Secur.Net
Always online, always secure!

Solução de Segurança Checkpoint

RELOAD - CONSULTORIA INFORMATICA, LDA

Assinado de forma digital por RELOAD - CONSULTORIA INFORMATICA, LDA
DN: c=PT, ou=Certificate Profile - Qualified Certificate - Representative, ou=Terms of use at https://www.digitalsign.pt/ECDIGITALSIGN/rpa, ou=Entitlement - ASSINAR EM PLATAFORMAS ELECTRONICAS DE CONTRATACAO, ou=ID - 506210855, ou=Address1 - RUA DR. JOAQUIM MANUEL DA COSTA, N.946 FRACCAO B, ou=PostalCode - 4420-437, ou=Representative Name - FABIO CLAUDIO DE JESUS TEIXEIRA MELRO, ou=Representative ID - CC 13393263, cn=RELOAD - CONSULTORIA INFORMATICA, LDA, email=fabio.melro@securnet.pt
Dados: 2016.11.29 17:36:25 Z

Cliente	Município de Pombal
Account Manager	Sílvio Paiva
N.º Proposta	PRP20160740
Versão	5.0
Data	28-11-2016

Índice

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

Versões documentais

Data	Versão	Autor	Notas
24-06-2016	1.0	Sílvio Paiva	Elaboração da presente proposta
28-06-2016	2.0	Sílvio Paiva	Elaboração da presente proposta
02-08-2016	3.0	Sílvio Paiva	Elaboração da presente proposta
24-10-2016	4.0	Sílvio Paiva	Elaboração da presente proposta
28-11-2016	5.0	Sílvio Paiva	Elaboração da presente proposta

Aprovação do documento

Versão	Revisto por:	Notas
1.0	Miguel Santiago	
2.0	Miguel Santiago	
3.0	Miguel Santiago	
4.0	Miguel Santiago	
5.0	Miguel Santiago	

Confidencialidade

Este documento foi elaborado pela SecurNet para a Município de Pombal. A Município de Pombal não tem qualquer limitação na utilização deste documento dentro da sua infraestrutura. A utilização, cópia, distribuição fora da infraestrutura da Município de Pombal sem o prévio consentimento escrito da SecurNet é estritamente proibido.

Contactos

Todas as questões originadas na interpretação do presente documento devem ser dirigidas a:

Gestor de Engenharia e Projeto		Gestor Comercial	
Miguel Santiago		Sílvio Paiva	
Telefone:	+ 351 22 467 30 94	Telefone:	+ 351 22 467 30 94
Movél:	+ 351 91 220 27 36	Movél:	+ 351 91 030 54 20
Email:	miguel.santiago@Securnet	Email:	silvio.paiva@Securnet.pt

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

1 Breve Introdução

1.1 A ReLoad – SecurNet

A SecurNet é uma empresa de consultoria informática que actua primordialmente nas áreas da segurança de dados, comunicações e sistemas.

A empresa tem escritórios em Lisboa e Porto, contando com colaboradores certificados em tecnologias de informação, com experiência de projeto nas áreas de segurança perimétrica, segurança interna, acessos remotos, portais seguros, antivírus, gestão de patches, redes de comunicações, storage e backup.

A SecurNet apresenta uma especialização para auditorias práticas, onde se beneficia a deteção de problemas e a sua imediata correção, fornecendo desta forma um serviço integrado de consultoria e auditoria com base em "best practices" e no ISO 27001/27005, tendo realizado trabalhos de auditoria e preparação para a certificação.

Para além dos serviços de consultoria e auditoria, a empresa presta serviços de NOC (Network Operation Center) sobre as infraestruturas dos seus clientes, fornecendo serviços de monitorização e gestão dos recursos informáticos, sistemas de segurança e comunicações, estando igualmente disponíveis serviços de monitorização 7x24 de sistemas Internet, com alarmística de problemas via WEB e SMS.

Áreas de Actividade

- Monitorização remota de Serviços
- Monitorização de vulnerabilidades
- Consultoria de comunicações e segurança
- Auditorias de segurança, comunicações
- Infraestruturas de segurança
- Sistemas de gestão de Patches
- Redes Wireless
- Storage, NAS e Backup
- Alta disponibilidade de sistemas

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

1.2 Parcerias

As soluções da SecurNet encontram-se relacionadas com diversas entidades e fabricantes. Consideramos determinante a existência de uma estrutura de ligação, capaz de proporcionar um elevado nível de conhecimento.

Este esforço de adaptação contínuo, e a constante preocupação com a satisfação das necessidades dos seus clientes, leva a que a Secur.Net tenha estabelecido e mantido acordos estratégicos com os principais líderes tecnológicos a nível mundial.

Serviços especializados

A SecurNet é uma empresa especializada em serviços avançados de consultoria, integração e manutenção!

Estratégia e Desenho

É a fase mais crítica de qualquer solução! Onde se analisam os requisitos do cliente e valida a estratégia que melhor se adapta.

A SecurNet integra nos seus quadros uma equipa com vasta experiencia em planeamento e desenho de soluções TI.

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

Integração

Mais de 12 anos de experiencia permitem à SecurNet desenvolver fortes parcerias com os principais fabricantes líderes de mercado mas também encontrar visões inovadoras na abordagem aos principais paradigmas atuais das TI.

A SecurNet investe em planos de formação e certificação contínua da sua equipa técnica para garantir a melhor solução para cada área!

1.3 Operação e Manutenção

A SecurNet oferece um conjunto de opções para ajudar o cliente a produzir e manter um plano apropriado e atualizado, refletindo as necessidades atuais e futuras!

- Suporte Proactivo - Assistir no diagnóstico e resolução de incidentes e problemas relacionados com desempenho e capacidade!
- Suporte 8x5/24x7 – Apoio na resolução de incidentes no regime que melhor se adequa às necessidades do negócio do cliente!
- Operação – Apoio em regime de prestação de serviços total ou parcial permitindo que o cliente se dedique à continuidade do seu negócio!

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

2 Descrição da Proposta

2.1 Objetivo e âmbito

O principal objetivo desta proposta é a apresentação de uma solução de segurança de perímetro para a infraestrutura TI do Município de Pombal em resposta ao procedimento "Aquisição de Solução de Firewall" Processo nº 077/AJD/SA/16.

A solução apresentada cumpre com os requisitos técnicos do presente Caderno de Encargos:

1. A *appliance* a fornecer deverá ser composta pelos seguintes requisitos gerais:
   a. 1 x Appliance 5400 Next Generation Threat Extraction (NGTX) ou equivalente;
   b. 1 x Smart-1 205 Appliance with Policy, Log and Event Security Management for 5 Security Gateways, ou equivalente;
   c. Permitir 50 vpns em concorrência (Blade Mobility-50 ou equivalente);
   d. Deverá ser instalado num servidor virtual a ser disponibilizado pelo Município de Pombal) de forma a permitir o armazenamento periódico dos logs da Firewall pelo menos com um período de retenção de 1 ano;
   e. Deverá estar contemplado a funcionalidade de Anti-SPAM;
   f. A Appliance atual 4400 servirá como spare da nova solução;
   g. A solução deverá contemplar um sistema de prevenção do dia Zero (SandBlast Threat Prevention, ou equivalente);
   h. As funcionalidades da solução deverão ser:

	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPSec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
URL Filtering	✓	✓
SandBlast Threat Emulation	×	✓
SandBlast Threat Extraction	×	✓

2. Componente VPN:
   a. Suporte de IKEv1 e IKEv2
   b. Tem que suportar criptograficamente 3DES e AES-256 para IKE Phase I e II IKEv2
   c. Tem que suportar pelo menos os seguintes grupos de Diffie-Hellmas: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
   d. IKE Phase2 – Encriptação de Dados (DES, 3DES, AES-128, AES-192, AES-256,e NULL)
   e. IKE Phase2 - Suporte Integridade dos Dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
   f. Suporte de VPNs Site to Site – Full Mesh (all to all) ou Star (Remote to center)
   g. Suporte de IKE com PKI e pre-shared Secret
   h. Aprovisionamento automático de VPNs site-to-site

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

i. Gestão automática de túneis IPSec de backup
j. Suporte routing dinâmico em VPN IPSec
k. Cliente VPN (Windows XP, MacOS, iOS, Android)
l. Suporte de One-Time Password para VPN sem recurso a terceiros fabricantes ou servidores adicionais
m. Criptografia (3DES, IKE, AES)
n. Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores
o. Single Sign On VPN
p. SSL VPN para 50 utilizadores concorrentes (mínimo)

3. Componente de Gestão:
   a. Interface de gestão em plataforma Web por HTTPS
   b. Alertas (Email, SMS, Consola, Traps SNMP)
   c. Comunicação Cliente-Servidor cifrada
   d. SNMP v2/v3
   e. Possibilidade de alta disponibilidade da componente de Gestão
   f. Os módulos de inspeção e de gestão deverão correr na mesmo equipamento físico
   g. Suporte de "Change Management" embebida
4. Funcionalidades de Logging:
   a. Logging de toda a comunicação que atravessa o firewall
   b. Logging de toda a comunicação rejeitada pelo firewall
   c. Permitir a análise de logs com programa apropriado
   d. Logging de todas as configurações alteradas no Firewall (explicitando Quem/Quando/o Quê?)
5. Componente Networking:
   a. Suporte Multiplos Links WAN - Redundância
   b. Suporte Multiplos Links WAN - Balanceamento de carga
   c. Routing baseado em políticas
   d. Rotas Estáticas
   e. IPv6
   f. 802.1q- VLAN Tagging
   g. DHCP Relay e DHCP Server
   h. Spanning-Tree (802.1d)
   i. Suporte 802.3.ad e também LACP – Agregação de Links (Activo-Activo ou Activo-Passivo)
   j. Suporte de Dead Gateway Detection
   k. Job Scheduler
   l. Suporte TOS/DiffServ
   m. Suporte para Virtual Switch
6. Componente de Networking em IPv6:
   a. Rotas estáticas
   b. RIPv6
   c. BGP4+
   d. OSPFv3
   e. DNS

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

   f. Endereçamento de interfaces
   g. IPv6 Tunnel sobre IPv4
   h. IPv4 tunnel sobre IPv6
   i. Packet e network sniffing
   j. NAT
   k. Troubleshooting específico IPv6
7. Protocolos de Routing:
   a. OSPF
   b. BGP
   c. RIP
   d. IGMP
   e. PIM SM
   f. PIM DM
8. Requisitos mínimos Performance:
   a. Firewall througput: >=10 Gbps
   b. IPS througput: >=1.08 Gbps
   c. NGFW througput (Firewall, Application Control, IPS): >= 690Mbps
   d. VPN througput AES-128: >=2.16 Gbps
   e. Conexões Concorrentes (Firewall) >= 1,2 Milhões
   f. Novas sessões por segundo (Firewall) >= 40000
   g. Nº túneis IPsec VPN >= 25000
   h. Nº Vlans >=1024
   i. Nº conexões concurrentes em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 20000
   j. Nº de transações HTTP por segundo em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 2700
   k. Nº de utilizadores concurrentes suportados em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 250
   l. Nº de novas conexões por segundo em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 650
9. Certificações necessárias:
   a. ICSA Labs IPSec 1.3
   b. ICSA Labs Corporate Firewall
   c. Common Criteria EAL2+ e EAL4+
   d. DoD UC APL
   e. AVA VLA.3
   f. VPN Consortium - VPNC Certified
   g. FIPS 140-2 Nível 1 e Nível 2
10. Monitorização e Reporting:
   a. Visualização em tempo real das ligações activas
   b. Capacidade de Criação reports directamente dentro da Firewall
   c. O módulo de reporting e e de correlação de eventos de segurança deverá correr no mesmo equipamento que faz a inspeção do tráfego
   d. Estatisticas da performance do hardware
   e. Gráficos de utilização por protocolo, máquina, utilizadores num determinado momento

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

f. Top de ataques de segurança
g. Top de destinos de ataques
h. Top de origem de ataques
i. Top Serviços
j. Top de regras usadas
k. Top de regras de rejeição
l. Top de regras de aprovação
m. Top de tráfego por serviço de rede
n. Top de tráfego por utilizador
o. Top de tráfego Web

11. Funcionalidade de Application Control e URL Filtering:
    a. Actualização de assinaturas automática
    b. Controlo granular de redes sociais, aplicações e funcionalidades dentro de aplicações: identificar, permitir, bloquear ou limitar o uso;
    c. Granularidade das políticas e reporting ao nível do utilizador ou do grupo;
    d. Alertas para o utilizador em tempo real, educação sobre riscos e políticas organizacionais através do UserCheck;
    e. Relatórios intuitivos, granulares e com visibilidade interna utilizando ferramentas forenses;
    f. Reconhecimento de widgets Web 2.0 >=240000
    g. Reconhecimento de aplicações >=4700
    h. Solução tem que ter categorizado >= 200 milhões URLs e ter uma cobertura de mais do que 85% da Alexa's top 1Milhão de sites
    i. Controlo por largura de banda de cada aplicação Web 2.0
    j. Inspecção SSL
    k. Criação de assinaturas personalizadas e privadas
    l. Criação de regras pelo índice de criticidade de segurança da aplicação
    m. Criação de regras pelo índice de popularidade da aplicação
    n. Criação de regras pela categoria da aplicação
    o. Criação de regras pela tecnologia da aplicação
    p. Criação de regras pelo fabricante da aplicação
    q. Controlo de utilizadores dentro de uma solução de VDI ou Terminal Services
    r. Inspeccionar o trafego mesmo dentro de SSL encriptado. Trafego tanto Inbound como Outbound
    s. Alertar e questionar os utilizadores através de popups sobre a utilização das diferentes aplicações.
12. Componente de Antivirus:
    a. Fabricante deve ter um Anti-Virus integrado na firewall de próxima geração.
    b. O modulo de Anti -Virus deve ser administrado a partir de uma consola central.
    c. O modulo de Anti-Virus deve ter uma correlação de eventos centralizado e mecanismo de reporting.
    d. Aplicação de anti-vírus deve ser capaz de impedir o acesso a sites mal-intencionados
    e. Modulo de anti-vírus deve ser capaz de inspecionar tráfego com criptografia SSL.
    f. Anti-Virus deve ser ter atualizações em tempo real a partir de um serviço baseado na nuvem do fabricante.

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

g. Anti-Virus deve ser capaz de parar a entrada de ficheiros maliciosos.
h. Políticas anti-vírus deve ser gerido centralmente com uma política granular e eficaz.

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

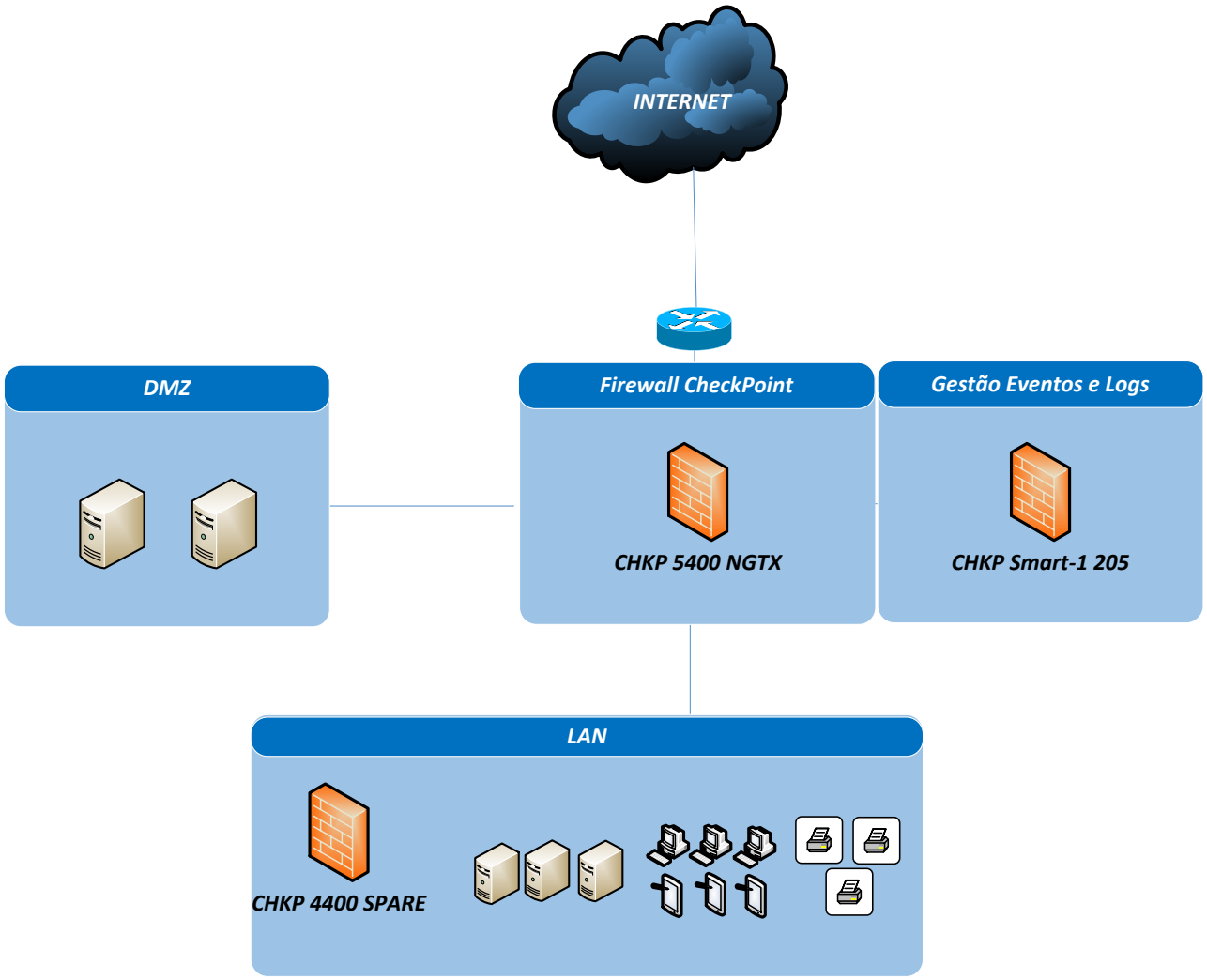
NIF 506 210 855

3 Topologia Proposta

Solução CheckPoint 5400 NGTX + Smart-1 205 – Gestão de Eventos e Logs.

A Appliance Check Point 4400 atual ficará como spare da nova solução.

Será criado um Syslog para armazenar os logs desta plataforma.



ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

4 Descrições técnicas

A nova plataforma de segurança periférica apresentada é baseada numa solução com tecnologia Check Point UTM, a qual permite a gestão integrada de todos os fluxos de informação e concentra toda a análise, configurações e logs sobre uma única plataforma de gestão. Esta solução permitirá, assegurar serviços de segurança e gestão. Esta situação permite ganhos na gestão dos recursos tecnológicos, humanos e financeiros. Através da arquitectura proposta, centralizam-se de um modo seguro as interfaces de gestão da infra-estrutura de segurança e a gestão das políticas de segurança para o nó central.

A arquitectura desta solução tem um nó de inspecção que aloja uma "Plataforma de Segurança Check Point" que é responsável por implementar e gerir as políticas de segurança na rede. Na arquitectura Check Point, existe um "SmartCenter", que é responsável pelas políticas de segurança a implementar e serve de igual forma como repositório dos logs. Os eventos de segurança são igualmente reportados à "Management Station", pelo que é possível através de uma única interface de gestão saber o estado das ligações, o accounting, e eventos de segurança do IPS. Como informação adicional também é possível saber a taxa de utilização do CPU, da memória, o número de pacotes/segundo e o número de sessões IPSEC.

A plataforma de Firewall proposta será ainda responsável pela gestão de largura de banda de todos os circuitos existentes, maximizando de uma forma simples e transparente os acessos aos serviços da rede Lan. Através da solução de QoS da Check Point, será possível garantir largura de Banda para aplicações criticas.

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

NIF 506 210 855

4.1 Principais Funcionalidades Check Point

As appliances baseadas na nova tecnologia Blade System (R77) permitem um sistema de segurança lógico, independente, modular e gerido centralmente. Os Blades permitem a rápida activação e configuração de acordo com as especificidades de cada empresa. Sempre que as necessidades evoluem é possível adicionar e activar novos Blades e respectivas funcionalidades, estendendo assim a plataforma de segurança existente, sem a necessidade de substituição de hardware.

Principais Benefícios desta Arquitectura:

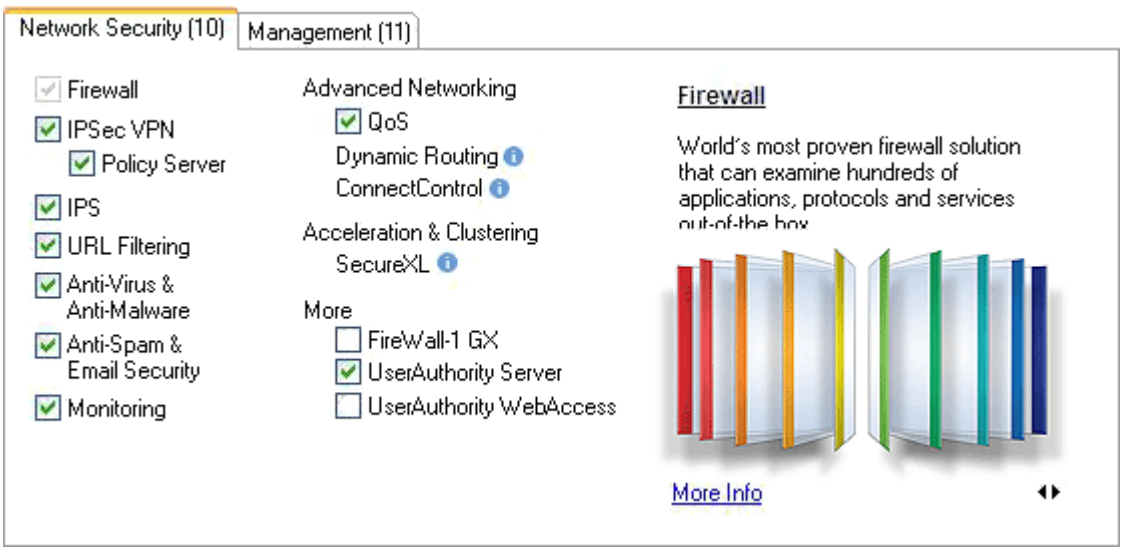
- **Flexibilidade –** Permite o nível de protecção ao mesmo nível de investimento
- **Gestão –** Facilita o deployment rápido dos serviços de segurança, Incrementando a produtividade através da gestão centralizada
- **Total Security –** Permite o nível de segurança apropriado para cada enforcement point e em todas as layers da rede.
- **Baixo TCO –** O investimento está protegido através da consolidação e do hardware na infra-estrutura
- **Performance Garantida –** Permite o provisioning dos recursos que garantem os níveis de serviço.

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855



4.1.1 Acessos Remotos – Check Point Mobile Blade

Hoje em dia é cada vez mais natural que parceiros e funcionários acedam às aplicações e recursos da rede através de terminais não seguros. O acesso a aplicações Web permite o crescimento e potencia os negócios de maneira mais fácil e de forma mais económica, embora aumente de igual forma os riscos de segurança, ou seja, a promoção de um negócio e a sua maximização, são inversamente proporcionais à segurança no acesso aos dados. A Check Point tem investido amplamente nestas tecnologias e respetivas funcionalidades que vão para além da conectividade SSL, neste momento todo o esforço realizado pela Check Point traduz na oferta de grau de proteção mais abrangente às aplicações Web e aos terminais utilizados no respetivo acesso.

O Mobile Blade possui as seguintes características:

- Conectividade WEB Segura
- Segurança para os Servidores
- Segurança Adaptativa para Clientes
- Acesso Remoto com VPN SSL
- Gestão e Configuração Simples

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

As ligações VPN SSL via browser oferecem um meio conveniente para o acesso de funcionários remotos e parceiros de negócios à rede corporativa a partir de qualquer lugar. Esse método simplifica a conectividade e reduz os custos nos acessos. No entanto, as ligações remotas tornam a segurança das informações uma tarefa complexa. Por exemplo: o acesso via browser permite que qualquer utilizador ou parceiro possa aceder à rede através de um computador fora da organização, tal como escritórios remotos, cybercafés, etc. Esses terminais remotos oferecem pouca ou nenhuma segurança de software ou podem ainda conter "malware". A conectividade de terminais remotos sem proteção através de uma gateway VPN SSL deixa a organização vulnerável a ataques e atividades maliciosas. A falta de gestão eficaz da segurança dos terminais remotos e da proteção contra ataques nas ligações VPN SSL, aliada à simplicidade inerente destas soluções VPN SSL, expõe a organização a vários tipos de ameaças.

O Mobile Blade é uma gateway que fornece acesso de utilizadores e parceiros de negócio remotos aos recursos da rede corporativa via Web. O acesso à rede é realizado através de ligações seguras (SSL), incrementando o nível de segurança através da inspeção e validação do terminal remoto que deseja ligar-se à infraestrutura, impedindo a ligação de terminais que não cumpram a politica de segurança adoptada na Infraestrutura.

Através de um portal Web Mobility Blade integrado, os utilizadores podem aceder a recursos e aplicações Web, partilhar ficheiros e mensagens de mail. Para maior flexibilidade, o portal Mobility Blade pode ser personalizado, incluindo suporte a diversos idiomas.

Para as aplicações cliente-servidor não baseadas em ambientes Web, o Mobile Blade fornece acesso seguro à rede através do SSL Network Extender™. Este modulo consiste numa extensão do browser, capaz de encapsular o tráfego das aplicações do terminal remoto através de ligações SSL. Oferece suporte a qualquer aplicação baseada em IP tais como TCP, UDP e ICMP, sem necessidade de configurações complexas para cada aplicação.

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

4.1.2 Identity Awareness Software Blade

Check Point Identity Awareness Software Blade providencia uma visibilidade granular dos utilizadores, grupos ou máquinas, fornecendo uma aplicação imcomparável no controlo de acesso através da criação de políticas precisas baseadas na identificação.

Aumento da visibilidade sobre as actividades dos utilizadores

- Acessos dos utilizadores aos recursos da empresa e às aplicações da internet são geridos centralmente.
- Enforcement de Políticas granulares por user, grupo e máquina.
- Facilidade em diferenciar diversos grupos tais como: empregados, convidados, clientes, etc.

Aumento do controlo dos recursos da Empresa

- Acesso granular para data centers, aplicações e segmentos de rede por user, máquina ou local.
- Prevenção de acessos não autorizados aos recursos, enquanto permite o trabalho remoto de funcionários da empresa.
- Prevenção de ameaças e de perda de informação através da restrição, de acesso aos recursos, de users e máquinas.

Fácil de Implementar em qualquer organização

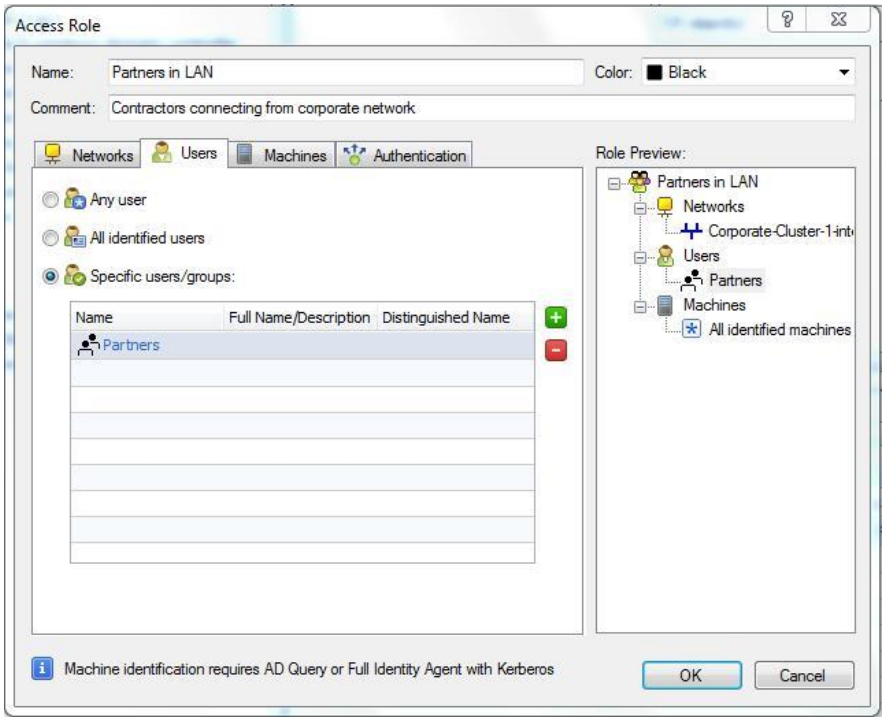
- Integrada na arquitectura de software blade da Check Point.
- Permite identidade escalável na partilha entre gateways.
- Fácil integração com a Active Directory (AD) com múltiplas opções de deployment, clientless, Captive Portal ou Identity Agent.

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855



4.1.3 O Módulo ADN

O FloodGate-1 controla precisamente o fluxo de tráfego de entrada e de saída nos pontos de acesso da Internet, baseando-se em políticas de qualidade do serviço (QoS). Uma política de QoS consiste nas regras de tráfego que atribuem privilégios da largura de banda a classes de tráfego específicas.

Cada regra define critérios da classificação do tráfego e controles correspondentes de QoS.

O ADN classifica o tráfego usando os seguintes critérios:

- Pelo endereço de origem, pelo de destino, pelo sentido do tráfego, pelas horas do dia
- Por tipos de serviço IP associado a aplicações (mais de 150 que são suportados)
- Por grupos de utilizadores (em ambientes de endereços IP fixos e dinâmicos)
- Por endereços URL específicos

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

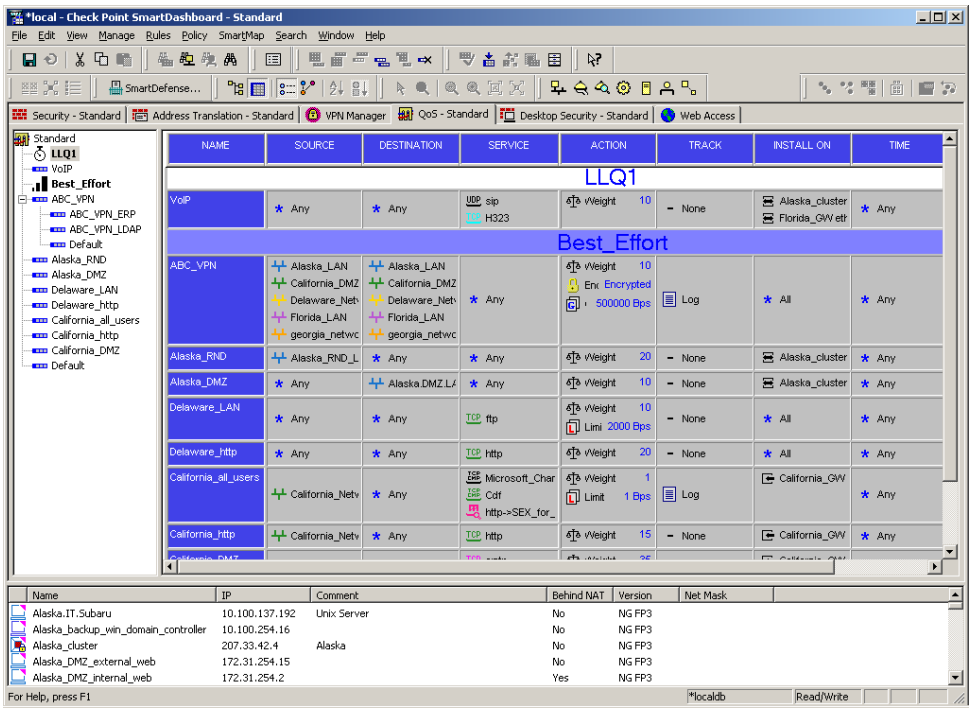
www.securnet.pt

NIF 506 210 855

Assim que um pacote é classificado, os seus campos de controlo de QoS são alterados de forma a assignar-lhe mais privilégios caso se trate de tráfego crítico, ou menos privilégios caso se trate de tráfego pouco importante.

Com a manipulação destes parâmetros nos pacotes é possível gerir a largura de banda dum acesso atendendo a objectivos de negócio. Assim, por exemplo, num determinado site, pode ser duas vezes mais importante o tráfego HTTPS (responsável pelo transporte de transações electrónicas seguras) que o trafego em HTTP (responsável pelo transporte de informação de consulta a um catálogo de compras). Quando ocorrer congestão de tráfego, o FloodGate-1 assegura-se de que a relação dos dados transportados nas transacções seguras e o de acesso às páginas do catálogo seja mantida em 2:1.

Numa outra implementação, pode ser mais importante atribuir maior largura de banda aos acessos dos utilizadores remotos que usam VPNs, por se tratarem de vendedores que estão a colocar encomendas em determinado sistema. Sem controlo de largura de banda, em situações de congestionamento de tráfego, estas operações destes vendedores seriam perturbadas, por exemplo, pelo tráfego de carácter lúdico. A figura seguinte ilustra uma implementação de gestão de largura de banda:



ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

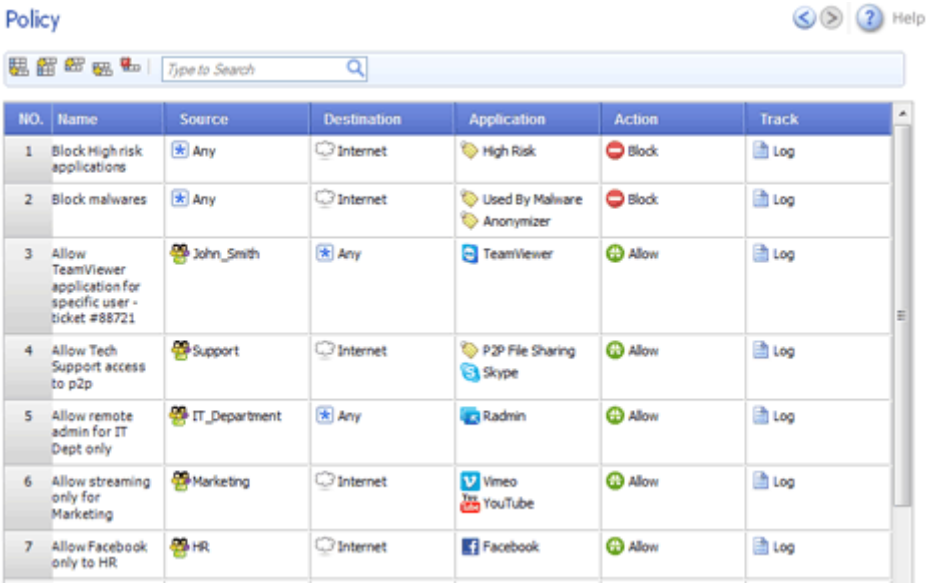
NIF 506 210 855

4.1.4 Application Control

A Check Point possui uma Base de Dados de aplicações conhecidas muito alargada que permite obter total visibilidade e controlo sobre as aplicações existentes e utilizadas na internet. Este Blade inclui updates de milhares de novas aplicações e serviços baseados em Cloud para Widgets das redes sociais.

Algumas das funcionalidades que destacamos do Application Control são:

- Controlo granular de redes sociais, aplicações e funcionalidades dentro de aplicações: identificar, permitir, bloquear ou limitar o uso.
- Granularidade das políticas e reporting ao nível do utilizador ou do grupo.
- Alertas para o utilizador em tempo real, educação sobre riscos e políticas organizacionais através do UserCheck.
- Relatórios intuitivos, granulares e com visibilidade interna utilizando ferramentas forenses.
- Mais de 150 Categorias agrupadas de uma forma intuitiva – incluindo Web 2.0, IM, P2P, Voice & Video e File Share.

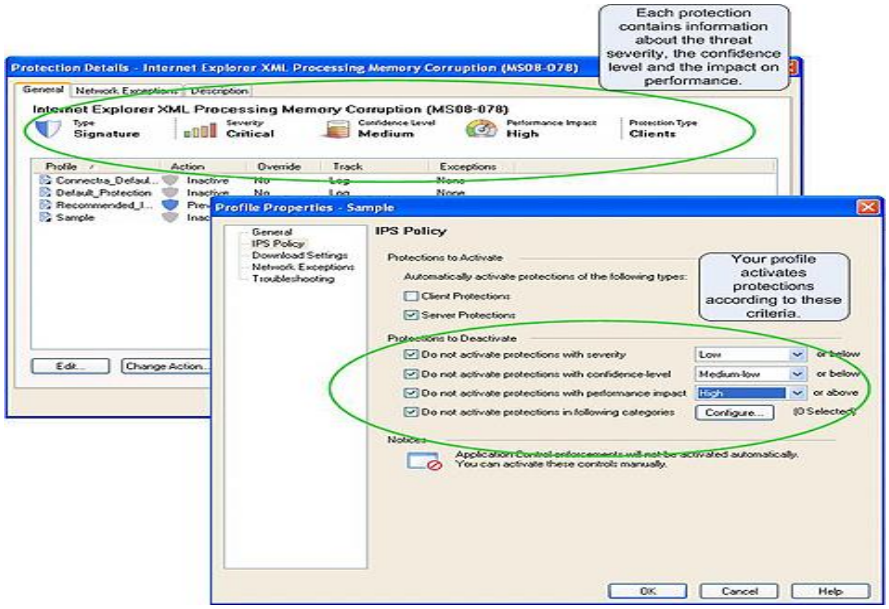


ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855



4.1.5 IPS

NSS Labs top-rated IPS Software Blade oferece prevenção completa e pró-ativa intrusão. Classificado como 1 em cobertura ameaça Microsoft e Adobe 3 anos em uma fileira, ele protege sua rede através do navegador e vulnerabilidade aplicação exploits oportuna e efetivamente impedindo .

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

5 Especificações do Hardware

5.1 Appliance Checkpoint 5400

Abaixo é apresentada uma imagem ilustrativa da Appliance Check Point 5400:

No quadro abaixo são apresentadas a s performances em ambiente produtivo desta appliance:

Production Environment Performance[1]	
SecurityPower™ Units (SPU)	600 SPU
Firewall throughput	10 Gbps
IPS throughput	1.08 Gbps
NGFW throughput (Firewall, Application Control, IPS)	690 Mbps
Threat prevention throughput[2]	330 Mbps
Ideal Testing Conditions Performance (RFC 3511, 2544, 2647, 1242)	
Firewall throughput, 1518 byte UDP	22 Gbps
Connections per second	150,000
Concurrent connections	3.2 to 6.4[3] million
VPN throughput, AES-128	2.16 Gbps
IPS throughput	3.9 Gbps
NGFW throughput (Firewall, Application Control, IPS)	3.4 Gbps

[1] Performance measured with real-world traffic blend and content, a typical rule base, updated recommended signatures, NAT and logging enabled, [2] FW, IPS, APPCTRL, AV, AB, URLF, [3] with maximum memory

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

5.2 Checkpoint Smart-1 205 Appliance

Appliances	205
	
Policy & Log Performance	
Managed Gateways	5
Maximum Domains (Multi-Domain Management)	-
Indexed Logs/Sec [3]	3,000
SmartEvent NGSE Performance	
Events per day [4]	350,000
Log size per day (GB) [5]	3.5
Number of users [5]	900
Hardware Specifications	
Storage (HDD)	1 x 1 TB
RAID Type	-
Storage (SSD)	-
Memory Extension (RAM)	default 4GB
Interfaces	
Built-in Network Interfaces	4xCopper GbE
Extended Network Interfaces	-
Fiber Channel SAN Card	-
Management (Console Port)	1xRJ45
Out-of-band Management (LOM)	-
USB Ports	2

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855

6 Serviços

Na proposta apresentada estão contabilizados os serviços necessários para a implementação, configuração e testes à solução necessários.

As tarefas definidas a desempenhar serão:

- Reunião de Arranque do Projeto
- Instalação Física das Appliances
- Configuração de SecurePlatform
- Configuração de SmartCenter
- Configuração da Politica de Segurança
- Configuração de Application Control blade
- Configuração do IPS
- Configuração da Smart-1 205
- Configuração de Servidor Syslog
- Testes à Solução Implementada
- Formação "On Job"
- Memória Descritiva da Solução

6.1 Requisitos e pressupostos

O âmbito desta proposta pressupõe a existência de todas a condições necessárias para o correto funcionamento dos equipamentos, nomeadamente espaço em bastidores, cablagem de infraestrutura e demais condições infraestruturais prévias (nomeadamente conectividade e energia) à instalação dos equipamentos propostos.

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

7 Condições Comerciais

7.1 Proposta Comercial

Cliente:	Municipio de Pombal	**Data:**	28-11-2016
Contacto:	Nuno Salvador		
Descrição da Solução:	Solução de Segurança Check Point - 3 Anos		
Proposta Nº	PRP20160740	**Revisão:**	V.5

P/N	Qtd.	Descrição	Valor Unit.	Valor Total
Solução Check Point com suporte válido por 3 anos				
CPAP-SG5400-NGTX	1	5400 Next Generation Threat Extraction Appliance	3.010,64 €	3.010,64 €
CS-CPAP-SG5400-NGTX	3	CES Standard for 5400 Next Generation Threat Extraction Appliance	940,86 €	2.822,58 €
CPSB-NGTX-5200-2Y	1	Next Generation Threat Extraction Package for 2 year for 5200 Appliance	6.047,66 €	6.047,66 €
CPAP-SM205	1	Smart-1 205 Appliance with Policy, Log and Event Security Management for 5 Security Gateways	1.027,66 €	1.027,66 €
CS-CPAP-SM205	3	CES Standard for Smart-1 205 Appliance with Policy, Log and Event Security Management for 5 Security Gateways	330,32 €	990,96 €
CPSB-EVS-SM205-2Y	1	Smart Event and Smart Reporter for Smart-1 205 Appliance, for 2 years	1.364,37 €	1.364,37 €
CP-CES-MOB-50	1	CES Standard MOB-50 (Valores de renovação por 3 anos)	397,82 €	397,82 €
Serviços				
SERVICOS	1	Serviços de Implementação e Configuração da Solução	3.250,00 €	3.250,00 €

Total da Solução	**18.911,69 €**

7.2 Imposto sobre o Valor Acrescentado

Todos os preços indicados para a solução proposta não incluem Imposto sobre o Valor Acrescentado (I.V.A.), à taxa legal em vigor.

7.3 Condições de Pagamento

De acordo com as condições vigentes no procedimento "Aquisição de Solução de Firewall" Processo nº 077/AJD/SA/16.

7.4 Prazo e Validade da Proposta

De acordo com as condições vigentes no procedimento "Aquisição de Solução de Firewall" Processo nº 077/AJD/SA/16.

ReLoad – Consultoria Informática, Lda.
www.securnet.pt
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94
Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04
NIF 506 210 855

7.5 Prazo de Entrega e Execução

De acordo com as condições vigentes no procedimento "Aquisição de Solução de Firewall" Processo nº 077/AJD/SA/16.

7.6 Estimativas de Valores para Anos futuros

A presente solução é apresentada com suporte de Hardware e Software direta do fabricante Check Point por um período de 36 meses (3 anos) após este período o preço estimado de renovação da solução por um novo período de 3 anos é de 10 000€ + IVA.

7.7 Garantia de Sigilo

De acordo com as condições vigentes no procedimento "Aquisição de Solução de Firewall" Processo nº 077/AJD/SA/16.

ReLoad – Consultoria Informática, Lda.
Norte:
R. Dr. Joaquim Manuel da Costa, N.º 946 Fracção B
4420-437 Valbom Gondomar
Telefone: 22 467 30 94

Sul:
Rua Campos Júnior n.º 5 A
1070 – 306 Lisboa
Telefone: 21 362 22 04

www.securnet.pt

NIF 506 210 855