



OI SMARTCLOUD

# 01 SMARTWALL O QUE É?



A **SmartWall** é o firewall que irá proteger o conjunto de redes virtuais geridas pelo cliente.

O seu console Web de configuração permite ao cliente autonomia na gestão da sua rede.

# 02 SMARTWALL ACESSO



Acesso encontra-se disponível no portal.

**SmartCloudPT** PT Prime PT Negócios

PT Comunicações S.A. DTI/APS/DCA (ID da conta: 1018818)

A minha conta | SmartCloudPT | **Gerir e utilizar serviços** | Seleccionar subscrição | Ajuda e suporte | Serviços adicionais | Terminar sessão

Subscrição: 1017295

Serviços Web

- Gestão de Recursos
- Servidores Privados**
  - Visão Geral
  - Servidores

Gerir e utilizar serviços > Serviços Web > Servidores Privados

## Servidores

Screen ID: 2.21.05.51 [Actualizar](#)

### Servidores

**VISÃO GLOBAL**

IP Público: 62.48.141.216 [ Gerir Firewall ]

[Criar Rede](#) [Criar Grupo](#) [Novo Servidor](#)

Servidor Ligado  Servidor Ligado com Notificações  Backup  Servidor gerido  
 Servidor Desligado  Servidor Ligado com Alertas  Servidor Externo  Servidor Indisponível

Redes	
FE	BE

# 03 SMARTWALL FUNCIONALIDADES



- ✓ Regras
- ✓ NAT
- ✓ Interfaces
- ✓ DHCP
- ✓ Apoio ao Diagnóstico
- ✓ OpenVPN

# 04 SMARTWALL REGRAS



- ✓ Nas regras podemos permitir ou bloquear acessos para as redes virtuais do cliente.
- ✓ Por omissão o acesso **WAN (Rede Pública) => LAN (Rede Privada)** é negado, sendo necessário criar regras específicas para permitir a transmissão de dados.
- ✓ Por omissão o acesso **LAN => WAN** é permitido , sendo necessário criar regras específicas para negar a transmissão de dados.

# 04 SMARTWALL REGRAS



## Firewall

firewall.local : Logout

Sistema Interfaces Firewall Serviços VPN Estado Diagnosticos

### Firewall: Regras

WAN LAN1 LAN3

	Protocolo	Origem	Porta	Destino	Porta	Gateway	Calendarização	Descrição	
<input type="checkbox"/>	TCP	*	*	endereço WAN	1194 (OpenVPN)	*		Acesso via OpenVPN	
<input type="checkbox"/>	TCP	*	*	endereço WAN	4443	*		Acesso a consola Firewall	
<input type="checkbox"/>	TCP	*	*	172.16.2.80	22 (SSH)	*		NAT rmp	
<input type="checkbox"/>	TCP	*	*	172.16.2.32	22 (SSH)	*		NAT ssh-imap01	

permitir      bloquear      rejeitar      registar em log  
 permitir (inactiva)      bloquear (inactiva)      rejeitar (inactiva)      registar em log (inactiva)

**Dica:**  
As regras são testadas com a lógica 'first-match' (isto é, a acção da primeira regra que abranja o pacote será executada). Isto significa que se usar regras de bloqueio, terá que prestar atenção à ordem das regras. Tudo que não é explicitamente permitido é bloqueado por defeito.

Firewall 2011 por Portugal Telecom. Todos os direitos reservados. [ver licença]

# 04 SMARTWALL REGRAS – ADICIONAR REGRA



### Firewall: Regras: Edição

**Acção\***    
Selecione o que fazer com os pacotes abrangidos pelo critério especificado abaixo.  
Dica: a diferença entre bloquear e rejeitar é que os pacotes rejeitados (TCP RST or ICMP port unreachable for UDP) é devolvido à origem, enquanto que os pacotes bloqueados são descartados silenciosamente. Em qualquer dos casos, o pacote original é descartado. A rejeição funciona apenas quando o protocolo é definido como TCP ou UDP (mas não "TCP/UDP") abaixo.

**Inactivo**  **Desactivar esta regra**  
Selecione esta opção para desactivar esta regra sem a remover da lista.

**Interface\***    
Selecione o interface pelo qual os pacotes devem entrar para aplicar esta regra.

**Protocolo\***    
Selecione o protocolo IP alvo desta regra.  
DICA: na maior parte dos casos, deve especificar *TCP* aqui.

**Origem\***  **not**  
Utilize esta opção para inverter a lógica desta regra.

Tipo:    
Endereço:  /

- Show source port range

**SO de origem** Tipo de OS:    
Nota: só funciona para regras TCP

**Destino\***  **not**  
Use esta opção para inverter a lógica da regra.

Tipo:    
Endereço:  /

**Intervalo de portas de destino** de:     
para:

Especifique a porta ou intervalo de portas de destino dos pacotes para esta regra.  
DICA: pode deixar o campo 'para' em branco se pretende apenas filtrar uma porta individual.

**Registo de log**  **Registrar em log os pacotes abrangidos por esta regra**  
Dica: a firewall tem espaço de disco limitado. Não active o registo para tudo. Se pretende registar uma quantidade elevada de tráfego considere usar um servidor remoto de registo de log (veja a página [Diagnosticos: Logs de Sistema: Configurações](#)).

**Opções avançadas**  - Mostrar opções avançadas

**Tipo de estado**  - Mostrar estado

# 05 SMARTWALL NAT



Configurar um NAT permite que uma porta de um servidor na rede interna seja disponibilizado no IP publico (para acesso a partir do exterior).

No exemplo que se segue, é disponibilizado o acesso a porta 22 (SSH) do host 172.16.2.128 via porta 10022 do IP público (62.48.143.143).

**Firewall: NAT: Redireccionamento de portas**

Redireccionamento de portas **1:1** NAT de saída

	Interface	Protocolo	Intervalo de portas externas	IP de NAT	Intervalo de portas internas	Descrição	
<input type="checkbox"/>	WAN	TCP	10022	172.16.2.128 (ext.: 62.48.143.143)	22 (SSH)	web-ssh	  
<input type="checkbox"/>	WAN	TCP	922	172.16.2.127 (ext.: 62.48.143.143)	22 (SSH)	db-ssh	  
<input type="checkbox"/>	WAN	TCP	80 (HTTP)	172.16.2.128 (ext.: 62.48.143.143)	80 (HTTP)	www	  
<input type="checkbox"/>	WAN	TCP	443 (HTTPS)	172.16.2.128 (ext.: 62.48.143.143)	443 (HTTPS)	ssl	  

# 05 SMARTWALL NAT – ADICIONAR NAT



## Firewall: NAT:Redirecionamento de portas: Editar

### Interface\*

WAN

Escolha o interface ao qual esta regra se aplica.  
Dica: na maior parte dos casos é pretendido o interface WAN.

### Endereço externo

Endereço do interface

Se desejar que esta regra seja aplicada a outro endereço IP que não o interface escolhido em cima, seleccione-o aqui (deve definir um IP virtual primeiro). Note que se está a redirecionar ligações no interface LAN, deve seleccionar a opção "qualquer"

### Protocolo\*

TCP

Selecione o protocolo IP alvo desta regra.  
Dica: na maior parte dos casos deve especificar TCP aqui.

### Intervalo de portas externas \*

from: (outra) 10022  
to: (outra)

Especifique a porta ou intervalo de portas no endereço externo da firewall para este mapeamento.  
Dica: Pode deixar o campo 'to' em branco se só pretende mapear uma porta individual.

### IP de NAT\*

172.16.2.128

Insira o IP interno do servidor no qual pretende mapear as portas.  
por exemplo 192.168.1.12

### Porta local\*

(outra) 22

Especifique a porta na máquina com o endereço IP inserido acima. No caso de um intervalo de portas, especifique a porta inicial do intervalo (a porta final será calculada automaticamente).  
Dica: Esta porta é normalmente idêntica à porta de 'origem' acima.

### Descrição

web-ssh

Pode inserir aqui uma descrição para sua referência (não é usada internamente).

Gravar

Cancelar



Podem ser criadas varias redes e editadas as configurações das respectivas interfaces.

Nos seguintes slides, é mostrado como criar uma rede e editar a sua configuração.

**Notas:** Sempre que reconfigurar o endereçamento de um interface de rede, deve rever a respectiva configuração do Servidor DCHP.

# 07 SMARTWALL CRIAR REDE



**Servidores**

## VISÃO GLOBAL

IP Público: 62.48.141.216 [ Gerir Firewall ]

**Criar Rede** Criar Grupo Novo Servidor

Servidor Ligado     Servidor Ligado com Notificações     Backup     Servidor gerido  
 Servidor Desligado     Servidor Ligado com Alertas     Servidor Externo     Servidor Indisponível

Redes		
	FE	BE
Default	0 Servidores	0 Servidores

Servidores » Redes » Nova Rede

## NOVA REDE

**Nome:**  
Back-end

**Descrição:**  
Rede Sem acesso a Internet

Cancelar

Passo 1 de 2 **Criar Rede**

# 07 SMARTWALL CRIAR REDE & EDITAR REDE



Servidores » Redes

**REDES**

REDE BACK-END  
Rede Sem acesso a Internet

**Editar Rede >**

**Back-end**  
Rede Sem acesso a Internet

**BE**  
VLAN Backend

**FE**  
VLAN Frontend

**Rede criada com sucesso.**

Default

RM

PF

**Interfaces: Opcional 2 (LAN2)**

Configuração do Interface Opcional

**Activar Interface 2**

Descrição\* LAN2

Configuração IP

Activar *Bridge* com nenhum

Tipo Static

Endereço IP\* 172.16.3.1 / 24

Gateway

Se este interface for uma ligação à Internet, introduza o caminho por defeito (default gateway ou router) para o tráfego IP. Caso contrário deixe a opção em branco.

Assistente FTP

Assistente FTP  Desactivar a aplicação de FTP-Proxy

Configuração de cliente DHCP

Nome do Servidor

O valor deste campo é enviado como identificador do cliente e nome do servidor aquando do pedido de um endereço DHCP (lease).

**Gravar**



## CONFIGURAÇÃO AUTOMÁTICA DE IPS

O DHCP evita erros de configuração e ajuda a prevenir conflitos de endereços.

Adicionalmente, a utilização de servidores DHCP pode diminuir significativamente o tempo de configuração e reconfiguração de servidores na rede.

Por omissão, o DHCP encontra-se ativo para todas as redes disponibilizadas, podendo ser desativado na opção “Serviços: Servidor DHCP”.

Nesta opção existe ainda a possibilidade configurar mapeamentos de IP estáticos.



<input checked="" type="checkbox"/> <b>Activar o servidor DHCP no interface LAN1</b>	
<input type="checkbox"/> <b>Rejeitar clientes desconhecidos</b> Se esta opção estiver activa, apenas os clientes listados abaixo poderão obter endereços por DHCP deste servidor.	
<b>Subrede</b>	172.16.2.0
<b>Máscara de rede</b>	255.255.255.0
<b>Intervalo disponível</b>	172.16.2.0 - 172.16.2.255
<b>Intervalo*</b>	<input type="text" value="172.16.2.2"/> a <input type="text" value="172.16.2.128"/>
<b>Servidores WINS</b>	<input type="text"/> <input type="text"/>
<b>Servidores DNS</b>	<input type="text"/> <input type="text"/>
NOTA: deixe em branco para usar os servidores DNS pré-definidos do sistema - o endereço IP deste interface se o DNS forwarder estiver activo, caso contrário, os servidores configurados na página de configuração geral.	
<b>Gateway</b>	<input type="text"/> O comportamento pré-definido é o uso do endereço IP deste interface da firewall como gateway. Especifique aqui um gateway alternativo se este não for o gateway correcto para a sua rede.
<b>Tempo de contrato pré-definido</b>	<input type="text"/> segundos Isto é usado para clientes que não pedem um tempo de contrato específico. O valor pré-definido é 7200 segundos.
<b>Tempo máximo do contrato</b>	<input type="text"/> segundos Este é o tempo máximo de contrato para clientes que pedem um tempo de contrato específico. O valor pré-definido é 86400 segundos.
<b>Substituição em falha por IP:</b>	<input type="text"/> Deixe em branco para desactivar. Insira o endereço real de outra máquina. As máquinas devem usar CARP.
<b>ARP estático</b>	<input type="checkbox"/> <b>Activar entradas de ARP estático</b> <b>Nota:</b> Apenas as máquinas listadas abaixo poderão comunicar com a firewall neste NIC.
<b>DNS dinâmico</b>	<input type="button" value="Avançadas"/> - Mostrar DNS dinâmico
<b>Servidores NTP</b>	<input type="button" value="Avançadas"/> - Mostrar configurações de NTP

# 09 SMARTWALL DIAGNÓSTICO



Seguem algumas ferramentas que podem ser úteis no diagnóstico de possíveis problemas.

## Diagnósticos: Ping

Endereço\*

Interface\*

Número de pedidos\*

Ping

## Diagnósticos: Traceroute

Endereço\*

Número máximo de saltos\*

Usar ICMP

Traceroute

# 09 SMARTWALL DIAGNÓSTICO



## Resumo do sistema

### Informação do sistema

<b>Nome</b>	firewall.local
<b>Versão</b>	<b>1.2.3-pt10</b> de Sun Dec 6 23:21:36 EST 2009
<b>Plataforma</b>	Firewall
<b>Tempo ligado</b>	98 days, 22:00
<b>Tamanho da tabela de estados</b>	170/10000 <a href="#">Visualizar estados</a>
<b>Utilização de MBUF</b>	2685 /3465
<b>Utilização de CPU</b>	 0%
<b>Utilização de memória</b>	 76%
<b>Utilização de SWAP</b>	 22%
<b>Utilização do disco rígido</b>	 25%

# 09 SMARTWALL DIAGNÓSTICO



## Estado: Serviços

Serviços	Descrição	Estado	
dnsmasq	DNS Forwarder	A correr	
ntpd	NTP clock sync	A correr	
dhcpd	DHCP Service	A correr	

## Diagnósticos: Logs do Sistema: Sistema

Sistema

Firewall

DHCP

Balanceamento de carga

OpenNTPD

Configurações

Últimas 50 entradas no log do sistema

Mar 6 17:15:58

syslogd: kernel boot file is /boot/kernel/kernel

Limpar o log

Filtrar



A OpenVPN permite autenticação ponto-a-ponto através de chaves secretas compartilhadas e certificados digitais.

No slide seguinte encontramos a página “cliente VPN” onde podemos fazer o download do software e certificados que permitem abrir um canal VPN para a rede privada do datacenter virtual.

# 10 SMARTWALL OPENVPN



## VPN: Configuração de cliente OpenVPN

1. [Instale o cliente de OpenVPN](#) a partir do site [OpenVPN downloads](#).

Instale com as opções pré-definidas.

**Nota:** A instalação pára e fica a aguardar a aceitação, por parte do utilizador, da instalação dos drivers necessários. Desvie a janela de instalação para proceder à referida aceitação.

2. Coloque os ficheiros seguintes ficheiros em **C:\Program Files\openvpn\config**

1. **ca.crt** com o conteúdo de *certificado CA*
2. **ovpn\_client1.key** com o conteúdo de *chave de cliente*
3. **ovpn\_client1.crt** com o conteúdo de *certificado de cliente*.

3. Crie o ficheiro "**C:\Program Files\openvpn\config\SmartCloudPT.ovpn**" com o conteúdo:

```
client
dev tun
proto tcp
remote 62.48.141.216 1194
ping 10
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert ovpn_client1.crt
key ovpn_client1.key
ns-cert-type server
comp-lzo
pull
verb 3
cipher AES-256-CBC
```

4. O seu cliente de VPN está configurado. Apenas necessita executar a aplicação OpenVPN (atalho disponível no login de instalação) e activar a ligação de gestão, para aceder a todos os servidores do seu data center virtual.

instalação) e activar a ligação de gestão, para aceder a todos os servidores do seu data center virtual.

4. O seu cliente de VPN está configurado. Apenas necessita executar a aplicação OpenVPN (atalho disponível no login de