



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 2/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

EQUIPAMENTOS ATIVOS DE REDES - ATR

INTRODUÇÃO E OBJETIVO

O objetivo deste memorial é de descrever as características funcionais e operacionais dos equipamentos ativos da rede de armazenagem e processamento de informações dos Sistemas Eletrônicos.

Nos equipamentos ativos descritos neste documento, serão processadas as informações dos seguintes Sistemas Eletrônicos:

- Sistemas de automação predial e BMS (building management system) - AUT;
- Sistemas de Circuito Fechado de TV - CTV;
- Sistemas de controle de acesso - SCA;
- Sistemas de detecção e alarme de incêndio - INC;
- Sistemas de alarme de intrusão - ALA;
- Sistema de backupeamento das informações geradas pelos Sistemas Eletrônicos acima.

Este Memorial complementa as especificações descritas nos demais memoriais descritivos de cada disciplina.

Este documento não dimensiona os ativos das redes de gestão e operacionais a serem implantadas na edificação. Os ativos dimensionados neste Memorial atenderão exclusivamente aos sistemas de segurança descritos acima.

SISTEMAS INTERNOS

Os sistemas eletrônicos da edificação atendem a todas as cargas prediais das áreas a serem ocupadas e gerenciadas pelo Prédio do Museu do Amanhã.

EQUIPAMENTOS ATIVOS

Neste documento serão descritas as características de cada um dos seguintes equipamentos:

- 1- Servidores tipo 1 - Sistema de automação predial e BMS (building management system);
- 2- Servidores tipo 2 - reserva (hot line) em tempo real (reserva do servidor 1);
- 3- Servidores tipo 3 - Sistema de backupeamento e storage;
- 4- Switches;
- 5- Firewall;
- 6- UPS;
- 7- Estações de trabalho – monitoramento, cadastramentos e operações;
- 8- Impressora.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 3/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

DESCRIÇÕES DOS EQUIPAMENTOS

SERVIDORES:

Os servidores deverão ser conectados diretamente no Switch Core, através de portas metálicas uplink 1GBP, por meio de patch-cords Cat 6A, a serem instalados dentro dos racks como indicado em projeto.

SERVIDORES TIPO 1 E 2: Servidor 1 para Sistemas de automação predial e BMS (building management system) e servidor 2 para Reserva (hot line) em tempo real (reserva do servidor 1);

Item	Cartacterístcas do Servidor: Plataforma Windows Server 2010
Processador Recomendado (mínimo)	2 Processadores Quad Core 2.33 GHz Xeon.
Memória RAM	16 GB ou superior
Cardholder Capacity	> 20K cardholders
Point Capacity	> 15,000 points
Disco Rígido	500 GB ou superior
Mídia auxiliar - Load device	DVD-ROM (Dual layered)
Dispositivo de armazenamento (storage)	SCSI tape drive, ZIP drive, CR-RW, DVD
Saída serial	COM1, COM2 or Stallion EC8/64-PCI-K EasyConnection Smart Host Adaptor PCI bus with Stallion PA-EC-8D4K, 8-Port RS232/422/485 Async module (DB25)
Conversor RS232/485	BlackBox LD485A-HS or IC109AE or Honeywell CN590 or Honeywell XL Adaptor or CesCom CE-0022H
Placas de rede	Pelo menos 2 placas de rede 10 Gb RJ-45 Dell integradas
Certificação UL (Underwriters Laboratories)	Equipamento deverá possuir certificação UL
Alarme sonoro	Auto falante interno our Soundblaster Pro
Integração de vídeo	Flashpoint 3Dx Lite PCI Flashbus MV Lite PCI Flashbus Spectrim Lite
Câmera Digital	Any windows compatible camera
Impressora - auxiliar	Epson StylusPro XL
Impressora de alarme e eventos	132 column Epson compatible dot matrix printer qualified for local language EPSON 6200L TVS HD745 (OKI Micro line 391 Turbo 24 pin printer)
Impressora	Windows compatible printer EPSON 6200L TVS HD745 (OKI Micro line 391 Turbo 24 pin printer)
Signature Pad	Interlink Electronics ePadInk Topaz SigLite 1x5 T-L460-HSB
Terminal Server	Latronix UDS 1100 Systech NDS 1111 Emulex 2500 series Lantronix MSS1-T



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA:
MUSEU DO AMANHÃ

ETAPA:
Projeto Executivo

Nº DO DOCUMENTO:
MDA-PE-ATR-MD-300

REVISÃO:
R02

DATA:
28/08/2013

PÁGINA:
4/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

	Acola Cobox v1.02 Stallion EasyServer II Rev 1.10 Cobox UDS-200 (Encryption). SDS-1100 (Encryption) Digi One TS High Speed Intelligent 1 Port (RS232/422/485 Switchable)
Tipo de gabinete	Módulo para instalação em rack 19"
Modem	Modem compatível com sistema Windows – sugestões: 1. D-Link DU560M USB Modem 2. US Robotics 3com FAX Modem and 56K message modem 3. NetComm 56K USB modem AM5067
Monitor	LED 21" full HD
Sistema Operacional	Windows Server 2008 ou superior
Local de instalação	Servidores 1 e, 2: Em rack fechado nas salas de ativos de rede do BMS.

SERVIDOR 3 - BACKUPEAMENTO E STORAGE

O servidor 3 deverá ser fornecido com unidade de backupeamento externo e sistema de gravação de arquivos de backup. Este servidor deverá processar o backupeamento de todas as informações e dados gerados pelos seguintes sistemas:

- Sistemas de automação predial e BMS (building management system) - AUT;
- Sistemas de controle de acesso Restrito - SCA;
- Sistemas de detecção e alarme de incêndio - INC;
- Sistemas de alarme de intrusão – ALA.

Cada servidor de backupeamento deverá possuir as características mínimas descritas a seguir:

SERVIDOR

- Mínimo de 2 Processadores Quad-Core Intel Xeon E5620 2.4Ghz 12M CacheTurbo, 5.86 GT/s QuickPath Interconnect, Tecnologia Turbo Hyper-Threading (Limita a velocidade da memória a 1066MHz)
- Pelo menos 16 GB de memória DDR-3 Unbuffered DIMM, 1066 MHz (2 x 2 GB)
- Placa controladora PERC H700 6Gb/s, 512MB Cache e bateria (Suporta RAID 0, 1, 5, 6, 10, 50, 60)
- Pelo menos 4 discos rígidos Hot Plug de 2000GB SAS 6GB 3.5" 15.000rpm
- Configuração dos discos em RAID 6
- 2 interfaces de rede 10 GBPS UTP integradas
- Placa de rede Intel Gigabit ET, Dual Port, Copper, PCIe-4
- Teclado com tecla silenciosa, português



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 5/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

- Mouse Ótico de 2 botões incluso
- Fontes de alimentação (1000W)
- Unidade de DVD-RW de 8x
- Sistema Operacional Windows 2010 O&M ou superior
- 5 anos de garantia ProSupport for IT com Missão Crítica e com atendimento on-site 7x24 com 4 horas de tempo de resposta
- Chassi para instalação em rack 19"
Estação de trabalho em rack de 2U ou 4U
Profundidade:
Com tampa frontal 28,84 pol. (73,25 cm)
Sem tampa frontal 26,95 pol. (68,45 cm)

SISTEMA DE BACKUP EXTERNO

- Unidade de fita LTO3 (400/800GB) externa
- Controladora SCSI LSI U320 Single Channel PCI-e
- Cabo SCSI de 4m
- 5 anos de garantia ProSupport for IT com atendimento on-site no próximo dia útil

SISTEMA DE BACKUP DE ARQUIVOS

Symantec Backup Exec Server Express Essentials 2012

- Fácil gerenciamento do backup e recuperação dos dados
- + Agente Remoto do Symantec Backup Exec 2010 para Backup Online do Microsoft SQL Server
- Com 1 ano de suporte 24x7 (1 licença por servidor)
- Implementação e configuração não inclusa (Podendo ser orçada à parte)



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 6/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

SWITCHES PARA SISTEMAS ELETRÔNICOS

SWITCH CORE

INTERFACES

- Possuir , no mínimo, 7 slots para a inserção de módulos.
- Os switches deverão permitir as seguintes capacidades máximas:
 - Até 60 portas 10G (BASE-SR ou LR) em cada chassis com oversubscription máximo de 2.5:1;
 - Até 240 portas 10/100/1000 RJ-45 em cada chassis SEM oversubscription;
 - Até 120 portas 1G (BASE-SR ou LX/LH) em cada chassis SEM oversubscription
 - As interfaces de 10GE deverão ser aderentes aos padrões IEEE 802.3aq, IEEE 802.3ae e IEEE 802.3ak.
- Deverão ser fornecidos os GBIC ou SFP necessários para todas as portas, inclusive portas existentes nos módulos de supervisão.
- Possuir, no mínimo, 12 portas 10GBase-LRM switching gigabit ethernet, full-duplex, para fibras óticas monomodo. Deverão ser fornecidos os GBIC ou SFP necessários.
- Possuir, no mínimo, 48 portas Ethernet 10/100/1000 com autosensing de velocidade e com conectores RJ-45.
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control).
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX)
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
- Implementar VLANs por porta.
- Implementar VLANs compatíveis com o padrão IEEE 802.1q.
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.
- Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
- Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.
- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

DISPONIBILIDADE

- Permitir a instalação de módulos de supervisão redundantes, sendo cada módulo capaz de suportar sozinho o controle da operação de todos os módulos de interface do switch em capacidade máxima.
- Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação.
- Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- Permitir a agregação de portas que residam em módulos diferentes do switch.
- Os módulos de supervisão deverão ter sincronismo dos protocolos de camada 2 e camada 3, além de todas as outras informações do switch, provendo "statefull switchover" de supervisoras.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 7/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
--------------------	---

- Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos.
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.

DESEMPENHO

- Possuir capacidade para pelo menos 55.000 endereços MAC na tabela de comutação.
- Implementar, no mínimo, 4096 vlans simultaneamente.
- Implementar, no mínimo, 4096 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas.
- A conexão dos módulos de interface fornecidos com a switching fabric do switch não poderá apresentar coeficiente de oversubscription superior a 250%.
- Possuir backplane de, no mínimo, 560 Gbps e uma taxa e de encaminhamento de no mínimo 250 milhões de pacotes por segundo (Mpps) para IPv4 e 125 milhões de pacotes por segundo (Mpps) para IPv6.
- A conexão de cada slot com o backplane deve ser de, no mínimo, 48 Gbps.
- Suportar Jumbo frames de no mínimo 9216 Bytes.

PROTOCOLOS E FACILIDADES SUPORTADOS

- Implementar Telnet para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet.
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 8/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

- Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:
 - IP de origem/destino;
 - Parâmetro "protocol type" do cabeçalho IP;
 - Porta TCP/UDP de origem/ destino;
 - Interface de entrada do tráfego.
- Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída (e também para ambos os sentidos simultaneamente) em uma dada interface do roteador;
- A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado;
- Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN.
- Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
 - ICMP echo;
 - TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
 - UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
 - O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
- Implementar o protocolo SNTP ou NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação entre os peers.
- Implementar DHCP Relay e DHCP Server em múltiplas VLANs.
- Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway.
- Possuir suporte ao protocolo GRE (Generic Routing Encapsulation), conforme RFCs 1701 e 1702.
- Implementar roteamento estático.
- Implementar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).
- Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Implementar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Implementar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF
- Permitir o roteamento nível 3 entre VLANs.
- Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway.
- Implementar, no mínimo, 256 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente.
- Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
- Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 9/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

- Suportar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.
- Suportar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway para IPv6.
- Suportar, no mínimo, 256 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente, para IPv6.
- Implementar mecanismo de controle de multicast através de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Implementar roteamento multicast PIM (Protocol Independent Multicast) nos modos "sparse-mode" (RFC 2362) e "dense-mode". Deve ser suportada, por interface, a operação simultânea nos modos "sparse-mode" e "dense mode".
- Suportar no mínimo 255 grupos multicast para IPv4.
- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.
- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request
 - ICMP Reply
 - ICMP Neighbor Discovery Protocol (NDP)
 - ICMP MTU Discovery
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

GERENCIAMENTO

- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - Sem autenticação e sem privacidade (noAuthNoPriv);
 - Com autenticação e sem privacidade (authNoPriv);
 - Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.
- Possuir suporte a MIB II, conforme RFC 1213.
- Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 10/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

- O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.

QUALIDADE DE SERVIÇO

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point" - nível 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).
- Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).

SEGURANÇA

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.
 - Implementar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
 - Proteger a interface de comando do equipamento através de senha.
 - Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
 - Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
 - Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
 - Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
- 2..1 Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
 - Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
 - Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elemento de rede, independente do método de gerenciamento.
 - Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 11/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta.
- Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo "ARP Poisoning".

PADRONIZAÇÃO

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN, com suporte a, no mínimo, 32 instâncias simultâneas.
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- Implementar padrão IEEE 802.3ad.
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol) , com suporte a, no mínimo, 32 instâncias simultâneas.
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 32 instâncias simultâneas do protocolo Spanning-Tree.
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS.
- Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.

DIVERSOS

O equipamento deverá vir acompanhado de todos os módulos e/ou dispositivos e software necessários para seu perfeito funcionamento e operação, em conformidade com as especificações técnicas aqui apresentadas, mesmo que esses não constem desta especificação.

O Equipamento deverá ser novo e sem uso anterior e estar em linha normal de produção.

O equipamento deverá ser homologado pela ANATEL. Na apresentação da proposta deve constar cópia do certificado de homologação.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 12/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

SWITCH ACESSO

Switch de acesso com 24 ou 48 portas 10/100/1000 UTP, 2 portas 10Gbps Ethernet (fibra ótica), PoE.

PORTAS

- Possuir, no mínimo, 2 portas 10Gbase-LRM switching 10 gigabit ethernet, full-duplex, para fibras óticas monomodo. Deverão ser fornecidos os GBIC ou SFP necessários.
- Possuir modelos de 24 ou 48 portas Ethernet 10/100/1000 com autosensing de velocidade e com conectores RJ-45.
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control).
- Implementar Power Over Ethernet (PoE) de acordo com os padrões IEEE 802.3af e 802.3at em todas as portas ethernet 10/100/1000.
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
- Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX)
- Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
- Implementar VLANs por porta.
- Implementar VLANs compatíveis com o padrão IEEE 802.1q.
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.
- Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
- Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

FONTE DE ALIMENTAÇÃO

- Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
- Suportar alimentação elétrica redundante capaz de suportar o equipamento com todas as funcionalidades (NÃO É NECESSÁRIO FORNECER A FONTE DE ALIMENTAÇÃO REDUNDANTE).
- A fonte de alimentação deverá possuir no mínimo 370W para alimentação PoE, além da energia necessária para funcionamento do switch.
- Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 13/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

DIMENSÕES

- a) Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

VISUALIZAÇÃO

- a) Possuir LEDs para a indicação do status das portas e atividade, além de duplex e PoE.

GERENCIAMENTO

- a) Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
- b) Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - a. Sem autenticação e sem privacidade (noAuthNoPriv);
 - b. Com autenticação e sem privacidade (authNoPriv);
 - c. Com autenticação e com privacidade (authPriv).
- c) Possuir suporte a MIB II, conforme RFC 1213.
- d) Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
- e) Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
- f) Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.
- g) Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
- h) Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
- i) Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
- j) Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
- k) Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757
- l) Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.
- m) Implementar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 4 unidades, com velocidade de empilhamento de 40Gbps full-duplex.
- n) A pilha deverá ser gerenciada através de um único endereço IP, permitindo agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

FACILIDADES

- a) Implementar Telnet para acesso à interface de linha de comando.
- b) Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.
- c) Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- d) Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
- e) Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 14/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

- f) Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- g) Permitir que a sua configuração seja feita através de terminal assíncrono.
- h) Permitir a gravação de log externo (syslog).
- i) Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- j) Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- k) Permitir o espelhamento do tráfego de portas que residem em um dado switch para uma porta que reside em switch diferente da pilha.
- l) Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- m) Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- n) Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
- o) Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- p) Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- q) Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas ("promíscuas"), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas ("promíscuas") de uma dada VLAN.
- r) Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
- s) Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- t) Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).
 - a. Devem ser suportadas no mínimo as seguintes operações de teste:
 - i. ICMP echo;
 - ii. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
 - iii. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
 - iv. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

PROTOCOLOS

- a) Implementar o protocolo NTPv3 (Network Time Protocol, versão 3). Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 1305.
- b) Implementar DHCP Relay e DHCP Server em múltiplas VLANs.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 15/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

DESEMPENHO

- Possuir capacidade para pelo menos 8.000 endereços MAC na tabela de comutação.
- Implementar , no mínimo, 255 vlans simultaneamente.
- Deve possuir switch-capacity de no mínimo 144Gbps e taxa de encaminhamento de no mínimo 77 Mpps.
- Suportar Jumbo frames de no mínimo 9216 Bytes.

SEGURANÇA

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.
- Implementar filtragem de pacotes (ACL - Access Control List).
- Proteger a interface de comando do equipamento através de senha.
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- Possuir controle de *broadcast*, *multicast* e *unicast* por porta.
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
- Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta.
- Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo "ARP Poisoning".



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 16/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

PADRÕES

- a) Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- b) Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- c) Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- d) Implementar padrão IEEE 802.3ad.
- e) Implementar padrão IEEE 802.3af.
- f) Implementar padrão IEEE 802.3at.
- g) Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- h) Os processos de Autenticação, Autorização e *Accounting* associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x.
- i) Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
 - a. Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
 - i. A estação não tem cliente 802.1x (suplicante);
 - ii. As credenciais do usuário não estão corretas (falha de autenticação).
 - b. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).
 - c. Implementar "accounting" das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - i. Nome do usuário;
 - ii. Switch em que o computador do usuário está conectado;
 - iii. Porta do switch utilizada para acesso;
 - iv. Endereço MAC da máquina utilizada pelo usuário;
 - v. Endereço IP do usuário;
 - vi. Horários de início e término da conexão;
 - vii. Bytes transmitidos e recebidos durante a conexão.
 - d. Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
 - e. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
 - f. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
 - g. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
 - h. Implementar suporte ao serviço *DHCP Server* em múltiplas VLANs simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
 - i. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
 - j. Deve ter tratamento de autenticação 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
- j) Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.
- k) Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
- l) Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 17/34

DISCIPLINA:
ATR

TÍTULO:
MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

MULTICAST

- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.

QUALIDADE DE SERVIÇO (QoS)

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point" - nível 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).
- Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).

INTERNET PROTOCOL VERSÃO 6 (IPv6)

- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.
- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
 - ICMP request
 - ICMP Reply
 - ICMP Neighbor Discovery Protocol (NDP)
 - ICMP MTU Discovery
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 18/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

FIREWALL PARA ACESSO INTERNET

Deverá ser fornecido e instalado na sala PTA um firewall para controle do acesso à internet pelos diversos usuários das redes.

Este equipamento deverá controlar os acessos externos de todos os dispositivos e usuários a serem instalados dentro do prédio. Não será permitida a instalação de pontos de conexão dos sistemas internos a internet, não cobertos por este firewall.

CARACTERÍSTICAS BÁSICAS

- Equipamento do tipo “appliance”;
- Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários);
- Deve ser fornecido com fontes redundantes internas ao equipamento;
- Deve ser fornecido com pelo menos 08 interfaces 10/100/1000 auto-sense e 02 (duas) interfaces 10Gigabit Ethernet;
- As interfaces de 10Gigabit poderão ser ativadas via licença;
- Deve suportar o acréscimo de pelo menos 08 interfaces Gigabit Ethernet ;
- Deve suportar o acréscimo de pelo menos 02 interfaces 10Gigabit Ethernet (10GE);
- Deve suportar agregação de portas GigabitEthernet e 10GigabitEthernet;
- Deve ser possível formar grupos de até 08 portas GigabitEthernet e 04 portas 10GigabitEthernet;
- Deve suportar funcionalidade de Stateful Firewall com performance mínima de 4 Gbps e mínimo de 1 milhão de conexões simultâneas;
- Deve suportar a criação de pelo menos 50.000 (cinquenta mil) novas conexões por segundo e encaminhamento de pelo menos 1,5 milhões de pacotes por segundo;
- Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall;
- Deve suportar a definição de VLAN trunking conforme padrão IEEE 802.1q. Deve ser possível criar pelo menos 250 interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre estas;
- Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”;
- O equipamento deve permitir a “randomização” do número de seqüência TCP, ou seja, funcionar como um “proxy” de número de seqüência TCP de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de seqüência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;
- Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas;
- Deve suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos: hosts, redes IP, serviços. Deve ser possível verificar a utilização (“hit counts”) de cada regra de filtragem (“Access Control Entry”) individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos;
- A solução fornecida deve possuir a funcionalidade de “proxy” de autenticação (“authentication proxy”), permitindo a criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Deve ser possível obter as informações de usuário/senha



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 19/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
--------------------	---

por meio de pelo menos os seguintes protocolos: HTTP, HTTPS e Telnet. Deve ser possível ao Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação;

- Deve suportar autenticação usando base local de usuários (interna ao equipamento);
- Implementar políticas de controle de acesso baseadas em informações de horário ("time-based access control");
- Deve implementar remontagem virtual de fragmentos ("Virtual Fragment Reassembly") em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem;
- Possuir suporte a inspeção "stateful" para pelo menos os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP;
- Possuir suporte à inspeção stateful dos protocolos de sinalização de telefonia H.323(v1,v2,v3,v4), SIP (Session Initiation Protocol), MGCP e SCCP. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos.
- Possuir capacidade de limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);
- Possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP);
- Possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de destino especificado;
- Possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para um endereço de destino especificado;
- Deve permitir simultaneamente com a implementação de "Network Address Translation" a filtragem "stateful" de pelo menos as seguintes aplicações:
 - a) H.323 (v1,v2, v3,v4) , Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol);
 - b) Microsoft Networking client and server communication (NetBIOS over IP);
 - c) Oracle SQL*Net client and server communication;
 - d) Domain Name System (DNS);
 - e) SUN Remote Procedure Call (RPC);
 - f) File Transfer Protocol (FTP) – modos "standard" e "passive".
- O equipamento deve permitir a inspeção detalhada de conexões HTTP , contemplando, no mínimo, as seguintes funcionalidades :
 - a) Verificação de conformidade das requisições HTTP com a RFC 2616 e suporte a bloqueio de requisições não conformes;
 - b) Verificação do comprimento do "Header" das mensagens HTTP (requisições dos clientes e respostas dos servidores). Deve ser possível bloquear conexões cujos comprimentos do Header HTTP não estejam em conformidade com os valores pré-definidos na política de Segurança aplicada ao equipamento;
 - c) Possibilidade de bloqueio de requisições cujo comprimento do URI não esteja dentro dos limites pré-definidos pela Política de Segurança aplicada ao equipamento;
 - d) Possibilidade de bloqueio de requisições cujo comprimento da parte de dados do HTTP ("content-length") não esteja dentro dos limites pré-definidos pela Política de Segurança aplicada ao equipamento;
 - e) Possibilidade de bloqueio de conexões HTTP de acordo com o tipo de conteúdo por elas transportado. O equipamento deve prover suporte a filtragem de no mínimo os seguintes tipos de conteúdo : audio/mpeg, audio/x-ogg, audio/x-adpcm, audio/x-wav , image/jpeg, image/x-3ds, image/portable-bitmap, image/cgf, image/png, image/x-bitmap, image/x-portable-greymap, image/gif, , video/-flc, video/sgi, video/x-mng, video/mpeg, video/x-avi, video/x-msvideo, video/quicktime, video/x-flv, video/x-niff, video/tiff , application/zip, application/x-gzip, application/postscript;



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 20/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
--------------------	---

- f) Possibilidade de bloqueio de requisições HTTP de acordo do método ("request method") utilizado pelo cliente web;
- g) Deve possuir capacidade de filtrar "applets" Java e controles ActiveX.
 - O equipamento deve permitir a inspeção detalhada de conexões FTP, contemplando, no mínimo, as seguintes funcionalidades:
 - a) Permitir o bloqueio seletivo de comandos utilizados em requisições FTP ("request commands");
 - b) Verificar se os comandos "PORT" e "PASV" foram truncados, permitindo o "reset" da sessão TCP caso isto tenha ocorrido;
 - c) Garantir que o comando "PORT" só ocorra na parte cliente da conexão FTP, sendo possível promover o "reset" da sessão TCP caso tal comando seja detectado em uma mensagem enviada por um servidor FTP;
 - d) Garantir que o comando "PASV" só ocorra na parte servidor da conexão FTP, sendo possível promover o "reset" da sessão TCP caso tal comando seja detectado em uma mensagem enviada por um cliente FTP;
 - e) Verificar a negociação de portas TCP a serem usadas na conexão, permitindo a finalização da sessão TCP caso uma porta entre 1 e 1024 tenha sido negociada;
 - f) Permitir a substituição da resposta enviada pelo servidor FTP a um comando "SYST" para evitar que o "system-type" do servidor seja revelado aos clientes.
 - Possuir suporte a tecnologia de Firewall Virtual, sendo fornecido com pelo menos 2 (duas) instâncias totalmente isoladas entre si. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas:
 - a) Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC;
 - b) Dentro de cada instância de Firewall deve ser possível limitar (promover "rate limiting") os recursos de taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog;
 - c) A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias;
 - d) Deve suportar a adição de novas instâncias virtuais através de licenças de software. Devem ser suportadas pelo menos 100 instâncias virtuais de Firewall.

SUPORTE À VPN

- A solução deve suportar a terminação de pelo menos 5.000 (cinco mil) túneis de IPSEC VPN simultaneamente. Não deve haver limitação de usuários por licença;
- Deve haver versões do cliente IPSEC VPN fornecido com o concentrador para, no mínimo, os seguintes sistemas operacionais: Windows XP, Windows Vista, Windows 7, Linux (Intel), MAC OS, Apple IOS e Windows Mobile;
- A solução deve suportar a terminação de pelo menos 5.000 (cinco mil) sessões SSL-VPN simultaneamente, através da adição de licença;
- Caso a solução não suporte todas as especificações de VPN (SSL e IPSEC) em um único chassis, poderá ser fornecido um concentrador VPN externo, do mesmo fabricante do firewall, desde que conectado a este através de pelo menos 02 interfaces 10Gbps. Tais interfaces 10Gbps deverão ser diferentes daquelas originalmente especificadas para o firewall;
- Deve ser possível ao concentrador terminar túneis IPSEC do tipo "site-to-site" (LAN-to-LAN);
- O concentrador VPN deve suportar a terminação simultânea de conexões IPSEC VPN e SSL VPN;



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 21/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
--------------------	---

- Suporte à criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES. Deve possuir desempenho de no mínimo 1 Gbps para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado;
- Deve ser possível ao concentrador fornecido operar em modo "cluster". O líder do "cluster" deve ser responsável por direcionar conexões para os demais membros do "cluster";
- Suportar alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em "standby". Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final;
- Deve suportar negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica;
- Suporte à integração com servidores RADIUS para tarefa de autenticação, autorização e accounting (AAA) dos usuários que ganharam acesso via conexão VPN ("Extended Authentication");
- O concentrador VPN deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente : endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC;
- O concentrador de VPN deve ser capaz de configurar nos VPN clients uma lista de acesso de "split tunneling", de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo "all tunneling", em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida;
- O concentrador deve permitir a criação de "banners" personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa;
- O concentrador VPN deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento;
- O concentrador deve permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento;
- O concentrador VPN deve se integrar com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes;
- O concentrador deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema;
- Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN;
- O concentrador deve permitir a definição dos horários do dia e dos dias da semana em que um dado usuário pode requisitar uma conexão VPN;
- O concentrador VPN deve suportar NAT (Network Address Translation);
- O concentrador VPN deve suportar operação no modo transparente a NAT ("NAT-transparent mode"), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation)
- O concentrador VPN deve permitir a terminação de conexões no modo IPSEC over TCP;
- O concentrador VPN deve permitir a terminação de conexões no modo IPSEC over UDP;
- Deve ser possível visualizar no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas;
- Deve ser possível visualizar no cliente VPN o endereço privado adquirido durante a negociação da conexão IPSEC;
- Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 22/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

(IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES, AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5 e 7) e tempo de duração ("lifetime") da conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN client;

- Deve suportar a utilização de certificados digitais padrão X.509 para o próprio concentrador VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs) : Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve ser suportado o protocolo SCEP para "enrollment" automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC);
- O concentrador VPN deve suportar protocolo Syslog para geração de logs de sistema;
- Para SSL VPN devem ser suportadas no mínimo as seguintes aplicações transportadas sobre conexões SSL para o concentrador : HTTP, POP3S, IMAP4S, SMTPS;
- Para SSL VPN devem ser suportados, via "Port Forwarding", no mínimo as seguintes aplicações : Telnet, SSH, FTP over SSH, Windows Terminal Services, Outlook/Outlook Express e Lotus Notes;
- Deve ser possível criar diferentes grupos de usuários SSL VPN, com definição por grupo, do tipo de serviço permitido sobre as conexões SSL para o concentrador (WEB, e-mail, sistemas de arquivos);
- Deve ser possível especificar as URLs acessíveis através de conexões SSL VPN;
- Deve ser possível a criação de portal customizado para acesso SSL VPN. O portal deve refletir os recursos disponíveis (aplicações e URLs acessíveis, possibilidade de download do cliente SSL VPN, "banner de acesso") para o grupo a que o usuário que requisita acesso pertence;
- Deve ser possível acesso SSL-VPN a pelo menos os seguintes aplicativos (Telnet, SSH, VNC, RDP e Citrix) sem necessidade de software cliente na máquina remota. O acesso será viabilizado através de "plug-ins" para browsers;
- Deve suportar autenticação SSL-VPN através de teclado virtual apresentado ao usuário;
- Deve implementar protocolo DTLS (TLS over UDP) de acordo com a RFC 4748;
- Deve ser possível realizar verificação de parâmetros na máquina do usuário antes da apresentação das credenciais de identificação ("pre-login") . Deverá ser possível verificar pelo menos os seguintes atributos : Chaves de Registro, Arquivos, Endereços IP, Versão do Sistema Operacional e Certificados Digitais;
- Deve ser possível a criação de regras para verificação da conformidade da máquina com a política de segurança. Dever ser possível verificar no mínimo os seguintes elementos : a instalação, habilitação e atualização do software antivírus e anti-spyware e existência de personal firewall habilitado;
- Deve ser possível estabelecer, por grupo, os serviços de acesso remoto disponíveis para os usuários deste : IPSEC VPN, SSL-VPN (com cliente), SSL-VPN (sem cliente) e qualquer combinação destes métodos;
- Deve ser possível definir no concentrador VPN o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS;
- Deve implementar funcionalidade de Desktop Seguro Virtual em partição criptografada isolada com no mínimo as seguintes funcionalidades:
 - a) o download do desktop seguro virtual deve ser feito de forma automática quando da tentativa de estabelecimento da sessão SSL-VPN;
 - b) Proteção contra KeyLoggers e ScreenLoggers;
 - c) Bloqueio da porta USB durante conexão VPN Bloqueio de impressão durante conexão VPN;
 - d) Proteção contra modificação do registro conexão VPN;
 - e) Bloqueio de compartilhamento de arquivos durante conexão SSL VPN;
 - f) Bloqueio da utilização de prompt de comando (DOS).
- Deve ser possível a criação de políticas de SSL VPN dinâmicas baseadas pelo menos nos seguintes parâmetros:
 - a) Sistema Operacional Utilizado;
 - b) Anti-vírus;



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 23/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
--------------------	---

- c) Anti-spyware;
- d) Chave de Registro (existência e valor específico a ela atribuído);
- e) Arquivos do sistema;
- f) existência de um certificado digital na máquina de onde provém a tentativa de acesso;
- g) Atributos LDAP.

SUPORTE À IPS INTEGRADO

- O appliance deve suportar inclusão futura de uma solução integrada de Intrusion Prevention System (IPS) para inspeção detalhada do tráfego decifrado. A performance mínima de IPS deve ser de 2 Gbps;
- Deve ser possível selecionar, através de listas de controle de acesso, o tráfego que será enviado para inspeção pela solução de IPS;
- A solução integrada de IPS deve suportar no mínimo as seguintes funcionalidades:
 - a) Deve analisar cada um dos pacotes que trafegam pela rede a que está conectado e também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede (análise de contexto);
 - b) Deve utilizar assinaturas construídas com base em informações de vulnerabilidade e não somente em "exploits" específicos;
 - c) Deve suportar a modificação de assinaturas, isto é, permitir a edição de assinaturas existentes na base de dados, ajustando-se ao perfil de tráfego de rede;
 - d) Deve suportar a criação de assinaturas, isto é, permitir que se possam criar novas assinaturas e anexá-las à base de dados existente, adaptando-se as reais necessidades de tráfego de rede (na criação das novas assinaturas deve ser permitida a utilização de parâmetros de nível 2 a nível 7 do modelo OSI);
 - e) Deve ser possível criar assinaturas do tipo "string-match" e associá-las a qualquer porta TCP para verificação da ocorrência de conjunto de caracteres definidos pelo administrador de política de segurança no conteúdo dos pacotes IP que trafegam pela rede;
 - f) Devem ser suportados no mínimo os seguintes tipos de reação (configuráveis por assinatura de ataque) : geração de alerta, gerar trap SNMP, fazer "logging" dos pacotes gerados pelo sistema "vítima", fazer "logging" dos pacotes gerados pelo sistema que está efetuando o ataque, promover "reset" da conexão TCP, bloquear o pedido de conexão, bloquear o endereço que está gerando o ataque de conexão, negar "in-line" os pacotes associados ao ataque.

GERENCIAMENTO E CONECTIVIDADE

- Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers;
- Deve ser gerenciável via SNMP, SNMPv2c e SNMPv3;
- Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS;
- Deve possuir mecanismo interno de captura de pacotes. Deve ser possível selecionar através de guias de configuração ("wizards") quais os pacotes (IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser capturados);
- Deve permitir o armazenamento de pacotes capturados em formato tcpdump;
- Deve possuir memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento;
- Implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 24/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviadas ao servidor TACACS+;

- Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN e Firewall;
- Deve implementar, por interface, as funções de DHCP Server, Client e Relay;
- Deve suportar a criação de rotas estáticas e pelo menos os seguintes protocolos de roteamento dinâmicos : RIP, RIPv2 e OSPF. Deve suportar a utilização de pelo menos dois processos de roteamento simultâneos e independentes;
- Implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode;
- Suporte a operação como IGMP Proxy Agent;
- Deve suportar inspeção stateful de tráfego IPv6;
- Deve suportar simultaneamente a criação de regras IPv4 e IPv6;
- Deve suportar roteamento estático de tráfego IPv6;
- Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6;
- Deve implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6;
- Deve suportar pelo gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS;
- Deve suportar stateful failover de conexões IPv6;
- Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

ESPECIFICAÇÃO TÉCNICA DE REFERÊNCIA

Produto	Part Number	Descrição	Quantidade
Cisco ASA 5585	ASA5585-S10-K9	ASA 5585-X Chassis with SSP10, 8GE, 2GE Mgt, 1 AC, 3DES/AES	1
	ASA-SSP-10-INC	ASA 5585-X SSP-10 with 8GE,2SFP, incl with bundle	1
	ASA5585-BLANK-F	ASA 5585-X Full Width Blank Slot Cover	1
	ASA5585-BLANK-HD	ASA 5585-X Hard Drive Blank Slot Cover	2
	ASA5585-PWR-AC	ASA 5585-X AC Power Supply	1
	ASA5585-PWR-AC	ASA 5585-X AC Power Supply	1
	CAB-US515P-C19-US	NEMA 5-15 to IEC-C19 13ft US	2
	GLC-LH-SM	GE SFP, LC connector LX/LH transceiver	2
	ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	1
	ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	1
	SF-ASA558X-8.4-K8	Software release ASA 8.4	1



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 25/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

SISTEMA DE ALIMENTAÇÃO ININTERRUPTA (UPS) 19"

GERAL

Esta especificação define as características e requisitos elétricos e mecânicos para um sistema de alimentação ininterrupto de serviço contínuo (UPS). A UPS deve fornecer energia AC de alta qualidade para cargas de equipamentos eletrônicos sensíveis a queda de energia.

A UPS oferece baterias internas, baterias externas opcionais e capacidade de bypass interno, resultando em atividade contínua para o equipamento conectado.

UPS (UNINTERRUPTIBLE POWER SUPPLY) - 3000VA

CARACTERÍSTICAS

- Design Interativo linha com saída senoidal;
- 2U de altura para modos de rack padrão 19";
- Até 7 tomadas por bateria;
- Opções de bateria estendida;
- USB e rede de comunicações;
- Avançar desligamento de alerta precoce;
- Mínimo de cinco minutos de tempo de backup de bateria;
- Janela da tensão de entrada configurável (220, 230 e 240);
- Proteção contra surtos de Dados-line;
- Baterias hot-swappable;
- Cold-start com bateria;
- UPS monitoramento remoto através de SNMP / Web cartão;
- Totalmente compatível com RoHS.

UPS (UNINTERRUPTIBLE POWER SUPPLY) - 10000VA

GERAL

Esta especificação define as características e requisitos elétricos e mecânicos para um sistema de alimentação ininterrupto de serviço contínuo (UPS). A UPS deve fornecer energia AC de alta qualidade para cargas de equipamentos eletrônicos sensíveis a queda de energia.

A UPS oferece baterias internas, baterias externas opcionais e capacidade de bypass interno, resultando em atividade contínua para o equipamento conectado.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA:

MUSEU DO AMANHÃ

ETAPA:

Projeto Executivo

Nº DO DOCUMENTO:

MDA-PE-ATR-MD-300

REVISÃO:

R02

DATA:

28/08/2013

PÁGINA:

26/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

CARACTERÍSTICAS

- Design Interativo linha com saída senoidal;
- 3U de altura para modos de rack padrão 19”;
- Até 7 tomadas por bateria;
- Opções de bateria estendida;
- USB e rede de comunicações;
- Avançar desligamento de alerta precoce;
- Mínimo de cinco minutos de tempo de backup de bateria;
- Janela da tensão de entrada configurável (220, 230 e 240);
- Proteção contra surtos de Dados-line;
- Baterias hot-swappable;
- Cold-start com bateria;
- UPS monitoramento remoto através de SNMP / Web cartão;
- Totalmente compatível com RoHS.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA:
MUSEU DO AMANHÃ

ETAPA:
Projeto Executivo

Nº DO DOCUMENTO:
MDA-PE-ATR-MD-300

REVISÃO:

R02

DATA:
28/08/2013

PÁGINA:
27/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

ESTAÇÕES DE TRABALHO

As estações de trabalho para monitoramento e controle dos Sistemas Eletrônicos serão instaladas na sala do BMS. Deverão possuir as características mínimas descritas a seguir:

OptiPlex 980 Technical Specifications				
Processor Options ¹	Intel® Core™ i7 Quad; Intel® Core™ i5 Dual Core; Intel® Core™ i3 Dual Core; Intel® Pentium			
Chipset	Intel® Q57 Express Chipset			
Operating System Options	Microsoft® Windows 7® Ultimate (32/64 bit); Microsoft® Windows 7® Professional (32/64 bit); Microsoft® Windows 7® Home Premium; Microsoft® Windows 7® Basic Microsoft® Windows Vista® Ultimate; Microsoft® Windows Vista® Business (32/64 bit); Microsoft® Windows Vista® Home Basic Microsoft® Windows® XP Professional. Downgrade via Windows 7® Professional. Ubuntu® Linux® (select countries); FreeDOS for N-series			
Graphic Options ²	Integrated Intel® Graphics Media Accelerator HD 256MB ATI® RADEON HD 3450; 512MB ATI RADEON HD 4550; 512MB NVIDIA NV5420; 1GB NVIDIA GeForce GT330 (MT only, DP/DVI)			
Memory Options ³	Four DIMM slots; Non-ECC dual-channel 1333MHz DDR3 SDRAM, up to 16GB maximum system memory			
Networking Options	Integrated Intel® 82576DM GbE Ethernet LAN 10/100/1000; Dell Wireless 1520 mini PCIe WLAN card (802.11n)			
Standard I/O Ports	MT-10 USB 2.0 ports; 1 Parallel; 1 Serial; 1 RJ-45; 1 VGA; 1 Display Port; 1 eSATA; 2 Line-in (stereo/microphone); 2 Line-out (headphone/speaker) DT/SFF-8 USB 2.0 ports; 1 Parallel; 1 Serial; 1 RJ-45; 1 VGA; 1 Display Port; 1 eSATA; 2 Line-in (stereo/microphone); 2 Line-out (headphone/speaker)			
Removable Media	Blu-ray Writer; DVD+/-RW; DVD-ROM; Dell 19 in 1 Media Card Reader			
Hard Drive Options ⁴	3.5" Hard Drives: up to 500GB 7200 RPM SATA 3.0GB/s, up to 160GB 10K RPM SATA 3.0GB/s 2.5" Hard Drives: up to 320GB 7200 RPM SATA 3.0GB/s, up to 250GB SATA Full Disk Encryption, up to 128GB SATA Solid State Drive RAID 0 & 1 support on select configurations All chassis support Dell's Flexible Computing Solution diskless option			
Chassis Options ⁵		MT	DT	SFF
	Dimensions (H x W x D) Inches/(cm)	16.06 x 7.33 x 19.96 in. 40.80 x 18.70 x 43.09 cm	15.61 x 4.20 x 13.70 in. 39.65 x 10.9 x 34.80 cm	11.40 x 3.35 x 12.74 in. 28.96 x 8.52 x 32.36 cm
	Weight (lbs/kg)	25.0lbs / 11.4kg	18.4lbs / 8.3kg	13.0lbs / 5.9kg
	Number of Bays	2 internal 3.5"; 1 external 3.5"; 2 external 5.25"	1 internal 3.5"; 1 external 3.5"; 1 external 5.25"	1 internal 3.5"; 1 external 3.5"; 1 external 5.25"
	Expansion Slots	2 full height PCIe x16 (1 slot routed as x4);	2 low-profile PCIe x16 (1 slot routed as x4); 2 low-profile PCI	1 low-profile PCIe x16; 1 low-profile PCI
	Power Supply ⁶	305W Standard PSU or optional 255W up to 90% Efficient PSU	255W Standard PSU or optional 255W up to 90% Efficient PSU	235W Standard PSU or optional 235W up to 90% Efficient PSU
Peripheral Options	All-in-One Small Form Factor Stand with Display options (SFF only): 19" P190S Standard, 19" P1909W Wide and 22" P2210 Wide			
	Keyboards: Dell QuietKey™ Keyboard, Dell Multimedia Pro Keyboard, Dell Smartcard Keyboard			
	Mouse: Dell USB Optical Mouse, Dell Laser Mouse			
	Audio Speakers: Internal Dell Business audio speaker, Dell AX210 2.0 and AY410 2.1 Desktop Speakers; Dell AX510 and AX510PA Sound Bar Speakers			
Security Options	Trusted Platform Module (TPM) 1.2, Non-TPM (in select countries only), Dell ControlPoint, Chassis lock slot and lock loop support, optional Chassis Intrusion Switch, Setup/BIOS Password, I/O Interface Security, Smart Card keyboards, Intel® Trusted Execution Technology, BIOS support for optional Computrace SM			
Systems Management Options ¹⁰	Intel® Core i7/i5 vPro™ Technology enabled (iAMT Professional 6.x); Intel® Standard Manageability (iAMT Professional 6.x); No Out-of-Band Systems Management			
Environmental and Regulatory Standards	Environmental Standards (eco-labels): ENERGY STAR® 5.0 (select configurations), EPEAT Gold (select configurations), CECP, TCO 05, WEEE, Japan Energy Law, CES, Japan Green PC, FEMP, South Korea Eco-label, EU RoHS, China RoHS Other Environmental Options: Dell Energy Smart settings (select configurations); Carbon Off-set; Dell Asset Recovery Service			
Warranty and Service Options ¹¹	Limited Hardware Warranty ⁷ ; Standard 3-year Next Business Day On Site Service after Remote Diagnosis ⁸ (3-3-3); Optional 3-year Dell ProSupport™ for IT; 4 year and 5 year extended warranty, service and support options ¹²			



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 28/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

Dispositivos de Segurança:

Suporte para cabo de travamento do chassi (com travas de cabo disponíveis);
Detector de violação do chassi;
Senha de configuração/BIOS;
Segurança de interface de E/S;
Leitor de Smart Card opcional, tecnologia Intel® Trusted Execution.

Todas as estações de trabalho deverão ser fornecidas com sistema operacional Windows 7 ou superior, com as devidas licenças e também com licenças call para acesso aos servidores. As estações deverão também possuir os softwares de aplicativos (SCA, AUT, CTV, INC e ALA) e as respectivas as licenças.

IMPRESSORA

A impressora descrita a seguir deverá ser instalada na sala BMS.
Características mínimas:

CARACTERÍSTICAS MÍNIMAS	
Velocidade de impressão preto (normal, A4)	No mínimo 30 ppm
Velocidade de impressão cor (normal, A4)	No mínimo 30 ppm
Velocidade de impressão preto (normal, carta)	No mínimo 30 ppm
Velocidade de impressão colorido (normal, carta)	No mínimo 30 ppm
Nota de rodapé sobre velocidade de impressão	Mensurado usando a ISO/IEC 24734, exclui o primeiro conjunto de documentos de teste. Para obter mais informações, consulte http://www.hp.com/go/printerclaims . A velocidade exata varia dependendo da configuração do sistema, do aplicativo de software, do driver e da complexidade do documento.
Qualidade de impressão preto (ótima)	No mínimo 600 x 600 dpi
Qualidade de impressão cor (ótima)	No mínimo 600 x 600 dpi
Tecnologia de impressão	Laser
Ciclo de trabalho (mensal, A4)	No mínimo 120.000 páginas



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 29/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

Nota sobre ciclo de trabalho	O ciclo de trabalho é definido como o número máximo de páginas por mês de saída de imagens.
Volume mensal mínimo de páginas recomendado	10.000
Memória padrão	1 GB
Memória máxima	1 GB
Capacidade do disco rígido	Padrão, 8 GB
Velocidade do processador	800 MHz

MOBILIÁRIO TÉCNICO PARA AS ESTAÇÕES DE TRABALHO

Deve ser fornecido para as salas de controle (BMS) mobiliário completo (mesas, cadeiras, plataformas, suportes, consoles, etc..) de negócios projetados para uso em ambientes tecnológicos. Possui recursos que permitem a acomodação dos equipamentos de informática em função das necessidades do usuário, e possibilitam a distribuição eficaz do sistema de cabeamento, sempre com características que respeitam o conforto e ergonomia.

Consoles produzidos com estrutura em chapas de aço retangular que recebem tratamento antiferruginoso através de banhos fosfatizantes e pintura a base de resina epoxi pó, constituída por cavaletes metálicos modulares autoportantes. Braço estrutural com função de instalação e apoio dos tampos: principal (área de trabalho) em madeira termo estabilizada revestida em laminado melamínico de alta pressão, com encabeçamento em madeira de lei ou perfil maciço de PVC, e tampos secundários (apoio ajustável para monitores), em chapa de aço dobrada com flexibilidade de ajuste na altura, inclinação e profundidade, acoplado ao quadro por simples encaixe. Painéis de fechamento em madeira termo estabilizada, com 30 mm de espessura, revestidos em laminado melamínico.

ACESSÓRIOS DO MOBILIÁRIO

- Pannel Multifuncional (Slat Wall) utilizado para fixação de suportes de monitores e acessórios como caixa para documentos e manuais;
- Canaleta de Fiação para régua de tomadas elétricas e tomadas de dados/voz;
- Painéis de fechamento lateral / traseiros;
- Cadeiras com assento giratório e rodízios, revestimento em tecido, com regulagem de altura do assento e do encosto, conforme conceitos ergonômicos aplicáveis;

Esta especificação de mobiliário contempla os itens a serem fornecidos para as estações de monitoramento da **SALA BMS**.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 30/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

GERENCIAMENTO

- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
 - a) Sem autenticação e sem privacidade (noAuthNoPriv);
 - b) Com autenticação e sem privacidade (authNoPriv);
 - c) Com autenticação e com privacidade (authPriv).
- Possuir suporte a MIB II, conforme RFC 1213;
- Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;
- Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757;
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE;
- Implementar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 9 unidades, com velocidade de empilhamento de 128 Gbps full-duplex;
- A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha;
- Suportar o compartilhamento de fontes entre diferentes elementos da pilha de switches, possibilitando a redução do número de fontes solicitadas para o conjunto;
- Permitir a configuração automática da porta do switch de acordo com o tipo de dispositivo conectado à mesma;
- Permitir a gerência e controle do consumo energético dos dispositivos conectados às portas do switch.

QUALIDADE DE SERVIÇO

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nível 2) e DSCP ("Differentiated Services Code Point" - nível 3), conforme definições do IETF (Internet Engineering Task Force);
- Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing";
- Deve ser possível a especificação de banda por classe de serviço;
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote;
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN;



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 31/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection);
- Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).

SEGURANÇA

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando;
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino;
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Possuir controle de broadcast, multicast e unicast por porta;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede;
- Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2;
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w);
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta.

PADRONIZAÇÃO

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging);
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- Implementar padrão IEEE 802.3ad;
- Implementar padrão IEEE 802.3af;
- Implementar padrão IEEE 802.3at;



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 32/34

DISCIPLINA: ATR	TÍTULO: MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)
---------------------------	--

- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
 - Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
 - a) A estação não tem cliente 802.1x (suplicante);
 - b) As credenciais do usuário não estão corretas (falha de autenticação).
 - Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan);
 - Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
 - a) Nome do usuário;
 - b) Switch em que o computador do usuário está conectado;
 - c) Porta do switch utilizada par acesso;
 - d) Endereço MAC da máquina utilizada pelo usuário;
 - e) Endereço IP do usuário;
 - f) Horários de início e término da conexão;
 - g) Bytes transmitidos e recebidos durante a conexão.
 - Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);
 - Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x;
 - Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;
 - Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS;
 - Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;
 - Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
 - Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra;
 - Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS;
 - Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
 - Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA: MUSEU DO AMANHÃ	
ETAPA: Projeto Executivo	
Nº DO DOCUMENTO: MDA-PE-ATR-MD-300	
REVISÃO: R02	
DATA: 28/08/2013	PÁGINA: 33/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)

DIVERSOS

Fornecimento de cabos de força e cabo serial, além de qualquer dispositivo e/ou acessório e softwares necessários ao perfeito funcionamento do equipamento.

O Equipamento deverá ser novo e sem uso anterior e estar em linha normal de produção.

O equipamento deverá ser homologado pela ANATEL. Na apresentação da proposta deve constar cópia do certificado de homologação.

ENSAIOS

Para efeito de entrega e aceitação do ATR, deverão ser efetuados ensaios para verificação das condições de funcionamento de todos os equipamentos, em atendimento às exigências normativas. Tais ensaios deverão ser executados pela Contratada, que para tanto deve dispor de todos os equipamentos, instrumentos e pessoal técnico capacitado e demais meios necessários.

AS BUILT

A instaladora deverá fornecer ao final dos serviços, versão as built (como executado) dos projetos. Este projeto as built deverá ser assinado pelo Engenheiro Responsável Técnico pela instalação.

Nos projetos as built, deverão ser registrados todos os percursos e componentes da instalação, bem como as modificações realizadas em relação ao projeto executivo.

Deverá ser emitido junto ao projeto as built, um documento indicando todos os endereços IP do ATR.

GARANTIA

Todos os componentes e o conjunto completo de equipamentos fornecidos e instalados deverão ser garantidos pelo fornecedor e / ou instalador durante o prazo mínimo de 5 (cinco) anos, a partir da data de recebimento e aceitação da instalação.

A garantia se estende para qualquer defeito de fabricação ou funcionamento.

CONSIDERAÇÕES FINAIS

Desde que atenda às premissas técnicas de projeto e as aqui especificadas, promovendo o perfeito funcionamento do sistema, a contratada poderá optar por outros fabricantes dos equipamentos que comporão o sistema de ATR.



Prefeitura da cidade do Rio de Janeiro

COMPANHIA DE DESENVOLVIMENTO URBANO DA REGIÃO
DO PORTO DO RIO DE JANEIRO

CONSÓRCIO CONSTRUTOR:

COORDENAÇÃO DE PROJETOS:

PROJETISTA:



fernandes /
arquitetos
associados



OBRA:

MUSEU DO AMANHÃ

ETAPA:

Projeto Executivo

Nº DO DOCUMENTO:

MDA-PE-ATR-MD-300

REVISÃO:

R02

DATA:

28/08/2013

PÁGINA:

34/34

DISCIPLINA:

ATR

TÍTULO:

MEMORIAL DESCRITIVO DOS SISTEMAS DE ATIVOS DE REDE (ATR)