+55 61 3033 5190
contato@infosecti.com.br
www.infosecti.com.br

Proc. Ref. PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS N° 11636/2025
LICITAÇÃO Nº 90003/2025
UASG 80013 - TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIAO

STF – "A observância ao princípio constitucional da preponderância da proposta mais vantajosa para o Poder Público se dá mediante o cotejo das propostas válidas apresentadas pelos concorrentes, não havendo como incluir na avaliação a oferta eivada de nulidade." (RMS 23640/DF)

. **A INFOSEC TECNOLOGIA DA INFORMAÇÃO LTDA.,** já conhecida no referido processo, vem, por sua representante legal, na forma de seu Contrato Social, com fundamento no Art. 165 da Lei 14.133/21, ofertar o presente **RECURSO ADMINISTRATIVO** em face da decisão administrativa que habilitou a licitante Soow Sigma Ltda pelas razões de fato e de direito a seguir aduzidas.

(I) HISTÓRICO

. Trata-se de Pregão Eletrônico para Registro de Preços cujo objeto é para aquisição de solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access); Voucher de Treinamento para solução SASE e ZTNA.

. A Licitante recorrida foi indevidamente habilitada no presente certame sem cumprir com diversas exigências editalícias, dentre as quais se destacam por maior gravidade: (i) a funcionalidade de FWaaS não é suportada nos clientes para sistemas operacionais Linux e Android; e (ii) ao contrário do que determina o Instrumento

Convocatório, as funcionalidades disponibilizadas pela Recorrida **não serão** ofertadas em nuvem;

(II) DO MÉRITO

(II.I) A Funcionalidade de Fwaas Não É Suportada

. Em que pese a diligência com que conduz o presente certame, essa D. Comissão está sendo levada a erro ao habilitar uma solução que descumpre o instrumento convocatório e que não será suportada nos sistemas operacionais Linux e Android.

. O item do instrumento convocatório é cristalino ao determinar que *"A solução deverá suportar capacidades de Firewall como serviço* ***via agentes instalados nas máquinas dos usuários*** *nas plataformas Windows,* ***Linux****, IOS, MacOS e* ***Android****;"*

. A exigência editalícia em referência foi inclusive objeto de questionamento, tendo essa D. Administração reforçado a importância da exigência que se justifica para garantir o nível de visibilidade, controle e segurança esperado na proteção dos dispositivos de acesso.

É sabido que as respostas de esclarecimentos, quando não implicam em alteração da proposta, vinculam tanto os licitantes quanto a administração pública. Mais ainda, ao responder diretamente ao questionamento, impõe-se à Administração no curso do processo licitatório um ônus argumentativo maior, de modo que tal exigência fica ainda mais em evidência, não podendo ser afastada por um suposto formalismo moderado.

. Conforme o manual de licitações e contratos do TCU (Tribunal de Contas da União), o item 5.1.1 deixa claro que:

> *"Se a impugnação for acolhida ou o pedido de esclarecimento resultar em alteração do edital (ou dos seus anexos), será necessária a republicação, na mesma forma de divulgação inicial, e os prazos originalmente previstos deverão ser reabertos, exceto*

> *quando a alteração não comprometer a formulação das propostas[4]. **Ademais, as respostas aos pedidos de esclarecimentos vinculam os licitantes e a Administração. Portanto, essas respostas devem ser devidamente registradas, pois poderão afetar o julgamento das propostas e a execução contratual** (p. ex., respostas de caráter técnico poderão afetar o recebimento provisório do objeto).”* - https://licitacoesecontratos.tcu.gov.br/5-1-1-impugnacao-e-pedidos-de-esclarecimento/

. Adicionalmente, conforme o subitem 20.3 do Edital, em relação aos Pedidos de Esclarecimentos e das Impugnações ao Edital, **item 20**, o TRT12 deixa claro que os esclarecimentos prestados vinculam os participantes (licitantes) e a Administração (TRT12), veja-se:

> *“20.3. **As respostas aos pedidos de esclarecimento e às impugnações serão divulgadas ao público exclusivamente na página do Tribunal na Internet**, no endereço https://portal.trt12.jus.br/licitacoes, e **vincularão os participantes e a Administração.**”*

. Não há, portanto, margem para se deixar de aplicar os requisitos editalícios, especialmente quando tais requisitos tiveram sua importância reafirmada por oportunidade dos pedidos de esclarecimentos.

. Desta maneira, conforme esclarecimentos prestados em portal de acesso público - https://portal.trt12.jus.br/licitacoes/PE-11636_2025/esclarecimentos – o TRT12, deixam claro que **a solução deve estar em total conformidade com o item 3.1.3.1, desta maneira, a solução oferecer suporte às soluções Linux e Android para a instalação de agente com suporte às funcionalidades de FWaaS (Firewall as a Service)**, veja-se:

> *“3.1.3.1. A solução deverá suportar capacidades de Firewall como serviço **via agentes instalados nas máquinas dos usuários** nas plataformas Windows, **Linux**, IOS, MacOS e **Android**;”*

Infosec Data Security
+55 61 3033 5190
contato@infosecti.com.br
www.infosecti.com.br

Questionamento 1) Acerca do subitem 3.1.3.1, integrante do item 3.1.3, que trata das Características para funcionalidades de FWaaS (Firewall as a Service):

"3.1.3.1. A solução deverá suportar capacidades de Firewall como serviço via agentes instalados nas máquinas dos usuários nas plataformas Windows, Linux, IOS, MacOS e Android;"

Nestes termos, a exigência de implementação exclusivamente via agentes locais em todos os sistemas operacionais mencionados, pode restringir a competitividade da licitação, ao excluir soluções modernas que utilizam arquiteturas de segurança mais flexíveis e escaláveis.

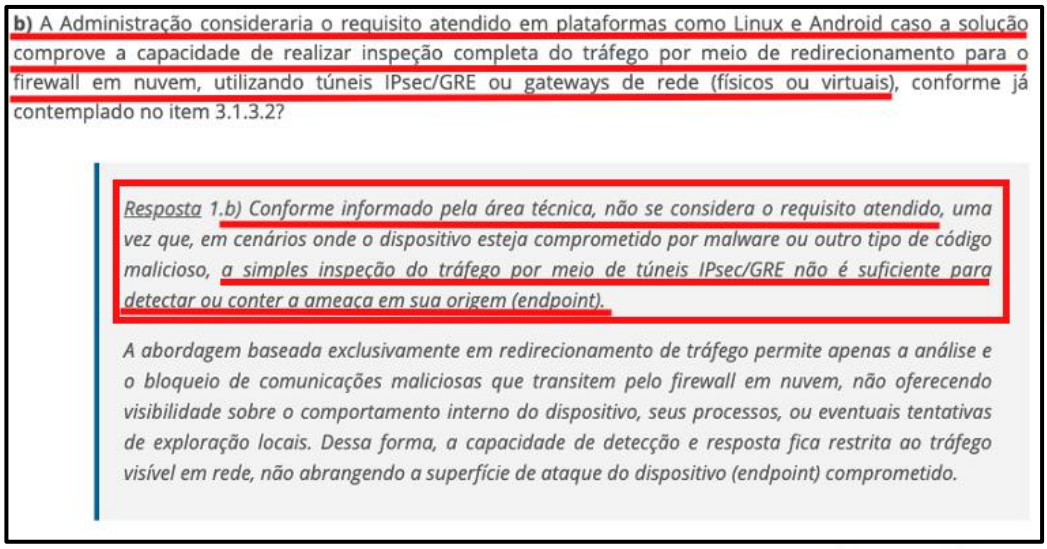
O próprio edital já prevê, em seu subitem 3.1.3.2, a obrigatoriedade de suporte a túneis IPsec de 350 Mbps, e, no item 3.1.3.3, estabelece que toda a inspeção e aplicação de políticas de Firewall deverá ser realizada na nuvem, independentemente do método de implantação. Esses dois requisitos evidenciam que a Administração admite o uso de abordagens agentless, como túneis de rede (IPsec/GRE) ou gateways de acesso seguro, em complemento ou alternativa aos agentes locais.

Adicionalmente, ressaltamos que em plataformas como Linux e Android existe uma grande diversidade de versões de kernel, distribuições e bibliotecas, o que implica em uma necessidade de atualizações frequentes e adaptações constantes dos agentes locais. Esse fator pode comprometer a estabilidade da solução e gerar riscos operacionais, enquanto métodos agentless (como os já previstos no edital) oferecem maior robustez e escalabilidade.

Diante disso, questionamos:

a) O objetivo principal do requisito é garantir a instalação de um agente local em cada sistema operacional listado, ou assegurar que a solução seja capaz de inspecionar e aplicar políticas de segurança a todo o tráfego originado nessas plataformas, conforme previsto no item 3.1.3.3?

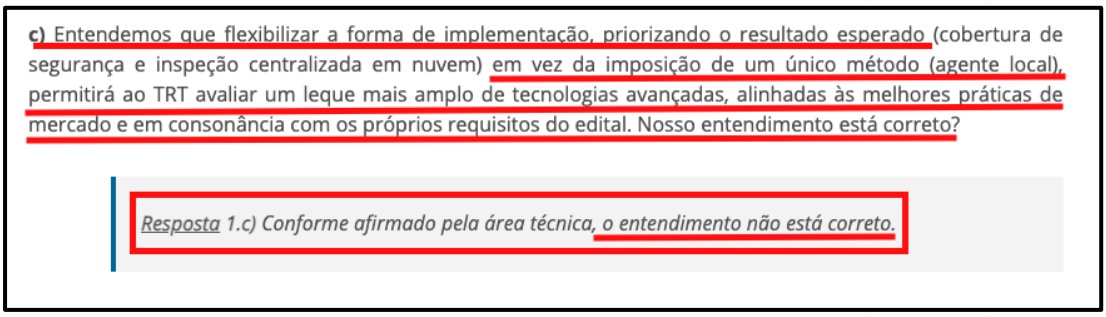
> *Resposta 1.a) Conforme informado pela área técnica, o objetivo do requisito é assegurar que dispositivos com os principais sistemas operacionais do mercado sejam devidamente protegidos pela solução de FWaaS. Essa abrangência é especialmente relevante para acessos realizados por meio de dispositivos móveis, como celulares e notebooks.*
>
> *Nesse contexto, uma solução SASE com cliente instalado (agent-based) possibilita uma análise mais profunda e contextualizada das vulnerabilidades e do comportamento do dispositivo protegido. Em contrapartida, uma solução clientless (sem agente) oferece uma visibilidade mais limitada, uma vez que depende exclusivamente do tráfego que transita por gateways ou do acesso realizado via navegador.*
>
> *Dessa forma, mantém-se a exigência da utilização de agente instalado como requisito essencial para garantir o nível de visibilidade, controle e segurança esperado na proteção dos dispositivos de acesso.*



b) A Administração consideraria o requisito atendido em plataformas como Linux e Android caso a solução comprove a capacidade de realizar inspeção completa do tráfego por meio de redirecionamento para o firewall em nuvem, utilizando túneis IPsec/GRE ou gateways de rede (físicos ou virtuais), conforme já contemplado no item 3.1.3.2?

Resposta 1.b) Conforme informado pela área técnica, não se considera o requisito atendido, uma vez que, em cenários onde o dispositivo esteja comprometido por malware ou outro tipo de código malicioso, a simples inspeção do tráfego por meio de túneis IPsec/GRE não é suficiente para detectar ou conter a ameaça em sua origem (endpoint).

A abordagem baseada exclusivamente em redirecionamento de tráfego permite apenas a análise e o bloqueio de comunicações maliciosas que transitem pelo firewall em nuvem, não oferecendo visibilidade sobre o comportamento interno do dispositivo, seus processos, ou eventuais tentativas de exploração locais. Dessa forma, a capacidade de detecção e resposta fica restrita ao tráfego visível em rede, não abrangendo a superfície de ataque do dispositivo (endpoint) comprometido.



c) Entendemos que flexibilizar a forma de implementação, priorizando o resultado esperado (cobertura de segurança e inspeção centralizada em nuvem) em vez da imposição de um único método (agente local), permitirá ao TRT avaliar um leque mais amplo de tecnologias avançadas, alinhadas às melhores práticas de mercado e em consonância com os próprios requisitos do edital. Nosso entendimento está correto?

Resposta 1.c) Conforme afirmado pela área técnica, o entendimento não está correto.

Da Análise de não atendimento aos itens:

Do Não Atendimento Ao Item 3.1.3.1

Em análise a documentação oficial da Netskope é possível verificar que a solução ofertada, conforme proposta comercial, não atende às especificações e requisitos referentes ao item 3.1.3.1, de maneira que, a funcionalidade de FWaaS não é suportada nos clientes para sistemas operacionais Linux e Android:

Referência:

https://docs.netskope.com/en/netskope-client-supported-os-and-platform

Print:

Linux	• Ubuntu 22.04, 24.04 LTS desktop version • Linux Mint Desktop Versions 21 (Cinnamon Edition) • Red Hat Enterprise Linux version 9.4 (Plow) • Debian 12 (Bookworm)	• Netskope Cloud Firewall (CFW) is not supported on Netskope Client for Linux. • Netskope Private Access (NPA) also supports Ubuntu 24.04. • System reserved domains like .local for Private Apps are not supported on Ubuntu. • Netskope also supports WSLv2(Beta). • Netskope announces end-of-support for Ubuntu 20.04 and Linux Mint versions 19 and 20 by May 31, 2025. To learn more, view End-of-support for Linux versions.

Google	• **Android**
	  • 13 (Tiramisu), 14 (Upside Down Cake), 15(Vanilla Ice Cream), 16 (Baklava)
	• **ChromeOS**
	  • ChromeOS 120 to 142
	  • Android Runtime Version 9, 11
		• Netskope Client does not support ARM32 based Android devices.
		• Cloud Firewall(CFW) is not supported on the Netskope Client for Android devices.
		• Netskope Private Access periodic re-authentication is n supported on Android and Chromebook.

O Efeito Cascata em Decorrência do Não atendimento: Os itens 3.1.3.9, 3.1.3.10, 3.1.3.11, 3.1.3.12, 3.1.3.13, 3.1.3.14 e 3.1.3.15 também deixam de ser atendidos

A consequência lógica da ausência de suporte para Linux e Android é que os itens 3.1.3.9, 3.1.3.10, 3.1.3.11, 3.1.3.12, 3.1.3.13, 3.1.3.14 e 3.1.3.15 também não são serão suportados pela solução ofertada pela licitante recorrida, de maneira que tais itens tratam da funcionalidade de DNS security para o cliente FWaaS, veja-se:

> *"3.1.3.9. **A solução de FWaaS** deverá possuir a capacidade de criar **políticas específicas granulares para proteção de DNS**;*
> *3.1.3.10. **A solução deverá suportar políticas de proteção de DNS** granulares contendo, no mínimo, metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino;*
> *3.1.3.11. **Para a proteção de DNS** a solução deverá permitir ações como bloqueio ou redirecionar para um IP de BOTNETS para página de bloqueio;*

3.1.3.12. ***A solução deverá ter proteção nativa contra ataques de DNS Tunneling*** *que permita bloqueio de destinos maliciosos conhecidos, além de conter mecanismo de detecção de assinaturas de ataques utilizando ferramentas conhecidas de DNS Tunneling como iodine, independente do domínio utilizado;*

3.1.3.13. ***A proteção de DNS deverá permitir bloqueio via DNS,*** *independente do protocolo da aplicação, de domínios com baixa reputação ou com histórico de ser malicioso para Phishing, Conteúdo Malicioso e utilizados para Botnets;*

3.1.3.14. ***A solução deverá detectar e redirecionar requisições de DNS utilizando DOH*** *(DNS over HTTPS), de forma transparente, para aplicação de políticas de DNS, detalhadas nos itens acima, Serão aceitas soluções que bloqueiem o DOH e realizem apliquem as políticas da resolução de DNS tradicional;*

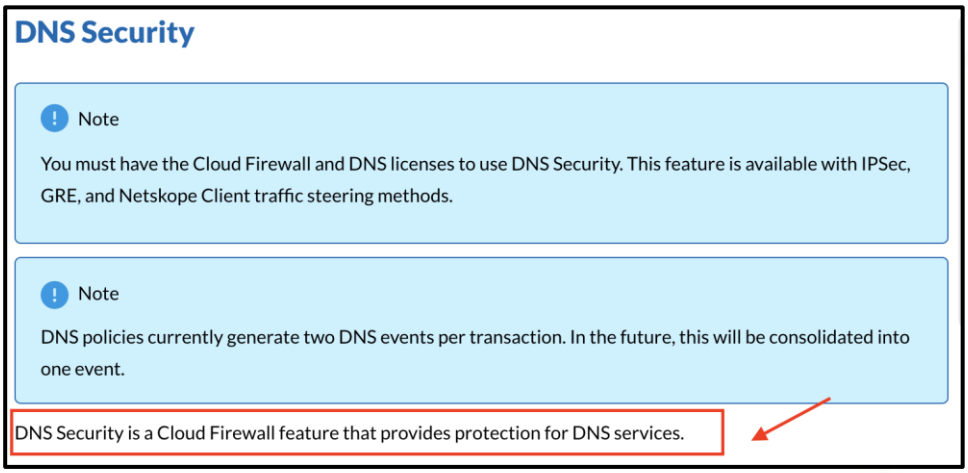
3.1.3.15. ***Assim como todo o escopo do FWaaS, a solução de proteção de DNS deverá suportar a implementação via agentes instalados nos dispositivos dos usuários;****"*

Desta maneira, é evidente que a solução ofertada não atende às especificações referentes a segurança de DNS, principalmente ao **item 3.1.3.15**, de maneira que, tal funcionalidade é uma feature do cliente FWaaS, conforme documentação oficial da própria Netskope, veja-se:

Referência:

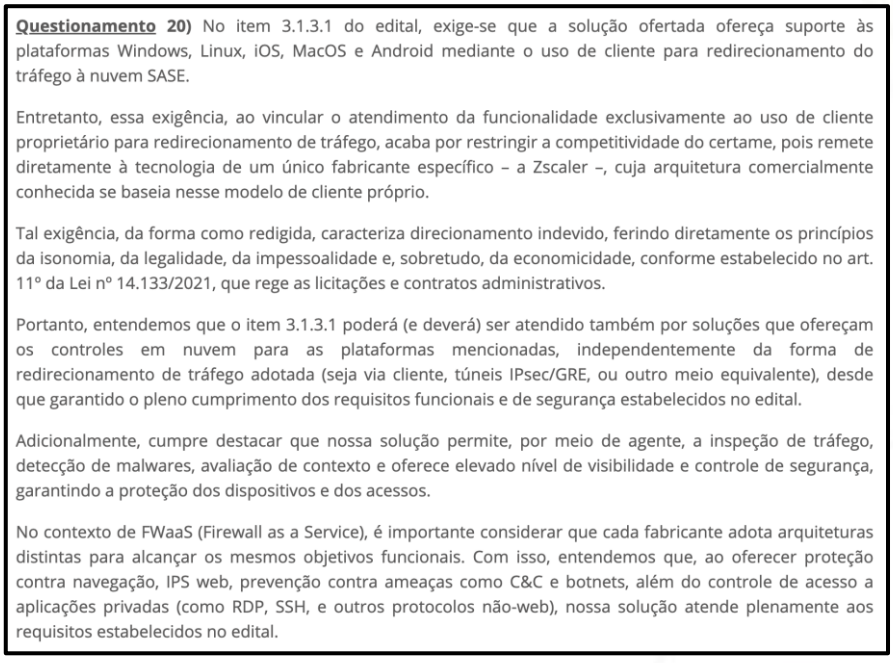
https://docs.netskope.com/en/dns-security

Print:



O Descompasso entre o Permissivo Editalício para Composição de Produtos e a Falta de a Vinculação ao Instrumento Convocatório

O Instrumento convocatório, por meio de resposta ao questionamento nº 20, traz importante item por meio do qual considera que serão aceitas propostas em que se utilize de composição de produtos para atender à exigência da demanda referente aos sistemas operacionais Linux e Android.



Questionamento 20) No item 3.1.3.1 do edital, exige-se que a solução ofertada ofereça suporte às plataformas Windows, Linux, iOS, MacOS e Android mediante o uso de cliente para redirecionamento do tráfego à nuvem SASE.

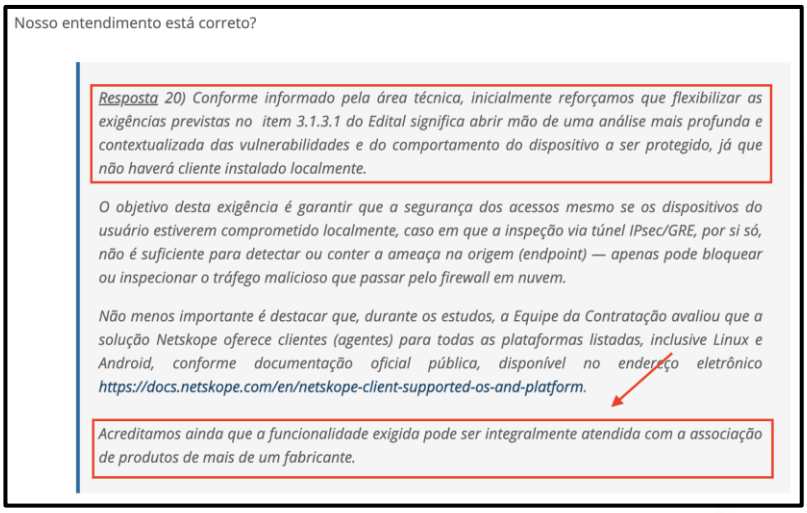
Entretanto, essa exigência, ao vincular o atendimento da funcionalidade exclusivamente ao uso de cliente proprietário para redirecionamento de tráfego, acaba por restringir a competitividade do certame, pois remete diretamente à tecnologia de um único fabricante específico – a Zscaler –, cuja arquitetura comercialmente conhecida se baseia nesse modelo de cliente próprio.

Tal exigência, da forma como redigida, caracteriza direcionamento indevido, ferindo diretamente os princípios da isonomia, da legalidade, da impessoalidade e, sobretudo, da economicidade, conforme estabelecido no art. 11º da Lei nº 14.133/2021, que rege as licitações e contratos administrativos.

Portanto, entendemos que o item 3.1.3.1 poderá (e deverá) ser atendido também por soluções que ofereçam os controles em nuvem para as plataformas mencionadas, independentemente da forma de redirecionamento de tráfego adotada (seja via cliente, túneis IPsec/GRE, ou outro meio equivalente), desde que garantido o pleno cumprimento dos requisitos funcionais e de segurança estabelecidos no edital.

Adicionalmente, cumpre destacar que nossa solução permite, por meio de agente, a inspeção de tráfego, detecção de malwares, avaliação de contexto e oferece elevado nível de visibilidade e controle de segurança, garantindo a proteção dos dispositivos e dos acessos.

No contexto de FWaaS (Firewall as a Service), é importante considerar que cada fabricante adota arquiteturas distintas para alcançar os mesmos objetivos funcionais. Com isso, entendemos que, ao oferecer proteção contra navegação, IPS web, prevenção contra ameaças como C&C e botnets, além do controle de acesso a aplicações privadas (como RDP, SSH, e outros protocolos não-web), nossa solução atende plenamente aos requisitos estabelecidos no edital.



Nosso entendimento está correto?

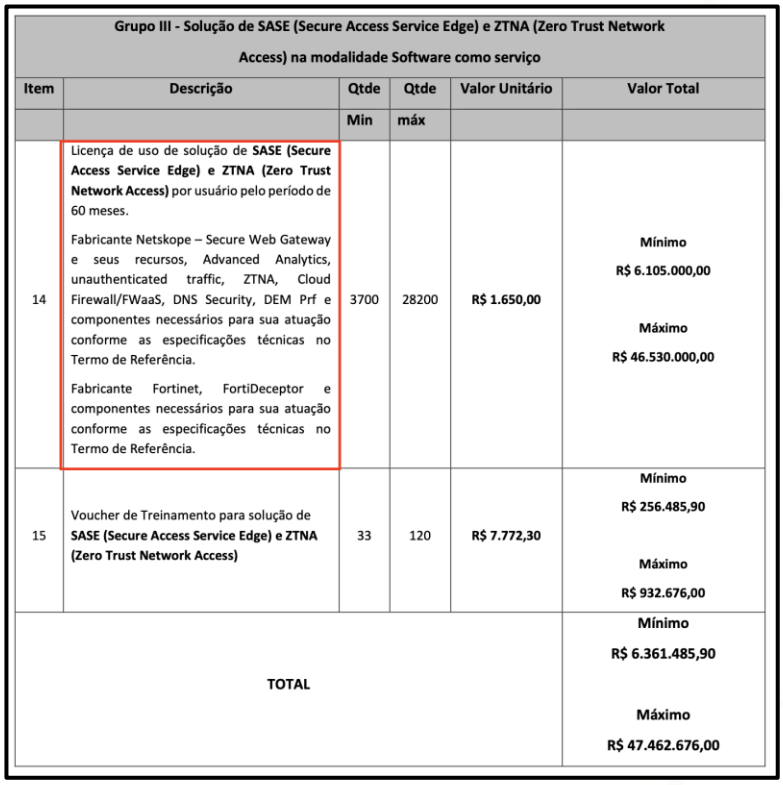
Resposta 20) Conforme informado pela área técnica, inicialmente reforçamos que flexibilizar as exigências previstas no item 3.1.3.1 do Edital significa abrir mão de uma análise mais profunda e contextualizada das vulnerabilidades e do comportamento do dispositivo a ser protegido, já que não haverá cliente instalado localmente.

O objetivo desta exigência é garantir que a segurança dos acessos mesmo se os dispositivos do usuário estiverem comprometido localmente, caso em que a inspeção via túnel IPsec/GRE, por si só, não é suficiente para detectar ou conter a ameaça na origem (endpoint) — apenas pode bloquear ou inspecionar o tráfego malicioso que passar pelo firewall em nuvem.

Não menos importante é destacar que, durante os estudos, a Equipe da Contratação avaliou que a solução Netskope oferece clientes (agentes) para todas as plataformas listadas, inclusive Linux e Android, conforme documentação oficial pública, disponível no endereço eletrônico https://docs.netskope.com/en/netskope-client-supported-os-and-platform.

Acreditamos ainda que a funcionalidade exigida pode ser integralmente atendida com a associação de produtos de mais de um fabricante.

Contudo, ainda que, com a possibilidade de compor a solução para o pleno atendimento dos itens, a Recorrida não declara qualquer produto em composição com Netskope para o pleno atendimento dos itens, veja-se:



Grupo III - Solução de SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access) na modalidade Software como serviço					
Item	**Descrição**	**Qtde Min**	**Qtde máx**	**Valor Unitário**	**Valor Total**
14	Licença de uso de solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)** por usuário pelo período de 60 meses. Fabricante Netskope – Secure Web Gateway e seus recursos, Advanced Analytics, unauthenticated traffic, ZTNA, Cloud Firewall/FWaaS, DNS Security, DEM Prf e componentes necessários para sua atuação conforme as especificações técnicas no Termo de Referência. Fabricante Fortinet, FortiDeceptor e componentes necessários para sua atuação conforme as especificações técnicas no Termo de Referência.	3700	28200	**R$ 1.650,00**	**Mínimo** **R$ 6.105.000,00** **Máximo** **R$ 46.530.000,00**
15	Voucher de Treinamento para solução de **SASE (Secure Access Service Edge) e ZTNA (Zero Trust Network Access)**	33	120	**R$ 7.772,30**	**Mínimo** **R$ 256.485,90** **Máximo** **R$ 932.676,00**
TOTAL					**Mínimo** **R$ 6.361.485,90** **Máximo** **R$ 47.462.676,00**

. Em outras palavras: existe o permissivo no Edital de que a solução poderia ser composta pela associação de produtos para se atingir o objetivo final que é garantir o

nível de visibilidade, controle e segurança esperado na proteção dos dispositivos de acesso.

. Apesar disso, a Recorrida não consignou em sua proposta qualquer produto associado. Assim, como a solução ofertada, por si só, não atende à exigência editalícia, a Recorrida deveria se socorrer da composição de produtos, mas não o fez, operando-se a preclusão lógica em relação à proposta apresentada, devendo ser desclassificada pelo não atendimento à exigência do Termo de Referência e reforçada por ocasião da resposta ao questionamento.

. Assim, resta evidenciado que a solução não atende às determinações do termo de referência. Apesar dos esclarecimentos do TRT-12 em relação à importância da instalação do agente nos dispositivos dos usuários, não apenas em versões de Sistemas operacionais Windows, Mac e IOS, mas também em sistemas operacionais Linux e Android, de acordo com as versões definidas no termo de referência. Contudo, a Licitante Recorrida não atende aos itens 3.1.3.1, 3.1.3.9, 3.1.3.10, 3.1.3.11, 3.1.3.12, 3.1.3.13, 3.1.3.14 e 3.1.3.15, principalmente aos itens 3.1.3.1 e 3.1.3.15, que deixa evidente, sem qualquer dúvida a necessidade de ter as funcionalidades de FWaaS e DNS Security instaladas em seu pleno funcionamento em soluções Linux e Android, o que não é suportado, conforme evidências anexas neste documento.

. Admitir a manutenção da Recorrida no presente certame, além de violar preceitos constitucionais de isonomia e vinculação ao instrumento convocatório, expõe o sistema do TRT12 a riscos que podem, eventualmente, levar a uma responsabilização tanto da licitante quanto do gestor já que alertado da incompatibilidade da solução com as pretensões da Administração Pública.

Do Não Atendimento Ao Item 3.1.1.25

No termo de referência a especificação do item 3.1.1 define as características gerais da solução ofertada, neste sentido, o item 3.1.1.14 é muito claro ao determinar que **toda a solução e funcionalidades devem ser ofertadas em nuvem**, veja-se:

> "3.1.1.14. **Todas as funcionalidades deverão ser ofertadas em nuvem**, como serviço e por meio de um único agente instalado na máquina do usuário. A nuvem deverá ser distribuída globalmente, incluindo o Brasil e deverá ser licenciada por usuário, conforme quantitativo definido por cada participante;"

Contudo, ao analisar a documentação apresentada pela licitante recorrida, evidencia-se que a solução ofertada para o atendimento ao requisito do item 3.1.1.25 não atende às especificações de características gerais da solução, de maneira que, o item determina que a solução deve suportar a autenticação de usuários baseada em integrações com o Active Directory, utilizando os protocolos SAML e LDAP via OpenLDAP, veja-se:

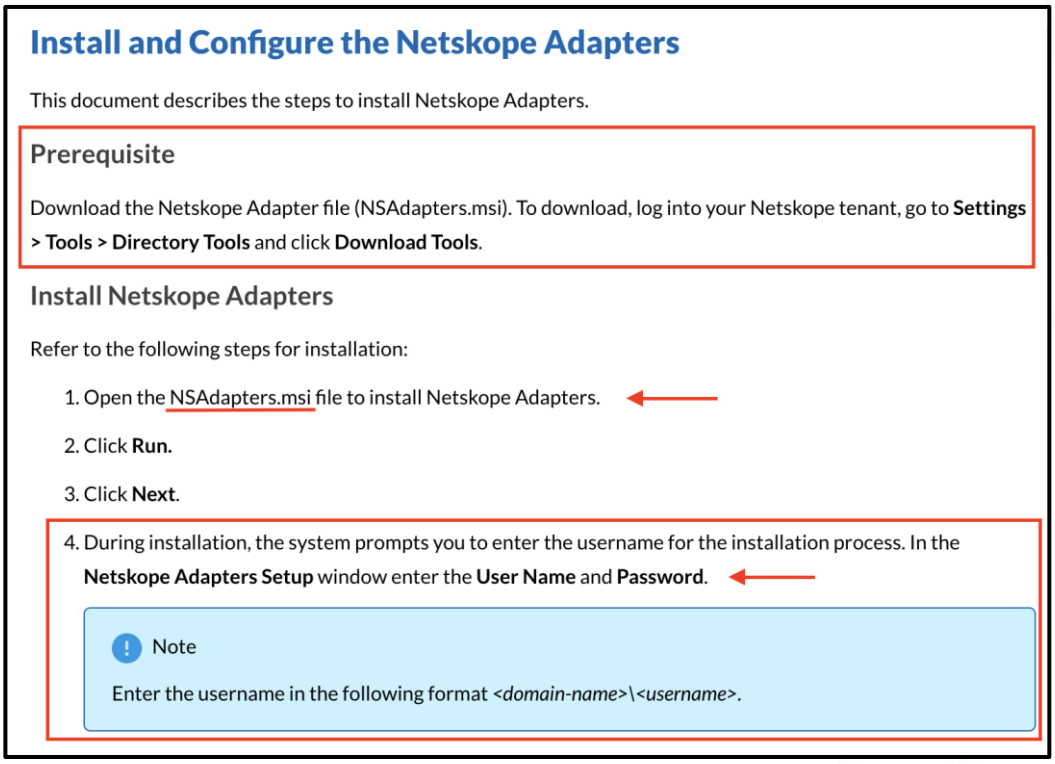
> "3.1.1.25**. Toda a solução proposta deverá ser implementada com autenticação dos usuários** integrada e suportar aplicações de políticas granulares com base em nome do usuário, e grupos**, integrados com a plataforma Microsoft AD utilizando protocolo SAML (Security Assertion Markup Language) e LDAP via OpenLDAP;**"

Deste modo, analisando a solução ofertada, a licitante recorrida apresenta uma abordagem onde há a necessidade de instalação de um agente .msi on-premisses em um dispositivo baseado em Windows Server, veja-se:

Referência:

https://docs.netskope.com/en/install-and-configure-the-netskope-adapters

Print:



Install and Configure the Netskope Adapters

This document describes the steps to install Netskope Adapters.

Prerequisite

Download the Netskope Adapter file (NSAdapters.msi). To download, log into your Netskope tenant, go to **Settings > Tools > Directory Tools** and click **Download Tools**.

Install Netskope Adapters

Refer to the following steps for installation:

1. Open the NSAdapters.msi file to install Netskope Adapters.
2. Click **Run.**
3. Click **Next**.
4. During installation, the system prompts you to enter the username for the installation process. In the **Netskope Adapters Setup** window enter the **User Name** and **Password**.

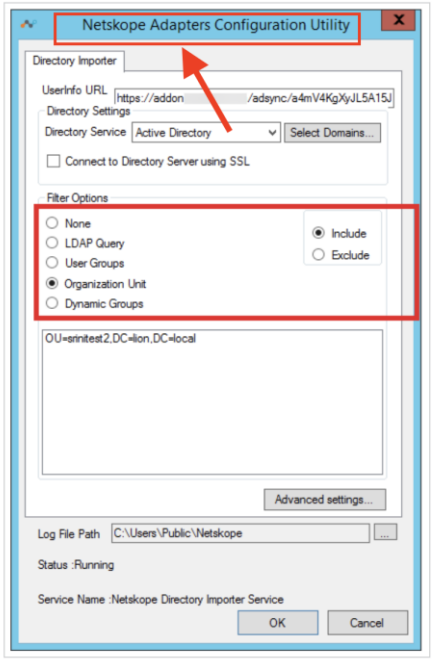
> Note
>
> Enter the username in the following format *<domain-name>\<username>*.

Referência:

https://docs.netskope.com/en/configure-directory-importer

Print:

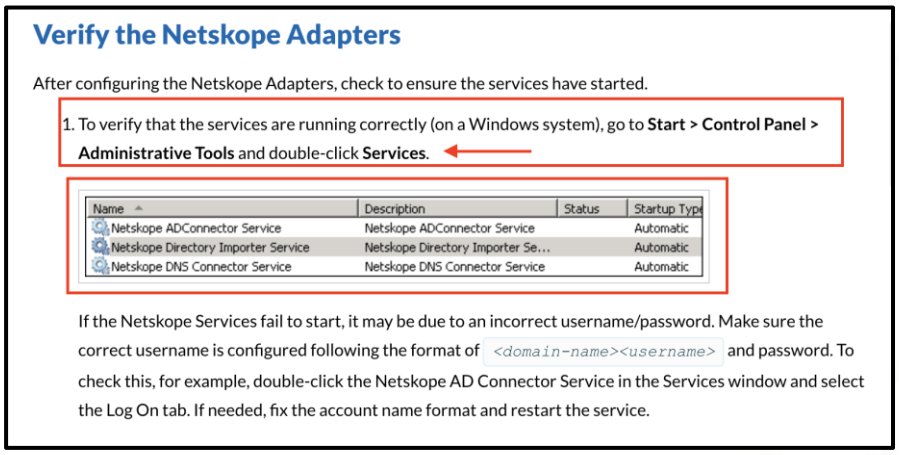
When the Netskope Adapters open, the first tab displayed is for Directory Importer.



Referência:

https://docs.netskope.com/en/verify-the-netskope-adapters

Print:



A documentação apresentada claramente demonstra que o uso da plataforma Microsoft Windows para o funcionamento do componente é mandatório e indispensável, o que por si só, pode impactar o TRT-12, gerando custos adicionais com licença de software Microsoft Windows, sem contar com os recursos computacionais e de rede que, necessariamente, seriam alocados.

Resta evidenciado que o componente Directory Services consiste em um software instalado on-premises, sob a plataforma Microsoft Windows e que a configuração da opção “Other Directory Services” não assegura o suporte e compatibilidade, de forma oficial, pelo fabricante Netskope para o uso do sistema LDAP via OpenLDAP.

Frisamos que, conforme informado por este exímio Tribunal, em fase de diligência, o TRT-12 utiliza o sistema LDAP via OpenLDAP como forma de gestão de identidades e a ausência dessa integração inviabilizaria o uso do produto em seu ambiente.

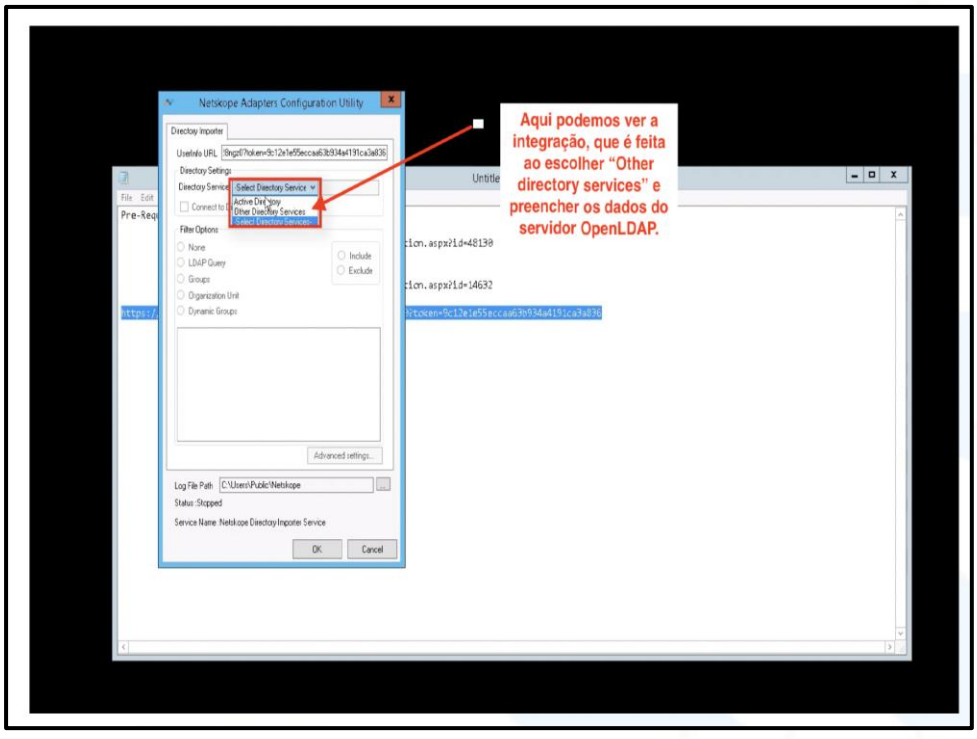
Em análise a documentação apresentada pela licitante recorrida, durante a fase de pregão a Recorrida referenciou o sítio oficial do fabricante: https://www.netskope.com/wp-content/uploads/2024/05/2025-03-Netskope-Client-DS-509-11.pdf.

Durante a fase de diligência a Recorrida apresentou documentação para comprovação da conformidade deste requisito técnico, através do documento “INFORMACOES DILIGENCIA.pdf”. Deste documento foi informado que a

conformidade com o requisito ocorre através do uso de um componente chamado "Directory Importer". No sítio oficial do fabricante: "https://docs.netskope.com/en/install-and-configure-the-netskope-adapters", constam informações básicas sobre esse componente, após vasta pesquisa não encontramos uma documentação pública detalhada.

Atentemos que a Recorrida não apresentou nenhuma documentação, vídeo ou captura de tela que conste referência ao suporte e integração com o serviço de diretórios LDAP via OpenLDAP. Além disso, não apresenta documentação que informa quais são os recursos de infraestrutura computacional e de rede necessários, nem mesmo, os requisitos mínimos de compatibilidade para uso do componente Directory Importer, nas dependências do datacenter local no TRT-12.

Ademais, em relação a documentação comprobatória, a Recorrida afirma, sem apresentar qualquer informação ou documentação que confirme tal alegação, que esse componente possui o suporte ao OpenLDAP através do uso da opção "Other directory services", conforme captura de tela extraída do documento de resposta da diligência "INFORMACOES DILIGENCIA.pdf".



A Recorrida induz a equipe técnica ao erro ao afirmar que o uso da opção de seu conector de diretórios (“Directory Importer”) com o uso da opção “Other directory services” possui suporte e é integrado ao OpenLDAP. Além disso, omite detalhes sobre o componente Directory Importer, o qual consiste em um software instalado on-premises, ou seja, que será instalado utilizando recursos da infraestrutura do Tribunal, conforma já evidenciado.

É importante ressaltar que objeto desta aquisição é uma solução de SASE (Secure Access Service Edge), e conforme é exigido no requisito técnico do item 3.1.1.14, **todas as funcionalidades deverão ser ofertadas em nuvem como serviço**, como já devidamente apresentado pela Recorrente.

A utilização de um componente para integração com o serviço de diretório em uso no TRT12, que é primordial e crucial para o correto funcionamento da solução SASE, na modalidade on-premises é uma total e completa afronta ao objeto desta contratação.

Da análise conclui-se que os requisitos técnicos exigem de forma clara que a solução SASE ofertada possua todas as suas funcionalidades como serviço em nuvem e que toda a solução proposta seja implementada com autenticação integrada e suportada com a plataforma LDAP via OpenLDAP.

Buscamos trazer a luz da equipe técnica deste exímio Tribunal, de forma bastante clara e transparente, que o fabricante Netskope, por meio do componente Directory Importer, não suporta a integração nativa e de forma oficial com serviços de diretório OpenLDAP.

Nos sentimos no dever de alertar dos riscos inerentes a não viabilidade técnica na integração com o serviço de gestão de identidades OpenLDAP em uso no Tribunal, e consequentemente a inviabilidade do uso da solução ofertada neste e em demais Tribunais participes desta contratação.

Desta forma, resta evidente e clara a não conformidade com o requisito técnico do item 3.1.1.25. Ademais, como demostrado a não conformidade da solução, quando analisado demais requisitos técnicos com o do item 3.1.1.14.

Do Não Atendimento Ao Item 3.1.3.10

O item 3.1.3.10 visa garantir que a solução ofertada suporta a criação de políticas de proteção de DNS granulares contendo, no mínimo, metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino.

> *"3.1.3.10. A solução deverá suportar políticas de proteção de DNS granulares contendo, no mínimo, metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino;"*

Durante a fase de pregão a Recorrida apresentou documentação para comprovação da conformidade deste requisito técnico, através dos sítios do fabricante: https://docs.netskope.com/en/dns-security e https://docs.netskope.com/en/inline-policies. Também apresentou o documento "DT-TRT12-Anexo Suplementar.pdf" com captura de telas para comprovar a conformidade deste requisito técnico.

Perceba que o Edital é cristalino quanto aos requisitos da solução, sendo necessário que as empresas licitantes comprovassem o suporte a políticas de proteção de DNS granulares contendo metadados do IdP.

Importante frisar que a solução de IdP (Identity Provider) ou provedor de identidade, que conforme informado em sede de diligência pelo TRT12, de acordo com o documento 092 – "092 - DOCUMENTO - Manifestação infra - Avaliação Grupo 3 - Empresa SOOW após 1ª diligência.pdf", utiliza o OpenLDAP:

> *"O TRT12 usa o sistema OpenLDAP como forma de gestão de identidades e a ausência dessa integração inviabiliza o uso do produto proposto."*

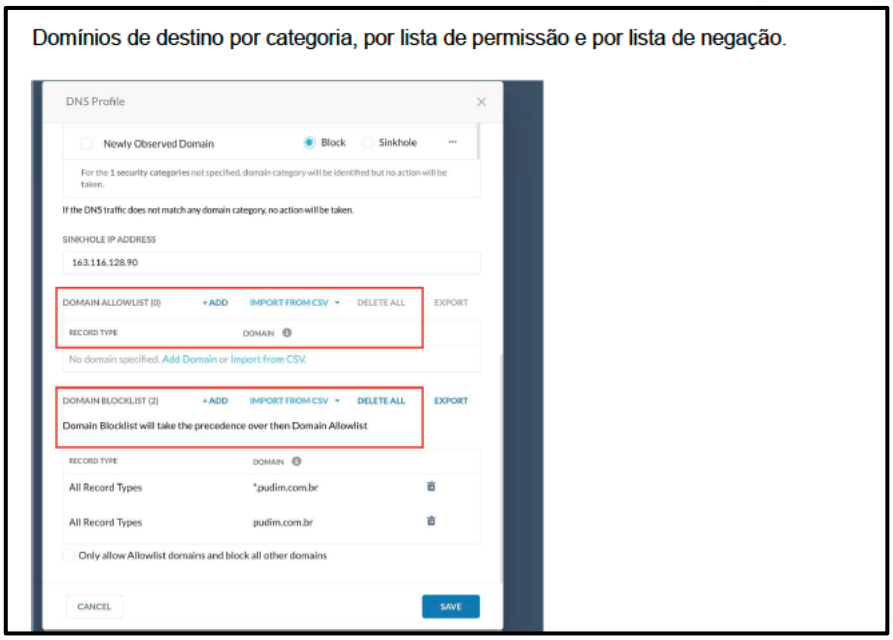
E conforme já esclarecido e devidamente evidenciado pela Recorrente, a solução ofertada pela Recorrida não possui conformidade técnica com o requisito do item 3.1.1.25 para com o serviço de gestão de identidades OpenLDAP.

O item 3.1.1.25 informa que o *import* dos atributos deve ser feito via **OpenLDAP,** no caso do TRT12.

Voltando agora ao requisito técnico original em questão do item 3.1.3.10,

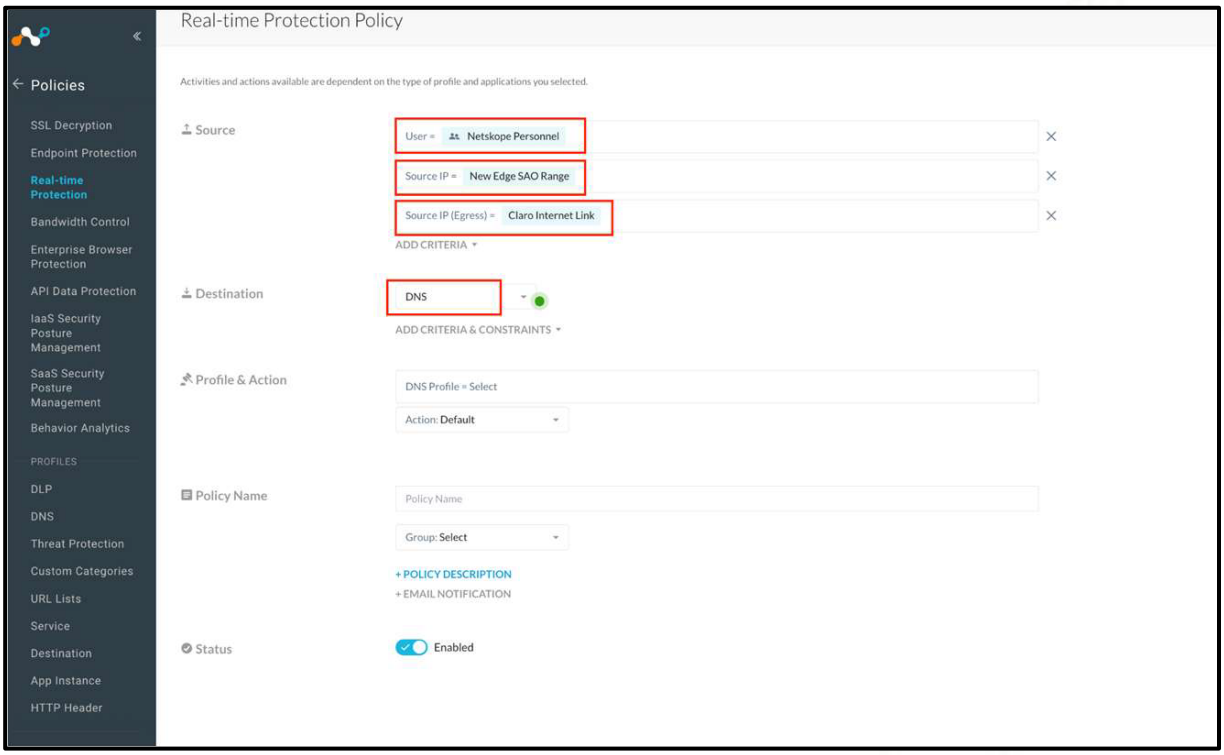
entende-se claramente que a feature de proteção a DNS da solução deve suportar a criação de políticas granulares com, pelo menos, os seguintes parâmetros: “metadados do IdP (usuário, grupos e departamento), Localidades, Origem e Domínios Destino.

No documento apresentado “DT-TRT12-Anexo Suplementar.pdf”, a SIGMA indicou ter a capacidade de criação de “Política com Metadados do IDP, proteção DNS, localidade de origem, localidade de destino”, abordaremos esse tópico adiante, em específico para o metadado de “departamento”, e seguiu para o tópico "Domínios de destino por categoria, por lista de permissão e por lista de negação.", com a seguinte afirmação e captura de tela:



Como pode ser observado, claramente a solução não atende ao requisito técnico deste item, devido a seguinte afirmação presente na própria captura de tela do produto apresentada pela Recorrida: *“If the DNS Traffic does not match any domain category, no action will be taken”*. Traduzindo para a língua portuguesa: *“Se o tráfego DNS não corresponder a nenhuma categoria de domínio, nenhuma ação será tomada”*. Como o propósito do requisito técnico é proporcionar a criação de políticas com base no destino, independente da categorização deste Destino, inclusive este foi o método (Categorização de Destino) o qual a Recorrida utilizou para induzir a equipe técnica do tribunal ao erro de interpretação da conformidade, **a comprovação se mostra, mais uma vez, incoerente e fora de conformidade com o requisito técnico.**

Retornando a criação de políticas, curiosamente, a Recorrida não apresentou em sua documentação, a possibilidade de utilização do metadados do IdP (usuário, grupos e departamento), no que tange aos metadados de “grupo” e “departamento”, conforme evidencia-se na captura de tela apresentada, da qual consta somente o metadado de Usuário (User) e outros não solicitados no requisito técnico:



Juntando-se o requisito técnico em questão com o item 3.1.1.25, principalmente considerando, conforme já abordado, que a comprovação considera a integração com o OpenLDAP, conforme solicitado no edital, fica clara a total não conformidade técnica da solução ofertada.

Observe que este é cristalino ao informar os requisitos mínimos e documentação que deveriam ser apresentadas pelas empresas licitantes, porém, a Recorrente, de forma desidiosa, participou da licitação sabendo sobre as condições de participação e, mesmo assim, não apresentou solução compatível, fato este que reforça a necessidade urgente de revisão da decisão da equipe técnica e do Ilmo. Pregoeiro no aceite da proposta ofertada pela licitante SIGMA.

Do não atendimento do item 3.1.1.29

O item 3.1.1.29 do Anexo I – Especificações Técnicas para a Solução, deixa explicito que a solução **deve** fornecer visibilidade em tempo real para a visualisação de logs, veja-se:

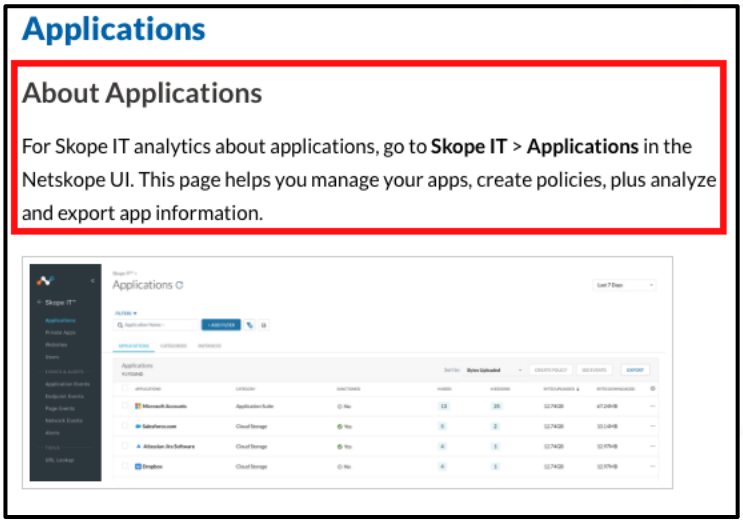
> *"3.1.1.29. A solução deve ser capaz de fornecer a visualização de logs em tempo real;"*

Contudo, mais uma vez a licitante Recorrida tenta induzir o TRT-12 ao erro, ao não comprovar claramente o suporte ao requisito, de maneira que, ao analisar a documentação comprobatória, não há qualquer mensão a visualização de logs em tempo real, mas sim uma explicação que a solução de logs permita a visualizaçao de logs gerados pela engine de proteção em tempo real, veja-se:

Links de comprovação:

https://docs.netskope.com/en/about-applications

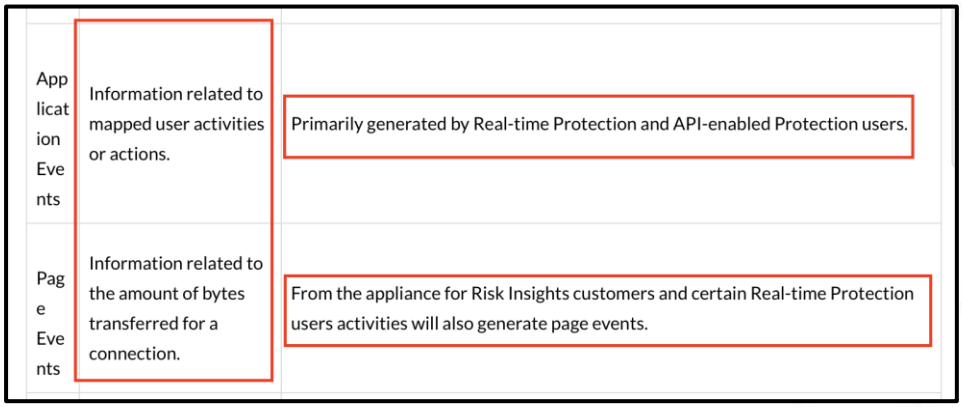
Print:



Links de comprovação:

https://docs.netskope.com/en/about-events

Print:



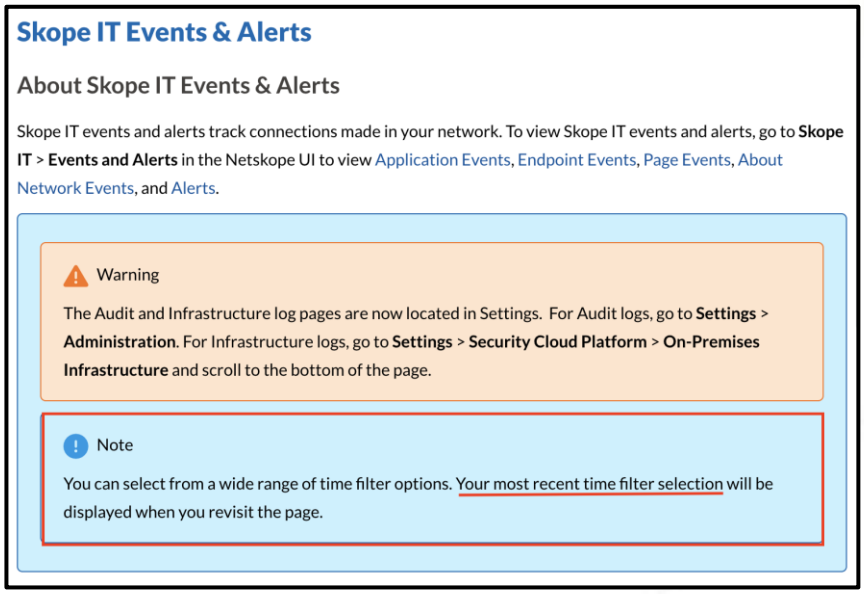
Application Events	Information related to mapped user activities or actions.	Primarily generated by Real-time Protection and API-enabled Protection users.
Page Events	Information related to the amount of bytes transferred for a connection.	From the appliance for Risk Insights customers and certain Real-time Protection users activities will also generate page events.

A documentação comprobatória, apresentado pela licitante Recorrida apenas demonstra que o recurso na solução que permite a visualização de logs é via “Skope IT”, contudo, mais uma vez, na mesma documentação verifica-se que, a solução em questão, oferece apena um range de tempo pré-determinado, e o administrador da solução pode filtrar pelo tempo mais recente, veja-se:

Links de comprovação:

https://docs.netskope.com/en/about-events

Print:



Skope IT Events & Alerts

About Skope IT Events & Alerts

Skope IT events and alerts track connections made in your network. To view Skope IT events and alerts, go to **Skope IT** > **Events and Alerts** in the Netskope UI to view Application Events, Endpoint Events, Page Events, About Network Events, and Alerts.

Warning

The Audit and Infrastructure log pages are now located in Settings. For Audit logs, go to **Settings** > **Administration**. For Infrastructure logs, go to **Settings** > **Security Cloud Platform** > **On-Premises Infrastructure** and scroll to the bottom of the page.

Note

You can select from a wide range of time filter options. Your most recent time filter selection will be displayed when you revisit the page.

Desta maneira, resta evidenciado, mais uma vez, que a solução ofertada pela licitante Recorrida, não está em conformidade com os requisitos técnicos do Edital, o que pode causar imenso prejuízo ao Erário.

Do não atendimento do item 3.1.2.3

Conforme determina o item, a solução deve identificar portas fora do padrão HTTP/HTTPS, além de realizar a inspeção em profunda em tráfegos criptografados SSL/TLS, ou seja, a solução deve realizar a inspeção do tráfego SSL/TLS, veja-se:

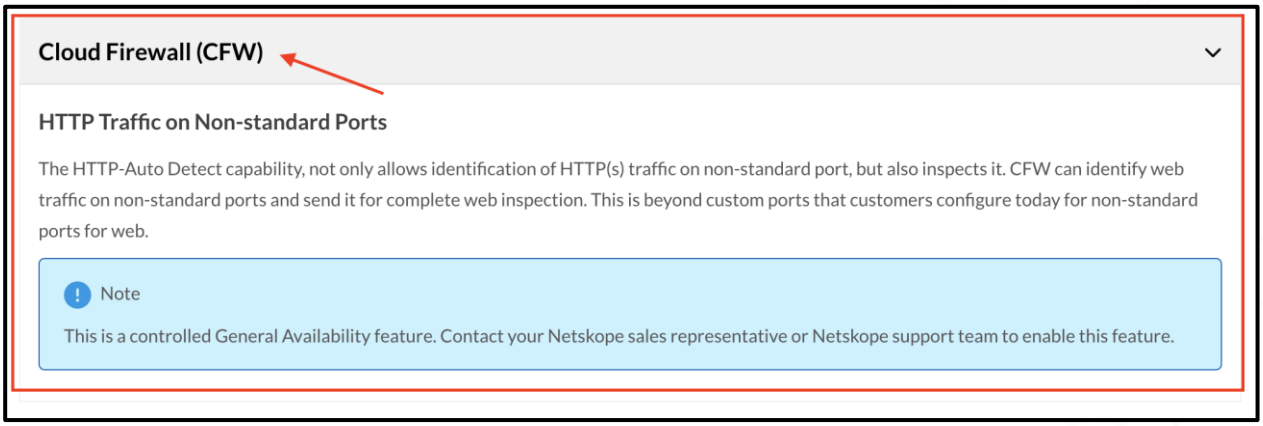
> "3.1.2.3. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção Web completa, incluindo inspeção SSL/TLS e todas as funcionalidades de controle de acesso e segurança, mesmo em uma arquitetura de proxy transparente;"

Contudo, a documentação do fabricante Netskope, mais uma vez, explicita a limitação da solução, uma vez que a solução de HTTP on Non-Standart Traffic não é suportada para sistemas operacionais Linux e Android, veja-se:

Referência:

https://docs.netskope.com/en/netskope-release-notes-version-117-0-0

Print:



A documentação oficial da Netskope deixa claro que o HTTP Traffic on Non-standard Ports é uma feature referente a solução Cloud Firewall (CFW), desta maneira, para que a solução realize a identificação e, consequentemente, a inspeção do tráfego SSL/TLS em portas fora do padrão, a solução Cloud Firewall (CFW) deve estar habilitada, porém, em consonância com o esclarecimento prestado neste mesmo recurso, conforme determina o item 3.1.3.1, veja-se:

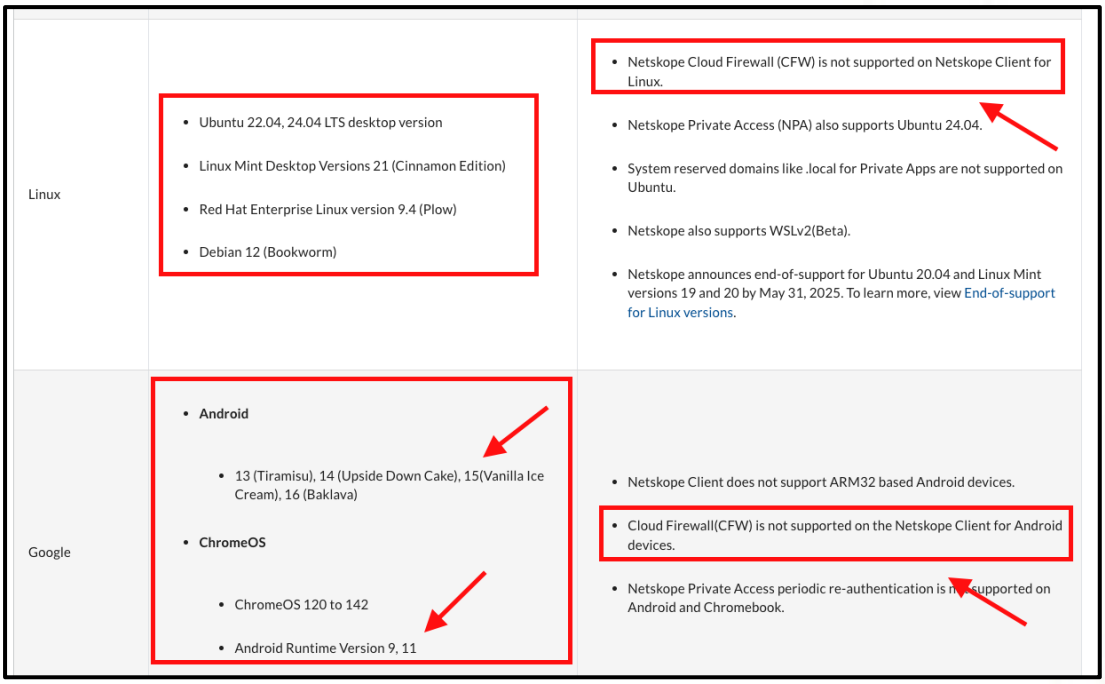
"3.1.3.1. A solução deverá suportar capacidades de Firewall como serviço ***via agentes instalados nas máquinas dos usuários*** *nas plataformas Windows,* ***Linux****, IOS, MacOS e* ***Android****;"*

Contudo, houve a demonstração que a solução ofertada pela Netskope não atende ao requisito em questão, de maneira que, a solução Cloud Firewall (CFW) não oferece suporte aos sistemas operacionais Linux e Android, veja-se:

Referência:

https://docs.netskope.com/en/netskope-client-supported-os-and-platform

Print:



Portanto, mais uma vez, evidencia-se a fragilidade da solução e o não atendimento a diversos itens críticos para o seu pleno funcionamento, ademais, fica clara a criticidade do não atendimento ao item 3.1.3.1, de maneira que impacta, mais uma vez, de maneira imensurável em prejuízo ao Erário. Outro ponto que se deve considerar, ante aos pontos desqualificadores da proposta da licitante Recorrida, é o Art. 59, alínea II, da lei 14.133/2021 - https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm:

"(...) **Art. 59. Serão desclassificadas as propostas que:**
I - contiverem vícios insanáveis;

II - não obedecerem às especificações técnicas pormenorizadas no edital;(...)"

Desta maneira, a solução proposta pela Recorrida não deve ser aceita pelo Tribunal Regional do Trabalho da 12ª Região, de maneira que não obedeça às especificações técnicas editalícias.

Do não atendimento do item 3.1.1.31.

O item 3.1.1.31 determina que a solução deve, minimamente, oferecer a capacidade de detectar, em logs de auditória, qual foi a origem da ação executada por qualquer administrador da solução, veja-se:

> *"**3.1.1.31. Os logs de auditoria devem conter no mínimo:***
> *a) Ação: Login, Criação, Deleção;*
> ***b) Interface utilizada: API, Console Administrativa, e;***
> *c) Categoria: Gerenciamento, Controle de Acesso, Gerenciamento de funções, Controle de acesso Web, Segurança Web e configurações avançadas."*

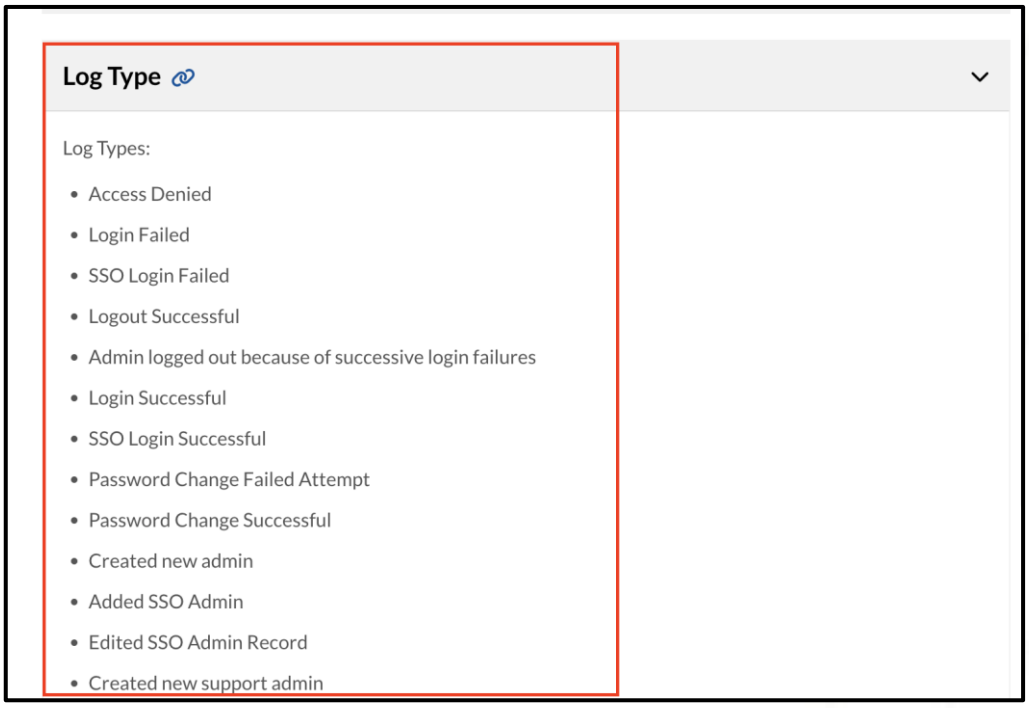
Desta maneira, a solução deve minimamente entregar, informações conforme o requisito determina, neste sentido, fica explicito que tais funcionalidades são capacidades indispensáveis e, para a aceitabilidade da solução, estas são capacidades é o mínimo que a solução deve suportar. O fato de o termo de referência definir que este é o mínimo esperado, nada menos que isso será aceito.

Desta maneira, analisando a documentação de comprovação do item, verifica-se que não há qualquer informação que comprove que, nos logs de auditória, as informações da plataforma de origem das ações realizadas na solução, se as ações foram realizadas por meio de API ou por meio da console, veja-se:

Referência:

https://docs.netskope.com/en/audit-log-1

Print:



A documentação comprobatória, utilizada no processo de habilitação técnica pela licitante Recorrida, não tem qualquer informação que valide a capacidade referente a origem das ações tomadas, sejam estas por meio de console ou API Gateway, deste modo, a solução ofertada não atende à especificação referente ao item 3.1.1.31.

Do não atendimento do item 3.1.1.31.

O item 3.1.7.9, é claro ao determinar que a solução referente a Deception, deve possuir, no mínimo, a capacidade de manipular e criar iscas no Active Directory, tais tipos de iscas são importantes e indispensáveis, considerando que tal funcionalidade visa garantir a integridade do diretório de domínios do TRT-12, veja-se:

> "3.1.7.9. Possuir, **pelo menos**, os seguintes tipos de Iscas/Chamarizes:
>
> a) Iscas de Rede: Espalhadas em segmentos de rede específicos;
>
> **b) Iscas no Active Directory: Criação de usuário e computadores falsos, e;**

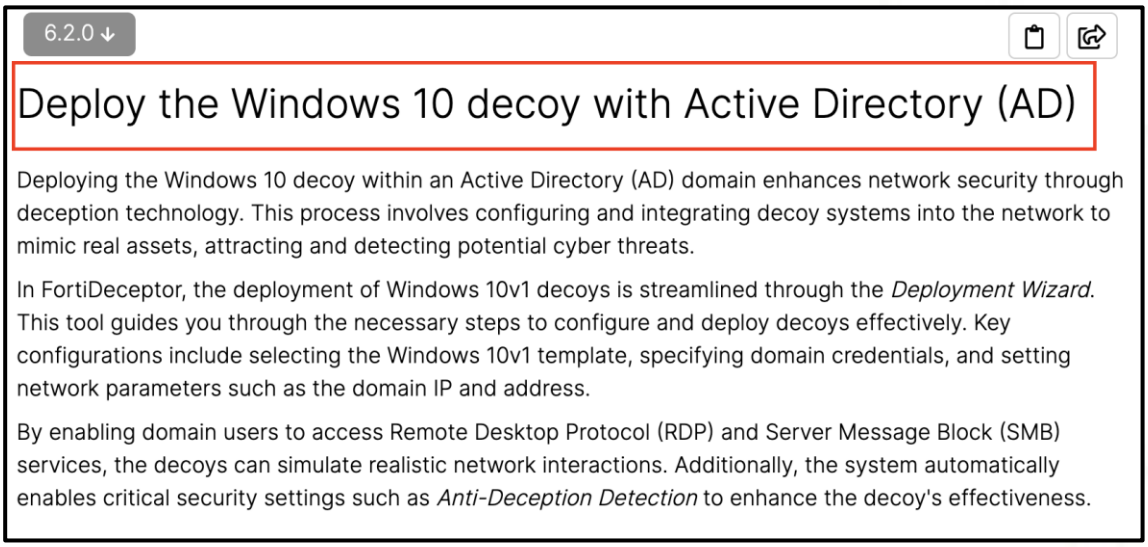
c) Iscas nos Endpoints: Criação de arquivos, aplicações e credenciais falsas.”

Contudo, mais uma vez, a documentação apresentada pela licitante Recorrida, não tem qualquer informação que se refere a criação de iscas/decoys no Active Directory, ainda que o TRT-12 seja muito claro ao determinar que a solução deve **pelo menos**, suportar tal funcionalidade, desta maneira, não será aceita soluções que entreguem menos que isso, vejamos a documentação oficial da Fortinet, em relação ao Fortideceptor:

Referência:

https://docs.fortinet.com/document/fortideceptor/6.2.0/administration-guide/619085/deploy-the-windows-10-decoy-with-active-directory-ad

Print:


6.2.0

Deploy the Windows 10 decoy with Active Directory (AD)

Deploying the Windows 10 decoy within an Active Directory (AD) domain enhances network security through deception technology. This process involves configuring and integrating decoy systems into the network to mimic real assets, attracting and detecting potential cyber threats.

In FortiDeceptor, the deployment of Windows 10v1 decoys is streamlined through the *Deployment Wizard*. This tool guides you through the necessary steps to configure and deploy decoys effectively. Key configurations include selecting the Windows 10v1 template, specifying domain credentials, and setting network parameters such as the domain IP and address.

By enabling domain users to access Remote Desktop Protocol (RDP) and Server Message Block (SMB) services, the decoys can simulate realistic network interactions. Additionally, the system automatically enables critical security settings such as *Anti-Deception Detection* to enhance the decoy's effectiveness.

A única documentação oficial que faz referências ao Active Directory, é a possibilidade de utilizar a base local para criação de usuários fictícios em um ambiente controlado de Decoys, contudo, não há a capacidade da criação de iscas/decoys no Active Directory. Desta maneira, o item não é suportado pela solução proposta.

Do não atendimento ao item 3.1.7.17:

Conforme a determinação do item 3.1.7.17, a solução deve permitir que a solução possibilite a filtragem de eventos de decoys, conforma informações mínimas, entre as quais, em que a fase do framework kill Chain o evento foi gerado, veja-se:

> *"3.1.7.17. Dentre as formas de pesquisa a solução **deve ser capaz de filtrar no mínimo** as seguintes informações:*
> *a) Endereço IP do Atacante;*
> *b) IP de Destino;*
> *c) Porta de destino;*
> *d) Duração da conexão;*
> *e) Score de Risco do atacante;*
> *f) Protocolo de rede;*
> ***g) Fase do Kill Chain, e;***
> *h) Tipo da isca;"*

Contudo, ainda sendo uma característica que a solução deve suportar, ainda que minimamente, a documentação apresentada pela Licitante recorrida, não trás qualquer informação detalhada no que se refere ao framework kill chain, veja-se:

Referência:

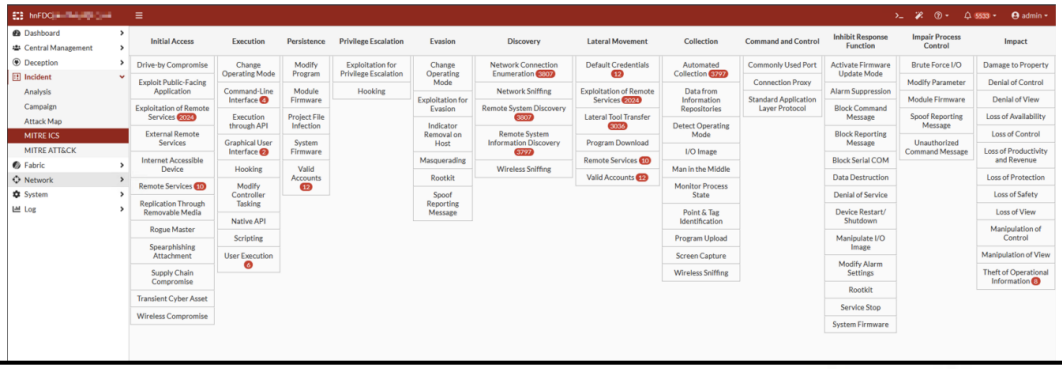
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/2a1e05c4-9a5f-11f0-855d-6af4c3636dc7/FortiDeceptor-6.2.0-Administration_Guide.pdf

Print:

Viewing the MITRE ICS matrix

After the FortiDeceptor appliance is tagged, go to *Incident* > *MITRE ICS* to view the matrix. The matrix displays the *Tactics* as columns and the *Techniques* as tiles. Management devices display a blue banner at the top of the matrix that shows the tagged appliances in the network. Standalone devices do not display the banner. When an incident meets the Tactic criteria, the Technique tile displays a red dot with the number of incidents.

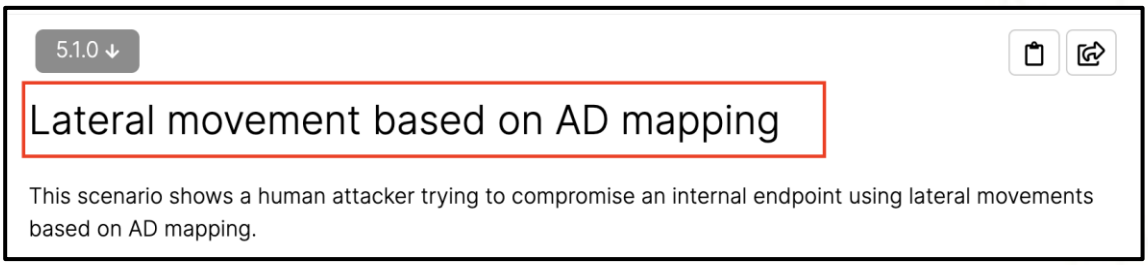
To view the MITRE ICS incidents, click a *Technique* tile in the *Tactics* column.



Referência:

https://docs.fortinet.com/document/fortideceptor/5.1.0/administration-guide/393363/lateral-movement-based-on-ad-mapping

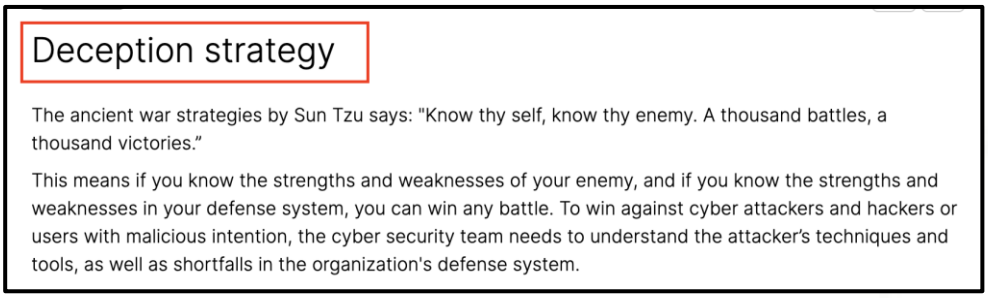
Print:



Referência:

https://docs.fortinet.com/document/fortideceptor/5.1.0/administration-guide/587085/deception-strategy

Print:


Deception strategy

The ancient war strategies by Sun Tzu says: "Know thy self, know thy enemy. A thousand battles, a thousand victories."

This means if you know the strengths and weaknesses of your enemy, and if you know the strengths and weaknesses in your defense system, you can win any battle. To win against cyber attackers and hackers or users with malicious intention, the cyber security team needs to understand the attacker's techniques and tools, as well as shortfalls in the organization's defense system.

Verifica-se que a documentação apresentada pela licitante Recorrida, apesar de trazer informações referentes a matriz do Mitre, não há qualquer referência ao framework Kill Chain. É importante ressaltar que, o fato da licitante Recorrida, mesmo sabendo que este se trata de um item indispensável para o TRT-12, e não comprova o item, demonstra a intenção de induzir o TRT-12 ao erro, o que se traduz em má-fé, uma vez que a licitante Recorrida, visa o benefício próprio, o que pode comprometer diretamente a lisura deste processo, em caso de aceitabilidade da proposta desta licitante Recorrida.

(III) A FUNDAMENTAÇÃO JURÍDICA

. (III.I) A Vedação Ao Comportamento Contraditório E O Controle Da Legalidade Do Ato Administrativo A Ensejar Análise Por Parte Do Poder Judiciário

. Conforme já exposto, a Administração Pública, ao responder aos questionamentos reforçando a necessidade estratégica dos requisitos editalícios impôs a si mesma um rigor maior ao deliberar sobre o atendimento das propostas referente ao item questionado. Admitir que qualquer licitante vença o certame licitatório sem atender à referida exigência é comportamento contraditório vedado pelo direito, que ultrapassa os limites do mérito administrativo e enseja o controle de legalidade por parte do Poder Judiciário. Essa é a posição pacífica do Egrégio Tribunal Regional Federal da 2ª Região que se pede vênia para colacionar precedente jurisprudencial:

> *[...]*
>
> *2. <u>**O controle pelo Poder Judiciário de ato administrativo ilegal ou abusivo não viola o princípio da separação dos poderes**</u>, podendo o Judiciário analisar, inclusive, questões relativas à*

proporcionalidade e à razoabilidade do ato impugnado. Precedente: TRF2, 5ª Turma Especializada, AC 0001377-51.2011.4.02.5101, Rel. Des. Fed. ALUISIO GONÇALVES DE CASTRO MENDES, EDJ2R 12.12.2014."[1]

(III.II) A VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

. A discussão travada no presente recurso é tão basilar que o próprio Art. 3º Da Lei de Licitações já dá a pista da solução para casos como o presente ao determinar:

> *Art. 5º Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da* ***igualdade,*** *do planejamento, da transparência, da eficácia, da segregação de funções, da motivação,* ***da vinculação ao edital, do julgamento objetivo****, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).*

. A manutenção da decisão data máxima vênia, permitirá com que licitante que não atende aos requisitos mínimos do Instrumento convocatório se sagre vencedora do certame, gerando insegurança jurídica e violando a isonomia no processo licitatório, bem como esgarçando o princípio da vinculação ao instrumento convocatório.

. A esse propósito, dentre as principais garantias Constitucionais de um processo licitatório, **destaca-se a vinculação da Administração ao Edital** que regulamenta o certame licitatório. Trata-se de uma segurança para o licitante e para o

[1] Tribunal Regional Federal da 2ª Região TRF-2 - Apelação: AC 0141667-82.2017.4.02.5109 RJ 0141667-82.2017.4.02.5109

interesse público, extraída do princípio do procedimento formal, que determina à Administração que observe as regras por ela própria lançadas no instrumento que convoca e rege a licitação.

. O Professor Lucas Rocha Furtado, Procurador do Ministério Público junto ao Tribunal de Contas da União, leciona que o instrumento convocatório

> *"é a lei do caso, aquela que irá regular a atuação tanto da administração pública quanto dos licitantes. Esse princípio é mencionado no art. 3º da Lei de Licitações, e enfatizado pelo art. 41 da mesma lei que dispõe que "a Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada". (Curso de Direito Administrativo, 2007, p.416)"*

. No mesmo sentido, a Suprema Corte brasileira, em oportunidade na qual enfrentou o tema (RMS 23640/DF), decidiu que:

> *"EMENTA: RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. CONCORRÊNCIA PÚBLICA. PROPOSTA FINANCEIRA SEM ASSINATURA. DESCLASSIFICAÇÃO. PRINCÍPIOS DA VINCULAÇÃOAO INSTRUMENTO CONVOCATÓRIO E DO JULGAMENTO OBJETIVO. 1. Se o licitante apresenta sua proposta financeira sem assinatura ou rubrica, resta caracterizada, pela apocrifia, a inexistência do documento. 2.* ***Impõe-se, pelos princípios da vinculação ao instrumento convocatório e do julgamento objetivo, a desclassificação do licitante que não observou exigência prescrita no edital de concorrência****. 3.* ***A observância ao princípio constitucional da preponderância da proposta mais vantajosa para o Poder Público se dá mediante o cotejo das propostas válidas apresentadas pelos concorrentes, não havendo como incluir na avaliação a oferta eivada de nulidade****. 4. É imprescindível a assinatura ou rubrica do licitante na sua*

proposta financeira, sob pena de a Administração não poder exigir-lhe o cumprimento da obrigação a que se sujeitou. 5. Negado provimento ao recurso."

. É nesse sentido o pacífico entendimento do Tribunal de Contas da União que em diversas oportunidades consolidou sua jurisprudência no seguinte sentido:

REPRESENTAÇÃO. PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇO. EXIGÊNCIA DE ATESTADOS DE CAPACIDADE TÉCNICA EM PERCENTUAL MÍNIMO DE 50% PARA TODOS OS ITENS LICITADOS. ILEGALIDADE. ACEITAÇÃO DE ATESTADOS DOS VENCEDORES EM DESACORDO COM O PRÓPRIO EDITAL. ***MALFERIMENTO DOS PRINCÍPIOS DA ISONOMIA E DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO. APLICAÇÃO DE MULTA AOS RESPONSÁVEIS.*** *DETERMINAÇÕES. PEDIDO DE REEXAME. CONHECIMENTO. NEGATIVA DE PROVIMENTO (Acórdão 4091/2012 - Segunda Câmara)*

. Em mais uma oportunidade, a Egrégia Corte de Contas, que tem jurisdição para analisar a presente contratação, concluiu o seguinte:

REPRESENTAÇÃO. LICITAÇÃO. POSSÍVEIS IRREGULARIDADES EM PREGÃO ELETRÔNICO. CONSTATAÇÃO DE ALGUMAS FALHAS RELACIONADAS À INOBSERVÂNCIA DO PRINCÍPIO DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO. PROCEDÊNCIA PARCIAL. DETERMINAÇÃO. (Acórdão 966/2011 - Primeira Câmara)

. Recentemente, decidiu sua Excelência, o Ministro Marcos Bemquerer que:

21. O princípio da vinculação ao instrumento convocatório impõe a fiel observância às disposições editalícias, não

> *permitindo à comissão de licitação ou ao pregoeiro deliberar de forma desatrelada das normas que regem o certame.*
>
> *[...]*
>
> *23. **Portanto, não há exceções para o descumprimento aos termos do instrumento convocatório** que regeu o Pregão Eletrônico 1.859/2019.*
>
> *24. Havendo previsão no edital de avaliação de amostras a sua realização será obrigatória. Nesse sentido, é o entendimento consignado na Nota Técnica 04/2009 da Sefti/TCU, extensivo às licitações albergadas pela Lei 13.303/2016, porque fundamentado no princípio da vinculação ao instrumento convocatório:*

. O que se conclui dos precedentes jurisprudenciais colacionados é que o princípio da vinculação ao instrumento convocatório **obriga** a Administração e o licitante a observarem as regras e condições previamente estabelecidas no Edital. Foi rigorosamente o que ocorreu no presente processo.

(III.III)A POSSIBILIDADE DE APLCAÇÃO DE MULTA AO PREGOEIRO QUE ATUAR EM DESCOMPASSO COM CLARA DETERMINAÇÃO LEGAL

. A Lei Orgânica do Tribunal de Contas da União prevê a possibilidade de aplicação de multa ao gestor que deixar de observar clara determinação legal, como é o presente caso. Pede-se vênia para colacionar trecho do Art. 58, II da Lei 8.443/92:

> *Art. 58. O Tribunal poderá aplicar multa de Cr$ 42.000.000,00 (quarenta e dois milhões de cruzeiros), ou valor equivalente em outra moeda que venha a ser adotada como moeda nacional, aos responsáveis por:*

> *II - ato praticado com grave infração à norma legal ou regulamentar de natureza contábil, financeira, orçamentária, operacional e patrimonial;*

. O Tribunal de Contas da União não hesita em aplicar o referido dispositivo em casos análogos ao presente. Pede-se licença para colacionar precedentes jurisprudências nos quais se aplicou multa ao pregoeiro pela **inobservância de dispositivo legal**, qual seja, vinculação ao instrumento convocatório:

> *7. Por essas razões, não há dúvidas de que foram incluídas no edital pela Universidade Federal de Santa Catarina exigências desconformes com a Lei nº 8.666/1993 e com a jurisprudência do TCU, impedindo que outras empresas participassem da licitação.* ***Além disso, cometeu outra irregularidade na medida em que permitiu que algumas participantes se sagrassem vencedoras sem atender às exigências do próprio edital.***
>
> *8. Diante desses fatos, processo licitatório foi irregular, razão porque poder-se-ia determinar que a UFSC adotasse providências para a sua anulação, inclusive a rescisão dos contratos dele derivados. Todavia, considerando que os referidos contratos têm validade de 12 meses e que já se passaram mais de 8 meses de vigência, bem como que os serviços vêm sendo executados conforme as necessidades da UFSC, a relação custo-benefício de um novo procedimento, a esta altura, recomenda que não haja solução de continuidade dos serviços até agora prestados pelas empresas contratadas, sem prejuízo, porém, de recomendar-se à Universidade que providencie um novo procedimento licitatório a vigorar ao final dos atuais contratos, escoimado das falhas ora constatadas.*
>
> *9. Este posicionamento, todavia, não afasta o caráter das irregularidades verificadas no certame, razão pela qual* ***acolho, neste particular, as conclusões da unidade técnica, de modo a***

> ***aplicar ao Pró-Reitor, Sr. João Batista Furtuoso, e à Pregoeira, Sra. Silvana de Freitas Ribeiro, revel nestes autos, a multa do art. 58, inciso II, da Lei 8.443/1992.39.*** *Desta forma, e considerando-se as análises constantes dos tópicos anteriores, verifica-se que tanto o Pró-Reitor quanto a Pregoeira, responsáveis pelo certame, cometeram atos com grave infração à norma legal, devendo-se aplicar a multa prevista no art. 58, inciso II, da Lei 8.443/1992. (Acórdão 8239/2011 – TCU 2ª Câmara)*

. Em outra oportunidade, mais uma vez a Corte de Contas reafirmou seu posicionamento e propósito da aplicação da multa prevista no citado artigo. Pede-se vênia para colacionar a reflexão do Eminente Ministro Aroldo Cedraz:

> *5. Corroborando esse entendimento,* ***cabe esclarecer-lhes que a "grave infração à norma legal ou regulamentar" a que se refere os arts. 58, inciso II, da Lei 8.443/1992 e 268, inciso II, do Regimento Interno/TCU não pressupõe necessariamente prejuízo ao erário ou a terceiros, estando caracterizada, no caso em estudo****, pela restrição ao caráter competitivo do certame (irregularidade sintetizada no subitem 3.1 supra) e* ***pela afronta aos princípios da isonomia, do julgamento objetivo e da vinculação ao instrumento convocatório*** *(falha descrita no subitem 3.2). (Acórdão 7011/2012 – TCU Segunda Câmara)*

(IV) A POSSIBILIDADE DE ABERTURA DE NEGOCIAÇÃO COM A PRÓXIMA COLOCADA

. Caso a Recorrida seja desclassificada a próxima colocada deverá ser convocada e oportunizada negociação em relação ao valor inicialmente ofertado. Tal permissivo encontra fundamento no Art. 61 da Lei 14.133/21 que estabelece que a

negociação é uma **etapa inerente ao procedimento**, que sucede o julgamento das propostas:

> *Art. 61. Definido o resultado do julgamento, a Administração **poderá negociar** condições mais vantajosas com o primeiro colocado.*

. A jurisprudência dos Tribunais de Contas entende a negociação não como uma mera faculdade, mas como uma obrigação funcional do agente público, um verdadeiro **poder-dever**.

Nesse sentido, o Tribunal de Contas do Estado de Minas Gerais já se manifestou:

> *A negociação entre o pregoeiro e a empresa responsável pela proposta classificada em primeiro lugar trata-se de poder-dever da Administração Pública, visando a contratação mais vantajosa, ainda que o preço encontrado após a disputa seja inferior àquele objeto da pesquisa de preços constante da fase interna da licitação. (TCE-MG - DEN: 1088782, Relator: CONS. SUBST. ADONIAS MONTEIRO, Data de Julgamento: 10/05/2022, Data de Publicação: 04/07/2022)*

. Ademais, a obrigatoriedade de buscar a melhor proposta **se estende aos licitantes subsequentes**, caso o primeiro colocado não atenda às exigências ou sua proposta não seja exequível, como bem aponta o Egrégio Tribunal de Justiça de Mato Grosso:

> *(...) cabe ao pregoeiro examinar a proposta subsequente e, assim, sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital. (TJ-MT - EMBDECCV: 10031823820168110000 MT, Relator: ANTONIA SIQUEIRA GONCALVES, Data de Julgamento: 04/05/2017, Data de Publicação: 06/06/2017)*

(V) CONCLUSÃO E PEDIDOS

Por todo o exposto, não resta à Recorrente senão pleitear pelo recebimento do presente recurso para, no mérito, desclassificar do presente certame licitatório a licitante Recorrida pelo evidente desatendimento às exigências editalícias, convocando-se a próxima licitante mais bem colocada para análise de habilitação.

PATRICIA ANGELINA DA CONCEICAO:34699483801

Assinado de forma digital por PATRICIA ANGELINA DA CONCEICAO:34699483801
Dados: 2026.02.02 20:18:00 -03'00'