consulta segue o link onde vai direto para esta informação:

https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/580649/link-health-monitor

Para o pleno atendimento deste requisito, o FortiGate possui a funcionalide de “File Filter”, responsável por filtrar arquivos por extensão ou tipo.

Note na imagem abaixo, Vide configuração de uma regra da funcionalidade de “File Filter”, trazendo o destaque em vermelho para a direção do tráfego, ora as opções: “Incoming” (entrada), “Outgoing” (saída) ou “Both” (ambos os sentidos):



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.2. <u>Subitem 2.5.4.37</u>

> *2.5.4.37. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.*
>
> ***<u>Referência/URL</u>***
>
> *"Technical Tip: How to use DLP to block traffic from messages that contain credit card information*
>
> *Description: This article describes how to use DLP to block traffic from messages that contain credit card information.*
>
> *(...)*
>
> *Testing:*
>
> *The user tries to send an email that contains credit card information and gets blocked.*
>
> *<screenshot>"*
>
> ***<u>Comprovação/Link</u>***
>
> *https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-DLP-to-block-traffic-from-messages-that/ta-p/302999*

<u>De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão</u>:

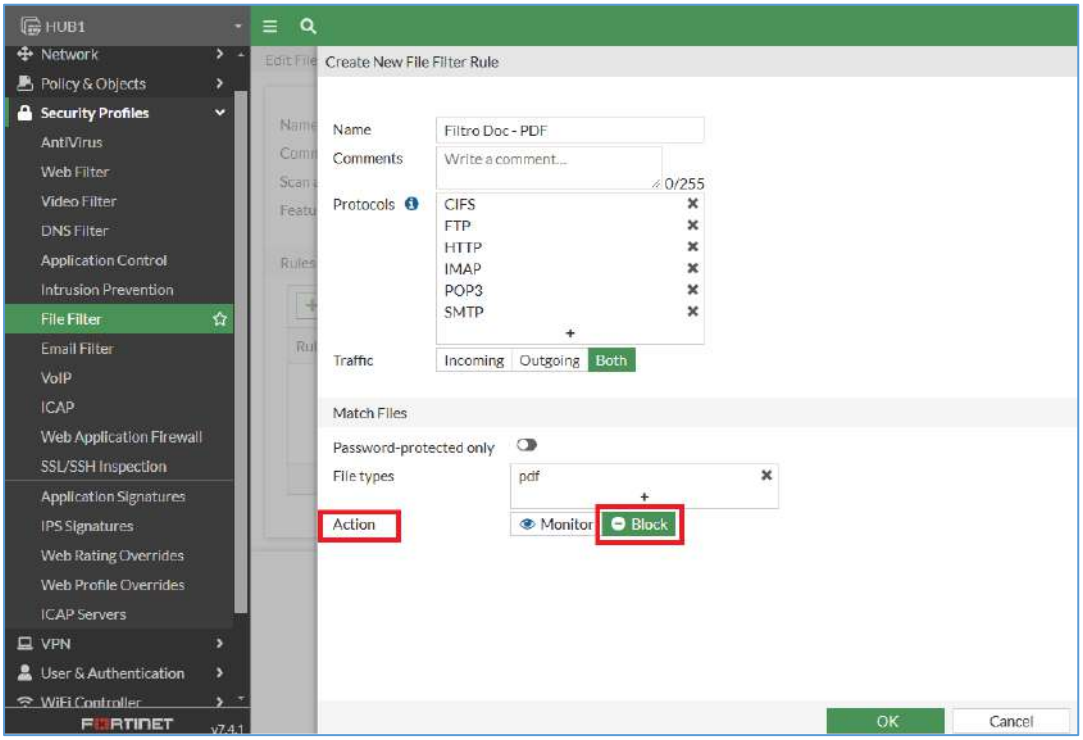
A página WEB disponibilizada no ponto a ponto, descreve o fluxo de aprovisionamento da funcionalidade e no item "Testing" ela mostra o resultado de uma

simulação de envio de um e-mail com arquivo em anexo que fere a política de DLP criada.

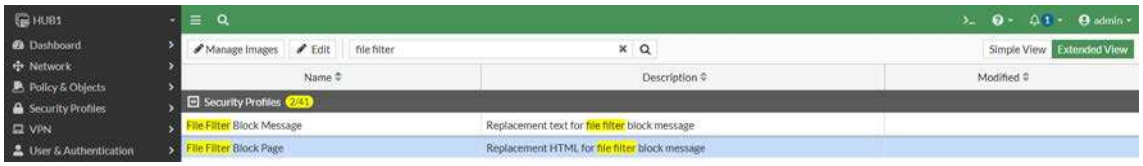
Ao clicar diretamente em cima da penúltima figura da página é possível ver um exemplo de alerta de bloqueio que o usuário vai receber ao tentar enviar um conteúdo que viola essa política.

Para o pleno atendimento deste requisito, o FortiGate possui a funcionalide de “File Filter”, responsável por filtrar arquivos por extensão ou tipo.

Conforme configuração do perfil de segurança “File Filter” notamos as ações “Monitor” ou “Block” conforme imagem abaixo, note a ação de “Block” dentro da funcionalidade de “File FIlter”.:



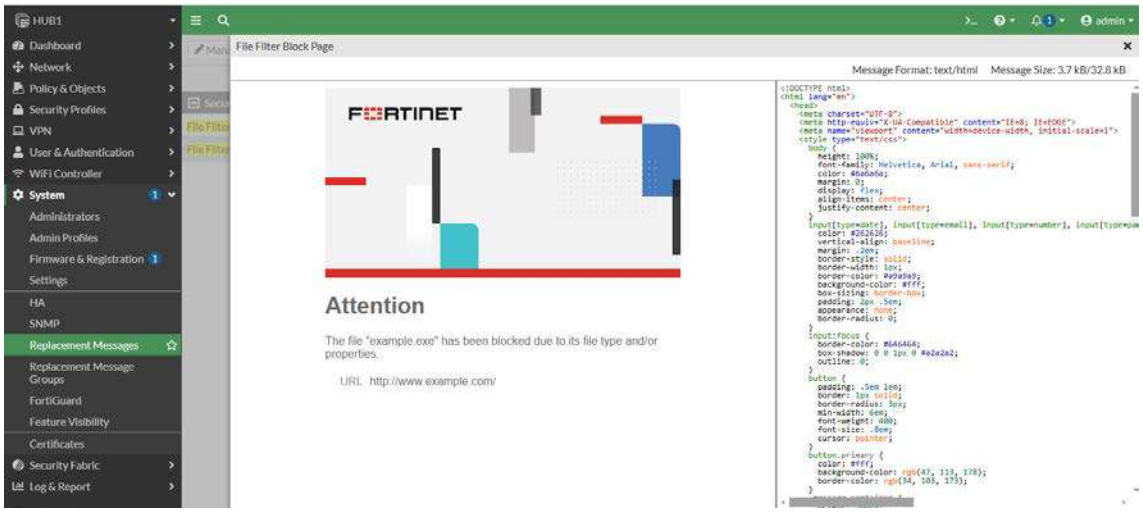
Note a página de bloqueio da ação



Note a imagem da página de bloqueio do “Filter Filter” disponível para visualização e edição.

Rubrica

DS



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.3. Subitem 2.5.8.9

2.5.8.9. Todas as máquinas virtuais (Windows e Linux) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

Referência/URL

"FortiSandbox Data Sheet | Pág. 7

Sandboxing (Dynamic AI Scan) Support

(…)

• OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems"

Comprovação/Link

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A página do datasheet que foi citada no ponto a ponto, informa as opções de sistemas operacionais que podem ser utilizados para a verificação dos arquivos.

De acordo com o manual da solução, as alocações das VM com os seus respectivos sistemas operacionais podem ser definidas no momento da implementação

Rubrica

DS

da ferramenta deixando as opções de sistemas operacionais prontas para serem utilizadas para a verificação dos arquivos.

Após a implementação o sistema gerencia sem a necessidade de intervenção do administrador.

De forma complementar e afim de facilitar a consulta segue o link onde vai direto para esta informação:

https://docs.fortinet.com/document/fortisandbox-cloud/latest/cloud-deployment/275752/assigning-sandboxing-vm-clones

A solução de Sandbox ofertada para este certame chama-se FortiSandbox Cloud (Paas), conforme url https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf , na página 5, no trecho "*Fortinet maintains, updates, and operates the platform on your behalf.*", concluindo assim que como a solução ofertada é baseada na nuvem do Fabricante Fortinet, todos os updates são administrados pela própria Fortinet.

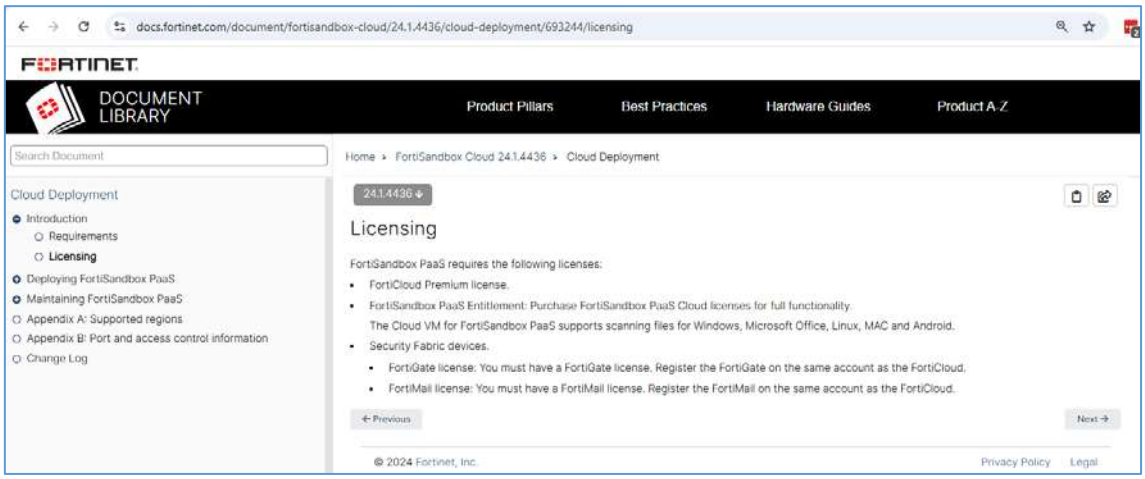
Na proposta comercial, conforme licenças informadas na proposta: FN-FC2-10-SACLP-433-01-36, "FortiSandbox Cloud - Windows (5 VMs) FortiSandbox Cloud 5-VM Expansion - Expands dedicated sandbox instance by 5 Windows cloud VMs. FortiSandbox Cloud supports up to 200 Windows VMs, and provides AI powered sandbox analysis. (requires FortiCloud Premium".

Nota-se a oferta na Proposta Comercial da Solução "FortiSandbox Cloud PaaS", sendo composta por bundles licenças múltiplo de 5 VMs em ambiente Sandbox.

Esta solução é integrada ao firewall FortiGate via API. O fluxo operacional de um arquivo suspeito é iniciado no momento em que o FortiGate identifica o arquivo passando por ele, sendo este "offloaded" descarregado) do tráfego e enviado para a Nuvem do FortiSandbox, onde este arquivo passa a ser inspecionado em ambiente controlado sandbox, caso seja identificado comportamento malicioso, o FortiSandbox gera uma assinatura, e envia o veredito da inspeção para o FortiGate.

O licenciamento permite ativar todo o ambiente em nuvem, descartando qualquer necessidade de integração com os hosts de rede, ou seja: tudo acontece na camada de rede quando o tráfego passa pelo FortiGate, os hosts de rede não possuem nenhum agente ou aplicativo instalado para comunicação com o FortiGate.

Visando melhor explicar, o licenciamento do "*FortiSandbox Cloud PaaS*", conforme url https://docs.fortinet.com/document/fortisandbox-cloud/24.1.4436/cloud-deployment/693244/licensing , no trecho conforme imagem, comprova-se que todo o licenciamento necessário foi ofertado, evidenciando desta forma que os licenciamentos pertinentes as VMs: Windows, Microsoft Office, Linux, MAC e Android já estão inclusos na licença do "FortiSandbox PaaS" e licença de aceso a nuvem com o "FortiCloud Premium License".



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.4. <u>Subitem 1.5.8.16</u>

2.5.8.16. Quantidade de arquivos que estão em emulação;

<u>Referência/URL</u>

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year).

The Scan Performance dashboard contains the following charts:

Scanned Count: The total number of scanned jobs per time unit.

VM Scan count: The total number of jobs that entered the VM for dynamic scan per time unit.

Average Processing Wait Time: The wait time in the initial processing queue.

Average VM Wait time: The wait time prior to entering the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.

Average Process Time: The processing time from receiving to completing the scan based on the average calculated time divided by total jobs per time unit.

Average VM Scan Time: The processing time within the VM for dynamic scan based on the average calculated time divided by total jobs per time unit."

Comprovação/Link

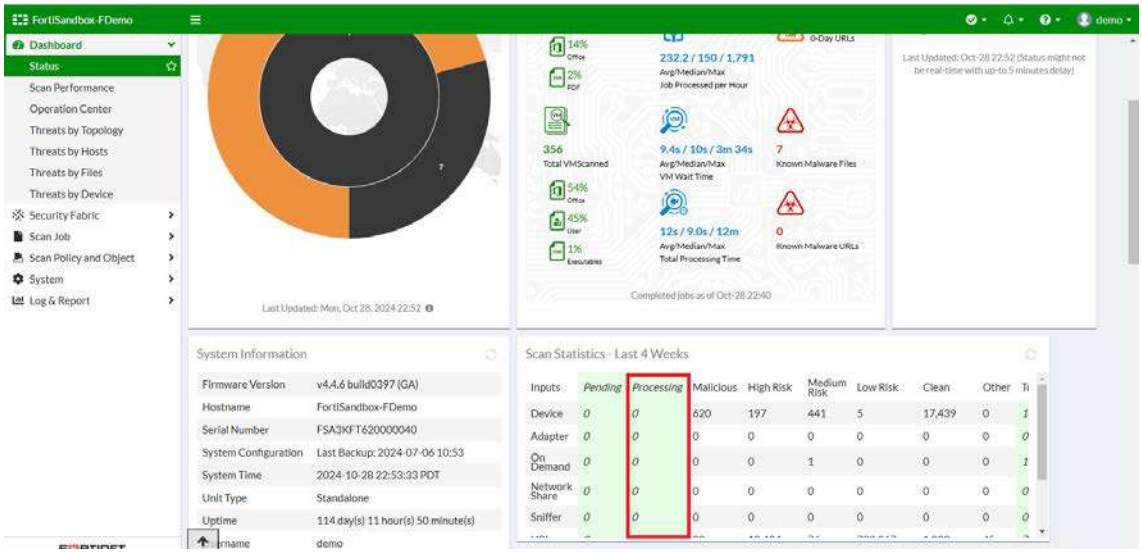
https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Conforme podemos observar no link disponibilizado o *VM Scan count - The total number of jobs that entered the VM for dynamic scan per time unit.*

Trata-se da contagem de varredura de VM, ou seja, o número total de trabalhos que entraram na VM para varredura dinâmica por unidade de tempo.

Nota-se conforme destaque em vermelho, a relação de arquivos que estão em Processamento.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.5. Subitem 1.5.8.17

2.5.8.17. Número de arquivos emulados;

Referência/URL

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

Rubrica

DS

The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year).

The Scan Performance dashboard contains the following charts:

Scanned Count: The total number of scanned jobs per time unit.

VM Scan count: The total number of jobs that entered the VM for dynamic scan per time unit.

Average Processing Wait Time: The wait time in the initial processing queue.

Average VM Wait time: The wait time prior to entering the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.

Average Process Time: The processing time from receiving to completing the scan based on the average calculated time divided by total jobs per time unit.

Average VM Scan Time: The processing time within the VM for dynamic scan based on the average calculated time divided by total jobs per time unit."

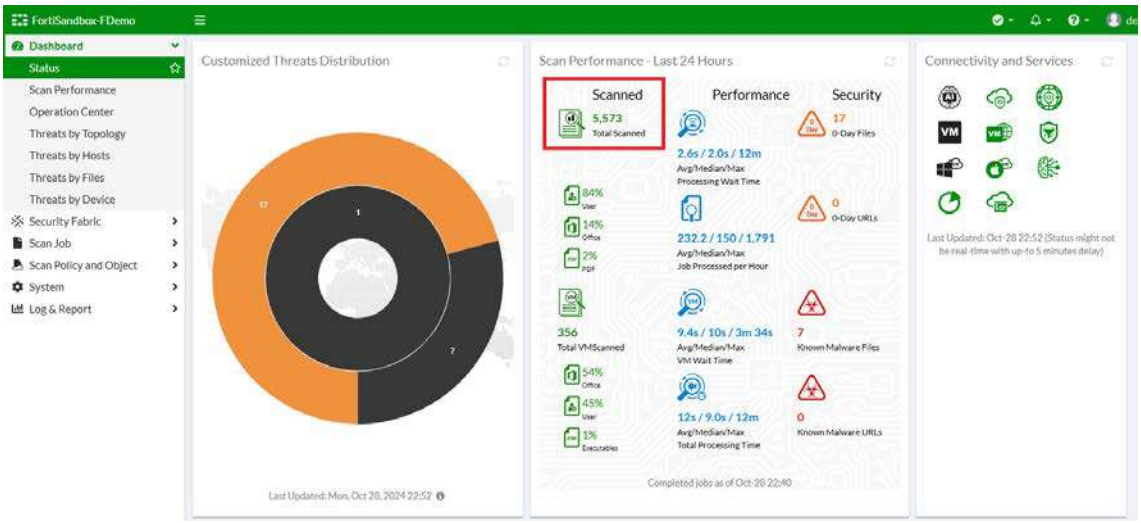
Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Conforme podemos observar no link disponibilizado o *Scanned Count - The total number of scanned jobs per time unit*. trata-se da contagem de arquivos escaneados, ou seja, o número total de trabalhos escaneados por unidade de tempo. *Número de arquivos emulados;*

Nota-se em destaque vermelho na imagem abaixo, a quantidade de arquivos emulados ou escaneados.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.6. <u>Subitem 1.5.8.18</u>

2.5.8.18. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

<u>Referência/URL</u>

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year)."

<u>Comprovação/Link</u>

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

<u>De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão</u>:

A solução possui um filtro temporal onde permite que seja alterado para visualização das estatísticas.

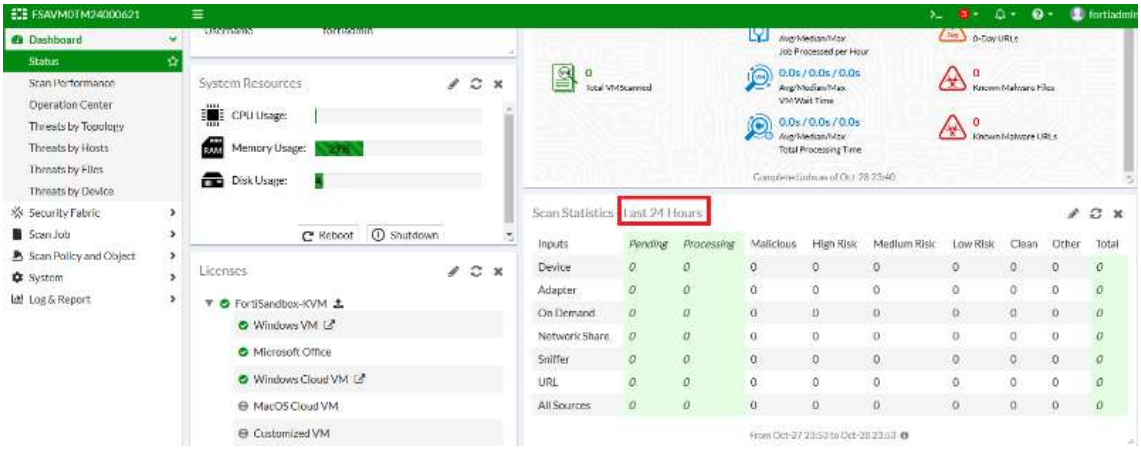
As opções para a unidade de tempo variam de acordo com o intervalo de tempo. Por exemplo, a visualização por hora é exibida em intervalos de tempo mais curtos (1

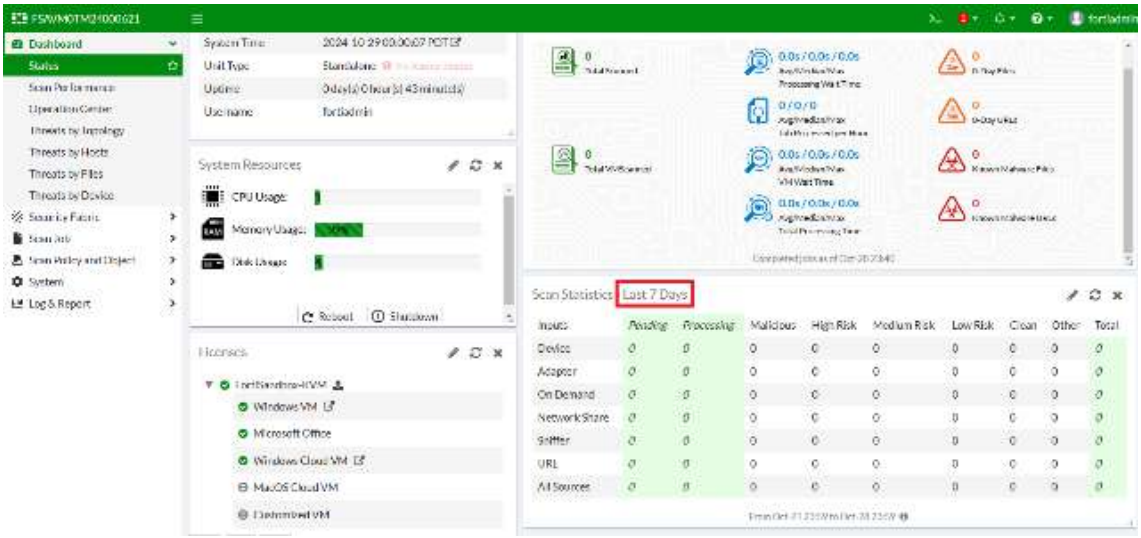
Rubrica

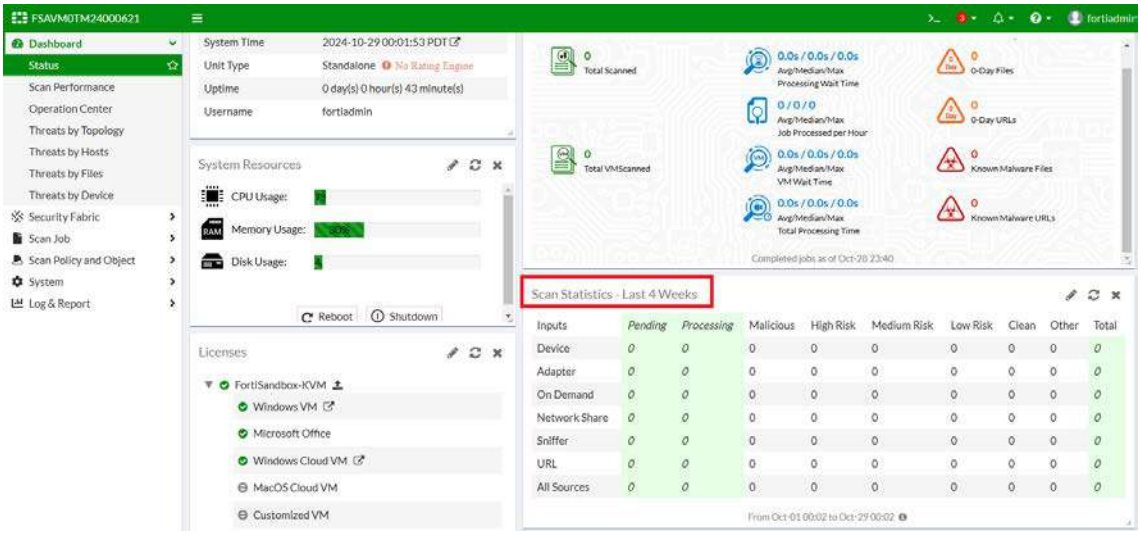
DS

dia, 3 dias e 7 dias), enquanto a visualização por dia é exibida em intervalos mais longos (4 semanas e 1 ano), permitindo assim a visualização último dia, última semana ou últimos 30 dias.

Nota-se imagens extraídas do FortiSandob com com destaques de tempo variados entre: “Last 24 hours” (últmas 24 horas), “Last 7 Days” (últimos sete dias) e Last 4 Weeks (último mês).







Rubrica

DS

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.7. Subitem 2.5.8.19

> *2.5.8.19. Arquivos scaneados;*
>
> ***Referência/URL***
>
> *"Scan Performance (dashboard)*
>
> *The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.*
>
> *(...)*
>
> *The Scan Performance dashboard contains the following charts:*
>
> *Scanned Count: The total number of scanned jobs per time unit."*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard*

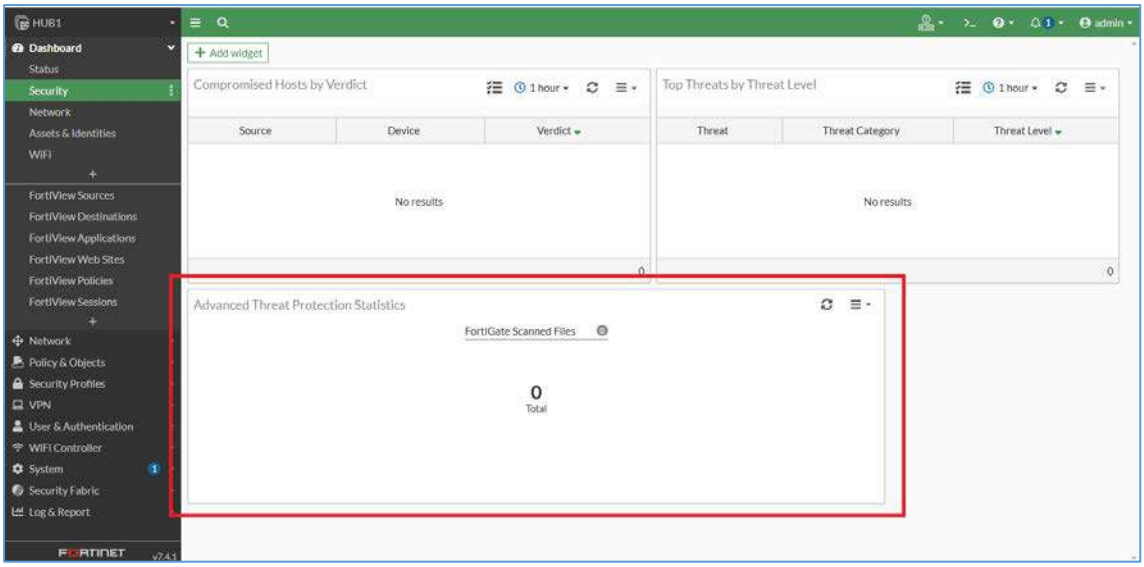
De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Em outro capitulo do mesmo documento citado no link de comprovação constante no ponto a ponto, existe um outro capitulo chamado *"File Scan"* que demonstra de forma mais detalhadas os arquivos escaneados e o veredito de avaliação de cada arquivo.

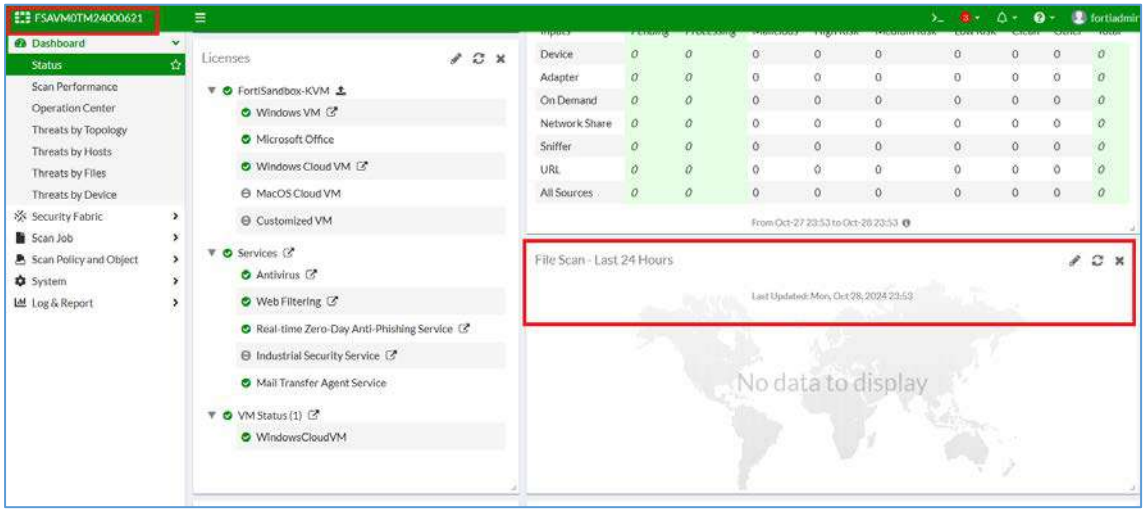
Afim de não restar duvidas, será fornecido de forma complementar mais uma referência com mais informações:

> *https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/414737/file-scan*

Nota-se o campo de arquivos scaneado conforme trecho “Fortifate Scanned Files” no FortiGate.



Nota-se o campo “File Scan” melhor evidenciando no FortiSandbox.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

4.8. <u>Subitem 1.5.8.20</u>

2.5.8.20. Arquivos maliciosos;

<u>Referência/URL</u>

"Threats by Hosts

On this page you can view and drill down all threats grouped by hosts. The Host can be a user name or email address (if it is available) or a device that is the target of a threat. This page displays all threats that have occurred to the user or victim host during a time period. Click the View Jobs icon or double-click an entry in the table to view the second level.

Rubrica

DS

(...)

# of Malicious Files: The number of unique malicious files associated with the user for the time period selected. Click the column header to sort the table by this column.

# of Suspicious Files: The number of unique suspicious files associated with the user for the time period selected. Click the column header to sort the table by this column.

# of Network Threats: The number of unique network threats (attacker, botnet, and suspicious URL events) associated with the user for the time period selected. Click the column header to sort the table by this column."

Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/667617/threats-by-hosts

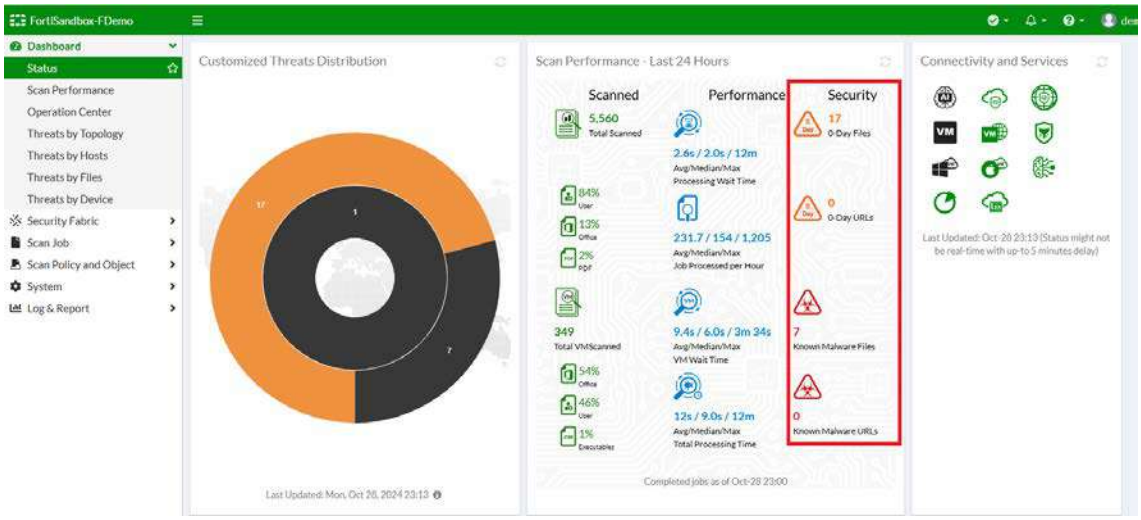
De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Em outro capitulo do mesmo documento citado no link de comprovação, constante no ponto a ponto, existe um capitulo chamado "Scan Statistics" que demonstra de forma mais detalhadas dos arquivos escaneados e o veredito de avaliação de cada arquivo.

Afim de não restar duvidas, será fornecido de forma complementar mais uma referência com mais informações:

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/652586/scan-statistics

Note a coluna dedicada apenas aos arquivos idenficados como “Maliciosos”.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

Rubrica

DS

5. 2.6. SERVIÇO DE PROTEÇÃO DE DATACENTER GRANDE PORTE

5.1. Subitem 2.6.2.10

2.6.2.10. Capacidade para suportar, pelo menos, 30 contextos virtuais;

Referência/URL

"Datasheet FortiGate 2600F Series | Pág. 8

Specifications

System Performance and Capacity

Virtual Domains (Default / Maximum): 10 / 500"

Comprovação/Link

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-2600f-series.pdf

Pg 8.

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

O documento utilizado como referência informado no ponto a ponto, demonstra as quantidades de VDOMs (Instancias Virtuais) que o equipamento suporta.

A quandidade mínima (10) já vem por padrão no sistema operacional do equipamento, tanto que o documento menciona como "default".

Para expandir a quantidade e atender a necessidade de 30, conforme exigido na especificação técnica, consideramos na proposta comercial os part numbers FG-VDOM-15-UG - Virtual Domain License Add 15 e FG-VDOM-5-UG - Virtual Domain License Add 5 que a soma dos dois habilitam mais 20 VDOMs em cada equipamento para atender ao mínimo que foi exigido no edital.

Vale destacar que o referido item menciona o termo suportar que no âmbito de licitação significa que a solução ofertada deve suportar uma capacidade para uso futuro, garantindo assim que a solução ofertada permita o futuro incremento, nivelando assim a oferta durante a licitação.

Ademais a proposta ofertada foi além e cotou como composição de oferta a inclusão de algumas instâncias de firewall, ora VDOM, Licenças FN-FG-VDOM-15-UG e FN-FG-VDOM-5-UG, afim de atender 100% das necessidades, porem foi informado na proposta um quantitativo de “1” para cada licença, ocorre que ouve um erro material ao transpor a quantidade correta de “4 licenças” para a proposta.

Rubrica DS

Neste sentido ratificamos que o projeto foi elaborado e construído considerando a quantidade correta de “4” licenças cada afim de atender os requisitos do edital, sem nenhum prejuízo para a PRODAM.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.2. **Subitem 2.6.4.36**

> *2.6.4.36. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam defini das no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".*
>
> ***Referência/URL***
>
> *"Data loss prevention*
>
> *The FortiGate data loss prevention (DLP) system prevents sensitive data from leaving or entering your network by scanning for various patterns while inspecting traffic passing through the FortiGate. Data that matches defined sensitive data patterns is blocked, logged, allowed, or quarantined when it passes through the FortiGate."*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/153498/data-loss-prevention*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A página WEB disponibilizada no ponto a ponto, descreve a funcionalidade como um todo e abre subpáginas dependentes a esta com detalhes e particularidades referente ao item em questão.

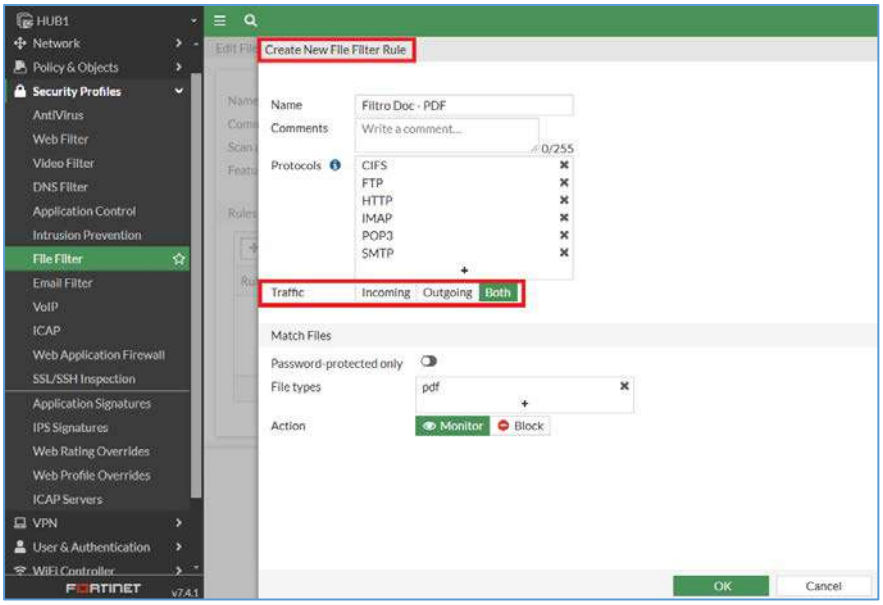
Ao navegar no portal, indo até o final da página mencionada, encontramos um hiperlink *"DLP examples"*, que ao acessar, abre-se uma nova página com os exemplos de criação de regras / políticas que fazem controle do tráfego nos sentidos upload, download e ambos.

De forma complementar e afim de facilitar a consulta segue o link onde vai direto para esta informação:

> *https://docs.fortinet.com/document/fortigate/7.4.2/administration-guide/580649/link-health-monitor*

Para o pleno atendimento deste requisito, o FortiGate possui a funcionalide de “File Filter”, responsável por filtrar arquivos por extensão ou tipo.

Note na imagem abaixo, Vide configuração de uma regra da funcionalidade de “File Filter”, trazendo o destaque em vermelho para a direção do tráfego, ora as opções: “Incoming” (entrada), “Outgoing” (saída) ou “Both” (ambos os sentidos):



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.3. **Subitem 2.6.4.37**

> *2.6.4.37. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.*
>
> ***Referência/URL***
>
> *Technical Tip: How to use DLP to block traffic from messages that contain credit card information*
> *Description: This article describes how to use DLP to block traffic from messages that contain credit card information.*
> *(...)*
> *Testing:*
> *The user tries to send an email that contains credit card information and gets blocked.*
> *<screenshot>*
>
> ***Comprovação/Link***
>
> *https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-DLP-to-block-traffic-from-messages-that/ta-p/302999*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Rubrica

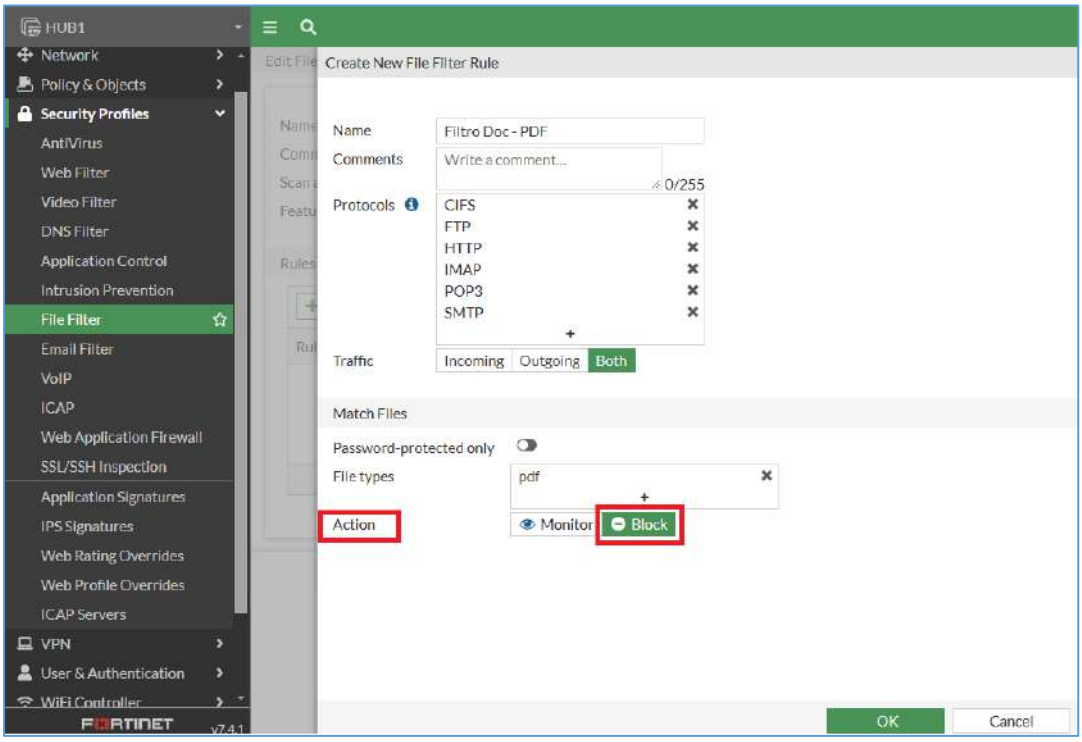
DS

A página WEB disponibilizada no ponto a ponto, descreve o fluxo de aprovisionamento da funcionalidade e no item "Testing" ela mostra o resultado de uma simulação de envio de um e-mail com arquivo em anexo que fere a política de DLP criada.

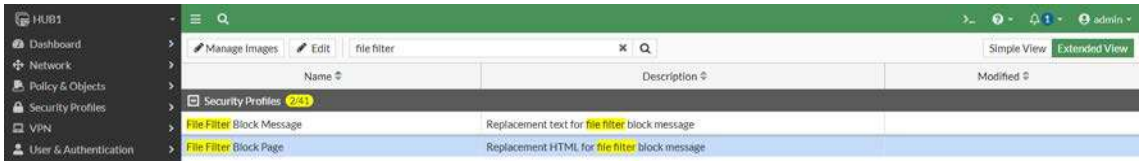
Ao clicar diretamente em cima da penúltima figura da página é possível ver um exemplo de alerta de bloqueio que o usuário vai receber ao tentar enviar um conteúdo que viola essa política.

Para o pleno atendimento deste requisito, o FortiGate possui a funcionalide de “File Filter”, responsável por filtrar arquivos por extensão ou tipo.

Conforme configuração do perfil de segurança “File Filter” notamos as ações “Monitor” ou “Block” conforme imagem abaixo, note a ação de “Block” dentro da funcionalidade de “File FIlter”.:



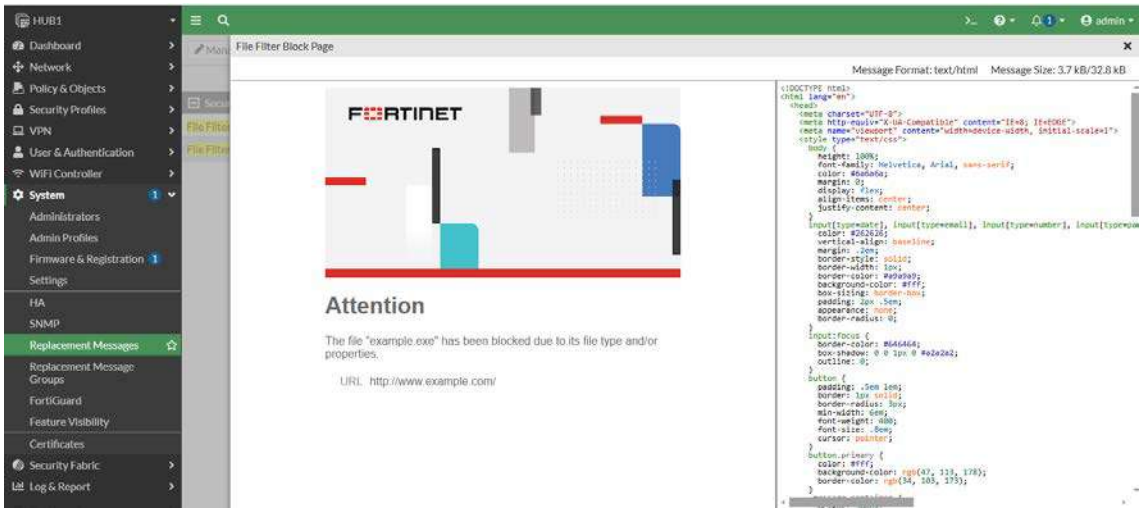
Note a página de bloqueio da ação de bloqueio do “File Filter”.



Note a imagem da página de bloqueio do “Filter Filter” disponível para visualização e edição.

Rubrica

DS



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.4. **Subitem 2.6.8.9**

2.6.8.9. Todas as máquinas virtuais (Windows e Linux) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

Referência/URL

"FortiSandbox Data Sheet | Pág. 7

Sandboxing (Dynamic AI Scan) Support

(…)

• OS type supported: Windows 11/10/8.1/7, macOS, Linux, Android, and ICS systems"

Comprovação/Link

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

Pg 7

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

A página do datasheet que foi citada no ponto a ponto, informa as opções de sistemas operacionais que podem ser utilizados para a verificação dos arquivos.

De acordo com o manual da solução, as alocações das VM com os seus respectivos sistemas operacionais podem ser definidas no momento da implementação da ferramenta deixando as opções de sistemas operacionais prontas para serem utilizadas para a verificação dos arquivos.

Rubrica

DS

Após a implementação o sistema gerencia sem a necessidade de intervenção do administrador.

De forma complementar e afim de facilitar a consulta segue o link onde vai direto para esta informação:

https://docs.fortinet.com/document/fortisandbox-cloud/latest/cloud-deployment/275752/assigning-sandboxing-vm-clones

A solução de Sandbox ofertada para este certame chama-se FortiSandbox Cloud (Paas), conforme url https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf , na página 5, no trecho "*Fortinet maintains, updates, and operates the platform on your behalf.*", concluindo assim que como a solução ofertada é baseada na nuvem do Fabricante Fortinet, todos os updates são administrados pela própria Fortinet.

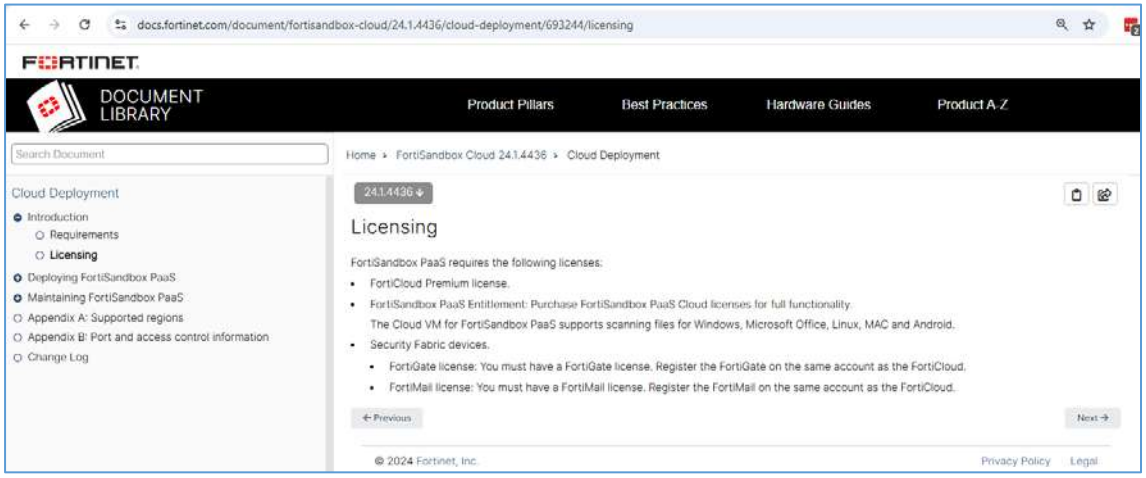
Na proposta comercial, conforme licenças informadas na proposta: FN-FC2-10-SACLP-433-01-36, "FortiSandbox Cloud - Windows (5 VMs) FortiSandbox Cloud 5-VM Expansion - Expands dedicated sandbox instance by 5 Windows cloud VMs. FortiSandbox Cloud supports up to 200 Windows VMs, and provides AI powered sandbox analysis. (requires FortiCloud Premium".

Nota-se a oferta na Proposta Comercial da Solução "FortiSandbox Cloud PaaS", sendo composta por bundles licenças múltiplo de 5 VMs em ambiente Sandbox.

Esta solução é integrada ao firewall FortiGate via API. O fluxo operacional de um arquivo suspeito é iniciado no momento em que o FortiGate identifica o arquivo passando por ele, sendo este "offloaded" descarregado) do tráfego e enviado para a Nuvem do FortiSandbox, onde este arquivo passa a ser inspecionado em ambiente controlado sandbox, caso seja identificado comportamento malicioso, o FortiSandbox gera uma assinatura, e envia o veredito da inspeção para o FortiGate.

O licenciamento permite ativar todo o ambiente em nuvem, descartando qualquer necessidade de integração com os hosts de rede, ou seja: tudo acontece na camada de rede quando o tráfego passa pelo FortiGate, os hosts de rede não possuem nenhum agente ou aplicativo instalado para comunicação com o FortiGate.

Visando melhor explicar, o licenciamento do "*FortiSandbox Cloud PaaS*", conforme url https://docs.fortinet.com/document/fortisandbox-cloud/24.1.4436/cloud-deployment/693244/licensing , no trecho conforme imagem, comprova-se que todo o licenciamento necessário foi ofertado, evidenciando desta forma que os licenciamentos pertinentes as VMs: Windows, Microsoft Office, Linux, MAC e Android já estão inclusos



Rubrica

DS

na licença do “FortiSandbox PaaS” e licença de aceso a nuvem com o “FortiCloud Premium License”.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.5. **Subitem 2.6.8.16**

2.6.8.16. Quantidade de arquivos que estão em emulação;

Referência/URL

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year).

The Scan Performance dashboard contains the following charts:

Scanned Count: The total number of scanned jobs per time unit.

VM Scan count: The total number of jobs that entered the VM for dynamic scan per time unit.

Average Processing Wait Time: The wait time in the initial processing queue.

Average VM Wait time: The wait time prior to entering the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.

Average Process Time: The processing time from receiving to completing the scan based on the average calculated time divided by total jobs per time unit.

Average VM Scan Time: The processing time within the VM for dynamic scan based on the average calculated time divided by total jobs per time unit."

Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

Rubrica

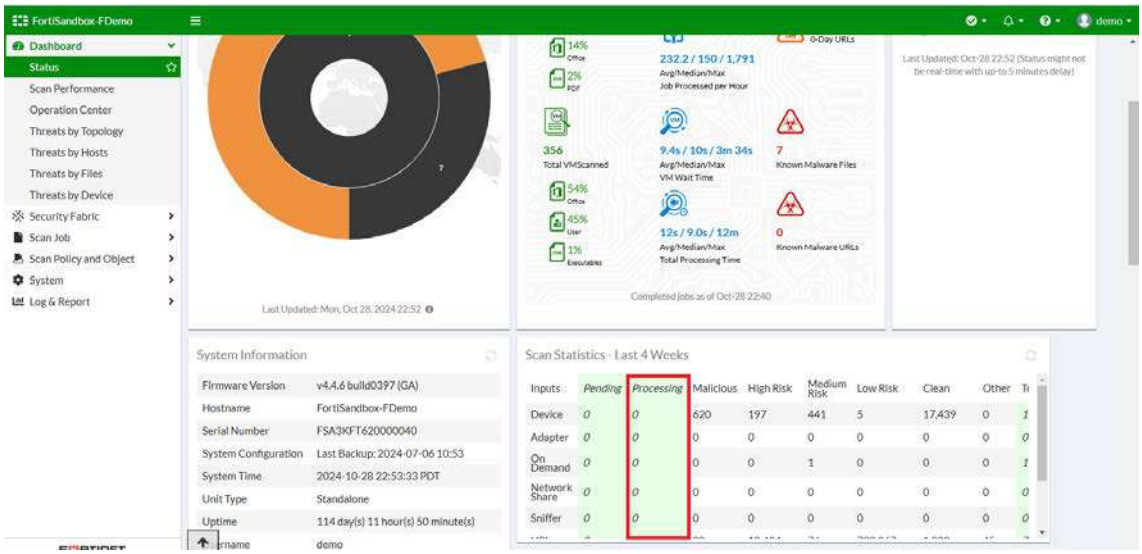
DS

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Conforme podemos observar no link disponibilizado o *VM Scan count - The total number of jobs that entered the VM for dynamic scan per time unit.*

Trata-se da contagem de varredura de VM, ou seja, o número total de trabalhos que entraram na VM para varredura dinâmica por unidade de tempo.

Nota-se conforme destaque em vermelho, a relação de arquivos que estão em Processamento.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.6. **Subitem 2.6.8.17**

2.6.8.17. Número de arquivos emulados;

Referência/URL

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year).

Rubrica

DS

The Scan Performance dashboard contains the following charts:

Scanned Count: The total number of scanned jobs per time unit.

VM Scan count: The total number of jobs that entered the VM for dynamic scan per time unit.

Average Processing Wait Time: The wait time in the initial processing queue.

Average VM Wait time: The wait time prior to entering the VM for dynamic scan based on the average calculated time divided by total jobs per time unit.

Average Process Time: The processing time from receiving to completing the scan based on the average calculated time divided by total jobs per time unit.

Average VM Scan Time: The processing time within the VM for dynamic scan based on the average calculated time divided by total jobs per time unit."

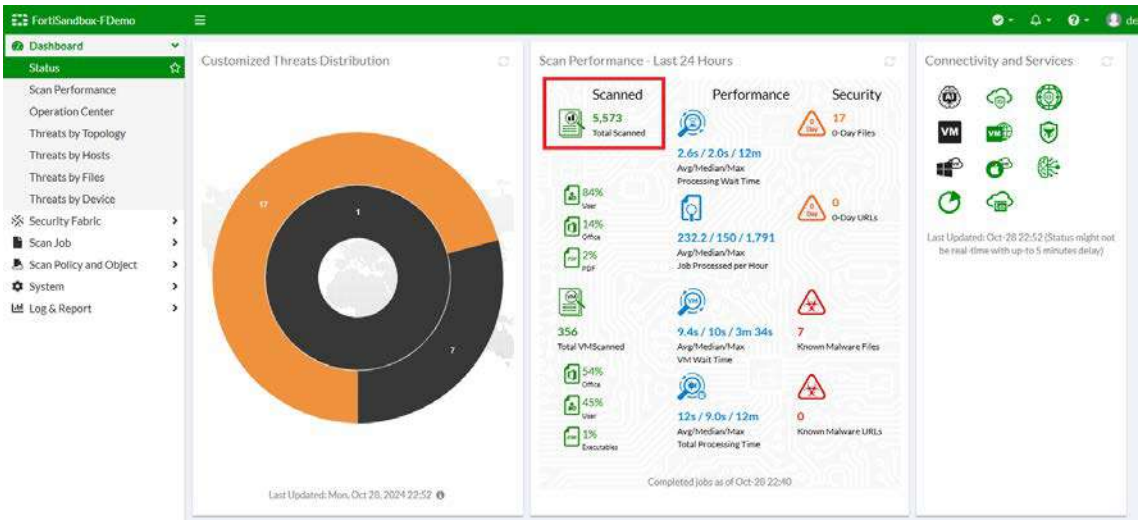
Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Conforme podemos observar no link disponibilizado o *Scanned Count - The total number of scanned jobs per time unit*. trata-se da contagem de arquivos escaneados, ou seja, o número total de trabalhos escaneados por unidade de tempo.

Nota-se em destaque vermelho na imagem abaixo, a quantidade de arquivos emulados ou escaneados.



Rubrica FHL

DS

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.7. **Subitem 2.6.8.18**

> *2.6.8.18. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:*
>
> ***Referência/URL***
>
> *"Scan Performance (dashboard)*
>
> *The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.*
>
> *The options for the unit of time will vary based on the time range. For example, the hourly view is displayed in shorter time ranges (1 day, 3 days and 7 days), whereas the day view is displayed in longer ranges (4 weeks and 1 Year). "*
>
> ***Comprovação/Link***
>
> *https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

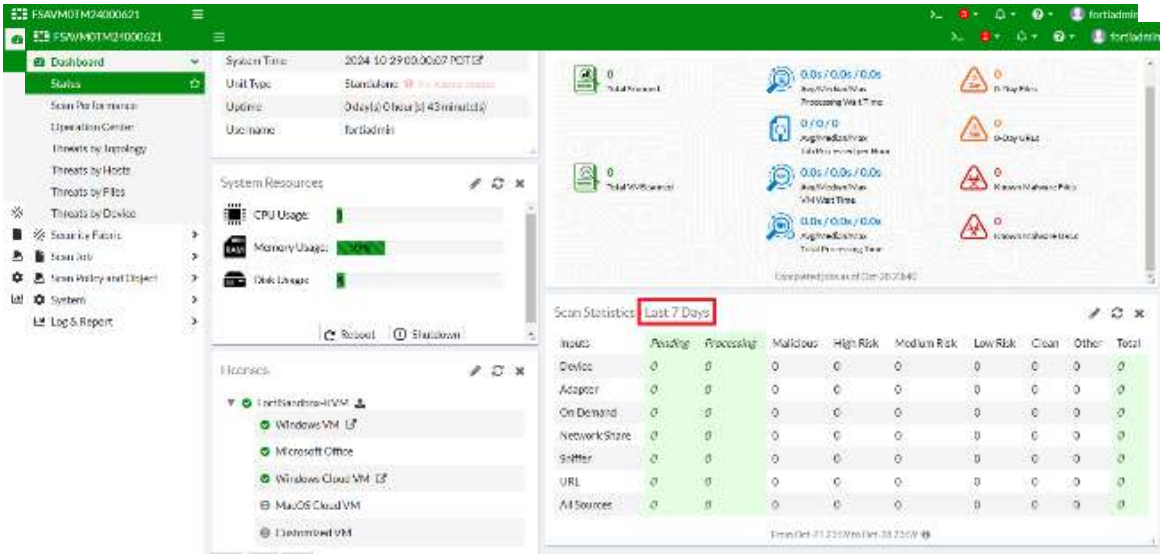
A solução possui um filtro temporal onde permite que seja alterado para visualização das estatísticas.

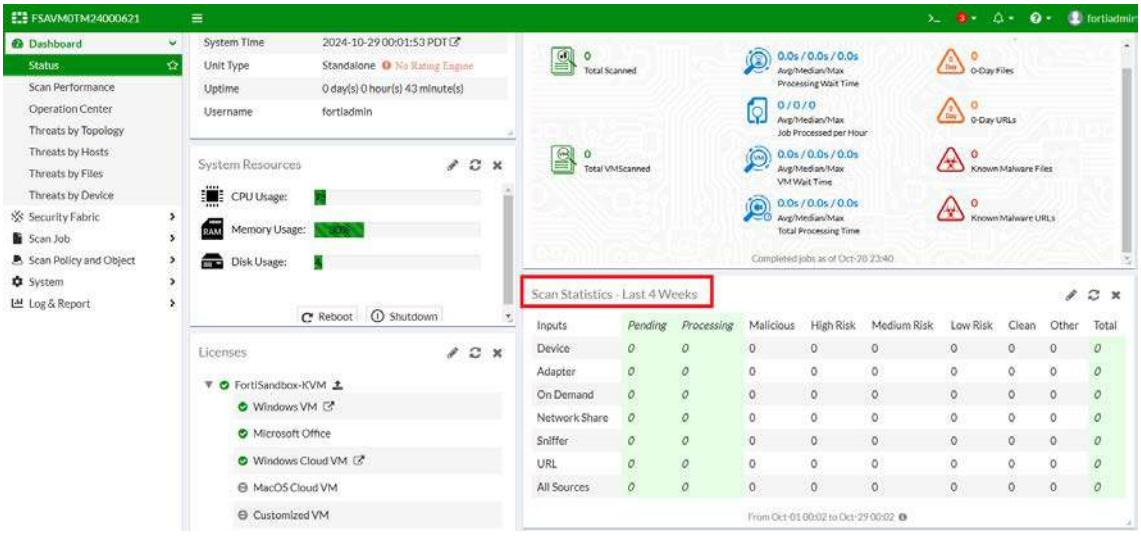
As opções para a unidade de tempo variam de acordo com o intervalo de tempo. Por exemplo, a visualização por hora é exibida em intervalos de tempo mais curtos (1 dia, 3 dias e 7 dias), enquanto a visualização por dia é exibida em intervalos mais longos (4 semanas e 1 ano), permitindo assim a visualização último dia, última semana ou últimos 30 dias.

Rubrica FHL

DS MCFM

Nota-se imagens extraídas do FortiSandob com com destaques de tempo variados entre: “Last 24 hours” (últmas 24 horas), “Last 7 Days” (últimos sete dias) e Last 4 Weeks (último mês).





Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.8. **<u>Subitem 2.6.8.19</u>**

2.6.8.19. Arquivos scaneados;

<u>Referência/URL</u>

"Scan Performance (dashboard)

The Scan Performance dashboard tracks the FortiSandbox performance over time. The data is similar to the Scan Performance widget and is accumulated every 10 minutes. The page is automatically refreshed every 5 minutes. To view the Scan Performance dashboard, go to Dashboard > Scan Performance.

(...)

Rubrica

DS

The Scan Performance dashboard contains the following charts:

Scanned Count: The total number of scanned jobs per time unit."

Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/787289/scan-performance-dashboard

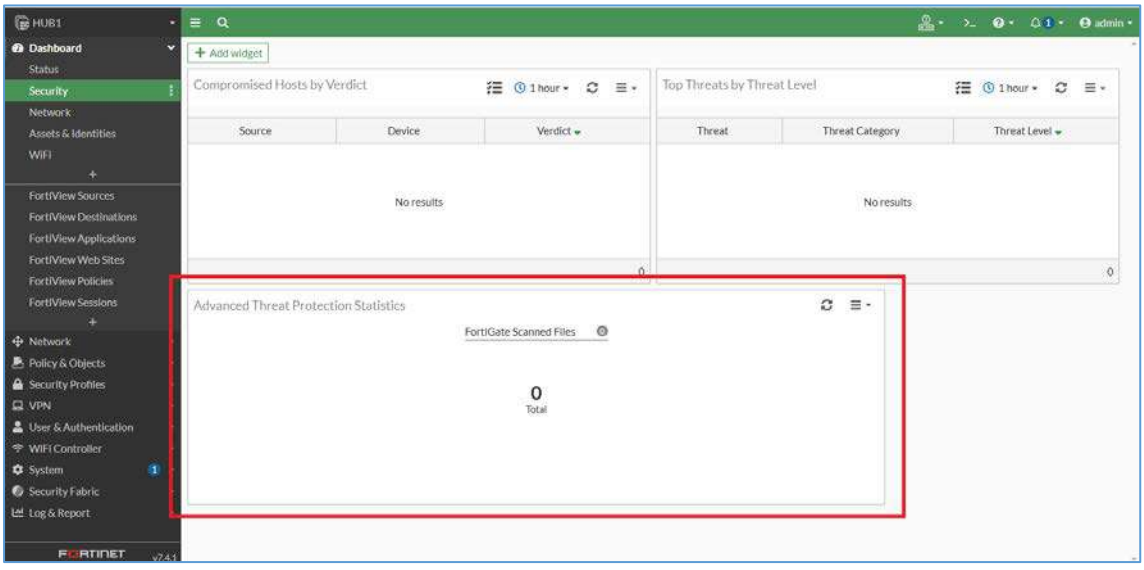
De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Em outro capitulo do mesmo documento citado no link de comprovação constante no ponto a ponto, existe um outro capitulo chamado *"File Scan"* que demonstra de forma mais detalhadas os arquivos escaneados e o veredito de avaliação de cada arquivo.

Afim de não restar duvidas, será fornecido de forma complementar mais uma referência com mais informações:

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/414737/file-scan

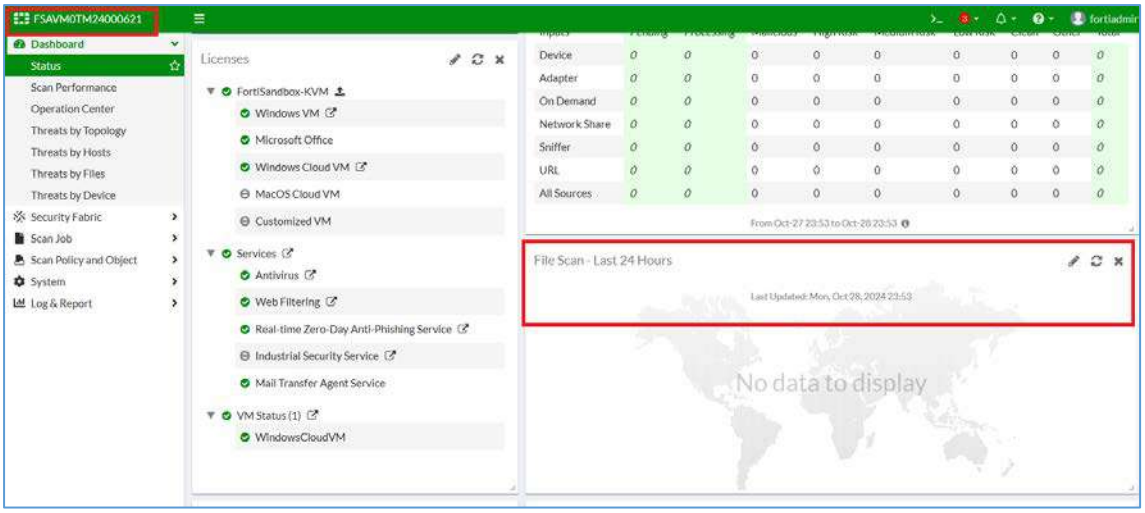
Nota-se o campo de arquivos scaneado conforme trecho “Fortifate Scanned Files” no FortiGate.



Nota-se o campo “File Scan” melhor evidenciando no FortiSandbox.

Rubrica

DS



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

5.9. **Subitem 2.6.8.20**

2.6.8.20. Arquivos maliciosos;

Referência/URL

"Threats by Hosts

On this page you can view and drill down all threats grouped by hosts. The Host can be a user name or email address (if it is available) or a device that is the target of a threat. This page displays all threats that have occurred to the user or victim host during a time period. Click the View Jobs icon or double-click an entry in the table to view the second level.

(...)

# of Malicious Files: The number of unique malicious files associated with the user for the time period selected. Click the column header to sort the table by this column.

# of Suspicious Files: The number of unique suspicious files associated with the user for the time period selected. Click the column header to sort the table by this column.

# of Network Threats: The number of unique network threats (attacker, botnet, and suspicious URL events) associated with the user for the time period selected. Click the column header to sort the table by this column."

Comprovação/Link

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/667617/threats-by-hosts

Rubrica

DS

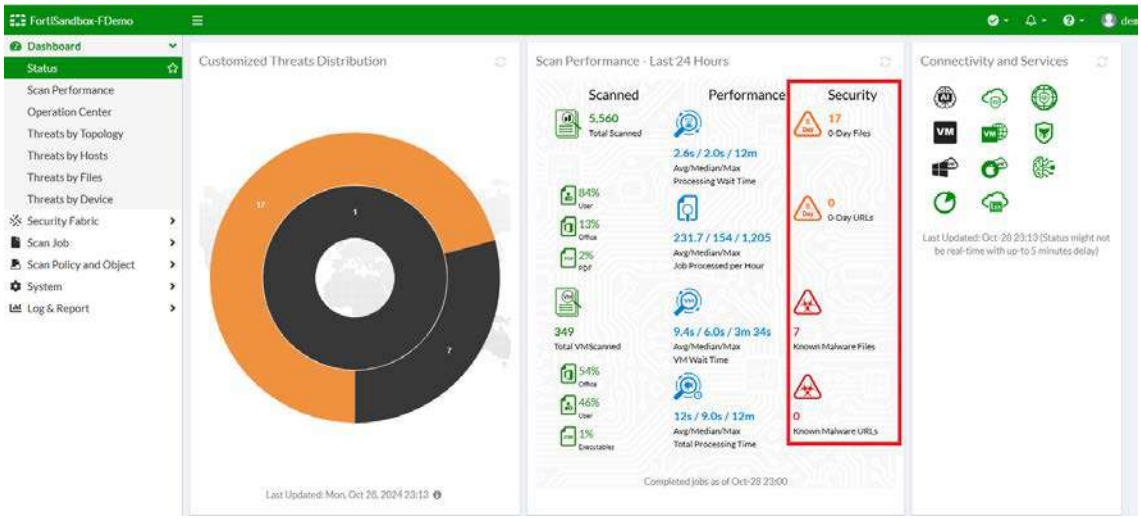
De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Em outro capitulo do mesmo documento citado no link de comprovação, constante no ponto a ponto, existe um capitulo chamado "Scan Statistics" que demonstra de forma mais detalhadas dos arquivos escaneados e o veredito de avaliação de cada arquivo.

Afim de não restar duvidas, será fornecido de forma complementar mais uma referência com mais informações:

https://docs.fortinet.com/document/fortisandbox/4.4.6/administration-guide/652586/scan-statistics

Note a coluna dedicada apenas aos arquivos idenficados como “Maliciosos”.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

6. ANEXO 1-B – GERENCIAMENTO

6.1. Subitem 5

5. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

Referência/URL

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

Comprovação/Link

Rubrica

DS

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

Conforme demonstrado no datasheet da solução FortiAnalyzer informado na proposta comercial, modelo FortiAnalyzer 3.100G, além de ser um repositório/gerenciador de logs também fornece relatórios estendidos.

Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

6.2. **Subitem 25**

25. POST ou Request Body logados;

Referência/URL

"HTTP Body Enter the HTTP body of the message that should be sent by the connector.

For example, { \"text\": \"<message to send>\" }."

Comprovação/Link

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/93abf76c-cd9e-11ed-8e6d-fa163e15d75b/FortiAnalyzer-7.4-New_Features_Guide.pdf

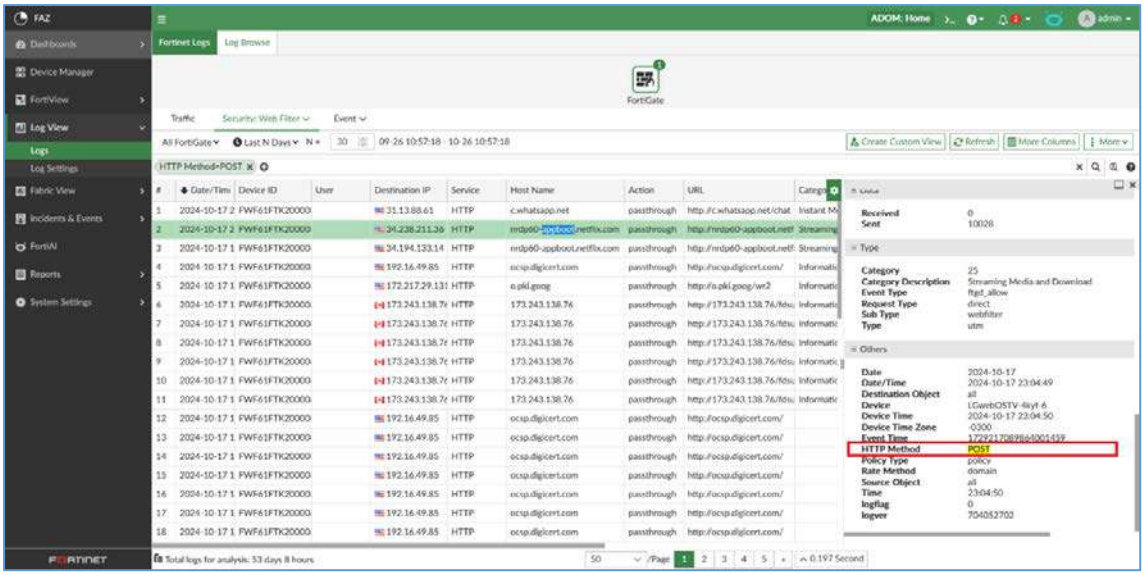
De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

O link informado traz o documento completo constante no servidor do fabricante, onde também é possível localizar essa mesma página no documento a seguir:

https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide/145903/itsm-connectors

Buscar em "Conctores ITSM", na descrição é retratado como fazer para criar um conector e enviar mensagens tipo POST ou Request Body para a aplicação do TEAMS, pode-se utilizar a mesma estrutura para envio dessas informações para outras farramentas (ex.: ServiceNow, Slack, Webhood e demais) via conector.

Nota-se o destaque em vermelho para o grau de inserção e recepção de logs, trazendo registros contendo o campo “HTTP Method.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

6.3. **Subitem 26**

26. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

Referência/URL

Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.

Comprovação/Link

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

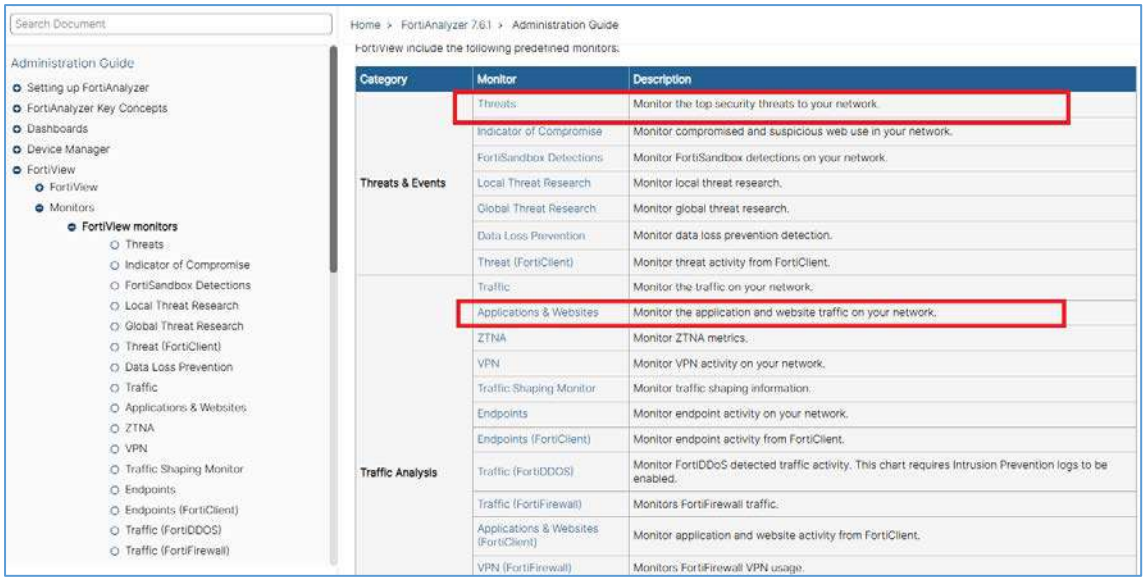
No link informado, com a integração junto ao FortiFabric, fornece recursos de análise de segurança centralizada de ponta a ponta em tempo real através de uma equipe de operação do FortiGuard, dessa forma sendo identificado e mitigado possíveis ameaças pelo Fortigate, com o log habilitado no FortiAnalyzer é possível visualizar através das dash e exportar via relatório, mais detalhes de como exportar o relatório no link que segue:

https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide/002854/list-of-report-templates

Rubrica

DS

Nota-se destaques em vermelho de “Threats” e “Applications e Websites”.



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

6.4. **Subitem 27**

> *27. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;*
>
> ***Referência/URL***
>
> *Integrated with the Fortinet Security Fabric, FortiAnalyzer enables Network and Security Operations Teams with real-time detection capabilities, centralized security analytics and end-to-end security posture awareness to help analysts identify advanced persistent threats (APTs) and mitigate risks before a breach can occur.*
>
> ***Comprovação/Link***
>
> *https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortianalyzer.pdf*

De acordo com as informações disponibilizadas segue a Justificativa comprovando o atendimento ao referido Item em questão:

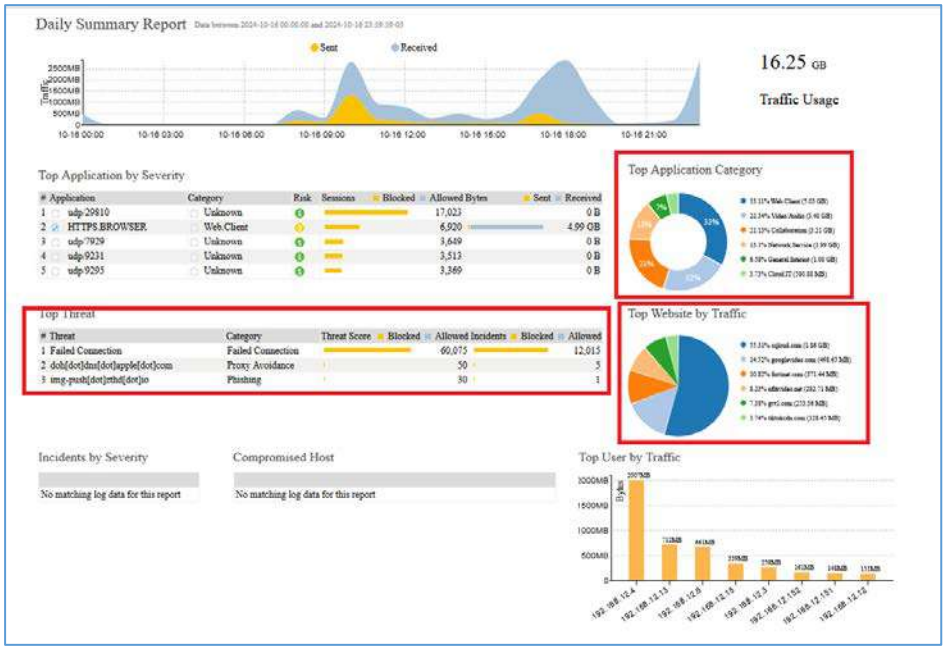
No Link informado, com a integração junto ao FortiFabric, fornece recursos de análise de segurança centralizada de ponta a ponta em tempo real através de uma equipe de operação do FortiGuard, dessa forma sendo identificado e mitigado possíveis ameaças pelo Fortigate, com o log habilitado no FortiAnalyzer é possível visualizar de forma centralizada nas dashes do Fortianalyzer, mais detalhes em como visualizar de forma sumarizada através do link que segue:

Rubrica

DS

https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide/002854/list-of-report-templates

Nota-se os destaques sumarizados de “Threats” (ameaças), “Top Application Category” (aplicações) e “Top Website by Traffic” (websites ou url).



Logo está comprovado o atendimento ao referido Item que gerou a desclassificação de forma equivocada.

7. DA EQUIVOCDA CLASSIFICAÇÃO DA EMPRESA IT PROTECT

Seguindo o rito do processo licitatório, após a desclassificação da Oi, o pregoeiro classificou a proposta da empresa IP Protect, terceira proposta classificada na fase de lances, conforme mensagem abaixo:

> *Mensagem do Pregoeiro*
>
> *Srs. licitantes, informamos que a proposta da licitante IT PROTECT SERVICOS DE CONSULTORIA EM INFORMATICA LTDA, classificada em 3º lugar, atende tecnicamente as exigências editalícias, bem como está devidamente habilitada. O valor global ofertado é de R$ 22.544.950,00. Os documentos estão disponíveis no portal de transparência da PRODAM, assim como no sistema comprasnet.*
>
> Enviada em 30/10/2024 às 15:37:07h.

Rubrica FHL DS MCFM

Não obstante, cumpre mencionar que IT Protect apresentou a proposta com valor global de R$ 22.544.950,00, ou seja, R$ 1.399.950,04 acima do valor arrematado pela empresa OI, trazendo assim um prejuízo para a PRODAM.

Adicionalmente, ao avaliarmos toda a documentação, proposta e ponto a ponto apresentado pela empresa IT Protect verifica-se que a mesma ofertou os mesmos modelos de equipamentos apresentados pela Oi.

Na proposta apresentada pela Oi tem mais detalhes sobre os equipamentos ofertados, além da informação de modelo, consta as licenças que serão fornecidas, as Gbics exigidas no edital, bem como a solução de Gerenciamento da solução que não consta na proposta da IT Protect.

Sendo assim, está evidente que a proposta da Oi atendeu a todas as exigências do instrumento convocatório e é a mais vantajosa economicamente para a Administração Pública.

Vale destacar que a vantajosidade não é sinônimo de menor preço, vantajosidade é sim o menor preço, mas o menor preço de uma proposta que atenda plenamente a necessidade da Administração e todas as exigências constantes no Edital.

O que significa dizer que se exige da Administração que se busque sempre a melhor proposta e não somente aquela que oferecer o menor preço, mas também, e principalmente, a que guardar consonância com os requisitos impostos pela Administração como necessários à sua elaboração.

O procedimento licitatório tem um objetivo, que é oportunizar a formalização de contrato entre a Administração e o licitante vencedor. Desta forma, se uma licitante não apresenta especificações técnicas e capacidade técnica, imprescindíveis à análise de sua solução, sua participação configura-se como inapta tecnicamente. O contrário disso ferirá a competitividade, desatendendo o essencial objetivo do instituto licitatório.

Rubrica

DS

A necessidade de revisão da decisão ora combatida advém do zelo pela regularidade do processo e da segurança jurídica que deve ser garantida a todos os licitantes, bem como da consonância com a Lei Geral de Licitações, em seu art. 3º, que dispõe, aqui utilizada de forma subsidiária:

> *"Art. 3º. A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos."*

Ressalte-se, que com base no Princípio da Legalidade aplicável à Administração Pública, esta só pode – e deve – fazer aquilo que está previsto em lei, e, portanto, deve cumprir o disposto na Lei que fundamentou o certame e sujeitar-se aos termos e condições previstos no seu instrumento convocatório – o Edital, sob pena de ilegalidade passível de tornar nulo o procedimento e a contratação que dele derivar.

No caso em comento, não há dúvidas que houve violação ao princípio da isonomia, considerando a proposta que foi classificada em detrimento da proposta da Oi.

Por tudo que se expôs, resta evidente que a OI cumpriu todas as exigências editalícias e está plenamente apta para prestar o serviço ora licitado, razão pela qual vem através do presente Recurso Administrativo solicitar que o I. Pregoeiro da PRODAM se digne a reformar a decisão que declarou inabilitada e desclassificou sua proposta, sob pena de grave prejuízo financeiro à Administração Pública, além de violação clara aos princípios norteadores dos procedimentos licitatórios.

Rubrica

DS

8. Pedido

Ante o exposto, a OI SOLUÇÕES S.A requer que seja devidamente processado o presente Recurso Administrativo para que o I. Pregoeiro da PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S.A, se digne a reformar a decisão que desclassificou a sua proposta, sob pena de grave ofensa aos princípios norteadores das licitações.

Termos em que,

Pede deferimento.

Manaus – AM, 01 de novembro de 2024.

Assinado por:
Francisco Hericsson de Lima
7A74FE3C134B4DF...

Francisco Hericsson de Lima
CPF: 797.497.983-68
Gerente de Vendas

DocuSigned by:
D0B5A52D5B804CF...

Marcos Cesar de Freitas Mello
CPF: 562.199.382-91
Executivo de Negócios

DocuSign

Certificado de Conclusão

Identificação de envelope: 6DD71DA3552A47B592D003DDB1E04694
Status: Concluído
Assunto: Complete com o Docusign: Recurso Administrativo - PRODAM_v2.pdf
Envelope fonte:
Documentar páginas: 70
Assinaturas: 2
Remetente do envelope:
Certificar páginas: 5
Rubrica: 138
Marcos Cesar de Freitas Mello
Assinatura guiada: Ativado
Rua do Lavradio 71
Selo com EnvelopeId (ID do envelope): Ativado
Rio de Janeiro, RJ 20230-070
Fuso horário: (UTC-03:00) Brasília
marcos.freitas@oi.net.br
Endereço IP: 187.46.90.191

Rastreamento de registros

Status: Original
04/11/2024 11:49:58
Portador: Marcos Cesar de Freitas Mello
marcos.freitas@oi.net.br
Local: DocuSign

Eventos do signatário	Assinatura	Registro de hora e data
Francisco Hericsson de Lima hericsson@oi.net.br Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	Assinado por: Francisco Hericsson de Lima 7A74FE3C134B4DF... Adoção de assinatura: Estilo pré-selecionado Usando endereço IP: 170.150.201.246	Enviado: 04/11/2024 12:14:02 Visualizado: 04/11/2024 12:15:43 Assinado: 04/11/2024 12:17:26

Termos de Assinatura e Registro Eletrônico:
Aceito: 04/11/2024 12:15:43
ID: 7c3495bb-b3ce-486b-b32f-0c37cd348ec2

Marcos Cesar de Freitas Mello marcos.freitas@oi.net.br Executivo de Negócios III OI S.A Nível de segurança: E-mail, Autenticação da conta (Nenhuma)	DocuSigned by: D0B5A52D5B804CF... Adoção de assinatura: Imagem de assinatura carregada Usando endereço IP: 187.46.90.191	Enviado: 04/11/2024 12:14:01 Visualizado: 04/11/2024 12:14:36 Assinado: 04/11/2024 12:15:59

Termos de Assinatura e Registro Eletrônico:
Não oferecido através do DocuSign

Eventos do signatário presencial	Assinatura	Registro de hora e data
Eventos de entrega do editor	**Status**	**Registro de hora e data**
Evento de entrega do agente	**Status**	**Registro de hora e data**
Eventos de entrega intermediários	**Status**	**Registro de hora e data**
Eventos de entrega certificados	**Status**	**Registro de hora e data**
Eventos de cópia	**Status**	**Registro de hora e data**
Eventos com testemunhas	**Assinatura**	**Registro de hora e data**
Eventos do tabelião	**Assinatura**	**Registro de hora e data**

Eventos de resumo do envelope	Status	Carimbo de data/hora
Envelope enviado	Com hash/criptografado	04/11/2024 12:14:02
Entrega certificada	Segurança verificada	04/11/2024 12:14:36

Eventos de resumo do envelope	Status	Carimbo de data/hora
Assinatura concluída	Segurança verificada	04/11/2024 12:15:59
Concluído	Segurança verificada	04/11/2024 12:17:26

Eventos de pagamento	Status	Carimbo de data/hora

Termos de Assinatura e Registro Eletrônico

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Oi Soluções - Sub Account (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Oi Soluções - Sub Account:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: niara.santos@oi.net.br

To advise Oi Soluções - Sub Account of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at niara.santos@oi.net.br and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Oi Soluções - Sub Account

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to niara.santos@oi.net.br and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Oi Soluções - Sub Account

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to niara.santos@oi.net.br and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Oi Soluções - Sub Account as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Oi Soluções - Sub Account during the course of your relationship with Oi Soluções - Sub Account.