Visualização de Recursos, Contra-Razões e Decisõess

CONTRA RAZÃO :

ILUSTRÍSSIMA SRA. PREGOEIRA E COMISSÃO DE LICITAÇÃO DA CÂMARA MUNICIPAL DE BELO HORIZONTE
Ref. Contra Razões ao Recurso administrativo do Edital de pregão Eletrônico nº 36/2016.
CONTRARRAZÕES AO RECURSO ADMINISTRATIVO
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA, pessoa jurídica de direito privado, inscrita sob CNPJ de nº 05.250.796/0001-54, situada na Rua Capitão Melo, 3373 – Bairro
220 – Fortaleza/CE, neste ato representada pela sua procuradora Srta. Tatiana Ribeiro Leite, Gerente Comercial Nacional, devidamente qualificada no presente processo vem na f
conformidade ao Art.4º, XVIII da Lei nº 10.520/2002, até Vossa Senhoria, para tempestivamente, interpor nossas CONTRARRAZÕES, ao inconsistente recurso apresentado pela emp
perante essa distinta administração que de forma coerente declarou a contrarrazoante vencedora do processo licitatório em pauta, requerendo conforme o exposto abaixo, a m
recorrida.
1. DAS CONSIDERAÇÕES INCIAIS
Ilustríssima Sra. Pregoeira e Comissão de Licitação da Câmara Municipal de Belo Horizonte.
O respeitável julgamento das contrarrazões interposto recai neste momento para sua responsabilidade, o qual a empresa CONTRARRAZOANTE confia na lisura, na isonomia e na im
julgamento em questão, buscando pela proposta mais vantajosa para esta digníssima administração, onde a todo o momento demostraremos nosso Direito Liquido e Certo e o c
exigências do presente processo de licitação.
2. DOS FATOS
No dia 19 de Setembro de 2016, a empresa RECORRENTE, 4TECH TECOLOGIA LTDA., motivou sua intenção de recurso para o qual usou as seguintes alegativas: Motivo Intenção: A 4
manifestar sua intenção em recorrer da decisão do Pregão Eletrônico nº 36/2016. Nos termos deste edital, item 9, subitem 9.1, apresentaremos a síntese de nossas razões da de
motivação do recurso, iremos versar acerca da incapacidade técnica do proponente NETWORK SECURE SEGURANCA DA INFORMACAO LTDA., CNPJ/CPF: 05.250.796/0001-54, on
atende a todos os requisitos técnicos do edital.
O recurso apresentado pela empresa RECORRENTE, alegando o não cumprimento do edital por parte da CONTRARRAZOANTE, demonstra de forma clara e precisa, o descon
recorrente quanto aos requisitos técnicos aos Produtos/Equipamentos apresentados pela empresa CONTRARRAZOANTE, no qual demonstraremos por fatos, o cumprimento integral a
Segundo a empresa 4TECH TECNOLOGIA LTDA., a empresa CONTRARRAZOANTE deixou de atender aos seguintes requisitos para os quais apresentamos os seguintes esclarecimer
links consultivos, para o inconsistente recurso:
1. A empresa RECORRENTE apontou quanto ao item 4.1.11.18, alegando que a empresa CONTRARRAZOANTE não apresentou a capacidade da solução apresentada trabalhar de f
tipos de implementação conforme site: http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Interfaces/One-armed%20sniffer.htm . in verbis: "O
sniffer is used to configure a physical interface on the FortiGate unit as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the config
control list. Matches are logged and then all received traffic is dropped. Sniffing only reports on attacks. It does not deny or otherwise influence traffic. Using the one-arm sniffer, yo
to operate as an IDS appliance by sniffing network traffic for attacks without actually processing the packets. To configure one-arm IDS, you enable sniffer mode on a FortiGate inte
to a hub or to the SPAN port of a switch that is processing network traffic. To assign an interface as a sniffer interface, go to System > Network > Interface, edit the interface anc
check box is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs or other features in which a physical interface is s
Conforme link acima supracitado, é possível o conhecimento pleno as funcionalidades da solução fornecida, cumprindo-se assim os requisitos do edital e termo de referência ao Iten
recurso da empresa recorrente.
2. Adiante a empresa RECORRENTE aponta quanto ao subitem 4.1.11.18.4, onde alega quanto ao trabalho em modo misto de trabalho Sniffer L2 e L3 em diferentes interfaces, pa
esclarecimentos: Conseguimos implementar os modos L2 e L3 de forma simultânea através do recurso "Virtual Wire Pair" (http://help.fortinet.com/fos50hlp/54/Conte
54/Top_VirtualWirePair.htm). In verbis: Virtual Wire Pair This feature (276013), available in NAT and Transparent mode, replaces the Port Pair feature available in FortiOS 5.2 in Tran
two physical interfaces are setup as a Virtual Wire Pair, they will have no IP addressing and are treated similar to a transparent mode VDOM. All packets accepted by one of the inte
only exit the FortiGate through the other interface in the virtual wire pair and only if allowed by a virtual wire pair firewall policy. Packets arriving on other interfaces cannot be rout
wire pair. A FortiGate can have multiple virtual wire pairs. You cannot add VLANs to virtual wire pairs. However, you can enable wildcard VLANs for a virtual wire pair. This means
pass through the virtual wire pair if allowed by virtual wire pair firewall policies.
Com este recurso é possível implementar um par de portas em modo transparente com o equipamento configurado em modo L3 (NAT mode). Para implementar o terceiro modo sni
L3, basta configurar qualquer interface do equipamento em modo "One-Armed Sniffer", através da configuração de "addressing mode" ind
(http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Interfaces/Interface%20settings.htm). Não há qualquer restrição na operação simultânea de
e L3. In verbis: Interface settings. In System > Network > Interface, you configure the interfaces, physical and virtual, for the FortiGate unit. There are different options for c
FortiGate unit is in NAT mode or transparent mode. On FortiOS Carrier, you can also enable the Gi gatekeeper on each interface for anti-overbilling.
Conforme link supracitado acima, comprovamos nosso atendimento ao subitem 4.1.11.18.4, não prosperando o recurso da empresa recorrente.

3. Logo mais a RECORRENTE aponta quanto ao item 4.2.1, sobre suportar controles por zona de segurança, para esse item prestamos os seguintes esclarecimentos: A compro
seguinte URL http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Interfaces/Zones.htm . In verbis: Zones. Zones are a group of one or more Fo
and virtual, that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security polic
segments can use the same policy settings and protection profiles. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each in
and routing is still done between interfaces, that is, routing is not affected by zones. Security policies can also be created to control the flow of intra-zone traffic. For example, in the
includes three separate groups of users representing different entities on the company network. While each group has its own set of port and VLANs, in each area, they can all us
protection profiles to access the Internet. Rather than the administrator making nine separate security policies, he can add the required interfaces to a zone, and create three
simpler. Network zone. You can configure policies for connections to and from a zone, but not between interfaces in a zone. Using the above example, you can create a security p
zone 3, but not between WAN2 and WAN1, or WAN1 and DMZ1. This example explains how to set up a zone to include the Internal interface and a VLAN. To create a zone - web-bas
Network > Interface.2.Select the arrow on the Create New button and select Zone.3.Enter a zone name of Zone_1.;4.Select the Internal interface and the virtual LAN interface vlan_
5.Select OK.

Conforme link e esclarecimentos acima, comprovamos nosso atendimento ao subitem 4.2.1, não prosperando o recurso da empresa recorrente.

4. Continuando, a RECORRENTE aponta quanto ao subitem 4.3.17, item que trata sobre a permissão nativa a criação de assinaturas personalizadas para reconhecimento de aplic
interface gráfica da solução, para o qual fazemos os seguintes esclarecimentos: "A comprovação deste item encontra na seção "Creating a New Custom Application
http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Enable%20Application%20Control.htm . In verbis:
Enable application control. Application control examines your network traffic for traffic generated by the applications you want it to control. General configuration steps. Follow the
order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results. 1.Create an application sensor. 2.Configure the
for the application traffic you want the FortiGate unit to detect. 3. Enable any other applicable options. 4.Enable application control in a security policy and select the application
sensor. You need to create an application sensor before you can enable application control. To create an application sensor. 1. Go to Security Profiles > Application Control. 2.Select
bar of the Edit Application Sensor window. 3.In the Name field, enter the name of the new application sensor. 4.Optionally, you may also enter a comment. Adding applications to a
have created an application sensor, you need to need to define the applications that you want to control. You can add applications and filters using categories, application ove
Categories will allow you to choose groups of signatures based on a category type. Application overrides allow you to choose individual applications. Filter overrides allow you to se
override the application signature settings for them. To add a category of signatures to the sensor. 1.Go to Security Profiles > Application Control. 2.Under Categories, you may se
Business; Cloud.IT; Collaboration; Email; Game; General.Interest; Mobile; Network.Service; P2P; Proxy; Remote.Access; Social.Media; Storage.Backup; Update; Video/Audio
Applications. When selecting the category that you intend to work with, left click on the icon next to the category name to produce drop down menu that includes these actions: Allo
View Signatures. These actions are briefly defined under Application Control actions. 3.If you wish to add individual applications, select Add Signatures under Application Overrides.
to narrow down the list of possible signatures by a series of attributes.b.When finished, select Use Selected Signatures.4. If you wish to add advanced filters, select Add Filter under
Filter search field to narrow down the list of possible filters by a series of attributes. B.When finished, select Use Filters. 5.Select, if applicable, from the following options: Allow anc
Messages for HTTP-based Applications 6. Select OK. There is a disabled category called Industrial. This category is disabled by default, however it can be applied through use of the
none will mean no signatures are excluded, and that industrial will exclude all industrial signatures. CLI Syntax. config ips global set exclude-signatures [none | industrial] end Crea
Signature If you have to deal with an application that is not already in the Application List you have the option to create a new application signature. 1.Go to Security Profiles > Appli
in the upper right corner, [View Application Signatures]. 3. Select the Create New icon. 4. Give the new signature a name (no spaces) in the Name field.5. Enter a brief description in t
text for the signature in the signature field. Use the rules found in the Custom IPS signature chapter to determine syntax. 7.Select OK. You can configure rate based application contr
using similar IPS signature rate CLI commands. For more information on this and the CLI syntax, see IPS signature rate count threshold. Messages in response to blocked applicatio
sensor has been configured to block a specified application and applied to a policy it would seem inevitable that at some point an application will end up getting blocked, even if it is
the control. When this happens, the sensor can be set to either display a message to offending user or to just block without any notification. The default setting is to display a messag
CLI. config application list edit set app-replacemsg {enable | disable}end. P2P application detection. P2P software tends to be evasive. You may be able to enhance P2P application
found in the most recent three minutes of P2P traffic to determine if new traffic is P2P. Three minutes is the length of time information about matched P2P traffic remains in shared
commands below will result in the Intrusion Prevention System (IPS) looking for patterns formed by Skype traffic. config application list. edit . set p2p-black-list skype. End. End.
Conforme link e descrição acima, esclarecemos e comprovamos o atendimento ao subitem 4.3.17, não prosperando o recurso da empresa recorrente.
5. Para os itens 39 e 40, das razões recursais da RECORRENTE, subitem 4.13.18, a mesma aponta quanto a capacidade da solução em atendimento aos requisitos de upgrade v
seguinte consideração: "A comprovação deste item encontra-se nas seguintes URLs: Interface de gerenciamento: Fonte: http://help.fortinet.com/fos50hlp/54/Content/FortiOS/f
54/Firmware/Upgrading%20the%20firmware%20-%20web-based%20manager.htm . In verbis: Upgrading the firmware - web-based manager Installing firmware replaces you
definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions
http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Firmware/Upgrading%20the%20firmware%20-%20CLI.htm . in verbis: "Upgrading the firmv
replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that
are up to date. You can also use the CLI command execute update-now to update the antivirus and attack definitions. For more information, see the System Administration handbook
have a TFTP server running and accessible to the FortiGate unit."
SCP: A realização de backup da configuração é necessária quando for realizado rocedimento de upload de firmware via TFTP, conforme explica manual na seção "Configuration B
successfully configure the FortiGate, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate to factory defaults or perform
which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it.". O procedimento p
da configuração via SCP está localizado na seção "Backup and restore a configuration file using SCP". URL para consulta é http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortig
Admin/7-configuration-backups.htm?Highlight=SCP
Configuration Backups. Once you successfully configure the FortiGate, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGat
a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be use
backup the local certificates, as the unique SSL inspection CA and server certificates that are generated by your FortiGate by default are not saved in a system backup. It is also rec
configuration after any future changes are made, to ensure you have the most current configuration available. Also, backup the configuration before any upgrades of the FortiGa
happen to the configuration during the upgrade, you can easily restore the saved configuration.
Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, U
last two are configurable through the CLI only. If you have VDOMs, you can back up the configuration of the entire FortiGate or only a specific VDOM. Note that if you are using
backups are performed and the option to backup individual VDOMs will not appear. Backing up the configuration using the GUI. 1. 1.Go to the Dashboard and locate the System Infor
Configuration, select Backup.3.Direct the backup to your Local PC or to a USB key.The USB Disk option will be grayed out if no USB drive is inserted in the USB port. You can also ba
the CLI.4.If VDOMs are enabled, select to backup the entire FortiGate configuration (Full Config) or only a specific VDOM configuration (VDOM Config).5.If backing up a VDOM config
from the list.6.Select Encrypt configuration file.Encryption must be enabled on the backup file to back up VPN certificates. 7.Enter a password and enter it again to confirm it. You wil
the file. 8.Select Backup. 9.The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension. Backing up the confic
following command:

execute backup config management-station ... or ...execute backup config usb []... or for FTP, note that port number, username are optional depending on the FTP site...execute backup
...execute backup config tftp
Use the same commands to backup a VDOM configuration by first entering the commands: config vdom. edit Backup and restore the local certificates
This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server.
running and accessible to the FortiGate before you enter the command. Backing up the local certificates. Connect to the CLI and use the following command: execute vpn certificate
name of the server certificate. • is a name for the output file. • is the IP address assigned to the TFTP server host interface. Restoring the local certificates – GUI. 1.Move the o
location to the management computer. 2.Go to System > Certificates and select Import. 3.Select the appropriate Type of certificate and fill in any required fields. 4.Select Browse
management computer where the exported file has been saved, select the file and select Open. 5.If required, enter the Password needed to upload the exported file. 6.Select OK. F
CLI. Connect to the CLI and use the following command: execute vpn certificate local import tftp Backup and restore a configuration file using SCP. You can use secure copy p
configuration file from the FortiGate as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and adm
SSH on a port used by the SCP client application to connect to the FortiGate. SCP is enabled using the CLI commands: config system global. set admin-scp enable. End Use the same
configuration by first entering the commands: config global. set admin-scp enable. End. config vdom. edit Enable SSH access on the interface. SCP uses the SSH protocol to pı
interface you use for administration must allow SSH access. To enable SSH - GUI: 1.Go to Network > Interfaces. 2.Select the interface you use for administrative access and sele
Access section, select SSH. 4.Select OK. To enable SSH - CLI: config system interface
edit set allowaccess ping https ssh end.

Conforme link e descrito retirado do link supramencionados acima, comprovamos o atendimento pleno ao subitem 4.13.18, não prosperando o recurso da empresa recorrente.

6. Para esclarecimentos ao itens 42 à 44, das razões recursais, subitem 4.3.18.1, quanto a capacidade da solução em suportar a criação de assinaturas de aplicações utilizando p
trazemos a tona dos seguintes esclarecimentos: "A comprovação deste item encontra-se em dois locais. Segundo a capacidade de criar assinaturas de aplicações utilizando pa
encontra-se na seguinte URL http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/IPS/Custom%20signature%20keywords.htm

Custom signature keywords: •information •session •content •IP header •TCP header •UDP header •ICMP •other Information keywords. attack_id Syntax: --attack_id ; Description: Us
the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiGate automatically assigns an attack ID to the signature. If you are u
appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs. An attack ID you assign must be between 1000 and 9999. Ex
Syntax: --name ; Description: Enter the name of the rule. A rule name must be unique. If you are using VDOMs, custom signatures appear only in the VDOM in which you create th
name for signatures in different VDOMs. The name you assign must be a string greater than 0 and less than 64 characters in length. Example: --name "Buffer_Overflow"; Sessior
{from_client[,reversed] | from_server[,reversed] | bi_direction }; Description: Specify the traffic direction and state to be inspected. They can be used for all IP traffic. Exa
bi_direction; The signature checks traffic to and from port 41523. If you enable "quarantine attacker", the optional reversed keyword allows you to change the side of the connecti
signature is detected. For example, a custom signature written to detect a brute-force log in attack is triggered when "Login Failed" is detected from_server more than 10 times
quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker. Previous FortiOS versions used to_client a
now deprecated, but still function for backwards compatibility. Service. Syntax: --service {HTTP | TELNET | FTP | DNS | SMTP | POP3 | IMAP | SNMP | RADIUS | LDAP | MSSQL | RPC |
SSH | SSL}; Description: Specify the protocol type to be inspected. This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capa
any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any por
Syntax: --weight ; Description: Specify the weight to be assigned to the signature. This keyword allows a signature with the higher weight to have priority over a signature with a lov
between 0 an 255. Most of the signatures in the Application Control signature database have weights of 10; botnet signatures are set to 250. A range of 20 to 50 is recommended
keywords byte_extract Syntax: byte_extract:, , \ [, relative][, multiplier][,]\ [, string][, hex][, dec][, oct][, align][, dce]; Description: Use the byte_extract option to write rules ag
This reads some of the bytes from the packet payload and saves it to a variable. byte_jump Syntax: --byte_jump , [, multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [,
the byte_jump option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pat
This keyword allows relative pattern matches to take into account numerical values found in network data. The available keyword options include:•: The number of bytes to examine
of bytes into the payload to start processing.•[multiplier]: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the res
an offset relative to last pattern match.•big: Process the data as big endian (default).•little: Process the data as little endian.•string: The data is a string in the packet.•hex: The conv
in hexadecimal notation.•dec: The converted string data is represented in decimal notation.•oct: The converted string data is represented in octal notation. •align: Round up the nu
next 32-bit boundary. byte_test Syntax: --byte_test , , , [multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct]; Description: Use the byte_test keyword to compare a by
(with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options i
to compare.•: The operation to perform when comparing the value (<,>,=,!,&).•: The value to compare the converted value against. •: The number of bytes into the payload to
multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped. •relative: Use an offset relative to last p
data as big endian (default). •little: Process the data as little endian. •string: The data is a string in the packet. •hex: The converted string data is represented in hexadecimal notat
data is represented in decimal notation. •oct: The converted string data is represented in octal notation. Depth Syntax: --depth ; Description: Use the depth keyword to search for t
number of bytes after the starting point defined by the offset keyword. If no offset is specified, the offset is assumed to be equal to 0. If the value of the depth keyword is smaller tha
content keyword, this signature will never be matched. The depth must be between 0 and 65535. Distance Syntax: --distance ; Description: Use the distance keyword to search for t
number of bytes relative to the end of the previously matched contents. If the within keyword is not specified, continue looking for a match until the end of the payload. The distance
Content Syntax: --content [!]""; Description: Deprecated, see pattern and context keywords. Use the content keyword to search for the content string in the packet payload. The cor
double quotes. To have the FortiGate search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string. Multiple content iter
The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign(|) and colon(:) characters must
if specified in a content string.

If the value of the content keyword is greater than the length of the value of the depth keyword, this signature will never be matched. Context Syntax: --context {uri | header | boc
the protocol field to look for the pattern. If context is not specified for a pattern, the FortiGate unit searches for the pattern anywhere in the packet buffer. The available context var
pattern in the HTTP URI line. •header: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages. •body: Search for the pattern in HTTP body or SMTP/
Search for the pattern in HTTP HOST line. no_case Syntax: --no_case; Description: Use the no-case keyword to force the FortiGate unit to perform a case-insensitive pattern m
Description: Use the offset keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload.
the depth keyword to stop looking for a match after a specified number of bytes. If no depth is specified, the FortiGate unit continues looking for a match until the end of the payload
and 65535. Pattern Syntax: --pattern [!]""; Description: The FortiGate unit will search for the specified pattern. A pattern keyword normally is followed by a context keyword to defin
in the packet. If a context keyword is not present, the FortiGate unit looks for the pattern anywhere in the packet buffer. To have the FortiGate search for a packet that does not co
exclamation mark (!) before the URI. Example: --pattern "/level/" --pattern "|E8 D9FF FFFF|/bin/sh" --pattern !"|20|RTSP/" pcre Syntax: --pcre [!]"//[ismxAEGRUB]"; Description: Si
use the pcre keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A pcre keyword can be followed by a context keyword to define where to look for t
context keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer. For more information about PCRE syntax, go to http://www.pcre.org. The switches i
Include newlines in the dot metacharacter. •m: By default, the string is treated as one big line of characters. ^ and $ match at the beginning and ending of the string. When m is s
following or immediately before any newline in the buffer, as well as the very start and very end of the buffer. •x: White space data characters in the pattern are ignored except whe
class. •A: The pattern must match only at the start of the buffer (same as ^). •E: Set $ to match only at the end of the subject string. Without E, $ also matches immediately bef
newline (but not before any other newlines). •G: Invert the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by ?.

•R: Match relative to the end of the last pattern match. (Similar to distance:0;). •U: Deprecated, see the context keyword. Match the decoded URI buffers. Uri Syntax: --uri [!]"'
pattern and context keywords. Use the uri keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("). To have the FortiGate unit search for
the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data
pipe (|) character. The double quote ("), pipe sign (|) and colon (:) characters must be escaped using a back slash (\) if specified in a URI string. Within Syntax: --within ; Descrip
distance keyword to search for the contents within the specified number of bytes of the payload. The within value must be between 0 and 65535. IP header keywords dst_addr Synt
Use the dst_addr keyword to search for the destination IP address. To have the FortiGate search for a packet that does not contain the specified address, add an exclamation mark
can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets. Example: dst_addr [172.20.0.0/16, 10.1.0.0/16,192.168.0.0/16]
ip_dscp Syntax: --ip_dscp Description: Use the ip_dscp keyword to check the IP DSCP field for the specified value. ip_id Syntax: --ip_id ; Description: Check the IP ID field for the sp
--ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any}; Description: Use the ip_option keyword to check various IP option settings. The available options include: •rr: Check i
present. •eol: Check if IP EOL (end of list) option is present. •nop: Check if IP NOP (no op) option is present. •ts: Check if IP TS (time stamp) option is present. •sec: Check if IP SEC
•lsrr: Check if IP LSRR (loose source routing) option is present. •ssrr: Check if IP SSRR (strict source routing) option is present. •satid: Check if IP SATID (stream identifier) option is
option is present. ip_tos Syntax: --ip_tos ; Description: Check the IP TOS field for the specified value. ip_ttl Syntax: --ip_ttl [< | >] ; Description: Check the IP time-to-live val
Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol. Protocol Syntax: --protocol { | tcp | udp | icr
protocol header. Example: --protocol tcp; src_addr Syntax: --src_addr [!]; Description: Use the src_addr keyword to search for the source IP address. To have the FortiGate unit se
contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in squaı
192.168.13.0/24 TCP header keywords ack Syntax: --ack ;
Description: Check for the specified TCP acknowledge number. dst_port Syntax: --dst_port [!]{ | : | : | :}; Description:
Use the dst_port keyword to specify the destination port number. You can specify a single port or port range: • is a single port. •: includes the specified port and all lower numbered
port and all higher numbered ports. •: includes the two specified ports and all ports in between.seq Syntax: --seq [operator,][,relative]; Description: Check for the specified TC
includes =,<,>,!. •relative indicates it's relative to the initial sequence number of the TCP session. src_port Syntax: --src_port [!]{ | : | : | :}; Description:
Use the src_port keyword to specify the source port number. You can specify a single port or port range: • is a single port. •: includes the specified port and all lower numbered port
and all higher numbered ports. •: includes the two specified ports and all ports in between. tcp_flags Syntax: --tcp_flags [!|*|+] [,]; Description: Specify the TCP flags to match in a
•A: Match the ACK flag. •F: Match the FIN flag. •R: Match the RST flag. •U: Match the URG flag. •P: Match the PSH flag. •1: Match Reserved bit 1. •2: Match Reserved bit 2.
•0: Match No TCP flags set. •!: Match if the specified bits are not set. •*: Match if any of the specified bits are set. •+: Match on the specified bits, plus any others. The first part if tl
must be present for a successful match. Example: --tcp_flags AP only matches the case where both A and P bits are set.
The second part ([,]) is optional, and defines the additional bits that can be present for a match. For example tcp_flags S,12 matches the following combinations of flags: S, S and
modifiers !, * and + cannot be used in the second part. window_size Syntax: --window_size [!]; Description:
Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by 0x. To have the FortiGate
specified window size, add an exclamation mark (!) before the window size. UDP header keywords dst_port Syntax: --dst_port [!]{ | : | : | :}; Description: Specify the destination
single port or port range:• is a single port. •: includes the specified port and all lower numbered ports. •: includes the specified port and all higher numbered ports. •: includes the twc
between. src_port Syntax: --src_port [!]{ | : | : | :}; Description: Specify the destination port number. You can specify a single port or port range: • is a single port. •: includes
numbered ports. •: includes the specified port and all higher numbered ports. •: includes the two specified ports and all ports in between. ICMP keywords. icmp_code Syntax: --icmp_
Description: Specify the ICMP code to match. icmp_id Syntax: --icmp_id ; Description: Check for the specified ICMP ID value. icmp_seq Syntax: --icmp_seq ; Description: Check fc
value. icmp_type
Syntax: --icmp_type ; Description: Specify the ICMP type to match.Other keywords data_size Syntax: --data_size { | < | >; Description: Test the packet payload size. With data_size
turned off automatically. So a signature with data_size and only_stream values set is wrong. • is a particular packet size. •< is a packet smaller than the specified size. •> is a packe
Examples: •--data_size 300; •--data_size <300; •--data_size >300; data_at Syntax: --data_at [, relative]; Description: Verify that the payload has data at a specified offset, option
the end of the previous content match. dump-all-html Syntax: --dump-all-html Description: Dump all HTML files for benchmarking via iSniff. When there is no file type specified, a
Syntax: --rate ,; Description: Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a spe
specified time period. • is the number of times a signature must be detected. • is the length of time in which the signature must be detected, in seconds. For example, if a custom sig
entry will be created every time the signature is detected. If --rate 100,10; is added to the signature, a log entry will be created if the signature is detected 100 times in the previous
with --track to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all
rpc_num [, | *][, | *>]; Description: Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wild card can be used for version and procedure
same_ip; Description: Check that the source and the destination have the same IP addresses. Track Syntax: --track {SRC_IP |DST_IP |DHCP_CLIENT |DNS_DOMAIN}[,block_int];
rate, this keyword narrows the custom signature rate totals to individual addresses. •SRC_IP: tracks the packet's source IP.•DST_IP: tracks the packet's destination IP.•DHCP_CLIEN
address. •DNS_DOMAIN: counts the number of any specific domain name. •block_int has the FortiGate unit block connections for the specified number of seconds, from the client
which is specified. For example, if --rate 100,10 is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiGa
regardless of source and destination address. If the same custom signature also includes --track client; matches are totaled separately for each source address. A log entry is added
100 times in 10 seconds within traffic from the same source address. The --track keyword can also be used without --rate. If an integer is specified, the client or server will be bloci
seconds every time the signature is detected.

Segundo o passo a passo de configuração encontra-se na seção "Creating a New Custom Application Signature" da seguinte URL http://help.fortinet.com/fos50hlp/54/Content/For

54/Application_Control/Enable%20Application%20Control.htm . In verbis: "Enable application control. Application control examines your network traffic for traffic generated by the ap
General configuration steps. Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration
Create an application sensor. 2. Configure the sensor to include the signatures for the application traffic you want the FortiGate unit to detect. 3. Enable any other applicable options. 4
security policy and select the application sensor. Creating an application sensor. You need to create an application sensor before you can enable application control. To create an app
Profiles > Application Control. 2.Select the Create New icon in the title bar of the Edit Application Sensor window. 3.In the Name field, enter the name of the new application sensor. 4
a comment. Adding applications to an application sensor. Once you have created an application sensor, you need to need to define the applications that you want to control. You can a
categories, application overrides, and/or filter overrides. Categories will allow you to choose groups of signatures based on a category type. Application overrides allow you to choo
overrides allow you to select groups of applications and override the application signature settings for them. To add a category of signatures to the sensor. 1.Go to Security Profile
Categories, you may select from the following: Botnet; Business; Cloud.IT; Collaboration; Email; Game; General.Interest; Mobile; Network.Service; P2P; Proxy; Remote.Access;
Update; Video/Audio; VoIP; Web.Clients; Unknown Applications. When selecting the category that you intend to work with, left click on the icon next to the category name to pr
includes these actions: Allow; Monitor; Block; Quarantine; View Signatures
These actions are briefly defined under Application Control actions.3.If you wish to add individual applications, select Add Signatures under Application Overrides.a.Use the Add Filter
list of possible signatures by a series of attributes.b.When finished, select Use Selected Signatures.4.If you wish to add advanced filters, select Add Filter under Filter Overrides.a.U
narrow down the list of possible filters by a series of attributes.b.When finished, select Use Filters.4.Select, if applicable, from the following options: Allow and Log DNS Traffic; Re
based Applications. 6. Select OK.
There is a disabled category called Industrial. This category is disabled by default, however it can be applied through use of the CLI command below. Note that none will mean no sig
industrial will exclude all industrial signatures. CLI Syntax. config ips global set exclude-signatures [none | industrial] end
Creating a New Custom Application Signature If you have to deal with an application that is not already in the Application List you have the option to create a new application signat
Application Control. 2.Select the link in the upper right corner, [View Application Signatures]. 3.Select the Create New icon. 5. Give the new signature a name (no spaces) in th
description in the Comments field. 6.Enter the text for the signature in the signature field. Use the rules found in the Custom IPS signature chapter to determine syntax. 7. Select OK."
Conforme exposto e elucidado pelo link e menções acima, comprovamos nosso pleno atendimento ao subitem 4.3.18.1, não prosperando o recurso da empresa recorrente.
Em esclarecimento aos itens 45 à 47, das razões recursais, subitem 4.3.26.3, fazemos os seguintes esclarecimentos: O equipamento FortiGate atende este item através da criaçã
aplicação com os recursos "Application Override" ou "Filter Override" ativos (http://help.fortinet.com/fos50hlp/54/Content/For
54/Application_Control/Enable%20Application%20Control.htm). In verbis:
"Enable application control. Application control examines your network traffic for traffic generated by the applications you want it to control. General configuration steps Follow the
order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results. 1.Create an application sensor. 2.Configure the
for the application traffic you want the FortiGate unit to detect. 3.Enable any other applicable options. 4.Enable application control in a security policy and select the application sensor
You need to create an application sensor before you can enable application control. To create an application sensor 1.Go to Security Profiles > Application Control. 2.Select the Create
Edit Application Sensor window. 3.In the Name field, enter the name of the new application sensor. 4.Optionally, you may also enter a comment. Adding applications to an application
an application sensor, you need to need to define the applications that you want to control. You can add applications and filters using categories, application overrides, and/or filter
you to choose groups of signatures based on a category type. Application overrides allow you to choose individual applications. Filter overrides allow you to select groups of applicatic
signature settings for them. To add a category of signatures to the sensor. 1.Go to Security Profiles > Application Control. 2.Under Categories,
following:•Botnet•Business•Cloud.IT•Collaboration•Email•Game•General.Interest•Mobile•Network.Service•P2P•Proxy•Remote.Access•Social.Media•Storage.Backup•Update•Video/Au
ApplicationsWhen selecting the category that you intend to work with, left click on the icon next to the category name to produce a drop down
actions:•Allow•Monitor•Block•Quarantine•View SignaturesThese actions are briefly defined under Application Control actions.3.If you wish to add individual applications, select Ad
Overrides.
a.Use the Add Filter search field to narrow down the list of possible signatures by a series of attributes.b.When finished, select Use Selected Signatures.4.If you wish to add advance
Filter Overrides.a.Use the Add Filter search field to narrow down the list of possible filters by a series of attributes.b.When finished, select Use Filters.4.Select, if applicable, from the f
DNS Traffic •Replacement Messages for HTTP-based Applications 6.Select OK.There is a disabled category called Industrial. This category is disabled by default, however it can be
command below. Note that none will mean no signatures are excluded, and that industrial will exclude all industrial signatures.CLI Syntax config ips global set exclude-signatures [n
New Custom Application Signature If you have to deal with an application that is not already in the Application List you have the option to create a new application signature.1.Go to
Control. 2.Select the link in the upper right corner, [View Application Signatures]3.Select the Create New icon4.Give the new signature a name (no spaces) in the Name field.5.
Comments field
6.Enter the text for the signature in the signature field. Use the rules found in the Custom IPS signature chapter to determine syntax.7.Select OK."
Ao criar um sensor de controle de aplicação, podemos configurar todas as categorias com ação "bloquear", e através do "Application Override" ou "Filter Override" definir um númer
usuários poderão acessar, desta forma criando uma sub-categoria de aplicações.

Conforme exposto e link mencionado acima, comprovamos o atendimento ao subitem 4.3.26.3, não prosperando o recurso da empresa recorrente.

Em esclarecimento aos itens 48 à 50, das razoes recursais, subitem 4.3.26.4, quanto a criação de grupos de aplicações baseados em aplicações que usem técnicas evasivas, fazemos
"O equipamento FortiGate atende este item através da criação de um sensor de controle de aplicação com os recursos "Application Override" ou
(http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Enable%20Application%20Control.htm). In verbis: "
Enable application control. Application control examines your network traffic for traffic generated by the applications you want it to control. General configuration steps Follow the
order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results. 1. Create an application sensor.2.Configure the
for the application traffic you want the FortiGate unit to detect.3.Enable any other applicable options.4.Enable application control in a security policy and select the application senso
You need to create an application sensor before you can enable application control. To create an application sensor Go to Security Profiles > Application Control. Select the Create Ne
Application Sensor window.3.In the Name field, enter the name of the new application sensor.4.Optionally, you may also enter a comment.
Adding applications to an application sensor Once you have created an application sensor, you need to need to define the applications that you want to control. You can add applicatic
application overrides, and/or filter overrides. Categories will allow you to choose groups of signatures based on a category type. Application overrides allow you to choose individu
allow you to select groups of applications and override the application signature settings for them. To add a category of signatures to the sensor. 1.Go to Security Profiles > Applicat
you may select from
following:Botnet;Business;Cloud.IT;Collaboration;Email;Game;General.Interest;Mobile;Network.Service;P2P;Proxy;Remote.Access;Social.Media;Storage.Backup;Update;Video/Audio;
Applications. When selecting the category that you intend to work with, left click on the icon next to the category name to produce a drop down
actions:Allow;Monitor;Block;Quarantine;View Signatures. These actions are briefly defined under Application Control actions. 3.If you wish to add individual applications, select Ad
Overrides.a.Use the Add Filter search field to narrow down the list of possible signatures by a series of attributes.b.When finished, select Use Selected Signatures.4.If you wish to a
Filter under Filter Overrides.a.Use the Add Filter search field to narrow down the list of possible filters by a series of attributes.6. When finished, select Use Filters.b.Select, if
options:Allow and Log DNS Traffic ; Replacement Messages for HTTP-based Applications 6.Select OK. There is a disabled category called Industrial. This category is disabled by def
through use of the CLI command below. Note that none will mean no signatures are excluded, and that industrial will exclude all industrial signatures. CLI Syntax config ips global
industrial] end Creating a New Custom Application Signature
If you have to deal with an application that is not already in the Application List you have the option to create a new application signature.1.Go to Security Profiles > Application
upper right corner, [View Application Signatures] 3.Select the Create New icon 4.Give the new signature a name (no spaces) in the Name field.5.Enter a brief description in the Com
the signature in the signature field. Use the rules found in the Custom IPS signature chapter to determine syntax. 7.Select OK."
Ao criar um sensor de controle de aplicação, podemos configurar todas as categorias com ação "Allow" por exemplo, e através do "Application Override" ou "Filter Override" selecio
comportamento (Behavior) evasivo (Evasive). Uma das categorias de aplicações consideradas como evasivas é P2P, ver seção "P2P application d
(http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Application_Control/Enable%20Application%20Control.htm). In verbis: " Enable application contro
your network traffic for traffic generated by the applications you want it to control. General configuration steps. Follow the configuration procedures in the order given. Also, note tha
actions between procedures, your configuration may have different results. 1.Create an application sensor. 2.Configure the sensor to include the signatures for the application traffic
detect. 3.Enable any other applicable options. 4.Enable application control in a security policy and select the application sensor. Creating an application sensor You need to create a
can enable application control. To create an application sensor 1.Go to Security Profiles > Application Control. 2.Select the Create New icon in the title bar of the Edit Application Sens
enter the name of the new application sensor. 4.Optionally, you may also enter a comment. Adding applications to an application sensor. Once you have created an application sensor,
applications that you want to control. You can add applications and filters using categories, application overrides, and/or filter overrides. Categories will allow you to choose groups of
type. Application overrides allow you to choose individual applications. Filter overrides allow you to select groups of applications and override the application signature settings f
signatures to the sensor. 1.Go to Security Profiles > Application Control. 2.Under Categories, you may select
•Botnet•Business•Cloud.IT•Collaboration•Email•Game•General.Interest•Mobile•Network.Service•P2P•Proxy•Remote.Access•Social.Media•Storage.Backup•Update•Video/Audio•VoIP•
ApplicationsWhen selecting the category that you intend to work with, left click on the icon next to the category name to produce a drop down
actions:•Allow•Monitor•Block•Quarantine•View Signatures. These actions are briefly defined under Application Control actions.3.If you wish to add individual applications, select Ac
Overrides. a.Use the Add Filter search field to narrow down the list of possible signatures by a series of attributes.b.When finished, select Use Selected Signatures.4.If you wish to a
Filter under Filter Overrides.a.Use the Add Filter search field to narrow down the list of possible filters by a series of attributes.b.When finished, select Use Filters.4.Select, if
options:•Allow and Log DNS Traffic •Replacement Messages for HTTP-based Applications 6.Select OK. There is a disabled category called Industrial. This category is disabled by de
through use of the CLI command below. Note that none will mean no signatures are excluded, and that industrial will exclude all industrial signatures.CLI Syntax config ips global
industrial] end."
De forma mais explícita, no documento que aborda especificamente o controle de aplicação do FortiGate (http://docs.fortinet.com/uploaded/files/3277/INSIDE-AC-DAT-R2-201608.p
na página 1: "Allows organization to strengthen security policies by controlling evasive application communications.", traduzindo para o português "Permite que organizações refo
através do controle da comunicação de aplicações evasivas"."
Conforme exposto e supracitado do link acima, comprovamos que atendemos ao subitem 4.3.26.4, não prosperando o recurso da empresa recorrente.

-Para os itens 51 à 53, das razões recursaias, subitem 4.5.3, fazemos os seguintes esclarecimentos: "Item comprovado através da seguinte URL http://help.fortinet.com/fos50hl
sandbox-inspection-54/1-sandbox-introduction/4-Appliance-vs-Cloud.htm"
Conforme link acima mencionado, por meio da tabela FortiSandbox Appliance vs FortiCloud, comprovamos que atendemos ao subitem 4.5.3, não prosperando o recurso da empresa
-Para os itens 54 à 56, das razões recursais, subitem 4.5.5, fazemos os seguintes esclarecimentos: "Nossa solução é capaz de identificar dezenas de milhares de variações de códig
10.000 variações ou "comportamentos maliciosos" de vírus. No manual online da solução FortiSandbox em http://help.fortinet.com/fsandbox/olh/2-3-0/index.htm , temos a segui
atendimento ao item: "Fortinet's dynamic scanning is based on our custom Compact Pattern Recognition Language (CPRL) and ASIC hardware acceleration. The result is fast, powerf
that uses a single signature to identify tens of thousands of variations of viral code.", traduzindo para português temos "O escaneamento dinâmico da Fortinet é baseado em nossa
de Padrão Compacto (sigla inglesa CPRL) customizado e aceleração em hardware ASIC. O resultado é detecção rápida e poderosa, característica única da Fortinet, que utiliz
identificar DEZENAS de MILHARES de variações de código de vírus."
Conforme esclarecimentos acima, apoiados pelo link acima mencionado, comprovamos que atendemos ao subitem 4.5.5, não prosperando o recurso da empresa recorrente.
Para os itens 57 à 59, das razões recursais, subitem 5.1.13, fazemos os seguintes esclarecimentos: "A comprovação do item está na seção "Zones" na URL http://help.fortinet.com
values.html"
Conforme a tabela de valores mencionados no link acima mencionado, comprovamos o atendimento ao subitem 5.1.13, não tendo nada que nos desabone, não prosperando o recurs
Para os itens 60 à 62, das razões recursais, subitem 5.1.7, quanto a existência de 10 interfaces de rede 10/100/1000 base-TX, fazemos os seguintes esclarecimentos: "No me
http://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_600D.pdf é possível verificar a existência de 10 interfaces GE RJ45. Portas 9 à 16 (8 portas) e porta
perfazendo um total de 10 interfaces de rede 10/100/1000 base-tx."
Conforme exposto acima, comprovado por meio do link mencionado, comprovamos o pleno atendimento ao subitem 5.1.7, não tendo assim, nada que nos desabone, não pros
recorrente.
Por fim, quanto aos itens 63 ao 65, das razões recursais, subitem 5.1.9, que aponta quanto capacidade de atendimento da solução na integra, fazemos os seguintes esclareciment
qualquer interface pode ser usada de forma dedicada para alta disponibilidade. As portas de alta disponibilidades são escolhidas de acordo com a conveniência do usuário, nenh
disponibilidade ao sair da fábrica, mas o usuário tem a flexibilidade de poder escolhê-las. No mesmo datasheet encontrado em http://www.fortinet.com/content/dam/fortinet/assets/
é possível verificar a existência de várias interfaces que podem ser utilizadas de forma dedicada para sincronismo de alta disponibilidade, como por exemplo as portas 17 e 18. Um
todas as portas do equipamentos são mostradas como opções para interface de alta disponibilidade (Heartbeat interface) é mos
http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_config_basic_example.htm" In verbis: "How to set up FGCP clustering (recommended steps)".

Conforme exposto acima, comprovado por meio do link mencionado, comprovamos o pleno atendimento ao subitem 5.1.9, não tendo assim, nada que nos desabone, não prosı
recorrente.

3. COMENTÁRIOS GERAIS
Diante dos esclarecimentos prestados acima, demostramos a essa respeitosa Administração quanto a nossa íntegra capacidade de atendimento e cumprimento ao Ato Convoca
solicitada em Edital pela Administração, não procedendo assim, o recurso apresentado pela empresa 4TECH, interposto como forma à deturpar o processo.
Vale pontuar que a CONTARRAZOANTE NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA., é uma empresa séria, que atua no mercado de Informática, há mais de 1 (uma) (
comprometimento, primazia e impecabilidade no atendimento as exigências editalícias, Termo de Referência e Anexos, confiando assim na isonomia e na imparcialidade a ser pratica
por essa digníssima Administração, conforme previsão legal no art. 37, da Constituição Federal: "Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União,
e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência."
Salientamos que a proposta apresentada pela NETWORK SECURE, foi julgada de forma objetiva e impessoal, atendendo a todos os requisitos do edital, uma vez que as alegações
devem ser afastadas e restando óbvio que os requisitos exigidos no procedimento licitatório foram observados, não há dúvida de que deve ser preservado o interesse público, c
recorrente pela ofertou da melhor e mais vantajosa proposta, julgada de forma imparcial e objetiva pela Administração, sendo no caso aqui trazido à pessoa jurídica: NETW
INFORMAÇÃO LTDA, sendo posteriormente Adjudicada e Homologada, conforme item 10, do referido Edital e Procedidos pelo Art. 3º da Lei 8.666/93: "A licitação destina-se a gara
constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável e será processada e julgada en
princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julga
são correlato."
Conforme ficou comprovado, os pleitos do recorrente não se sustentam e uma vez que se mostram frágeis e sem qualquer embasamento, devem ser desconsiderados.
4. DO PEDIDO
Diante de tudo o que aqui foi alegado e restando comprovado que não ocorreu qualquer afronta ao processo licitatório aqui tratado, estando respeitados de forma contumaz os
NETWORK SECURE SEGURANÇA DA INFOMRAÇÃO LTDA., vem, com todo o respeito necessário, requerer que Vossa Excelência de digne de:
1) Negar em sua totalidade o recurso administrativo interposto pela empresa 4TECH TECNOLOGIA LTDA.,
2) Manter em sua integralidade o resultado já exarado para o Pregão Eletrônico nº 36/2016, realizando a posterior adjudicação e homologação à nosso favor.
3) Em entendendo pelo acolhimento do recurso administrativo, encaminhar as contrarrazões aqui exaradas à Autoridade Superior para análise, apreciação e manifestação.
Nestes termos, Pedimos Bom Senso, Legalidade e Deferimento.
NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

Fechar