CONSULTA PRELIMINAR AO MERCADO

N.º CPM/01/AECC/2024

Aquisição de bens e serviços para a implementação da rede Wi-Fi e Segurança na Associação de Ensino Cristóvão Colombo

(artigo 35.º-A do Código dos Contratos Públicos)

ÍNDICE

1. TERMOS DA CONSULTA PRELIMINAR AO MERCADO

2. ENQUADRAMENTO

3. FORMA DE PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

4. INFORMAÇÃO PRETENDIDA

5. PRAZO DA CONSULTA

1 – TERMOS DA CONSULTA PRELIMINAR AO MERCADO

A realização da presente consulta preliminar ao mercado, ao abrigo do disposto no artigo 35.º-A do Código dos Contratos Públicos na sua redação atual (doravante CCP), visa habilitar a Associação de Ensino Cristóvão Colombo na preparação do subsequente procedimento pré-contratual a adotar, garantindo o cumprimento pelos Princípios da Concorrência, da Igualdade de Tratamento e da Não Discriminação e da Transparência, enquanto princípios basilares da contratação pública.

A presente consulta preliminar tem uma natureza informativa e informal, conforme dispõe o n.º 1 do artigo 35.º-A do CCP, pelo que, os elementos que sejam voluntariamente remetidos pelos operadores económicos que pretendam participar, não têm um carácter vinculativo, ficando, assim, na discricionariedade da Associação de Ensino Cristóvão Colombo, a sua incorporação, ou não, nas peças do procedimento para a formação do contrato a celebrar.

Em cumprimento dos números 3 e 4 do artigo 35.º-A do CCP, a Associação de Ensino Cristóvão Colombo adota, desde já, seguintes medidas adequadas à prossecução do Princípio da Concorrência, da Igualdade de Tratamento e da Não Discriminação e da Transparência:

a) Publicitação da presente consulta preliminar de forma aberta, com acesso de participação a todos os operadores económicos interessados, no seguinte sítio da internet da Associação de Ensino Cristóvão Colombo, **até ao próximo dia 28 de outubro de 2024**: https://epcc.pt/

b) Incorporação de uma cláusula específica no caderno de encargos respeitante à informação relativa à realização da presente consulta preliminar ao mercado, e disponibilização de todas as informações pertinentes trocadas no âmbito da presente consulta preliminar, caso sejam solicitadas, aquando do termo do prazo para apresentação de propostas, como medida que garante o cumprimento do Princípio da Concorrência, com exceção das informações prestadas cujos

participantes tenham solicitado previamente à Associação de Ensino Cristóvão Colombo a sua classificação como confidenciais à luz das normas legais em vigor aplicáveis a esta matéria.

2 – ENQUADRAMENTO

A Associação de Ensino Cristóvão Colombo pretende contratar serviços descritos no anexo único, os quais deverão ser fornecidos nas suas instalações.

3. FORMA DE PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

A prestação voluntária de informação pelos operadores económicos deverá ser feita através de email para o seguinte endereço de correio eletrónico: financeiro@epcc.pt

4. INFORMAÇÃO PRETENDIDA

Em face do exposto, pretende-se, assim, com esta consulta preliminar ao mercado que antecede a decisão de contratar, auscultar o mercado, com o propósito de obter as seguintes informações relevantes à construção das peças do procedimento a adotar:

a) Documento contendo os preços unitários, indicando também o preço global. A informação relevante que a Associação de Ensino Cristóvão Colombo pretende obter neste âmbito é o valor máximo de mercado, a fim de ficar habilitada à construção do preço base adequado.

b) Indicação do prazo razoável para o fornecimento e calendarização.

A adjudicação será feita segundo o critério da proposta economicamente mais vantajosa, determinada pela modalidade da avaliação do preço, prevista na alínea b) do n.º 1 do artigo 74.º do CCP.

5. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite até à data de **28/10/2024**.

Anexo Único

(Caraterísticas técnicas)

Equipamento Ativo

Rede Ativa* - Trabalhos e Materiais	Quantidade
Equipamentos networking	
Switch 48 portas Gibabit e PoE, 4*GE SFP ports, PoE+,AC	3
Equipamentos WIFI	
AP tipo cluster Sala Aulas, com as características indicadas	10
Suporte fabricante /atualizações	10
Equipamentos Segurança Periférica	
HW segurança periférica, exemplo Palo Alto Networks PA-450 ou similar	1
Montagem em rack adapters e todos os acessórios ao pleno funcionamento da solução.	1

Serviços de instalação e manutenção

Deverá ser assegurada a instalação e manutenção pelo período de 36 meses de todos os equipamentos contantes na proposta com as seguintes condições:

a) Operação e manutenção, suporte fabricante e gestão da solução para os elementos core;
b) Fornecimento e gestão da segurança periférica;
c) Assegurar a existência de um modelo de acompanhamento e monitorização de incidentes que garanta um horário ininterrupto, 24 horas por dia, 7 dias por semana, de atendimento técnico, um número telefónico único e a adequada identificação das avarias reportadas para resolução das mesmas;
d) Garantir a intervenção nas instalações da entidade adjudicante para resolução da avaria na impossibilidade de resolução remota da mesma;
e) Substituição / reparação em caso de avaria ou falha de funcionamento por uma unidade igual ou equivalente;
f) Facultar informação sobre o estado e evolução da resolução da avaria;
g) Garantir um serviço de manutenção eficaz com tempos de resposta e qualidade de serviço adequados à realidade escolar no prazo máximo de 6 horas lineares;
h) Permitir a monitorização de report de avarias dos equipamentos disponível online;
i) Garantir a gestão da solução de telecomunicações (networking e segurança periférica)

Fornecimento e Instalação de rede ativa WLAN

Rede Ativa* - Trabalhos e Materiais	Quantidade
Equipamentos networking	
Switch 48 portas Gibgabit e PoE, 4*GE SFP ports, PoE+,AC	3
Equipamentos WIFI	
AP tipo cluster Indoor, com as características indicadas	10
Suporte fabricante /atualizações	10
Equipamentos Segurança Periférica	
HW segurança periférica, exemplo Palo Alto Networks PA-445 ou similar	1
Montagem em rack adapters e todos os acessórios ao pleno funcionamento da solução.	1

Access Points

Pretende-se a aquisição de Access Point Gama Normal Indoor.

Obs. A solução terá de permitir uma gama maior densidade (ex. auditórios, embora não objeto de aquisição neste projeto).

Todas as tipologias deverão assegurar as seguintes características:

- Dual Radio 2,4GHz e 5GHz
- Certificação Wifi Alliance 802.11ax
- Certificação Wifi Alliance WPA3
- Certificação Passpoint Release 2
- Suporte de até 16 SSIDs no mesmo AP por rádio
- Filtros RF específicos para co-existência com redes móveis celulares (GSM, 3G, LTE) minimizando o seu impacto e/ou interferência na rede wifi.
- Beacon bluetooth 5 nativamente integrado

- Rádio Zigbee nativamente integrado
- Suporte de 802.11n/ac/ax packet aggregation: A-MPDU, A-MSDU
- Suporte de:
- MRC
- CDD/CSD
- STBC
- LDPC
- Capacidade de funcionar como analizador de espectro dedicado ou hibrido (spectrum analyzer e acessso Wifi)
- Suportar até pelo menos 256 dispositivos associados por rádio
- Capacidade de com o mesmo hardware/access point implementar solução/arquitectura do tipo:
    - AP Standalone
    - Cluster de APs (virtual controller) (integrando com os actuais APs da Secretaria Regional de Educação da Madeira)
- Gerida através de uma controladora centralizada wireless física ou virtual
- Gerida através de solução nativamente cloud – com capacidade de manter serviço wireless mesmo com perda de ligação à internet
- Access Point Remoto com criação de túnel seguro e encriptado com IPSec entre AP e aplliance centralizadora, para transporte de tráfego de clientes, através de redes não corporativas, de modo a difundir SSIDs corporativos em sites remotos e sem acesso via WAN corporativa.
- Mesh

Quando em funcionamento em modo cluster de access points deverão assegurar as seguintes funcionalidades:

- Funcionamento sem necessidade appliance de controladora wireless centralizada

- IP único para gestão e configuração de todo o cluster
- Ponto único de configuração
- Capacidade "plug-and-play" para adicionar APs ao cluster, passando um novo access point a assumir a configuração e SSIDs do cluster, sem necessidade de configuração adicional, sendo para tal apenas necessário que tenha:
    - Energia
    - Endereço IP válido (estático ou obtido através de DHCP)
    - Conectividade L2 com os restantes APs do cluster
- Solução de cluster escalável até pelo menos 128 AP e 2.000 dispositivos wireless clientes ligados em simultâneo no mesmo cluster
- Processamento distribuído de sessões de clientes pelos APs
- Data Plane e Control Plane distribuído.
- Redundância da funcionalidade de controlo do cluster entre todos os APs do cluster. Em caso de falha do AP principal outro assume automaticamente.
- Ajuste automático de potência e frequência
- Statefull Firewall integrada para controlo de acesso do tráfego wireless
- Captive Portal integrado
- Capacidade de configurar Denylist de clientes
- Visibilidade do tráfego a transitar na rede wireless com capacidade de identificar:
    - Sessões IP
    - Aplicações
    - Protocolos
    - Destinos
    - Clientes que efetuam o tráfego identificado
- Profiling do tipo de clientes que se estão a ligar na rede:
    - Tipo de dispositivo

- Sistema operativo
- Perfis de serviço para controlo de acesso com determinação de:
- largura de banda máxima por SSID ou User
- tipos de aplicações autorizados
- Web cathegories e Web Reputations autorizados (com base em subscrição de serviços específico)
- IP, redes e domínios de destino autorizados

Suporte de:

- WPA3 Simultaneous Authentication of Equals (SAE)
- Enhanced Open Authentication
- WPA3 Enterprise Suite B
- WPA2/AES link layer encryption.
- WEP link layer encryption.
- WPA/TKIP link layer encryption
- MPSK ou equivalente

Capacidade de implementar políticas acesso que integrem simultaneamente regras de:

- Controlo de acesso, incluindo ao nivel da aplicação, com capacidade de detetar e priorizar tráfego aplicacional
- Regras de de content filtering
- QoS com bandwidth throttling
- Horário definido para permissão de acesso

Funcionalidades de deteção e neutralização/contenção de equipamentos wireless rogue em todos os AP.

Chip integrado para controlo de idoneidade do sistema operativo instalado, identificação unívoca do equipamento e criação de canais de comunicação segura da infraestrutura, baseada em certificados.
Suporte de DC power direto e Power over Ethernet.

Adicionalmente às características acima especificadas dos AP de cada tipologia deverá ainda assegurar as seguintes características específicas descritas abaixo:

Gama Normal Indoor (Salas de aula)

- 2x2 MIMO com 2SS na banda dos 2.4GHz e 5GHz
- Capacidade de débito wireless agregado de até pelo menos 1,49 Gbps
- 2 antenas omnidireccionais dual-band downtilt, integradas no AP
- Suporte de 802.11ax High Efficiency (HE) com HE 20/40
- Suporte de 802.11ac Very High Throughput (VHT) com VHT 20/40/80
- Suporte de 802.11n/ac/ax packet aggregation: A-MPDU, A-MSDU
- Preparado para suportar até 8 resource units 802.11ax OFDMA
- 1 interface 10/100/1000 Base-T
- 1 Interfaces USB 2.0 com capacidade de fornecer 1A/5W de alimentação a um dispositivo aí ligado
- Interface de consola serial micro-B USB
- Temperatura de operação entre os 0ºC e os 50ºC, ou melhor
- Humidade de operação entre os 5% e os 93%, ou melhor

Gama Alta Densidade

- Access Point indoor WIFI 6, adequado para ambientes de maior densidade.
- IEEE 802.11a/b/g/n/ac/ax
- 2.4 GHz: 574Mbps; SU MIMO: 2x2:2

- 5 GHz: 2400Mbps; SU/MU MIMO: 4x4:4
- Até 512 clientes por AP
- Até 16 SSID por AP
- Quatro antenas internas, dual band downtilt, omnidireccionais
- WPA, WPA2, WPA3 and Enhanced Open Security, SAE, WPA2-MPSK, VPN Tunnels, TPM
- Hotspot 2.0
- OFDMA e MU-MIMO (5 GHz)
- Bluetooth Low Energy (BLE5.0)
- Zigbee
- Fontes de Energia: AC/DC power e PoE
- Temperatura: 0°C (32°F) a +50°C (122°F)
- Dimensão: 200mm (L) x 200mm (P) x 46mm (A)
- 1 Porta WAN GE (10/100/1000BASE-T)
- PoE-PD: 48Vdc (nominal) 802.3af/at POE (classe 3 ou 4)
- 1 Porta WAN 2.5GE
- 1 Porta USB 2.0, Tipo A (capaz de fornecer até 1A/5W a um dispositivo que se conecte)
- 1 Porta USB micro-B (consola)
- Wireless LAN (WiFi 802.11a/b/g/n/ac/ax)

Controladora Wireless

Assegurar Cluster único ou máximo 2 clusters.

Permitir cluster físico, embora não seja adquirida nesta consulta base.

Solução Segurança

A solução a ser proposta deve ter características de *Next Generation Firewall* e tem de cumprir as seguintes especificações:

Hardware (obrigatório dentro do mesmo equipamento)

- Número de portas 1Gbit/s RJ45 >= 8
- Disco rígido eMMC >= 128GB
- Porta USB >= 2
- Porta de gestão dedicada "Out of Band"
- Porta de consola RJ45
- Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção
- Deverá estar garantido que a appliance de Firewall quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa

Performance

- Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) >= 2,4 Gbps
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) >= 1,0 Gbps
- Performance da appliance com a funcionalidade de VPN IPSec >= 1,6 Gbps
- Número de novas sessões por segundo >= 39 000
- Número máximo de sessões >= 200 000

Gestão

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio

- Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (por Firewall, por número de firewalls) - Multi-tenancy
- Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio
- Possibilidade de editar configurações pendentes que ainda não foram aplicadas
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas
- Possibilidade de descartar alterações à configuração realizadas
- Possibilidade de armazenar diferentes versões da configuração
- Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada
- Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.
- Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão
- Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas
- Na gestão centralizada deve ser possível gerir até 25 firewalls num único servidor de gestão
- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento
- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça

- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade

Networking

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3
- Suporte de IEEE 802.1Q
- Suporte de iEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP
- Suporte de routing estático
- Suporte de DHCP, NAT e PAT
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas
- Capacidade de realizar policy based routing através do IP ou rede de origem
- Capacidade de realizar policy based routing através do utilizador ou grupo
- Capacidade de realizar policy based routing através do tipo de aplicação
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo
- Permitir a criação de clusters de alta disponibilidade até 6 membros
- Suporte para TLS 1.3 e capacidade de desencriptar este tráfego

Identificação de Utilizadores

- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP

- Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory
- Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores
- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores
- Possibilidade de gerir utilizadores através de API XML
- Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local
- Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing

Solução de Acessos Remotos e Gestão de Identidades

- A solução deve dar a capacidade de estender as funcionalidades da Firewalls (módulos avançados de segurança Threat Prevention, URL Filtering e outros) aos utilizadores remotos
- A solução deve ser capaz de garantir a segurança dos acessos aos recursos internos como também às aplicações de cloud
- Capacidade de garantir a segurança também do acesso à internet do utilizador que esteja fora da rede
- Proteger os utilizadores remotos contra-ataques de phishing e roubo de credenciais
- Capacidade de fazer quarentena a utilizadores remotos utilizando parâmetros e características imutáveis

- Suporte de VPNs por Aplicação e por utilizador
- Capacidade de fornecer acesso seguro e sem agente para parceiros e entidades externas às organizações
- Suporte de identificação automatizada de equipamentos que não são geridos pela entidade da firewall
- Capacidade de implementar Zero Trust efetuando uma identificação muito clara do utilizador
- Fornecer também a capacidade de efetuar a identificação de parâmetros do sistema operativo para poder criar regras de acesso do tipo NAC
- O módulo de identificação tem que obrigatoriamente ser capaz de identificar os seguintes parâmetros do equipamento que está a aceder à rede: validar se o Patch Management está ativo, Firewall local está ativa, Anti-Malware está instalado, Plataforma de Backups está ativa, Mecanismo de Encriptação de disco está ativo, Módulo de DLP está ativo e parâmetros customizados do sistema operativo como processos, registos ou property lists
- A solução deve disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 7 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04
- O mesmo agente de acessos remotos deve também ser possível funcionar como agente de identidades dentro da infraestrutura para identificação do utilizador e mapeamento de políticas baseadas em identidades

Funcionalidades Gerais de Segurança

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança

- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas
- Capacidade de identificação de subfunções dentro de uma aplicação
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL
- Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança
- Capacidade de forçar o uso de MFA para acesso a determinados recursos. Deve ser possível configurar políticas que forcem qualquer utilizador em

determinada subnet, a utilizar MFA se tentar aceder a um recurso em determinado segmento de rede da organização.

- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes

IDS/IPS

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas
- Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possa realizar com base nestas categorias
- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades
- Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis
- Deve ser possível converter assinaturas snort e suricata para dentro da plataforma

Antivirus & Anti-Malware

- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C
- Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware
- Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)
- Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso
- Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações
- Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros
- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro

- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.
- Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

URL Filtering

- Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc)
- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud
- Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)

- Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet
- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

DNS Security

- A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos
- Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.
- Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente.
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente

- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas.
- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos
- Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains
- A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças.
- A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.

Sandboxing

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a que se permita o envio desta informação para análise atendendo aos critérios: tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)

- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.
- Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.
- Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10
- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),
- Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)
- Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.
- Capacidade de desencriptar malware (unpacker) para utilização na análise estática e machine learning.

Relatórios & Logs

- A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais
- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a largo prazo
- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: aplicações mais utilizadas, aplicações de alto risco, informação geral do sistema, estado das interfaces, logs relativos às ameaças mais observadas, logs de URLs filtrados, recursos do sistema
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que

mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos

- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível

Network Packet Broker

- O equipamento deve ter capacidades de Network Packet Broker de forma a permitir filtrar e encaminhar tráfego para uma cadeia externa de dispositivos de segurança de terceiros para uma análise estendida
- Capacidade para usar um ou mais dispositivos de segurança de terceiros (Security Chain) como parte do conjunto geral de segurança
- Capacidade de definir o tráfego encaminhado com base em aplicações, utilizadores, zonas, dispositivos e endereços de IP
- Capacidade para encaminhar tráfego TLS (Decryption Broker) desencriptado e sem ser desencriptado
- Capacidade para assegurar que o caminho para a cadeia de segurança está íntegro e que tenha opções para lidar com o tráfego se a cadeia não estiver operacional
- Capacidade para suportar tráfego unidirecional e bidirecional na cadeia (Client-to-server e Server-to-client) no mesmo par de interfaces (broker interfaces)
- Capacidade de definir múltiplos perfis e associar o perfil a uma regra/politica
- As regras/politicas devem definir o tráfego a ser encaminhado para a cadeia de segurança e o perfil deve definir como encaminhar esse tráfego,

incluindo os interfaces para encaminhamento, monitorização da integridade da cadeia, distribuição de sessão entre várias cadeias e escolha da forma como é encaminhada Routing (Layer 3) ou Transparente Bridge (Layer 1)

Outras Funcionalidades

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade
- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de desencriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados
- Capacidade de criar exceções à desencriptação para determinado tipo de tráfego
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC)
- Possibilidade de enviar tráfego após desencriptação para uma interface de port mirror para análise de terceiras partes
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção

Switchs

Switch 48 portas

Ciclo de Vida do equipamento

- Equipamento totalmente licenciado de forma vitalícia de modo a permitir a exploração de todas as capacidades e funcionalidades.
- Garantia vitalícia ou até 5 anos a data de end-of-sale do equipamento (incluindo fontes de alimentação e ventoinhas de refrigeração)

Características base

- Altura de 1 RU
- Arquitetura database-centric na qual todos os processos de software comunicam com a base de dados e não entre si
- 1 porta de consola (RJ-45 serial ou USB)
- 1 porta USB para transferência de ficheiros entre o switch e uma USB flash drive
- 4 portas de uplink SFP 1GbE (ou superior)
- 48 portas GbE Class 4 PoE (IEEE 802.3af, IEEE 802.3at, até 30W ou superior)
- Temperatura de Operação (até aos 1,5Km de altitude) entre 0ºC e 45ºC (ou amplitude superior)
- Componente/Módulo de gestão com 4GB (ou superior) de memória e 16GB (ou superior) de flash/storage
- Componente/Cartas de I/O com 1MB (ou superior) de packet buffer
- Débito (throughput, pps) de 77,3 Mpps (ou superior)
- Capacidade de routing/switching (bps) de 104 Gbps (ou superior)
- Latência inferior a 3 microsec
- Dimensão da tabela de MAC addresses: 8K entradas (ou superior)

- Dimensão da tabela de hosts: 1K entradas (ou superior)
- Dimensão da tabela de routing >= 512 entradas (IPv4 e IPv6)

Funcionalidades L2

- Link Layer Discovery Protocol (LLDP, IEEE 802.1AB e LLDP-MED)
- Cisco Discovery Protocol v2 (CDP) para uso em aplicações de voz (voice VLAN)
- Spanning Tree Protocol (STP, IEEE 802.1D), Rapid STP (RSTP, IEEE 802.1w), e Multiple STP (MSTP, IEEE 802.1s)
- Rapid Per-VLAN spanning tree plus (RPVST+)
- Link Aggregation Control Protocol (LACP, IEEE 802.3ad) com pelo menos 8 interfaces por LAG
- VLANs (IEEE 802.1Q) >= 512
- IGMP Snooping

Funcionalidades L3

- Endereçamento IP atribuído a interfaces VLAN / Switch Virtual Interface (SVI)
- Suporte de subnet mask /31 (RFC 3021)
- Routing estático IPv4 e IPv6
- Multicast routing IGMP v2 (RFC 2236) e IGMP v3 (RFC 3376)
- Multicast routing MLD v1 (RFC 2710) e MLD v2 (RFC 3810)

Funcionalidades relacionadas com eficiência, alta disponibilidade e resiliência

- Detecção de conectividade e falhas de links Uni-directional link detection (UDLD, RFC 5171)

- Detecção de falhas em cabos UTP via Time-Domain Reflectometer (TDR)
- Detecção de comportamentos/sintomas indesejados de erros de links e condições de tráfego na rede tais flapping de links, excessivo TX drops, excessivo CRC errors, etc.
- Detecção / protecção de loops de Layer 2
- Eficiência energética assente no standard Energy Efficient Ethernet (EEE, IEEE 802.3az) aplicável a interfaces 1GbE

Funcionalidades de QoS

- Mecanismos de QoS de traffic classification/(re)marking baseados em ACLs e nos campos dos pacotes Layer 2 e Layer 3 (IPv4, IPv6)
- Mecanismos de QoS de traffic policing: Drop, Mirror, Marking e Policing (baseados no Commited Information Rate (CIR))
- Mecanismos de QoS de traffic policing aplicados a interfaces de Layer 2 (físicas e LAGs) e interfaces VLAN
- Mecanismos de QoS de queueing / scheduling baseados em Strict Priority (SP)
- Protocolo de flow control (IEEE 802.3x)
- Jumbo Frames superior a 9,1Kbytes

Funcionalidades de Segurança de controle de acessos à rede

- Mecanismos de tracking e visibilidade de clientes com endereçamento IP estático ou DHCP mesmo quando ligados directamente à porta do switch em L2 ou atrás de outro dispositivo: switch, access point, telefone IP, etc.
- Traffic accounting baseado em sFlow (RFC 3176)
- Cópia de tráfego (mirroring) proveniente de portas e LAGs
- Capacidade de definição do modo de autenticação dos acessos à rede: orientada ao "cliente" (autenticação de todos os clientes ligados à porta do

switch) e ao "dispositivo" (autenticação apenas do primeiro cliente ligado à porta do switch)

- Capacidade de autenticação de múltiplos clientes na mesma porta do switch (> 30 dispositivos por porta)
- Capacidade de autenticação de acessos concorrentes IEEE 802.1x e MAC-based authentication
- Capacidade de controlo da sequência de autenticação de acessos à rede (802.1x e MAC-based), permitindo a definição da ordem e prioridade da autenticação
- Autorização dinâmica de Radius baseada em pacotes CoA Disconnect-Request e CoA-Request (RFC 3576)
- Capacidade de autenticação web-based recorrendo a captive portal externos
- Capacidade de aplicação de políticas de acesso à rede (entregues a portas ou utilizadores), obtidas localmente (isto é, políticas residentes localmente nos switches) e, também, remotamente a partir de servidor Radius/atributos Radius
- Capacidade de aplicação de diferentes políticas de acesso em função das condições de autenticação: sucesso da autenticação, insucesso da autenticação, indisponibilidade do(s) servidor(es) de Radius, e, também, no caso de não ter sido identificada nenhuma política aplicável (política de recurso)
- Capacidade de aplicação de políticas de acesso dinâmicas à sessão de clientes com aplicação de configurações, tais como, VLAN ID, período de reautenticação, período de inactividade, PoE priority, MTU
- Capacidade de aplicação de políticas de acesso dinâmicas sobre o tráfego de clientes: bloqueio, rate limiting, remarcação de QoS
- Controlo de MAC addresses por porta (Port Security)

- Capacidade de filtragem/bloqueio de pacotes recebidos numa determinada interface de entrada e que têm como destino um conjunto específico de interfaces de saída
- Controlo de acessos baseado em ACLs

Funcionalidades de Segurança contra ameaças dirigidas aos equipamentos

- Autenticação do acesso à shell do sistema operativo de boot (System Bootloader) usado, habitualmente, p/ actualização, carregamento de firmware e outras funções básicas de gestão do file system do switch
- Protecção do control plane / Control Plane Policing (CoPP)
- Protecção do Spanning Tree Protocol assente em mecanismos, tais como, BPDU Protection e Root Guard
- Protecção de ataques IP source address spoofing assente em mecanismos, tais como, DHCP snooping
- Protecção de ataques ARP assente em mecanismos, tais como, ARP protection
- Protecção contra ataques de flood (storms protection contra storms de tráfego broadcast, multicast e unknow unicast)

Funcionalidades de Segurança ao nível da administração dos equipamentos

- Sincronização de relógio baseado em Network Time Protocol (NTP)
- Controlo de acessos à gestão do switch baseado em ACLs IP4 e IPv6
- Controlo de acessos à gestão baseado em serviço AAA local assente em passwords locais e autorização usando Role-Based Access Control (RBAC)
- Controlo de acessos à gestão baseado em serviço AAA remoto assente servidores de autenticação RADIUS e TACACS+ e de autorização usando TACACS+

- Suporte de registo de certificados sobre TLS (Enrollment over Secure Transport (EST), RFC 7030)
- Suporte de SSH para encriptação de acessos remotos command-line
- Suporte de FTP sobre SSH (SFTP) para transporte seguro de ficheiro
- Suporte de SSL/TLS para encriptação do tráfego HTTP para fins de gestão
- Suporte de Syslog (RFC 5424) sobre TLS
- Suporte de protocolos SNMP v3
- Suporte de chip TPM (Trusted Platform Module)

Capacidades de Gestão, Diagnóstico e Automação/Orquestração

- Simplificação da instalação do equipamento por via de mecanismos Zero Touch Provisioning (ZTP)
- Possibilidade de gestão e configuração por linha de comando industry-standard (CLI)
- Possibilidade de execução de job schedulers integrados nos equipamentos
- Possibilidade de gestão e configuração via interface web nativa nos próprios equipamentos
- Disponibilização de interface de programação RESTful API
- Possibilidade de gestão e configuração por ambiente gráfico assente em ferramenta instalada on-prem
- Possibilidade de gestão e configuração por ambiente gráfico assente em plataforma SaaS (nativamente cloud-based)

- Capacidade de integração com Ansible

NOS TERMOS DO DISPOSTO NO ARTIGO 49.º DO CÓDIGO DOS CONTRATOS PÚBLICOS (CCP):

- TODAS AS REFERÊNCIAS A NORMAS/HOMOLOGAÇÕES E A ESPECIFICAÇÕES TÉCNICAS NAS PEÇAS DO PROCEDIMENTO DEVEM SER CONSIDERADAS, PARA OS DEVIDOS EFEITOS, ACOMPANHADAS DA MENÇÃO «OU EQUIVALENTE»;

- TODAS AS INDICAÇÕES A MARCAS COMERCIAIS OU INDUSTRIAIS DE PATENTES OU MODELOS PRESENTES NAS PEÇAS DO PROCEDIMENTO DEVEM SER CONSIDERADAS, PARA OS DEVIDOS EFEITOS, ACOMPANHADAS DA MENÇÃO «OU EQUIVALENTE».