ILUSTRÍSSIMO SENHOR

PREGOEIRO/CHEFE DA COMISSÃO DE LICITAÇÃO

RECEBIDO
EM: 23/05/2019
POR:

Ref: PREGÃO PRESENCIAL Nº 007/2019

A empresa BRASIL DIGITAL SERVICOS DE INFORMATICA E COMERCIO EIRELI, pessoa jurídica de direito privado, inscrita no CNPJ sob o Nº 14.629.705/0001-87, com sede na RUA DOM PEDRO II Nº 2669, BAIRRO SÃO CRISTÓVÃO - PORTO VELHO - RO, neste ato por sua representante legal MIRIAM BELEZA MATIAS, CPF Nº 805.299332-68, vem, TEMPESTIVAMENTE, conforme permitido no § 2º, do Art. 41, da Lei nº 8666/93, e na Lei 10.520/2002, em tempo hábil, à presença de Vossa Senhoria a fim de IMPUGNAR os termos do Edital em referência, que adiante específica o que faz na conformidade seguinte:

DA ADMISSIBILIDADE DA IMPUGNAÇÃO E DA TEMPESTIVIDADE.

A Lei nº 8.666/93 disciplina o exercício dessas manifestações no seu art. 41, nos seguintes moldes:

> Art. 41 A Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada.
>
> § 1º Qualquer cidadão é parte legítima para impugnar edital de licitação por irregularidade na aplicação desta Lei, devendo protocolar o pedido até 5 (cinco) dias úteis antes da data fixada para a abertura dos envelopes de habilitação, devendo a Administração julgar e responder à impugnação em até 3 (três) dias úteis, sem prejuízo da faculdade prevista no § 1º do art. 113.
>
> § 2º Decairá do direito de impugnar os termos do edital de licitação perante a administração o licitante que não o fizer até o segundo dia útil que anteceder a abertura dos envelopes de habilitação em concorrência, a abertura dos envelopes com as propostas em convite, tomada de preços ou concurso, ou a realização de leilão, as falhas ou irregularidades que viciariam esse edital, hipótese em que tal comunicação não terá efeito de recurso.

Como se vê, a Lei nº 8.666/93 não distingue os prazos para o particular impugnar o edital ou solicitar esclarecimentos. Em vez disso, a Lei de Licitações fixa prazos distintos apenas em função de quem se dirige à Administração (cidadão ou licitante).

Por sua vez, a Lei nº 10.520/02, que instituiu o pregão, não disciplinou prazos para apresentação de pedidos de esclarecimento e impugnações aos editais. Regra geral, essa disciplina foi fixada pelos decretos que disciplinam o pregão em suas formas presencial e eletrônica.

De acordo com a disciplina do art. 12 do Decreto nº 3.555/00, que regulamenta a forma presencial do pregão no âmbito da Administração Pública federal, "*até dois dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório do pregão*" (Grifamos). Nota-se ser idêntico o prazo para solicitar esclarecimentos e impugnar o edital, bem como não haver distinção de prazos em função do status de quem exerce essas manifestações.

A presente impugnação foi apresentada no dia 23/05/2019, quinta-feira.

Logo, a impugnante não só é parte legítima para o ato, como também o pratica tempestivamente.

De toda sorte, é poder-dever do Administrador Público conhecer e rever, de ofício, aqueles atos administrativos que afrontem a legislação pátria, eis que a existência de ilegalidades nestes atos, caso não sejam sanadas em tempo hábil, fatalmente ensejarão no fracasso do certame licitatório, seja por macular todas suas fases sucessivas, seja por eivar o próprio contrato dela decorrente de nulidade, causando enormes prejuízos à Administração Pública, o que não é admissível.

Portanto, a presente impugnação deverá ser recebida pelo Pregoeiro Oficial e sua equipe de apoio para que, na forma da lei, seja admitida, processada e, ao final, julgada procedente, nos termos do requerimento.

FATOS.

A subscrevente tem interesse em participar da licitação para registro de preços do objeto "***PRESTAÇÃO DE SERVIÇO DE ACESSO À INTERNET COM PROTEÇÃO NO BACKBONECONTRA ATAQUES DDOS***", conforme consta no Termo de Referência anexo ao edital.

Ao verificar as condições para participação na licitação citada, constatou-se que o presente edital restou por exigir itens desnecessários e desproporcional, frustrando inevitavelmente o caráter competitivo do certame.

Indiscutivelmente o referido Edital foi reproduzido direcionando vários objetos para determinadas MARCAS de forma explicita e prejudicial a diversos licitantes.

Pela forma apresentada nas exigências do Edital do Pregão Presencial Nº 007/2019 do SENAC-RO, apenas a empresa FORTINET seria capaz de atende-las, sendo a única no mercado brasileiro a enquadrar-se nos requisitos dos produtos apresentados.

É possível ser feita tal verificação em diversos itens onde na descrição dos equipamentos fica evidente o direcionamento a determinada marca sem descrição sobre a possibilidade de poder oferecer um produto "SIMILAR". Vejamos;

- "Todo o ponto **7.1.15**, que trata de '***SISTEMAS VIRTUAIS LÓGICOS***', só é atendido em alguns modelos de equipamento, para o Throughput especificado, poucos equipamentos atendem a essa especificação, sendo possível até mesmo isso limite a aplicação apenas à Firewall's de maior porte";

- "O ponto **7.3.50**, fala de HA (Alta disponibilidade), isso se aplica à utilização de Firewall's retundantes. Para tal situação deveria haver previsão da utilização de 02 Firewall's por Localidade, suficiente para atender as necessidades";

- "O ponto **7.6.41**, onde é Citado 'Proteção contra ataques de Zero Day', é citado o Protocolo Proprietário Security Fabric (Fortinet). E ainda cita 'SANDBOX On-Premisse e Nuvem sem Dimensionamento), sem oportunizar uso de similares";

- "Todo o ponto **7.13**, fala sobre '***CONTROLADORA WIFI***', mas o presente Termo não indica em seu objeto a utilização de AP's esses os quais seriam controlados, podendo assim o Firewall com Controladora, ser incompatível com a solução de AP dos Licitantes";

Em nenhum desses itens contem expressões como "OU EQUIVALENTE", "OU SIMILAR" e "OU DE MELHOR QUALIDADE". Neste giro, é fundamental destacar que há outras marcas capazes de atender as necessidades dos serviços.

Nestes casos a indicação da marca de referência está amparada em mera preferência do gestor ou solicitante, não aparado em critérios técnicos objetivos. Especificações que o gestor não consegue justificar o motivo e que para piorar direcionam para a MARCA pretendida.

Destaca-se que a Impugnante é empresa interessada no certame, possuindo capacidade de fornecimento de produto capaz de atender a demanda do SENAC-RO. Contudo, por evidente direcionamento nas especificações, sem possibilitar a utilização de equipamentos equivalentes, que em nada modificaria o objeto final, a Impugnante (e muitas outras empresas "tanto que o primeiro certame compareceu apenas uma empresa participante) se vê elidida de participar, caso não seja revisto o edital.

DO DIRECIONAMENTO DA LICITAÇÃO EM FAVOR DA FABRICANTE "FORTINET".

AUSÊNCIA DE COMPETITIVIDADE

O direcionamento de licitação a determinado fabricante constitui conduta nefasta aos princípios que norteiam a Administração Pública, os servidores públicos e causam, consequentemente, danos à população, quando veem seus impostos sendo mal empregados.

Em tempos atuais, de condutas firmes de órgãos de controle contra a malversação de recursos públicos, não mais se admite calado que contratações sejam direcionadas visando o fim único de privilegiar, por qualquer razão, determinado fabricante ou fornecedor.

No presente caso, como é demonstrado acima, somente o produto da marca "FORTINET", é capaz de atender às exigências do edital, em flagrante direcionamento da licitação em seu favor, sem qualquer justificativa para tal postura por parte do Órgão Contratante.

Pode ser facilmente comprovado que produtos dos concorrentes podem executar as mesmas funcionalidades, com desempenho igual ou superior, e, possivelmente, por um custo inferior ao que seria desembolsado pelo Erário para aquisição do produto objeto do direcionamento.

Seguem DATASHEET's de outros Fabricantes que podem atender a parte de FIREWALL-NG, se algumas das Características do produto forem modificadas:

- ANEXO-01_SOPHOS_DATASHEET.pdf,
- ANEXO-02_SONICWALL_DATASHEET.pdf,
- ANEXO-03_CHECKPOINT_DATASHEET.pdf).

DA APLICAÇÃO DAS LEIS nº 10.520/2002, nº 8.666/93 E DO PRINCÍPIO DA IGUALDADE (ISONOMIA)

O disposto no artigo 1º da Lei 10.520/2002 (que institui a modalidade Pregão) dispõe que a modalidade Pregão pode ser utilizada nos casos de aquisição de bens comuns, cuja definição seja padronizada e de acessível e objetiva descrição.

O artigo 3º da referida Lei dispõe que deve ser observado a definição do objeto, sendo vedadas as especificações que limitem a competição, in verbis:

> No Art. 3º A fase preparatória do pregão observará o seguinte:
>
> II - a definição do objeto deverá ser precisa, suficiente e clara, vedadas especificações que, por excessivas, irrelevantes ou desnecessárias, limitem a competição;

Como a requerente ingressa neste Pregão na qualidade de interessada pretende concorrer nesta Licitação, para atender mais adequadamente os fins do interesse público.

Mas esta participação está condicionada a readaptação do texto do edital tendo em vista que está sendo exigida a apresentação de proposta de determinadas marcas. Neste sentido, resta mister a todos que estão interessados em satisfazer o interesse público, a busca da adaptação do Edital, para que a licitação corra de forma saudável até seu destino.

Esse é o ímpeto que move a presente impugnação. A redação atual deste edital impede absolutamente qualquer forma de competição; posto que se trata de direcionamento de objeto a determinada empresa que fornece o material, o que impede que outras empresas possam concorrer neste pregão.

Portanto verifica-se que o Edital do pregão em questão viola frontalmente o princípio da igualdade (isonomia) que assegura o direito à competição. A competitividade é a essência da licitação, porque só pode-se promover esse certame, essa disputa, onde houver competição. É uma questão lógica.

Com efeito, onde há competição, a licitação não só é possível, como em tese, é obrigatória; onde ela não existe a licitação é impossível. Destarte a licitação caracteriza-se pela disputa entre interessados e nesse caso a redação atual do edital, especificando itens por marca infringe as legislações

A lei de licitações e contratos espelha em seu Art. 3° que:

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

Portanto, sem muitas voltas, a Lei 8666/93 é bastante e suficientemente clara ao impor a observância dos princípios da moralidade, da probidade administrativa e que as licitações devem selecionar a proposta mais vantajosa para a administração

PEDIDOS.

Em face do exposto, requer que seja a presente IMPUGNAÇÃO julgada procedente, com efeito de constar no Edital.

Ou que os pontos citados acima possam ser suprimidos ou desconsiderados, desde que o restante da discriminação seja adequado à Lei 2.126-B de 2011.

Requer ainda que seja determinada a republicação do Edital, inserindo a alteração aqui pleiteada, reabrindo-se o prazo inicialmente previsto, conforme § 4°, do art. 21, da Lei n° 8666/93.

Porto Velho – RO, 23 de Maio de 2019.

Nestes Termos

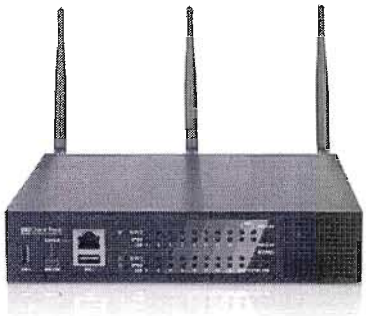
Pede Deferimento.

Mirian Beleza Matias

CPF: 805.299.332-68

RG:1.250795 SSP-RO

(Representante Legal)



1400 SECURITY APPLIANCES
BRANCH AND SMALL OFFICE SECURITY

CHECK POINT 1400 APPLIANCES

Branch and Small Office Security

Product Benefits

- All-in-one protection against viruses, spam, bots, dangerous applications, malicious websites and zero-day threats with SandBlast
- Continuous security updates from ThreatCloud™
- Fast set-up, instant protection
- Secure remote access for your mobile workers
- Multiple management options to address any organization's needs
- Simplified web-based local management
- Centralized with our enterprise Security Management or Multi-Domain Management products

Product Features

- Highest ranked Next Generation Firewall
- Profile-based management designed for large-scale deployments
- Multiple internet access options including DSL and support of external 3G/4G/LTE modems
- Integrated 802.11ac wireless security with guest access
- Power over Ethernet (PoE and PoE+) option

THE BRANCH OFFICE CHALLENGE

In the age of global business and a more distributed workforce, remote and branch staff demand access to corporate resources in order to work effectively and efficiently. However, even a small data breach can expose companies to crippling lawsuits, penalties and loss of reputation. Branch offices need an inexpensive, yet effective solution to provide secure access to critical resources from anywhere, while minimizing the risk of a data breach.

OUR SOLUTION

The Check Point 1400 Appliance family is a simple, affordable and easy to deploy all-in-one solution for delivering industry leading security to protect the weakest link in your enterprise network—the remote branch offices. Protect against cyber threats with Check Point Threat Prevention all in a quiet, compact desktop form factor.

	NGTP	+ SandBlast
Firewall	✓	✓
VPN (IPsec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
Anti-Spam	✓	✓
SandBlast Threat Emulation	✗	✓

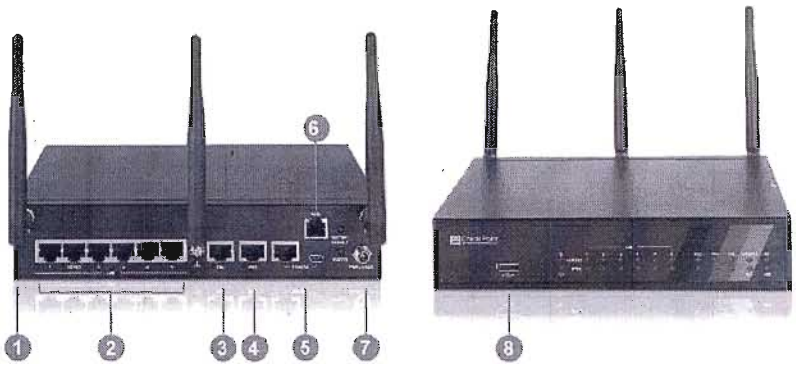
* Full SSL/TLS inspection is available when centrally managed

Setup is done in minutes using our step-by-step configuration wizard. The 1400 Appliances are manageable centrally by means of the Check Point enterprise Security Management or Multi-Domain products. Available in two appliances, the 1430/1450 and the 1470/1490, these appliances come standard with eight (8) 1-Gigabit or sixteen (16) Ethernet ports respectively. Connect securely from any device directly or through secure authenticated Wi-Fi.

Check Point
SOFTWARE TECHNOLOGIES LTD.

1430/1450 (Wi-Fi DSL options)

1. 802.11n/ac wireless (optional)
2. 6x 1GbE LAN ports
3. 1x 1GbE DMZ port
4. 1x 1GbE WAN port
5. RJ-45/micro USB Console port
6. DSL port
7. 12V power connector
8. USB port



	1430	1450
Ideal Testing Conditions		
Firewall 1518 Byte UDP Packets (Mbps)	2,000	2,500
IPS Throughput (Mbps)	325	575
NGFW Throughput (Mbps) [1]	300	490
Threat Prevention (Mbps) [2]	225	400
VPN AES-128 Throughput (Mbps)	275	500
Connections per Second	20,000	27,000
Concurrent Connections	500,000	500,000
Real-World Production Conditions		
SecurityPower	75	141
Firewall Throughput (Mbps)	900	1,100
IPS Throughput (Mbps)	175	225
NGFW Throughput (Mbps) [1]	100	210
Threat Prevention (Mbps) [2]	90	150
Software		
Security	Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Anti-Spam and SandBlast Threat Emulation (sandboxing)	
Unicast, Multicast Routing	OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP	
Mobile Access User License	100 in default package, 150 maximum	100 in default package, 150 maximum
Hardware		
WAN	1x 10/100/1000Base-T RJ-45 port	
DMZ	1x 10/100/1000Base-T RJ-45 port	
LAN Switch	6x 10/100/1000Base-T RJ-45 ports	
Wi-Fi (optional)	802.11 b/g/n/ac MIMO 3x3	
Radio Band (association rate)	1 radio band: 2.4Ghz (max 450 Mbps) or 5Ghz (max 1300 Mbps)	
Console Port	1x RJ-45, 1x Mini USB	
USB Port	1x USB 3.0	
SD Card Slot	Micro SDHC slot	
3G/4G Modem Support	Yes	
DSL (optional)	VDSL: G.993.1 (VDSL), G.993.2 (VDSL2), G.993.5 (VDSL2 Vectoring), G.998.4 (G.INP) VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, and 17a ADSL: Annex A (POTS), Annex B (ISDN), G.992.1 (ADSL), G.992.3 (ADSL2), G.992.5 (ADSL2+), Annex M (ADSL2/2+) ,Annex L Reach-extended (ADSL2) Dying Gasp, DSL Forum TR-067, TR-100, TR-114 Conformity	
Dimensions		
Enclosure	Desktop	
Dimensions WxHxD	210 x 42.5 x 155 mm, 8.3 x 1.7 x 6.1 in.	
Weight	1.3 kg (2.8 lbs.)	
Environment		
Operating / Storage	0°C ~ 40°C / -45°C ~ 60°C (5~95%, non-condensing)	
Power Requirements		
AC Input	110 – 240V, 50 – 60 Hz	
Power Supply Rating	12V/3.33A 40W desktop adaptor	
Power Consumption (Max)	25W (non-Wi-Fi), 30W (Wi-Fi option)	
Heat Dissipation	85.3 BTU/hr (non-Wi-Fi), 102.4 BTU/hr (Wi-Fi option)	
Certifications		
Safety / Emissions / Environment	UL/c-UL, IEC 60950 CB / EMC: EN55022 Class B, FCC: Part 15 Class B / RoHS, REACH, WEEE	

[1] Includes Firewall, Application Control and IPS

[2] Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection

Aplicativos da série XG Sophos – rapidamente

Com os modelos de desktop para pequenas empresas que buscam Unified Threat Management (gestão unificada de ameaças) para firewalls de alto desempenho de última geração para alta disponibilidade em ambientes de centro de dados, nossos aparelhos com base em Intel® abrangem várias situações de implementação.

Matriz de produtos

Modelo	Especificações						Taxa de transferência			
	Formato	Portas máximas de rede (GE)	WiFi	Armazenamento	RAM (GB)	Componentes que podem ser trocados	Firewall (Mbps)	VPN (Mbps)	IPS (Mbps)	AV-proxy (Mbps)
XG 85(w) Rev. 1	desktop	4	opcional com 802.11 a/b/g/n	8 GB eMMC	2	n/d	2000	200	510	330
XG 105(w) Rev. 2	desktop	4	opcional com 802.11 a/b/g/n	64 GB SSD	2	n/d	3000	300	700	430
XG 115(w) Rev. 2	desktop	4	opcional com 802.11 a/b/g/n	64 GB SSD	4	n/d	3.500	350	900	520
XG 125(w) Rev. 2	desktop	8	opcional com 802.11 a/b/g/n/ac	64 GB SSD	4	n/d	5.000	410	1.000	590
XG 135(w) Rev. 2	desktop	8	opcional com 802.11 a/b/g/n/ac	64 GB SSD	6	n/d	7.000	950	1.750	1.400
XG 210 Rev. 2	1U	14 (6 + 1 módulo)	n/d	120 GB SSD	8	n/d	14.000	1.350	2.700	2.300
XG 230 Rev. 1	1U	14 (6 + 1 módulo)	n/d	120 GB SSD	8	n/d	18.000	1.500	4.200	2.800
XG 310 Rev. 1	1U	18 (8 + 2SFP + 1 módulo)	n/d	180 GB SSD	12	n/d	25.000	2.500	5.500	3.300
XG 330 Rev. 1	1U	18 (8 + 2SFP + 1 módulo)	n/d	180 GB SSD	12	n/d	30.000	3.200	8.500	6.000
XG 430 Rev. 1	1U	24 (8 + 2 módulos)	n/d	240 GB SSD	16	n/d	37.000	4.800	9.000	6.500
XG 450 Rev. 1	1U	24 (8 + 2 módulos)	n/d	2*240 GB SSD (RAID-1)	16	opcional Potência	45.000	5.500	10.000	7.000
XG 550 Rev. 1	2U	24 (8 + 2 módulos)	n/d	2*300 GB SSD (RAID-1)	24	Potência, SSD	60.000	8.400	17.000	10.000
XG 650 Rev. 1	2U	32 (8 + 3 módulos)	n/d	2*480 GB SSD (RAID-1)	48	Potência, SSD	80.000	9.000	20.000	13.000
XG 750 Rev. 1	2U	64 (8 + 7 módulos)	n/d	2* 512 GB SSD (RAID-1)	64	Potência, SSD, Fan	140.000	11.000	22.000	17.000

Isto é o que se obtém com cada aparelho da série XG:

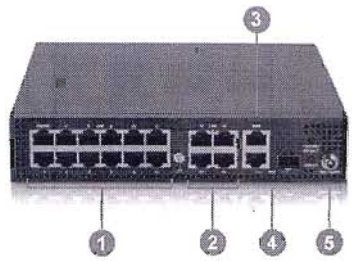
- A mais recente tecnologia Intel multi-core para desempenho e eficiência ideais
- Funcionalidades sofisticadas de segurança como Advanced Threat Protection (proteção avançada contra ameaças), disponível em todos os tamanhos de aparelhos
- SSD integrado como armazenamento para dados locais de quarentena, dados e relatórios*
- Módulos de porta FleXi disponíveis para todos os aparelhos 1U e 2U

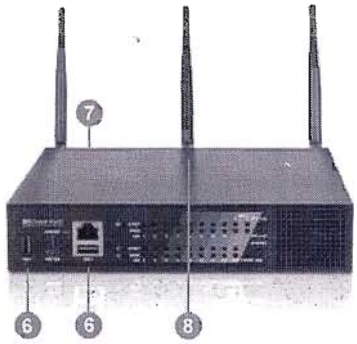
* Exclui XG 85/XG 85w

Check Point
SOFTWARE TECHNOLOGIES LTD.

1470/1490 (PoE and Wi-Fi options)

1. 12x 1GbE LAN ports
2. 4x PoE 1GbE LAN ports (PoE option)
3. 1x 1GbE WAN port
4. 1x 1GbE copper/fiber DMZ port
5. 12V power connector
6. 2x USB ports
7. RJ-45/micro USB console port
8. 802.11n/ac (Wi-Fi option)





	1470	1490
Ideal Testing Conditions		
Firewall 1518 Byte UDP Packets (Mbps)	3,200	4,000
IPS Throughput (Mbps)	700	800
NGFW Throughput (Mbps) [1]	625	800
Threat Prevention (Mbps) [2]	500	550
VPN AES-128 Throughput (Mbps)	500	1,000
Connections per Second	30,000	40,000
Concurrent Connections	500,000	500,000
Real-World Production Conditions		
SecurityPower	194	233
Firewall Throughput (Mbps)	1,600	1,800
IPS Throughput (Mbps)	285	375
NGFW Throughput (Mbps) [1]	240	310
Threat Prevention (Mbps) [2]	175	220
Software		
Security	Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Anti-Spam and SandBlast Threat Emulation (sandboxing)	
Unicast, Multicast Routing	OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP	
Mobile Access User License	200 in default package, 300 maximum	200 in default package, 300 maximum
Hardware		
WAN	1x 10/100/1000Base-T RJ-45 port	
DMZ	1x 10/100/1000Base-T RJ-45 / 1x 1000BaseF SFP (transceiver not included) port	
LAN Switch	16x 10/100/1000Base-T RJ-45 ports (total)	
PoE Ports (optional)	4x 10/100/1000Base-T RJ-45 out of the 16 LAN ports	
Wi-Fi (optional)	802.11 b/g/n and 802.11 n/ac MIMO 3x3	
Radio Band (association rate)	2 concurrent: 2.4Ghz (max 450 Mbps) and 5Ghz (max 1300 Mbps)	
Console Port	1x RJ-45, 1x Mini USB	
USB Port	2x USB 3.0	
SD Card Slot	Micro SDHC slot	
3G/4G Modem Support	Yes	
Dimensions		
Enclosure	Desktop	
Dimensions WxHxD	210 x 42.5 x 200.5 mm, 8.3 x 1.7 x 7.9 in.	
Weight	1.6 kg (3.6 lbs.)	
Environment		
Operating / Storage	0ºC ~ 40ºC / -45ºC ~ 60ºC (5~95%, non-condensing)	
Power Requirements		
AC Input	110 – 240V, 50 – 60 Hz	
Power Supply Rating	12V/5.4A 65W, 12V/12.5A 150W (PoE option)	
Total Available PoE Power	Max load on each 4x PoE ports: 15.4 W (802.3af), or use only 2x PoE ports with max load of 31W (802.3at) each	
Power Consumption (Max)	55W (wired), 60W (Wi-Fi option), 130W (PoE option)	
Heat Dissipation	187.7 BTU/hr (wired), 204.7 BTU/hr (Wi-Fi option), 443.6 BTU/hr (PoE option)	
Certifications		
Safety/Emissions/Environment	UL/c-UL, IEC 60950 CB / EMC: EN55022 Class B, FCC: Part 15 Class B / RoHS, REACH, WEEE	

[1] Includes Firewall, Application Control and IPS

[2] Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection

ORDERING INFORMATION

WI-FI or WI-FI +DSL (1430/1450) APPLIANCE OPTION (replace –xx in the SKU to specify the Wi-Fi region) [1]	
1430 Security Appliance with Threat Prevention security suite	CPAP-SG1430-NGTP-W or WDSL-xx
1430 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1430-NGTX-W or WDSL-xx
1450 Security Appliance with Threat Prevention security suite	CPAP-SG1450-NGTP-W or WDSL-xx
1450 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1450-NGTX-W or WDSL-xx
1470 Security Appliance with Threat Prevention security suite	CPAP-SG1470-NGTP-W-xx
1470 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1470-NGTX-W-xx
1490 Security Appliance with Threat Prevention security suite	CPAP-SG1490-NGTP-W-xx
1490 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1490-NGTX-W-xx
POWER OVER ETHERNET (PoE) APPLIANCE OPTION [1]	
1470 Security Appliance with Threat Prevention security suite, Wired, PoE	CPAP-SG1470-NGTP-PoE
1470 Security Appliance with Threat Prevention security suite and SandBlast, Wired, PoE	CPAP-SG1470-NGTX-PoE
1490 Security Appliance with Threat Prevention security suite, Wired, PoE	CPAP-SG1490-NGTP-PoE
1490 Security Appliance with Threat Prevention security suite and SandBlast, Wired, PoE	CPAP-SG1490-NGTX-PoE
WIRED APPLIANCE [1]	
1430 Security Appliance with Threat Prevention security suite	CPAP-SG1430-NGTP
1430 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1430-NGTX
1450 Security Appliance with Threat Prevention security suite	CPAP-SG1450-NGTP
1450 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1450-NGTX
1470 Security Appliance with Threat Prevention security suite	CPAP-SG1470-NGTP
1470 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1470-NGTX
1490 Security Appliance with Threat Prevention security suite	CPAP-SG1490-NGTP
1490 Security Appliance with Threat Prevention security suite and SandBlast	CPAP-SG1490-NGTX

WI-FI REGIONS (replace –xx in the SKU to specify the Wi-Fi region)			
USA, Canada	add -US	Israel	add –IL
Europe	add -EU	China	add –CN
Japan	add -JP	India, Chile	add –IN
Australia, Argentina	add -AU	New Zealand	add –NZ
Latin America, Singapore, Hong Kong, Thailand, Sri-Lanka	add -LA		

[1] Threat Prevention includes IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, and Anti-Spam updates for the first year; SandBlast includes Threat Emulation (sandboxing).

EXTEND YOUR SOLUTION

SECURITY SERVICE EXTENSION [1]	
Next Generation Threat Prevention Blades Package for 1 year for 14x0 Appliance	CPSB-NGTP-14x0-1Y
Next Generation Threat Prevention Blades Package and SandBlast for 1 year for 14x0 Appliance	CPSB-NGTX-14x0-1Y
ADDITIONAL SOFTWARE BLADES [2]	
Mobile Access Blade for 50 concurrent connections	CPSB-MOB-50

[1] NGTP and NGTX SKUs for 2 and 3 years are available, see the online Product Catalog

[2] The base packages include a license for 100 (1430/1450) and 200 (1470/1490) concurrent Mobile Access users. The MOB license is additive.

ACCESSORIES	
SFP short range transceiver (for the DMZ 1000BaseF port)	CPAC-TR-1SX-1200R
SFP long range transceiver (for the DMZ 1000BaseF port)	CPAC-TR-1LX-1200R
SD memory card 8 GB	CPAC-8GB-SD-1200R
SD memory card 32 GB	CPAC-32GB-SD-1200R
1400 appliance single/dual chassis rack shelf kit	CPAC-RM-700/1400
Additional/Replacement AC Power Supply for 770, 790, 1470 and 1490 appliances	CPAC-PSU-790/1490

SONICWALL

SonicOS Platform

The SonicOS architecture is at the core of every SonicWall physical and virtual firewall including the TZ, NSa, NSv and SuperMassive Series. SonicOS leverages our patented*, single-pass, low-latency, Reassembly-Free Deep Packet Inspection* (RFDPI) and patent-pending Real-Time Deep Memory Inspection™ (RTDMI) technologies to deliver industry-validated high security effectiveness, SD-WAN, real-time visualization, high-speed virtual private networking (VPN) and other robust security features.

Firewall features

REASSEMBLY-FREE DEEP PACKET INSPECTION (RFDPI) ENGINE	
Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.
FIREWALL AND NETWORKING	
Feature	Description
Secure SD-WAN	An alternative to more expensive technologies such as MPLS, Secure SD-WAN enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public internet services.
REST API	Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
High availability/clustering	Supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI2 and Active/Active clustering high availability modes.2 Active/Active DPI offloads the deep packet inspection load to passive appliance to boost throughput.
DDoS/DoS attack protection	SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The firewall can be deployed in wire, network tap NAT or Layer 2 bridge2 modes.

FIREWALL AND NETWORKING (CONTINUED)	
Feature	Description
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. Policy-based routing Creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.
Single and cascaded Dell N-Series and X-Series switch management2	Manage security settings of additional ports, including Portshield, HA, PoE and PoE+, under a single pane of glass using the firewall management dashboard for Dell's N-Series and X-Series network switches.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credential from social networking service such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.
Multi-domain authentication	Provides a simple and fast way to administer security polices across all network domains. Manage individual policy to a single domain or group of domains.

MANAGEMENT AND REPORTING	
Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Analytics or other tools that support IPFIX and NetFlow with extensions.

VIRTUAL PRIVATE NETWORKING (VPN)	
Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

CONTENT/CONTEXT AWARENESS	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression matching and filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

Breach prevention subscription services

CAPTURE ADVANCED THREAT PROTECTION[1]	
Feature	**Description**
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK plus multiple operating systems including Windows, Android, Mac OS and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWALL Capture subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Capture Client	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and rollback to a previous uninfected state.
ENCRYPTED THREAT PREVENTION	
Feature	**Description**
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden inside of encrypted traffic. Included with security subscriptions for all models except SOHO. Sold as a separate license on SOHO.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspects data traversing over SSH tunnels to prevent attacks that leverage SSH.
INTRUSION PREVENTION[1]	
Feature	**Description**
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols as they attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.
THREAT PREVENTION[1]	
Feature	**Description**
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
Capture Cloud malware protection	A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbond threats.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP. Decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

APPLICATION INTELLIGENCE AND CONTROL[1]	
Feature	Description
Application control	Controls applications, or individual application features that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures. This increases network security and enhances network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network.
Application bandwidth management	Application bandwidth management granularly allocates and regulates available bandwidth for critical applications (or application categories), while inhibiting nonessential application traffic.
Granular control	Controls applications (or specific components of an application) based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.
CONTENT FILTERING[1]	
Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced content filtering client	Extends policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Blocks content using any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.
Local CFS Responder	Local CFS Responder can be deployed as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V. This provides deployment flexibility option (Light weight VM) of CFS ratings database in various customer network use cases that require a dedicated on premise solution that speeds up CFS ratings request and response times, supports large number of allowed/blocked URL list (+100K), and adds up to 1000 SonicWall firewalls for CFS rating lookups.
ENFORCED ANTI-VIRUS AND ANTI-SPYWARE[1]	
Feature	Description
Multi-layered protection	Utilizes the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block viruses entering the network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

[1] *Requires added subscription*
[2] *Not supported NSv firewall series*

SonicOS feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/SYN flood)
- IPv4/IPv6 support
- Biometric authentication for remote access
- DNS proxy
- REST APIs

TLS/SSL/SSH decryption and inspection[2]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[2]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated & manual submission
- Real-time threat intelligence updates
- Block until verdict
- Capture Client

Intrusion prevention[2]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection engine
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[2]

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application identification[2]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

HTTP/HTTPS Web content filtering[2]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Secure SD-WAN
- Auto-provision VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (RIP/OSPF/BGP)

Networking

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NSa 2650 and above)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller1
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation[1] (static and dynamic)
- Port redundancy[1]
- A/P high availability with state sync
- A/A clustering1
- Inbound/outbound load balancing
- L2 bridge,1 wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover[1]
- Asymmetric routing
- Common Access Card (CAC) support

VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

[1] Not supported on NSv Series firewalls
[2] Requires added subscription.

SONICWALL

SonicOS feature summary (continued)

Management and monitoring

- Web GUI
- Command-line interface (CLI)
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen[1]
- Dell N-Series and X-Series switch management including cascaded switches[1]

Wireless[1]

- SonicWave AP cloud management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- Guest cyclic quota
- LHM guest portal

Integrated Wireless (TZ Series only)

- Dual-band (2.4 GHz and 5.0 GHz)
- 802.11 a/b/g/n/ac wireless standards
- Wireless intrusion detection and prevention
- Wireless guest services
- Lightweight hotspot messaging
- Virtual access point segmentation
- Captive portal
- Cloud ACL

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-SonicOSplatform-US-KJ-MKTG5158

SONICWALL

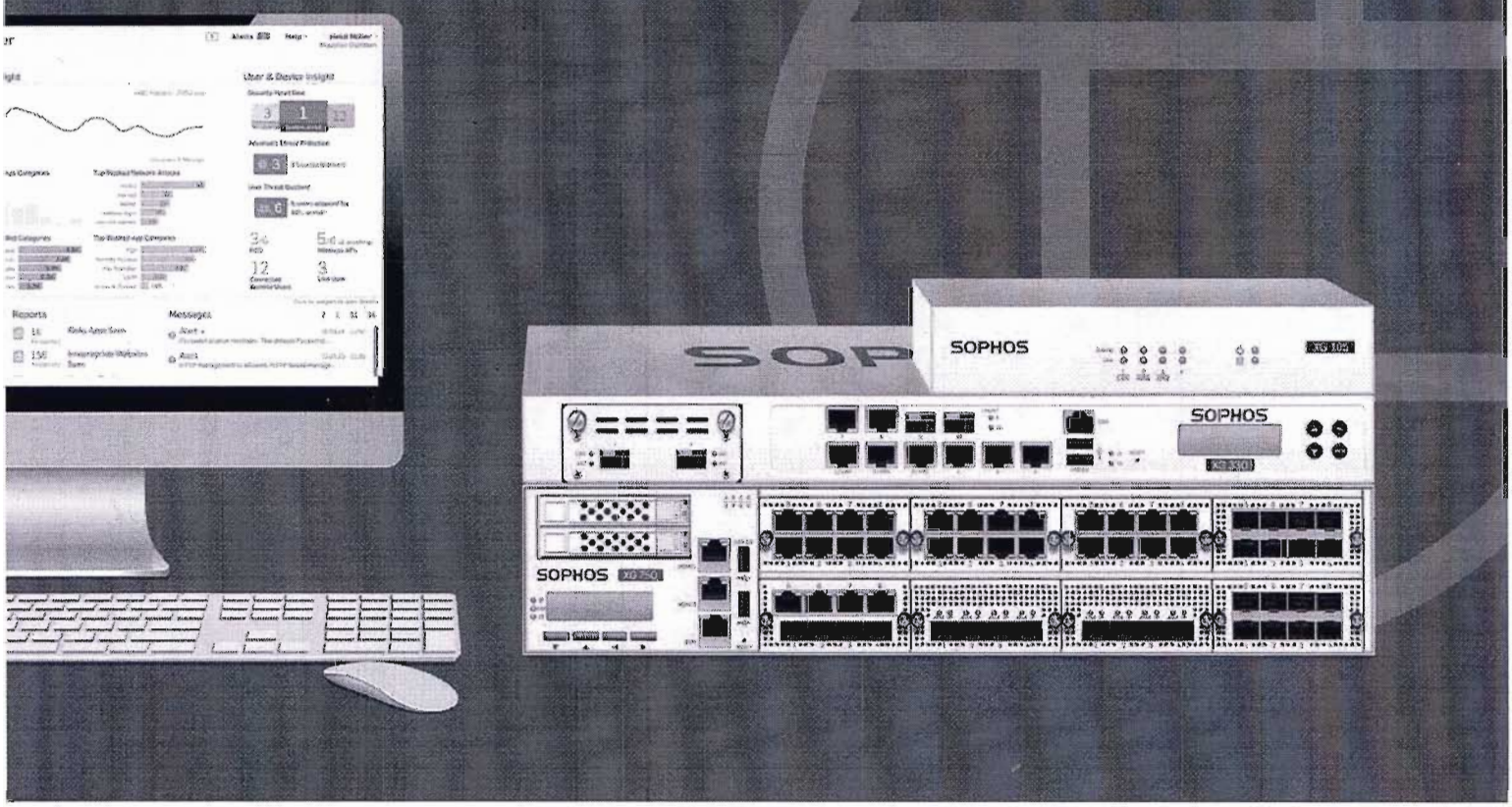
SOPHOS

Security made simple.

Sophos XG Firewall

Desempenho, segurança e controle sem igual

Sophos XG Firewall adota uma abordagem inovadora em todas as áreas de segurança de rede. Desde o modo como os firewalls são gerenciados até o modo como relatam informações e como funcionam com outros sistemas de segurança ao redor deles, oferecendo um nível sem precedentes de simplicidade, percepção e proteção avançada contra ameaças.



Sophos XG Firewall – O melhor pacote de segurança

Com uma interface projetada para eliminar complexidade desnecessária, permite utilizar os recursos avançados sem precisar se tornar um especialista em segurança de computadores.

Proteção avançada de modo simples

Muitos produtos de firewall fazem com que você configure e gerencie políticas através de vários módulos e telas. Não é o caso do Sophos. Nós fornecemos um modelo avançado de política unificada que permite gerenciar, visualizar, filtrar e classificar todas as suas políticas de usuários, aplicativos e rede em uma única tela.

Potente, avançado... rápido

Você obtém todas as funcionalidades de firewall de última geração de que precisa e que não encontra em nenhum outro lugar – incluindo nosso revolucionário Security Heartbeat™, firewall completo de aplicativo da Web e completo anti-spam para e-mail, criptografia e DLP [data loss prevention software (software para prevenção de perda de dados)]. Sem necessidade de hardware extra. Sem custos extra. Simplesmente escolha o que deseja implementar.

Relatórios na caixa incluídos como padrão

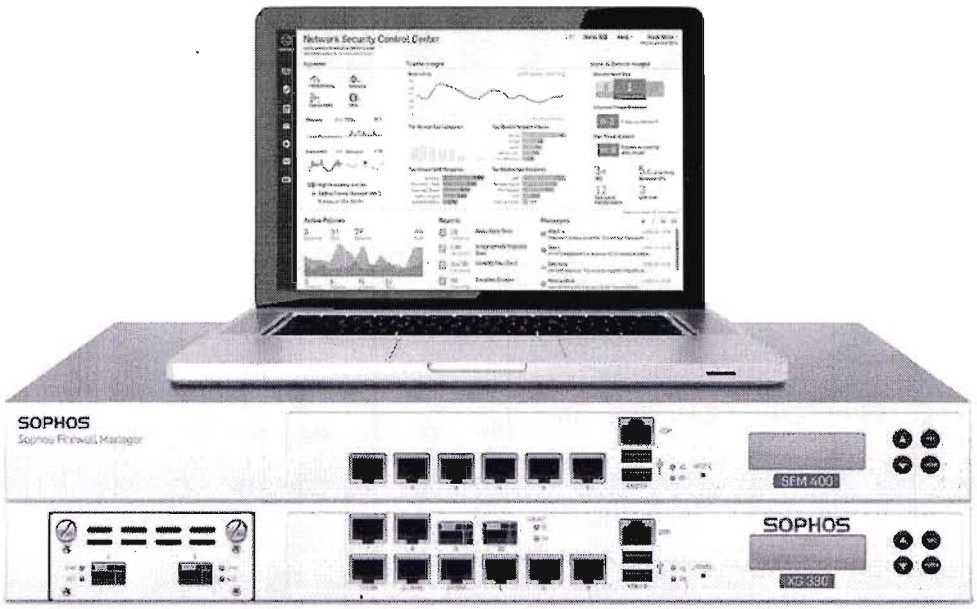
Com centenas de relatórios integrados você saberá exatamente o que está acontecendo com seus usuários e sua rede. Oberá relatórios detalhados como padrão, armazenados localmente, sem necessidade de ferramentas separadas. E nossos relatórios exclusivos de Quociente de Ameaças de Usuários mostram quais de seus usuários estão colocando em risco a sua segurança.

Mais proteção em um pacote

Projetamos o XG Firewall para proporcionar um desempenho notável. Nossos aparelhos são construídos utilizando tecnologia Intel de vários núcleos, drives de estado sólido e rastreamento acelerado de conteúdo na memória. Além disso, a tecnologia de otimização do pacote Sophos FastPath garante que você sempre obterá a máxima taxa de transferência.

Gerencie vários firewalls de modo simples

O gerenciador Sophos Firewall Manager oferece um único console para completa gestão central de vários firewalls SF-OS. E se também desejar consolidar relatórios através de vários SF-OS, os aparelhos Sophos UTM v9.x e Cyberoam OS, com Sophos iView isto é possível.



Funcionalidades de segurança que não se pode obter em nenhum outro lugar

Além de simplificar tarefas essenciais de segurança de rede, o Sophos proporciona abordagens inovadoras para garantir que você obtenha ainda mais proteção.

Modelos de diretivas fazem com que você seja protegido rapidamente

Modelos predefinidos de diretivas permitem que você proteja rapidamente aplicativos comuns como Microsoft Exchange ou SharePoint. Simplesmente selecione-os a partir de uma lista, forneça algumas informações básicas e o modelo cuida do resto. Ele define todas as configurações de regras e segurança de firewall de entrada e saída para você automaticamente, exibindo a diretiva final em uma declaração em vocabulário simples.

Controle de identidade patenteado Layer-8

A identidade do usuário é aplicada a toda uma nova camada com nossa tecnologia de diretiva com base em identidade Layer-8, permitindo controles em nível de usuário sobre aplicativos, largura de banda e outros recursos de rede, independentemente de endereço IP, localização, rede ou dispositivo. Literalmente eleva as diretivas de firewall para uma camada toda nova.

Implementação flexível, sem compromissos

Ao contrário de nossos concorrentes, quer você escolha hardware, software ou virtual nós não fazemos com que você se arrisque. Todas as funcionalidades estão disponíveis em cada modelo e configurações básicas.

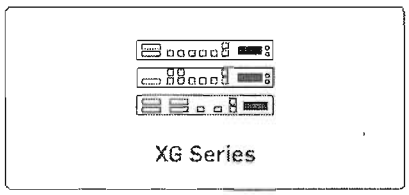
Relatórios automatizados de riscos de usuários

O indicador Sophos User Threat Quotient (UTQ; quociente de ameaças de usuários) é uma funcionalidade exclusiva que fornece informações que podem ser acionadas sobre comportamento de usuários. Nosso firewall correlaciona os hábitos de navegação e as atividades de cada usuário com acionados avançados de ameaças e histórico para identificar os usuários com comportamentos propensos a riscos.

Uma revolução em proteção avançada contra ameaças – Sophos Security Heartbeat™

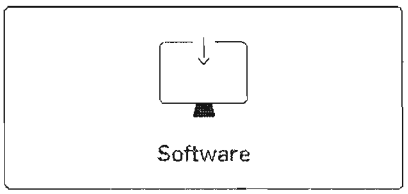
O primeiro no segmento, nosso Security Heartbeat vincula seus endpoints e seu firewall para combinar seus sistemas de informações e identificação comprometidos por ameaças desconhecidas anteriormente. O status Heartbeat é integrado nas configurações da diretiva de segurança para acionar instantaneamente ações em níveis de endpoint e rede para isolar ou limitar acesso até que os sistemas estejam íntegros novamente. Esta funcionalidade exige a proteção avançada de endpoint Sophos Cloud Endpoint Protection Advanced ou a proteção de usuário final em nuvem Sophos Cloud Enduser Protection.

Para saber mais, visite www.sophos.com/xgfirewall



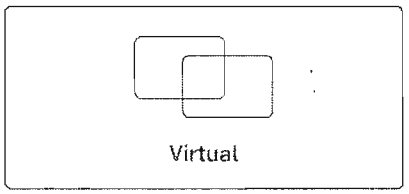
XG Series

Dispositivos construídos com objetivos para proporcionar o melhor em desempenho.



Software

Instale a imagem do sistema operacional Sophos Firewall em seus próprios hardware ou servidor Intel.



Virtual

Instale em VMware, Citrix, Microsoft Hyper-V e KVM.

Como comprar

Todos os aparelhos vêm com nosso Base Firewall como padrão e incluem IPSec e SSL VPN e proteção sem fio abrangente. Você poderá ampliar a proteção com nossos agrupamentos de proteção total ou ao adicionar módulos de proteção individualmente.

Proteção de rede

Toda a proteção de que precisar para interromper ataques sofisticados e ameaças avançadas e, ao mesmo tempo, proporcionar acesso seguro à rede para aqueles em que confiar.

Proteção sem fio

Configure, gerencie e proteja redes sem fio em poucos minutos com o controlador sem fio integrado UTM que funciona com toda a nossa gama de pontos de acesso sem fio.

Proteção na Web

Proteção abrangente das mais recentes ameaças na Web e ferramentas de diretivas avançadas garante que seus usuários fiquem seguros e produtivos on-line.

Heartbeat™ de segurança

Vincula os endpoints do Sophos ao firewall para oferecer proteção sem igual em relação a ameaças avançadas e reduz o tempo e a complexidade das respostas a incidentes de segurança.

Proteção para e-mails

Proteção completa para mensagens de SMTP e POP em relação a spam, phishing e perda de dados com nossa proteção exclusiva tudo em um que combina criptografia de e-mails com base em diretivas com DLP e anti-spam.

Porta do Servidor Web

Fortaleça os aplicativos de negócios e dos servidores da Web contra tentativas de invasões e, ao mesmo tempo, forneça acesso seguro para usuários externos com autenticação de proxy inversa.

Uma abordagem simples para um suporte abrangente

Nós projetamos produtos que são simples e, no entanto, abrangentes. E temos a mesma postura com nossa assistência. Com opções que vão de assistência técnica básica às que incluem acesso direto a assistência avançada por parte de engenheiros e atendimento personalizado.

Nomes de licenças	Padrão Incluídos com a compra	Aprimorado Incluídos em todos os agrupamentos	Extras aprimorados
Suporte Por meio de telefone e e-mail	Por 90 dias (somente em horário comercial)	Incluído (24 horas por dia, 7 dias por semana)	Acesso VIP (24 horas por dia, 7 dias por semana)
Atualizações e patches de segurança Por toda a vida útil do produto	Incluído com uma inscrição ativa ao software	Incluído com uma inscrição ativa ao software	Incluído com uma inscrição ativa ao software
Atualizações e aprimoramentos das funcionalidades do software	Incluído em 90 dias	Incluído	Incluído
Consultoria Consulta remota sobre configuração e segurança do firewall junto aos Engenheiros da Assistência Técnica Avançada Sophos			Incluído (até 4 horas)
Garantia e RMA [Return Merchandise Authorization (Autorização de Devolução de Mercadoria (ADM)] Para todos os aparelhos de hardware	1 ano (retorno/substituição)	Troca avançada (máx. 5 anos)	Troca avançada (máx. 5 anos)
Gerente de Contas Técnicas Gerente de Contas Técnicas indicado especificamente		Opcional (custo extra)	Opcional (custo extra)