AO TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO/MG

AO ILUSTRÍSSIMO PREGOEIRO OFICIAL E A RESPECTIVA EQUIPE DE APOIO

REF.: PREGÃO ELETRÔNICO 90017/2024 [1]

TELETEX COMPUTADORES E SISTEMAS LTDA., pessoa jurídica de direito privado, inscrita no CNPJ/MF sob nº. 79.345.583/0001-42, sediada na Rod. BR 116, nº 12.500, CEP 81.690-200, bairro Parolin, cidade de Curitiba, estado do Paraná (denominada de "Recorrida"), vem, respeitosamente, por seu procurador que adiante subscreve, à presença de Vossa Senhoria, apresentar:

CONTRARRAZÕES AO RECURSO ADMINISTRATIVO

interposto por **ARVVO TECNOLOGIA, CONSULTORIA E SERVIÇOS LTDA.** (denominada de "Recorrente"), em face da decisão que **aceitou a proposta e habilitou** a empresa **TELETEX COMPUTADORES E SISTEMAS LTDA.**, conforme as razões adiante aduzidas.

1. DA ADMISSIBILIDADE E TEMPESTIVIDADE

[1] **OBJETO**: REGISTRO DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE TIC COM A FINALIDADE DE ATENDER ÀS NECESSIDADES DE FUNCIONAMENTO DOS SISTEMAS DO TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO.

Nos termos do **Item 11.7.**[2] do Edital do **PREGÃO ELETRÔNICO 90017/2024**, o prazo para apresentação das contrarrazões recursais é de 3 (três) dias úteis, "*contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses*".

A intenção de recurso da Recorrente foi apresentada em **19/03/2025 (segunda-feira).**

19/03/2025 às 14:17:01	Fornecedor ARVVO TECNOLOGIA, CONSULTORIA E SERVICOS LTDA, CNPJ 25.359.140/0001-81 registra a intenção de recurso na fase habilitação.

Por sua vez, a Recorrente apresentou recurso administrativo em **24/03/2025** (segunda-feira).

exigidos no instrumento convocatório. Vejamos.

II. **TEMPESTIVIDADE**

4. Conforme registrado no sistema ComprasNet, a data limite para registro das razões recursais é dia **24/03/2025**, de modo que é tempestiva, portanto, a presente manifestação.

Assim, o prazo iniciou em **25/03/2025 (terça-feira)**, findando em **27/03/2025 (quinta-feira).**

Portanto, as presentes contrarrazões são **tempestivas**, devendo serem recebidas e analisadas por este D. Órgão, nos termos adiante expostos.

[2] **Item 11.7.** - O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

2. DAS RAZÕES PARA A REFORMA DA DECISÃO

2.1. ACERCA DA VALIDADE DO ATESTADO DE CAPACIDADE TÉCNICA

Em resposta às alegações de que o atestado de capacidade técnica apresentado pela **TELETEX** não atenderia às exigências editalícias, faz-se necessário esclarecer e rebater os pontos levantados, **demonstrando a regularidade do documento** e a aptidão técnica da empresa para executar o objeto licitado.

O atestado apresentado pela **TELETEX** descreve com clareza que a empresa realizou serviços **plenamente compatíveis** com o objeto do presente certame, abrangendo **instalação, customização, suporte, treinamento e operação assistida**, conforme exigido no item **4.2.1.1.1** do Termo de Referência.

Para fins de argumentação, a redação do atestado pode não ser idêntica aos termos utilizados no Edital, mas contempla todos os pontos relevantes para demonstrar a experiência na execução de soluções de cibersegurança, redes e serviços correlatos, em estrita consonância com o objeto licitado.

Ainda que não haja menção literal e detalhada de cada subatividade (por exemplo, "operação assistida"), o atestado descreve, de forma objetiva, a participação da TELETEX em todas as fases do projeto — o que, de fato, **comprova** a execução dos serviços tecnicamente semelhantes aos requeridos.

Em procedimentos licitatórios, a **equivalência fática** das atividades listadas no atestado é suficiente para demonstrar a aptidão técnica da licitante, atendendo ao fim visado pela Administração: resguardar-se contra a inexperiência.

A interpretação proposta pela Recorrente incorre em formalismo excessivo, em desconformidade com os princípios estabelecidos no artigo 5º e no artigo 64 da Lei nº 14.133/2021, os quais são de observância obrigatória nas licitações. O artigo 5º da referida Lei preconiza que, na sua aplicação, devem ser observados, dentre outros, os princípios da razoabilidade, da ampla competitividade, da vinculação ao edital, da segurança jurídica e da economicidade.

Já o artigo 64 dispõe que: *"Na análise dos documentos de habilitação, o agente de contratação poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica."*

Com isso, a interpretação restritiva proposta pela Recorrente contraria os princípios de razoabilidade e ampla competitividade, uma vez que visa à desclassificação sem que haja prejuízo substancial à validade da documentação apresentada.

2.1.1 DA POSSIBILIDADE DE COMPLEMENTAÇÃO, SE ASSIM ENTENDER O PREGOEIRO

Ainda que se entenda necessária a complementação de informações, é importante frisar que, em hipótese alguma, caberia a desclassificação imediata da proposta ou qualquer outra medida que desconsiderasse a decisão já proferida pelo pregoeiro e pelo time técnico do TRF6.

Caso houvesse dúvidas quanto ao atendimento às exigências do Edital, o ente licitante, conforme a legislação vigente, poderia solicitar diligência, conforme realizado com a empresa CISCO, ou ainda poderia abrir diligência para a complementação de documentos, nos termos da Lei nº 14.133/2021.

Ademais, a empresa TELETEX está plenamente apta a apresentar declaração complementar ou documentos acessórios (como escopo técnico, contrato ou relatórios de aceite) que comprovem que a prestação de serviços incluiu as atividades mencionadas, tais como instalação, operação assistida e capacitação, sempre em conformidade com a solução de *SSE Cisco* fornecida à HAVAN.

2.2. COMPATIBILIDADE TÉCNICA

A compatibilidade técnica consiste em demonstrar que a TELETEX executou projetos com **grau de complexidade similar** ao objeto do Edital. O atestado revela o uso de equipamentos e funcionalidades de alta complexidade tecnológica, alinhando-se à necessidade de experiência em cibersegurança (**Itens 4.2.1.2.1 e 4.2.1.2.2** do **Termo de Referência**), o que reforça a legalidade e eficácia do documento.

2.3. LISTA DE GLOBAL PARTNERS

A TELETEX **já integra** a lista de global partners do fabricante da solução, possuindo **autorização formal** para fornecimento de produtos, serviços e suporte de alto nível.

Tal condição satisfaz os requisitos de confiabilidade e respaldo tecnológico exigidos no **Item 4.2.1.2** do **Termo de Referência**, reforçando a adequação e a legitimidade do atestado quanto aos quesitos de origem, controle, garantia e suporte.

Para elucidar quaisquer dúvidas, a Recorrida apresenta as evidências que rebatem os argumentos trazidos pela parte Recorrente:

A finalidade primordial do atestado é **comprovar a aptidão** da empresa para executar serviços com as mesmas especificações do Edital. Os serviços prestados

pela **TELETEX**, indicados no atestado, **guardam correlação direta** com as atividades aqui licitadas, abrangendo soluções de cibersegurança e componentes críticos de infraestrutura de TI, o que confirma a experiência técnica exigida.

Por isso, pugna-se pelo provimento desprovimento do recurso administrativo da Recorrente.

2.1 AS SUPOSTAS ALEGAÇÕES DE IMPOSSIBILIDADE DE DILIGÊNCIAS E DE SUPOSTO DESRESPEITO AO JULGAMENTO OBJETIVO E À VINCULAÇÃO AO EDITAL

Em que pese o respeito aos argumentos apresentados, cumpre esclarecer que a pretensão de impedir a realização de diligências para esclarecimentos não se sustenta diante do ordenamento jurídico e do próprio Edital, pelos motivos a seguir delineados.

A possibilidade de diligências não se confunde com a reabertura de prazos ou substituição integral de documentos. Trata-se, antes, de um mecanismo que permite à Administração esclarecer eventuais incongruências ou obter informações complementares sobre documentos já apresentados, nos termos do art. 64 da Lei nº 14.133/2021 e das disposições do Edital (item 8.13).

Fazendo um parêntese, as inovações trazidas pela nova lei de licitações, tanto as instituições públicas quanto as privadas passaram por uma fase de treinamento e adequação, a fim de evitar interpretações equivocadas sobre a legislação e, em especial, sobre os princípios que regem a igualdade entre os concorrentes. Esse princípio, previsto na própria Constituição Federal, em seu art. 37, § XXI, dispõe que:

> "Ressalvados os casos especificados na legislação, as obras, serviços, compras e alienações serão contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes, com cláusulas que estabeleçam obrigações de pagamento, mantidas as condições efetivas da proposta, nos termos da lei, o qual somente permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações."

No presente caso, a **TELETEX** não está requerendo a apresentação de um documento completamente diverso do que já foi exibido, mas sim explicitar aspectos técnicos que podem não estar detalhados na linguagem exata do edital, porém estão implícitos e demonstrados na documentação já juntada.

O **Edital (Item 8.13)** admite a realização de diligências "*para complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame*". dessa redação deixa claro que, se o documento (por exemplo, o atestado) **já foi tempestivamente apresentado**, mas algum ponto suscite dúvidas, a diligência é cabível para verificar sua veracidade ou complementar detalhes técnicos.

Com isso, **não se viola o princípio da vinculação ao instrumento convocatório**, mas, ao contrário, **cumpre-se o que o próprio edital prevê**, pois a diligência é expressamente contemplada como faculdade do Pregoeiro, visando ao julgamento objetivo e à correta apuração da capacidade técnica.

O julgamento objetivo consiste em verificar, de **forma imparcial**, se as propostas (e a documentação) atendem aos requisitos do edital. Implica examinar o conteúdo e a substância dos documentos apresentados, não se restringindo a formalidades

excessivas que conduzam a resultados contrários ao interesse público e ao princípio da competitividade.

Caso se impeça qualquer diligência, mesmo quando há indicativos de que o documento atende ao escopo exigido, a Administração corre o risco de desqualificar indevidamente um licitante que, de fato, tenha condições de executar o objeto. Isso violaria o caráter competitivo do certame e, em última análise, **prejudicaria o princípio da isonomia.**

Nesse sentido, colecionamos a seguinte jurisprudência:

> "(...) Dessa maneira, a interpretação e a aplicação *das* regras estabelecidas devem ter por norte o atingimento dessas finalidades. 4 - No aspecto, admitir a juntada de documentos que apenas venham a atestar condição pré-existente à abertura da sessão pública do certame não fere os princípios da isonomia e igualdade entre os licitantes e, ainda, amplia a concorrência no certame". (TRF3. Acórdão. Processo nº 5027278-60.2023.4.03.0000. Órgão Julgador: 3ª Turma. Relator (a): Carlos Eduardo Delgado. Data do julgamento: 05/05/2024.)

Mais uma vez, pugna-se pelo desprovimento do recurso administrativo da Recorrente.

2.2 DA ALEGADA IMPOSSIBILIDADE DE APLICAÇÃO DO FORMALISMO MODERADO AOS PRAZOS DE LICITANTES E À SUPOSTA OFENSA AOS PRINCÍPIOS DA OBJETIVIDADE E IMPESSOALIDADE

O princípio do formalismo moderado, previsto e amplamente reconhecido na jurisprudência pátria, permite à Administração privilegiar a essência dos documentos e das informações, evitando que meras formalidades ou lacunas redacionais inviabilizem a correta avaliação da proposta.

A aplicação desse princípio **não implica reabertura de prazos para inserção de documentos inexistentes ou alteração integral da proposta já apresentada**, mas sim adequar a interpretação das exigências editalícias, a fim de se priorizar o interesse público e a competitividade, resguardando-se contra desclassificações por mero formalismo excessivo.

A aplicação do formalismo moderado não autoriza o descumprimento de exigências essenciais. **Ao contrário**, ela viabiliza que a Administração, no curso da habilitação, **averigue a real compatibilidade** entre o objeto do atestado e o exigido no edital, sem injustas desclassificações baseadas em detalhes meramente formais.

O próprio instrumento convocatório, no **Item 8.13**, reconhece a possibilidade de **complementação de informações** sobre documentos existentes para apurar fatos contemporâneos à abertura do certame, desde que não se trate de apresentação de documentos inéditos ou substituição integral do que foi juntado.

Dessa forma, **não** se deve acolher a tese de impossibilidade de aplicação do formalismo moderado, sob pena de se ensejar a desclassificação indevida de propostas qualificadas, com prejuízo à competitividade e à seleção da melhor proposta para a Administração.

2.3 DAS ALEGAÇÕES DE INOBSERVÂNCIA DAS EXIGÊNCIAS TÉCNICAS

O Edital, ao exigir comprovação de conformidade técnica, **visa garantir** que a solução ofertada atenda aos requisitos mínimos de uso e funcionamento para a finalidade pretendida.

A **TELETEX refuta** a alegação de que sua solução não cumpre tais requisitos, pois **apresentou documentação** apta a demonstrar a viabilidade e compatibilidade sejam eles equipamentos, softwares e serviços ofertados.

Cada um desses subitens, constante do **Anexo I** ou **Apêndice "A" (Especificações do LOTE 3)**, diz respeito a funcionalidades específicas da solução (por exemplo, requisitos de desempenho, compatibilidade de protocolos, níveis de segurança, padrões de conectividade, entre outros).

A documentação técnica e a proposta comercial da TELETEX **detalham como cada requisito é atendido**, seja por meio de especificações fornecidas pelo fabricante, seja pela demonstração da capacidade de integração, configuração e customização dos produtos ofertados.

A) ITEM 3.1.6. – SOBRE OS 02 (DOIS) DATACENTERS EM TERRITÓRIO BRASILEIRO PARA DISPONIBILIDADE E REDUNDÂNCIA

O Cisco Secure Access, conforme demonstrado em nossa documentação, adota uma estrutura de múltiplos sites no Brasil, contemplando tanto a infraestrutura AWS como data centers Cisco. Eis alguns pontos que comprovam a aderência ao requisito de utilização de, no mínimo, dois data centers para assegurar redundância e alta disponibilidade:

- Uso de AWS na Região São Paulo

- A Região São Paulo da AWS conta com 3 Zonas de Disponibilidade, conforme indicado em

https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/.

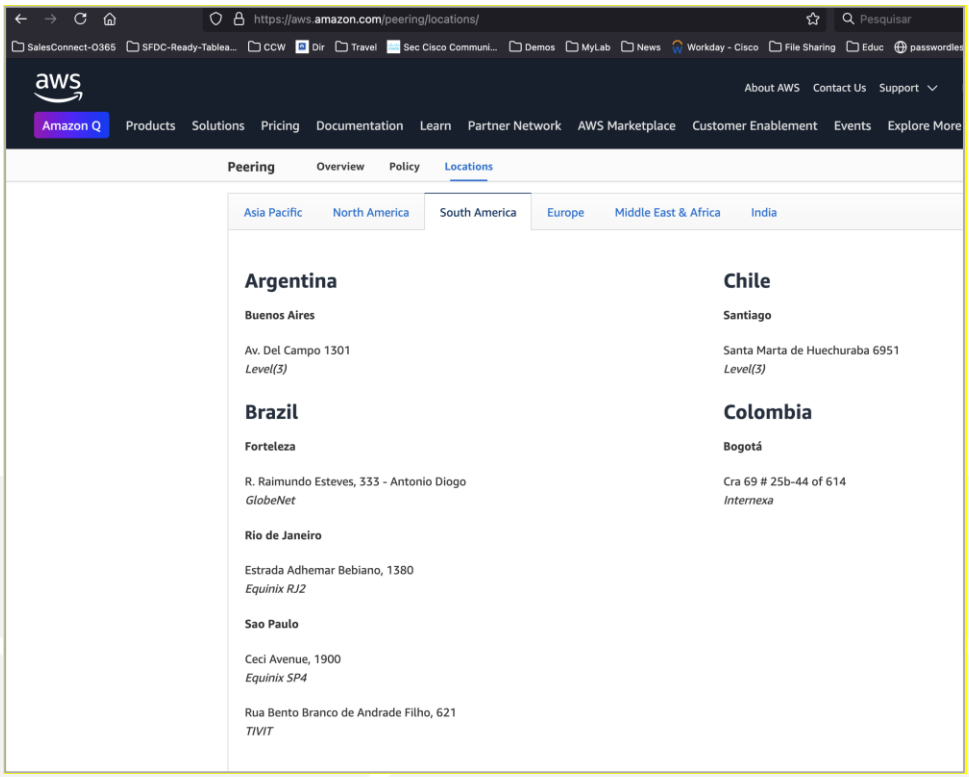
- Cada Zona de Disponibilidade (AZ) se caracteriza por ser um ou mais data centers distintos, com energia, rede e conectividade redundantes, capazes de oferecer alta disponibilidade e tolerância a falhas.

Pois bem, a região AWS São Paulo oferece 3 Zonas de Disponibilidade, conforme pode-se conferir em:

Sfio 1: https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/.

Sfio 2: https://aws.amazon.com/pt/about-aws/global-infrastructure/regions_az/ pode ser vista uma definição clara sobre Zona de Disponibilidade

Cada Zona de Disponibilidade (AZ) se caracteriza por ser um ou mais data centers distintos, com energia, rede e conectividade redundantes, capazes de oferecer alta disponibilidade e tolerância a falhas. Nessa modalidade Public Cloud on-demand, adotamos infraestruturas localizadas em São Paulo e no Rio de Janeiro para suportar serviços de SWG/DLP, FW, VPN e ZTA (ZTNA).



Complementarmente, para funções como DNS recursivo e, de maneira opcional, SWG/DLP e FW, utilizamos data centers próprios da Cisco no Rio de Janeiro e em São Paulo.

Ou seja, essa combinação reforça a redundância geográfica e a escalabilidade necessárias para garantir a continuidade dos serviços.

Dito de outra forma, alegar que não usamos 2 datacenters para o serviço **não é procedente e configura**, na nossa visão, uma tentativa de desqualificar o próprio serviço AWS, como se o uso de estrutura Multi-POP do provedor não oferecesse redundância geográfica, mesmo sendo usado por centenas de empresas e serviços e possuindo as principais certificações necessárias para indicar essa robustez.

A própria página indicada pelo recorrente, mostra isso:

https://aws.amazon.com/pt/local/saopaulo/#:~:text=A%20seguran%C3%A7a%20na%20AWS%20come%C3%A7a%20com%20nossa%20infraestrutura

> "A segurança na AWS começa com nossa infraestrutura. Todas as regiões da AWS são projetadas, construídas e auditadas regularmente para atender aos mais altos padrões de conformidade e fornecer um alto nível de segurança a todos os clientes da AWS. A Região da América do Sul da AWS (São Paulo) atende às normas ISO 27001, ISO 27017, ISO 27018, SOC 1 (anteriormente SAS 70), SOC 2 e SOC 3 Segurança e disponibilidade, PCI DSS nível 1, Health Data Host (HDS) e muitas outras."

Ora, a própria página da AWS enfatiza os rigorosos padrões de segurança e conformidade adotados, incluindo normas como ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3 e PCI DSS nível 1, entre outras, conforme pode ser verificado em https://aws.amazon.com/pt/local/saopaulo/.

Com isso, alegar que não usufruímos de data centers redundantes **ignora o fato de que a solução AWS oferece a robustez necessária para garantir a alta disponibilidade, sendo utilizada por centenas de empresas de diversos segmentos.**

O uso de uma estrutura Multi-POP (múltiplos pontos de presença) do provedor assegura a tolerância a falhas e a distribuição de carga, mitigando risco de indisponibilidade em um único local.

Nosso desenho de arquitetura contempla 3 data centers AWS e 2 data centers Cisco, o que não apenas cumpre, mas supera o requisito mínimo de dois data centers.

O Cisco Secure Access se qualifica como SaaS (Software as a Service) e, conforme a descrição pública do serviço em:

Stio 1:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/Cisco-Secure-Access-Product-Description.pdf, oferece SLA de 99,999% de disponibilidade, superando a exigência de 99,7% contida no item 3.1.15.

Portanto, a solução atende plenamente ao requisito de redundância entre data centers, haja vista que mantém múltiplas Zonas de Disponibilidade e pontos de presença, tanto na AWS quanto na infraestrutura própria da Cisco.

Eventuais alegações de que usamos apenas um data center são improcedentes, pois desconsideram a arquitetura multi-site adotada, que confere a robustez e a alta disponibilidade requisitadas no edital.

Portanto, entende-se que o item é plenamente atendido pelo Cisco Secure Access, pois, na verdade, usamos até mais de 2 datacenters, por possuirmos uma estrutura multi-site, totalmente redundante, combinando 3 datacenters AWS com 2 datacenters Cisco.

Vale ressaltar ainda que o Cisco Secure Access é uma solução SaaS que , conforme informado na descrição pública do serviço (https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/Cisco-Secure-Access-Product-Description.pdf), oferece 99,999% de disponibilidade, bem acima da requerida no item 3.1.15, que especifica 99,7%.

B) DEFESA EM RELAÇÃO AO ITEM 3.1.11

Em relação ao **Item 3.1.11**, que exige a utilização de datacenters em território brasileiro, informamos que a nossa arquitetura multi-site compreende a região AWS no Brasil (Public Cloud On-Demand) e data centers proprietários da Cisco no Rio de

Janeiro e em São Paulo. Dessa forma, o requisito de infraestrutura local é plenamente atendido.

C) ITEM 3.1.10

O Recurso deriva do desconhecimento acerca da arquitetura do Cisco Secure Access, solução que evoluiu do produto Cisco Umbrella (adquirido pela Cisco em 2015). Conforme a documentação disponível em:

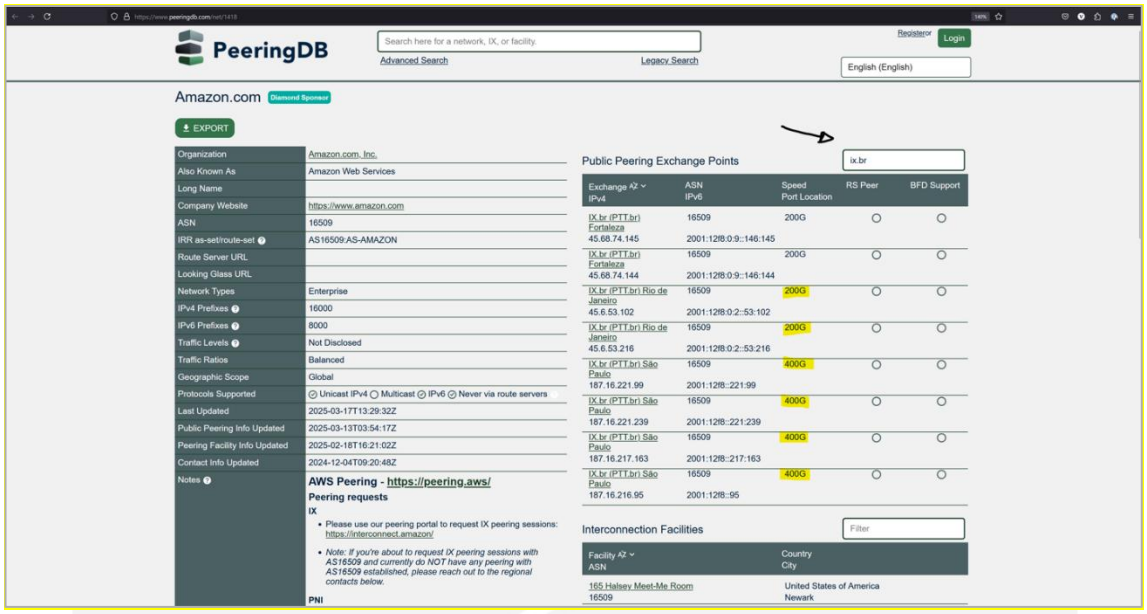
Stio 1: https://www.cisco.com/c/en_uk/products/collateral/security/hybrid-workforce-cloud-agile-security-ds.html

O Cisco Secure Access é uma solução SSE convergente que abrange SWG, CASB, ZTNA, FWaaS e outros recursos (como DLP, DNS Security, RBI, sandboxing, DEM insights e a inteligência de ameaças do Talos), tudo sob uma única licença e plataforma de gerenciamento.

Os sítios mencionados no recurso referem-se apenas à conectividade do Umbrella com o IX.BR, produto anterior que permanece em operação devido à sua base de clientes.

Já o Cisco Secure Access, conforme a página: https://docs.sse.cisco.com/sse-user-guide/docs/secure-access-regions, funciona em AWS, utilizando os peerings da própria AWS junto ao IX.BR (São Paulo e Rio de Janeiro).

Tais peerings estão listados em https://aws.amazon.com/peering e, ao acessar o "full list of locations and exchanges on PeeringDB", é possível filtrar por IX.BR, confirmando a presença de 4 x 400 Gbps para o IX.BR em São Paulo e 2 x 200 Gbps para o IX.BR no Rio de Janeiro.



Dessa forma, comprovamos que a solução Cisco Secure Access atende plenamente ao item 3.1.10 do edital, por dispor de conectividade robusta e redundante com as principais infraestruturas de troca de tráfego (IX.BR) no Brasil.

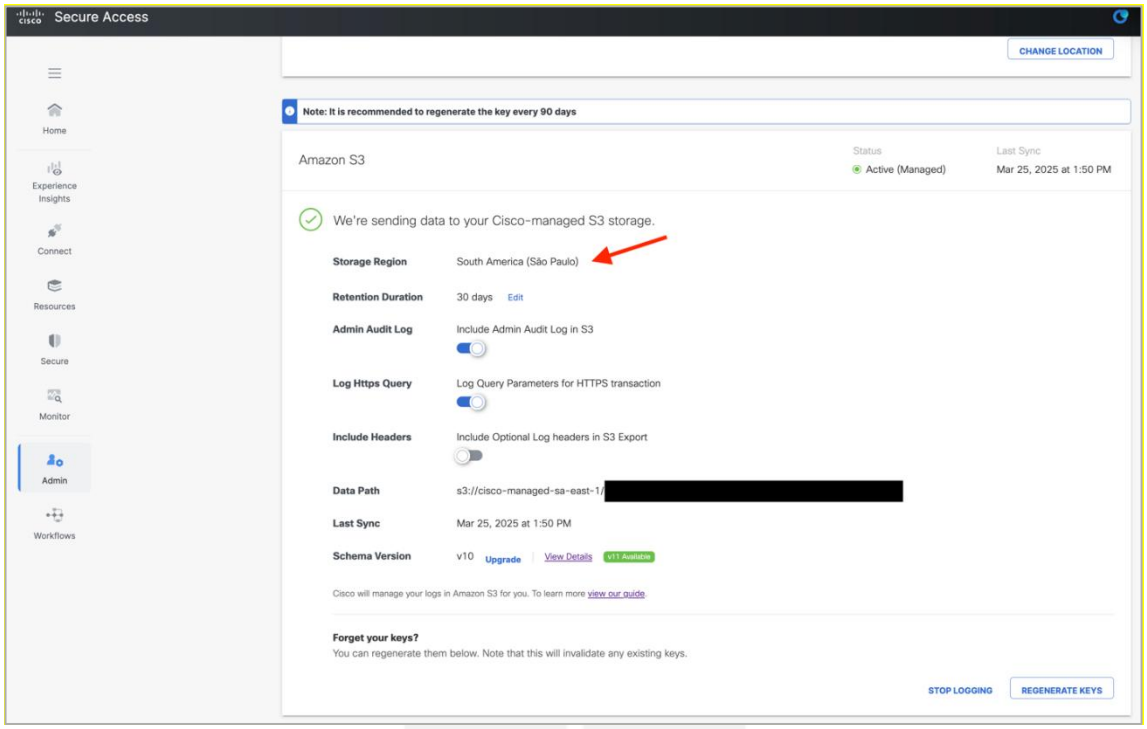
D) REQUISITO 3.1.12

Os logs do Cisco Secure Access são armazenados de acordo com o ajuste do administrador, podendo ser em bucket AWS S3 da Cisco incluído no produto ou próprio do cliente. Conforme indicado abaixo nos links abaixo, o administrador tem total libertade para indicar que tipo de S3 e qual região usar:

Sítio 1: https://docs.sse.cisco.com/sse-user-guide/docs/enable-logging-to-a-cisco-managed-s3-bucket

Sítio 2: https://docs.sse.cisco.com/sse-user-guide/docs/enable-logging-to-your-own-s3-bucket

Abaixo um exemplo de ambiente Secure Access que usa AWS São Paulo como região de log.



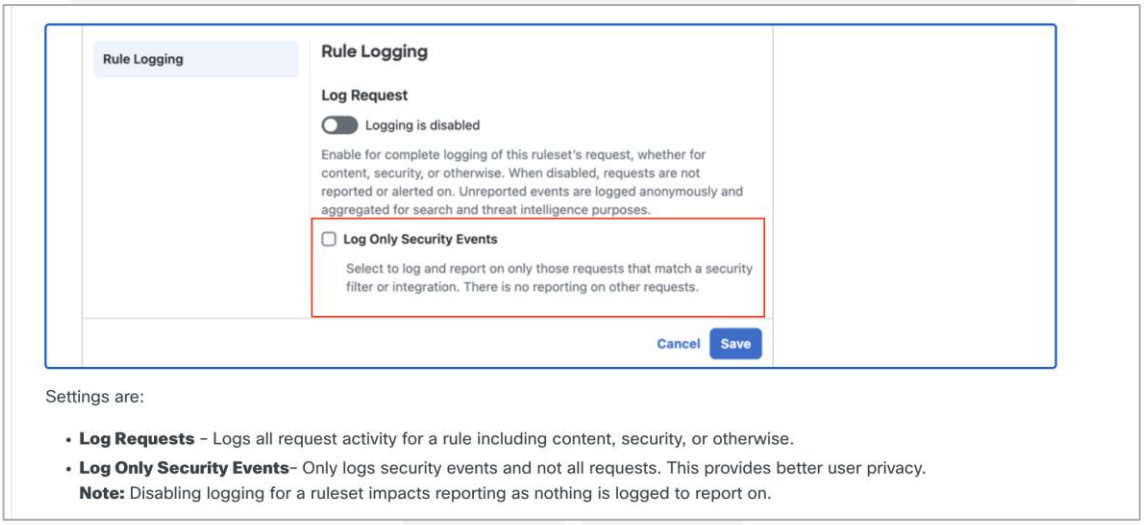
No que se refere à localização dos logs, diferentemente do que o Recorrente alega, **não** há obrigação de armazená-los nos Estados Unidos. O **Cisco Secure Access** é uma solução global que se adapta às necessidades locais de cada cliente, inclusive no Brasil, onde os logs são gravados em **AWS S3** na região brasileira.

Quanto às questões de **privacidade**, a documentação comprobatória anexada descreve detalhadamente as informações de cliente utilizadas pela solução, o propósito de cada coleta e o tempo de retenção. Para proteção de **dados pessoais** e **sensíveis**, o **Cisco Secure Access** oferece flexibilidade de configuração, permitindo ao administrador definir quais logs serão efetivamente registrados: todos, apenas os

relacionados à segurança (recomendado para fins de privacidade) ou, se necessário, desativar integralmente a gravação de logs.

A documentação do fabricante e a imagem ilustrativa da configuração seguem anexas para esclarecer esse ponto.

Stio 1: https://docs.sse.cisco.com/sse-user-guide/docs/enable-logging



Na tabela 5 (Table 5) abaixo, extraída do documento Cisco Secure Access Privacy Data Sheet - https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=SEcure%20access#/19304862119778772, podemos ver que tanto as comunicações quando os dados em repouso são criptografados:

7. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure. For additional information on Cisco Secure Access's data security program, please refer to Section 9 below.

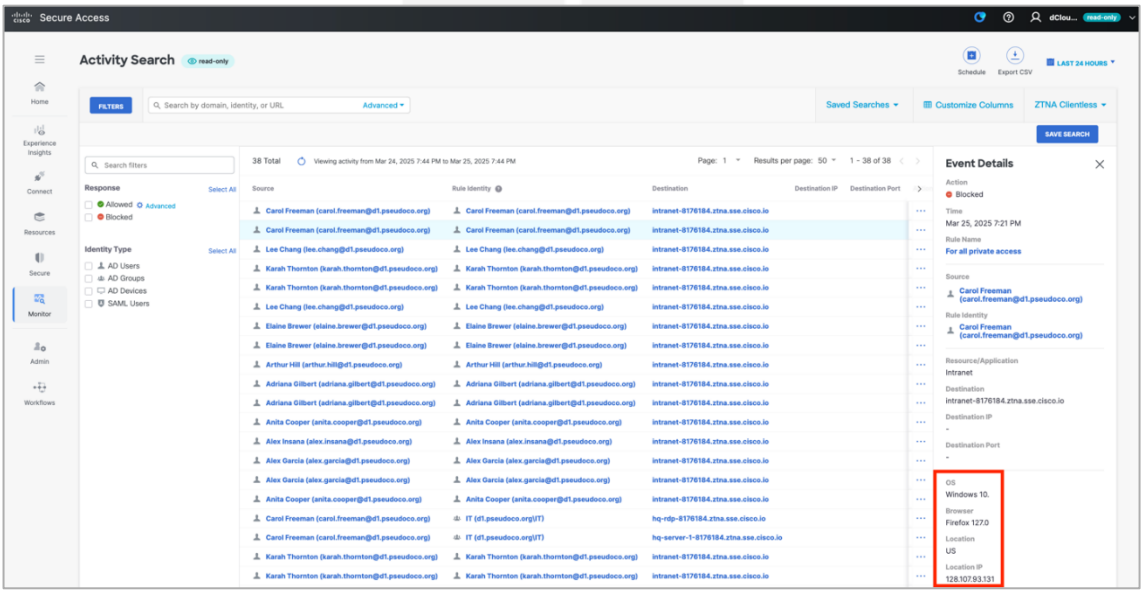
Table 5

Personal Data Category	Type of Personal Data	Security Controls and Measures (Subject to notes below this Table)
Account Data	See Table 1	Encryption in transit and at rest
Connection Data (ZTNA, VPN-as-a-Service, Roaming)	See Table 1	Encryption in transit and at rest
Device Posture Data	See Table 1	Encryption in transit and at rest
Security Data	See Table 1	Encryption in transit and at rest
Control Plane Data (Configuration, Policies, Identity)	See Table 1	Encryption in transit and at rest
	• OAuth Keys for Cloud Malware, including username of admin that authorized access • OAuth Keys for SaaS API-based DLP, including username and password of admin that authorized access	• Encryption in transit and at rest • Field level encryption on the OAuth Key • Customer can revoke OAuth keys at any time to terminate Cisco's access to the applicable SaaS environment
Cisco AI Assistant Data	See Table 1	Encryption in transit and at rest
Business and Usage Analytics Data	See Table 1	Encrypted in transit and at rest

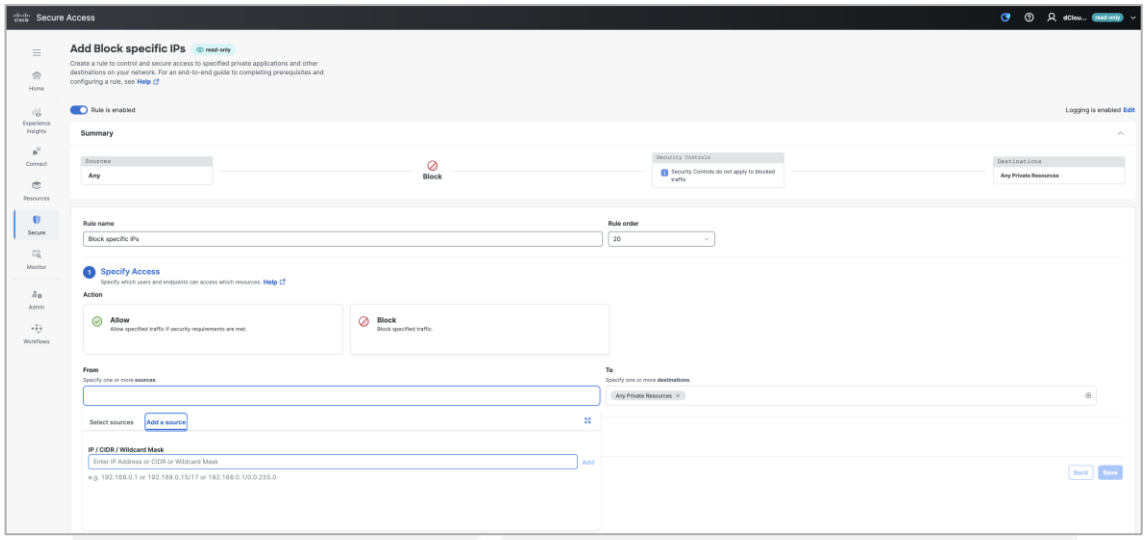
E) Requisito 3.1.29

Em relação aos itens indicados pelo recorrente, todas as interações durante fase de projeto e discussões técnicas deixaram claro que os requisitos são plenamente atendidos com a validação dos parâmetros em log do produto para o acesso clientless (via browser), da forma como incluídas na documentação comprobatória.

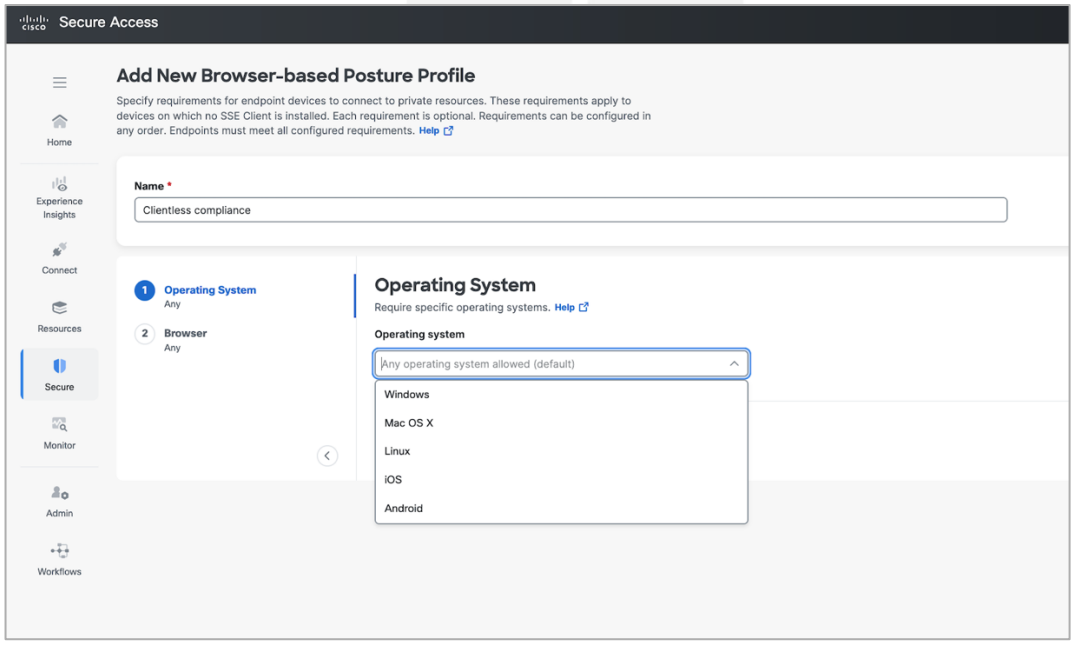
Abaixo temos um exemplo de tela apresentada pelo produto, incluindo todos os subitens do item 3.1.29:

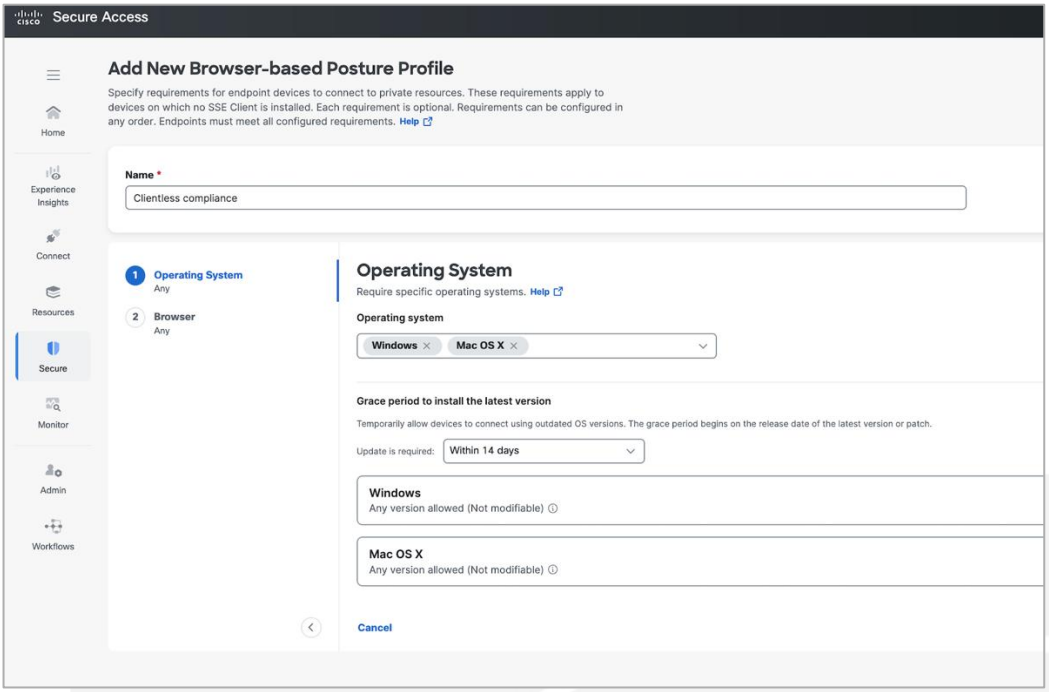


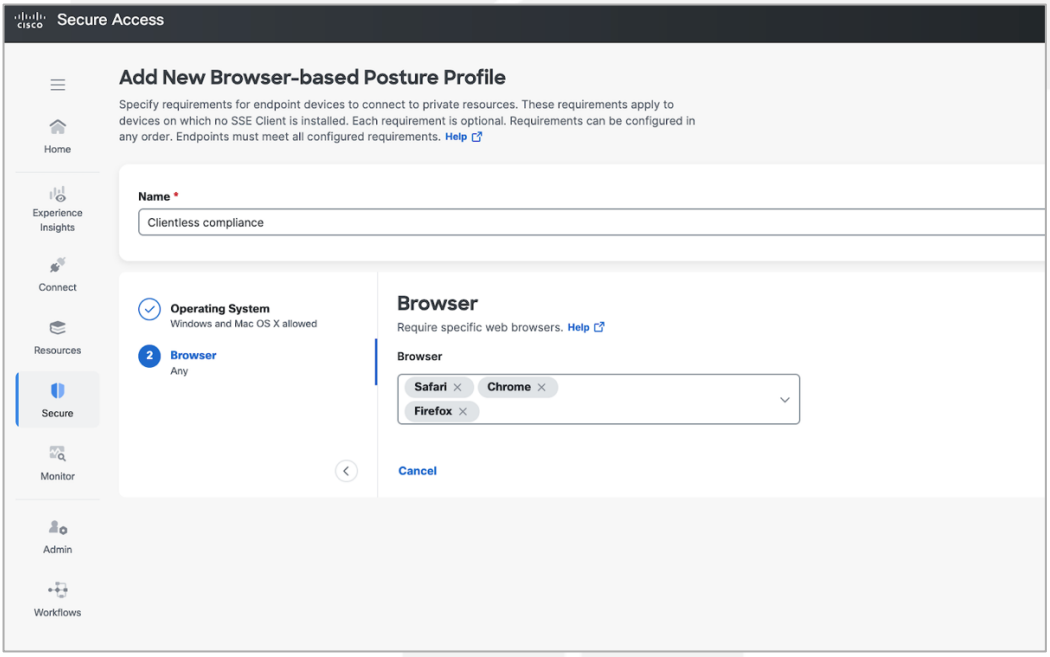
Para IP, SO e Browser, podemos, além da validação em log acima, realizar o controle e bloqueio. Abaixo um exemplo de como bloquear por IP/CIDR de origem:

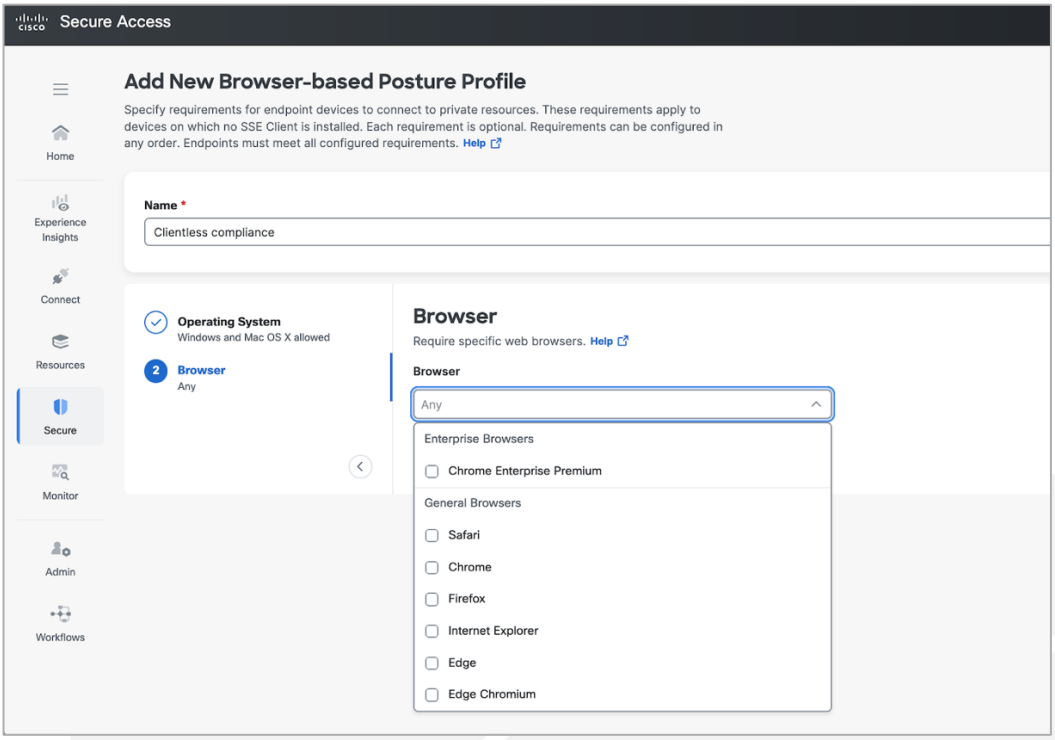


Para SO e Browser, o controle e bloqueio é feito diretamente via Profile, conforme abaixo:




Secure Access
Add New Browser-based Posture Profile
Specify requirements for endpoint devices to connect to private resources. These requirements apply to devices on which no SSE Client is installed. Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all configured requirements. Help
Name *
Clientless compliance
1 Operating System
Any
2 Browser
Any
Operating System
Require specific operating systems. Help
Operating system
Windows
Mac OS X
Grace period to install the latest version
Temporarily allow devices to connect using outdated OS versions. The grace period begins on the release date of the latest version or patch.
Update is required:
Within 14 days
Windows
Any version allowed (Not modifiable)
Mac OS X
Any version allowed (Not modifiable)
Cancel
Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows


Secure Access
Add New Browser-based Posture Profile
Specify requirements for endpoint devices to connect to private resources. These requirements apply to devices on which no SSE Client is installed. Each requirement is optional. Requirements can be configured in any order. Endpoints must meet all configured requirements. Help
Name *
Clientless compliance
Operating System
Windows and Mac OS X allowed
2 Browser
Any
Browser
Require specific web browsers. Help
Browser
Safari
Chrome
Firefox
Cancel
Home
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows



Caso surjam outras necessidades, é possível recorrer às APIs do Cisco Secure Access para atender aos requisitos adicionais. Por exemplo, ao criar uma política de acesso para permitir a conexão a recursos locais, o Cisco Secure Access gera um RuleID estático para cada regra, que pode ser facilmente obtido via API, possibilitando ativar ou desativar a regra conforme necessário.

Por meio do Resource Connector – um servidor interno que gerencia a comunicação entre usuários (via ZTNA) e aplicações locais – podem ser empregados scripts de API para verificar e modificar o status das regras em datas e horários específicos, atendendo eventuais demandas do TRF6.

Abaixo, apresentamos um exemplo de chamada de API para consultar as políticas existentes, configurada conforme a documentação oficial da Cisco.

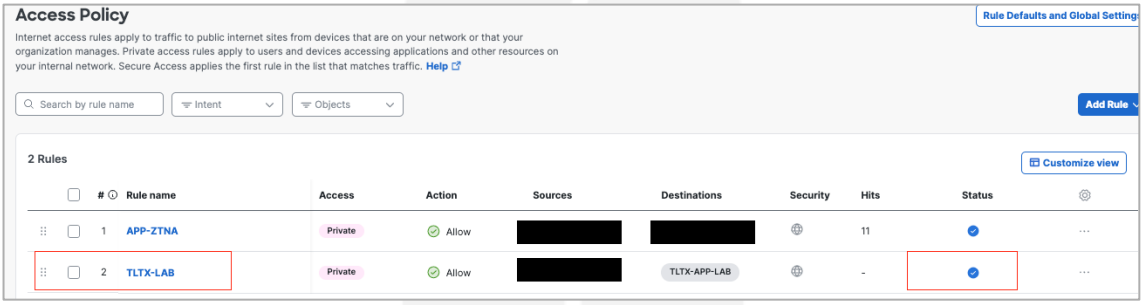
A imagem acima demonstra uma chamada de API para o Cisco Secure Access. O resultado em formato JSON exibe o campo 'ruleId', que varia entre as regras, não se repetindo.

Através desse 'ruleId', é possível modificar o status da regra, ativando-a o atributo ruleIsEnabled para true caso seja necessário que a regra seja ativada ou false para desativar a regra.

Para ilustrar a alteração via API, foi relizado uma chamada GET para a regra com ID ruleID:1124992. Observe que o campo 'ruleIsEnabled' está definido como 'True', indicando que a regra está atualmente ativa.

```
maiquel@Maiquels-MacBook-Pro ~ % curl -L --request GET \
--url https://api.sse.cisco.com/policies/v2/rules/{1124992} \
--header 'Authorization: Bearer '$accesToken'' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' |jq '.'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   815  100   815    0     0   1679      0 --:--:-- --:--:-- --:--:--  1680
{
  "createdAt": "2024-12-18T17:48:28+00:00",
  "modifiedBy": "org/8296961/user/8057523",
  "ruleIsDefault": false,
  "ruleName": "TLTX-LAB",
  "rulePriority": 2,
  "ruleIsEnabled": true,
  "ruleConditions": [
```

Na aplicação, o status da regra TLTX-LAB está marcado como ativo, conforme demonstrado no exemplo abaixo, no campo Status.



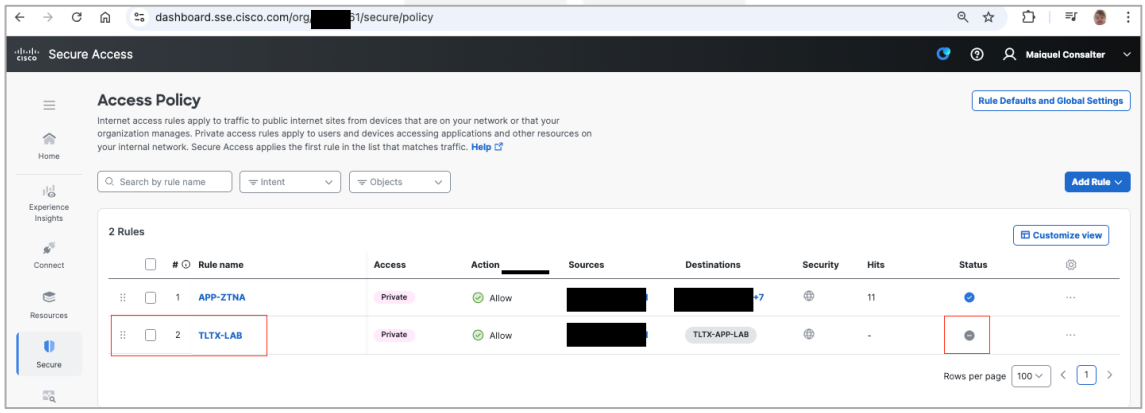
Para desativar a regra, foi criado uma chamada PUT para alterar o atributo 'ruleIsEnabled' de 'True' para 'False'.

Para desativar a regra, foi criado uma chamada PUT para alterar o atributo 'ruleIsEnabled' de 'True' para 'False'.

```
maiquel@Maiquels-MacBook-Pro ~ %
maiquel@Maiquels-MacBook-Pro ~ % curl -L --request PUT \
--url https://api.sse.cisco.com/policies/v2/rules \
--header 'Authorization: Bearer '$accesToken'' \
--header 'Content-Type: application/json' \
--header 'Accept: application/json' \
--data '{
   "ruleIds": [ 1124992 ],
   "properties": [
      {
         "ruleIsEnabled": false
      }
   ]
}' |jq '.'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   433  100   321  100   112    479    167 --:--:-- --:--:-- --:--:--   647
[
  {
    "createdAt": "2024-12-18T17:48:28",
    "modifiedBy": "org/8296961/user/8057523",
    "ruleIsDefault": false,
    "ruleName": "TLTX-LAB",
    "organizationId": 8296961,
    "rulesetId": 258178,
    "rulePriority": 2,
    "ruleIsEnabled": false,
    "ruleDescription": "",
    "ruleAction": "allow",
    "modifiedAt": "2025-03-26T01:09:55",
    "ruleId": 1124992
```

A imagem acima demonstra que, após a chamada de alteração via API, o atributo 'ruleIsEnabled' foi definido como 'False', indicando que a regra foi desativada.

Na aplicação, o status da regra TLTX-LAB aparece desmarcado/apagado, confirmando a desativação após a execução do script via Curl."



F) 3.1.29.3. LOCALIZAÇÃO (PAÍS DE ACESSO)

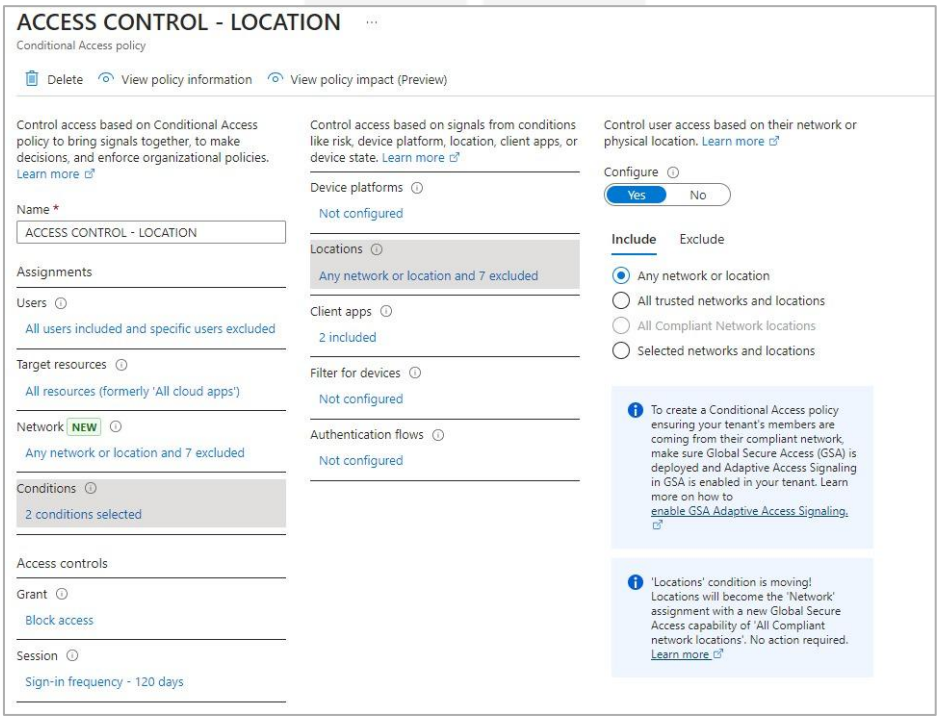
Para a autenticação de usuários via ZTNA, que permite criar regras de acesso mais granulares e autenticar usuários que se conectam a aplicações internas, é fundamental o uso do protocolo SAML (Security Assertion Markup Language). O SAML é um padrão aberto que possibilita que provedores de identidade (IdP) transmitam credenciais

de autorização para provedores de serviços (SP), sendo o Secure Access um exemplo de SP.

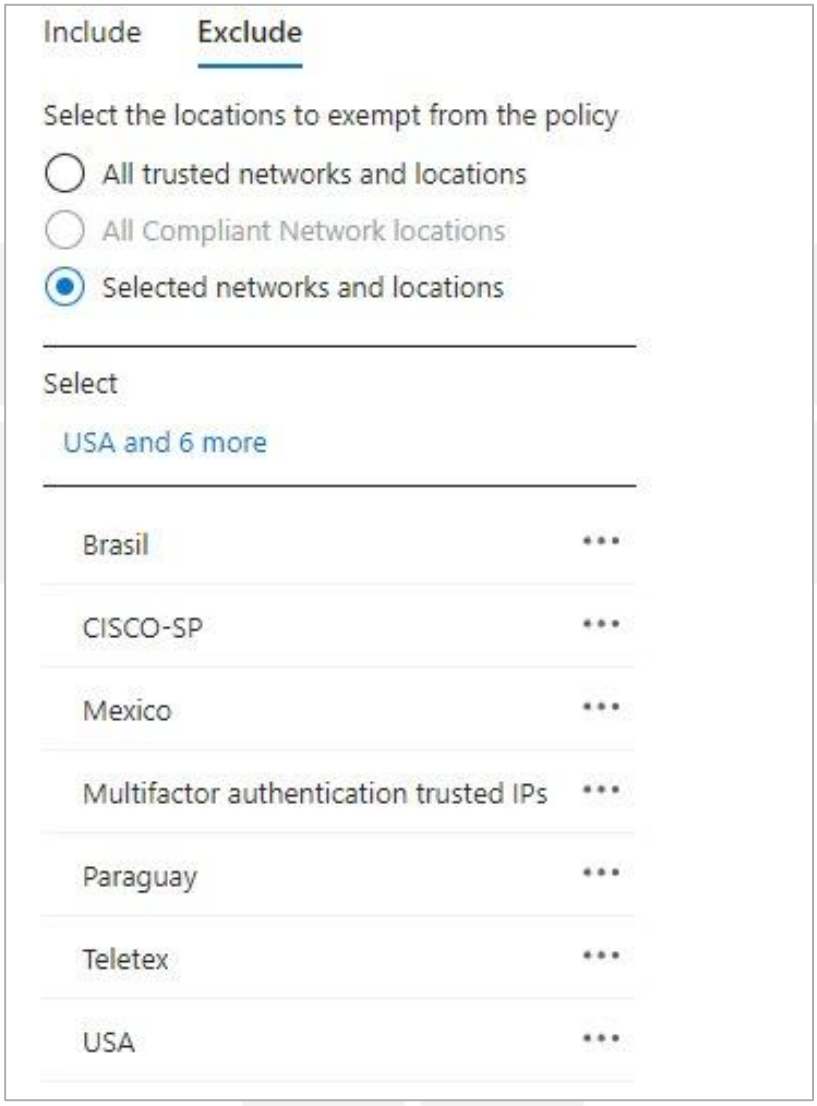
Devido ao uso do protocolo SAML, um cookie 'surrogate' é utilizado, permitindo a extração do endereço IP de origem do cliente. Com essa informação, o IdP pode criar regras de geolocalização, bloqueando ou permitindo a autenticação do usuário, controlando assim o acesso.

Exemplo de extração do endereço IP do cookie no serviço entraID:

Condicional:

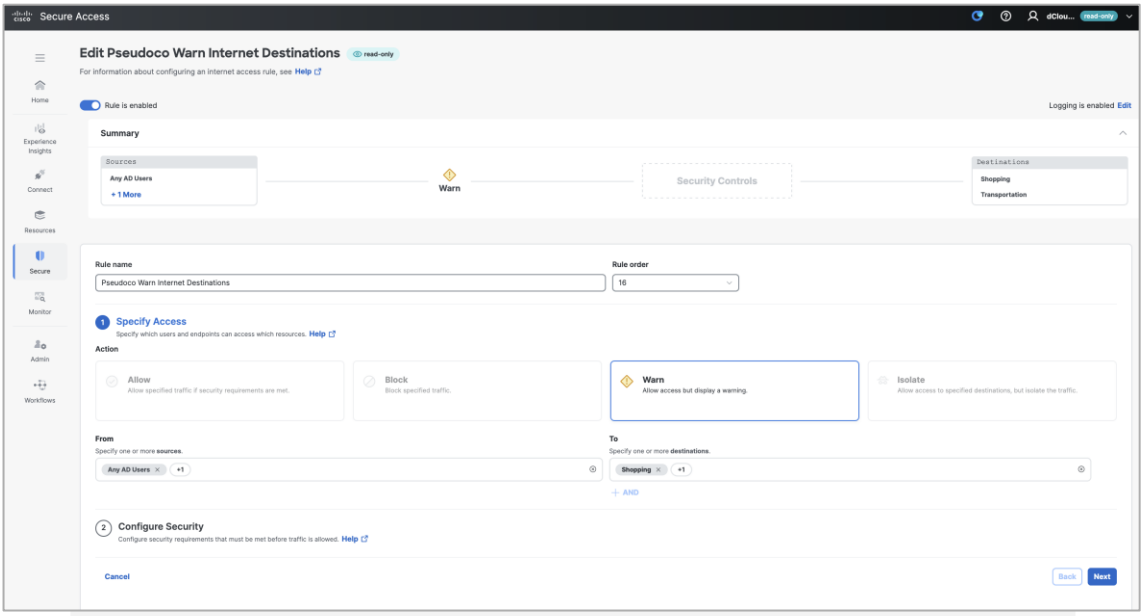


Regra por Geolocaiton, exemplo com permissão:

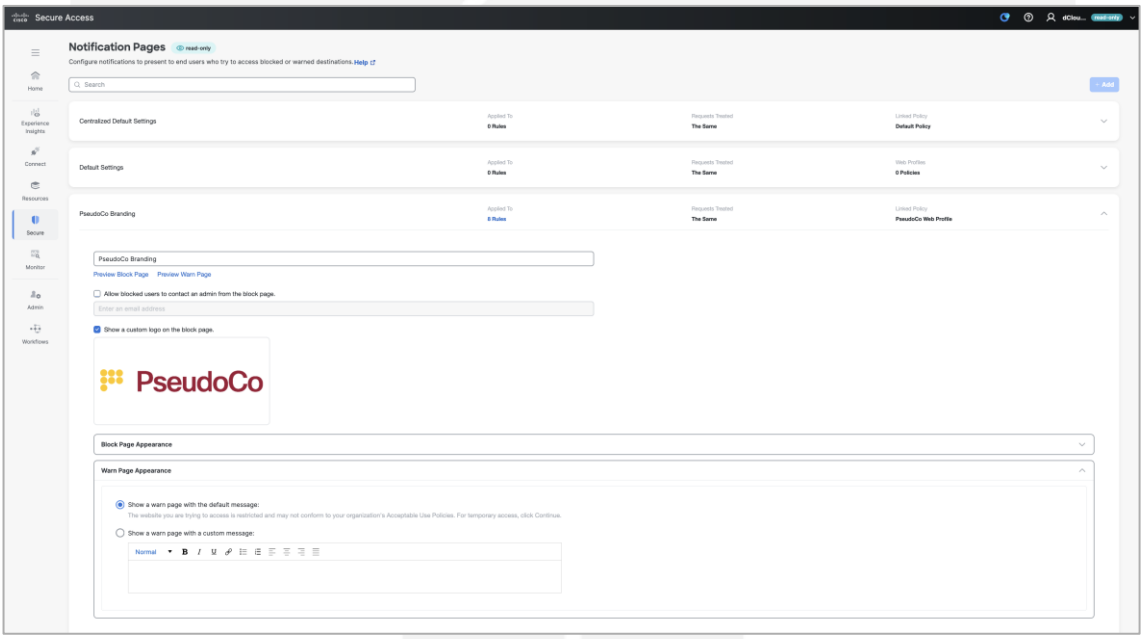


G) ITEM 3.3.2

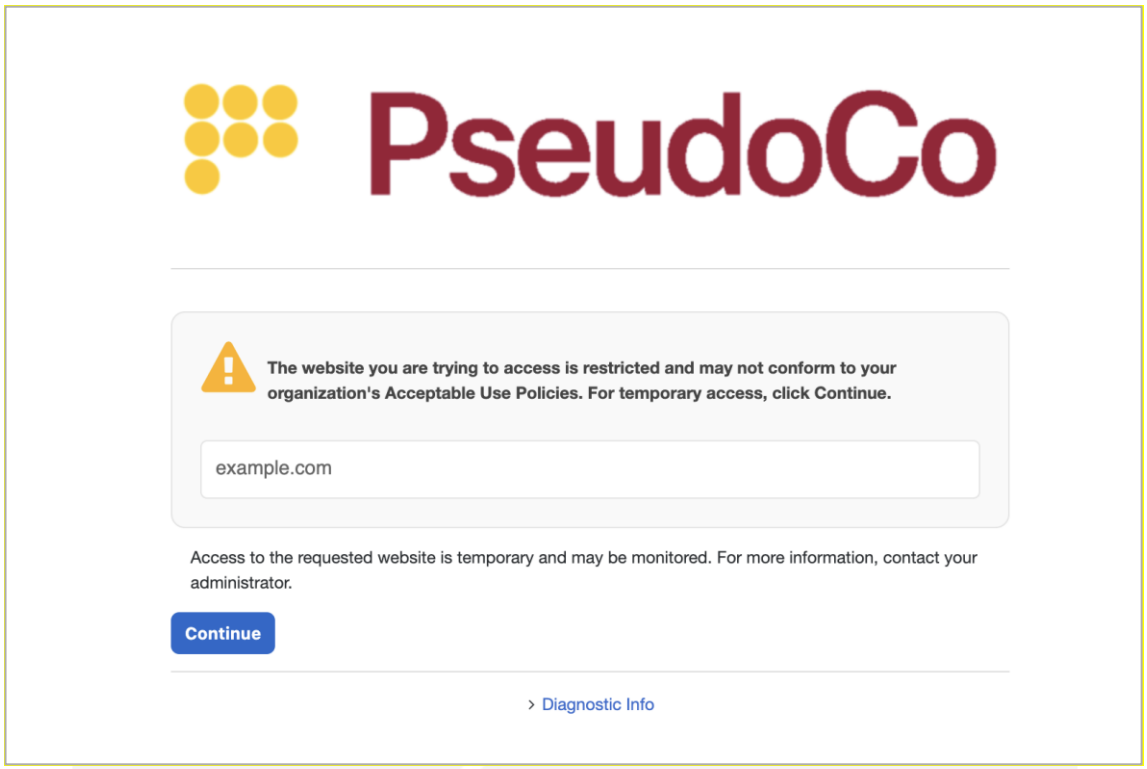
Conforme indicado claramente na documentação comprobatória, as ações disponíveis para regras de acesso internet são exatamente as 4 indicadas no requisito: Bloqueio (Block), Permissão (Allow), Alerta (Warn), e Isolamento (Isolate). A tela abaixo é um exemplo de construção de regra com ação de Alerta (Warn), que envia uma tela de alerta ao usuário e permite que ele continue.



Além disso, as páginas de Alerta, assim como de Block, são customizáveis, conforme abaixo:



O resultado é uma tela similar à abaixo:



O tráfego encaminhado para proxy (SWG) se refere a apenas os protocolos HTTP e HTTPS, que, por padrão, usam as portas 80 e 443. O tráfego nessas portas é enviados por padrão para a camada de proxy do Cisco Secure Access. Isso pode ser confirmado na documentação pública abaixo:

https://docs.sse.cisco.com/sse-user-guide/docs/configure-cisco-secure-client-settings#configure-dns-and-web-security-settings

> "The Cisco Secure Client with the Umbrella Roaming Security module steers web traffic on ports 80/443 to the Secure Web Gateway (SWG). All web traffic is evaluated against the organization's policy and Internet Access rules when a VPN connection is not established."

O uso de portas em proxies deve, por boas práticas de segurança, ser restrito. Levando isso em consideração, a Cisco deixa como opção a inclusão de quaisquer outras portas a partir do atendimento de suporte da solução. Uma vez configuradas as portas adicionais definidas pelo administrador, o tráfego HTTP(S) que as use, além das portas padrão (80, 443) são automaticamente encaminhadas para a camada de proxy da solução.

Outros protocolos não-HTTP, que usem outras portas, são tratados na camada de firewall/IPS da solução, com identificação e inspeção de milhares de aplicações L7 e possibilidade de regras com base nelas. A documentação comprobatória indica esse caso de uso.

H) Requisito 3.5.10

O software Cisco Secure Client, parte integrante da solução Cisco Secure Access é um agente unificado, multi-modular, com diferentes módulos sendo usados para diferentes funções ou camadas da solução. A Cisco renomeou o cliente anterior (Anyconnect) para Secure Client, mantendo o nome Anyconnect apenas para a porção VPN do cliente. O datasheet https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-mobility-client-ds.html mostra essa evolução.

Abaixo a lista dos principais módulos do Secure Client usados no produto Cisco Secure Access:

- DNS/SWG – Módulo herdado do Cisco Umbrella para encaminhamento do tráfego DNS e Proxy em desktops/laptops. Suportado em Windows e Mac. O link https://docs.sse.cisco.com/sse-user-guide/docs/manage-cisco-secure-client-internet-security dá mais detalhes e mostra como parte integrante do Cisco Secure Access. O tratamento para tráfego internet em dispositivos IOS e Android é feito conforme indicado nos links abaixo:

  - IOS - https://docs.sse.cisco.com/sse-user-guide/docs/cisco-security-connector-secure-access-setup-guide

  - Android - https://docs.sse.cisco.com/sse-user-guide/docs/android-client

- VPNaaS – Módulo Anyconnect VPN. O mesmo usado pela Cisco em todas as soluções de VPN e suportado em Windows, Mac, Linux, Android e IOS. O link https://docs.sse.cisco.com/sse-user-guide/docs/manage-virtual-private-network-on-cisco-secure-client mostra o módulo como parte do Cisco Secure Access. Mais detalhes de plataformas suportadas podem ser verificados no documento https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-mobility-client-ds.html#:~:text=Remote-Access%20VPN

- ZTA – Módulo para encaminhamento de tráfego ZTNA. Suportado em Windows e Mac. O link https://docs.sse.cisco.com/sse-user-guide/docs/manage-zero-trust-on-cisco-secure-client mostra o módulo como parte integrante do Cisco Secure Access e dá mais detalhes.

O tratamento de ZTNA em IOS e Android é feito com APPs específicos. O link https://docs.sse.cisco.com/sse-user-guide/docs/manage-client-based-zero-trust-access-mobile-devices mostra esses APPs como parte integrante do Cisco Secure Access e dá mais detalhes.

Outra fonte de informação pode ser o datasheet da solução Cisco Secure Access:

Stio 1: https://www.cisco.com/c/en_uk/products/collateral/security/hybrid-workforce-cloud-agile-security-ds.html#Packagingoptions

4. DA JURISPRUDÊNCIA APLICÁVEL E DOUTRINA PERTINENTE

Considerando o tanto apresentado, relaciona-se a seguinte

jurisprudência:

> "(...) Deveras, **o princípio da isonomia possui cunho eminentemente constitucional e deve ser plenamente respeitado pela Administração Pública.** Em tema de licitação, os princípios da competitividade e isonomia estão permanentemente vinculados". (STJ. Decisão Monocrática. Relator (a): Francisco Falcão. Data de publicação: 17/11/2022.)

> ADMINISTRATIVO. MANDADO DE SEGURANÇA. LICITAÇÃO. PREGÃO ELETRÔNICO. JUNTADA POSTERIOR DE DOCUMENTO FALTANTE. HABILITAÇÃO. POSSIBILIDADE. VINCULAÇÃO AO EDITAL. FORMALISMO MODERADO. ISONOMIA. VIOLAÇÃO. INOCORRÊNCIA. DESPROVIMENTO. 1. **A vinculação ao instrumento licitatório é um dos princípios que regem as licitações. A partir dele, tem-se que o edital é a "lei da licitação" e, portanto, as regras lá estabelecidas devem ser seguidas tanto pela Administração quanto pelos licitantes, assegurando-se a legalidade, a transparência e a isonomia no procedimento licitatório.** 2. No entanto, sem descuidar das regras estabelecidas no edital, o atuar a **Administração Pública deve ser regido pelo princípio do formalismo moderado**, o qual, inclusive, restou positivado no art. 12 da Lei 13.144/2021. "O edital não é o fim em si mesmo" (Acórdão 1211/2021 - PLENÁRIO, julgado em sessão de 26/05/2021). **3. No caso dos autos, o objetivo da exigência (comprovação da capacidade econômico-financeira do licitante) poderia ser atingido mediante análise do documento já apresentado (Balanço Patrimonial e Demonstrações Contábeis do Exercício de 2022) no momento previsto no edital.** Assim, o documento faltante (Balanço Patrimonial e Demonstrações Contábeis do Exercício de 2021) referia-se a condição atendida pelo licitante quando apresentou sua proposta (condição

> pré-existente), razão pela qual permitir sua juntada posterior não fere os princípios da isonomia e igualdade entre as licitantes e, tampouco, de vinculação ao instrumento convocatório. 4. A desclassificação do licitante, sem que lhe fosse conferida oportunidade para sanear os seus documentos de habilitação, é que resultaria em objetivo dissociado do interesse público, especialmente quando apresentada a proposta mais vantajosa à Administração Pública. 5. Apelo desprovido. (TRF4. Acórdão. Processo nº 5001563-53.2024.4.04.7113. Órgão Julgador: 3ª Turma. Relator (a): Roger Raupp Rios. Data do julgamento: 03/02/2025.)

Nessa perspectiva, o Tribunal de Contas da União (TCU) tem reiteradamente decidido que o descumprimento de disposições editalícias enseja a **desclassificação** das propostas que não atendam aos requisitos exigidos. Logo, a ausência de elementos de irregularidade da **TELETEX**, requerem, senão outra senão o reconhecimento do atendimento integral das condições do Edital. Assim se manifesta a jurisprudência, corroborando para o entendimento:

> REPRESENTAÇÃO. PREGÃO ELETRÔNICO. FORNECIMENTO E INSTALAÇÃO DE CABEAMENTO ESTRUTURADO. AUSÊNCIA DE CERTIFICAÇÃO DA ANATEL. APROVAÇÃO DE SOLUÇÃO TECNOLÓGICA VEDADA NO EDITAL. CONHECIMENTO. AUDIÊNCIA. ACOLHIMENTO DAS RAZÕES DE JUSTIFICATIVA EM RELAÇÃO AO PRIMEIRO PONTO. (...). 10. Quanto à aceitação de solução diversa da especificada no item 5.14.5 do Termo de Referência do certame, item 'b' da oitiva, no qual a Caixa alega ser adequada aos objetivos da contratação e que a especificação inserta no instrumento convocatório não atenderia ao objetivo definido no subitem 1.1.3 do edital, quanto ao estabelecimento de uma infraestrutura compatível com diversos equipamentos

(flexibilidade), pois representaria solução proprietária de uma única empresa fabricante, cumpre consignar que:

a) o edital é a lei interna da licitação, fixa as condições para participação dos licitantes e deve conter, obrigatoriamente, as especificações suficientes e necessárias à caracterização do objeto pretendido;

b) em observância ao princípio da vinculação ao instrumento convocatório, as exigências editalícias devem ser cumpridas integralmente, ressalvadas as consideradas ilegais (...) (TCU - RP: 03032420149, Relator: JOSÉ MUCIO MONTEIRO, Data de Julgamento: 09/03/2016, Plenário)

REPRESENTAÇÃO. POSSÍVEIS IRREGULARIDADES EM PREGÃO ELETRÔNICO. CONHECIMENTO. OITIVA PRÉVIA. DILIGÊNCIA. PROCEDÊNCIA. MEDIDA CAUTELAR PREJUDICADA. DETERMINAÇÃO. MONITORAMENTO. ARQUIVAMENTO. Análise: 9. Em relação ao principal motivo da desclassificação alegado, que diz respeito ao não atendimento das exigências do ato convocatório. (TCU - RP: 03808320191, Relator: RAIMUNDO CARREIRO, Data de Julgamento: 18/03/2020, Plenário).

Ainda, entende o Superior Tribunal de Justiça (STJ):

"(...) Cumpre asseverar que, consoante dispõe o art. 41 da Lei 8.666/93, a **Administração e demais participantes encontram-se estritamente vinculados ao edital de licitação**, não podendo descumprir as normas e condições dele constantes. (...)

A propósito, "**A Administração Pública não pode descumprir as normas legais, tampouco as condições editalícias**, tendo em vista o princípio da vinculação ao instrumento convocatório (Lei 8.666/93, art. 41)". (REsp n. 797.170/MT,

relatora Ministra Denise Arruda, Primeira Turma, julgado em 17/10/2006, DJ de 7/11/2006, p. 252.) (...)

É o instrumento convocatório que dá validade aos atos administrativos praticados no curso da licitação, de modo que o descumprimento às suas regras deverá ser reprimido". (STJ. Decisão Monocrática. Processo nº 1066977-60.2021.8.26.0053. Relator (a): Ministro Mauro Campbell Marques. Data de publicação: 07/09/2023.)

O principal objetivo da licitação é selecionar a proposta mais vantajosa para a Administração. Os princípios, sejam expressos ou implícitos em lei, encontram fundamento no art. 3º da Lei nº 8.666/1993, que enumera os princípios norteadores do procedimento licitatório, dentre os quais se destaca a garantia de observância do princípio constitucional da isonomia e a escolha da proposta mais vantajosa para a Administração. Estabelece o dispositivo legal que:

"A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração, sendo 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.**"

Por isso, entende o Professor Hely Lopes Meirelles:

"(...) a igualdade entre os licitantes é o princípio primordial da licitação agora previsto na própria Constituição da República (art.37, XXI), pois não pode haver procedimento seletivo com discriminação entre participantes, ou com cláusulas

> do instrumento convocatório que afastem eventuais proponentes qualificados ou os desnivelem no julgamento"[3].

Imperioso, portanto, que sejam observados os princípios que regem o procedimento licitatório. Quanto ao princípio da vinculação ao instrumento convocatório, a desclassificação das propostas que desatendem a critérios previamente definidos é impositiva.

Remete-se às palavras do jurista Lucas Rocha Furtado, Procurador do Ministério Público Federal junto ao Tribunal de Contas da União, sobre a vinculação da Administração ao Edital de licitação:

> "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."[4]

Reverbera o mesmo entendimento a jurisprudência pátria sobre a aplicação do princípio da vinculação ao edital, conforme julgado do Superior Tribunal de Justiça:

> ADMINISTRATIVO. LICITAÇÃO. CONSÓRCIO DE EMPRESAS. LEGITIMIDADE. SÚMULAS 5 E 7/STJ. REGRAS DO EDITAL. INTERPRETAÇÃO. IMPOSSIBILIDADE. SÚMULAS 5 E 7/STJ. DIVERGÊNCIA JURISPRUDENCIAL. AUSÊNCIA DE COTEJO ANALÍTICO. [...] 4. Na salvaguarda do procedimento licitatório, exsurge o princípio da vinculação,

[3] **MEIRELLES**, Hely Lopes. Licitação e contrato administrativo. 11 ed ver e atual. São Paulo: Malheiros, 1996.

[4] **FURTADO**, Lucas Rocha, *Curso de Direito Administrativo, 2007, p.416*

previsto no art. 41, da Lei 8.666/90, que tem como escopo vedar à administração o descumprimento das normas contidas no edital. Sob essa ótica, o princípio da vinculação se traduz na regra de que o instrumento convocatório faz lei entre as partes, devendo ser observados os termos do edital até o encerramento do certame. (Processo: AgRg no AREsp 458436 RS 2014/0001002-0. Relator(a): Ministro HUMBERTO MARTINS. Publicação: DJe 02/04/2014).

Dessa maneira, a Recorrida pugna pelo total improvimento do recurso ofertado pela **ARVVO.**

5. DO REQUERIMENTO

Por todo o exposto, respeitosamente, a Recorrida requer:

i. **o recebimento e o conhecimento** das presentes contrarrazões, por ser tempestivo e cumprir todos os requisitos legais e editalícios;

ii. **desprovimento integral do recurso administrativo ofertado pela ARVVO** e

iii. e, por fim, decisão final observe os **princípios** norteadores do procedimento licitatório, em especial os da **legalidade, supremacia do interesse público, vinculação ao edital** e **julgamento objetivo.**

Nestes termos, pede deferimento.

Curitiba, 27 de março de 2025.

MARIA DA CONCEICAO OLIVEIRA SILVA:66500630106

Assinado de forma digital por MARIA DA CONCEICAO OLIVEIRA SILVA:66500630106
Dados: 2025.03.27 23:52:14 -03'00'

TELETEX COMPUTADORES E SISTEMAS LTDA.

Maria da Conceição Oliveira Silva

Representante