



Análise de Processo Licitatório  
Firewall

ITEM	COMPROVAÇÃO NTSEC	CONTESTAÇÃO NCT	ATENDIMENTO
<b>1. ITEM 01 - MÓDULO DE SEGURANÇA (CLUSTER) - TIPO I - CARACTERÍSTICAS FÍSICAS E DEPERFORMANCE MÍNIMAS PARA CADA EQUIPAMENTO (...)</b>			
1.18. Deve suportar, no mínimo, 1.800 (mil e oitocentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim; - Grifos e destaques nossos.	Validar processo de entrega das licenças Segue link da comprovação pública <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>	A recorrida não comprovou com documentação PÚBLICA DO FABRICANTE que as soluções ofertadas atendem aos quantitativos mínimos de túneis de VPN previstos nos Itens 1.18, 2.13 e 3.9 do Caderno de Especificações Técnicas, requer-se seja reconhecido o não atendimento do Edital.	A licitante NTSEC atendeu a exigência, a comprovação foi realizada por meio do acesso por meio da consulta ao link de comprovação: <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>
<b>2. ITEM 02 - MÓDULO DE SEGURANÇA DO - TIPO II - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCEMÍNIMAS PARA CADA EQUIPAMENTO (...)</b>			
2.13. Deve suportar, no mínimo, 1.000 (mil) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim; O equipamento deverá ter homologação da Agência Nacional de Telecomunicações (ANATEL), exigência a ser comprovada por meio da apresentação pela Licitante do certificado quanto da entrega dos documentos de habilitação. - Grifos e destaques nossos.	Validar processo de entrega das licenças  <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>	A recorrida não comprovou com documentação PÚBLICA DO FABRICANTE que as soluções ofertadas atendem aos quantitativos mínimos de túneis de VPN previstos nos Itens 1.18, 2.13 e 3.9 do Caderno de Especificações Técnicas, requer-se seja reconhecido o não atendimento do Edital.	A licitante NTSEC atendeu a exigência através da documentçãõ publicada no link de comprovação. Link: <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>
<b>3. ITEM 03 - MÓDULO DE SEGURANÇA DO - TIPO III - CARACTERÍSTICAS FÍSICAS E DE PERFORMANCEMÍNIMAS PARA CADA EQUIPAMENTO (...)</b>			
3.9. Deve suportar, no mínimo, 500 (quinhentos) túneis de VPN client to site simultaneamente, estando devidamente licenciado para este fim; - Grifos e destaques nossos.	Validar processo de entrega das licenças  <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>	A recorrida não comprovou com documentação PÚBLICA DO FABRICANTE que as soluções ofertadas atendem aos quantitativos mínimos de túneis de VPN previstos nos Itens 1.18, 2.13 e 3.9 do Caderno de Especificações Técnicas, requer-se seja reconhecido o não atendimento do Edital.	A licitante NTSEC atendeu a exigência através da documentçãõ publicada no link de comprovação. Link: <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>
<b>4. ITEM 04 - FUNCIONALIDADES GERAIS DOS MÓDULOS DE SEGURANÇA TIPO I, TIPO II e TIPO III</b>			
4.8. Deve implementar Network Prefix Translation (NPTv6), NAT66 ou similar que traduza prefixos de endereços de rede IPv6;	<a href="https://support.checkpoint.com/results/sk/sk163313">https://support.checkpoint.com/results/sk/sk163313</a>	A planilha apresentada pela NTSEC indica que a comprovação de atendimento ao item está no documento “Quantum Security Management R81.20 Administration Guide”, mais especificamente, na página 275. No entanto, em consulta a esse documento (disponível em: <a href="https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/125834/FILE/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf">https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/125834/FILE/CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf</a> ), não foi possível confirmar a informação sobre a exigência de NAT66 ou similar que traduza prefixos IPv6	A licitante NTSEC atendeu a exigência através da documentçãõ publicada no link de comprovação. Link: <a href="https://support.checkpoint.com/results/sk/sk84560">https://support.checkpoint.com/results/sk/sk84560</a>
4.25.3. As configurações de perfis de SD-WAN devem partir de um ponto central permitindo alteração e criação dos elementos primordiais para o funcionamento da solução. Deve também entregar a criação automática dos túneis IPSEC entre as localidades.	<a href="#">Quantum SD-WAN Administration Guide</a>	Seguindo, em relação aos itens 4.25.3 a 4.25.8, os quais tratam das especificações técnicas do SD-WAN, é preciso mencionar que nenhuma das páginas indicadas pela Recorrida na sua planilha faz menção às comprovações de tais requisitos técnicos.	A licitante NTSEC atendeu a exigência através da documentçãõ anexada. Documento: Quantum SD-WAN Administration Guide
4.25.8. SD-WAN deve suportar os seguintes tipos de conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite desde que a sua terminação permita conectividade com interfaces ethernet.	<a href="https://resources.checkpoint.com/net-work-security/quantum-sd-wandatasheet">https://resources.checkpoint.com/net-work-security/quantum-sd-wandatasheet</a>	Seguindo, em relação aos itens 4.25.3 a 4.25.8, os quais tratam das especificações técnicas do SD-WAN, é preciso mencionar que nenhuma das páginas indicadas pela Recorrida na sua planilha faz menção às comprovações de tais requisitos técnicos.	A licitante NTSEC atendeu a exigência através da documentçãõ publicada no link de comprovação. Link: <a href="https://resources.checkpoint.com/network-security/quantum-sd-wandatasheet">https://resources.checkpoint.com/network-security/quantum-sd-wandatasheet</a>
4.26.13. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;	<a href="https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.htm">https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.htm</a>	Nesse ponto, destaca-se que o primeiro requisito mencionado, Item 4.26.13, não foi comprovado pela NTSEC, uma vez que, aparentemente, a solução não possui bloqueio por política de firewall.	A licitante NTSEC atendeu a exigência através da documentçãõ publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.htm">https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.htm</a>

4.26.18. Deve possuir ferramenta que indique as regras sobrepostas e objetos não utilizados para otimização das regras. Caso não possua essa funcionalidade será permitido a integração com ferramentas que executam esta função.	<a href="https://support.checkpoint.com/results/sk/sk161575">https://support.checkpoint.com/results/sk/sk161575</a>	Em relação à segunda exigência, Item 4.26.18, mais uma vez a Recorrida se limita a mencionar que a sua solução está “de acordo” com a exigência do edital, sem, no entanto, informar em qual documento pode ser comprovado que a solução consegue fazer a verificação de regras sobrepostas e objetos não utilizados para otimização das regras.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://support.checkpoint.com/results/sk/sk161574">https://support.checkpoint.com/results/sk/sk161574</a>
4.27.6. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estiverem sendo trafegados através de aplicações como: Dropbox-uploading, filedropper e outros.	<a href="https://appwiki.checkpoint.com/appwikisdb/public.htm">https://appwiki.checkpoint.com/appwikisdb/public.htm</a>	<p>No que tange o controle de aplicações, o Item 4.27.6 exige que a solução de controle de dados permita o inspecionamento e a prevenção do vazamento de arquivos, mesmos quando eles estiverem sendo trafegados através de aplicações como “dropbox-uploading, filedropper e outros”.</p> <p>Para comprovar o atendimento ao requisito mencionado, a Recorrida indicou a página 201 do documento “Quantum Security Management R81.20 Administration Guide”, cujo texto seria o seguinte:</p> <p>The Content Awareness Software Blade supports HTTP, HTTPS, SMTP, and FTP protocols on all ports. It is fully integrated with the Access Control unified Rule Base. Traffic over QUIC and WebSocket is not inspected. You can use 'Quic protocol' / 'WebSocket protocol' in a new Application rule to Drop or Allow this traffic.HTTP connections that are not RFC-compliant are not inspected.</p> <p>Em tradução livre, o texto utilizado como comprovação diz que:</p> <p>O Content Awareness Software Blade oferece suporte aos protocolos HTTP, HTTPS, SMTP e FTP em todas as portas. Ele está totalmente integrado à Regra Base Unificada de Controle de Acesso. O tráfego sobre QUIC e WebSocket não é inspecionado. Você pode usar o 'Protocolo Quic' / 'Protocolo WebSocket' em uma nova regra de aplicativo para bloquear ou permitir esse tráfego.</p> <p>Conexões HTTP que não estão em conformidade com o RFC não são inspecionadas.</p> <p>Assim, do texto indicado pela própria Recorrida, a solução só é capaz de inspecionar e prevenir vazamento de arquivos mesmos quando estiverem sendo trafegados; contudo, não há comprovação de que inspecionar e prevenir o vazamento de dados através das aplicações dropbox-uploading, filedropper e outros.</p> <p>Dito isso, resta evidenciado que a NTSEC não atende ao instrumento convocatório do certame.</p>	A funcionalidade é atendida através da blade de segurança Content-Awareness, presente no firewall da Check Point em conjunto com a blade Application Control, nesse link, <a href="https://appwiki.checkpoint.com/appwikisdb/public.htm">https://appwiki.checkpoint.com/appwikisdb/public.htm</a> , é indicado publicamente todas as aplicações padrões disponíveis. Sobre o Content Awareness segue documento que demonstra suas capacidades, <a href="https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.html">https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Content-Awareness-Blade.html</a>
4.28. PREVENÇÃO DE AMEAÇAS			
4.28.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado com a última base de assinatura instalada no momento em que a licença expirou, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.	<a href="https://support.checkpoint.com/results/sk/sk44175">https://support.checkpoint.com/results/sk/sk44175</a> - Conforme informações no site do fabricante, após o encerramento do contrato, o cliente não permanece com a última base atualizada, a mesma passará a utilizar assinaturas criadas até 2009.	No documento de comprovação fica claro que após o final da garantia todas as assinaturas são DESABILITADAS, restando, apenas, assinaturas anteriores a 2009. Isso significa que, de 2009 até a data de expiração, não haverá nenhuma assinatura ativa, descumprindo o exigido de manter as assinaturas até a data da expiração.	A licitante NTSEC atende as exigências solicitadas.
4.28.10. Deverá possuir os seguintes mecanismos de inspeção de IPS:			
a) Análise de padrões de estado de conexões;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.
b) Análise de decodificação de protocolo;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 34
c) Análise para detecção de anomalias de protocolo;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 35
d) Análise heurística;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 36
e) IP Defragmentation;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 37
f) Remontagem de pacotes de TCP;	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 38

g) Bloqueio de pacotes malformados.	CP_R81.20_ThreatPrevention_AdminGuide.pdf	Contudo, a despeito no que consta na planilha supramencionada, os itens acima não foram atendidos, nota-se, pelo texto citado, que ao final do prazo contratado, a funcionalidade de IPS restará se apresentará defasada.	A licitante NTSEC atendeu a exigência através da documentção.  Documento: Threat Prevention R81.20 Administration Guide Pg. 31 e Pg. 39
4.28.14. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;	CP_R81.20_ThreatPrevention_AdminGuide.pdf  <a href="https://www.checkpoint.com/downloads/products/intrusion-prevention-system-ips-datasheet.pdf">https://www.checkpoint.com/downloads/products/intrusion-prevention-system-ips-datasheet.pdf</a>  <a href="https://www.checkpoint.com/downloads/products/IPS_Engine_Architecture.pdf">https://www.checkpoint.com/downloads/products/IPS_Engine_Architecture.pdf</a>	Destaca-se também que o texto apontado no item 4.28.14 apenas cita a capacidade de mais de 1000 assinaturas de comportamento, mas não aponta, como deveria ter sido feito, os mecanismos de inspeção contra ameaças ou características que denotam o atendimento. Portanto, resta demonstrado que o produto ofertado é de qualidade inferior àquela exigida no Edital.	A licitante NTSEC atendeu a exigência através da documentção. Documento: Threat Prevention R81.20 Administration Guide Pg. 31  e  Adicionalmente segue os documentos de datasheet e IPS Engine Architecture que traz mais detalhes sobre as capacidades solicitadas, <a href="https://www.checkpoint.com/downloads/products/intrusion-prevention-system-ipsdatasheet.pdf">https://www.checkpoint.com/downloads/products/intrusion-prevention-system-ipsdatasheet.pdf</a> , pagina 1 e IPS_Engine_Architecture.pdf (checkpoint.com), pagina 7
4.28.15. Possuir assinaturas específicas para a mitigação de ataques DoS;	<a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a>	Continuando a série de desatendimentos da NTSEC, os itens 4.28.15 e 4.28.16 exigem que a solução seja capaz de possuir assinaturas “específicas para a mitigação de ataques DoS” e “para bloqueio de ataques de buffer overflow”. Para comprovar que as assinaturas atendem ao exigido, a Recorrida indicou o seguinte link (disponíveis em: <a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a> ):  No entanto, as assinaturas apontadas acima não comprovam mitigação de bloqueio para ataques específicos de DoS e Buffer, ou seja, a solução não tem capacidade de proteção contra DoS, violando, portanto, exigência específica do instrumento convocatório.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a>
4.28.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;	<a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a>	Continuando a série de desatendimentos da NTSEC, os itens 4.28.15 e 4.28.16 exigem que a solução seja capaz de possuir assinaturas “específicas para a mitigação de ataques DoS” e “para bloqueio de ataques de buffer overflow”. Para comprovar que as assinaturas atendem ao exigido, a Recorrida indicou o seguinte link (disponíveis em: <a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a> ):  No entanto, as assinaturas apontadas acima não comprovam mitigação de bloqueio para ataques específicos de DoS e Buffer, ou seja, a solução não tem capacidade de proteção contra DoS, violando, portanto, exigência específica do instrumento convocatório.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://advisories.checkpoint.com/advisories/page/2/">https://advisories.checkpoint.com/advisories/page/2/</a>
4.28.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;	Threat Prevention R81.20 Administration Guide e <a href="https://advisories.checkpoint.com/security-advisories-subscription/">https://advisories.checkpoint.com/security-advisories-subscription/</a>	Em relação ao Item 4.28.17, o Caderno de Especificações Técnicas prevê que a solução “deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto”. No texto indicado pela Recorrente em sua planilha, consta que “Check Point supports the use of SNORT rules as both the GUI and the SmartDomain Manager API's options. When you import a SNORT rule, it becomes a part of the IPS database. To perform these actions on a Check Point Management Server”. Em tradução livre, a comprovação da NTSEC apenas prevê que a solução “suporta o uso de regras snort (...)”. Isso é importante na medida em que o item é claro ao exigir que a solução permita a criação de regra via console e, não, somente a importação de regras de outro tipo de solução, visto que nesse segundo caso, não há possibilidade de customizar uma assinatura no Security Management Server do CheckPoint. Tem-se, portanto, mais uma violação das exigências previstas no Edital.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://advisories.checkpoint.com/security-advisories-subscription/">https://advisories.checkpoint.com/security-advisories-subscription/</a>
<b>4.34.12. A solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site para no mínimo as seguintes opções:</b>			
a) Sistema operacional;	<a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a>	O Item 4.34.12 prevê que “a solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site” para, no mínimo, sistema operacional, antivírus instalado, firewall no host, chaves de registro e processos ativos.  Segundo informações extraídas da planilha apresentada pela Recorrida, todas as comprovações estariam nas páginas 80 a 85 do documento “Remote Access VPN R81.20 Administration Guide”.  Bem, acessando o documento mencionada para conferir os argumentos trazidos pela NTSEC (disponível em: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm</a> ), é possível confirmar que a solução SCV não é suportada no SecuRemote.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a>
b) Antivírus instalado;	<a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a>	O Item 4.34.12 prevê que “a solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site” para, no mínimo, sistema operacional, antivírus instalado, firewall no host, chaves de registro e processos ativos.	A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a>

c) Firewall no host;	<a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____4">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____4</a>	<p>O Item 4.34.12 prevê que “a solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site” para, no mínimo, sistema operacional, antivírus instalado, firewall no host, chaves de registro e processos ativos.</p> <p>Segundo informações extraídas da planilha apresentada pela Recorrida, todas as comprovações estariam nas páginas 80 a 85 do documento “Remote Access VPN R81.20 Administration Guide”.</p> <p>Bem, acessando o documento mencionada para conferir os argumentos trazidos pela NTSEC (disponível em: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm</a>), é possível confirmar que a solução SCV não é suportada no SecuRemote.</p>	<p>A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a></p>
d) Chaves de registros (quando aplicável);	<a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____5">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____5</a>	<p>O Item 4.34.12 prevê que “a solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site” para, no mínimo, sistema operacional, antivírus instalado, firewall no host, chaves de registro e processos ativos.</p> <p>Segundo informações extraídas da planilha apresentada pela Recorrida, todas as comprovações estariam nas páginas 80 a 85 do documento “Remote Access VPN R81.20 Administration Guide”.</p> <p>Bem, acessando o documento mencionada para conferir os argumentos trazidos pela NTSEC (disponível em: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm</a>), é possível confirmar que a solução SCV não é suportada no SecuRemote.</p>	<p>A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a></p>
e) Processos ativos.	<a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____6">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____6</a>	<p>O Item 4.34.12 prevê que “a solução de VPN client-to-site deve estar devidamente licenciada para criar perfis customizados de conformidade dos clientes das VPNs clien-to-site” para, no mínimo, sistema operacional, antivírus instalado, firewall no host, chaves de registro e processos ativos.</p> <p>Segundo informações extraídas da planilha apresentada pela Recorrida, todas as comprovações estariam nas páginas 80 a 85 do documento “Remote Access VPN R81.20 Administration Guide”.</p> <p>Bem, acessando o documento mencionada para conferir os argumentos trazidos pela NTSEC (disponível em: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/SCV.htm</a>), é possível confirmar que a solução SCV não é suportada no SecuRemote.</p>	<p>A licitante NTSEC atendeu a exigência através da documentção publicada no link de comprovação. Link: <a href="https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2">https://sc1.checkpoint.com/documents/RemoteAccessClients_forWindows_AdminGuide/Content/Topics-RA-VPN-for-Win/Check-Point-SCV-Checks.htm?tocpath=Secure%20Configuration%20Verification%20(SCV)%7C____2</a></p>