

# Guia do Usuário

VERSAO 1.1 AGO/2016



**UTM**

**BLOCKBIT**  
Unified Threat Management



### **Sobre o material**

O conteúdo deste material é de propriedade intelectual BLOCKBIT, é proibida sua utilização, manipulação ou reprodução, por pessoas estranhas e desvinculadas de suas atividades institucionais sem a devida, expressa e prévia autorização, sujeitando-se o infrator às penas da lei, sem prejuízo das sanções civis pertinentes.

**Revisão:** Agosto/2016

**Release:** 2

**Fale com nossos especialistas.**

**Contatos:**

**AMÉRICA DO NORTE (Sede)**

1450 Brickell Avenue – 14th floor

Miami – FL – 33131

UNITED STATES

Tel: +1 305 373 4660

**EUROPA (Escritório Principal)**

2 Kingdom Street – 6th floor

Paddington – London – W2 6JP

UNITED KINGDOM

Tel: +44 203 580 4321

**AMÉRICA LATINA (Escritório Principal)**

R. Engenheiro Francisco Pitta Brito, 779 – 3º andar

São Paulo – SP – 04753-080

BRASIL

Tel: +55 11 2165 8888

**E-mail:** [support@blockbit.com](mailto:support@blockbit.com)

**Site:** [www.blockbit.com](http://www.blockbit.com)

## **APRESENTAÇÃO**

Obrigado por escolher as soluções de segurança BLOCKBIT! É fácil estar seguro.

Com mais de 18 anos de experiência de mercado, a BLOCKBIT possui uma grande rede de revendas com excelência técnica oferecendo suporte local, canais de suporte direto e conta também com o BLOCKBIT Global Intelligence Lab que trabalha 24x7x365 na pesquisa e análise de novas ameaças melhorando a segurança de sua empresa.

O BLOCKBIT UTM é uma solução de cibersegurança de última geração que unifica as tecnologias de Next Generation Firewall, IPS, VPN IPsec, Advanced Web Filter, Advanced Threat Protection e muito mais.

O BLOCKBIT UTM possui uma interface web intuitiva de fácil utilização onde as informações de todos os recursos são organizadas, agrupadas, ordenadas e exibidas no Dashboard, permitindo uma rápida Visão, Gestão e Tomadas de Decisão.

**Equipe BLOCKBIT**



# ÍNDICE

<b>1</b>	<b>PREPARAÇÃO</b>	<b>13</b>
1.1	Recomendações.....	14
1.1.1	<i>Perguntas Fundamentais para Elaboração da Política de Segurança .....</i>	14
1.2	Requisitos .....	14
<b>2</b>	<b>ACESSANDO A INTERFACE WEB</b>	<b>15</b>
2.1	Entendendo a Interface Web .....	16
2.1.1	<i>Menu de Opções.....</i>	16
<b>3</b>	<b>DASHBOARD</b>	<b>17</b>
3.1	Recursos do Dashboard.....	18
<b>4</b>	<b>CONFIGURANDO O BLOCKBIT UTM</b>	<b>19</b>
4.1	Configurações Básicas .....	19
4.2	Configurando Interfaces de Rede .....	20
4.2.1	<i>Configurando uma interface física .....</i>	20
4.2.2	<i>Adicionando uma interface virtual.....</i>	22
4.3	Link Aggregation .....	24
4.3.1	<i>Configurações.....</i>	26
4.3.2	<i>Alterando a prioridade das interfaces LAG .....</i>	28
4.4	Configurando Rotas .....	29
4.5	Licenciamento.....	30
<b>5</b>	<b>ADMINISTRAÇÃO DO SISTEMA</b>	<b>33</b>
5.1	Configurações .....	33
5.2	Administradores .....	35
5.3	Auditória .....	38
5.4	Bloqueados .....	39
<b>6</b>	<b>ARMAZENAMENTOS</b>	<b>40</b>
6.1	Adicionando um Armazenamento SMB .....	41
6.2	Adicionando um Armazenamento NFS.....	42
6.3	Adicionando um Armazenamento Disco .....	44
<b>7</b>	<b>BACKUP / RESTORE / SNAPSHOT</b>	<b>48</b>
7.1	Configurações .....	48
7.2	Backups do Dispositivo .....	50
7.3	Snapshot .....	52

<b>8</b>	<b>CERTIFICADOS</b>	<b>54</b>
8.1	Instalação da CA via GPO .....	57
<b>9</b>	<b>OBJETOS</b>	<b>64</b>
9.1	Objeto Endereços IP.....	65
9.1.1	<i>Adicionando um Objeto Endereço IP .....</i>	66
9.2	Objeto Endereços Mac.....	68
9.2.1	<i>Adicionando Objeto Endereços MAC.....</i>	69
9.3	Objeto Serviços .....	71
9.3.1	<i>Adicionando um Objeto Serviços .....</i>	72
9.4	Objeto Horários.....	75
9.4.1	<i>Adicionando Objeto Horários .....</i>	76
9.5	Objeto Períodos / Datas.....	78
9.5.1	<i>Adicionando um Objeto Período / Data .....</i>	79
9.6	Objeto Dicionários .....	80
9.6.1	<i>Adicionando um Objeto Dicionários .....</i>	81
9.7	Objeto Tipo de Content-type .....	84
9.7.1	<i>Gerenciando Objetos Content-type .....</i>	85
9.7.2	<i>Adicionando Objeto Content-type .....</i>	86
<b>10</b>	<b>AUTENTICAÇÃO</b>	<b>87</b>
10.1	Integrando Domínios e Usuários - Windows / LDAP .....	88
10.2	Autenticação Single Sign On .....	92
10.2.1	<i>Requisitos .....</i>	92
10.2.2	<i>Download do agente SSO .....</i>	93
10.2.3	<i>Construindo um EVENTO de login .....</i>	94
10.3	Gerenciando a Lista de Usuários.....	100
10.3.1	<i>Adicionando Domínios e Grupos Locais.....</i>	101
10.3.2	<i>Adicionando Grupos de Usuários para os Domínios Locais.....</i>	102
10.3.3	<i>Importando e Adicionando Usuários .....</i>	104
10.4	Adicionando Grupo de Auto Cadastro (Captive portal).....	107
10.5	Portal de Autenticação .....	109
10.6	Captive Portal.....	111
<b>11</b>	<b>FIREWALL</b>	<b>117</b>
11.1	Serviços .....	119
11.1.1	<i>Autenticação.....</i>	120
11.1.2	<i>Administração.....</i>	120
11.1.3	<i>DNS .....</i>	121
11.1.4	<i>DHCP .....</i>	121
11.1.5	<i>VPN .....</i>	122
11.1.6	<i>VPN SSL .....</i>	122
11.1.7	<i>Web Proxy.....</i>	123

11.2	Parâmetros de Segurança.....	124
11.2.1	<i>Proteção DOS .....</i>	124
11.2.2	<i>Proteção PortScan .....</i>	125
11.2.3	<i>Proteção Pacotes Inválidos .....</i>	125
11.2.4	<i>Proteção SYN flood.....</i>	125
11.2.5	<i>Proteção ICMP flood.....</i>	125
11.2.6	<i>Permite ICMP Redirect .....</i>	125
11.2.7	<i>Ignorar ICMP Broadcast .....</i>	126
11.2.8	<i>Source Routing .....</i>	126
11.3	Política Padrão.....	127
11.4	Zone Protection .....	128
11.5	Redirecionamentos (DNAT) .....	130
11.5.1	<i>Exemplo - Acesso Remoto ao Servidor de Câmeras .....</i>	131
11.5.2	<i>Exemplo - Acesso ao Servidor WEB – Extranet.....</i>	136
<b>12</b>	<b>WEB CACHE</b>	<b>139</b>
12.1	Serviços.....	140
12.2	Cache .....	141
12.3	Hierarquia .....	142
<b>13</b>	<b>WEB FILTER</b>	<b>144</b>
13.1	Categoria.....	145
13.2	Mensagem de Bloqueio.....	147
13.3	Domínios do Google .....	148
13.4	Pesquisa Segura .....	149
<b>14</b>	<b>IPS – SISTEMA DE PREVENÇÃO DE INTRUSOS</b>	<b>150</b>
14.1	Atualização da Base .....	151
<b>15</b>	<b>ATP – PROTEÇÃO AVANÇADA CONTRA AMEAÇAS</b>	<b>153</b>
15.1	Atualização da Base .....	154
<b>16</b>	<b>TRAFFIC SHAPING</b>	<b>157</b>
16.1	Definições das Prioridades .....	158
16.2	Habilitar Traffic Shaping .....	159
16.3	Exemplo .....	160
<b>17</b>	<b>MULTILINK</b>	<b>161</b>
17.1	Requisitos para Implementação de Multilink.....	162
17.2	Configurações de Redundância (Failover). ....	163
17.3	Alterando a Prioridade dos Links.....	165
17.4	Balanceamento de Tráfego.....	166

17.5	Serviços do Dispositivo .....	167
<b>18</b>	<b>DHCP</b>	<b>168</b>
18.1	Habilitação DHCP .....	170
18.2	Configurações .....	171
18.3	Range .....	172
18.4	Endereços Estáticos .....	174
18.4.1	<i>Exemplo – Definindo endereços estáticos por DHCP</i> .....	174
18.5	Monitor DHCP .....	176
<b>19</b>	<b>DNS</b>	<b>177</b>
19.1	Configurações .....	178
19.2	Redirecionamento .....	180
<b>20</b>	<b>DNS DINÂMICO (DDNS)</b>	<b>182</b>
20.1	Configuração DNS Dinâmico .....	183
<b>21</b>	<b>VPN IPSEC</b>	<b>185</b>
21.1	Requisitos para configuração VPN IPSEC .....	190
21.1.1	<i>Verificações e requisitos VPN IPSEC Túnel</i> .....	190
21.1.2	<i>Verificações e requisitos VPN IPSEC RAS</i> .....	191
21.1.3	<i>Recomendações e requisitos Gerais da VPN</i> .....	192
21.2	Configurando Túnel VPN IPSEC .....	193
21.3	Túnel VPN IPSEC FailOver .....	195
21.3.1	<i>VPN totalmente redundante</i> .....	195
21.3.2	<i>Funcionamento da VPN FailOver</i> .....	197
21.3.3	<i>VPN parcialmente redundante</i> .....	198
21.3.4	<i>Requisitos para a VPN FailOver</i> .....	199
21.4	Habilitando o túnel VPN IPSEC FailOver .....	200
21.5	Configurando Acesso Remoto – VPN RAS .....	203
21.6	Monitor VPN .....	207
<b>22</b>	<b>VPN SSL</b>	<b>208</b>
22.1	Lista de aplicações no acesso VPN SSL .....	209
22.2	Requisitos da VPN SSL .....	210
22.2.1	<i>Requisitos BLOCKBIT UTM - VPN SSL</i> .....	210
22.2.2	<i>Requisitos nos dispositivos remotos – VPN SSL</i> .....	211
22.3	Configurando VPN SSL .....	212
22.3.1	<i>Exemplo – Acesso web Tunnel para aplicações do tipo Cliente/ Servidor</i> . .....	213
22.3.2	<i>Exemplo – Acesso remoto – RDP (Remote Desktop)</i> . .....	214
22.3.3	<i>Exemplo – Acesso remoto – VNC (Remote Desktop)</i> . .....	214
22.3.4	<i>Exemplo – Acesso remoto – SSH (Secure Shell Remote Desktop)</i> . .....	215
22.3.5	<i>Exemplo – Acesso aplicação Web (Http/Https)</i> .....	215

22.3.6	<i>Exemplo – Acesso a serviços de compartilhamento SMB.</i>	216
22.4	Adicionando um Túnel (Aplicativo Cliente/ Servidor).	217
22.4.1	<i>Adicionando um acesso RDP.</i>	218
22.4.2	<i>Adicionando um acesso VNC.</i>	219
22.4.3	<i>Adicionando um acesso SSH.</i>	220
22.4.4	<i>Adicionando uma Aplicação Web</i>	221
22.4.5	<i>Adicionando um Compartilhamento SMB (samba).</i>	222
22.4.6	<i>Gerenciando e Definindo Permissões.</i>	223
22.5	Estabelecendo Acesso VPN SSL	224
<b>23</b>	<b>ENTENDENDO AS POLÍTICAS DE COMPLIANCE</b>	<b>227</b>
23.1	Básico de Políticas de Compliance	228
<b>24</b>	<b>POLÍTICAS DE COMPLIANCE</b>	<b>231</b>
24.1	Políticas Padrões	231
24.1.1	<i>Política 1 – Controle de Ameaças</i>	233
24.1.2	<i>Política 2 – Filtro de Conteúdo</i>	233
24.1.3	<i>Política 3 – SSL ByPass</i>	234
24.1.4	<i>Política 4 – Segurança Ética</i>	234
24.1.5	<i>Política 5 – Perda de Produtividade</i>	235
24.1.6	<i>Política 6 – Risco de Segurança</i>	235
24.1.7	<i>Política 7 – Skype</i>	236
24.1.8	<i>Política 8 – Whatsapp</i>	236
24.1.9	<i>Política 9 – Webex</i>	236
24.2	Interface de Políticas de Compliance	237
24.3	Origem	238
24.3.1	<i>Zona de Rede</i>	238
24.3.2	<i>Device</i>	239
24.3.3	<i>Endereço IP</i>	239
24.3.4	<i>Endereço MAC</i>	239
24.3.5	<i>Autenticado</i>	239
24.3.6	<i>Usuário</i>	240
24.3.7	<i>Grupo</i>	240
24.4	Destino	241
24.4.1	<i>Endereço IP</i>	241
24.4.2	<i>Serviços</i>	241
24.4.3	<i>Serviços WEB</i>	242
24.4.4	<i>Interceptar SSL</i>	242
24.5	Conteúdo	243
24.5.1	<i>Categorias</i>	243
24.5.2	<i>Aplicativos</i>	244
24.6	Roteamento	245
24.6.1	<i>Ação</i>	245
24.6.2	<i>Horário</i>	245
24.6.3	<i>Período</i>	245
24.6.4	<i>Multilink</i>	246

24.6.5	<i>NAT</i> .....	246
24.6.6	<i>Proxy Explícito</i> .....	246
24.7	Controle .....	247
24.7.1	<i>Controle de Banda</i> .....	247
24.7.2	<i>Filtrar por Tipo de Conteúdo</i> .....	248
24.7.3	<i>Filtrar Cabeçalho HTTP</i> .....	248
24.7.4	<i>Cota de Tempo</i> .....	248
24.7.5	<i>Cota de Tráfego</i> .....	249
24.7.6	<i>Tamanho Máximo de Download</i> .....	249
24.7.7	<i>Tamanho Máximo de Upload</i> .....	249
24.8	Avançado .....	250
24.8.1	<i>TTL</i> .....	250
24.8.2	<i>Tipo de Pacote</i> .....	250
24.8.3	<i>Conteúdo do Pacote</i> .....	251
24.8.4	<i>TOS</i> .....	251
24.8.5	<i>DSCP</i> .....	251
24.9	Geral.....	252
24.10	Observações Importantes.....	253
24.11	Exemplo 1 – Política de Navegação .....	254
24.11.1	<i>Origem</i> .....	254
24.11.2	<i>Destino</i> .....	255
24.11.3	<i>Roteamento</i> .....	255
24.11.4	<i>Controles</i> .....	256
24.11.5	<i>Geral</i> .....	256
24.12	Exemplo 2 – Política de Filtro WEB - bloqueando categorias .....	257
24.12.1	<i>Origem</i> .....	258
24.12.2	<i>Destino</i> .....	258
24.12.3	<i>Conteúdo</i> .....	259
24.12.4	<i>Roteamento</i> .....	260
24.12.5	<i>Geral</i> .....	260
24.13	Exemplo 3 – Política de Filtro WEB - bloqueando aplicativos WEB 2.0 .....	261
24.13.1	<i>Origem</i> .....	262
24.13.2	<i>Destino</i> .....	262
24.13.3	<i>Conteúdo</i> .....	263
24.13.4	<i>Roteamento</i> .....	264
24.13.5	<i>Geral</i> .....	264
24.14	Exemplo 4 – Política de NAT .....	265
24.14.1	<i>Origem</i> .....	266
24.14.2	<i>Destino</i> .....	267
24.14.3	<i>Roteamento</i> .....	267
24.14.4	<i>Geral</i> .....	268
<b>25</b>	<b>MONITOR</b>	<b>269</b>
25.1	Tráfego Geral .....	270
25.2	Tráfego WEB .....	271

<b>26</b>	<b>RELATÓRIOS</b>	<b>272</b>
26.1	Serviços.....	273
26.2	Políticas.....	273
26.3	Web Filter .....	274
26.4	Advanced Threat Protection.....	274
26.5	Aplicativos WEB / ATP .....	275
26.6	IPS – Intrusion Prevention System.....	275
26.7	Relatórios Tráfego Geral.....	278
26.7.1	<i>Estatísticas do Servidor e Desempenho.</i> .....	278
26.7.2	<i>Tempo Real e Histórico.</i> .....	278
26.8	Relatórios Tráfego Web.....	279
26.9	Relatórios Ameaças e Aplicações .....	285
26.10	Relatórios Intrusion Prevention System.....	293
<b>27</b>	<b>INTERFACE BLOCKBIT CLI (LINHA DE COMANDOS)</b>	<b>301</b>
27.1	[arp] .....	302
27.2	[arping] .....	303
27.3	[authsync] .....	304
27.4	[enable-bgp] .....	304
27.5	configure-bgp] .....	305
27.6	[disable-bgp].....	305
27.7	[enable-ospf] .....	306
27.8	[configure-ospf] .....	306
27.9	[disable-ospf] .....	307
27.10	[enable-rip] .....	307
27.11	[configure-rip].....	307
27.12	[disable-rip].....	308
27.13	[date] .....	308
27.14	[debug-auth].....	309
27.15	[debug-dhcp] .....	310
27.16	[debug-firewall] .....	310
27.17	[debug-threats].....	311
27.18	[debug-vpn] .....	311
27.19	[debug-web] .....	311
27.20	[dig] .....	312
27.21	[ethtool].....	313

27.22 [fdisk] .....	314
27.23 [fsck].....	315
27.24 [fwrecovery].....	316
27.25 [fwreload] .....	316
27.26 [help].....	317
27.27 [host].....	317
27.28 [Hostname] .....	318
27.29 [ifconfig].....	319
27.30 [ifstat].....	321
27.31 [iotest].....	322
27.32 [ipcalc].....	322
27.33 [iplist] .....	323
27.34 [iptraf] .....	323
27.35 [less] .....	324
27.36 [lscpu].....	325
27.37 [lsusb].....	325
27.38 [mkfs] .....	326
27.39 [more] .....	327
27.40 [mtr] .....	327
27.41 [netads].....	329
27.42 [nslookup] .....	330
27.43 [ntpdate] .....	330
27.44 [parted] .....	331
27.45 [passwd].....	332
27.46 [ping] .....	332
27.47 [reboot] .....	333
27.48 [reset-admin-blocks].....	333
27.49 [reset-admin-password].....	333
27.50 [reset-admin-sessions].....	334
27.51 [route] .....	334
27.52 [service-start].....	335
27.53 [service-stop] .....	336
27.54 [service-status].....	336
27.55 [show-auth-sessions] .....	337
27.56 [show-uuid] .....	337

27.57 [show-vpn-info] .....	338
27.58 [show-vpn-conn].....	339
27.59 [speedtest].....	339
27.60 [tcpdump] .....	340
27.61 [tcptop] .....	341
27.62 [tcptrack] .....	341
27.63 [telnet].....	342
27.64 [tracepath].....	343
27.65 [traceroute] .....	344
27.66 [update-blockbit] .....	347
27.67 [update-license].....	347
27.68 [rewizard].....	348
27.69 [shutdown] .....	348
27.70 [exit].....	348



## 1 Preparação

---

Antes de prosseguir a leitura deste manual, certifique-se de ler e seguir o **Guia Rápido de Instalação** do BLOCKBIT UTM que explica detalhadamente o procedimento inicial de configuração.

Agora que você está pronto e com acesso a interface web, leia com atenção o manual para configurar o seu BLOCKBIT UTM conforme suas necessidades.

Caso tenha dúvidas ou necessite suporte, consulte sua revenda local ou nossos canais de comunicação direta, nas primeiras páginas deste manual, teremos o maior prazer em atende-lo.

## 1.1 Recomendações

O administrador deve antes definir parâmetros iniciais, ou seja, políticas de segurança a serem aplicadas na rede.

Antes de definir as políticas iniciais para aplicar o FIREWALL, vamos levantar algumas informações:

É Importante que o administrador possua o layout “ESTRUTURA” da rede.

### 1.1.1 Perguntas Fundamentais para Elaboração da Política de Segurança

Quais serviços serão liberados para usuários?

Quais servidores precisam acesso à internet?

Quais servidores disponibilizam serviços na internet?

Como serão organizados os controles de acesso, por função, por departamento ou por usuário?

Quem necessita acesso a relatórios de segurança?

Com base nestas informações podemos definir uma política inicial para implementação do FIREWALL.

---

## 1.2 Requisitos

Para acesso a interface gráfica, é necessário a utilização de um navegador web recomendado:

### Navegadores web:

- Mozilla Firefox versão 45
- Google Chrome versão 51
- Microsoft Internet Explorer 9

## 2 Acessando a Interface Web

Para acessar a interface web, utilize um navegador recomendado (Ver [Seção 1.2 – Requisitos](#)).

**ATENÇÃO:** Neste manual utilizaremos o IP 192.168.1.1, que é o padrão do BLOCKBIT UTM, caso tenha configurado outro IP no procedimento do Guia Rápido de Instalação utilize-o no lugar.

Acesse: <https://192.168.1.1:98>



**Login:** admin

**Senha:** sua\_senha

**Idioma:** Selecione o idioma desejado para visualização da interface.

## 2.1 Entendendo a Interface Web

O BLOCKBIT UTM é administrado por uma interface Web moderna, ágil e responsiva, o que permite seu uso no desktop, tablet ou celular.

### 2.1.1 Menu de Opções

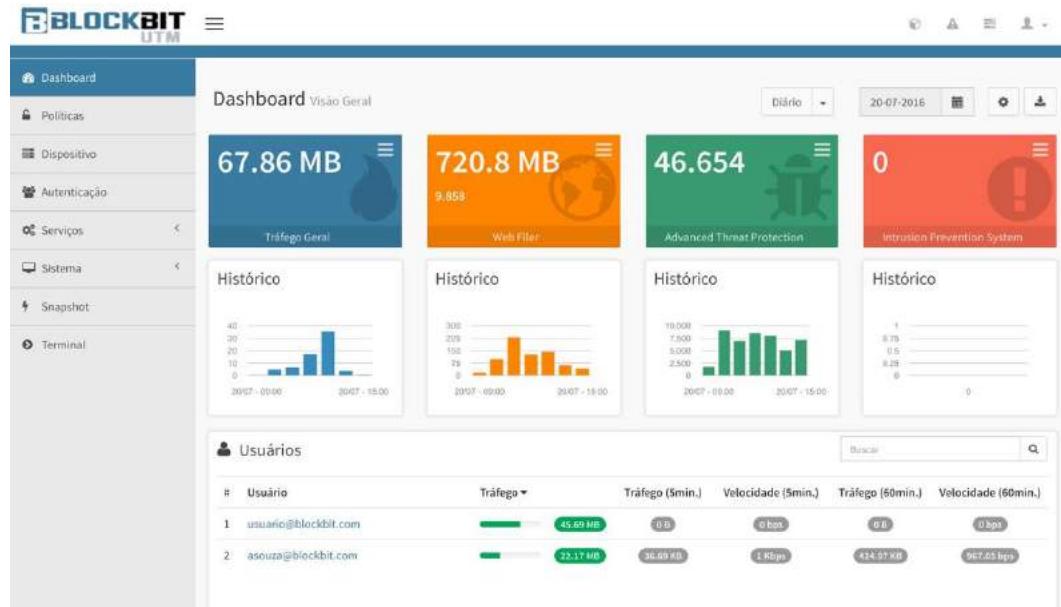
No lado esquerdo da interface há o menu de opções que dá acesso a todas as funções do BLOCKBIT UTM com até dois níveis de opções, caso esteja utilizando em tela de largura reduzida, o menu ficará oculto, mas acessível através de ícone 

#### Botões de ação

No canto superior direito da interface temos um grupo de ícones de ações importantes para o administrador:

				<b>Gerenciador de Objetos</b>
				Atalho para facilitar a configuração de objetos, como máquinas, redes, serviço e outros podendo ser utilizado sobre funções e formulários diversos. O gerenciamento completo de objetos pode ser acessado em: <b>&gt;&gt; SISTEMA &gt;&gt; Objetos</b>
				<b>Notificações</b>
				Mensagens e alertas em tempo real que informam o Administrador das ocorrências do sistema.
				<b>Fila de comandos</b>
				As configurações aplicadas no BLOCKBIT UTM ficam enfileiradas para que sejam aplicadas de uma única vez reduzindo o impacto em disponibilidade.
				<b>Perfil</b>
				Exibe o perfil do usuário.

### 3 Dashboard



O Dashboard é um painel que reúne as informações coletadas dos módulos de segurança e são exibidas de forma sumarizada por usuário, grupo, serviço e ameaças permitindo uma rápida visão, gestão e tomadas de decisão.

Através do Dashboard o administrador consegue entender rapidamente o que está acontecendo na rede sem gastar tempo em milhares de linhas de log.

O recurso Timeline, que mostra uma linha do tempo por usuário, onde pode ser analisado o seu comportamento, risco e impacto no uso de banda.

### **3.1 Recursos do Dashboard**

Acesso centralizado e consistente a todos os logs summarizados e eventos do sistema.

- Geração de relatórios summarizados.
  - Estatísticas do Servidor
  - Acesso Web (Tráfego).
  - Ameaças e Aplicações.
  - Intrusion detection.
- Geração de relatórios detalhados de até 7 (sete) dias.
- Alertas e notificações em tempo real e que podem ser disparados através de agendamento.

## 4 Configurando o BLOCKBIT UTM

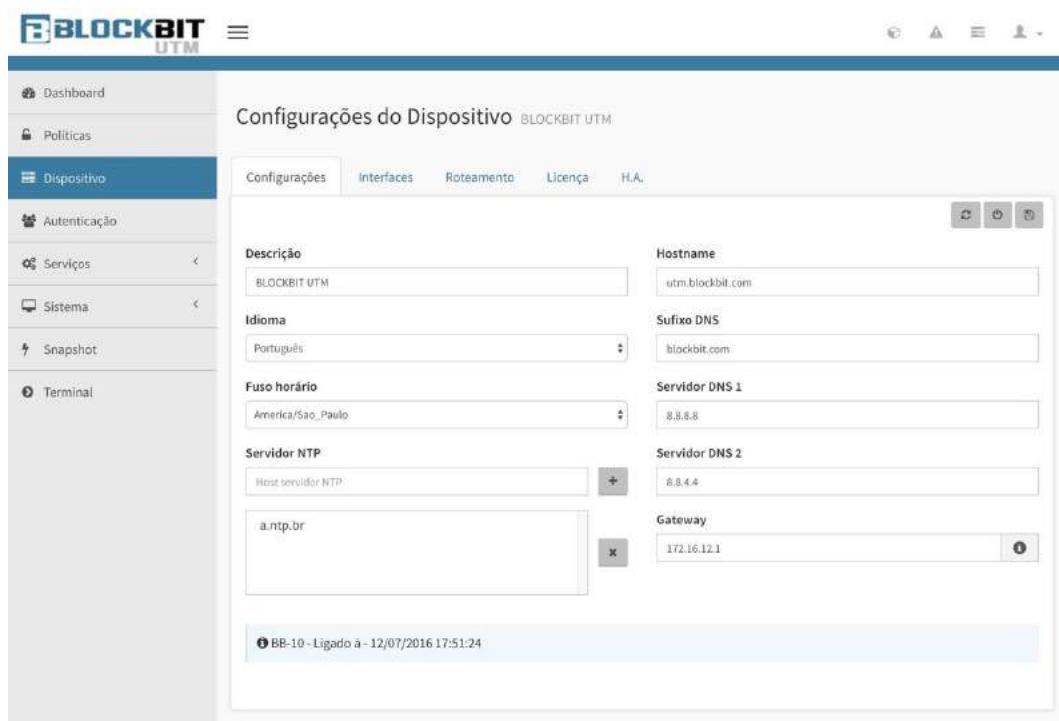
Este capítulo detalha as configurações iniciais do BLOCKBIT UTM, que devem ser seguidas para o seu correto funcionamento.

Antes de prosseguir a leitura deste manual, certifique-se de ler e seguir o **Guia Rápido de Instalação** do BLOCKBIT UTM que explica detalhadamente o procedimento inicial de configuração.

### 4.1 Configurações Básicas

Selecione o Menu **[Dispositivo]** para configuração.

Na aba **[Configurações]** o administrador pode alterar as configurações básicas, mas de grande importância que foram definidas no Wizard.



Na parte superior direita do formulário você encontra 3 ícones:



Atualizar informações de hardware



Reiniciar / Desligar



Salvar configurações

## 4.2 Configurando Interfaces de Rede

Na aba **[Interfaces]** podemos configurar e adicionar interfaces físicas e virtuais.

- Ethernet
- ADSL
- VLAN
- VIRTUAL

As interfaces “Ethernet” são identificadas automaticamente pelo sistema.

### 4.2.1 Configurando uma interface física

Para configurar uma interface física, clique na aba **[Interfaces]**, e edite a interface correspondente e configure de acordo com os campos e clique em **[Salvar]**.

Status	Interface	Endereço	Gateway	Tipo	Zona	Ação
Ativo	eth0	192.168.1.1/24	-	Física	LAN	
Ativo	eth1	Dinâmico	-	Física	WAN	
Ativo	eth2	-	-	Física	-	
Ativo	eth3	-	-	Física	-	

**IMPORTANTE:** Atualize as informações de hardware do servidor. Na Aba [Configurações] clique em **[ ]**

**Editar interface física**

<b>Nome</b>	eth0
<b>Descrição</b>	Local Network
<b>Zona de Rede</b>	LAN
<b>Endereço IP</b>	192.168.1.1
<b>Máscara</b>	255.255.255.0
<b>Gateway</b>	
<input type="checkbox"/> IP Dinâmico	<span style="color: blue;">i</span>
<span style="background-color: #0072BC; color: white; padding: 5px 10px; border-radius: 5px;">Salvar</span>	

Após salvar as configurações retorna a interface a seguir. Clique [  ] para habilitar [  ] a interface.

Configurações	Interfaces	Roteamento	Licença	H.A.																																			
<table border="1"> <thead> <tr> <th>Status</th> <th>Interface</th> <th>Endereço</th> <th>Gateway</th> <th>Tipo</th> <th>Zona</th> <th>Ação</th> </tr> </thead> <tbody> <tr> <td></td> <td> eth0</td> <td>192.168.1.1/24</td> <td>-</td> <td>Física</td> <td>LAN</td> <td> </td> </tr> <tr> <td></td> <td> eth1</td> <td>Dinâmico</td> <td>-</td> <td>Física</td> <td>WAN</td> <td> </td> </tr> <tr> <td></td> <td> eth2</td> <td>-</td> <td>-</td> <td>Física</td> <td>-</td> <td> </td> </tr> <tr> <td></td> <td> eth3</td> <td>-</td> <td>-</td> <td>Física</td> <td>-</td> <td> </td> </tr> </tbody> </table>					Status	Interface	Endereço	Gateway	Tipo	Zona	Ação		 eth0	192.168.1.1/24	-	Física	LAN	 		 eth1	Dinâmico	-	Física	WAN	 		 eth2	-	-	Física	-	 		 eth3	-	-	Física	-	 
Status	Interface	Endereço	Gateway	Tipo	Zona	Ação																																	
	 eth0	192.168.1.1/24	-	Física	LAN	 																																	
	 eth1	Dinâmico	-	Física	WAN	 																																	
	 eth2	-	-	Física	-	 																																	
	 eth3	-	-	Física	-	 																																	

#### 4.2.2 Adicionando uma interface virtual

Esta seção aborda a configuração de interfaces virtuais.

O BLOCKBIT UTM suporta adicionar interfaces do tipo “DSL”, “VLAN” e “Virtual”, e requer obrigatoriamente uma interface física [EthX] livre.

Para configurar uma interface, clique para **adicionar** []. Vamos exemplificar adicionando uma interface do tipo “Virtual”. Configure-o de acordo com os campos e clique em [].

Cadastro de interface

**VIRTUAL**

DSL	Interface	eth1
VLAN	Nome	eth1v0
VIRTUAL	Descrição	Interface Virtual Eth1:1 Link WAN Primária
	Zona de Rede	WAN
	Endereço IP	172.16.102.44
	Máscara	255.255.255.0
	Gateway	
	Endereço Mac	Opcional

**IMPORTANTE:** A configuração do campo **[Gateway]** é opcional. No entanto, é requerido para habilitação da respectiva interface pelo serviço **[Multilink]**. A identificação do campo gateway é utilizada pelo Multilink para definição da rota default para a respectiva interface.

Após salvar as configurações retorna a interface a seguir.

The screenshot shows the 'Configurações do Dispositivo' (Device Configuration) screen in the BLOCKBIT UTM web interface. The left sidebar has 'Dispositivo' selected, and the main content area shows the 'Interfaces' tab of the configuration table. The table lists network interfaces with the following data:

Status	Interface	Endereço	Gateway	Tipo	Zona	Ação
Ativo	eth0	192.168.1.1/24	-	Física	LAN	
Ativo	eth1	Dinâmico	-	Física	WAN	
Ativo	eth1v0	172.16.102.44/24	-	Virtual	WAN	
Ativo	eth2	-	-	Física	-	
Ativo	eth3	-	-	Física	-	

A note at the bottom of the interface says: **NOTA: Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:** (Note: Don't forget to apply the command queue, click on the icon). The icon is a small red square with the number '1' in white.

## 4.3 Link Aggregation

Nesta seção vamos abordar a agregação de link, este recurso combina múltiplas interfaces físicas em única interface lógica, que chamamos de “*LAG – (Link Aggregation Group)*” e tem por uma das principais finalidades aumentar a largura de banda do tráfego da rede para o total da largura de banda das interfaces físicas agregadas, proporcionando maior largura de banda bem como redundância de link, no caso de um dos links falhar, mantendo automaticamente o tráfego para a(s) outra(s) interface(s) do LAG.

Baseado no protocolo LACP – Link Aggregation Control Protocol, um protocolo de negociação de camada 2, que fornece métodos para controlar a agregação de várias portas físicas em um único grupo lógico. O LACP permite que um dispositivo de rede possa negociar um agrupamento automático de links enviando os pacotes LACP para outro dispositivo diretamente conectado que também implemente o LACP).

O BLOCKBIT UTM disponibiliza esse recurso em 3 (três) modos de operação:

### Modo Aggregation

Onde o tráfego é distribuído uniformemente sobre as interfaces físicas do grupo de links agregados, dessa forma somando a largura de banda das interfaces de rede no grupo e aumentando a confiabilidade da conexão.

**IMPORTANTE:** O LAG habilitado no modo “*Aggregation*” requer que os switches da rede contemplem suporte ao protocolo “*LACP – Link Aggregation Control Protocol (802.3ad)*”, e estejam devidamente configurados.

### Modo Balance

Onde o tráfego é distribuído na ordem sequencial da primeira interface do grupo para a última, basicamente o serviço distribui a carga, ou seja, os pacotes, alternadamente entre as interfaces LAG. Para uma mesma conexão os pacotes são enviados ora para a interface 1, ora para a interface 2 e assim sucessivamente da primeira interface até a última.

É o único modo que envia os pacotes da mesma conexão TCP/IP através de múltiplas interfaces.

**NOTA:** Ao utilizar múltiplos envios e várias conexões de entrada os pacotes podem muitas vezes ser recebidos fora de ordem e resultar em retransmissão.

### Modo Active / Backup

Neste modo o tráfego é enviado por uma única interface, o sistema habilita apenas uma interface como “Ativa” para o tráfego dos pacotes . As interfaces de rede adicionais trabalham no modo “Espera”, só se tornam ativas se a interface principal falhar.

O modo Active / backup é a melhor opção para configuração exclusiva para “*Alta disponibilidade*” com múltiplos switches interligados.

**NOTA:** Para todos os modos de operação o LAG suporta o serviço de redundância. Se um dos links na interface agregada se tornar indisponível, o tráfego continuará a fluir sobre a(s) interfaces disponíveis no grupo.

#### 4.3.1 Configurações

Para configurar o serviço de agregação de links, vamos criar um grupo de agregação, “*LAG - Link Aggregation Group*”, e definir quais links “*interfaces*” serão membros do grupo.

**NOTA:** Para configurar uma interface “*LAG*” as interfaces precisam estar “*desabilitadas*”.

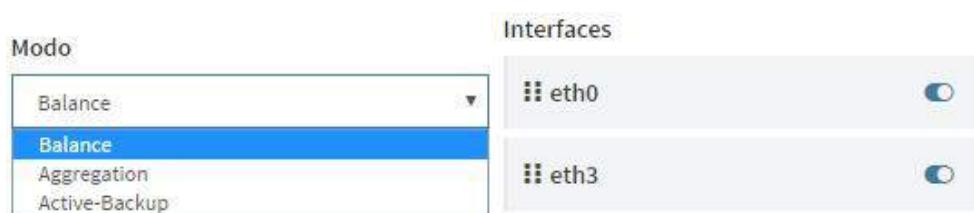
Clique na aba **[Interfaces]**, no lado direito clique no botão **Ações** [▼] e selecione a opção **[Aregar]**.

The dialog box has the title 'Link Aggregation Group'. It contains the following fields:

Nome	lag0	Zona de Rede	
Descrição		Endereço IP	
Modo	Balance	Máscara	255.255.255.0
Interfaces	eth0	Gateway	
	eth3	IP Dinâmico	<input type="checkbox"/>

At the bottom right is a blue 'Salvar' (Save) button.

Configure a interface do tipo LAG, selecionando o modo de agregação e as interfaces correspondentes que pretende agrupar, configure os demais campos de acordo suas definições, depois clique em [ ].



**Link Aggregation Group**

Nome	Zona de Rede
lag0	LAN
Descrição	Endereço IP
LAG Interface Rede Local	192.168.1.126
Modo	Máscara
Balance	255.255.255.0
Interfaces	Gateway
eth0	
eth3	
	<input type="checkbox"/> IP Dinâmico
<b>Salvar</b>	

**Configurações do Dispositivo** Server UTM 1.1

Configurações	Interfaces	Roteamento	Licença	H.A.		
+ / -						
Status	Interface	Endereço	Gateway	Tipo	Zona	Ação
	eth1	192.168.0.250/24	192.168.0.1	Física	WAN	
	lag0	192.168.1.126/24	-	Aggregation	LAN	

**NOTA:** Não se esqueça de APPLICAR A FILA DE COMANDOS, clique no ícone:



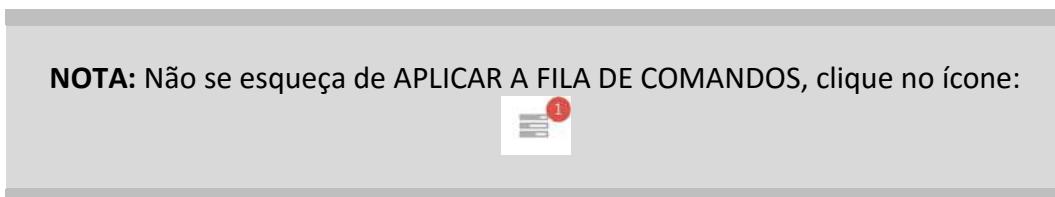
#### 4.3.2 Alterando a prioridade das interfaces LAG

É possível alterar a prioridade das interfaces de rede LAG. Importante frisar que a interface de maior prioridade responde como link principal e as demais como interfaces secundárias.

No modo Active / backup a ordem de prioridade indica qual interface responde como principal (interface Ativa) e quais interfaces respondem como secundárias (Espera), ou seja, interfaces failover.



Através da seleção da interface de rede. *Clique e arraste pelo símbolo [ ]* até a posição desejada de ordenação. Depois em clique em [ ].



## 4.4 Configurando Rotas

Na aba [Roteamento] podemos adicionar rotas estáticas entre as interfaces de rede com a finalidade de alcançar uma rede/ sub rede específica.

Para adicionar uma rota, clique em **adicionar** []. Depois clique em []. Configure de acordo com as especificações e os campos para definição do roteamento.

**Adicionar Rota**

**Descrição**  
Laboratório

**Interface**  
eth0

**IP/Rede de destino**  
192.168.10.0/24

**Gateway de destino**  
192.168.1.100/32

**Salvar**

**Configurações do Dispositivo** BLOCKBIT UTM

Status	Descrição	Interface	Endereço de destino	Gateway de destino	Ação
Ativo	Laboratório	eth0	192.168.10.0/24	192.168.1.100/32	

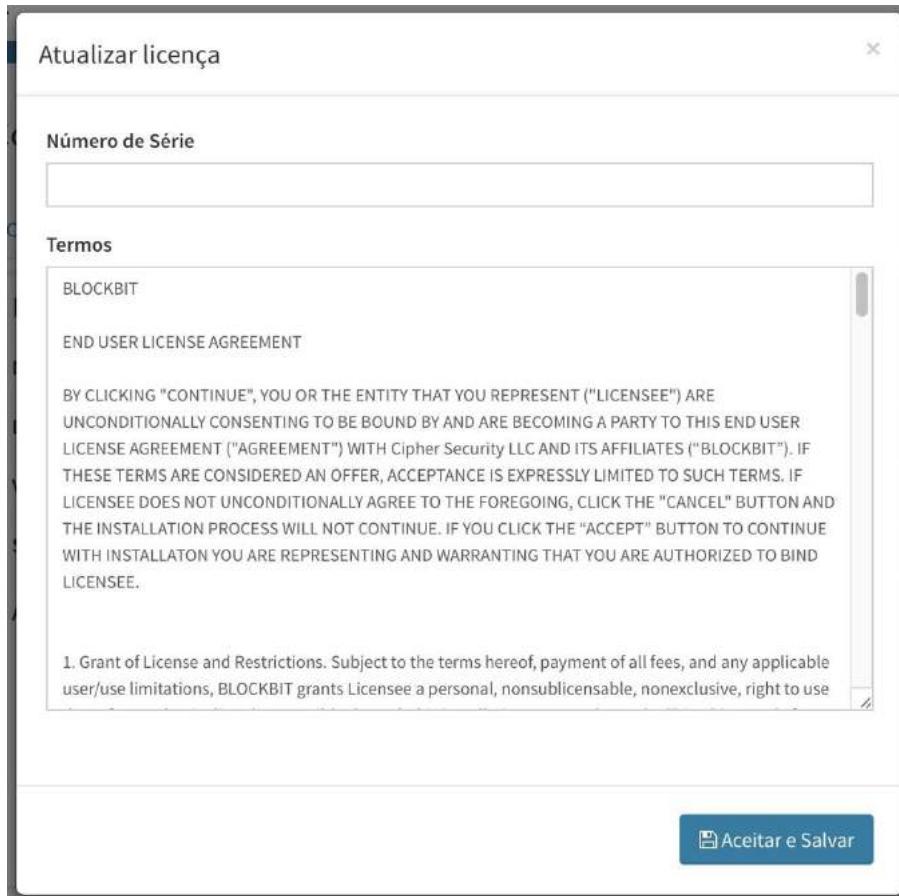
**NOTA:** Não se esqueça de APPLICAR A FILA DE COMANDOS, clique no ícone:



## 4.5 Licenciamento

Na aba [Licença] insira a chave de licenciamento fornecida. Lembre-se, você deve ter conexão à Internet para que o sistema possa validar a licença.

Clique em [  ], entre com os dados da licença e clique em [  Aceitar e Salvar ].



Após salvar a chave de licenciamento o servidor retorna à interface a seguir, ainda com a licença INATIVA.

**Dados da Licença**

- Número de série: 417F-1ABC-0BB7-F8CF
- Data do registro: -
- Validade da licença: -
- Status da licença: Inativa
- Atualização do servidor: 17:45

Subscription	Data inicial	Data final
Intrusion Prevention	2016-07-11	2016-08-31
Threat Protection	2016-07-11	2016-08-31
VPN SSL	2016-07-11	2016-08-31
Web Gateway Security	2016-07-11	2016-08-31

Para finalizar o processo requer **APLICAR** as configurações.

**NOTA:** Não se esqueça de **APLICAR A FILA DE COMANDOS**, clique no ícone:



Abaixo a Interface com os dados da licença já atualizados e com status da licença **ATIVA**.

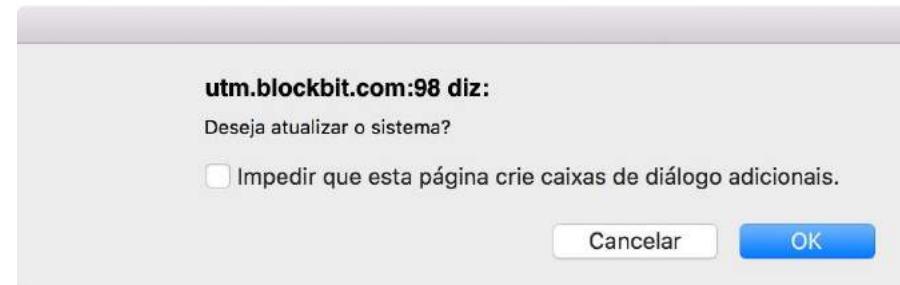
**Dados da Licença**

- Número de série: 417F-1ABC-0BB7-F8CF
- Data do registro: 2016/07/11
- Validade da licença: 2016/08/31
- Status da licença: Ativa
- Atualização do servidor: 17:45

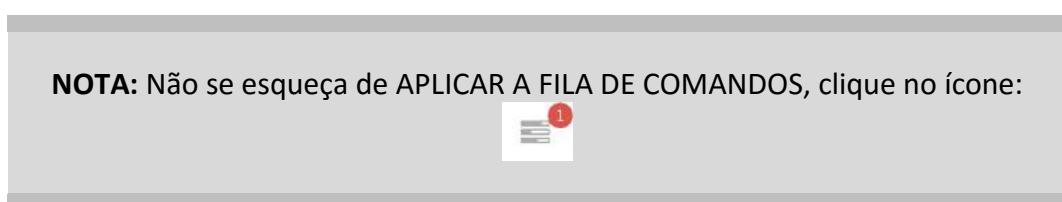
Subscription	Data inicial	Data final
Intrusion Prevention	2016-07-11	2016-08-31
Threat Protection	2016-07-11	2016-08-31
VPN SSL	2016-07-11	2016-08-31
Web Gateway Security	2016-07-11	2016-08-31

Após o registro do servidor é recomendável proceder com a atualização do sistema.

Para atualizar o servidor clique em [  ] e confirme.



Clique em **[OK]** para confirmar a atualização do servidor.



## 5 Administração do Sistema

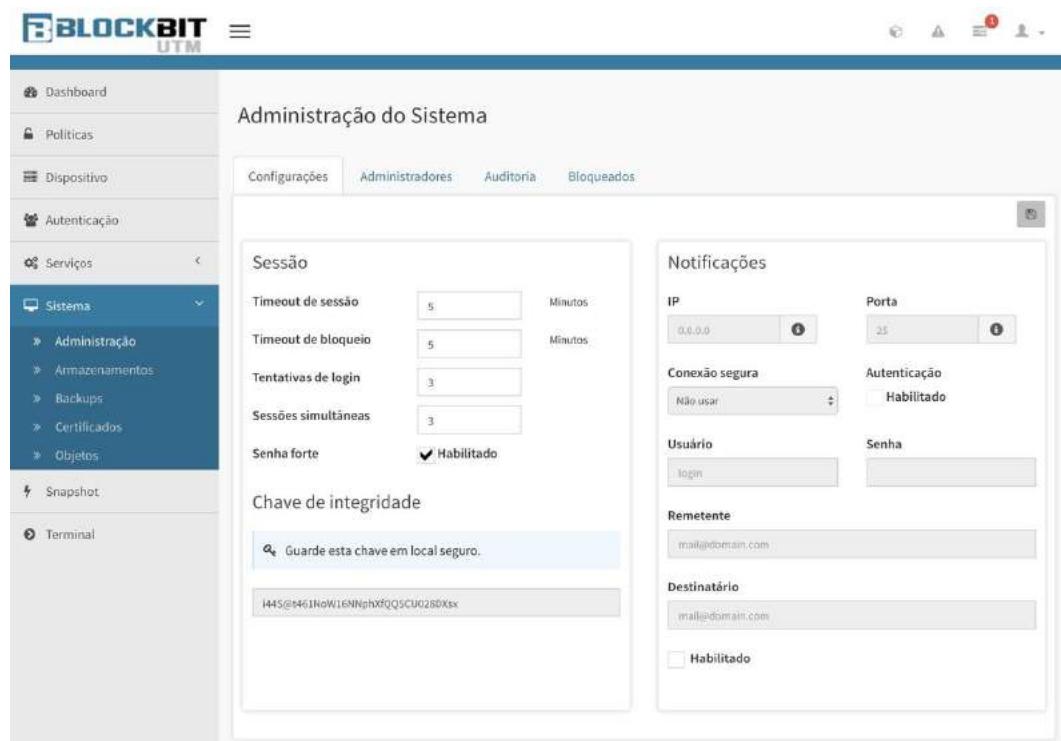
Para definir e configurar estes recursos acesse **[Sistema] >> [Administração]**.

O item Sistema Administração nos permite gerenciar o acesso à interface de administração WEB, definir e aplicar as configurações gerais, a gerencia no cadastro e permissões dos administradores do sistema, auditar os acessos e as configurações aplicadas, e ainda gerenciar os bloqueios por tentativas de acessos não autorizados.

### 5.1 Configurações

Este item nos permite definir as configurações de segurança em relação à interface de administração do sistema.

Na aba **[Configurações]** no quadro **[Sessão]** configure os campos de acordo com a política que pretende adotar.



**IMPORTANTE**

**INTEGRITY KEY:** Chave integridade do sistema, utilizada no processo de criptografia dos arquivos de backups, e do carimbo de integridade dos relatórios.

**Guarde-a em um local seguro!**

É importante saber que em casos de reinstalação o usuário precisa configurar este campo com o mesmo valor (chave) utilizada na instalação anterior.

O processo de restore de configurações e validação da chave de integridade da base de relatórios, dependem desta chave, a fim de ser mantida a integridade dos relatórios e obter sucesso no restore das configurações da base anterior.

No quadro **[Notificações]** você pode configurar o sistema para o envio de notificações por e-mail para um administrador exclusivo, determinado pelo endereço de e-mail do destinatário. Estas notificações são as mesmas devolvidas em tempo real, alertadas através do menu superior direito pelo ícone [  ]. Você pode configurar o sistema para usar um servidor de e-mail “local” ou “remoto”. Se pretende receber as notificações por e-mail, configure o serviço e clique em **Salvar** [  ].

## 5.2 Administradores

Este item permite você gerenciar o cadastro e permissões sobre os administradores do sistema. Por padrão o sistema já contempla o administrador “admin”, sua senha é definida no “*Wizard de configuração*”.

Na aba [Administradores] você visualiza todos os administradores cadastrados com as opções de “*Pesquisar*”, “*Editar*” ou “*Remover*” um administrador de sistema. Temos dois níveis de administradores do sistema:

**Super administrador:** Têm o privilégio total sobre a interface inclusive de gerenciar qualquer nível de administrador. Sem a necessidade de definir permissões.

**Administrador comum:** Direitos restritos sobre a administração exigem-se definir permissões sobre as funcionalidades que pode visualizar configurar e administrar.

Para adicionar um administrador do sistema, clique em [+], a interface de cadastro é dividida em 2 (duas) abas [**Informações**] e [**Interfaces**], configure a aba “*Informações*”, defina o tipo de administrador, caso opte em [V] **Super Administrador**, a aba “*Interfaces*” é ocultada, caso contrário, defina as permissões sobre as interfaces que o “*Administrator Comum*” terá direitos. Depois clique em [Salvar].

### Adicionar Administrador

Informações

Interfaces

Login  
suporte

Senha  
.....

Confirmação de senha  
.....

Nome  
Suporte

Email  
suporte@blockbit.com

Super administrador



### Adicionar Administrador

Informações

Interfaces

Acesso	Permissões
Autenticação	★
Dashboard	★
Dashboard > IPS	★
Dashboard > IPS	★
Dashboard > Produtividade	★
Dashboard > Relatórios	★
Dashboard > Timeline	★
Dashboard > Tráfego	★
Dashboard > Web	★
Dispositivos > Configurações do dispositivo	★

 Desabilitado    Visualizar    Editar



No exemplo temos:

The screenshot shows the BLOCKBIT UTM 1.1 administration interface. The left sidebar has a tree view with nodes like Dashboard, Políticas, Dispositivo, Autenticação, Serviços (expanded to show Sistema, Administração, Armazenamentos, Backups, Certificados, Objetos), Snapshot, and Terminal. The main area is titled "Administração do Sistema" and has tabs for Configurações, Administradores, Auditoria, and Bloqueados. The Administradores tab is active, showing a list with two entries: "admin" (Administradores, admin@blockbit.com, Online) and "suporte" (Suporte, suporte@blockbit.com, Offline). A search bar at the top right says "Buscar por login ou nome:".

## 5.3 Auditoria

Este recurso é muito importante, tem como finalidade principal proporcionar uma gestão de administração livre de dúvidas, nesta interface é possível “Auditar” todas as operações realizadas no sistema, desde “Visualização”, “Configuração de um serviço” e as “Definições” e ou “Alterações” de uma política de compliance realizada por qualquer um dos administradores do sistema, seja o “Super Administrador” ou “Administrador Comum”.

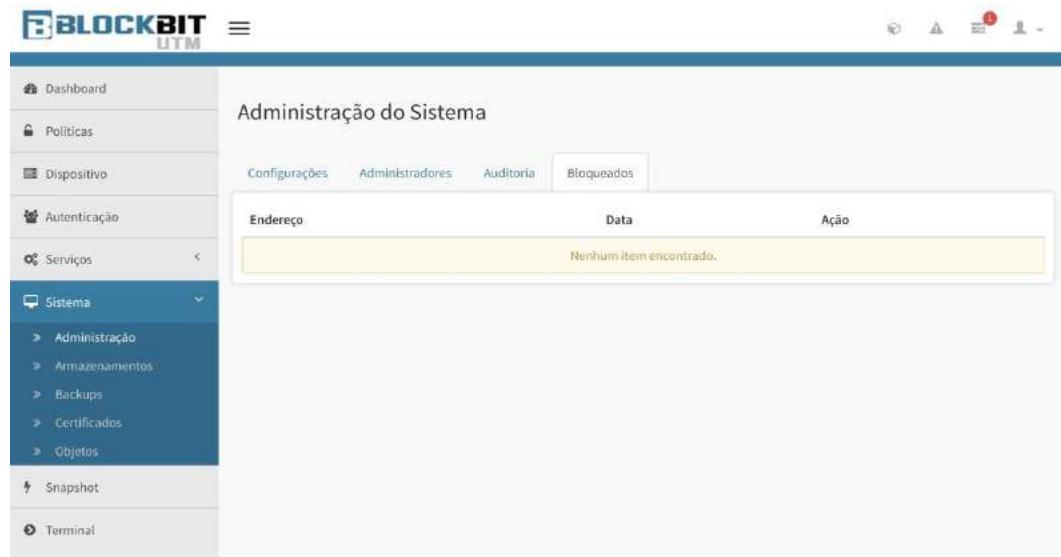
Clique na Aba **[Auditoria]** é possível aplicar filtros por: “Data inicial/final”, “Administradores”, “Interfaces” e ainda definir o limite que deseja exibir por página.

The screenshot shows the 'Audit' tab selected in the navigation bar. On the left, there is a sidebar with various menu items: Dashboard, Políticas, Dispositivo, Autenticação, Serviços (with 'Sistema' expanded), Administradores, Armazenamentos, Backups, Certificados, Objetos, Snapshot, and Terminal. The 'Sistema' item under 'Serviços' is currently selected. The main area is titled 'Administração do Sistema' and contains four tabs: Configurações, Administradores, Auditoria (which is active and highlighted in blue), and Bloqueados. Below these tabs, there are several filter options: Data inicial (set to 12-07-2016 00:00:00), Data final (set to 12-07-2016 23:59:59), Administradores (set to Todos), Interfaces (set to Todas), and Limite (set to 10 Itens). To the right, a table displays a list of audit logs with columns: Data, Descrição, Interface, and Ação. Each log entry includes a timestamp, a brief description of the action taken, the specific system or interface it affected, and two small buttons (minus and plus) for managing the log entry. There is also a search bar at the top of the log table.

Data	Descrição	Interface	Ação
12-07-2016 19:02:08	Administrador cadastrado	Sistema > Administração	- +
12-07-2016 18:28:32	Rota editada	Dispositivos > Configurações do dispositivo	- +
12-07-2016 18:27:19	Objeto de endereço IP auto cadastrado	Sistema > Objetos	- +
12-07-2016 18:27:19	Adicionada rota	Dispositivos > Configurações do dispositivo	- +
12-07-2016 18:27:18	Objeto de endereço IP auto cadastrado	Sistema > Objetos	- +
12-07-2016 18:20:00	Interface virtual adicionada	Dispositivos > Configurações do dispositivo	- +

## 5.4 Bloqueados

Na aba **[Bloqueados]** você visualiza a lista de IP/hosts bloqueados por tentativa de acesso não autorizado, e/ou tentativa de acesso persistente, com a possibilidade de remover a regra de bloqueio antes do timeout estabelecido nas configurações e políticas de acesso a interface de gerenciamento WEB.



Endereço	Data	Ação
		Nenhum item encontrado.

## 6 Armazenamentos

Nessa seção vamos expor os tipos de armazenamentos suportados pelo sistema e suas aplicações:

**SMB** – “*Server Message Block*” comumente utilizado em compartilhamento de pasta pelo Windows. Esse modelo de armazenamento é disponibilizado pelo sistema para acesso através do portal da VPN SSL.

**NFS** – “*Network File System*” comumente utilizado em compartilhamento de pastas em servidores UNIX. Esse modelo de armazenamento é disponibilizado pelo sistema para as aplicações de “Backup/ Restore”.

**Disco** – Dispositivo físico de armazenamento de dados. São suportados dispositivos do tipo (USB- HDD; USB- SSD). Esse modelo de “Storage” é disponibilizado pelo sistema para as aplicações de “Backup/ Restore”.

Acesse a interface de gerenciamento dos Armazenamentos, vá para **[Sistema] > [Armazenamentos]**.

The screenshot shows the BLOCKBIT UTM web interface. The left sidebar has a dark blue header with the BLOCKBIT logo and a light gray footer. The main menu is on the left, with 'Sistema' selected and 'Armazenamentos' highlighted under it. The main content area is titled 'Gerenciador de Armazenamentos' and contains a table with columns 'Descrição', 'Tipo', 'Tamanho', and 'Ação'. A message at the bottom of the table says 'Nenhum item encontrado.' (No items found).

## 6.1 Adicionando um Armazenamento SMB

Para adicionar um armazenamento SMB, clique em **[Sistema] > [Armazenamento]**, depois clique em **adicionar** []. Configure o formulário de acordo com as especificações para conexão com respectivo servidor SMB, depois clique em [].

Adicionar armazenamento SMB

SMB

NFS

Descrição: Documentos

Login: usuario

Senha: \*\*\*\*\*

IP: 192.168.254.10

Compartilhamento: docs

### Gerenciador de Armazenamentos

Armazenamentos				Ação
Descrição	Tipo	Tamanho	Ação	
Documentos	SMB	Armazenamento Indisponível	undefined%	

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 6.2 Adicionando um Armazenamento NFS

Para adicionar um armazenamento NFS, clique em **[Sistema] >> [Armazenamentos]**, depois clique em **adicionar** . Configure o formulário especificando os campos “*Descrição*”, “*IP*” e “*Diretório*” do servidor NFS para o armazenamento do recurso de backup/restore, depois clique em  **[Salvar]**.

**Adicionar armazenamento NFS**

SMB	<b>Descrição</b>
NFS	<input type="text" value="Backup"/>
IP	<input type="text" value="192.168.254.150"/> 
Diretório	<input type="text" value="/Backup"/>
Bytes leitura	<input type="text" value="4096"/>
Bytes escrita	<input type="text" value="4096"/>
Protocolo	<input type="checkbox"/> TCP <input type="text" value="Opcional"/> 
Porta	
Bytes tam bloco	<input type="text" value="4096"/>
Desabilitar locking	<input type="checkbox"/>
Modo de operação	<input checked="" type="radio"/> Hard <input type="radio"/> Soft <input type="checkbox"/> Habilitar posix
Opções extras	<input type="text" value="opt1=n,opt2=m"/>
 <b>Salvar</b>	

**NOTA:** O administrador não conhecendo detalhes da configuração do servidor NFS, pode manter os valores padrões de configuração da interface.

A configuração deste item pode ser definida com base nas configurações e especificações do servidor NFS.

## Gerenciador de Armazenamentos

Armazenamentos			
Descrição	Tipo	Tamanho	Ação
Backup	NFS	Armazenamento Indisponível	undefined%  
Documentos	SMB	Armazenamento Indisponível	undefined%  

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 6.3 Adicionando um Armazenamento Disco

Para identificar um dispositivo do tipo “Disco”, clique em **[Sistema] > [Armazenamentos]**, depois clique em **Atualizar** [  ] para reconhecimento do tipo de dispositivo, montagem e configuração da unidade de acesso de acordo com sua identificação.



**IMPORTANTE:** O sistema requer que os dispositivos do tipo “Disco” estejam formatados no sistema de arquivo tipo EXT4.

### Formatação do disco – padrão EXT4

Para Formatação do disco você pode acessar a console do BLOCKBIT UTM. Clique em **[Terminal]**

Para o acesso ao terminal, utilize o usuário admin e a senha personalizada.

Login: admin

Password: admin

```
utm login: admin
admin@utm.blockbit.com's password:
Last login: Wed Ago 31 09:13:26 2016 from utm
Welcome to BlockBit
Type '?' or 'help' to get the list of allowed commands

admin >
```

O acesso ao terminal é restrito, para listar os comandos disponíveis, digite: ?.

```
Type '?' or 'help' to get the list of allowed commands
admin >?
arp          disable-ospf  hostname  ntpdate      show-vpn-info
arping       disable-rip   ifconfig   parted       shutdown
authsync     enable-bgp   ifstat    passwd       speedtest
clear        enable-ospf  iostat    ping         sysctl
configure-bgp enable-rip   iotest    reboot      tcpdump
configure-hdmi enable-root  ip       reset       tcptop
configure-ospf enable-snmp  ipcalc   reset-admin-blocks  tcptrack
configure-rip ethtool     iplist   reset-admin-password telnet
conntrack    exit        iptraf   reset-admin-sessions tracepath
date         fdisk        less     rewizard   traceroute
debug-auth   free         lscpu   route       update-blockbit
debug-dhcp   fsck         lsusb    sar         update-license
debug-firewall fwrecovery mkfs    service-start uptime
debug-threats fwreload   more    service-status vmstat
debug-vpn    grep         mtr     service-stop whois
debug-web    help         netads   show-auth-sessions
dig          history     netstat  show-uuid
disable-bgp  host        nslookup show-vpn-conn
admin >
```

Para listar o novo disco, digite: **fdisk -l**

```
admin > fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes, 625142448 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000b93f6

Dispositivo Boot      Start        End    Blocks   Id  System
/dev/sda1  *        2048     1026047     512000   83  Linux
/dev/sda2          1026048   625141759   312057856   8e  Linux LVM

Disk /dev/mapper/root: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/swap: 4177 MB, 4177526784 bytes, 8159232 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/data: 293.9 GB, 293890686976 bytes, 574005248
sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 8000 MB, 8000110592 bytes, 15625216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >
```

Para formatar o disco identificado, digite “**mkfs -t ext4 [/dev/sdx??]**”,  
digite: ex. **mkfs -t ext4 /dev/sdb/**

```
admin > mkfs -t ext4 /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
488640 inodes, 1953152 blocks
97657 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2000683008
60 block groups
32768 blocks per group, 32768 fragments per group
8144 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736,
1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information:
done
admin >
```

O dispositivo uma vez conectado ao servidor e formatado no padrão EXT4, está pronto para listar em **[Sistema] >> [Armazenamentos]**, basta o click em **Atualizar** [  ], o sistema aplica o recurso “AUTO\_MOUNT” e o dispositivo fica automaticamente disponível para seleção.

**NOTA:** Não se esqueça de APPLICAR A FILA DE COMANDOS, clique no ícone:



## 7 Backup / Restore / Snapshot

A opção Backup do Sistema gera uma “imagem” completa do sistema, o que inclui desde o “Sistema Operacional”, o “banco de dados de configuração” e o “banco de dados de relatórios”, garantindo uma cópia íntegra absolutamente idêntica ao seu estado no momento do procedimento, dessa forma também é garantida sua restauração de maneira muito mais rápida e eficiente.

A opção Snapshot, oferece uma forma mais rápida e compacta para salvar as configurações do BLOCKBIT UTM.

Antes de configurar o serviço de backup, você precisar configurar o serviço de “Armazenamentos”.

Acesse a interface de gerenciamento de backup, vá para **[Sistema] >> [Backups]**.

### 7.1 Configurações

Nesta área você configura o serviço de backup e define o local de armazenamento entre as opções de armazenamento “NFS” ou “Disco”, previamente cadastrados em **[Sistema] >> [Armazenamentos]**.

Você ainda pode selecionar o tipo de backup: **[Diário] ou [Semanal]** e definir um horário para realizar o backup automaticamente.

O sistema também conta com o recurso de executar um backup na hora, manualmente, basta um clique em . O backup inclui toda a base de configurações inclusive os relatórios estatísticos.

**NOTA:** Não se esqueça de APLICAR  A DE COMANDOS, clique no ícone:

**IMPORTANTE:** O Backup é gerado no modo criptografado.

## 7.2 Backups do Dispositivo

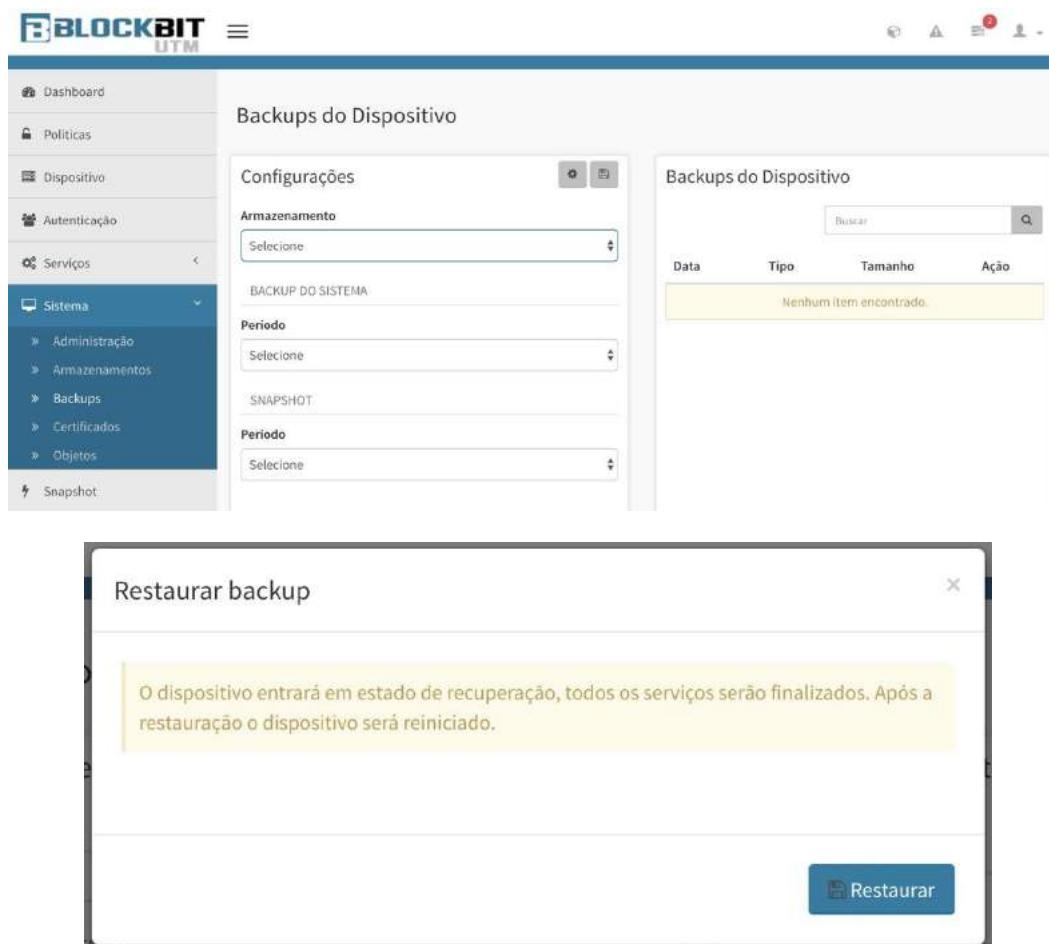
Nesta área o sistema retorna a lista dos arquivos de backup disponíveis no *armazenamento* selecionado e configurado na guia **[Configurações]**.

O arquivo é gerado com a data e hora do sistema no momento da sua realização.

Caso esteja fazendo uma reinstalação, lembrar que o backup foi salvo no modo “*criptografado*” e o algoritmo usado na criptografia utiliza-se da chave de integridade gerada no “*Wizard de configuração*” da instalação original do sistema para criptografia e decriptografia do backup/restore.

Para o sucesso no restore do backup na instalação atual, requer que seja usada a mesma chave de integridade e licença usadas para ativação do produto na instalação anterior.

Para restaurar um backup basta um clique em [  ] para o arquivo que deseja restaurar.



The screenshot shows the BLOCKBIT UTM web interface. On the left, there's a sidebar with navigation links: Dashboard, Políticas, Dispositivo, Autenticação, Serviços, Sistema (with sub-options: Administração, Armazenamentos, Backups, Certificados, Objetos), and Snapshot. The 'Sistema/Backups' link is currently selected. The main content area has a title 'Backups do Dispositivo'. It contains a 'Configurações' section with dropdown menus for 'Armazenamento' (set to 'Selecionar') and 'PERÍODO' (set to 'Selecionar'). To the right is a table titled 'Backups do Dispositivo' with columns: Data, Tipo, Tamanho, and Ação. A message at the bottom of this table says 'Nenhum item encontrado.' Below this is a modal dialog titled 'Restaurar backup'. Inside the dialog, a message states: 'O dispositivo entrará em estado de recuperação, todos os serviços serão finalizados. Após a restauração o dispositivo será reiniciado.' At the bottom right of the dialog is a blue button labeled 'Restaurar' with a gear icon.

**IMPORTANTE:** Durante o processo de restauração o sistema muda seu estado para o modo de RECUPERAÇÃO.

## 7.3 Snapshot

O Snapshot é uma forma mais rápida e compacta para salvar as configurações do BLOCKBIT UTM e pode ser acionando pelo menu **[Snapshot]** ou ser agendado e gerenciado pelo menu **[Sistema] >> [Backups]**.

Ao ser acessado pelo menu **[Snapshot]** é exibido uma caixa de diálogo com a opção de escolher um arquivo para ser restaurado ao clicar em **Restaurar** ou baixar um Snapshot imediatamente ao clicar em **Salvar**.



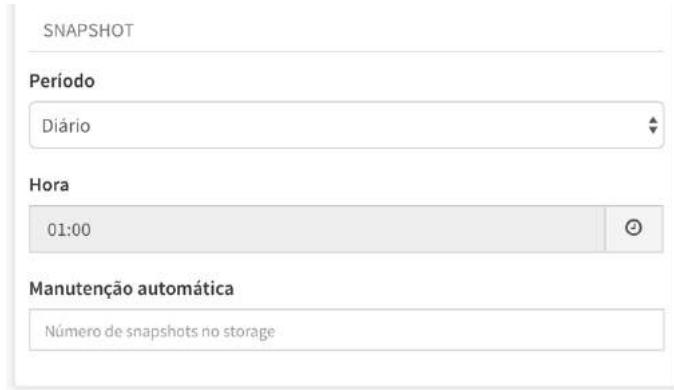
Através do menu **[Sistema] >> [Backups]**, é possível agendar a periodicidade do snapshot, sendo diário ou semanal.

Primeiro selecione o Armazenamento onde será salvo o snapshot, que pode ser configurado em **[Sistema] >> [Armazenamentos]**.



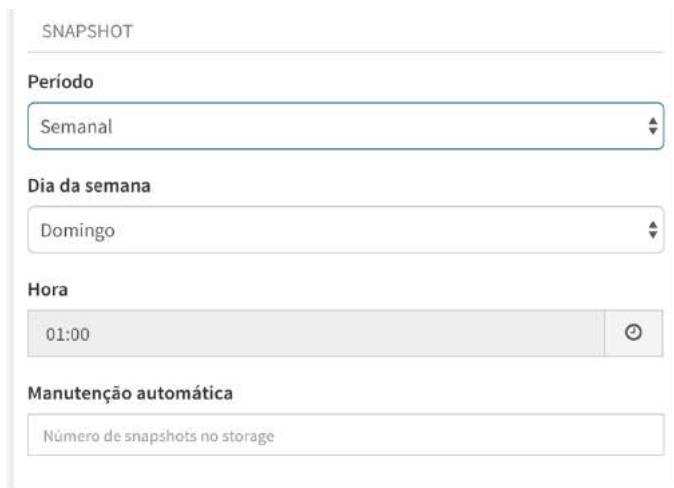
Em seguida selecione a periodicidade que deseja.

Selecionando Período Diário, pode ser escolhido a hora [  ] e a quantidade de snapshots que serão executados e mantidos no armazenamento escolhido.



The screenshot shows the 'SNAPSHOT' configuration screen. Under 'Período', 'Diário' is selected. In the 'Hora' field, '01:00' is entered, with a clock icon to its right. Under 'Manutenção automática', there is a text input field labeled 'Número de snapshots no storage'.

Selecionando Período Semanal, pode ser escolhido o Dia da semana, a hora [  ] e a quantidade de snapshots que serão executados e mantidos no armazenamento escolhido.



The screenshot shows the 'SNAPSHOT' configuration screen. Under 'Período', 'Semanal' is selected. In the 'Dia da semana' dropdown, 'Domingo' is chosen. The 'Hora' field contains '01:00' with a clock icon. The 'Manutenção automática' section includes a text input field for 'Número de snapshots no storage'.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 8 Certificados

O propósito de uma autoridade certificadora é confirmar a titularidade dos certificados, confirmando que o certificado recebido ao acessar determinado site ou endereço pertence realmente à entidade que o está fornecendo. É isso que garante que você está mesmo acessando os sites e endereços **SSL / HTTPS** de forma segura.

O **BLOCKBIT UTM** permite o administrador criar a própria autoridade certificadora, uma maneira simples e prática de se obter o certificado que será usado para garantir confiabilidade no acesso aos recursos da solução.

- **Interface WEB** do **BLOCKBIT UTM**.
- **Autenticação** web ou Captive portal.
- **Interceptação SSL** nos acessos via proxy.
- **VPN IPSEC RAS** em redes Windows.

No sistema **BLOCKBIT UTM** os certificados são configurados e gerados pelo “*Wizard de configuração*”, realizados no processo de instalação do sistema. Para acessar a interface de gerenciamento de certificados, vá para **[Sistema] >> [Certificados]**.

A interface **[Certificados]** se divide em **[Autoridade Certificadora]** e **[Certificado do Servidor]**.

No quadro **[Autoridade Certificadora]** você pode fazer “**download**” para importação nos dispositivos da rede, ou gerar uma “**nova**” CA (Certification Authority).

Para fazer download do certificado, clique em .

**IMPORTANTE:** Após o “Download” da CA. Instalar a CA em todos os dispositivos da rede.

Apenas em caso de necessidade especial o administrador pode gerar uma nova CA (Certification Authority), clicando em **Salvar** [  ].

**IMPORTANTE:** Salvar uma CA requer que o servidor gere uma nova entidade certificadora. Esta ação exige a reinstalação da nova CA em todos os dispositivos da rede.

*“Após regerar a CA, você também deve salvar para regerar o Certificado do Servidor, este procedimento requer a instalação da nova CA em todos os dispositivos da rede. Faça o download da CA e reinstale em todas as estações de trabalho. Lembrando que para validação da nova CA. você deve REINICIAR o servidor. Deseja continuar mesmo assim?”*

Clique em **[ OK ]**

*“Após regerar será necessário baixar e instalar a nova CA em todos os dispositivos. Quando regerado uma CA o processo não pode ser revertido. Deseja realmente continuar?”*

Clique em **[ OK ]**

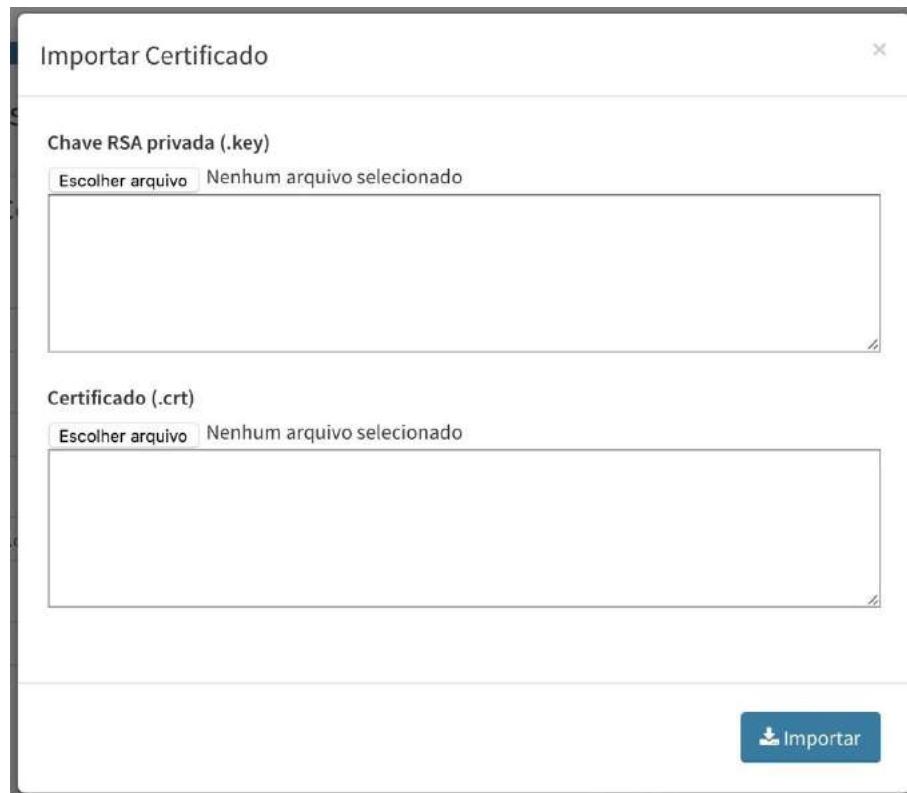
**IMPORTANTE:** Não é recomendável regerar a CA (Certification Authority).

No quadro **[Certificado do Servidor]** temos a opção de regerar o certificado do servidor para os casos em que a CA for regerada exigindo assim que também seja regerado o certificado do servidor.

Para regerar um certificado do servidor basta clicar em **Save** [  ].

*“Após regerar o certificado é necessário reiniciar o servidor. Deseja continuar?”  
Clique em **[OK]**.*

Outra opção é a Importação de um certificado assinado por alguma entidade certificadora. O certificado deve estar no formato “CRT” ou o administrador deve importar a chave RSA privada no formato “KEY”. Para a importação do certificado clique em [  ] selecione os arquivos correspondentes para a importação e clique em [  Importar ].



## 8.1 Instalação da CA via GPO

Para facilitar e automatizar o processo de instalação da CA nas estações, o administrador poderá distribui-la através de GPO (Group Policy Object) para seus equipamentos pertencentes ao domínio.

Nesta seção iremos detalhar este procedimento.

**ATENÇÃO:** Este procedimento está homologado para as versões Servers Windows 2012, Windows 2008 e estações com Windows 8, Windows 8.1 e Windows 10

Realize o download do arquivo da CA do BLOCKBIT UTM e salve-o em um diretório local no servidor Windows.

**Siga as etapas:**

No servidor BLOCKBIT acesse o Menu **[Sistema] >> [Certificados]**.

Clique em para fazer o download da CA.

**Construindo um GPO compatível com os navegadores MS Internet Explorer e Google Chrome.**

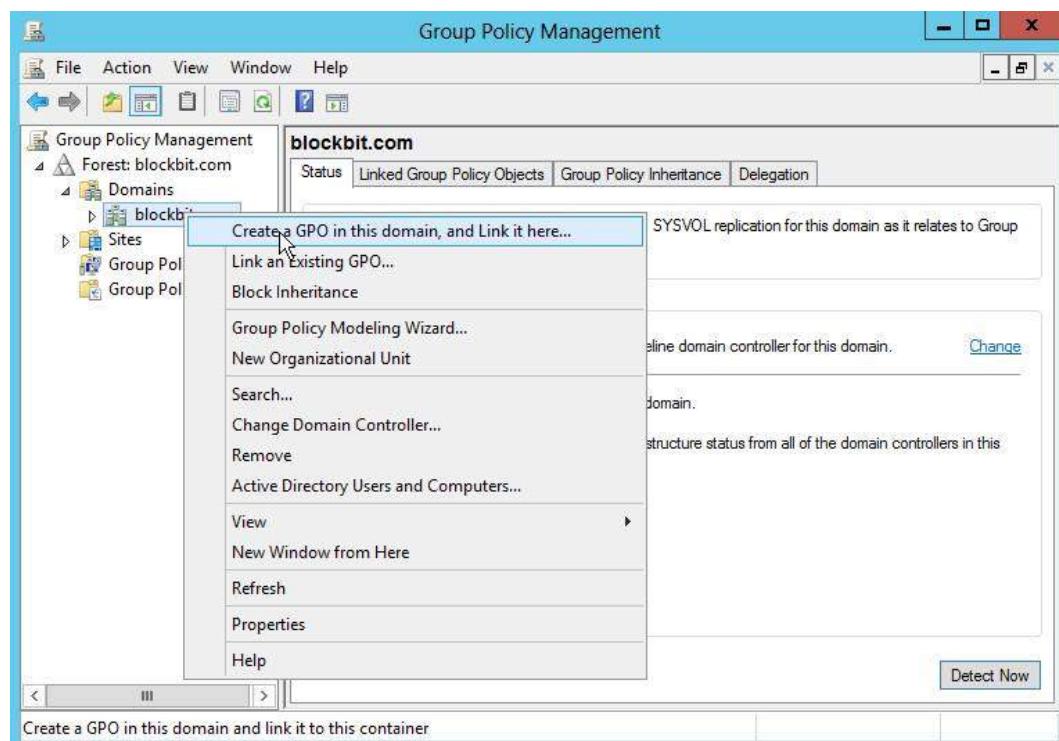
Todas as configurações foram realizadas para Windows Server 2012.

Abra o **Group Policy Management**.

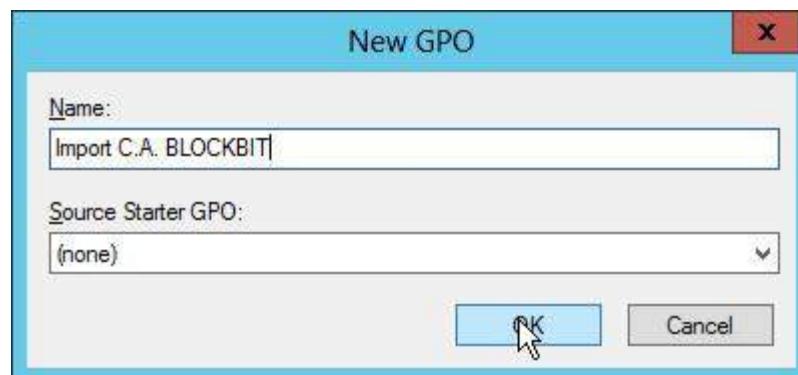


Na aba esquerda clique com o botão **[direito]** do mouse sobre o seu domínio.  
Ex. **[blockbit.com]**.

Clique em **[Create a GPO in this domain, and link it here...]**.

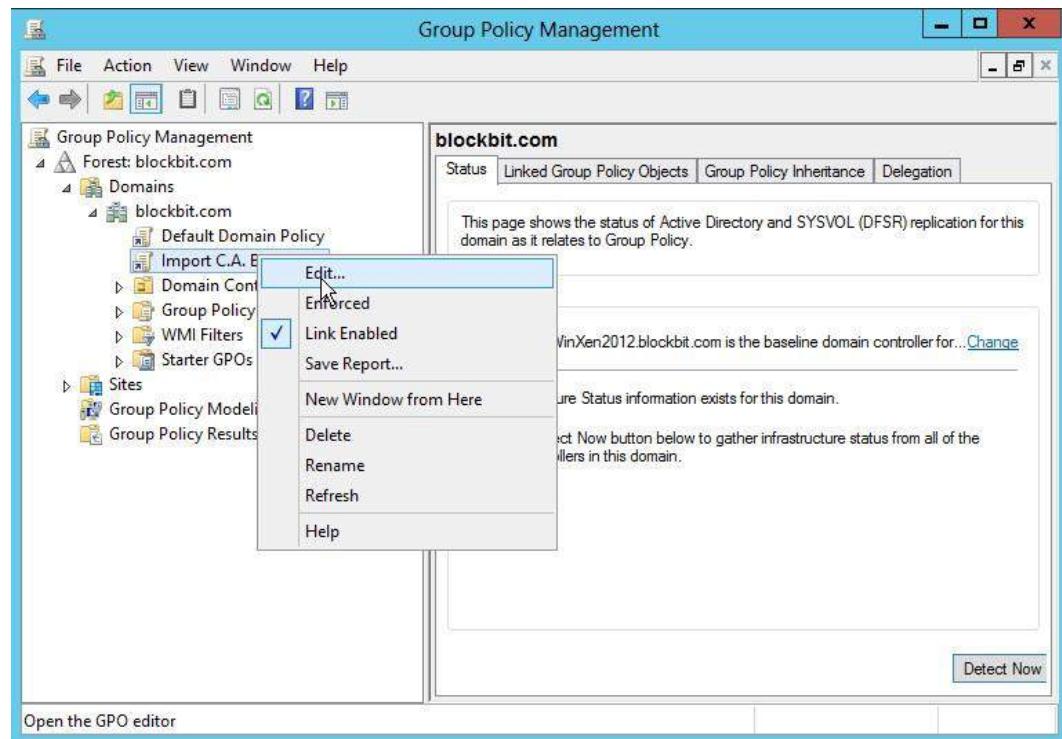


Defina um nome para o GPO: **[Import C.A. BLOCKBIT]** e clique em **[ OK ]**



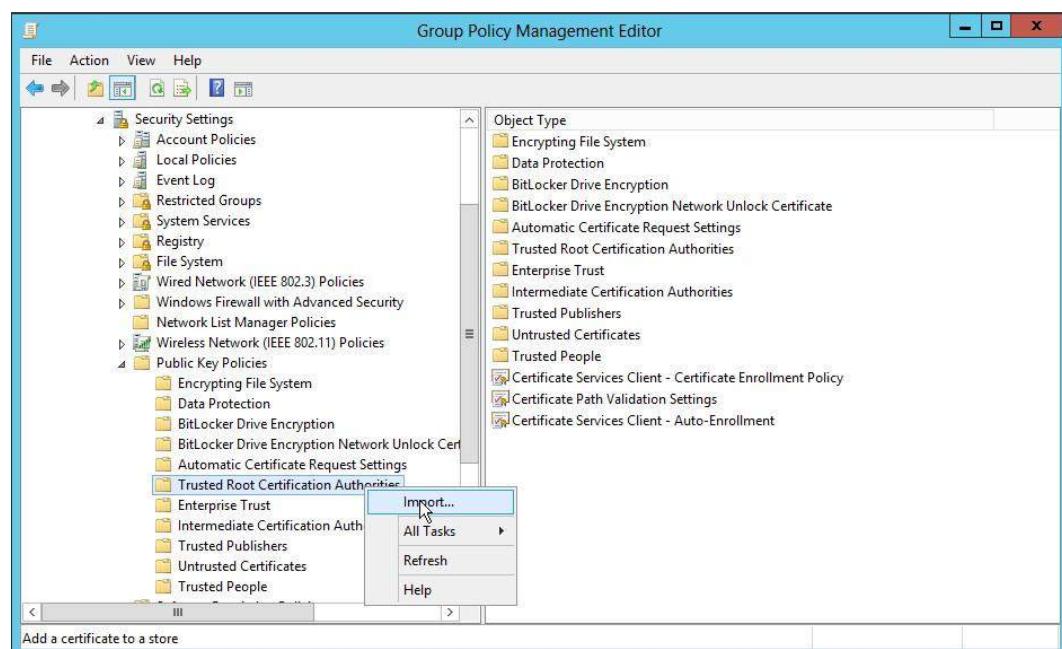
Clique para expandir o domínio [blockbit.com] e clique com o botão [direito] do mouse sobre o link do GPO [**Import C.A. BLOCKBIT**].

Clique em [**Edit**] – Group Policy Management Editor.



Clique para expandir >> [Computer Configuration] >> [Policies] >> [Windows Settings] >> [Security Settings] >> [Public key Policies].

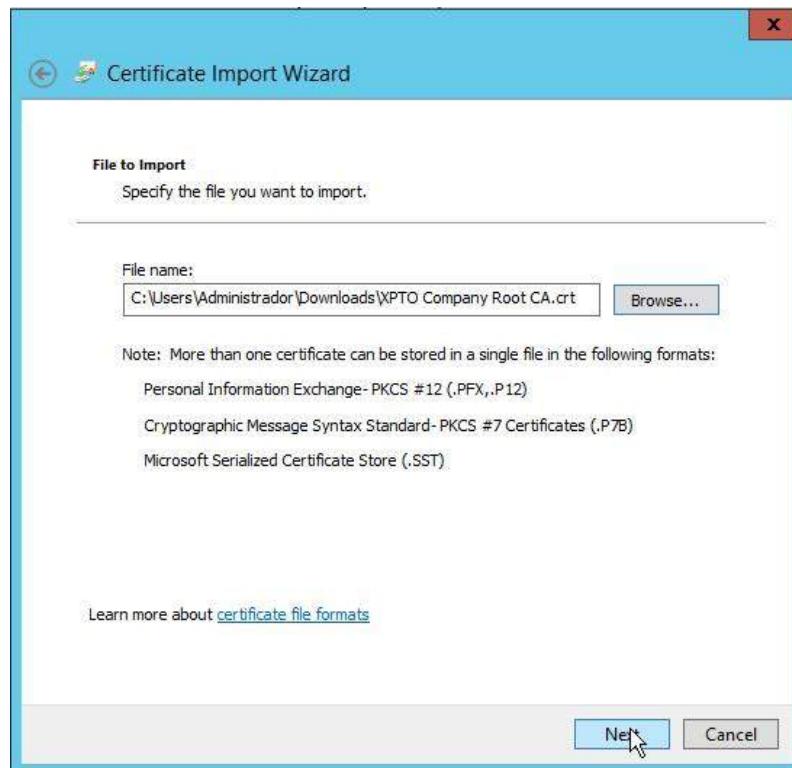
Clique com o botão [direito] do mouse sobre [**Trusted Root Certification Authorities**].



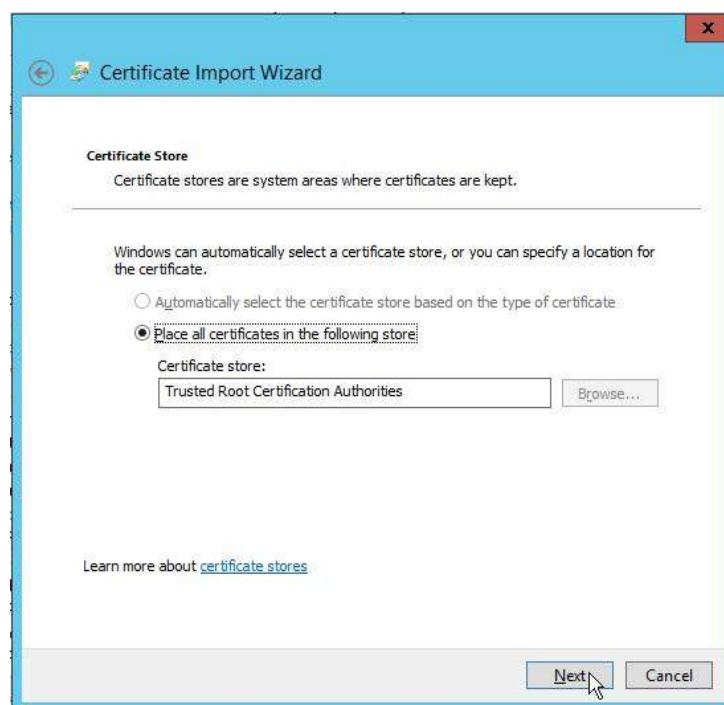
Clique em [Import] – Welcome to the Certificate Import Wizard.

Clique em [Next] e siga as etapas para importação da CA.

Clique em [Browse...] e localize a área de downloads onde salvou a CA. e clique em [Next].



Prossiga com a importação... clique em [Next] e [Finish].





**Importação realizada com sucesso.**

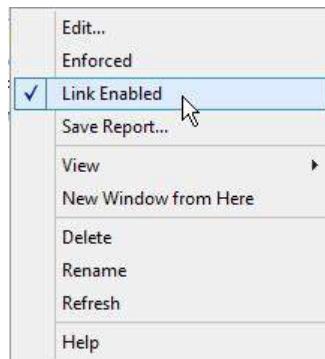


Finalize este processo fechando a janela do Group Policy Management Editor....

Ainda no Gerenciador de Política...

Clique para expandir o domínio ex: **[blockbit.com]**.

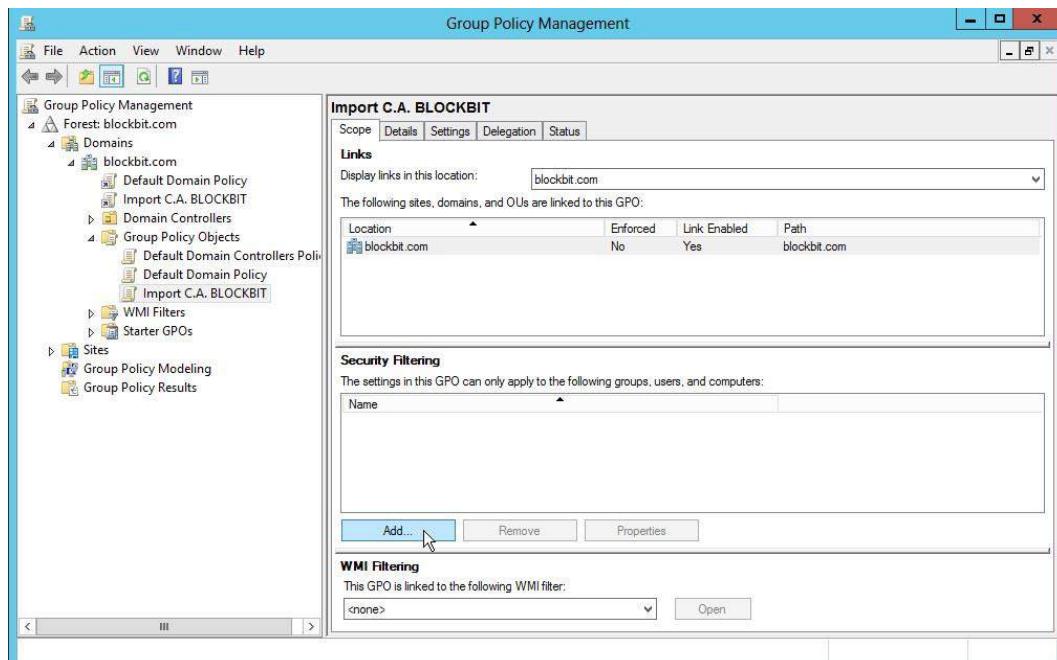
Clique com o botão **[direito]** do mouse sobre o GPO e certifique-se que a opção **[v] Link Enabled** esteja “**Selecionada**”.



Clique para expandir **[Group Policy Objects]** >> clique no GPO **[Import C.A. OMNE]**.

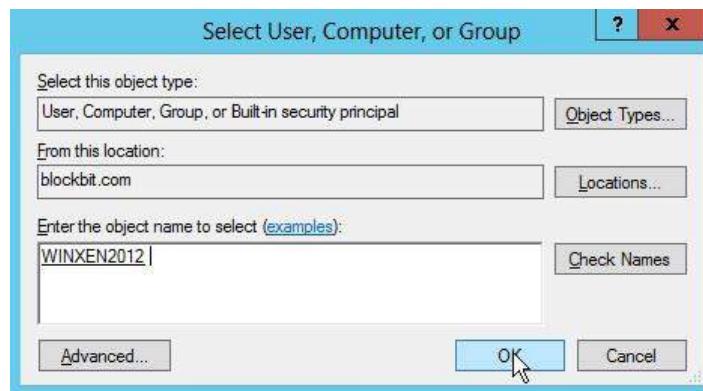
No frame lateral na aba inferior em **[Security Filtering]** remover a seleção pré-definida “**Autentication Users**”.

E **[Adicione]** a lista de computadores ou equipamentos ingressados no domínio que receberão este GPO.



**[Add]** a lista de computadores ou equipamentos ingressados no domínio que receberão este GPO.

Selecione o **[Object Types...]** >> **[\*] Computers**; Em **[Advanced]** selecione a lista de hosts e clique em **[OK]**.



Feche a janela do Gerenciador de Políticas....

Frequentemente para validar o GPO configurado é necessário executar o comando “**gpupdate**”.

No prompt de comandos e digite: **gpupdate /force**

```
Administrator: Command Prompt - gpupdate /force
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrador>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
-
```

Não é necessário reinicializar o servidor.

O GPO será aplicado na próxima reinicialização de cada estação de trabalho da rede.

## 9 Objetos

---

O sistema foi desenvolvido orientado a objetos para facilitar o processo de configuração, manutenção e leitura de regras e configurações.

Os Objetos podem ser compartilhados entre os serviços do sistema.

Tipos de objetos:

- Endereço IP
- Endereço MAC
- Serviços
- Horários
- Período/Datas
- Dicionários
- Content-type

A vantagem de trabalhar com o sistema orientado a objeto é o fato que suas definições são referenciadas no uso e aplicabilidade das configurações e habilitações de serviços e nas configurações das políticas de segurança.

Toda e qualquer alteração aplicada em um objeto são automaticamente replicadas e aplicadas em todos os serviços em uso pelo respectivo objeto. Atualizando o valor do seu conteúdo a configuração ou política associada ao objeto.

Para gerenciamento dos objetos clique em **[Sistema] >> [Objetos]**, temos aqui a interface **[Gerenciador de Objetos]** a partir desta interface podemos “*Adicionar*”, “*Editar*”, “*Remover*”, e inclusive “*Importar*” listas de alguns tipos de objetos.

## 9.1 Objeto Endereços IP

Clique em [Sistema] >> [Objetos] >> [Endereços IP]

Nesse quadro temos a gerência dos objetos [Endereços IP] que são utilizados em todo o sistema.

Por padrão, o sistema traz alguns objetos pré-cadastrados, exemplo, os objetos referentes às classes de rede não válidas: “*Classe A reservada*”, “*Classe B reservada*”, “*Classe C reservada*”.

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e habilitação dos serviços. Os objetos de endereço de rede são classificados em dois tipos:

IP ÚNICO

LISTA (suporte a múltiplos endereços IPs/ endereço de rede).

Esta definição é aplicada no momento do cadastro do objeto de endereço, que permite sinalizar se o endereço será do tipo **[V] IP único** ou não.

Nome	Ações
Classe A reservada	
Classe B reservada	
Classe C reservada	
Classes reservadas	
localhost	
Servidores Skype	
Servidores Webex	
Servidores Whatsapp	

### 9.1.1 Adicionando um Objeto Endereço IP

Para adicionar um objeto de endereço IP clique em **Adicionar** [+] e configure o objeto de acordo com as definições para aquele endereço de host e suas aplicações nas configurações dos respectivos serviços da solução e os campos do formulário. Depois clique em [ ]

Adicionar Objeto de Endereço IP

Nome	IP único
Servidor Web	<input checked="" type="checkbox"/>
IP/Host	Máscara
IP/Host	255.255.255.255
192.168.254.183	
Descrição	
Servidor Web	

**IMPORTANTE:** Uma vez definido o objeto do tipo **[V] IP único**, não é possível alterar.

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “*Endereço IP*”, no campo **[Buscar]**, digite de acordo com os métodos de pesquisas permitidas e clique em [ ] para listar o objeto recém-cadastrado.

The screenshot shows the BLOCKBIT UTM 1.1 web interface. The left sidebar has a dark blue header with the 'BLOCKBIT UTM' logo and a navigation menu. The main content area has a light gray header 'Gerenciador de Objetos'. Below it is a search bar with the placeholder 'Servidor Web' and a 'Search' button. To the right of the search bar are several small icons for filtering and sorting. A tooltip 'Servidor Web' is visible over one of these icons. The main content area contains a table with columns for 'Endereços IP', 'Endereços Mac', 'Serviços', 'Horários', 'Períodos/Datas', 'Dicionários', and 'Content-type'. The 'Servidores' column is currently selected, showing a single row for 'Servidor Web'.

## 9.2 Objeto Endereços Mac

Clique em [Sistema] >> [Objetos] >> [Endereços Mac]

Nesse quadro temos a gerência dos objetos [Endereços Mac] que podem ser utilizados pelas “*Políticas de compliance*” e pelo serviço “*DHCP*”.

Os objetos cadastrados ficam disponíveis para serem usados no processo de configuração do serviço “*DHCP*” e pelas “*Políticas de compliance*”. Os objetos de endereço MAC podem compor um único endereço MAC ou uma lista de endereços.



### 9.2.1 Adicionando Objeto Endereços MAC

Para adicionar um objeto de endereço MAC clique em **Adicionar** [+] e configure o objeto de acordo com as definições das políticas que pretende aplicar para hosts específicos e os campos do formulário. Depois clique em [  Salvar ]

Adicionar Objeto de Endereço MAC

**Nome**  
Telefones VOIP  MAC único

**Endereço Mac**  
Endereço Mac 

a2:21:60:13:32:c3  
a2:21:60:13:32:c4  
a2:21:60:13:32:c5 

**Descrição**  
Telefones VOIP 

**IMPORTANTE:** O endereço MAC possui 12 dígitos hexadecimais, agrupados dois a dois separados por dois pontos. Exemplo: 00:01:02:AA:CC:FF

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “*Endereços Mac*”, no campo **[Busca]**, digite de acordo com os métodos de pesquisas permitidas e clique em **[ ]** para listar o objeto recém-cadastrado.

The screenshot displays the BLOCKBIT UTM 1.1 web interface. The left sidebar features a vertical navigation menu with several sections: Dashboard, Políticas, Dispositivo, Autenticação, Serviços, Sistema, Administração, Armazenamentos, Backups, Certificados, and Objetos. The 'Objetos' section is currently active, indicated by a blue background. The main content area is titled 'Gerenciador de Objetos'. It includes a search bar at the top right labeled 'Buscar por mac, nome ou descrição' with a magnifying glass icon and a 'Items' button. Below the search bar are three tabs: 'Endereços IP', 'Endereços Mac' (which is highlighted in blue), and 'Telefones VOIP'. Under each tab, there is a list of object types: 'Serviços', 'Horários', 'Períodos/Datas', 'Dicionários', 'Content-type', and 'Content-type'. On the far right side of the main area, there are several small icons for managing files and objects, including download, add, and settings symbols.

## 9.3 Objeto Serviços

Clique em [Sistema] >> [Objetos] >> [Serviços]

Neste quadro temos gerência dos objetos **[Serviços]**, que compõem porta e protocolos.

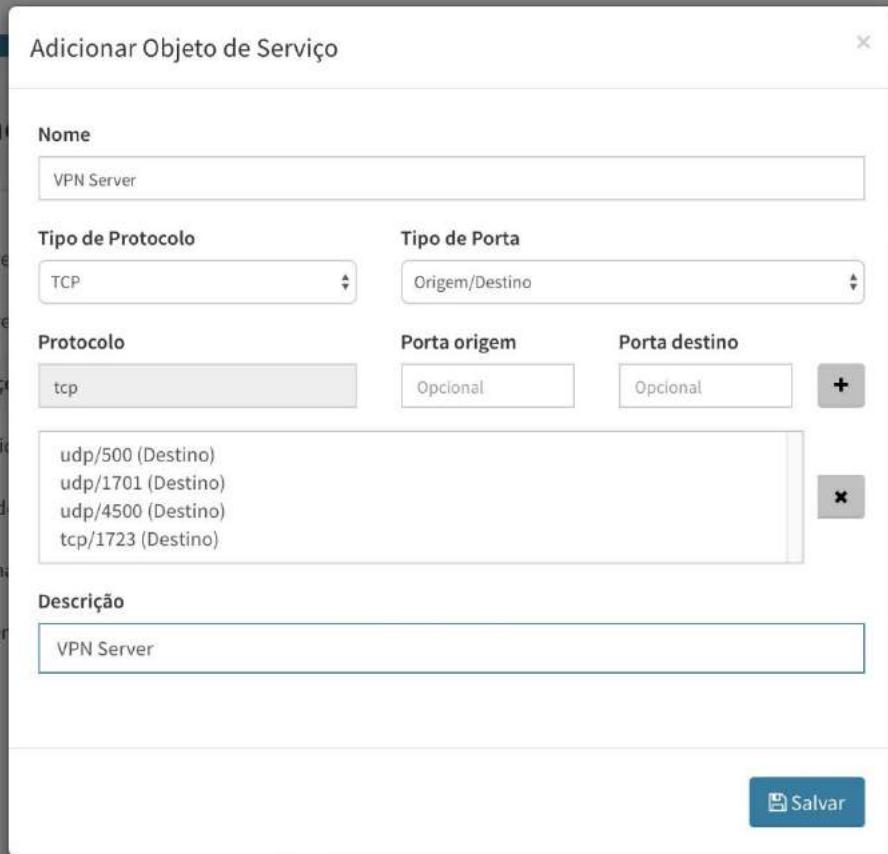
Por padrão, o sistema traz alguns objetos (portas/protocolos) pré-cadastrados, exemplo, os objetos referentes os protocolos e serviços mais comuns: Exemplo: “*DHCP*”, “*DNS*”, “*HTTP*”, “*HTTPS*”.

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e habilitação dos serviços. Os objetos de serviços podem ser compostos por um conjunto de protocolos e serviços diferentes, no objetivo de agrupar esses protocolos e serviços como um recurso comum para ser aplicado em uma finalidade específica, seja a configuração de um “*Serviço*” ou uma “*política de compliance*”.

Endereços IP	AH	
Endereços Mac	AOL	
<b>Serviços</b>	BGP	
Horários	BLOCKBIT-ADMIN	
Períodos/Datas	BLOCKBIT-PORTAL	
Dicionários	BLOCKBIT-PROXY	
Content-type	BLOCKBIT-VPNSSL	
	BLOCKBIT-VPNSSL	
	DHCP	
	DNS	
	ESP	

### 9.3.1 Adicionando um Objeto Serviços

Para adicionar um objeto de serviço clique em **Adicionar** [+] e configure o objeto de acordo com as definições das políticas que pretende aplicar para hosts específicos e os respectivos campos do formulário. Depois clique em [  Salvar ].



Nome  
VPN Server

Tipo de Protocolo  
TCP

Tipo de Porta  
Origem/Destino

Protocolo  
tcp

Porta origem  
Opcional

Porta destino  
Opcional

Descrição  
VPN Server

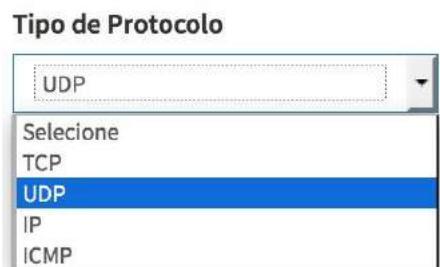
Salvar

Abaixo alguns apontamentos referentes alguns campos, quanto à seleção dos tipos de protocolos.

#### [Tipo de Protocolo].

O administrador pode selecionar entre os tipos de protocolo para compor o objeto. Esta seleção permite selecionar diferentes protocolos e agrupá-los no mesmo objeto:

Tipos de protocolos:



**TCP** – Associa-se a portas e ranges de portas referente os diversos serviços que executem suas aplicações sob o protocolo TCP. Ex.: “*Vpn pptp (1723), http (80), https (443), dns (53)*”.

**UDP** - Associa-se a portas e ranges de portas referente os diversos serviços que executem suas aplicações sob o protocolo UDP. Ex.: “*Vpn ike-isakmp (500), Vpn l2tp (1701), Vpn Nat-t (4500), dns (53)*”.

**IP** – Associa-se a outros protocolos da camada IP. Ex.: “ah, egp, esp, gre, icmp, igmp, sctp, tcp e udp”.

**ICMP** – Associa-se a tipos de tratamento e/ou resposta esperada referente o tráfego do protocolo ICMP. Ex.: “*Echo Request*”, “*Echo Replay*”, “*Destination unreachable*”, “*time exceeded*”.

#### [Tipo de Porta]

Você seleciona entre 2(dois) tipos de portas (serviços) que vai compor o objeto.

**[Origem/Destino]** Definição dos campos [Porta Origem] / [Porta Destino] referente a serviços que normalmente seguem padrões de RFC's e executam o serviço para uma porta específica (Porta Destino), geralmente em serviços que executam sob o protocolo TCP. Ex. “*HTTP (80); HTTPS (443), DNS (53)* ”. Existem casos de serviços que também executam sob o protocolo UDP. Ex. “*DNS (53)* ”.

**IMPORTANTE:** O campo [Porta Origem] é um campo opcional. Geralmente é executada sob uma porta alta [1024:65535] aleatória executa no start do serviço.

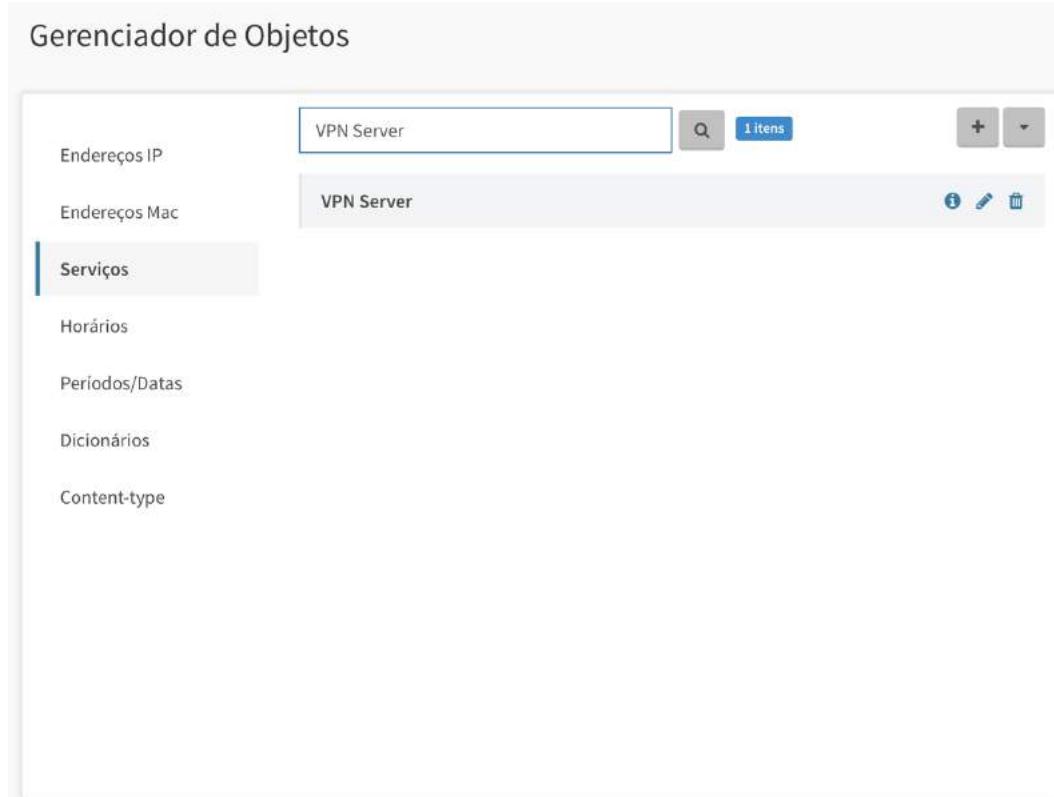
#### [Range]

Definição das portas ou serviços que executam normalmente dentro de uma classe de portas [Porta inicial] / [Porta final] geralmente em serviços que executam sob o protocolo UDP. Serviços que normalmente executam em ranges de portas. Ex.: “*VOIP - porta inicial 4500/UDP; porta final 5500/UDP.; Câmeras – porta inicial 10000/UDP; porta final 20000/UDP*”.

**IMPORTANTE:** Os Ranges de portas mesmo para aplicações do mesmo tipo podem variar de acordo com a especificação de cada aplicativo.

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “*Serviços*”, no campo **[Busca]**, insira a informação de acordo com os métodos de pesquisas permitidas e clique em **[]** para listar o objeto recém-cadastrado.

Gerenciador de Objetos



Endereços IP	Endereços Mac
VPN Server	VPN Server

The sidebar on the left lists other categories: Endereços IP, Endereços Mac, Serviços (which is selected and highlighted in blue), Horários, Períodos/Datas, Dicionários, and Content-type.

## 9.4 Objeto Horários

Clique em [Sistema] >> [Objetos] >> [Horários]

Neste quadro temos a gerência dos objetos **[Horários]**, os objetos são compostos pelos “*dias da semana*” e a “*hora inicial e final*”.

Por padrão, o sistema traz 2(dois) objetos de horário pré-cadastrados.

- Comercial
- Final de semana

Esses objetos estão disponíveis para serem usados nos processos de configuração de serviços e pelas “*Políticas de compliance*”.

Horários	Ações
Comercial	
Final de semana	

#### 9.4.1 Adicionando Objeto Horários

Para adicionar um objeto de horário clique em **Adicionar** [+] e configure o objeto de acordo com as definições das políticas que pretende aplicar e os campos do formulário. Depois clique em [  Salvar ].



The dialog box has the following fields:

- Nome:** Entretenimento
- Horário:** Dia da semana: Segunda; Hora inicial: 07:00 - 08:00, 12:00 - 13:30, 21:00 - 21:30; Hora final: (empty)
- Descrição:** Entretenimento

**IMPORTANTE:** A definição do objeto horário permite incluir diversos ranges de hora inicial/ hora final no mesmo objeto.

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “*Horários*”, no campo [**Buscar**], insira a informação de acordo com os métodos de pesquisas permitidas e clique em [  ] para listar o objeto recém-cadastrado.



## 9.5 Objeto Períodos / Datas

Clique em [Sistema] >> [Objetos] >> [Períodos/Datas]

Neste quadro temos a gerência dos objetos **[Períodos/Datas]**, os objetos são compostos pelas definições e um período que compete “*Data/hora inicial*” e “*Data/hora final*”.

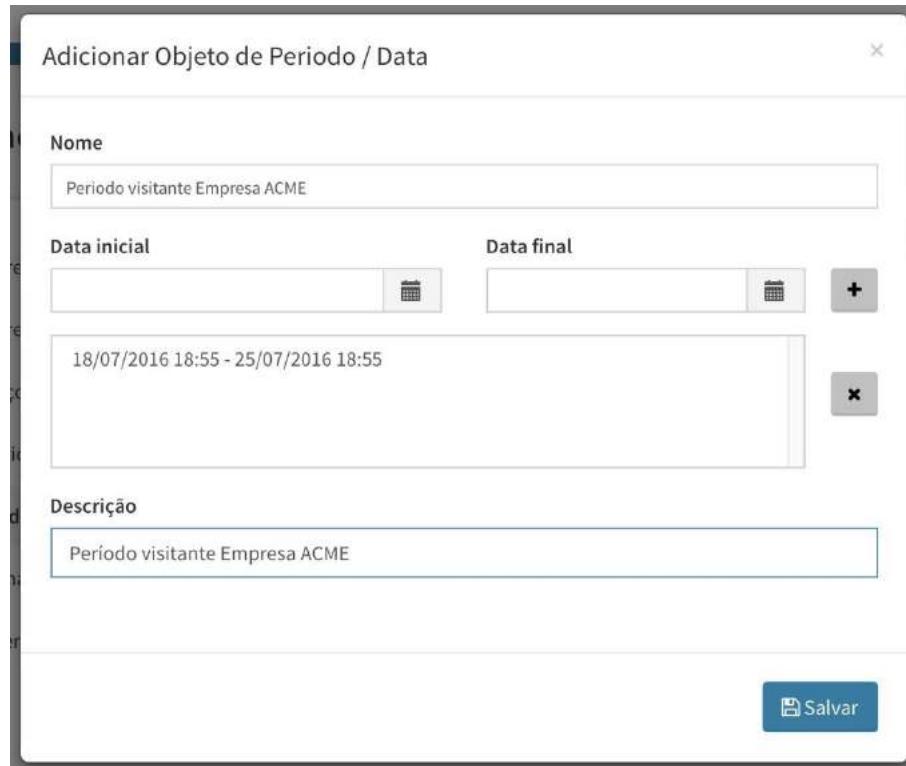
Os objetos cadastrados ficam disponíveis para serem usados nos processos de configuração e habilitação de alguns “*Serviços*”, e definições das “*Políticas de compliance*”.

**NOTA:** Vale ressaltar que os objetos **[Períodos/Datas]** tem uma finalidade bastante singular. Ex.: Quando se define políticas com tempo de validade, “*Data/hora início*” – “*Data/hora fim*”.



### 9.5.1 Adicionando um Objeto Período / Data

Para adicionar um objeto de Período / Data clique em **Adicionar** [+] e configure o objeto de acordo com as definições das políticas que pretende aplicar e os campos do formulário. Depois clique em [  Salvar ].



The dialog box has the following fields:

- Nome:** Periodo visitante Empresa ACME
- Data inicial:** (Initial Date field with calendar icon)
- Data final:** (Final Date field with calendar icon and a '+' button)
- Descrição:** Período visitante Empresa ACME
- Save button:**  Salvar

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “Período / Data”, no campo [**Buscar**], insira a informação de acordo com os métodos de pesquisas permitidas e clique em [  ] para listar o objeto recém-cadastrado.



The screenshot shows the following interface elements:

- Left Sidebar:** Shows navigation items like Dashboard, Políticas, Dispositivo, Autenticação, Serviços, Sistemas (with sub-options: Administração, Armazenamentos, Backups, Certificados, Objetos).
- Central Area:** Title "Gerenciador de Objetos". Search bar with input "ACME" and a "Buscar" button.
- Results Table:** Shows a list of objects found, including "Periodo visitante Empresa ACME". The table includes columns for Name, Type, and Actions (Edit, Delete).

## 9.6 Objeto Dicionários

Clique em [Sistema] >> [Objetos] >> [Dicionários]

Neste quadro temos a gerência dos objetos **[Dicionários]**, que pode ser composto por “*listas de palavras*” ou conjunto de combinações de “*expressões regulares*”.

Por padrão, o sistema traz alguns objetos pré-cadastrados. Ex.: “Alfanumérico”, “Endereço de Email”, “Link HTML”, “URL”.

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e definições das “*Políticas de compliance*”.

	Nome	Ações
1	Alfanumérico	
2	Cartão de Crédito	
3	Endereço de Email	
4	Endereço IP	
5	Link HTML	
6	URL	
7	URL Imagem	

### 9.6.1 Adicionando um Objeto Dicionários

Para adicionar um objeto Dicionário clique em **Adicionar** [+] e configure o objeto de acordo com as definições e filtros que pretende aplicar nas políticas de compliance, considerando os respectivos campos do formulário. Depois clique em [Salvar].

**IMPORTANTE:** Podemos incluir as “palavras-chaves” desejadas na lista de palavras do objeto “Dicionários” por lista de “palavras simples” sem espaços, adicionando “uma por linha” ou combinação por “Expressões regulares”.

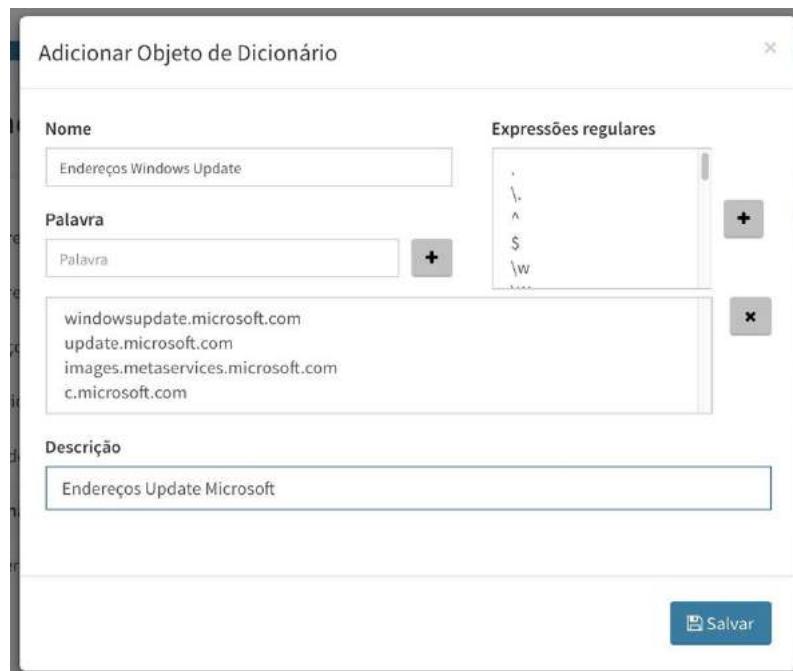
Vamos exemplificar o cadastro de um Objeto de dicionários com a lista de palavras simples “endereços dos servidores de Update Microsoft – Servers WSUS” adicionando manualmente “uma palavra por linha”.

windowsupdate.microsoft.com

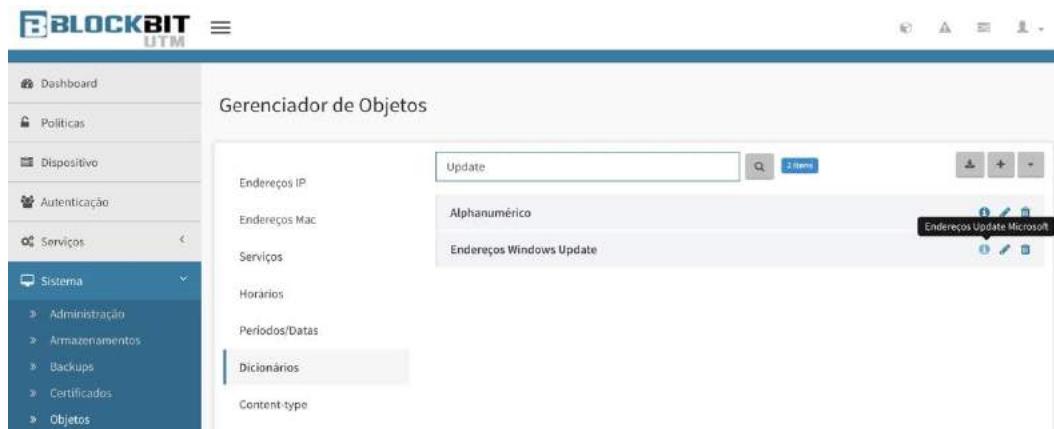
update.microsoft.com

images.metaservices.microsoft.com

c.microsoft.com



Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “Dicionários”, no campo [Buscar], digite de acordo com os métodos de pesquisas permitidas e clique em [  ] para listar o objeto recém-cadastrado.



Vamos adicionar outro objeto Dicionário, clique em Adicionar [  ]

Agora vamos exemplificar o cadastro de uma lista de palavras usando “expressões regulares”, notem o campo à esquerda [Expressões regulares], contempla uma lista de “regex” que podemos combinar para construir uma expressão regular e adicionar à lista de palavras-chave.



Para criar a combinação da expressão regular desejada. Ex.: “O regex: `$` corresponde a ao conteúdo de fim do texto, ou de uma linha, logo quando temos as seguintes expressões “`$.exe`”, “`$.bat`”, “`$.vbs`”, “`$.vb`”, o objeto cadastrado corresponde a lista de palavras chaves terminadas em extensões de arquivos suspeitos”.

Vamos usar esse exemplo e adicionar um novo objeto dicionário.

**Adicionar Objeto de Dicionário**

**Nome:** Extensões de executáveis

**Expressões regulares:** \$

**Palavra:** Palavra

**Descrição:** Extensões de executáveis

**Salvar**

Para pesquisar os objetos recém-cadastrados, na interface de gerenciamento do objeto “Dicionários”, no campo [Busca], digite de acordo com os métodos de pesquisas permitidas e clique em [ ] para listar os objetos recém-cadastrados.

## 9.7 Objeto Tipo de Content-type

Clique em [Sistema] >> [Objetos] >> [Content-type]

Neste quadro temos a gerência dos objetos **[Content-type]**, são compostos por agrupamentos de tipos de aplicações baseados no tipo de conteúdo que especificam sua característica.

Por padrão, o sistema traz alguns objetos pré-cadastrados que agrupam alguns tipos de aplicações com a finalidade de facilitar sua aplicabilidade no sistema. Ex.: “*ActiveX*”, “*Compactados*”, “*Executáveis*”, “*Imagens*”, “*Javascript*”, “*Multimedia*” e “*Office*”.

Todos esses objetos estão disponíveis para serem usados nos processos de configuração e definições das “*Políticas de compliance*”.

Endereços IP	Buscar por mime, nome ou descrição	Items	
ActiveX			
Compactados			
Executáveis			
Imagens			
Javascript			
Multimedia			
Office			

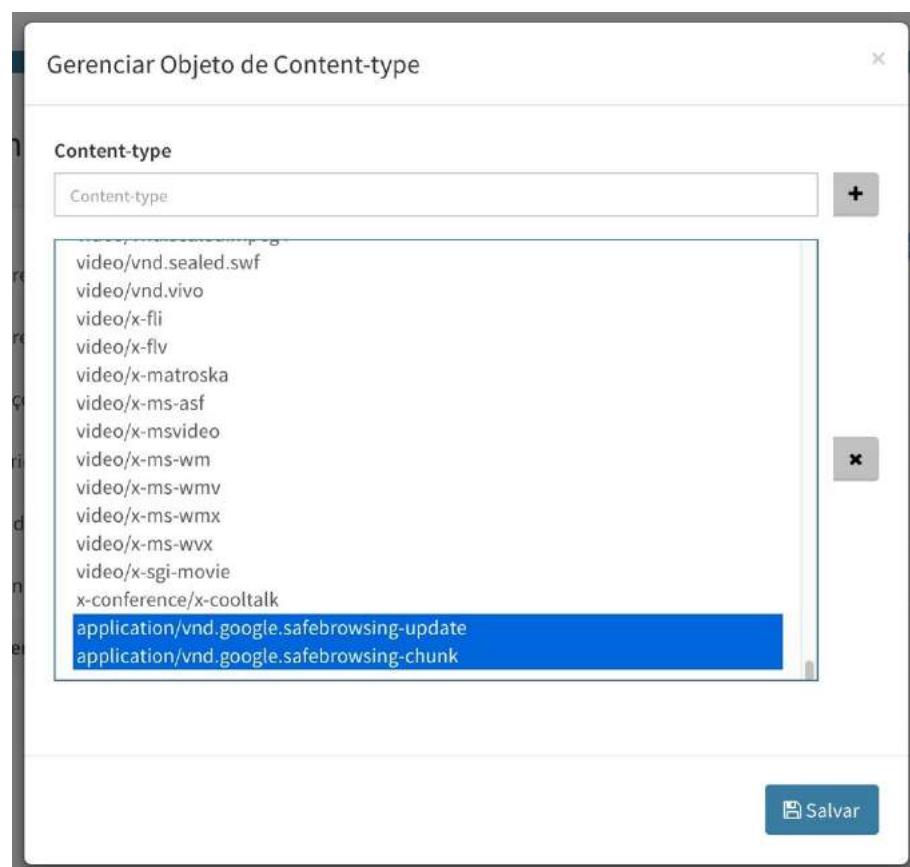
### 9.7.1 Gerenciando Objetos Content-type

O objeto **[Content-type]** conta com um recurso “extra” diferente dos demais objetos o “*Gerenciamento do objeto*”, por se tratar da especificação dos “*tipos de aplicações*” este modelo de objeto permite cadastrar não somente os agrupamentos, ou seja, os objetos do “*Content-type*” dos modelos de aplicações conhecidas, como também permite especificar novos modelos de “*Content-type*” cadastrando este “*novo tipo*” na base de conteúdo do sistema. O que agrega valor e permite adicionar este novo “*tipo de conteúdo*” a objetos já existentes ou adicionar a novos objetos.

Para adicionar um **[Content-type]** clique no botão **Gerenciar** [  ] especifique o Content-type que pretende adicionar e clique em **Adicionar** [  ] à lista.

Depois clique em [  Salvar ].

Vamos exemplificar adicionando 2 (dois) Content-type que se referem a aplicativos e serviços da Google.



**IMPORTANTE:** As especificações de novos Content-types podem ser identificadas a partir dos levantamentos dos registros nos logs detalhados.

### 9.7.2 Adicionando Objeto Content-type

Para adicionar um objeto Content-type clique em **Adicionar** [+] e configure o objeto de acordo com as definições e filtros que pretende aplicar nas políticas de compliance, considerando os respectivos campos do formulário. Depois clique em [Salvar].

**Adicionar Objeto de Content-type**

**Nome**  
Google Apps

**Content-type**  
vnd.google

**Descrição**

**Salvar**

The content-type section shows a list of values: application/vnd.google-earth.kml+xml, application/vnd.google-earth.kmz, application/vnd.google.safebrowsing-chunk, and application/vnd.google.safebrowsing-update. These values are highlighted with a blue rectangle.

Para pesquisar o objeto recém-cadastrado, na interface de gerenciamento do objeto “Content-type”, no campo **[Buscar]**, digite de acordo com os métodos de pesquisas permitidas e clique em [ ] para listar o objeto recém-cadastrado.

**BLOCKBIT UTM**

**Gerenciador de Objetos**

**Content type**

The screenshot shows the 'Content type' section of the Blockbit UTM interface. It includes a search bar with the value 'Google Apps', a button to add new items, and a list of existing items.

## 10 Autenticação

Neste item, o administrador define quais os padrões de autenticação serão usados. Existem dois métodos de autenticação: **Local e Integrada**.

O administrador tem a opção de sincronizar a base de usuários e grupos no BLOCKBIT UTM com uma base já existente na rede em um servidor “**LDAP**”, centralizando assim a administração de cadastro de todos os usuários e/ou grupos no respectivo servidor.

A autenticação integrada suporta autenticação **Windows AD e/ou Ldap**, é baseada no sincronismo da base de usuários. A autenticação baseada no sincronismo Windows AD requer que o servidor BLOCKBIT UTM seja integrado ao domínio. Já a autenticação baseada no sincronismo LDAP autentica diretamente na base LDAP, não necessitando integração ao domínio.

Esse recurso possibilita múltiplos domínios de autenticação, sendo:

- [N] domínios do tipo local;
- E até dois domínios integrados.
  - Base Windows.
  - Base Ldap.

**IMPORTANTE:** A integração de domínio, sincronismo e autenticação com servidores Windows foram homologados nas versões Windows 2008 Server, Windows 2008 Server R2, Windows 2012 Server e Windows 2012 Server R2

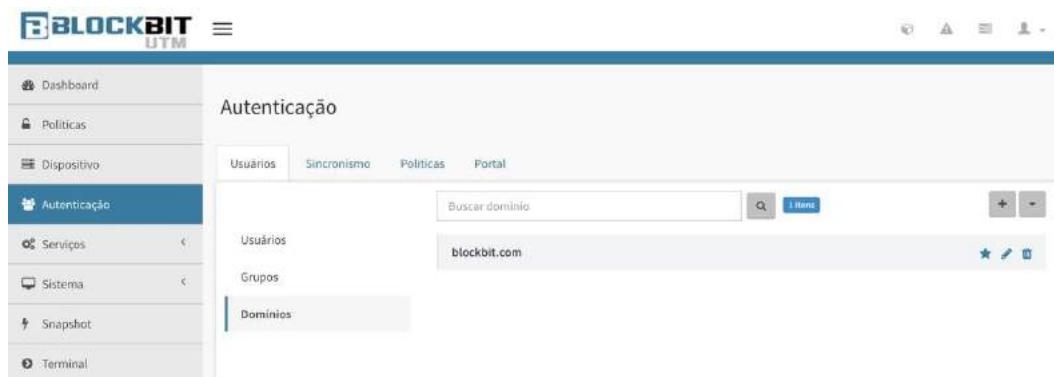
## 10.1 Integrando Domínios e Usuários - Windows / LDAP

Para o funcionamento adequado e seguro das conexões dos serviços BLOCKBIT UTM, com uma base de sincronismo Windows AD ou LDAP, é obrigatório pelo menos o cadastro de um domínio.

Clique em **[Autenticação] > [Usuários], aba [Usuários]**.

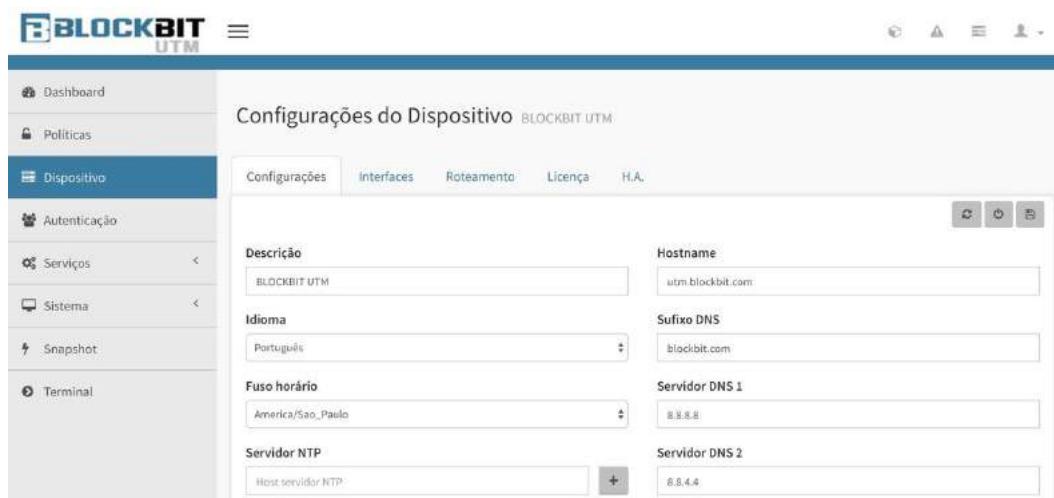
Selecione **[Domínios]**, nessa aba podemos “*Pesquisar*”, “*Adicionar*” ou “*Remover*” um domínio. Por padrão na ação de pesquisa retorna o “domínio” configurado no Wizard de Instalação. Este domínio vem pré-configurado como domínio “padrão”.

Clique em **pesquisar** [  ] para listar o domínio cadastrado no Wizard.



Como já foi mencionado, o processo de autenticação em uma base Windows requer a integração de domínio, para isso, antes de efetuarmos o processo de sincronismo, vamos certificar que o servidor esteja configurado adequadamente para o ingresso no controlador de domínio do servidor Windows.

Selecione o Menu **[Dispositivo] > [Configurações]**



Configuração	Valor
Hostname	utm.blockbit.com
Sufixo DNS	blockbit.com
Servidor DNS 1	8.8.8.8
Servidor DNS 2	8.8.4.4

Na aba **[Configurações]** temos os itens básicos de configuração, certifique-se que o endereço do campo **[DNS server 1]** esteja configurado para o endereço IP do controlador de domínio do servidor Windows que vamos aplicar o sincronismo de usuários.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



**Pronto!** Agora podemos configurar o item de sincronismo de usuários.

Clique em **[Autenticação] > [Usuários], aba [Sincronismo]**.

Nesta interface temos as **Abas [Windows] e [Ldap]**.

A configuração deste item é simples, mas requer alguns cuidados para não gerar erros ou falhas no sincronismo.

Vamos configurar o sincronismo Windows. Selecione **[Windows]** e clique em habilitar **[ ]** e configure os campos de acordo com as definições do seu controlador de domínio depois clique **[ ]**.

**IMPORTANTE:** Consulte a estrutura da floresta do seu servidor Windows AD.

Abaixo vamos especificar alguns campos:

**[Porta]**

Portas suportadas – 389 (LDAP), 3268 (LDAP Search), ou 636 (LDAPS) e 3269 (LDAPS Search).

**[Usuário]**

Especificar um usuário do servidor Windows com direitos de fazer pesquisa na base Ldap, geralmente usuário membro do grupo administradores.

**IMPORTANTE**

Recomenda-se criar um usuário específico para este fim.

Ex. No servidor Windows cadastre um usuário com o nome “blockbit.utm” e configure o perfil deste usuário com os seguintes parâmetros:

Senha nunca expira;

Permitir LOGON exclusivo do computador “BLOCKBIT UTM”;

Para configuração do campo “usuário” - Utilize a sintaxe “usuario@dominio”.

**[Filtros de usuários] e [Filtros de grupos]**

Nestas abas configuramos os campos que se referem à base de pesquisa e os seus respectivos filtros na base Ldap do servidor Windows AD.

Configure os campos “Base”, “Filtro”, “Atributo login”, “Atributo nome”, “Atributo membro” e “Atributo descrição” de acordo com os dados da base Ldap do respectivo servidor Windows.

Estes campos são preenchidos automaticamente ao clicar no botão .

**NOTA:** Por padrão o limite de objetos que podem ser pesquisados em uma consulta LDAP é: 1000 objetos.

Existem casos que o servidor Windows AD possui uma estrutura de (OU - Unidades organizacionais) com listas de objetos (usuários ou grupos) maior que 1000. Este caso requer alterar o valor padrão da variável “MaxPageSize” para maiores informações consulte o suporte Microsoft.

Na interface de sincronismo ainda temos as opções sincronizar agora [  ] e o agendamento do sincronismo [  ].

Para executar o sincronismo agora clique em [  ] e confirme para executar o sincronismo, clique em [OK].



Para criar um agendamento de sincronismo, clique em [  ], defina um intervalo de tempo, depois clique em [  ].



**ATENÇÃO:** O princípio de configuração do sincronismo de uma base LDAP é o mesmo.

No entanto é importante considerar que as configurações de filtros e base de busca em um servidor LDAP são criadas por quem implementa o serviço de diretório e é necessário ter essas informações para obter êxito na configuração.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 10.2 Autenticação Single Sign On

**ATENÇÃO:** Este procedimento esta homologado para as versões Servers Windows 2012 e Windows 2008.

O agente SSO do BLOCKBIT UTM não precisa ser distribuído entre os dispositivos (estações de trabalho) do domínio Windows. Agora ele é um agente que precisa ser disponibilizado apenas no servidor Windows que detém o controlador de domínio e mantém o AD (Active Directory) na sua rede, para integração e sincronismo de usuários.

O cliente SSO atua integrado com os eventos de login do AD. Assim sendo, qualquer dispositivo que faça login no AD terá sua sessão autenticada no UTM, incluindo outros sistemas operacionais que de alguma maneira se ingressam no AD.

### 10.2.1 Requisitos

Para o funcionamento do agente BLOCKBIT SSO e integração com o serviço de agendamento e evento do login, o sistema requer a instalação do aplicativo **.NET Framework versão 3.5** no servidor Windows.

Para instalação do aplicativo **.NET versão 3.5**, utilize os recursos de instalação disponíveis no painel do “**Gerenciador do servidor**”, item **[Adicionar funções e recursos]** do seu servidor Windows.

### 10.2.2 Download do agente SSO

Nesta seção detalhamos o procedimento de download do agente SSO.

Realize o download do arquivo do agente SSO e salve-o em um diretório local no servidor Windows.

**Siga as etapas:**

No BLOCKBIT UTM acesse o Menu **[Autenticação] >> [Sincronismo] >>** na aba **[Windows]**.



**[Clique aqui]** para baixar o agente de autenticação Single Sign On

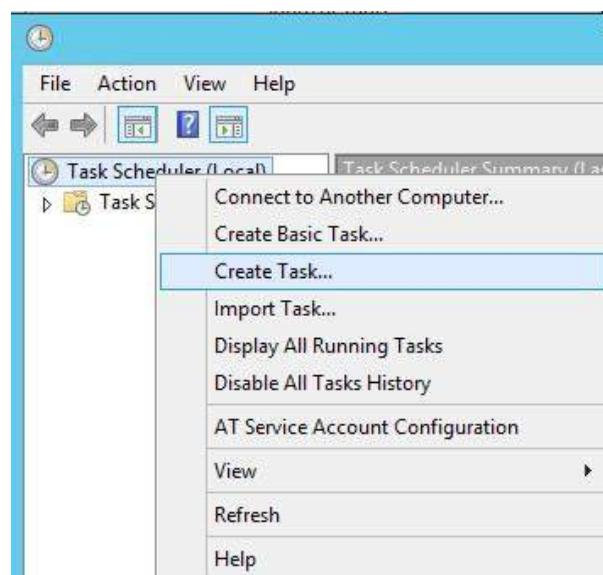
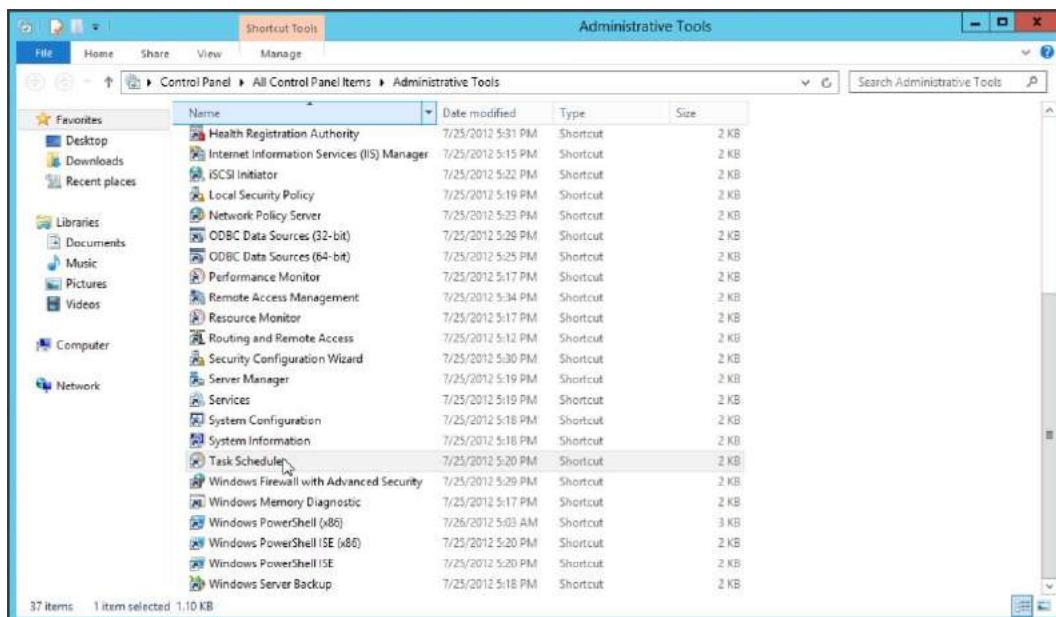
### 10.2.3 Construindo um EVENTO de login

Crie um agendamento no servidor Windows AD.

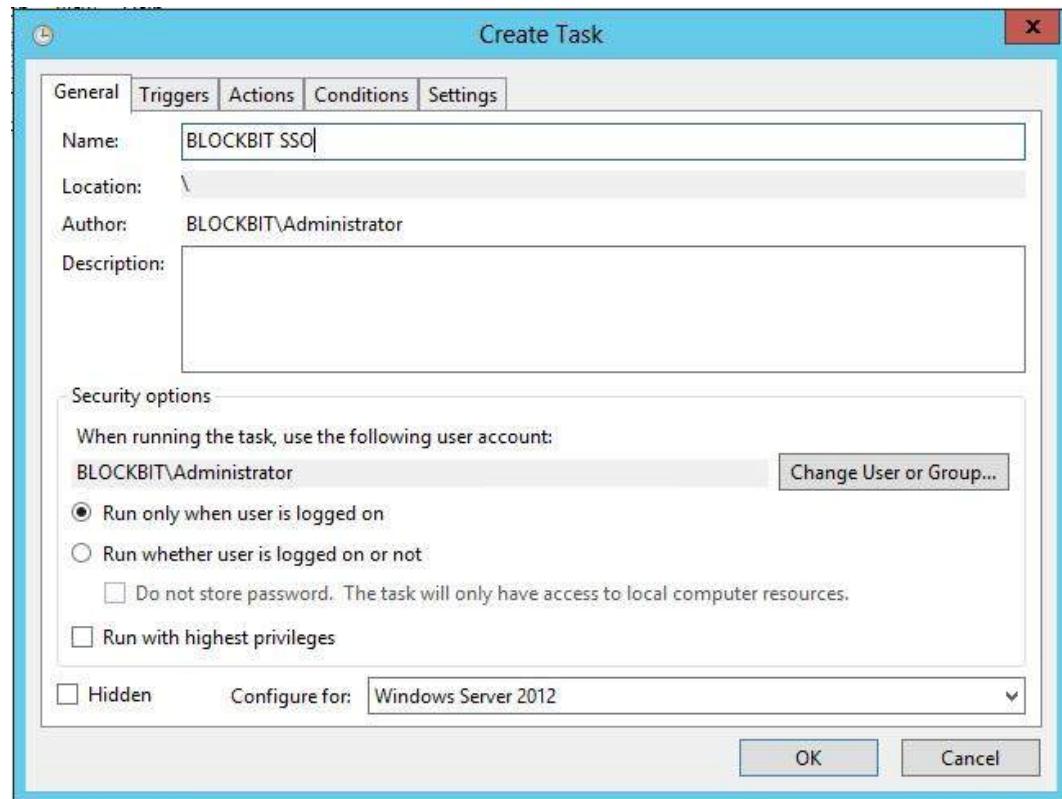
Abrir o gerenciador [Administrative Tools].



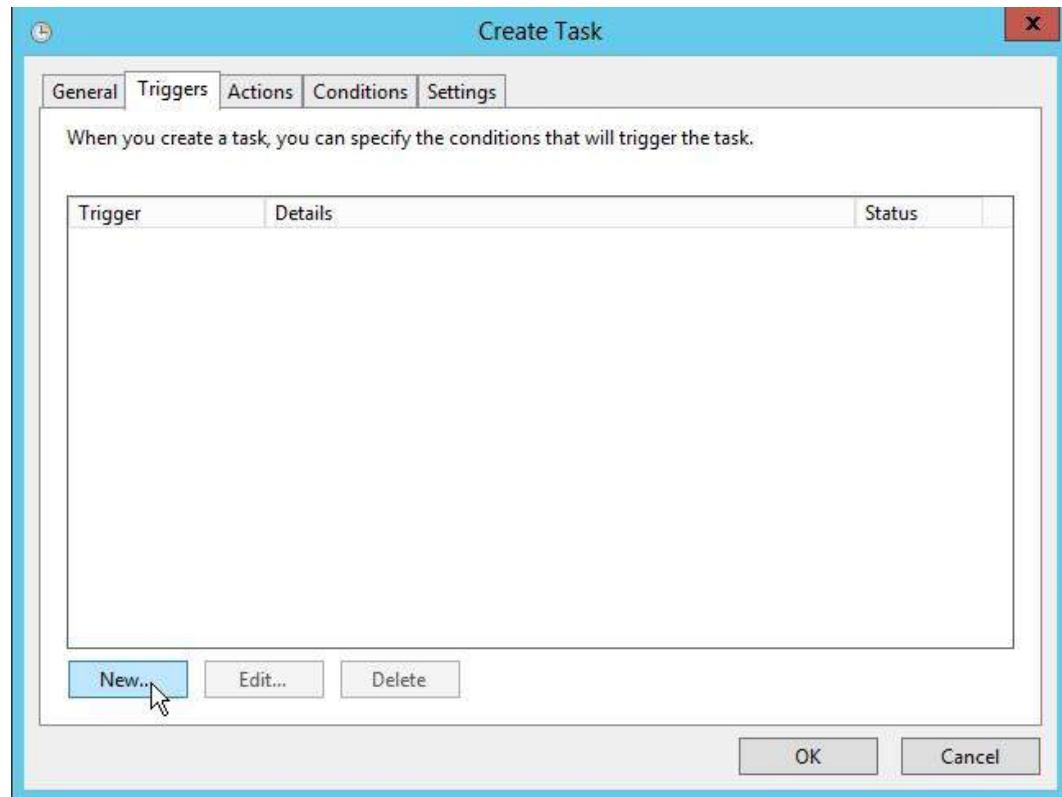
Clique em >> [Task Schedule]. Clique com o botão direito do mouse e depois clique em [Create task...]



Na aba [General] configure a tarefa de acordo com o exemplo abaixo, selecionando a versão correspondente do seu servidor Windows.

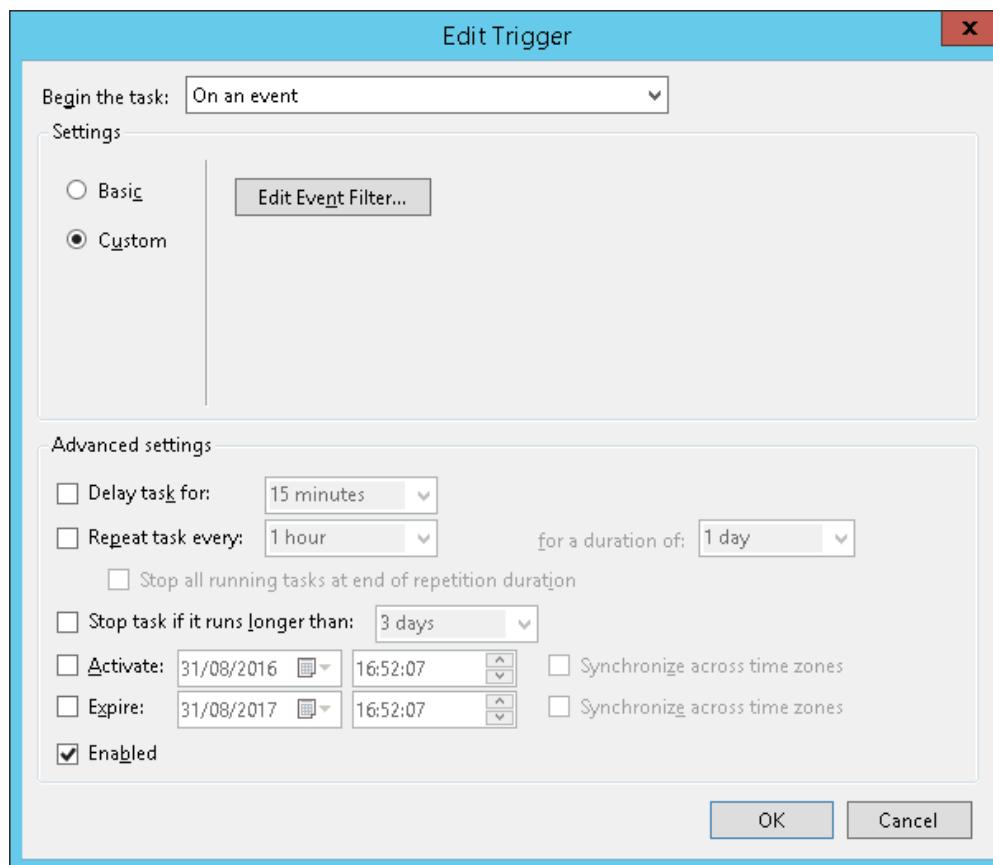


Na aba [Triggers] configure o agendamento para a execução: Clique em [New].



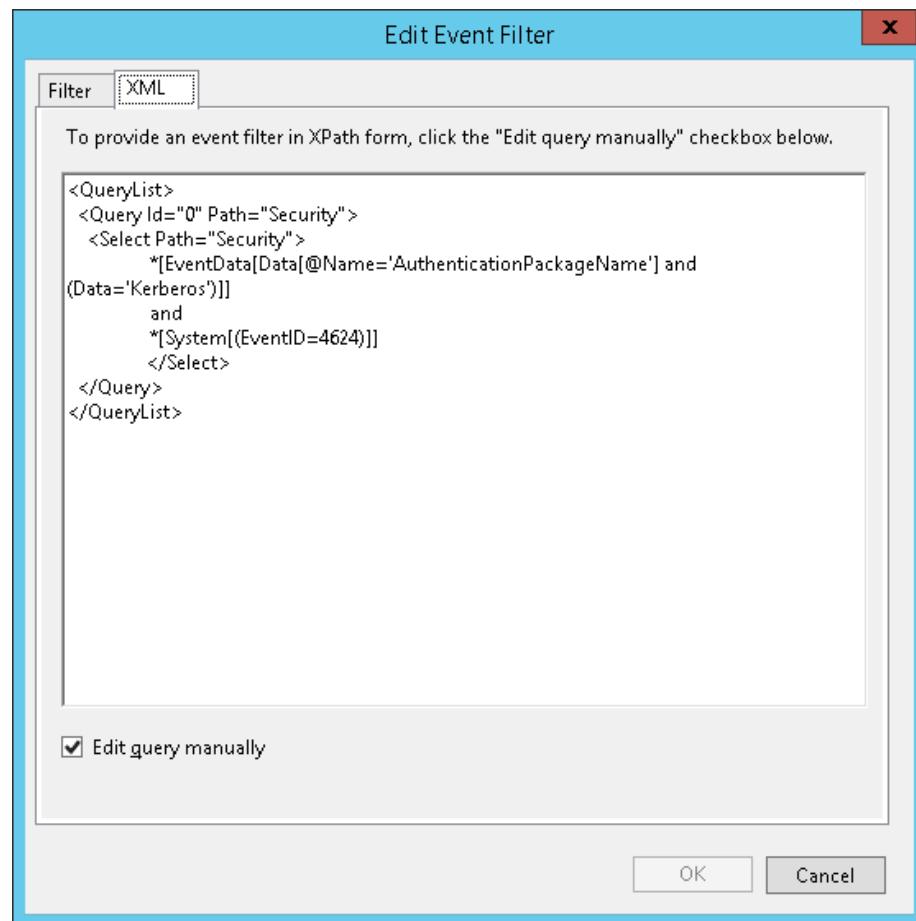
Selecione “**On an event**”. Configurando os itens de acordo com o exemplo abaixo.

Selecione “**Custom**” e clique em **[Edit Event Filter...]**

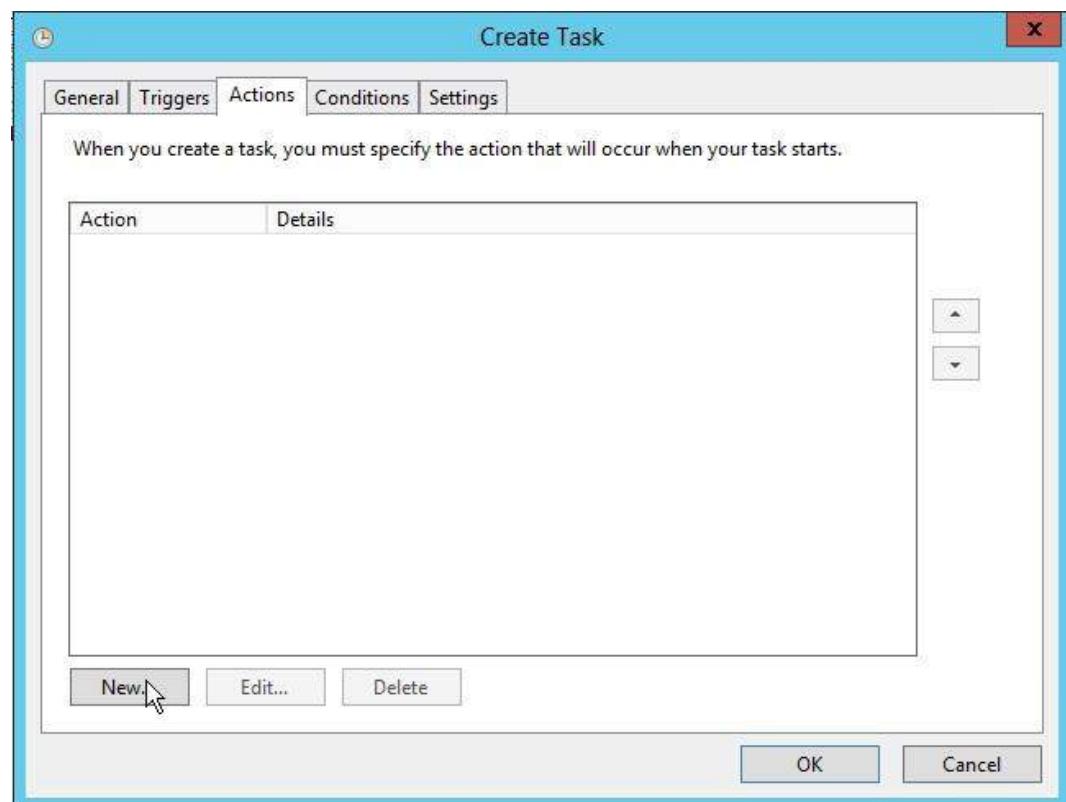


Na Aba **[XML]** adicione o conteúdo do texto abaixo, em seguida clique em **[ OK ]**:

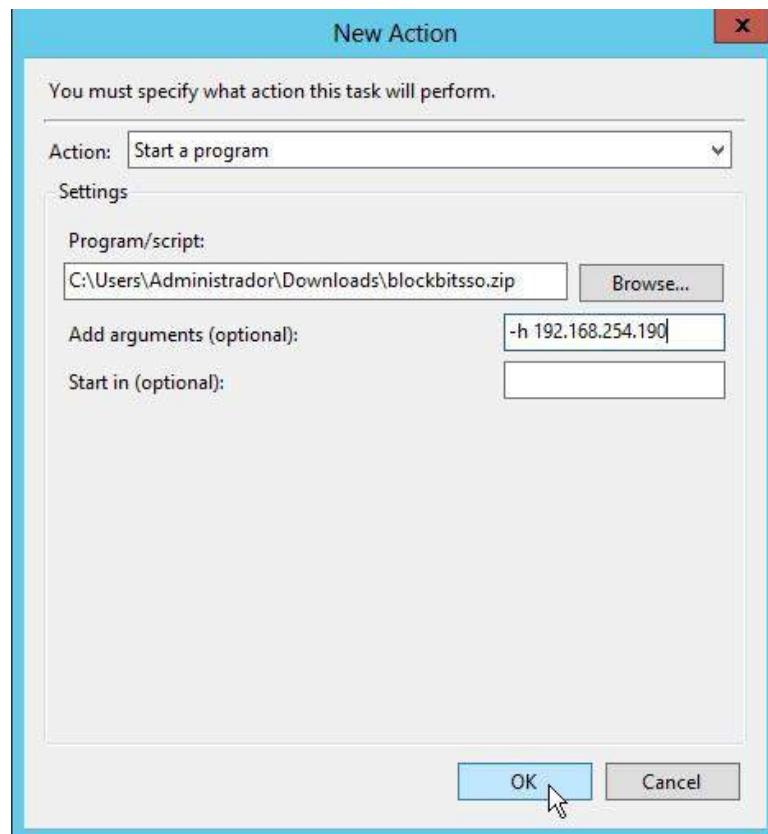
```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">
      *[EventData[Data[@Name='AuthenticationPackageName'] and
(Data='Kerberos')]]
      and
      *[System[(EventID=4624)]]
    </Select>
  </Query>
</QueryList>
```



Na aba **[Actions]** clique em **[New]**.

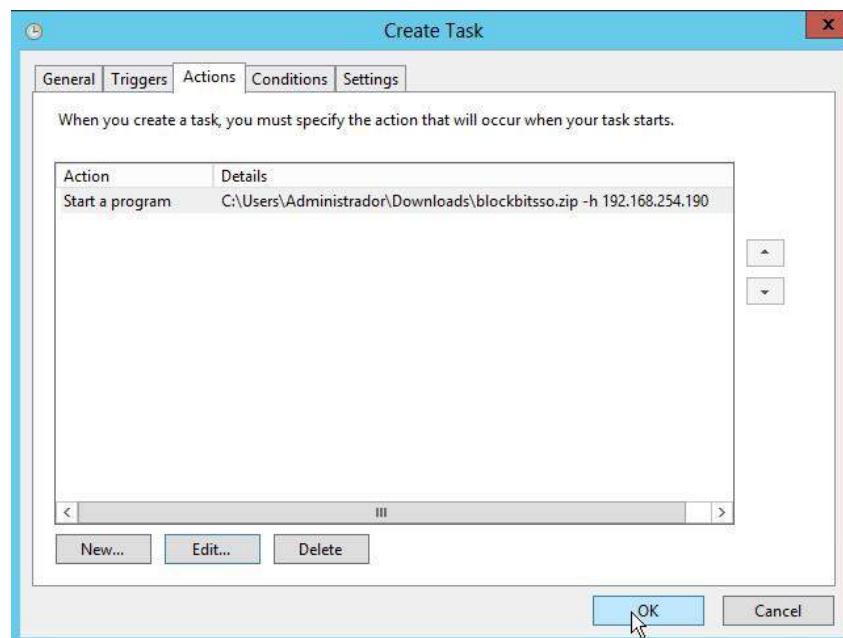


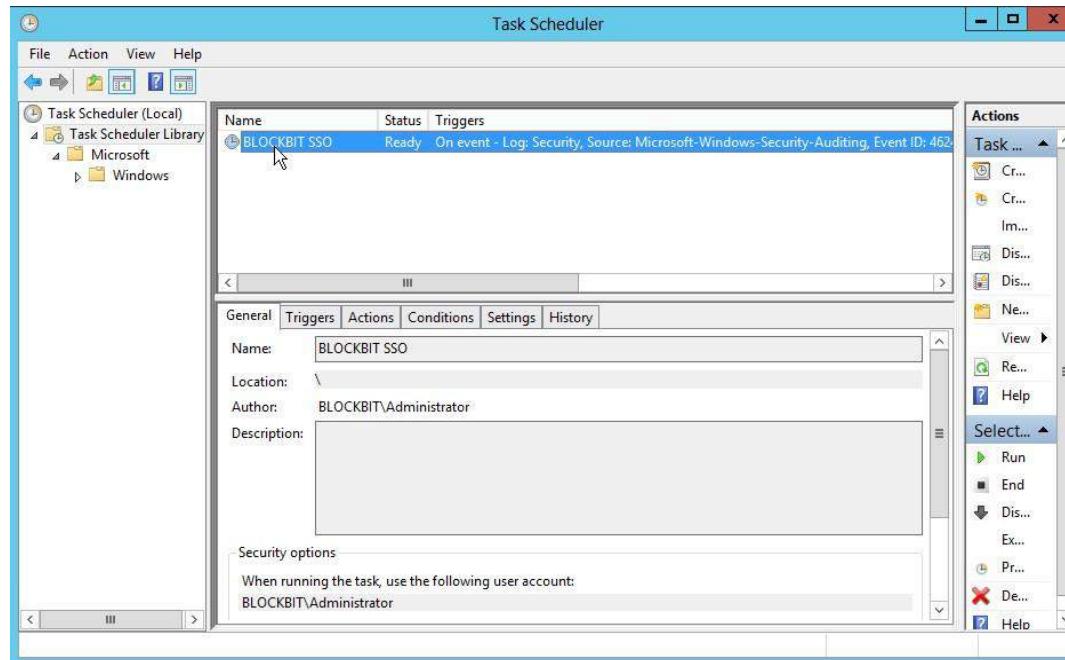
Configure a execução da tarefa, selecione: “**Start a program**”. E configure de acordo com o exemplo.



Clique em [Browse...] e localize a área de downloads onde salvou o agente SSO. Adicione em argumentos o “**endereço IP**” do servidor BLOCKBIT UTM para a integração do agente SSO de acordo com o exemplo: “*-h 192.168.254.190*”.

Depois clique em [ OK ] e [ OK ] para finalizar.





**FINALIZADO!** Agendamento de tarefas concluído.

**IMPORTANTE:** O processo de “*logon/logout*” é gerenciado por tempo de inatividade. Não requer nenhum controle do tipo “*keepAlive*”. O timeout de sessão é configurado no servidor BLOCKBIT UTM em:  
[Autenticação] >> [Políticas] >> Campo: [Timeout de sessão].

**ATENÇÃO:** O sistema mantém o login/privilégio da última autenticação, se um usuário se autenticar como “*user1*” e na sequencia acessar algum recurso da rede Windows como “*user2*”, exemplo um mapeamento de disco, a sessão de usuário válida no BLOCKBIT UTM passa a ser do “*user2*”.

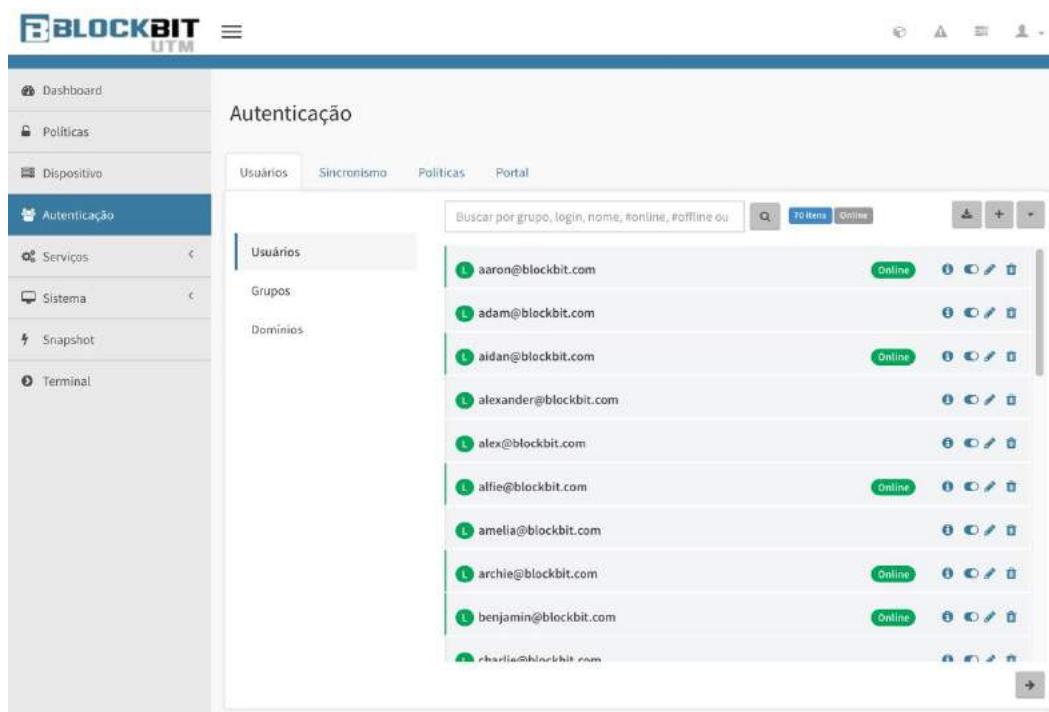
## 10.3 Gerenciando a Lista de Usuários

Clique em [Autenticação] >> [Usuários], aba [Usuários].

Neste item, o administrador pode “*Pesquisar*”, “*Importar*”, “*Adicionar*” ou “*Remover*” um usuário do sistema, definir de quais grupos que os mesmos participam. Inclusive habilitar ou desabilitar o usuário, o que implica diretamente na ação de login.

**IMPORTANTE:** Temos usuários do tipo “*Local*” e “*Remoto*”, e vale lembrar que a gerência dos usuários remotos é de responsabilidade do servidor de sincronismo “*Windows*” ou “*LDAP*”.

Para consultar a base de usuários, preencha o campo [**Buscar**] e clique em Pesquisar [].



The screenshot shows the BLOCKBIT UTM web interface. The left sidebar has a navigation menu with items like Dashboard, Políticas, Dispositivo, Autenticação (which is selected and highlighted in blue), Serviços, Sistema, Snapshot, and Terminal. The main content area is titled 'Autenticação' and contains four tabs: Usuários (selected), Sincronismo, Políticas, and Portal. The 'Usuários' tab displays a list of users with their email addresses and status (Online). Each user entry includes a small profile icon, the email, the status 'Online', and three icons for edit, delete, and other actions. There is also a search bar at the top of the list and a toolbar with various icons.

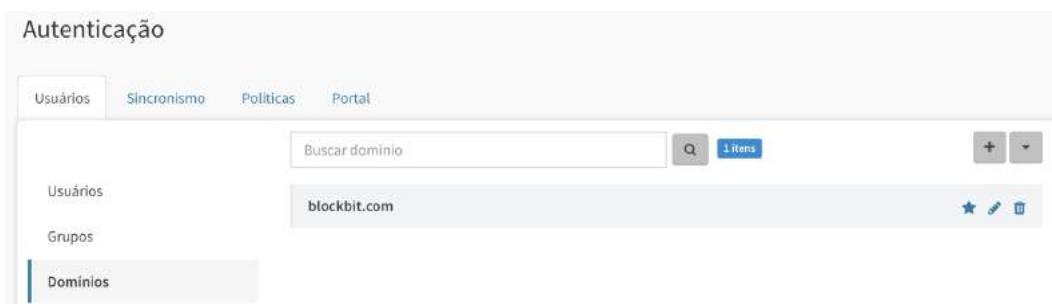
### 10.3.1 Adicionando Domínios e Grupos Locais

As ações **[Importar]** ou **[Adicionar]** usuários só são validos para domínios locais.

Para exemplificar vamos adicionar dois domínios do tipo local: “*local.net*” e “*guest*”, depois passamos para o processo de importação / adição de usuários.

#### Adicionando domínios “locais”

Para adicionar domínios, na aba **[Usuários]** clique em **[Domínios]**.



The screenshot shows the 'Autenticação' (Authentication) interface. At the top, there are tabs: 'Usuários', 'Sincronismo', 'Políticas', and 'Portal'. Below these tabs is a search bar with placeholder text 'Buscar domínio' and a search icon. To the right of the search bar is a button labeled '1 Itens'. Further to the right are three small icons: a star, a pencil, and a trash can. The main area is divided into sections: 'Usuários', 'Grupos', and 'Domínios'. The 'Domínios' section contains a single entry: 'blockbit.com'. Below the main area are three small icons: a star, a pencil, and a trash can.

Depois clique em **Adicionar** [+] depois clique em [ **Salvar** ].



The screenshot shows the 'Adicionar Domínio' (Add Domain) dialog box. It has two main sections: 'Dominio' and 'Validade das senhas'. In the 'Dominio' section, the input field contains 'local.net'. In the 'Validade das senhas' section, the input field contains '30' and the dropdown menu shows 'Dia(s)'. To the right of these fields are two checkboxes: 'Domínio padrão' (unchecked) and 'Senha forte' (checked). At the bottom right of the dialog box is a blue 'Salvar' (Save) button.



The screenshot shows the 'Adicionar Domínio' (Add Domain) dialog box again, this time for the 'guest' domain. The 'Dominio' input field contains 'guest'. In the 'Validade das senhas' section, the input field contains '7' and the dropdown menu shows 'Dia(s)'. To the right of these fields are two checkboxes: 'Domínio padrão' (unchecked) and 'Senha forte' (checked). At the bottom right of the dialog box is a blue 'Salvar' (Save) button.

### 10.3.2 Adicionando Grupos de Usuários para os Domínios Locais

Para os casos em que se utiliza “*domínios*” do tipo local, é recomendável para uma boa prática de administração definir também “*grupos*” de usuários de domínios, este recurso visa facilitar a gerência e definição das políticas de compliance que serão aplicadas posteriormente.

Para adicionar grupos, na aba [Usuários] clique em [Grupos].

Depois clique em **Adicionar** [+] depois clique em [ **Salvar** ].

**Adicionar Grupo**

<b>Nome</b>	<input type="text" value="financeiro"/>
<b>Domínio</b>	<input type="text" value="local.net"/> <input type="checkbox"/> Auto cadastro
<b>Usuários do domínio</b>	<input type="text" value=""/> <input type="button" value="Buscar"/> <input type="button" value=""/>
<input type="button" value="+"/> <input type="button" value="-"/>	
<b>Usuários do grupo</b>	<input type="text"/>
<b>Descrição</b>	<input type="text" value="Grupo Financeiro"/>
<input type="button" value="Salvar"/>	

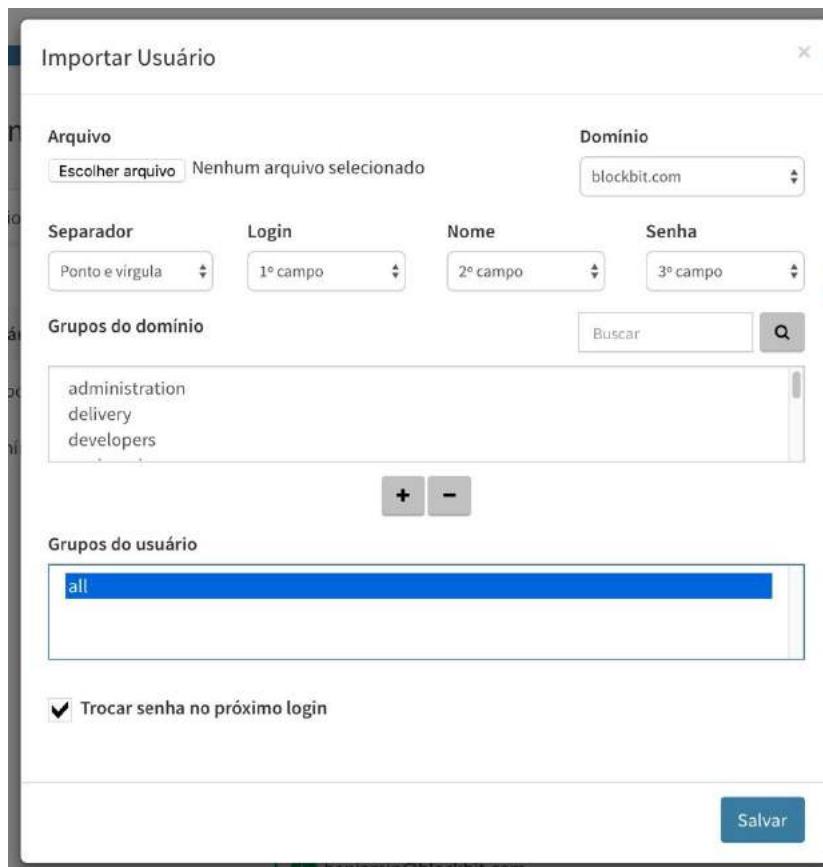
Para pesquisar os grupos recém-cadastrados, na interface de gerenciamento dos grupos, no campo **[Buscar]**, digite de acordo com os métodos de pesquisas permitidas e clique em **[ ]** para listar os grupos recém-cadastrados.

The screenshot shows the BLOCKBIT UTM web interface. The left sidebar has a navigation menu with items like Dashboard, Políticas, Dispositivo, Autenticação (which is selected and highlighted in blue), Serviços, Sistema, Snapshot, and Terminal. The main content area is titled 'Autenticação' and contains tabs for Usuários, Sincronismo, Políticas, and Portal. Under the 'Autenticação' tab, there are three sections: 'Usuários', 'Grupos', and 'Dominios'. The 'Grupos' section is currently active. It displays a table with two entries: 'financeiro@local.net' and 'usuarios@local.net'. Each entry has a small circular icon with a user symbol, followed by the email address, and then edit and delete icons.

### 10.3.3 Importando e Adicionando Usuários

Para realizar a importação de usuários clique na aba **[Usuários] >> [Usuários]**, depois clique no botão “**Importar**” [].

Esta interface permite o administrador importar os usuários a partir de um arquivo do tipo lista, com delimitadores de campo padrão (.csv). Preencha o formulário de acordo com o padrão do arquivo de importação, selecione o “**domínio**” correspondente e os “**grupos**” se houver, depois clique em [ **Salvar**].



The screenshot shows the 'Importar Usuário' (Import User) dialog box. In the 'Arquivo' (File) section, there is a 'Escolher arquivo' (Select file) button and a message 'Nenhum arquivo selecionado'. In the 'Dominio' (Domain) section, a dropdown menu is set to 'blockbit.com'. Under 'Separador' (Separator), 'Ponto e vírgula' (Comma and dot) is selected. For 'Login', 'Nome', and 'Senha', dropdown menus show '1º campo' (Field 1), '2º campo' (Field 2), and '3º campo' (Field 3) respectively. The 'Grupos do domínio' (Domain Groups) section contains a search bar and a list with 'administration', 'delivery', and 'developers'. Below it, a '+' and '-' button are visible. The 'Grupos do usuário' (User Groups) section has a list containing 'all', which is highlighted with a blue selection bar. At the bottom, a checked checkbox says 'Trocar senha no próximo login' (Change password at next login). A large blue 'Salvar' (Save) button is located at the bottom right.

**NOTA:** É comum em um processo de importação de usuários por lista, que se defina uma senha padrão para todos os usuários da lista. Por esse motivo é importante manter habilitada a opção “[v] Trocar senha no próximo login”

Após salvar o formulário de importação, a interface retorna com a lista de usuários já importados.

Para adicionar um usuário do tipo “local” clique em **Adicionar** [+] e preencha o formulário conforme o exemplo, depois clique em [Salvar].

**Adicionar Usuário**

<b>Nome</b> Antonio Silva	<input checked="" type="checkbox"/> Habilitado
<b>Login</b> asilva	<b>Domínio</b> local.net
<b>Senha</b> *****	<b>Confirma</b> *****
<b>Grupos do domínio</b> financeiro	
<b>Grupos do usuário</b> usuarios	
<b>Salvar</b>	

**BLOCKBIT UTM**

**Autenticação**

**Usuários**

usuárioss@blockbit.com	Online
asilva@local.net	Online

**NOTA:** Observe a lista de usuários, temos:

[ L ] significa que *este usuário* é do tipo local.

[ R ] significa que *este usuário* é do tipo remoto, sincronizado com uma base Windows ou LDAP.

[ Online ] significa que *este usuário* está com uma “sessão aberta”

[ Bloqueado ] significa que *este usuário* foi bloqueado por “exceder limite” na tentativa de acesso.

[ Expirado ] significa que a senha deste usuário expirou. No próximo “logon” será exigida a alteração da senha.

**NOTA:** Adicionar ou Importar usuários, não requer aplicar a fila de comandos.

O botão **Ações** [ ▾ ] retorna uma lista de outras ações permitidas na gerência de um usuário.



## 10.4 Adicionando Grupo de Auto Cadastro (Captive portal)

Existem casos em que o administrador precisa disponibilizar os recursos de rede e serviços de acesso a internet para usuários “itinerantes”, podemos classificar estes usuários como: “Usuários visitantes”.

Para o gerenciamento deste grupo de usuários “visitantes” o sistema permite adicionar “Grupos” a domínios do tipo “Local” e classificá-lo como um grupo “Auto cadastro”, habilitando a opção [v] “Auto Cadastro”. O modo Captive portal é usado para permitir o auto cadastro de um usuário, recomendado para usuários do tipo visitante.

Ainda conta com um recurso adicional o “Informações Pessoais” que solicita ao usuário visitante no momento do auto cadastro preencher um formulário com seus dados pessoais, o que garante ao administrador um registro de log pessoal para fins de auditoria.

Tudo isso com a finalidade de disponibilizar os recursos de acesso à internet, sem perder seu gerenciamento.

Para adicionar um grupo do tipo auto cadastro, clique na Aba **[Usuários] >> [Grupos]**, depois clique em **Adicionar** [+] depois clique em [Salvar].

The screenshot shows the 'Adicionar Grupo' (Add Group) dialog box. It has fields for 'Nome' (Name) containing 'visitantes', 'Dominio' (Domain) set to 'guest' with a checked 'Auto cadastro' checkbox, and sections for 'Usuários do domínio' (Domain users) and 'Usuários do grupo' (Group users), both currently empty. There is a 'Descrição' (Description) field with the text 'Grupo Visitantes - Auto Cadastro - Captive Portal'. At the bottom right is a blue 'Salvar' (Save) button.

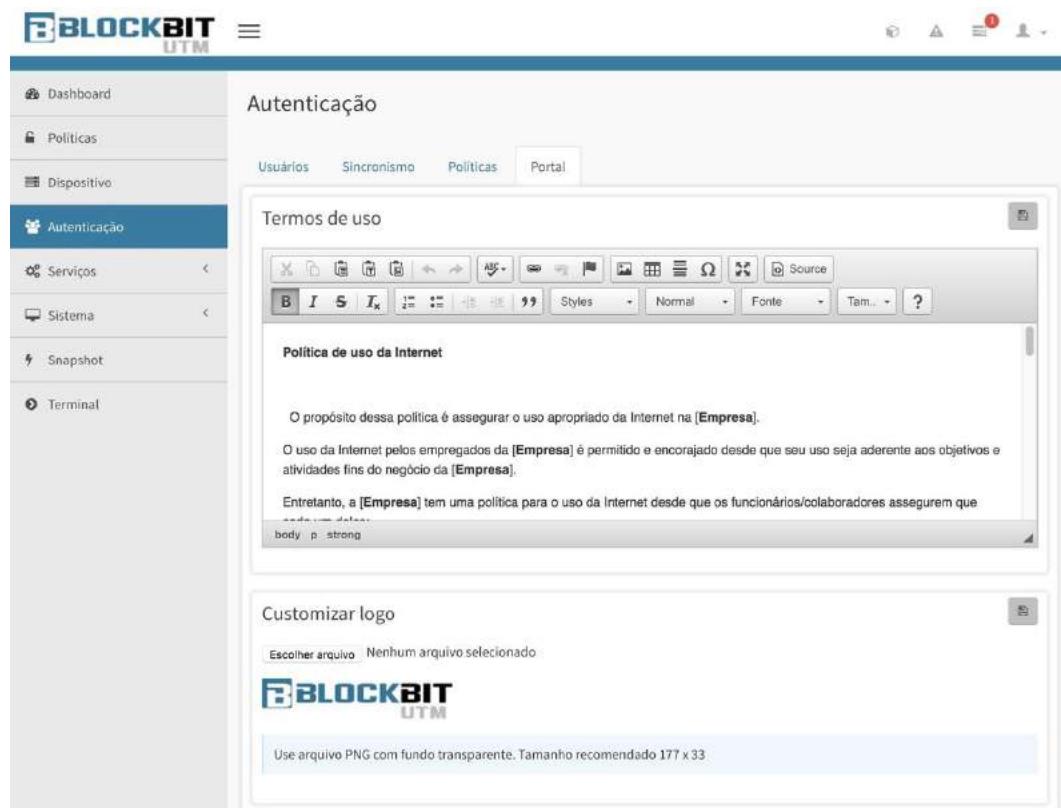
Temos um grupo do tipo auto cadastro associado ao domínio “*guest*”. Para atender as condições e recursos de gerenciamento que falamos acima, precisamos acessar a área de gerenciamento do portal de autenticação e definir um formulário de dados pessoais para preenchimento na ação do auto cadastro do usuário “*visitante*”.

## 10.5 Portal de Autenticação

O BLOCKBIT UTM conta com o portal de autenticação destinada ao serviço de logon do usuário na plataforma BLOCKBIT e servir também alguns outros recursos do sistema.

A interface de gerenciamento do portal no BLOCKBIT UTM permite ao administrador configurar uma “Página web com o *Termo de USO*” dos serviços de internet, customizar a “*Página de Logon*” com o *logotipo* da sua empresa, e ainda configurar um “Formulário de Dados Pessoais” para o serviço de auto cadastro do Captive portal para os usuários “*visitantes*”.

Para acessar a área de configuração do portal, clique em **[Autenticação]** vá para a Aba **[Portal]**



Para Adicionar um “*Termo de Uso*” basta acessar a área para edição do termo e inserir o respectivo texto, a interface de edição contempla recursos e serviços de formatação de texto e o administrador ainda pode inserir tags HTML. Após adicionar o “*Termo de Uso*”, clique [  ].

### [Customizar Logo]

Esta opção permite o administrador personalizar o logotipo inserido no portal de autenticação.

Basta clicar sobre o item **[Escolher arquivo]** e selecionar a respectiva imagem.

**NOTA:** Use o formato PNG com fundo transparente com tamanho 33 x 177

Depois clique [  ].



### [Informações Pessoais].

Esta opção permite ao administrador definir e criar um formulário de dados pessoais com a finalidade de registrar os usuários itinerantes. Este recurso visa criar um nível de proteção para sua corporação no âmbito de inquéritos judiciais nos quesitos de segurança da informação e no acesso a serviços WEB.

Para criar um formulário, você deve adicionar os campos que deseja para completar os dados pessoais do seu usuário itinerante.



Clique em **Adicionar** [  ]. Adicione os campos de acordo com os dados pessoais que deseja manter como registro dos usuários “visitantes”. Depois clique [  ].

Informações Pessoais			
Campo	Tipo	Caracteres	Linhas
Nome Completo	Texto (opcional)	55	1
Endereço	Texto (opcional)	60	2
Cidade	Texto (opcional)	30	1
Estado	Texto (opcional)	30	1
País	Texto (opcional)	30	1
CPF	Texto (opcional)	11	1

## 10.6 Captive Portal

A definição objetiva do Captive Portal é o “*Redirecionamento automático de autenticação*”. Este redirecionamento acontece para as políticas de segurança no acesso a qualquer serviço que exija autenticação. Toda vez que um usuário tentar usar algum recurso ou serviço, não autenticado, o sistema automaticamente o redireciona para o portal de autenticação.

### Aplicando um teste de logon.

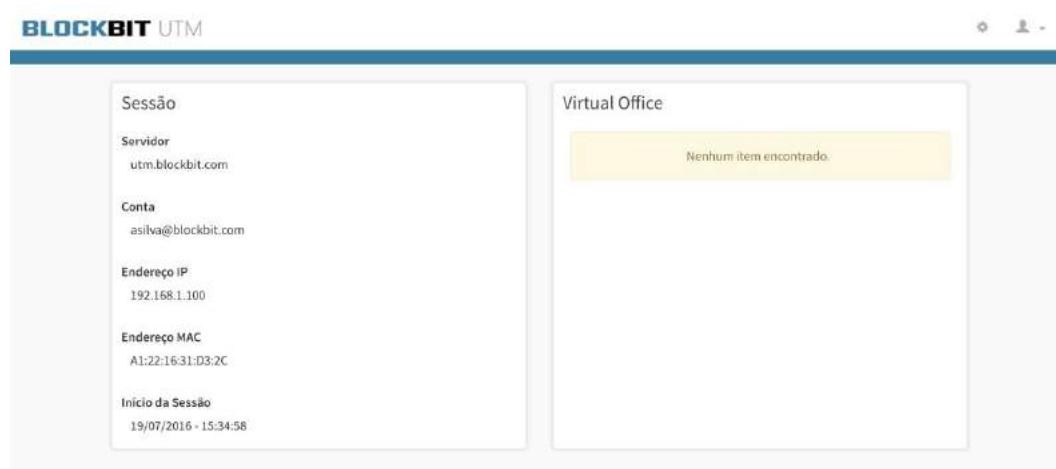
Para acesso ao portal de autenticação, digite:

Ex.: <https://utm.blockbit.com:9803> ou <https://192.168.1.1:9803>

Vamos fazer um acesso utilizando um usuário de autenticação do domínio padrão “*blockbit.com*” sincronizado com a base Windows AD



**NOTA:** O login dos usuários do domínio padrão, não requer digitar o “@domínio”.

**Interface do Portal de autenticação.**

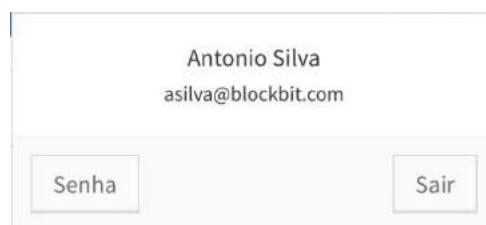
O portal de autenticação permite o usuário gerenciar alguns recursos da plataforma.

- Acessar o Termo de Uso.
- Fazer o download da CA (Certification Authority).
- Acessar relatórios personalizados.
- Alterar dados pessoais.
- Alterar senha.

Para ter acesso a esses recursos o usuário pode clicar em [ ]



Para trocar a senha [**Senha**] e desconectar da sessão [**Sair**] clique em [ ]



Na sessão do portal de autenticação a solução conta com o recurso “*Relatório*”. Este serviço de gerenciamento de relatórios estatísticos é permitido aos usuários com atribuição de receber através de agendamento um “*Link*” com os relatórios sumarizados referente ao tráfego de rede e utilização de recursos de outros usuários, que “*ele*” possa gerenciar.

Relatório sumarizado:

- Serviços utilizados.
- Categorias web acessadas.
- Categorias web bloqueadas.
- Incidência dos aplicativos utilizados detectados.

#### **Aplicando um cadastro de logon para os usuários “itinerantes”.**

Para os casos de usuários “*visitantes*”, ou seja, os usuários itinerantes ou não cadastrados, o portal de autenticação disponibiliza o recurso de Auto cadastro já mencionados em capítulos anteriores.

Toda vez que o usuário “*visitante*” tentar usar algum recurso ou serviço, não autenticado, o sistema automaticamente o redireciona para o portal de autenticação.

Após a exibição da interface basta clicar em **[Criar conta]**

<https://utm.blockbit.com:9803> ou <https://192.168.1.1:9803>



Criar conta

Domínio  
guest

Login

Nome

Senha

Confirma senha

Nome Completo  
limite de 55 caracteres

Endereço  
limite de 60 caracteres

Cidade  
limite de 30 caracteres

Estado  
limite de 30 caracteres

País  
limite de 30 caracteres

CPF  
limite de 11 caracteres



Agora que já temos o usuário “visitante” cadastrado, podemos fazer o teste de logon.



The screenshot shows the main dashboard of the BLOCKBIT UTM system. On the left, a sidebar titled 'Sessão' displays session details: 'Servidor' (Server) is set to 'utm.blockbit.com'. Under 'Conta' (Account), the email 'lsouza@guest' is listed. Below that, 'Endereço IP' (IP Address) is '192.168.1.100' and 'Endereço MAC' (MAC Address) is '08:21:61:33:3F:2C'. The 'Inicio da Sessão' (Session Start) is '19/07/2016 - 16:02:22'. On the right, a 'Virtual Office' section shows a message: 'Nenhum item encontrado.' (No items found).

**NOTA:** O login dos usuários dos domínios diferentes do domínio padrão, requer especificar “usuário@dominio”. Para validar sua autenticação.

[ **Online** ] significa que “este usuário” está com “sessão aberta”

O administrador pode remover a sessão aberta de qualquer usuário, basta clicar no botão [ **Online** ] e aplicar a ação **remover sessão** [  ].

Servidor	Data	IP	MAC	Ação
BLOCKBIT UTM	19/07/2016 - 16:02:22	192.168.1.100	81:10:61:13:31:1C	

## 11 Firewall

---

O Conceito de Firewall explica algumas ideias por trás dos seus componentes, técnicas e processos que estão envolvidos na construção, configuração e gestão de um firewall. O Firewall é um sistema que permite proteger os computadores de uma rede privada, das intrusões que provêm de uma rede pública, filtrando todos os pacotes que circulam na rede. Sua utilização é de extrema importância devido ao volume de tentativas de invasões a redes ou sistemas, identificados atualmente.

O Firewall opera no modo “*Stateful*” e dispõe de ferramentas que parametrizam os “*Níveis de segurança*” e os “*Controle das conexões*”, além das políticas de “*Filtros de Pacotes*” e “*Redirecionamento – DNAT*”.

O serviço é pré-configurado para permitir acesso aos serviços locais do BLOCKBIT UTM.

A interface é dividida em:

### [Serviços]

Habilitação e configuração das portas e serviços locais do BLOCKBIT UTM.

### [Parâmetros de Segurança]

Configuração dos parâmetros de segurança e controles de conexão do firewall.

### [Política Padrão]

Definição da Política Padrão “*Permitir Tudo*”.

Configurada e pré-estabelecida pelo sistema para permitir o mascaramento (NAT) da rede local (LAN) para a internet (WAN).

### [Zone Protection]

Configuração e permissões de acesso aos serviços UTM quando requer uma política de acesso específica.

### [Redirecionamentos (DNAT)]

Configurações e permissões de mascaramento e redirecionamento de tráfego entre os barramentos. Consiste em modificar o endereço de destino das máquinas clientes. O “*Destination Nat*” é muito usado para fazer redirecionamento de portas.

Abaixo a lista de serviços locais do BLOCKBIT UTM e suas respectivas portas/protocolos.

### Serviços Porta/ Protocolo

**Autenticação** 9803 /TCP

**Administração** 98 /TCP

**DNS** 53 /TCP  
53 /UDP

**DHCP** 67 /UDP

**VPN IPSEC** NAT-T/ 4500(UDP)  
ISAKMP/ 500(UDP)  
Protocolo ESP (50)  
Protocolo GRE(47)

**VPN SSL** 922 /TCP

**WebProxy** 128 /TCP

## 11.1 Serviços

O item “*Serviços*” vem pré-configurado e permitindo o acesso aos serviços UTM para as redes locais, definida e representada pela zona de rede **[LAN]**.

Para configuração dos serviços UTM acesse o menu **[Serviços] >> [Firewall] >>** quadro **[Serviços]**.

O administrador tem a opção de alterar o perfil padrão de permissão de acesso para qualquer um dos serviços locais, sejam as zonas de rede: **[DMZ], [LAN] e [WAN]** e/ ou a habilitação da opção **[V] [Autenticado]**, ou mesmo “Desabilitar” o serviço.

Serviços	
Autenticação	
Administração	
DNS	
DHCP	
VPN	
VPN SSL	
Web Proxy	

O Administrador tem a opção de clicar em **Editar** [] e alterar as permissões pré-estabelecidas pelo sistema.

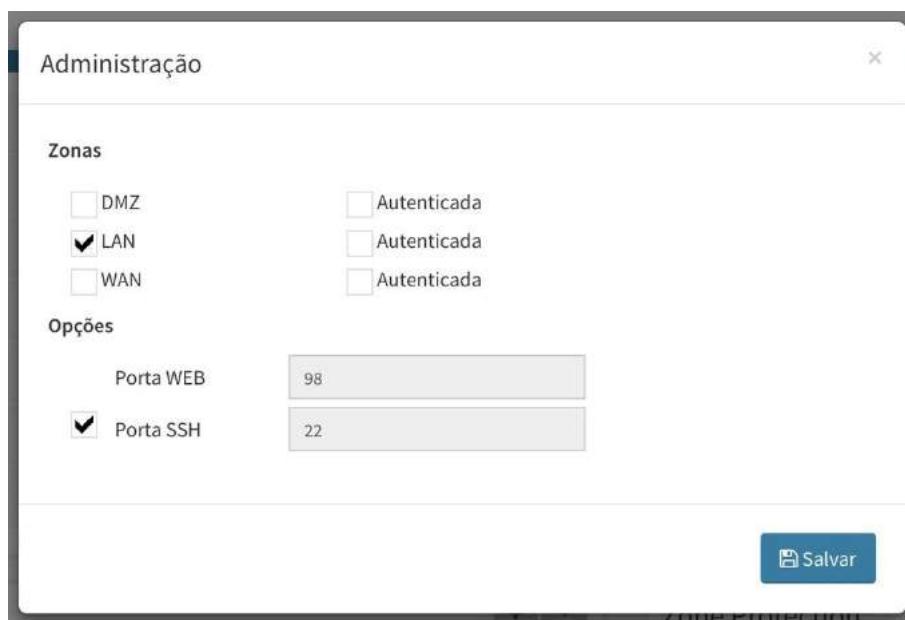
### 11.1.1 Autenticação

Permite configurar as zonas com permissão de acesso ao Captive Portal / Portal de Autenticação e a porta utilizada.



### 11.1.2 Administração

Permite configurar as zonas com permissão de acesso a interface de administração web e SSH, se é necessário estar autenticado e quais portas utilizar.



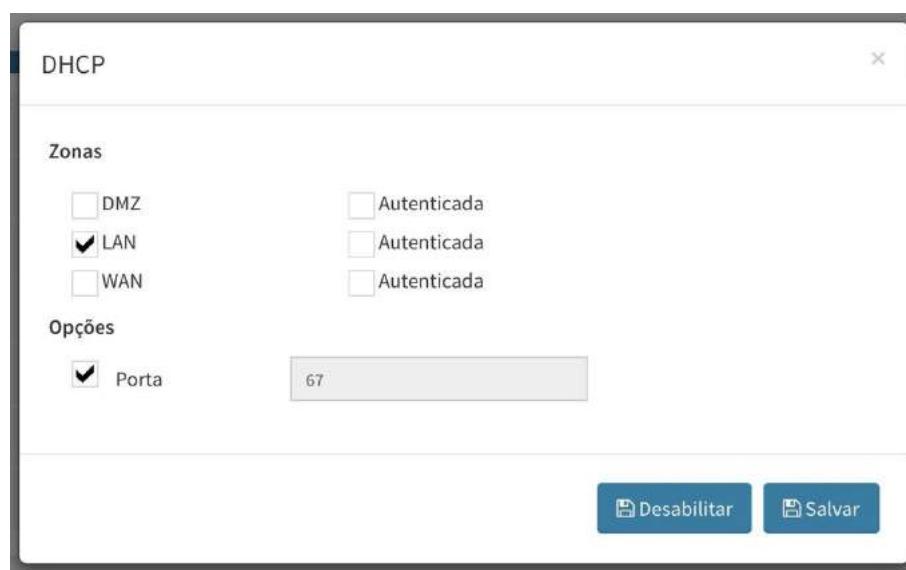
### 11.1.3 DNS

Permite configurar as zonas com permissão de acesso ao serviço DNS, se é necessário estar autenticado e quais portas utilizar.



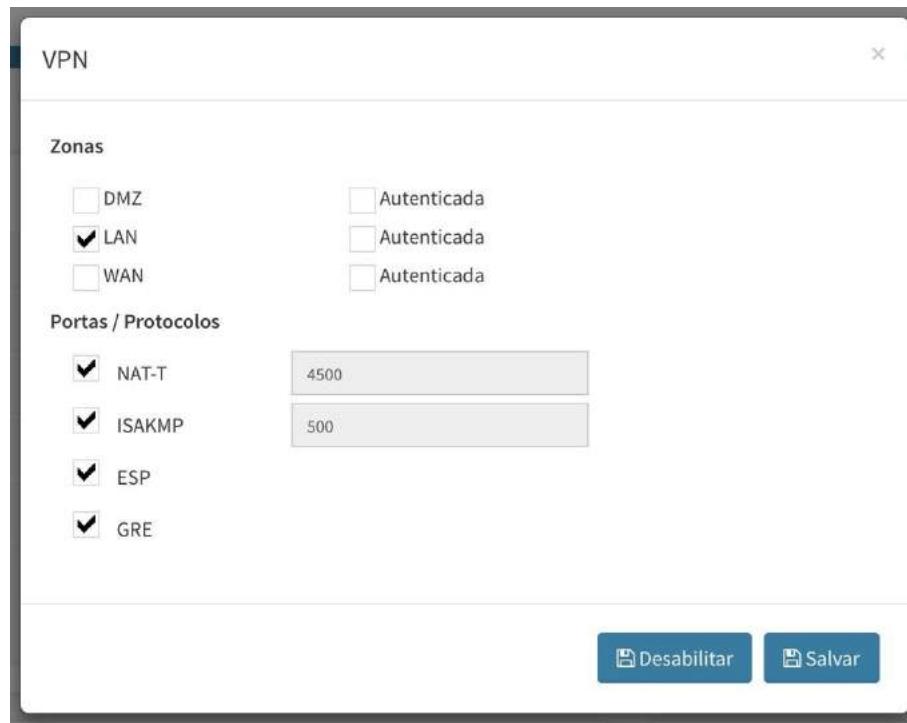
### 11.1.4 DHCP

Permite configurar as zonas com permissão de acesso ao serviço DHCP, se é necessário estar autenticado e qual porta utilizar.



### 11.1.5 VPN

Permite configurar as zonas com permissão de acesso ao serviço VPN, se é necessário estar autenticado e quais portas utilizar.



### 11.1.6 VPN SSL

Permite configurar as zonas com permissão de acesso ao serviço DHCP, se é necessário estar autenticado e qual porta utilizar.



### 11.1.7 Web Proxy

Permite configurar as zonas com permissão de acesso ao serviço Web Proxy e qual porta utilizar em caso de proxy ativo.



**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 11.2 Parâmetros de Segurança

Neste item temos as configurações de segurança do Firewall, este recurso suporta a configuração de controles gerais de segurança e que possuem valores padrões de habilitação sugeridos para os recursos dos controles de conexão, responsável em manter as informações do estado de todas as conexões e sessões do Firewall.

Acesse o menu **[Serviços] >> [Firewall] >>** quadro **[Parâmetros de Segurança]**.

The screenshot shows a configuration window titled 'Parâmetros de Segurança'. It lists various security features with their current status (checked or unchecked) and some numerical values. The features include:

Configuração	Status
Proteção DOS	<input checked="" type="checkbox"/> Habilitado
Proteção DOS limit	2000
Proteção DOS burst	5000
Proteção PortScan	<input checked="" type="checkbox"/> Habilitado
Proteção Pacotes Inválidos	<input checked="" type="checkbox"/> Habilitado
Proteção SYN flood	<input type="checkbox"/> Habilitado
Proteção ICMP flood	<input checked="" type="checkbox"/> Habilitado
Permite Ping	<input checked="" type="checkbox"/> Habilitado
Permite ICMP Redirect	<input checked="" type="checkbox"/> Habilitado
Ignorar ICMP Broadcast	<input type="checkbox"/> Habilitado
Source routing	<input type="checkbox"/> Habilitado

Detalhando alguns dos itens de configurações de segurança.

### 11.2.1 Proteção DOS

Este recurso permite o bloqueio contra ataques de negação de serviço (também conhecido como Denial of Service - DoS), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Recomendação: “[Habilitar]”.

### 11.2.2 Proteção PortScan

Este recurso permite identificação e o bloqueio de conexões com o objetivo de mapear as portas TCP e UDP. Aplicativos PortScan tentam identificar o status das portas, se estão fechadas, escutando ou abertas. Geralmente, os port scanners são utilizados por pessoas mal-intencionadas para identificar portas abertas, explorar vulnerabilidades e planejar invasões.

Recomendação: “[Habilitar]”.

### 11.2.3 Proteção Pacotes Inválidos

São considerados pacotes inválidos os que não respeitam o padrão do diagrama de estado TCP (handshake). O serviço de firewall descarta os pacotes considerados inválidos.

Recomendação: “[Habilitar]”.

### 11.2.4 Proteção SYN flood

Este recurso permite o bloqueio contra ataques de negação de serviço (também conhecido como Denial of Service - DoS), na qual o atacante envia uma sequência de requisições SYN para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação.

Recomendação: “[Habilitar]”.

### 11.2.5 Proteção ICMP flood

Habilitar este recurso garante o controle de conexões do tipo ICMP. Limitando o número de pacotes que podem ser enviados por um modelo simples de ataque onde o invasor basicamente envia um grande número de “pedidos ICMP Echo” conhecido como ping da morte.

Recomendação: “[Habilitar]”.

### 11.2.6 Permite ICMP Redirect

Este recurso é um tipo de mensagem utilizada por roteadores para notificar hosts do mesmo segmento de rede, que existe um caminho (rota) melhor para um determinado destino.

Recomendação: “[Desabilitar]”.

**Importante:** Este item vem com padrão [Habilitado] por identificação de inúmeras estruturas de rede mal definidas.

### 11.2.7 Ignorar ICMP Broadcast

Esse recurso ignora o tráfego ICMP Broadcast, usado para fazer com que servidores participem involuntariamente de ataques DOS, enviando grande quantidade de pings aumentando exponencialmente o tráfego NETBIOS da rede e tornando os serviços reais indisponíveis.

Recomendação: “[Habilitar]”.

### 11.2.8 Source Routing

Este recurso permite aplicar testes de roteamento atrás do firewall, permitem ao emissor do pacote especificar o caminho de ida e volta do pacote.

Recomendação: “[Desabilitado]”.

Os demais recursos pré-configurados referente os itens das “Configurações de conexões” desta interface referem-se aos parâmetros de controle das conexões, a alteração destes valores implica diretamente no resultado de desempenho do servidor.

### 11.3 Política Padrão

A solução contempla uma política padrão pré configurada para “*Permitir tudo da lan para a wan*”. Essa política visa a implementação básica no acesso aos serviços públicos da internet.

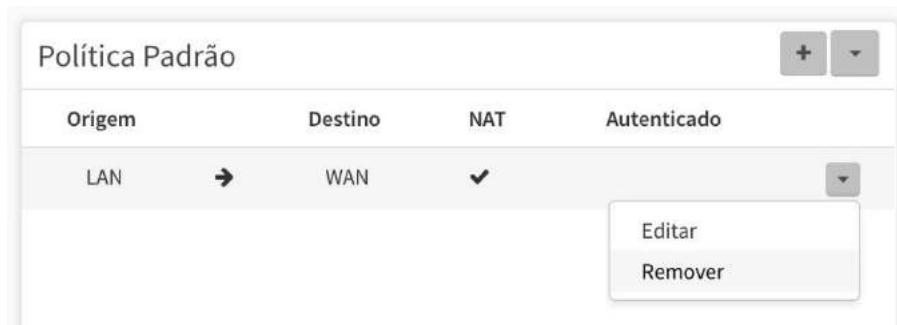
A implementação ÚNICA e EXCLUSIVA da política padrão não caracteriza que seu ambiente esteja com a melhor política implementada.

A política padrão tem como finalidade única, auxiliar a fase inicial de implementação e não tem intenção nenhuma de se propor como uma política final.

**IMPORTANTE:** A política padrão é aplicada somente após a verificação das políticas de compliance, (Ver [Seção 24 – Políticas de compliance](#)) ou seja, somente para o tráfego que não atenda ou não se enquadre nas regras de conformidade salvas no item **[Políticas]**.

Para visualizar, alterar ou desabilitar a política padrão, acesse o menu **[Serviços] >> [Firewall] >> quadro [Política Padrão]**.

No quadro **[Política Padrão]**, clique no botão de ação [▼]



Selezione **[Remover]** essa ação altera a política padrão do sistema para “*Proibir Tudo*”.



## 11.4 Zone Protection

Esta opção permite ao administrador configurar as permissões de acesso aos serviços do BLOCKBIT UTM quando requer uma política de entrada específica. Permite especificar “Zona de rede”, “IP de origem”, “IP de destino”, “horário”, “Usuários” e “Grupos”, inclusive com a opção de inspecionar o tráfego.

Acesse o menu **[Serviços] >> [Firewall] >>** quadro **[Zone Protection]**.

Zone Protection			
Serviço	Ação	Zona	Autenticado
SNMP	Allow	LAN	

Para adicionar uma política de entrada específica clique em **Adicionar** [+] uma nova política, configure de acordo com os campos e depois clique em [  Salvar ].

Zone Protection

**Política**

Habilitedo

**Condições**

Zona: WAN | Ação: Allow

Serviço: BLOCKBIT-ADMIN

Descrição: Acesso a interface administrativa

 Salvar

Zone Protection

Política

Condições

Autenticado

Usuários  
Adicionar tag

Grupos  
suporte@blockbit.com  Adicionar tag

IP de origem  
Adicionar tag

IP de destino  
IP eth1 BLOCKBIT UTM  Adicionar tag

Horário  
Selecione

Zone Protection

Serviço	Ação	Zona	Autenticado		
BLOCKBIT-ADMIN	Allow	WAN	<input checked="" type="checkbox"/>	<input type="button" value=""/>	<input type="button" value=""/>
SNMP	Allow	LAN		<input type="button" value=""/>	<input type="button" value=""/>

**IMPORTANTE:** As configurações de entrada para os serviços BLOCKBIT UTM no item **[Zone Protection]** visa melhorar os níveis de segurança no acesso aos serviços e recursos do firewall.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 11.5 Redirecionamentos (DNAT)

Neste item configuramos as permissões de mascaramento e redirecionamento de tráfego entre os barramentos. São regras de filtros de pacotes com a opção de tradução de endereços. Consiste em modificar o endereço de destino das máquinas clientes. O “Destination Nat” é muito usado para fazer redirecionamento de portas.

Acesse o menu **[Serviços] >> [Firewall] >>** quadro **[Redirecionamentos DNAT]**.

Redirecionamentos (DNAT)			
Descrição	Origem	Serviço	Destino
Nenhum item encontrado			

Para adicionar uma política de DNAT clique em **Adicionar** [].

A seguir vamos mostrar exemplos de políticas de redirecionamento.

### 11.5.1 Exemplo - Acesso Remoto ao Servidor de Câmeras

Este exemplo mostra o acesso à um servidor de câmeras e será liberado a partir da configuração de 3 políticas específicas.

*Política 1: Redirecionamento do acesso as portas do range - UDP 4500:5550.*

*Política 2: Redirecionamento do acesso a porta http – TCP 80.*

*Política 3: Redirecionamento do acesso a porta https – TCP 443.*

<b>IP Remoto</b>	199.99.99.99
<b>Portas</b>	UDP 4500:5500 TCP 80 (http) TCP 443 (https)
<b>IP Local</b>	192.168.254.174

**Política 1:**

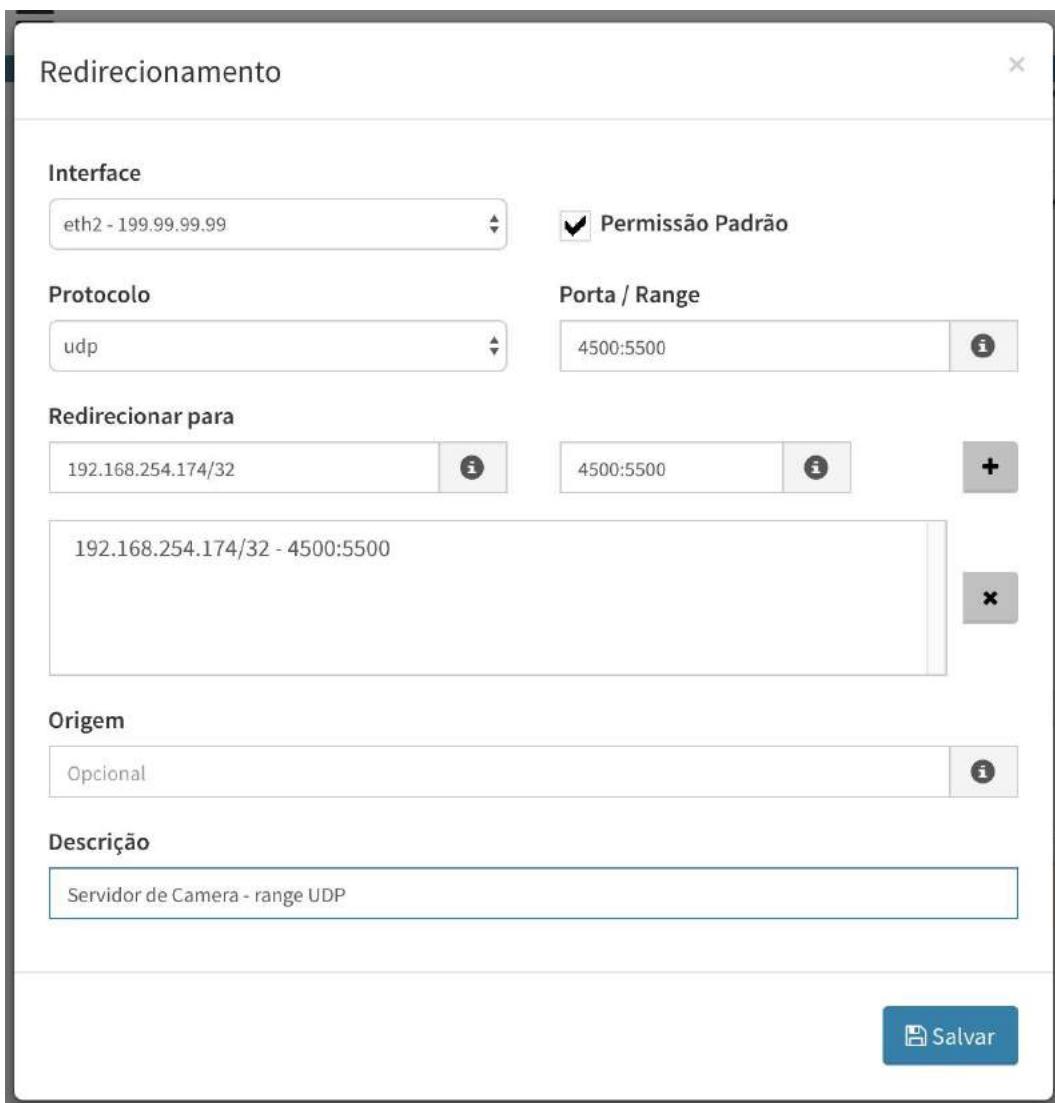
No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo. Depois clique em [  Salvar ].

“Interface – eth2 → 199.99.99.99”

“Protocolo – udp – Porta / Range → 4500:5500”;

“Redirecionar para → 192.168.254.174/32”;

“Descrição → Servidor de Câmera – range UDP”.



The screenshot shows the 'Redirecionamento' configuration window. It includes fields for Interface (set to 'eth2 - 199.99.99.99'), Protocol (set to 'udp'), and Porta / Range (set to '4500:5500'). The 'Permissão Padrão' checkbox is checked. The 'Redirecionar para' section contains two entries: '192.168.254.174/32' and '4500:5500'. A description field at the bottom is filled with 'Servidor de Camera - range UDP'. A blue 'Salvar' button is located at the bottom right.

**Política 2:**

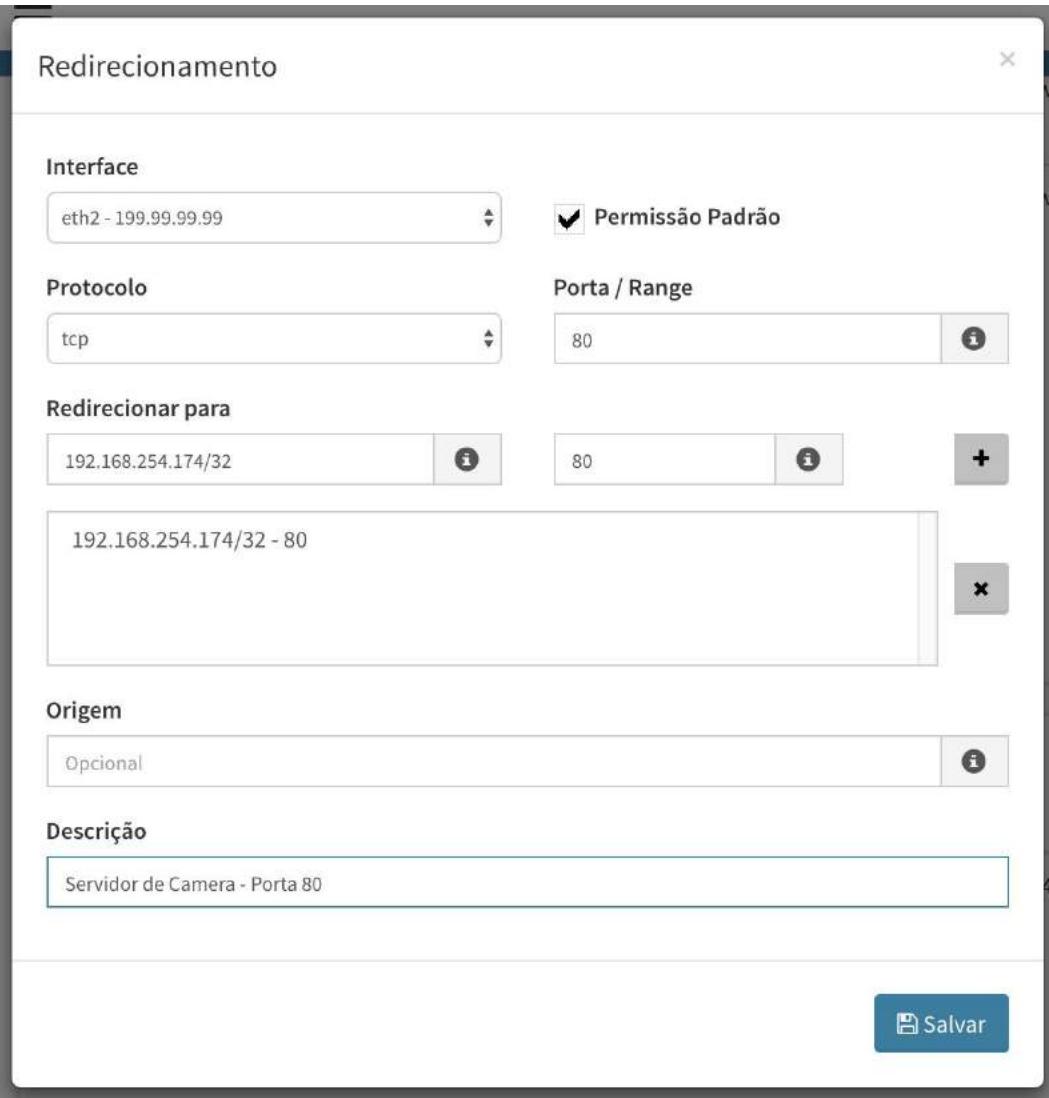
No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo. Depois clique em [  ].

“Interface – eth2 → 199.99.99.99”

“Protocolo – TCP – Porta / Range → 80”;

“Redirecionar para → 192.168.254.174/32 → 80”;

“Descrição: Servidor de Câmera – Porta 80”.



The screenshot shows the 'Redirecionamento' configuration dialog box. It contains the following fields:

- Interface:** eth2 - 199.99.99.99
- Protocolo:** tcp
- Porta / Range:** 80
- Redirecionar para:** 192.168.254.174/32 - 80
- Origem:** Opcional
- Descrição:** Servidor de Camera - Porta 80

A blue 'Salvar' (Save) button is located at the bottom right of the dialog box.

**Política 3:**

No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo. Depois clique em [  Salvar ].

“Interface – eth2 → 199.99.99.99”

“Protocolo – TCP – Porta / Range → 443”;

“Redirecionar para → 192.168.254.174/32 → 443”;

“Descrição: Servidor de Câmera – Porta 443”.

### Redirecionamento

**Interface**

eth2 - 199.99.99.99  Permissão Padrão

**Protocolo**

tcp **Porta / Range**

443

**Redirecionar para**

192.168.254.174/32 443

192.168.254.174/32 - 443

**Origem**

Opcional

**Descrição**

Servidor de Camera - Porta 443

 Salvar

No final da configuração o administrador precisa habilitar as políticas cadastradas, clique em **habilitar** [  ] cada política respectivamente.

Redirecionamentos (DNAT)				
Descrição	Origem	Serviço	Destino	
## Servidor de Camera - Porta 443	Todos	199.99.99.99 - 443/tcp	→ 192.168.254.174 - 443/tcp	[  ]
## Servidor de Camera - Porta 80	Todos	199.99.99.99 - 80/tcp	→ 192.168.254.174 - 80/tcp	[  ]
## Servidor de Camera - range UDP	Todos	199.99.99.99 - 4500:5500/udp	→ 192.168.254.174 - 4500:5500/udp	[  ]

### 11.5.2 Exemplo - Acesso ao Servidor WEB – Extranet

Este exemplo mostra como configurar o acesso ao servidor WEB (Extranet) será liberado a partir da configuração de uma política específica.

---

**IP Remoto** 199.99.99.90

---

**Porta** 443 (TCP)

---

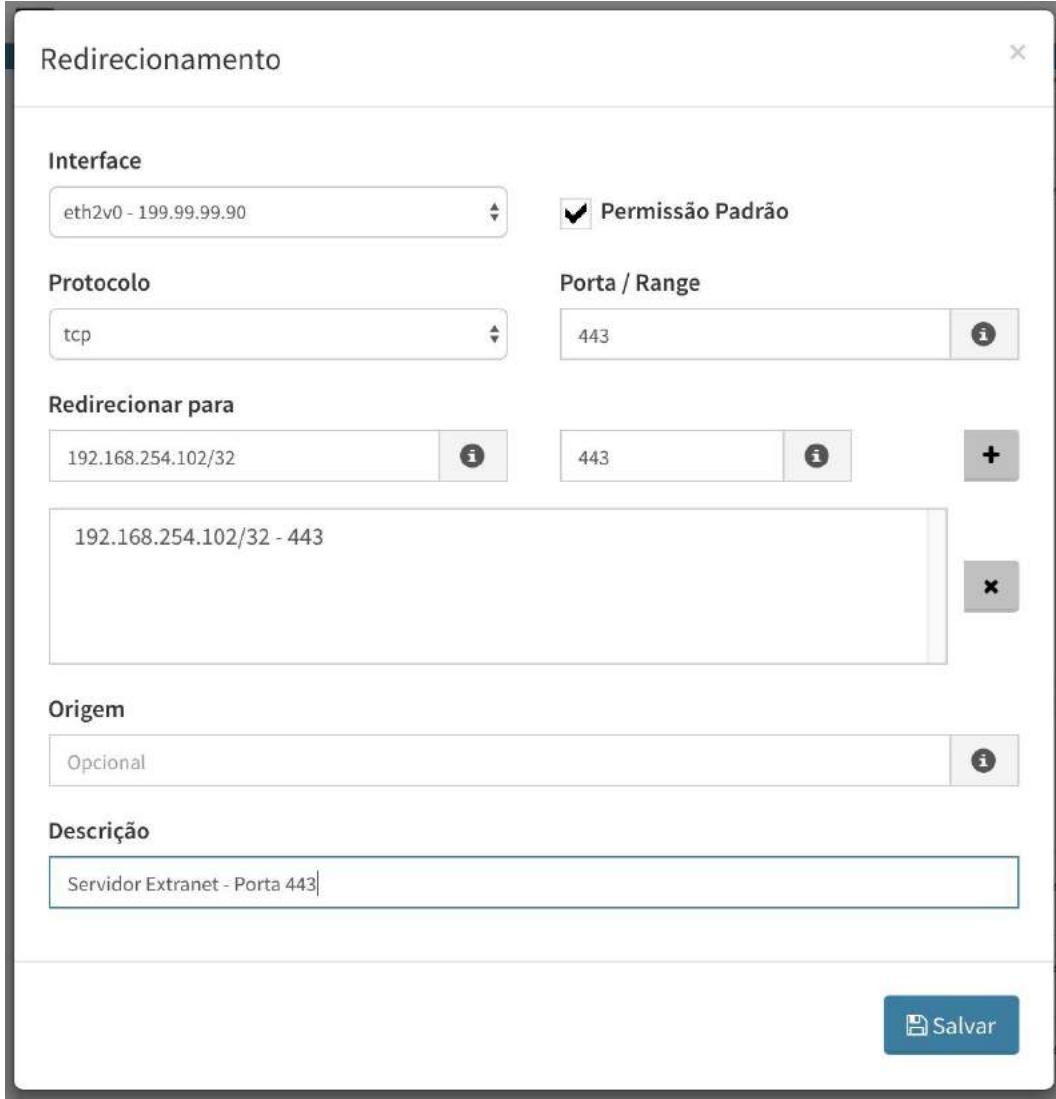
**IP Local** 192.168.254.102

---

**Política 4:**

No acesso ao formulário de configuração, vamos preencher os campos de acordo com as especificações definidas na política exemplo. Depois clique em [  Salvar ].

“Interface – eth2v0 → 199.99.99.90”  
“Protocolo – TCP – Porta / Range → 443”;  
“Redirecionar para → 192.168.254.102/32 → 443”;  
“Descrição: Servidor Extranet – Porta 443”.



The screenshot shows the 'Redirecionamento' configuration screen. It includes fields for Interface (set to 'eth2v0 - 199.99.99.90'), Protocol (set to 'tcp'), Porta / Range (set to '443'), Redirecionar para (set to '192.168.254.102/32 - 443'), Origem (set to 'Opcional'), and Descrição (set to 'Servidor Extranet - Porta 443'). A 'Permissão Padrão' checkbox is checked. A 'Salvar' button is visible at the bottom right.

No final da configuração não esquecer de habilitar a política cadastrada, clique em **habilitar** [  ] política.

Redirecionamentos (DNAT)			
Descrição	Origem	Serviço	Destino
■ Servidor Extranet - Porta 443	Todos	199.99.99.90 - 443/tcp	➔ 192.168.254.102 - 443/tcp
■ Servidor de Camera - Porta 443	Todos	199.99.99.99 - 443/tcp	➔ 192.168.254.174 - 443/tcp
■ Servidor de Camera - Porta 80	Todos	199.99.99.99 - 80/tcp	➔ 192.168.254.174 - 80/tcp
■ Servidor de Camera - range UDP	Todos	199.99.99.99 - 4500:5500/udp	➔ 192.168.254.174 - 4500:5500/udp

**NOTA:** A seleção do campo **[v] Permissão Padrão** – configura automaticamente uma política de permissão de encaminhamento [Forward] para a interface selecionada na política. Este recurso se aplica também na utilização de ambientes com MultiLink.

Para casos em que o administrador pretende aplicar “*Filtros específicos*” no acesso de redirecionamentos adicione uma política de compliance do tipo “*Encaminhamento*” para o host de destino local, no menu **[Políticas]**“

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



## 12 Web Cache

O serviço Web Cache consiste em oferecer um serviço de Proxy e Cache, tem como principal recurso, entre as suas diversas funcionalidades, permitir o acesso à Internet para usuários de uma sub-rede que não possuam acesso direto à rede pública, de forma simples, segura e eficiente.

Além disso, também contribui para controlar o uso irrestrito dos serviços web e diminuir o consumo de banda, já que possui os mecanismos de “*Web caching*” e integração ao serviço de “*Web Filter*” com controle de acesso por filtros de “*Conteúdo*” e “*Aplicativos*”, através das políticas de compliance que restringem a navegação dos usuários.

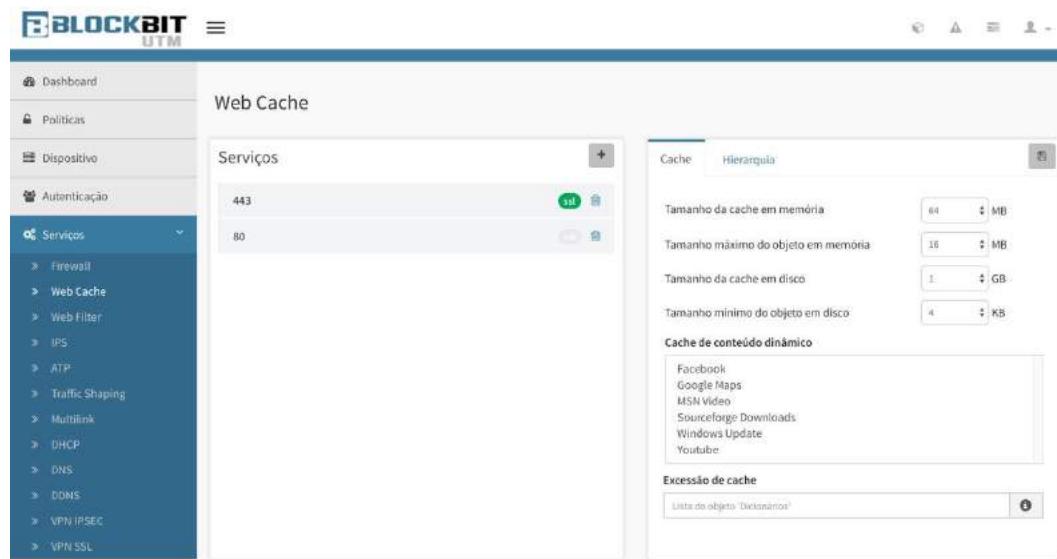
O BLOCKBIT UTM opera com proxy nos modos:

Transparente

Configurado

Porta padrão do Proxy: **[Porta 128]**

No menu principal acesse **[Serviços] >> [Web Cache]**.



A interface é dividida em:

- Serviços
- Cache
- Hierarquia

## 12.1 Serviços

No quadro **[Serviços]** temos a configuração dos serviços suportados pelo Web Cache com a opção de adicionar outros serviços que queira que sejam tratados pelo proxy.



As portas de serviços são configuráveis.

O serviço é pré-configurado para permitir acesso aos serviços web padrões “HTTP (porta 80) e HTTPS (porta 443) ”.

Suporte a serviços web “HTTP e HTTPS versões 1.0 e 1.1 e FTP”.

Para adicionar novos serviços com permissão de acesso ao Proxy, no quadro **[Serviços]**, clique em Adicionar [**+**].



**IMPORTANTE:** Para configuração de serviços que trabalham no modo SSL (modo criptografado). Não esquecer de habilitar o item **[v] SSL**.

## 12.2 Cache

Na aba **[Cache]** temos alguns recursos de gerenciamento e controle do serviço de cache que armazena em uma base local os documentos retornados dos servidores WEB requisitados, dessa forma é possível reutilizar o acesso a esses documentos sem que haja a necessidade de estabelecer uma nova conexão com o servidor remoto.

Configuração de web cache em memória e disco.

Habilitação de web cache de conteúdos dinâmicos.

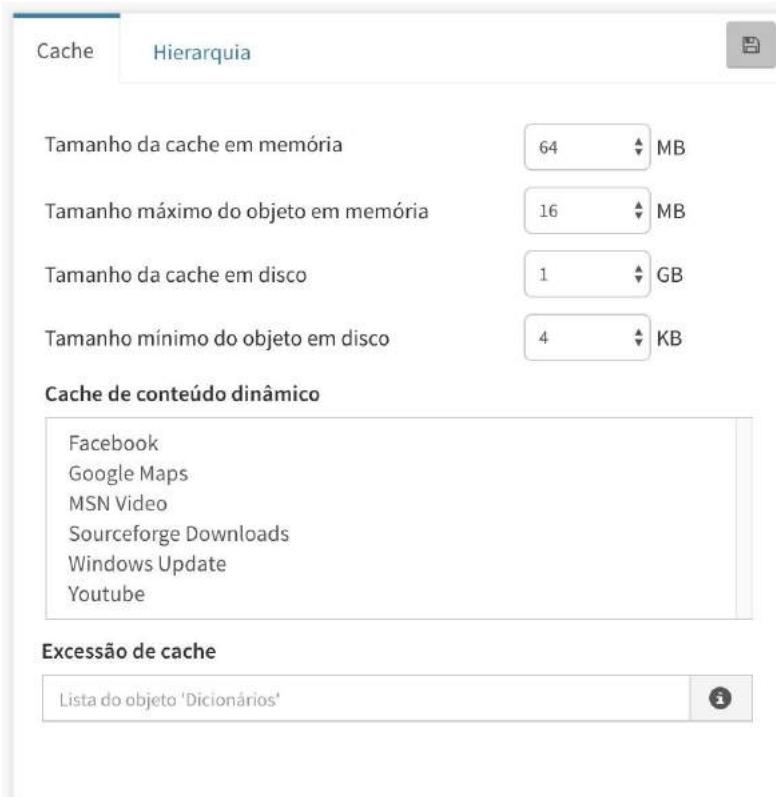
“Facebook, Google Maps, MSN Video, Sourceforge Downloads, Windows Update, Youtube”.

Existem conteúdos que são disponibilizados pelos servidores WEB de forma dinâmica e distribuída, são os chamados CDN (Content Delivery Network). Esse recurso utiliza uma tecnologia que responde a requisição do usuário pelos servidores web mais próximos da sua localização geográfica. Normalmente a resposta a requisição é atendida de forma dinâmica onde cada servidor da pilha de servidores próximos a requisição responde fragmentos do conteúdo solicitado.

O BLOCKBIT UTM possui um recurso de proxy capaz de concatenar estes fragmentos do conteúdo solicitado e guardar cache mesmo de origens diversas.

Exceção de cache, configurável por expressões regulares.

O serviço é pré-configurado para utilizar os recursos de armazenamento em cache com valores padrões para os tamanhos de arquivos recomendáveis pelo sistema.



## 12.3 Hierarquia

Na aba **[Hierarquia]** temos o recurso de configuração de redirecionamento do tráfego Proxy. Um modelo de Proxy hierárquico, que atua no modelo “*Proxy Parent*”.

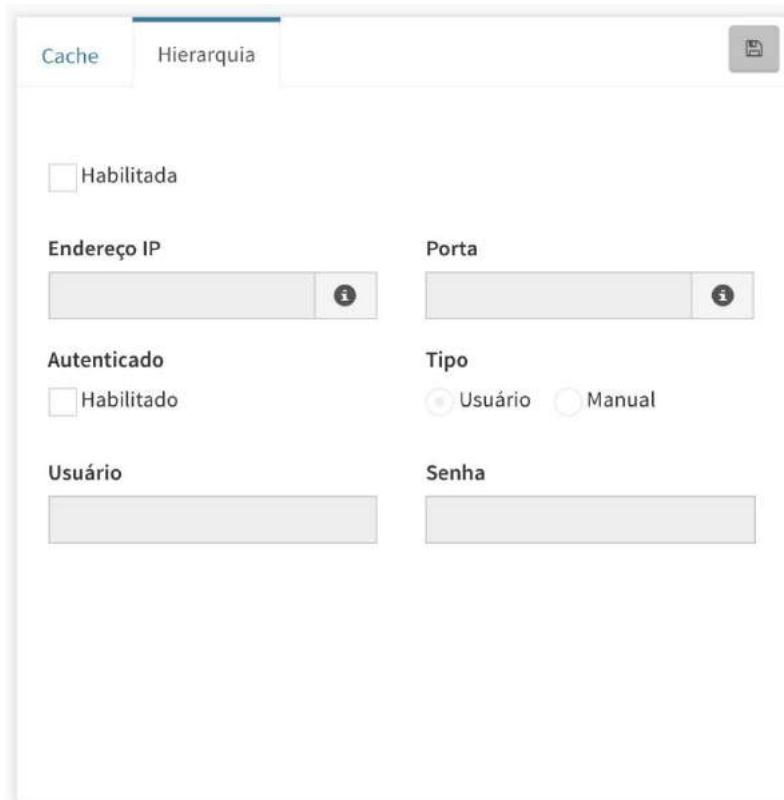
Algumas estruturas com subnets exigem que o tráfego de cada sub-rede mesmo que já gerenciada através de um servidor de Proxy, redirecione seu tráfego para um servidor Proxy hierárquico, seja para aplicar filtros de conexão por hierarquia de Proxy ou apenas para consulta em um servidor de cachê local antes do redirecionamento do acesso à internet.

A hierarquia de Proxy é muito usual para aplicação de filtros e tratamentos dos pacotes HTTP/HTTPS por aplicações de Antivírus HTTP.

Atende a estrutura de navegação através de hierarquia de Proxy com e sem autenticação.

Suporte à integração antivírus HTTP através de hierarquia de Proxy.

Clique na aba **[Hierarquia]** e configure os campos de acordo com os dados do “*Proxy Parent*”, para redirecionamento do tráfego HTTP. Depois clique [  ].



**NOTA:** Alguns Proxies mesmo atuando como Proxy Parent exclusivos para receber redirecionamento requer autenticação.

**Método autenticação Usuário →** Este método solicita autenticação diretamente ao usuário final, através de autenticação “*basic*” via browser.

**Método autenticação Manual →** Este método solicita autenticação “*mestra*” diretamente ao Proxy local.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 13 Web Filter

O Web Filter funciona como uma segunda camada para filtrar a navegação dos usuários. É o responsável pelo filtro de conteúdo e só pode ser utilizado quando as requisições de acesso Web HTTP/ HTTPS são repassadas por um servidor Proxy, antes de solicitar os dados ao servidor remoto, ele redireciona algumas informações da requisição (url, usuário e endereço IP do usuário) para o serviço de Web Filter.

Com base nas informações enviadas pelo Web Cache, o serviço de Web Filter procura um filtro por categoria de url's que se aplica, através das “*Políticas de compliance*”. Dependendo de como as políticas estão configuradas, o Web Filter responde ao Web Cache se a requisição foi permitida ou bloqueada.

Neste item podemos gerenciar o recurso através da “*Atualização*” da base de URLs de categorias, definir a “*Mensagem de Bloqueio*”, aplicar “*Controles de login por domínio para os serviços Google*” e ainda habilitar a integração do serviço de busca segura “*SafeSearch*” para os principais buscadores da web, “*Google, Yahoo e Bing*”.

Para configuração do serviço Web Filter, acesse o menu **[Serviços] >> [Web Filter]**.

The screenshot shows the BLOCKBIT UTM 1.1 web interface. The left sidebar has a navigation menu with items like Dashboard, Políticas, Dispositivo, Autenticação, Serviços (selected), Sistemas, Snapshot, and Terminal. Under Serviços, there are sub-options: Firewall, Web Cache, Web Filter (selected), IPS, ATP, Traffic Shaping, Multilink, DHCP, DNS, DDNS, VPN IPSEC, and VPN SSL. The main content area is titled 'Web Filter' and contains several configuration sections:

- Categorias:** A list of categories with checkboxes for each: Ativismo relacionado a direitos reprodutivos, Governo, Órgãos militares, Grupos políticos, Saúde, Sites pró-vida, Conteúdo ilegal/questionável, and Sites a favor da liberdade de escolha.
- Mensagem de bloqueio:** A text area containing the message: "As políticas de segurança impediram o acesso a este conteúdo. Em caso de dúvida, entre em contato com o administrador."
- Dominios do Google:** A section with checkboxes for 'Habilitado', 'Endereço IP' (with an 'Adicionar tag' button), 'Grupos' (with an 'Adicionar tag' button), 'Usuários' (with an 'Adicionar tag' button), and 'Dominios' (with an 'Adicionar tag' button).
- Pesquisa Segura:** A section with checkboxes for 'Habilitado', 'Endereço IP' (with an 'Adicionar tag' button), 'Grupos' (with an 'Adicionar tag' button), 'Usuários' (with an 'Adicionar tag' button), and 'Dominios' (with an 'Adicionar tag' button).

### 13.1 Categoria

Para atualização da base de URLs de categorias vá para **[Serviços] >> [Web Filter]**.

No quadro **[Categoria]** clique em **Atualizar base** [  ].

Categorias	Categoria e url	
Ativismo relacionado a direitos reprodutivos		
Governo		
Órgãos militares		
Grupos políticos		
Saúde		
Sites pró-vida		
Conteúdo ilegal/questionável		
Sites a favor da liberdade de escolha		



**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



Após a atualização da base o administrador pode aplicar testes de pesquisa à base.

Para pesquisar URLs da base de categorias WEB, no campo **[Buscar]**, insira o endereço da “URL” que deseja pesquisar e clique em [  ] para listar a “categoria” de classificação para a “URL” pesquisada.

Categorias    

Tecnologia da informação 

Categorias    

Mecanismos de busca e portais 

Categorias    

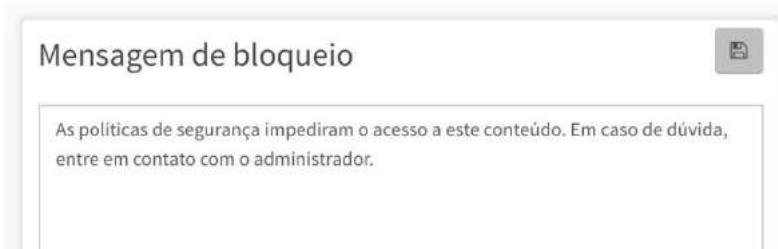
Conteúdo para maiores 

Categorias    

Esportes 

## 13.2 Mensagem de Bloqueio

O Sistema já vem pré-configurado com uma mensagem de bloqueio.



O Administrador pode reconfigurar este formulário e redefinir a mensagem de bloqueio para o seu ambiente, de acordo com seu plano de políticas.

Acesse o quadro **[Mensagem de bloqueio]**, altere a mensagem e clique **[ ]**.

### 13.3 Domínios do Google

Este recurso permite filtrar os domínios com direitos a acessar os serviços Google. O administrador tem a opção de controlar quais os domínios terão este direito.

Exemplo.: Se a empresa tiver contratado a Google para hospedar seus e-mails e direitos de usar aplicações google para seu domínio, o administrador pode optar em não liberar o uso do google para uso de e-mail e aplicações pessoais.

Como funciona:

Se o campo domínio for preenchido com empresa.com.br os usuários só poderão se logar no google com a conta da empresa [usuário@empresa.com.br](mailto:usuário@empresa.com.br). Se o usuário tentar acessar o google com sua conta pessoal [usuário@gmail.com](mailto:usuário@gmail.com) receberá uma tela de bloqueio.

No quadro **[Domínios do Google]**, habilite e configure os campos de controle com base nas políticas que pretende aplicar. Depois clique em [ ].



A definição do campo **[Domínios]** é obrigatória.

Os campos **[Endereço IP]**, **[Grupos]** e **[Usuários]**, requer que seja especificado ao menos 1 (hum) entre eles.

### 13.4 Pesquisa Segura

Suporte aos filtros Safe Search da Google que fornece a capacidade de impedir que sites com conteúdo inapropriado apareçam em seus resultados de pesquisa.

Este recurso aplica um filtro de pesquisa segura direto nas ações de “Pesquisa” dos usuários na sua estação de trabalho a partir dos browsers. Este recurso de pesquisa segura se aplica aos principais buscadores da WEB “Google, Yahoo e Bing”.

No quadro **[Pesquisa Segura]**, habilite e configure os campos de controle com base nas políticas que pretende aplicar. Depois clique em **[ ]**.

Pesquisa Segura

Habilitado

**Endereço IP**

**Grupos**

**Usuários**

**IMPORTANTE:** O serviço Web Filter contempla os recursos:

- Filtro de Conteúdo
- Controles de domínios dos serviços GOOGLE
- Safe Search para os principais buscadores da WEB.
- Interceptação SSL.
- Controle de aplicativos WEB 2.0.

Todos estes recursos são aplicados nas políticas de compliance.

Não se esqueça de APLICAR a fila de COMANDOS, clique no ícone **[ ]**

## 14 IPS – Sistema de Prevenção de Intrusos

O IPS é o responsável pela monitoração e análise do tráfego da rede, a fim de identificar o tráfego de códigos maliciosos, e ataques. Baseado em assinaturas; regras e sensores ele funciona como um farejador que analisa o conteúdo de todo tráfego passante por ele e gera os registros de todos os pacotes identificados na sua base de assinaturas.

Para o seu perfeito funcionamento requer que a base IPS esteja sempre atualizada.

O BLOCKBIT UTM analisa em tempo real os pacotes que são direcionados pelo firewall através das “*Políticas de Zone Protection*” e das “*Políticas de Compliance*”. Gera relatórios sumarizados por período dos ataques identificados e dos ataques bloqueados, e um histórico, inclusive do nível de impacto das assinaturas identificadas.

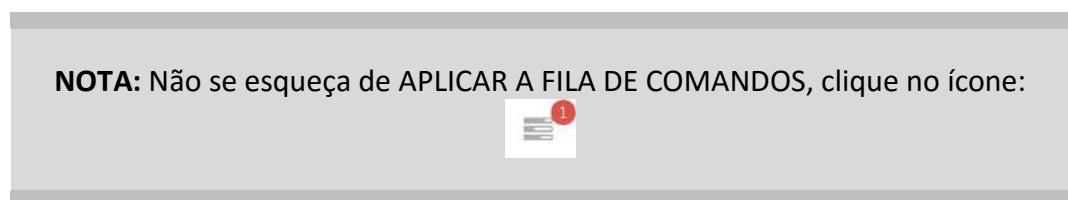
Para configuração do serviço, acesse o menu **[Serviços] >> [IPS]**.

Status	Bloqueio	Impacto	Categoria	Nome	SID
OK	OK	Médio	attack_response	ATTACK_RESPONSE ALBANIA id.php detected	2007656
OK	OK	Alto	attack_response	ATTACK_RESPONSE Backdoor reDuh http initiate	2011667
OK	OK	Médio	attack_response	ATTACK_RESPONSE C99 Modified phpshell detected	2007654
OK	OK	Médio	attack_response	ATTACK_RESPONSE c99shell phpshell detected	2007652
OK	OK	Médio	attack_response	ATTACK_RESPONSE Cisco TelShell TFTP Download	2009245
OK	OK	Médio	attack_response	ATTACK_RESPONSE Cisco TelShell TFTP Read Request	2009244
OK	OK	Alto	attack_response	ATTACK_RESPONSE FTP CWD to windows system32 - Suspicious	2008556
OK	OK	Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access AUX	2000507
OK	OK	Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM1	2000499
OK	OK	Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM2	2000500

## 14.1 Atualização da Base

Para a habilitação do serviço, basta atualizar a base de dados e automaticamente o serviço estará disponível para monitoração e inspeção do tráfego de rede.

Na aba [Assinaturas] clique em Atualizar base [].



O serviço [IPS] está pronto para monitorar e inspecionar o tráfego da rede.

Assinaturas					Exceções
Impacto:	Todos	Categoria:	Todos		
			attack_response	ATTACK_RESPONSE ALBANIA id.php detected	SID 2007656
			attack_response	ATTACK_RESPONSE Backdoor reDuh http initiate	SID 2011667
			attack_response	ATTACK_RESPONSE C99 Modified phpshell detected	SID 2007654

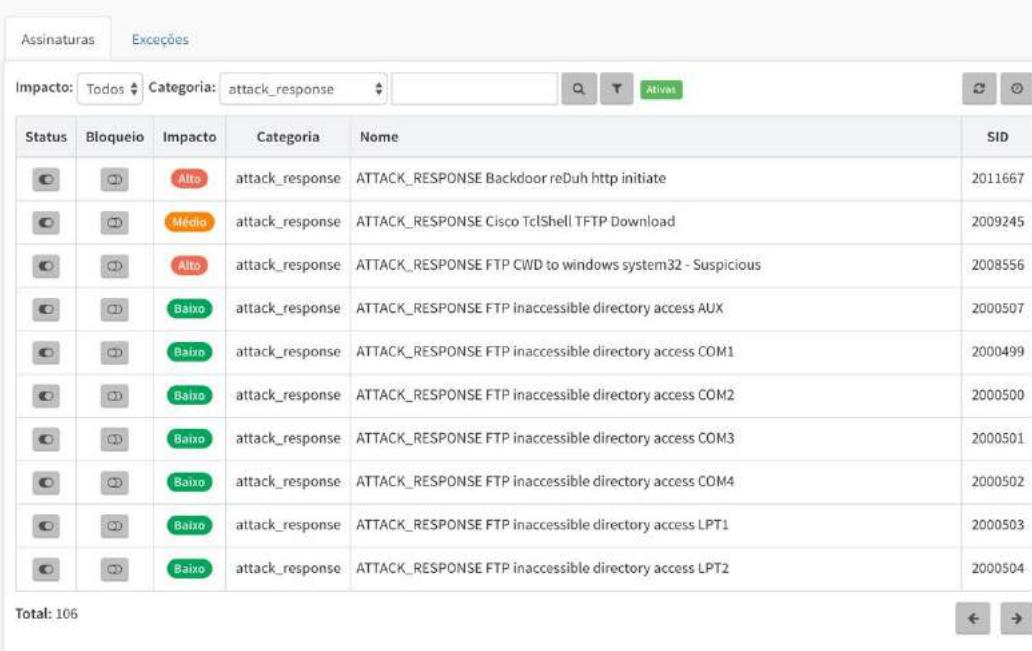
As ações de “Bloqueio” e somente “Log” status *habilitado*, dos pacotes identificados como códigos maliciosos e/ou ameaças dependem do perfil de configuração de cada assinatura e da ação de “Inspeção IPS” definidas nas políticas de segurança.

As assinaturas são os códigos de ataques armazenados em um banco de dados, bem semelhantes ao funcionamento de um antivírus que contém as assinaturas ou códigos de vírus, ou seja, existem estruturas de dados que, se forem encontradas por um fluxo de rede é identificado como um possível ataque, determinado pela ação da assinatura.

Para alterar a ação de determinada assinatura da base, clique no [ / ] de “Status” e “Bloqueio” da respectiva assinatura que deseja “Habilitar/Desabilitar”.

O administrador pode utilizar o recurso de **Pesquisa** [  ] e especificar pela seleção, “**Categoria: [Todos]**” qual assinatura ou grupo de assinaturas pretende alterar seu “Status”.

### Intrusion Prevention



Status	Bloqueio	Impacto	Categoria	Nome	SID
		Alto	attack_response	ATTACK_RESPONSE Backdoor reDuh http initiate	2011667
		Médio	attack_response	ATTACK_RESPONSE Cisco TelShell TFTP Download	2009245
		Alto	attack_response	ATTACK_RESPONSE FTP CWD to windows system32 - Suspicious	2008556
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access AUX	2000507
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM1	2000499
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM2	2000500
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM3	2000501
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access COM4	2000502
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access LPT1	2000503
		Baixo	attack_response	ATTACK_RESPONSE FTP inaccessible directory access LPT2	2000504

Total: 106

**NOTA:** A ação de “*BLOQUEIO*” do pacote identificado como malicioso requer ação de “*Inspecionar IPS*” nas políticas de segurança.

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



## 15 ATP – Proteção Avançada Contra Ameaças

O ATP (Advanced Threat Protection) é um serviço que se assemelha muito com o serviço IPS (Intrusion Prevention System), é o responsável por monitorar e analisar o tráfego da rede e identificar aplicativos e ameaças direcionadas e persistentes e efetuar os respectivos bloqueios/detecção. Integrado a uma base de assinaturas eletrônicas atua na camada de aplicação, capaz de analisar o conteúdo dos pacotes em tempo real, identificar e efetuar o bloqueio do pacote ou mesmo o IP de origem.

Baseado em assinaturas; regras e sensores ele funciona como um analisador que analisa o conteúdo de todo tráfego passante por ele e gera os registros de todos os pacotes identificados na sua base de assinaturas, seja a execução de aplicativos não autorizados. A função de bloqueio das assinaturas de ATP envia um comando de RESET para as conexões quando esse recurso é usado em conjunto com o serviço WEB.

Conta ainda uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware, e ao serviço de “Anti-APT (Advanced Persistent Threats) baseado em listas de reputação IP e Geolocalização IP.

Aliado a tecnologia Stateful Packet Inspection prevê o recurso de inspeção profunda, ou seja, inspeciona todos os pacotes redirecionados para ele, inclusive os pacotes HTTPS interceptados pelo proxy.

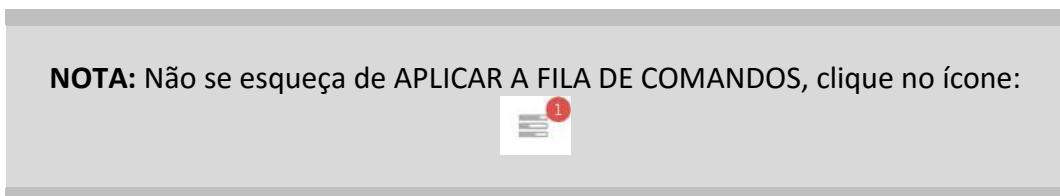
Para configuração do serviço, acesse o menu **[Serviços] >> [ATP]**.

The screenshot shows the 'Threat Protection' section of the BLOCKBIT UTM interface. On the left, a sidebar lists service categories like Firewall, Web Cache, Web Filter, IPS, ATP, and Traffic Shaping. The main area displays two large tables: one for 'Ameaças' (Threats) and one for 'Aplicativos' (Applications). The 'Ameaças' table lists items like 'activeX', 'app-detect', 'blacklist', 'botcc', etc., with counts ranging from 1 to 220. The 'Aplicativos' table lists categories such as ads, Cloud, collaboration, download, email, games, general, mobile, p2p, proxy, remote, social, storage, streaming, update, voip, and web, each with a corresponding icon and count. Below these are sections for 'Bloqueio de Ameaças' (Threat Blocking) and 'IP Reputation', which lists entries like abuse, anonymizers, and attacks. A 'Proteção por Geolocalização' (Geolocation Protection) section on the right lists countries like Afghanistan, Aland Islands, and Albania.

## 15.1 Atualização da Base

Para a habilitação do serviço, basta atualizar a base de dados e automaticamente o serviço estará disponível para monitoração e inspeção do tráfego de rede.

Na aba [Ameaças] clique em Atualizar base [  ].



Agora o serviço [ATP] está pronto para monitorar e inspecionar o tráfego da rede.

As ações de “Bloqueio” e somente “Log” status habilitado, dos aplicativos ou ameaças identificadas dependem do perfil de configuração de cada assinatura da base ATP e da ação de “Inspeção ATP” definida nas políticas de segurança.

As assinaturas são os códigos de identificação dos aplicativos e ameaças e tipos ataques armazenados em um banco de dados, semelhantes ao funcionamento do IPS, ou seja, existem estruturas de dados que, se forem encontradas por um fluxo de rede é identificado, registrado o log e determinado como ameaça determinado pela ação especificada na assinatura.

Para “Alterar” determinada assinatura da base, clique no botão **Editar** [  ] do respectivo grupo de assinaturas, Ex.: [malware] depois no botão [  /  ] de “Status” e “Bloqueio” da respectiva assinatura que deseja “Habilitar/Desabilitar”.

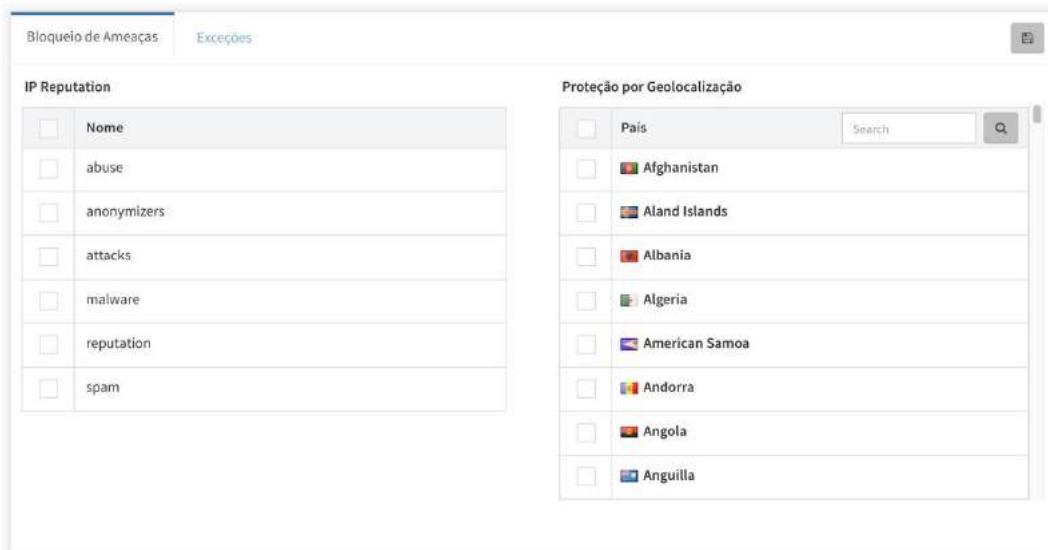
malware				
Status	Bloquear	Risco	Descrição	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware Actionlibs Download	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware config Download	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware Defs Download	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware Install	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware Keywords Download	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware (tracked event 2 reporting)	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions Spyware versionconfig POST	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions (Zango) Spyware Event Activity Post	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions (Zango) Spyware Installer Config 2	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Alto	MALWARE 180solutions (Zango) Spyware Installer Download	

Ainda na interface principal do **[ATP]** o administrador pode utilizar o recurso de **Filtro de Pesquisa** [  ] e especificar pela seleção múltipla de ameaças por categoria, “**Categoria: [Todos]**” qual assinatura pretende alterar seu “**Status**”.



No quadro **[Bloqueio de Ameaças]** temos o recurso de bloqueio, baseado em listas do tipo “*IP Reputation*” e “*Proteção por Geolocalização*”.

Para habilitar estes recursos habilite os itens desejados e clique em **Salvar** [  ]



Para o seu perfeito funcionamento requer que as bases ATP estejam sempre atualizadas.

**NOTA:** A ação de “*BLOQUEIO*” do pacote identificado como malicioso requer ação de “*Inspecionar ATP*” nas políticas de segurança.

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 16 Traffic Shaping

Temos aqui o gerenciamento de banda e controle de tráfego, a integração deste serviço é fundamental no tratamento e priorização dos serviços de rede. Tem a finalidade de permitir e especializar as redes de forma a melhorar sensivelmente a qualidade de conexão.

Especificações e recursos do Traffic Shaping.

- Controle por fila de prioridade
- Controle de velocidade máximo e garantido por nível de prioridade (item configurável)
- Habilitação do controle de velocidade permitindo especificar a largura de banda ou velocidade downstream e upstream de cada interface.

O serviço é pré-configurado com 5 (cinco) níveis de prioridades definidas pelo sistema:

- Muito Alta
- Alta
- Média
- Baixa
- Muito Baixa

Acesse o menu **[Serviços] > [Traffic Shaping]**.

#	Prioridades	Vel. Garantida	Vel. Máxima
0.	Muito Alta	100%	100%
1.	Alta	80%	80%
2.	Média	50%	50%
3.	Baixa	30%	30%
4.	Muito Baixa	10%	10%

#	Interface	Download	Upload
1	eth0	Velocidade c Kbps ↕	Velocidade c Kbps ↕
2	eth3	Velocidade c Kbps ↕	Velocidade c Kbps ↕
3	eth1	Velocidade c Kbps ↕	Velocidade c Kbps ↕
4	eth2	Velocidade c Kbps ↕	Velocidade c Kbps ↕

## 16.1 Definições das Prioridades

No quadro [Definições das Prioridades] o administrador tem a opção de clicar em **Editar** [  ] e redefinir os (%) percentuais de cada nível de prioridade “Traffic Shaping” de acordo com os padrões e políticas de qualidade de serviço que queira adotar.

Definição das Prioridades			
#	Prioridades	Vel. Garantida	Vel. Máxima
0.	Muito Alta	90 %	100 %
1.	Alta	70 %	80 %
2.	Média	50 %	50 %
3.	Baixa	30 %	30 %
4.	Muito Baixa	10 %	10 %

O modo [Edição] permite alterar o valor “% - percentual” de cada nível de prioridade, manipulando o gráfico com auxílio do movimento do “mouse” ou editando o formulário “manualmente”.



Depois clique em [  ]

## 16.2 Habilitar Traffic Shaping

Neste item definimos a velocidade “Download” e “Upload” especificada pela operadora de cada link respectivamente.

Esta informação é utilizada como base para aplicar o controle “% -percentual” de cada nível de prioridade definido no sistema.

#	Interface	Download	Upload		
<input type="checkbox"/>	eth0	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>
<input type="checkbox"/>	eth3	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>
<input type="checkbox"/>	eth1	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>
<input type="checkbox"/>	eth2	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>	<input type="text" value="Velocidade c."/>	<input type="button" value="Kbps"/>

**NOTA:** A definição de largura ou velocidade do link não é necessariamente a mesma velocidade do device físico.

No quadro **[Habilitar Traffic Shaping]**, selecione as interfaces de rede e parametrize as velocidades de Download e Upload respectivamente, de acordo com as especificações do link de cada operadora. Depois clique em [  ].

## 16.3 Exemplo

No exemplo, vamos especificar:

Link da interface Eth1:	10 Mbps	[Download]
	10 Mbps	[Upload]
Link da interface Eth2:	35 Mbps	[Download]
	6 Mbps	[Upload]

Habilitar Traffic Shaping					
#	Interface	Download	Upload		
<input type="checkbox"/>	eth0	Velocidade c Kbps	<input type="button" value="↑"/>	Velocidade c Kbps	<input type="button" value="↑"/>
<input type="checkbox"/>	eth3	Velocidade c Kbps	<input type="button" value="↑"/>	Velocidade c Kbps	<input type="button" value="↑"/>
<input checked="" type="checkbox"/>	eth1	10 Mbps	<input type="button" value="↑"/>	10 Mbps	<input type="button" value="↑"/>
<input checked="" type="checkbox"/>	eth2	10 Mbps	<input type="button" value="↑"/>	6 Mbps	<input type="button" value="↑"/>

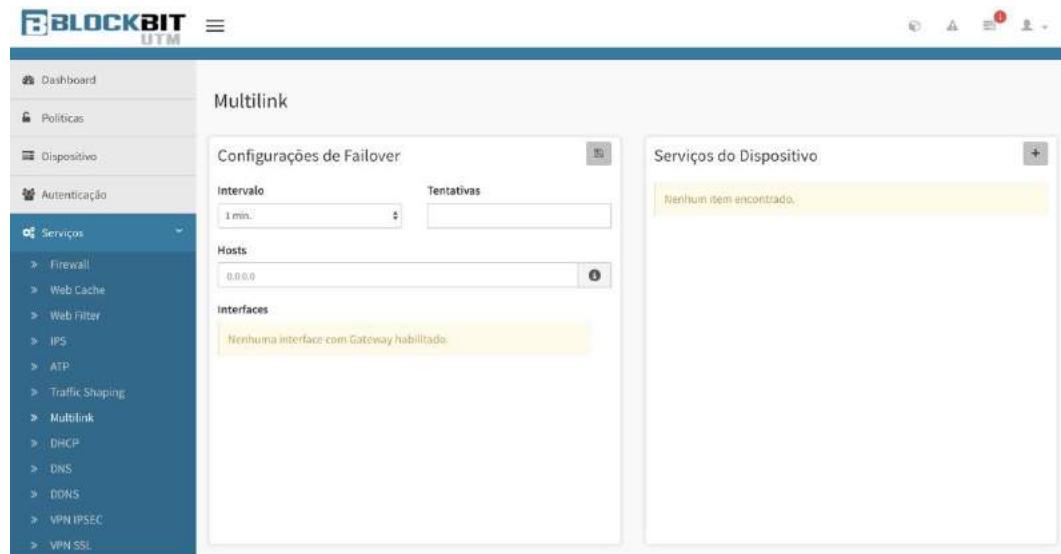
**NOTA:** A ação de QoS “Traffic Shaping” são aplicados nas “Políticas de compliance”.

Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone [  ].

## 17 Multilink

O Multilink é o responsável por segmentar e priorizar o tráfego através das interfaces de rede, permitindo o roteamento do tráfego através das interfaces configuradas.

Acesse o menu **[Serviços] >> [Multilink]**.



O Multilink contempla além da função de roteamento, a função de “*Tolerância a falhas*”, ou seja, um recurso de redundância (Failover), um controlador de falhas de link, capaz de aplicar testes de disponibilidade do link em tempo real.

### Recursos do Multilink

- Redundância – Failover.
- Ordenação e priorização do link – definição do gateway padrão.
- Balanceamento do tráfego - roteamento dinâmico por políticas de segurança.
- Roteamento de serviços do dispositivo.
- Reestabelecimento automático do roteamento dos links.
- Informativo de falhas e reestabelecimento dos links.

## 17.1 Requisitos para Implementação de Multilink

- Os links de internet devem ser do tipo:
  - Link dedicado.
  - Link IP.
  - Possuir endereço IP Fixo.
  - Configurar o endereço de “Gateway” nas interfaces de rede configuradas para os links de internet.

**ATENÇÃO:** O sistema requer que as interfaces de rede configurados para os Links IP do tipo WAN (links de internet), contemplem a configuração do campo “Gateway”, utilizado para determinar qual a rota de saída das respectivas interfaces.

- Definir endereços IP públicos para os testes de redundância “Failover”.

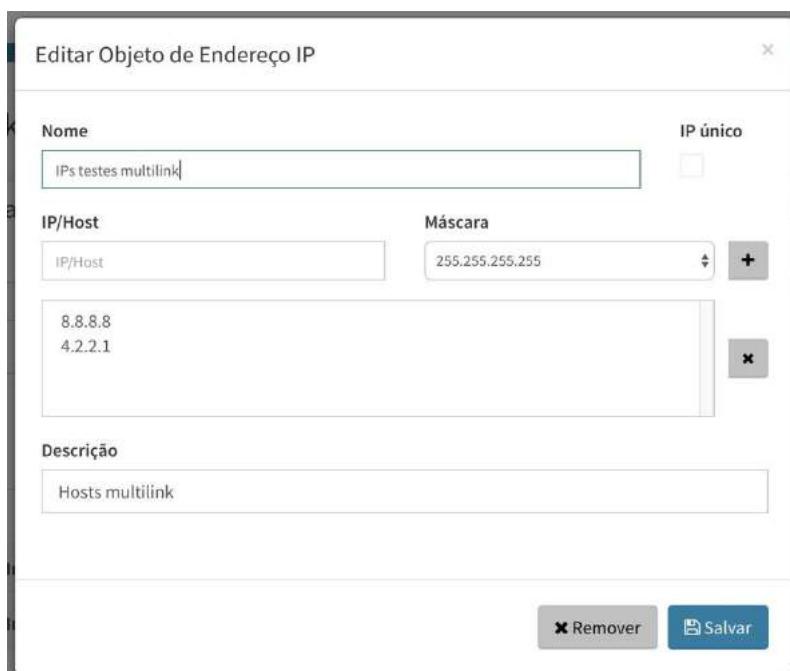
**IMPORTANTE:** Recomenda-se aplicar os testes para endereços de serviços Públicos redundantes - “*Alta disponibilidade*”.

## 17.2 Configurações de Redundância (Failover).

No quadro **[Configurações de Failover]**, configure o ambiente de testes, definindo o “Intervalo”; “Tentativas”; “Hosts”. Selecione as interfaces de rede que pretende habilitar para o Multilink. Depois clique em [  ].



Após salvar as configurações iniciais do serviço, o administrador tem a opção de editar o campo **[Hosts]** e adicionar novos endereços à lista para os testes de “Failover”. Clique em [  ].



Clique em **Adicionar** [+] para adicionar os novos endereços ao objeto IP “**Multilink**” e depois clique em [  ].



Depois clique em [  ].

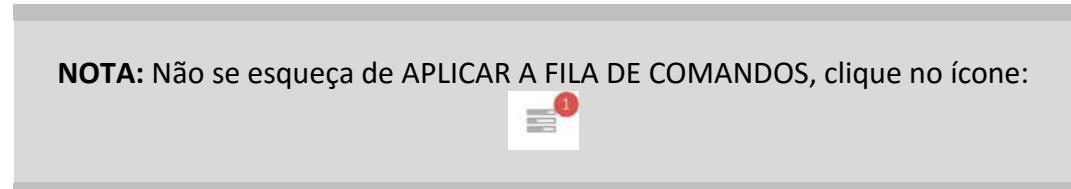
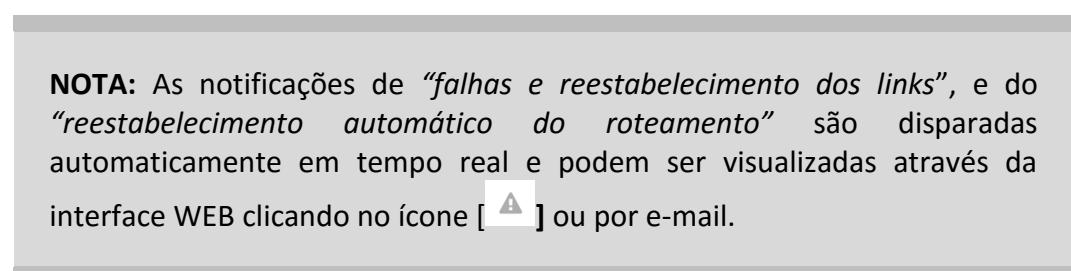
**NOTA:** Os testes de **[Failover]** retornam para o sistema o “Status” atual de cada link, de acordo com a resposta do status, se “*On-line*” ou “*Off-line*”. Este recurso alterna o endereço do “*Gateway*” padrão do servidor para o endereço do “*Gateway*” da próxima interface ou link configurado e disponível na lista de interfaces.

### 17.3 Alterando a Prioridade dos Links

É possível alterar a prioridade da realização dos testes de interface. A ordem de prioridade alterna o Gateway padrão. É importante frisar que a interface de maior prioridade responde como link principal do Multilink, e gateway padrão do sistema, por onde são direcionados os serviços e tráfegos permitidos a partir das “*Políticas de Compliance*”.



Através da seleção da interface de rede. *Clique e arraste pelo símbolo [⋮] até a posição desejada de ordenação. Depois em clique em [💾].*



## 17.4 Balanceamento de Tráfego

O recurso de Balanceamento de links ou tráfego, é definido nas ações de “Roteamento” através das “*Políticas de compliance*”.

Funciona como um serviço de roteamento dinâmico nas políticas de compliance e pode ser definido por:

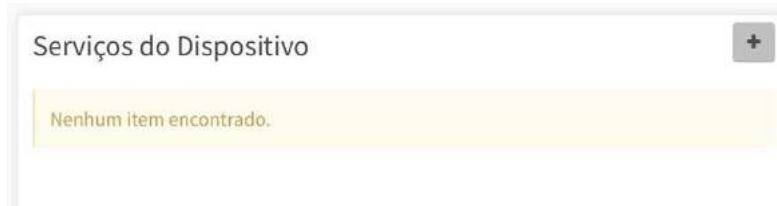
- Origem
  - Zona de rede
  - Device
  - Endereço IP
  - Endereço MAC
  - Autenticado
    - ◆ Usuário
    - ◆ Grupo
- Destino
  - Endereço IP
  - Serviços diversos
  - Serviço WEB
  - Com / Sem Interceptação SSL

Desta forma condicionando o recurso de Balanceamento de tráfego e links por “*Políticas de compliance*”.

## 17.5 Serviços do Dispositivo

O recurso [Serviços do Dispositivo] permite ao administrador definir políticas exclusivas de saída que correspondam aos serviços do sistema.

- HTTP Proxy (portas 80/TCP; 443/TCP); outros serviços suportados pelo proxy).
- Update BLOCKBIT (porta 80/TCP) para o endereço de destino dos servidores UPDATE BLOCKBIT. Ex. “*updates.blockbit.com*”



Para configurar uma política multilink para os serviços do BLOCKBIT UTM clique em **Adicionar** []. Depois clique em [].

Vamos exemplificar uma política de saída para o serviço de UPDATE da base BLOCKBIT.

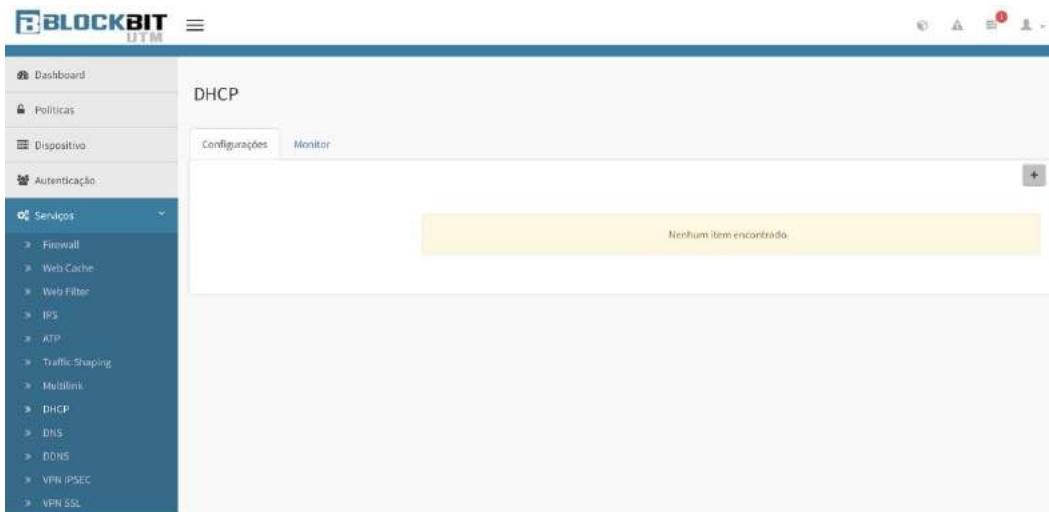


A política é salva “*desabilitada*”, clique em [] para habilitar a política antes de aplicar a fila de comandos.

## 18 DHCP

Gerenciador do protocolo DHCP que atua sobre camada de aplicação nas portas padrões do DHCP 67/68 UDP. Numa rede de arquitetura TCP/IP, todo computador tem que possuir um endereço IP distinto. O DHCP (Dynamic Host Configuration Protocol) é o protocolo que provê um meio para alocar estes endereços dinamicamente.

Acesse o menu **[Serviços] >> [DHCP]**.



O DHCP é responsável por distribuir os endereçamentos IPs e configurações de rede para seu ambiente corporativo. É uma eficiente solução já que, por meio dele, o servidor BLOCKBIT UTM distribui endereços IPs na medida em que os dispositivos da rede solicitam conexão. É importante frisar que, além do endereço IP, atribui outros parâmetros, tais como: nome do host, dns e rota default.

### Recursos do DHCP:

- Distribuição de endereços IPs por device/ por servidor.
  - Ethernet.
  - Vlan.
  - MacVlan (device de endereçamento virtual).
- Distribuição de endereços IPs por rede/sub-rede.
- Políticas para distribuição de endereço IP.
- Modelos.
  - Distribuição por range.
  - Distribuição de endereços estáticos. (Reserva de end. IP por filtro MAC).

- Filtros:
  - MAC.
  - Host.
- Parâmetros:
  - Gateway.
  - Sufixo DNS.
  - Múltiplos DNS.
  - Múltiplos Wins.
  - TTL (Time to live) Tempo de renovação.

## 18.1 Habilitação DHCP

Para habilitar o serviço DHCP e configurar uma política de DHCP, clique em **Adicionar** [], e selecione a **[Interface]** para a rede/subrede que pretende distribuir endereços IPs. Depois clique em [].



Ao salvar a seleção da **[Interface]** para distribuição dos endereços IPs, o sistema retorna a interface para configuração dos parâmetros DHCP.

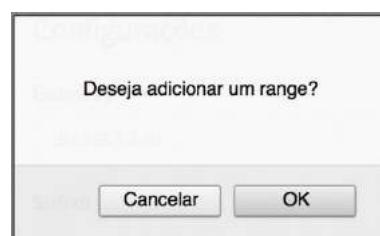
## 18.2 Configurações

Para configuração dos parâmetros básicos para distribuição de endereços IPs, no quadro **[Configurações]** configure os campos de acordo com o formulário e os respectivos valores e endereços IPs que pretende distribuir por DHCP. Depois clique em [  ].

**Configurações**

<b>Gateway</b>	192.168.1.1	
<b>Sufixo DNS</b>	blockbit.com	
<b>DNS</b>	192.168.1.1	
Endereço IP dns secundário		
<b>WINS</b>	Endereço IP wins Primário	
Endereço IP wins secundário		
<b>Tempo de renovação</b>	Segundos	
83400		

Em seguida ao **[Salvar]** os parâmetros de configurações do DHCP o serviço pergunta se você deseja aproveitar e definir o **[Range]** de endereços que irá distribuir. Se responder **[OK]** o sistema faz um redirecionamento automático para a interface de configurações do range.



## 18.3 Range

Neste quadro o administrador define qual o “range” ou “intervalo” de endereços IPs que pretende distribuir pelo serviço DHCP.



Para adicionar um *range ou intervalo* de endereço IP, clique em **Adicionar** [], e configure de acordo com os campos. Depois clique em [].

**NOTA:** Os intervalos “*inicial e final*” do range ou intervalo dos endereços IPs devem estar obrigatoriamente dentro do intervalo de rede/subrede declarada na interface selecionada para configuração.

**Adicionar range**

**Range**

**Configurações**

**Range inicial**  
192.168.1.100

**Range final**  
192.168.1.200

**Filtro MAC**  
Endereço MAC Address ex. 0a:1b:1c:3d:4e:5f

**Descrição**  
Range Estações

**Salvar**

### Adicionar range

**Range**

**Configurações**

**Gateway**  
192.168.1.1

**Sufixo DNS**  
blockbit.com

**DNS**  
192.168.1.1

**Endereço IP dns secundário**

**WINS**

**Endereço IP wins Primário**

**Endereço IP wins secundário**

**Tempo de renovação** Segundos  
83400

**Salvar**

### Ranges

192.168.1.100 → 192.168.1.200

**+**

**i** **✎** **✖**

## 18.4 Endereços Estáticos

O serviço ainda dispõe do recurso de distribuir endereços no modo estático, ou seja, fixando o mesmo “*Endereço IP*” para determinado “*Host*”, a partir da identificação do “*Endereço MAC*”.

Endereços estáticos			
Host	Endereço IP	Endereço MAC	Ação
Nenhum ítem encontrado.			

Para adicionar regras de distribuição de endereço IP no modo estático, por Host/Endereço MAC, clique em **Adicionar** [+] e configure de acordo com a definição de políticas para distribuição de endereços IPs. Depois clique em [ Salvar ].

### 18.4.1 Exemplo – Definindo endereços estáticos por DHCP

<b>Host</b>	WinXen2012
<b>Endereço IP</b>	192.168.1.54
<b>Endereço MAC</b>	90:B1:1C:F6:2F:E2

Adicionar host

<b>Host</b>	WinXen2012
<b>Endereço IP</b>	192.168.1.54
<b>Endereço MAC</b>	90:B1:1C:F6:2F:E2

**Salvar**

---

**Host** NFS\_CentOS7

---

**Endereço IP** 192.168.1.22

---

**Endereço MAC** 42:69:4C:9C:3F:00

---

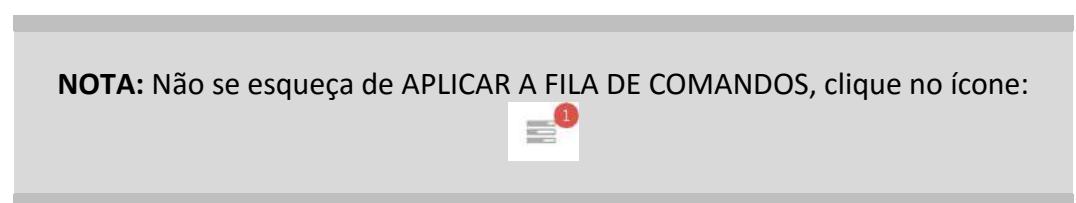
**Adicionar host**

<b>Host</b>	NFS_CentOS7
<b>Endereço IP</b>	192.168.1.22/32
<b>Endereço MAC</b>	42:69:4C:9C:3F:00

Salvar

Endereços estáticos			
Host	Endereço IP	Endereço MAC	Ação
WinXen2012	192.168.1.54	90:B1:1C:F6:2F:E2	
NFS_CentOS7	192.168.1.22	42:69:4C:9C:3F:00	

Para habilitar a distribuição automática dos endereços declarados no serviço DHCP, clique em habilitar [ ].



## 18.5 Monitor DHCP

A monitoração do DHCP é dinâmica e ainda conta com um recurso de filtro onde o administrador pode especificar:

- Hostname
- Usuário
- IP

Para acessar o monitor vá para **[Serviços] >> [DHCP]** e clique na aba **[Monitor]**.

The screenshot shows the 'Monitor' tab selected in the DHCP configuration interface. On the left, there are three input fields for filtering: 'Hostname', 'Usuário', and 'IP'. Below these is a blue 'Filtrar' button. To the right is a table displaying the following data:

Hostname	Mac	Usuário	IP	Data
Estacao001	8A:12:6B:A3:13:52		192.168.1.100	21/07/2016 - 10:59

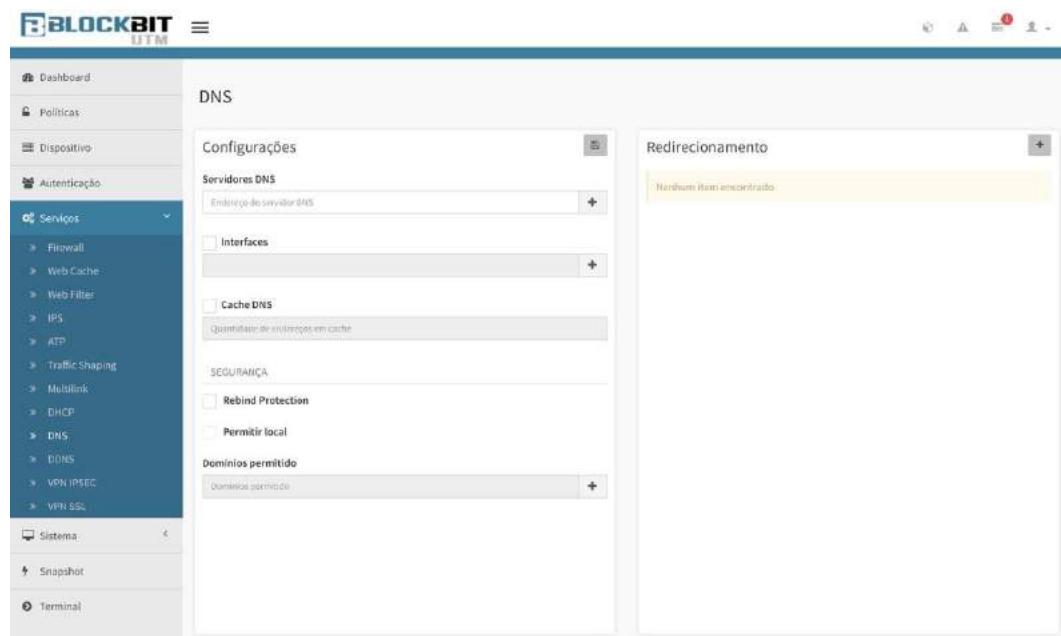
## 19 DNS

O Serviço de DNS é o responsável em fornecer o recurso de “*tradução de nomes de domínios*” para seus respetivos endereços IPs.

O BLOCKBIT UTM fornece o serviço de redirecionamento de DNS para outros servidores DNS recursivos, responsável por receber as consultas DNS de clientes DNS locais e consultar os servidores remotos ou externos, de modo a obter respostas às consultas efetuadas de qualquer domínio e responder aos clientes locais.

O serviço DNS conta com a integração ao recurso de Caching, lida com as consultas dos clientes DNS e também armazena a resposta em seu cache local por um determinado tempo permitido pelo TTL dos respectivos registros dos domínios consultados. O Cache é usado como uma fonte para os próximos pedidos, a fim de otimizar o tempo de busca das próximas requisições de domínios já pesquisados.

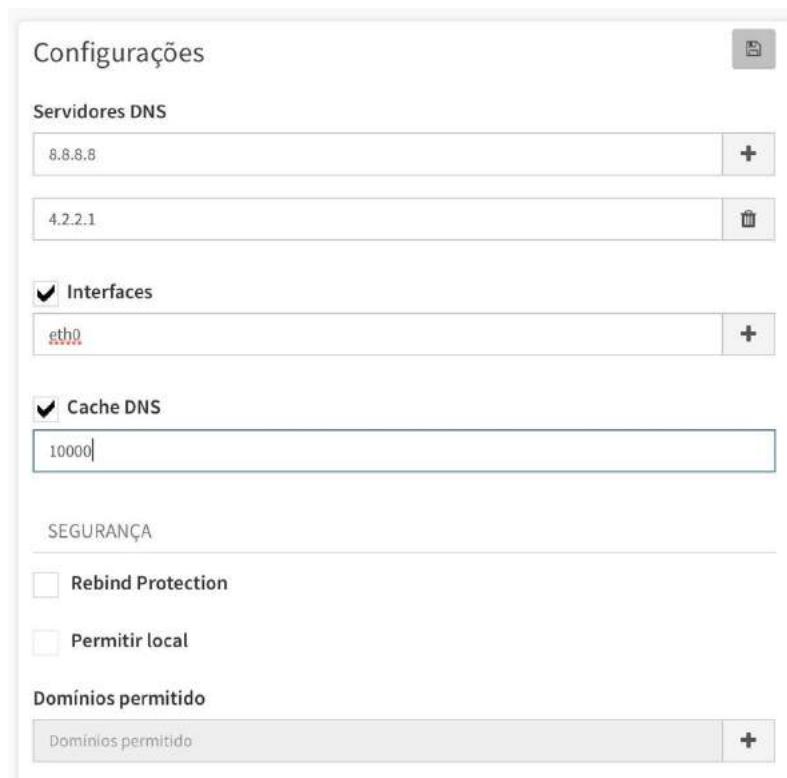
Clique em **[Serviços] >> [DNS]**.



## 19.1 Configurações

Neste item o administrador tem a opção de configurar o serviço de redirecionamento de DNS para outro servidor DNS Recursivo “remoto” ou “externo”, habilitar o “armazenamento de Cache local”, e um serviço de proteção que previne “ataques DNS rebinding”.

No quadro **[Configurações]** configure os campos de acordo com o formulário para o encaminhamento DNS para outro servidor DNS recursivo e clique em 



The screenshot displays the 'Configurações' (Configurations) screen. It includes sections for 'Servidores DNS' (DNS Servers) containing IP addresses 8.8.8.8 and 4.2.2.1; 'Interfaces' (Interfaces) with 'eth0' selected; 'Cache DNS' (DNS Cache) set to 10000; and 'SEGURANÇA' (Security) with options for 'Rebind Protection' and 'Permitir local' (Allow local). A 'Domínios permitido' (Allowed domains) section is also present.

Abaixo vamos especificar alguns campos:

### [Interfaces]

Seleção da interface de rede que será ativada para o modo “Listen”. O que permite fazer as requisições DNS recursivo desta origem.

### [Cache DNS]

Quantidade de endereços de cache para armazenamento no cache local”.

**[Rebind Protection]**

Muitos domínios são configurados para responder um TTL (Time to live) muito baixo. Esta publicação do TTL baixo previne a ação de guardar cache. Ataques do tipo “*DNS Rebind*” consistem em utilizar-se desse recurso que inibe guardar cache de “*domínios com TTL baixo*” para encaminhar códigos maliciosos na 1ª resposta à pesquisa de DNS, a fim de Autorizar a execução de scripts: “*Java*”, “*Javascript*” e “*Flash*” para acessar hosts dentro da rede privada e daí realizar os ataques propriamente dito.

Habilitar o **[Rebind Protection]**, evita este tipo de ataque.

O Serviço rebind Protection tem suporte à:

- Exceção host local.
- Exceção por domínio.

## 19.2 Redirecionamento

Neste item o administrador tem a opção de configurar o serviço de redirecionamento das requisições DNS para “*Que outros servidores DNS*” sejam os “*Responsáveis*” em realizar as consultas recursivas “*Exclusivas*” para uma “*lista de hosts*”.

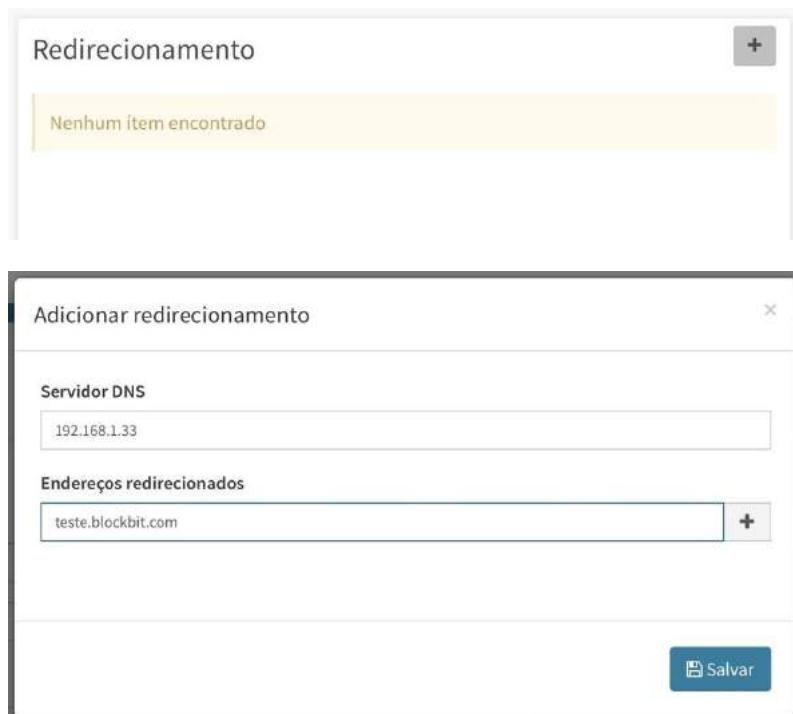
O serviço permite através da distribuição e balanceamento das pesquisas para hosts específicos, redirecionar o serviço para outro servidor DNS exclusivo para os hosts especificados.

Ainda pode ser usado inclusive para redirecionar as pesquisas para um “*DNS inválido*”, evitando a resolução de nomes de determinados endereços, logo bloqueando seu acesso.

- Redirecionamento DNS
  - Múltiplos servidores.
  - Encaminhamento por host/IP e fqdn.
  - Cache.

No quadro **[Redirecionamento]** clique em **Adicionar** [+] e configure apontando o endereço do servidor DNS e adicionando os endereços dos hosts que pretende redirecionar as pesquisas recursivas.

Vamos exemplificar o redirecionamento de uma lista de hosts para um servidor DNS local. Depois clique em [  ].



The image shows two screenshots of a web-based management interface. The top screenshot is titled 'Redirecionamento' and displays a message 'Nenhum ítem encontrado'. A '+' button is located in the top right corner. The bottom screenshot is a modal window titled 'Adicionar redirecionamento' (Add Forwarding). It contains fields for 'Servidor DNS' (DNS Server) with the value '192.168.1.33' and 'Endereços redirecionados' (Forwarded Addresses) with the value 'teste.blockbit.com'. A '+' button is next to the address field. At the bottom right of the modal is a blue 'Salvar' (Save) button.

Adicionar redirecionamento

Servidor DNS

192.168.1.33

Endereços redirecionados

teste.blockbit.com +

ww3.blockbit.com -

ftp.blockbit.com -

Salvar

Redirecionamento

192.168.1.33 | - -

**NOTA:** Não se esqueça de APLICAR A FILA DE COMANDOS, clique no ícone:



## 20 DNS Dinâmico (DDNS)

O serviço DDNS (Dynamic Domain Name System) é um gerenciador de um serviço de tradução de nomes para endereços IPs dinâmicos. O DDNS é o método usado para atualizar a tabela de IPs/hosts públicos automaticamente em um servidor DNS em tempo real e isso com o propósito de manter ativo e publicado um host ou endereço IP configurado para algum serviço ou recurso através de link dinâmico como: PPPOE, (DSL -Digital Subscriber Line) para prover seu acesso remoto.

Os endereços IPs dinâmicos representam um problema quando precisamos fazer algum acesso remoto em algum serviço da rede, tais como um serviço web (intranet/extranet), acesso remoto, configuração de VPN, entre outros.

Como os endereços IPs de links DSL podem mudar com frequência, associar nomes de hosts e domínios para endereços IPs dinâmicos é uma tarefa que exige um re-mapeamento quase que em tempo real para que os serviços continuem respondendo as requisições e acessos remotos sem a interrupção.

Alguns serviços como VPN IPSEC (site to site), VPN IPSEC RAS e mesmo o acesso remoto por redirecionamento do firewall (DNAT), utilizam-se deste recurso como ferramenta adicional para permitir de forma segura o acesso aos recursos da rede através de links DSL.

Acesse a interface de gerenciamento DynDNS, clique em **[Serviços] >> [DDNS]**.

## 20.1 Configuração DNS Dinâmico

Antes de adicionar um *DNS Dinâmico* vamos conhecer e identificar os recursos de configuração e como funcionam.

- Recursos DDNS
  - Suporte aos provedores de serviço.
    - ◆ NoIP.org
    - ◆ DynDNS.com
  - Suporte a interfaces.
    - ◆ Ethernet
    - ◆ Vlan
    - ◆ MacVlan (Interface virtual)
  - Integração com os serviços
    - ◆ DNS.
    - ◆ VPN.
    - ◆ Firewall.
    - ◆ Políticas de segurança.

A atualização dos hosts/domínios (ddns) configurados é automática, no entanto, o intervalo da atualização depende da operadora contratada.

O serviço DDNS pode ser habilitado para uma interface de rede específica “[EthX]” ou no modo “*Automático*”.

**ATENÇÃO:** A seleção de uma interface específica “[EthX]”, associa o “host” ao “endereço IP do link DSL” do respectivo device físico.

A seleção da interface no modo “*Automático*”, associa o “host” de forma dinâmica ao “endereço IP” em uso pelo link ativo associado ao device do gateway padrão.

Vamos exemplificar a configuração do “*Dymanic DNS*” para o host “*vpn-bb.blockbit.com*” para o provedor de serviços “*DynDNS*”. Usar os dados de usuário e senha fornecidos/cadastrado no respectivo provedor.

Clique em **[Serviços] >> [DDNS]**, depois clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com o provedor conforme o exemplo dado. Depois clique em []

Habilitar DDNS

<b>Serviço</b>	<input type="text" value="NoIP.org"/>
<b>Host</b>	<input type="text" value="vpn-bb.blockbit.com"/>
<b>Usuário</b>	<input type="text" value="blockbit"/>
<b>Interface</b>	<input type="text" value="Automático"/> Automático eth0 eth1 eth2 eth2v0 eth3

## DNS Dinâmico

Hosts		+ -	+ -	Ação
Host	Endereço IP	Interface		
vpn-bb.blockbit.com	-	-	<input type="button" value=""/>	<input type="button" value=""/>

**IMPORTANTE:** O recurso DDNS permite aplicar “*Redundância*” para os serviços:

- VPN IPSec (site to site).
- VPN IPSec RAS.
- Firewall - Redirecionamento (DNAT).

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



O Serviço DDNS já está configurado e o host “*vpn-bb.blockbit.com*” respondendo pelo endereço IP da interface de rede correspondente a rota default.

## 21 VPN IPSEC

O serviço VPN IPSEC é responsável por permitir configurar e estabelecer túneis entre redes não válidas através de meios públicos. Este serviço permite ao administrador interligar redes e prover o compartilhamento de dados seja entre filiais, colaboradores itinerantes, home offices, clientes e fornecedores, é fundamental manter um mecanismo de segurança para que o tráfego das informações seja seguro e sem riscos de acesso não autorizado.

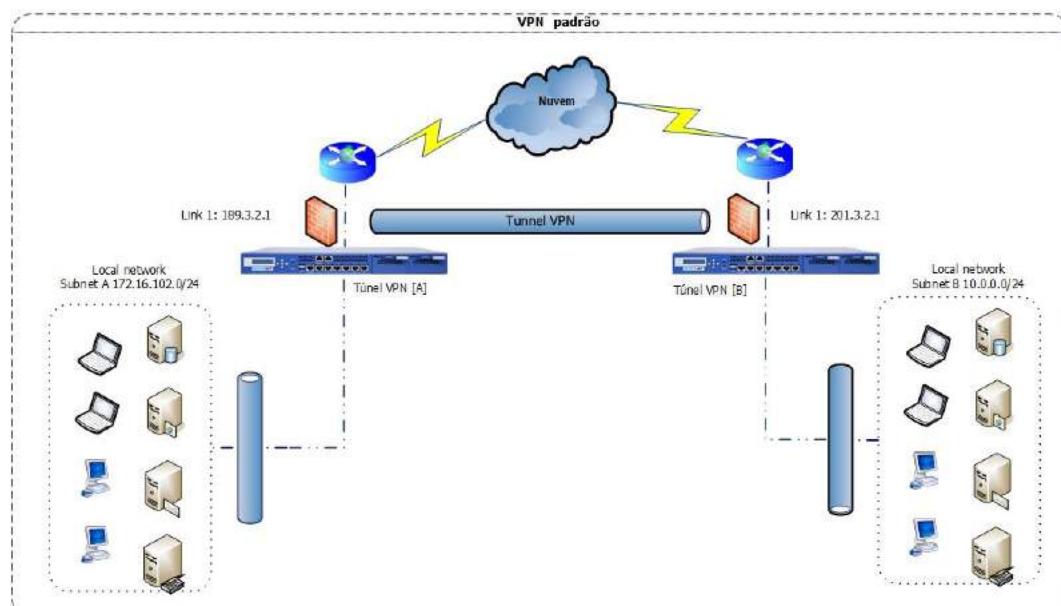
O serviço de VPN fornece alto nível de segurança através de protocolos de segurança IPSEC. Incorporando encapsulamento e criptografia dos dados usando uma suíte de protocolos e métodos de encriptação e autenticação na comunicação entre hosts da rede privada de forma que, se os dados forem capturados durante a transmissão, não possam ser decifrados.

IPSec é o protocolo padrão utilizado para encapsular pacotes IP e roda sobre a camada 3 (modelo OSI). Será utilizado para estabelecer túneis VPN em ambos os modelos de configuração: VPN IPsec túnel e VPN IPsec Remote Access.

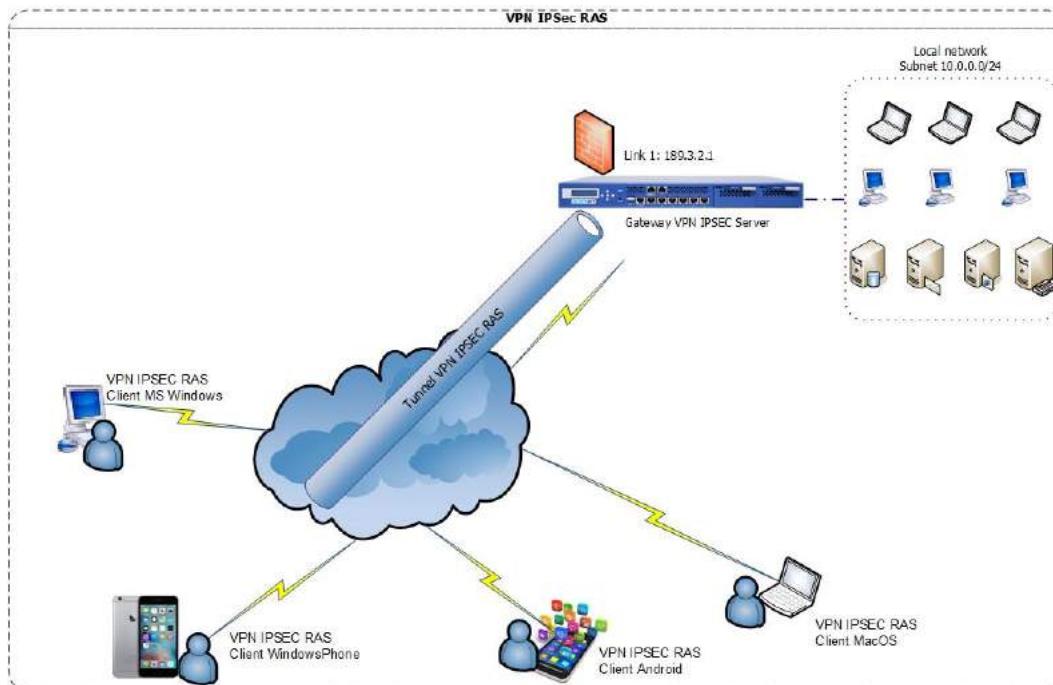
Abaixo algumas especificações técnicas:

### [Modos de operação]

- **VPN IPsec Túnel:** É o método do serviço VPN IPSEC que visa gerenciar múltiplos túneis virtuais de redes privadas. Provê uma conexão do tipo túnel site to site (LAN to LAN).



- **VPN IPsec RAS (Remote Access):** É o método do serviço VPN IPSEC que permite configurar um servidor de acesso remoto proporcionando aos usuários acesso seguro à rede interna através de qualquer conexão em uma rede pública (Internet). Este modelo define que os acessos serão realizados a partir de uma conexão cliente com chaves do tipo (PSK) e autenticação dos tipos: X-Auth ou (EAP-MSCHAP V2).



Abaixo especificações dos principais itens de configuração da VPN IPSEC.

#### [IKE]

O IKE – Internet Key Exchange é o protocolo usado para estabelecer uma associação de segurança (SA) na suíte de protocolos IPsec. O IKE se baseia no protocolo Oakley e ISAKMP, utiliza-se de uma chave de autenticação PSK ou certificados X509 e uma troca de chaves “Diffie Hellman”.

No BLOCKBIT UTM utilizamos a chave do tipo: “*PSK (Chave pré compartilhada)*”, e a troca de chaves “*Diffie Hellman*”. O sistema suporta as versões IKE v1 e IKE v2.

**NOTA:** Ambos os pontos VPN devem estar configurados para a mesma versão IKE.

**[Modos de Inicialização do túnel]**

- **Automático:** Adiciona e inicializa o Túnel.
- **Aguardar:** Adiciona e não inicializa o Tunnel. Aguarda requisição de demanda (tráfego) por parte da outra ponta VPN.
- **Sob demanda:** Inicializa e levanta o Túnel somente sob demanda, ou seja, quando houver tráfego de qualquer das ponta VPN.

**[ESP]**

O protocolo ESP fornece confidencialidade de dados (criptografia) e autenticação (integridade de dados e autenticação da origem dos dados). O ESP se baseia na utilização dos algoritmos AH (Authentication Header) e ESP (Encapsulating Security Payload).

**[Host Remoto]**

Endereço de comunicação do ponto VPN REMOTO para estabelecer o túnel. Deve ser identificado por: “*Endereço IP*” ou “*Hostname(fqdn)*”.

**[ID Local]**

Método de identificação da ponta VPN Local, utilizado também como método de autenticação do IKE na fase 1. Defina e configure a identificação entre os tipos: “*Endereço IP*”, “*Hostname(fqdn)*” ou “*email@dominio*”.

**[ID Remoto]**

Método de identificação da ponta VPN Remota, utilizado também como método de autenticação do IKE na fase 1. Defina e configure a identificação entre os tipos: “*Endereço IP*”, “*Hostname(fqdn)*” ou “*email@dominio*”.

**[Chave compartilhada PSK]**

É uma chave pré-compartilhada (Pre-Shared Key ou PSK) é um segredo compartilhado anteriormente entre as duas partes usando algum canal seguro antes de ser utilizado. Tais sistemas quase sempre usam algoritmos criptográficos de chave simétrica. Essa chave é utilizada no processo de autenticação pelo protocolo IKE.

O administrador deve definir essa chave e configurar em ambos os pontos VPN.

**[Keying tries]**

Este é o número de vezes que os pontos VPN vão renegociar o túnel ou tentar re-autenticação (re-key) depois que a chave expirar. Determina o número de tentativas para estabelecer a renegociação em cada fase de negociação do IKE/IPsec.

**[IKE lifetime]**

Determina o tempo de vida que o protocolo (IKE ou IPSEC dependendo da fase) irá aguardar para renegociar a SA (Security Association), que especifica os algoritmos a serem utilizados, as chaves criptográficas, e os tempos de vida destas chaves. O tempo de vida deve ser determinado em minutos.

O protocolo IKE é o autenticador e o negociador do IPsec.

**[Key lifetime]**

Determina o tempo de validade da chave de negociação bem-sucedida. O tempo de vida deve ser determinado em minutos.

**[Rekey Margin]**

Determina quanto tempo antes da conexão expirar os pontos VPN vão inicializar a renegociação das chaves do túnel. Tempo padrão 9 minutos.

**[Dead peer detection action]**

O item DPD (Dead peer detection action) controla o uso do protocolo de detecção dos pontos de VPN (perdidos). Onde as mensagens de notificação do protocolo IKE v1 e IKE v2 são enviados periodicamente a fim de verificar se os pontos IPSec estão respondendo, ou estão perdidos.

A seleção de qualquer valor “*clear*”, “*hold*” e “*reiniciar*”, ativa o serviço DPD e determina a ação a ser executada em um tempo limite.

A ação “*clear*” fecha, ou encerra a conexão sem tomadas de medidas prévias.

A ação “*hold*” configura uma política estratégica que captura o tráfego e tenta renegociar a conexão sob demanda.

A ação “*restart*” inicia imediatamente uma tentativa de renegociação da conexão.

O padrão é “*none*” ou nenhuma, desativa o envio automático das mensagens DPD.

**[Dead peer detection delay]**

Define o intervalo de tempo ou período, que as mensagens de troca IKE v1 e IKE v2 informativas são enviadas para os pontos VPN. Tempo padrão 30 segundos.

**[Dead peer detection timeout]**

Define o intervalo de tempo limite para o envio das mensagens, para o IKE v1 após todas as conexões para um ponto VPN serem perdidas em caso de inatividade. Tempo padrão 150 segundos.

Para o IKE v2 o tempo limite de retransmissão “*DPD delay*” sempre se aplica.

**[Algoritmos IKE Fase 1]**

Baseado no protocolo ISAKMP (IKE/SA): define o agrupamento dos algoritmos e especificações técnicas de autenticação da Fase (IKE/SA) para o dispositivo VPN utilizado para estabelecer o túnel VPN.

**[Algoritmos IPSEC Fase 2]**

Baseado nos protocolos AH e ESP (ESP/AS): define o agrupamento dos algoritmos e especificações técnicas de autenticação da Fase (IPSEC/SA) para o dispositivo VPN utilizado para estabelecer o túnel VPN.

## 21.1 Requisitos para configuração VPN IPSEC

Para o serviço VPN IPSEC conseguir gerenciar uma conexão segura precisamos antes certificar que atendemos alguns requisitos para então disponibilizar o serviço de VPN para a rede.

Antes de configurar um túnel é importante saber quais os modelos de hardwares e aplicações de VPN serão usados para estabelecer o túnel. Conhecer o modelo e característica de cada aplicação e definir exatamente que tipo de túnel VPN vai estabelecer.

### 21.1.1 Verificações e requisitos VPN IPSEC Túnel.

1. Quais os modelos dos hardwares/aplicações de VPN dos pontos remotos?
2. Identificar endereços de rede LAN de cada ponto de VPN – certificar de que cada ponto possui um endereçamento de rede em classes/sub-rede diferentes.
3. Qual o endereço dos pontos remotos (ID remoto)?
  - Endereço IP.
  - Host fqdn.
4. Definir uma chave de criptografia (PSK – Phrase Shared key).
5. Definir qual o modelo e identificação da fase 1 (IKE/SA).
  - Endereço IP;
  - Host fqdn;
  - Host;
  - email@dominio.
6. Definir o método de negociação “*Main mode/Agressive mode*”?
7. Definir os parâmetros para configuração da fase 1 (IKE/SA):
  - Parâmetros IKE (Fase 1) - Suporte IKE versão 1 e 2. Exemplo.:
    - Criptografia: “3DES, Aes, DES”.
    - Autenticação (HASH): “HMAC-MD5, SHA 1”.
    - Diffie-Hellman (DH Group): “modp 2048”.
8. Definir os parâmetros para configuração da fase 2 (IPSEC/ESP):
  - Parâmetros IPSEC – ESP (Fase 2). Exemplo:
    - Criptografia: “ESP-3DES, Aes, DES”.
    - Autenticação (HASH): “ESP-HMAC-MD5, SHA 1”.
    - Use PFS - Perfect Forward Secrecy: “modp 768”.

### 21.1.2 Verificações e requisitos VPN IPSEC RAS.

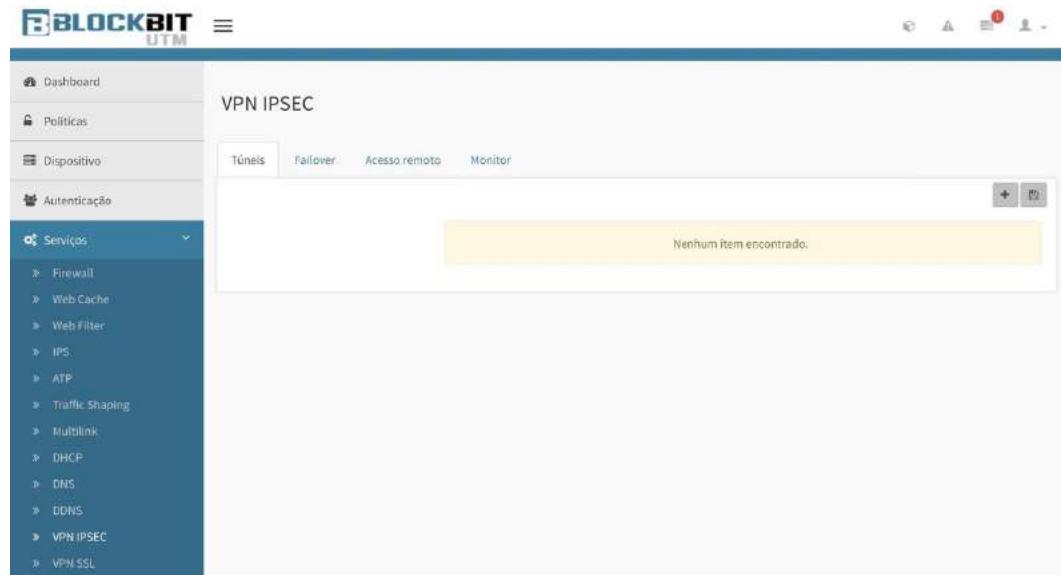
1. Identificar endereços de rede LAN do servidor BLOCKBIT UTM (VPN). Depois definir o endereçamento da “*Rede Virtual VPN RAS*” em uma classe/sub-rede diferente.
2. Qual o modelo do hardware/aplicação de VPN RAS (ponto remoto)?
  - Deve ser compatível com iOS 7 ou superior, Android 4.4.4 ou superior, MacOS X 10.6 ou superior, Linux 2.6.36 ou superior, Windows 7 ou superior”.
3. Definir uma chave de criptografia (PSK – Phrase Shared key).
4. Definir/ identificar os parâmetros para configuração da fase 1 (IKE/SA):
  - Parâmetros IKE (Fase 1) - Suporte IKE versão 2. Exemplo.:
    - Criptografia: “3DES, DES”.
    - Autenticação (HASH): “SHA 1”.
    - Diffie-hellman (DH Group) : “mopb 8192”.
5. Definir/ identificar os parâmetros para configuração da fase 2 (IPSEC /ESP):
  - Parâmetros IPSEC ESP (Fase 2). Exemplo.:
    - Criptografia: “ESP-3DES, DES”.
    - Autenticação: “SHA 1” .
    - Use PFS - Perfect Forward Secrecy: “Não”.

### 21.1.3 Recomendações e requisitos Gerais da VPN.

1. Recomendável que os pontos dos Appliances BLOCKBIT UTM que vão fornecer o serviço VPN IPSEC estejam configurados com endereço IP Válido e fixo. Exemplo: "*Link dedicado/ link IP*".
2. Caso alguns dos pontos da VPN IPSEC Tunnel ou VPN IPSEC RAS seja um BLOCKBIT UTM, o administrador deve:
  - Habilitar permissão no firewall para o serviço VPN IPSEC para a(s) "Zona(s) de rede" do(s) endereço(s) IPs válido(s).  
Acesse **[Serviços] >> [Firewall]** - (Ver [Seção 11.1 – Serviços](#)).
  - Configure uma “política de compliance” do tipo “Permitir” para encaminhamento entre as redes (LANs) dos pontos VPN para todos os protocolos. Ex. “TCP/ UDP/ ICMP”.  
Acesse **[Políticas]** - (Ver Seções 23 e 24 – Políticas de compliance).
3. Caso esteja configurando um ponto remoto, e esteja protegido por um Firewall, é necessário solicitar previamente ao administrador do firewall a liberação do acesso aos seguintes serviços e portas:
  - IKE – IPSec.
  - IKE (UDP porta 500).
  - IPSec ESP (IP type 50).
  - IPSec AH (IP type 51)
  - Mascaramento (NAT) protocolo UDP na porta (NATT – 4500).
  - Encaminhamento (FW) para as respectivas redes (local e remota).

## 21.2 Configurando Túnel VPN IPSEC

Acesse [Serviços] >> [VPN IPSEC].



Para configuração de Túnel abra a aba [Túneis] clique em Adicionar [+] e defina um nome para o Túnel que será estabelecido, depois clique em [Salvar]

Configure todos os campos do formulário baseado nas informações levantadas nas verificações dos requisitos pré-estabelecidos. Ao final clique em [V] Habilitado para habilitação do “Túnel” e selecione o modo de inicialização entre “Automático”, “Aguardar”, Sob demanda”, depois clique em [ ].

## VPN IPSEC

Túneis	Failover	Acesso remoto	Monitor	
<b>Matriz x Filial</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Habilitado</b>	<input type="checkbox"/>	<b>Inicialização do túnel</b>		
<b>Versão do IKE</b>	IKEV1	<b>Host remoto</b>	IP/ fqdn	
<b>ID local</b>	IP/ fqdn/ host/ email@domain	<b>ID remoto</b>	IP/ fqdn/ host/ email@domain	
<b>Chave compartilhada PSK</b>	text alpha	<b>Keying tries</b>	Nº de tentativas	
<b>IKE lifetime</b>	180	<b>Minutos</b>	<b>Dead peer detection action</b>	Selecionar
<b>Key lifetime</b>	60	<b>Minutos</b>	<b>Dead peer detection delay</b>	Segundos
<b>Rekey margin</b>	5	<b>Minutos</b>	<b>Dead peer detection timeout</b>	Segundos
<b>Fragmentação</b>	<input type="checkbox"/>	<b>Tamanho do fragmento (MTU)</b>		
<b>Redes locais</b>	0.0.0.0	<input type="checkbox"/>	<b>Redes remotas</b>	0.0.0.0
<b>Algoritmos IKE (phase 1)</b>		<b>Algoritmos ESP (phase 2)</b>		
Encryption	camellia256c	Hash	md5	DH Group
Encryption	camellia256c	Hash	md5	PFS Group

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



## 21.3 Túnel VPN IPSEC FailOver.

Failover é uma função importante para redes que necessitam de alta disponibilidade.

Esta seção aborda as opções para suportar VPN IPSEC Totalmente Redundante e IPSEC Parcialmente Redundante, usando abordagens baseadas no roteamento aplicado pelo multilink.

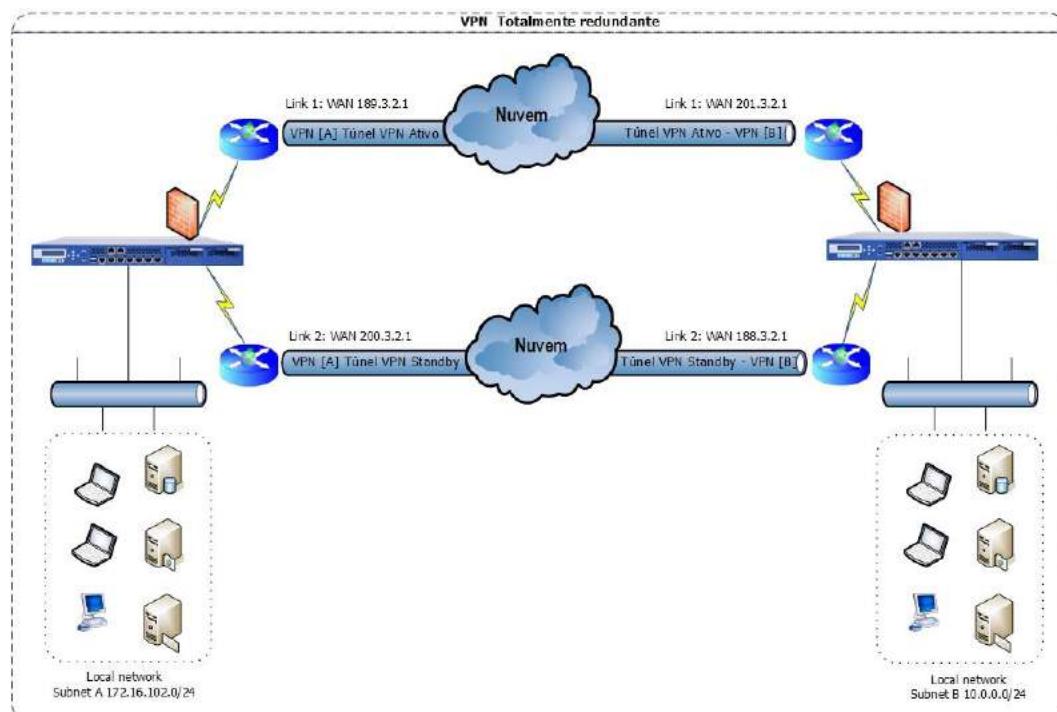
O BLOCKBIT UTM contempla o recurso de Multilink FailOver e este recurso é estendido para o serviço VPN IPSEC (lan to lan).

Com o serviço multilink configurado para duas ou mais interfaces de rede conectadas a internet, O BLOCKBIT UTM suporta a configuração para VPNs IPSEC redundantes para o mesmo ponto remoto. Se a conexão principal falhar, o BLOCKBIT UTM pode restabelecer a VPN usando a outra conexão automaticamente.

O administrador tem a opção de configurar túneis VPN e habilitar o modo FailOver para os tuneis configurados para a mesma rede de destino, definir níveis de prioridade e elencar o túnel VPN principal, com o objetivo de reestabelecer de forma automática a comunicação com a rede de destino sem a necessidade de intervenção manual.

### 21.3.1 VPN totalmente redundante:

A configuração totalmente redundante requer conexões redundantes à Internet em ambos os pontos da VPN.



Este exemplo de VPN redundante é baseado nas rotas do serviço multilink, e demonstra uma configuração totalmente redundante para VPN lan to lan.

Em cada ponto VPN o BLOCKBIT UTM tem duas interfaces conectadas à Internet através de diferentes provedores de internet - ISPs (Internet Service Provider).

---

BB UTM VPN [A] – WAN 1 ↔ BB UTM VPN [B] – WAN 1

---

BB UTM VPN [A] – WAN 2 ↔ BB UTM VPN [B] – WAN 2

---

Este método é confiável para garantir alta disponibilidade para uma conexão confiável entre dois dispositivos BLOCKBIT com endereços IP estáticos.

Em uma configuração de VPN totalmente redundante com multilink habilitado, podemos configurar pontos VPN para todas as interfaces redundantes do multilink, como resultado teremos o total de interfaces multilink e de rotas distintas para o tráfego da VPN lan to lan.

Quando temos apenas um dispositivo BLOCKBIT UTM com ponto VPN com conexões redundantes, a configuração é parcialmente redundante. (Ver [Seção 21.3.3 - VPN parcialmente redundante](#)).

**NOTA:** O BLOCKBIT UTM suporta comunicação VPN com qualquer dispositivo VPN com suporte a IPSec Padrão, redundante e não redundante.

### 21.3.2 Funcionamento da VPN FailOver

Cada interface WAN em um ponto VPN se comunica com outra interface WAN no outro ponto VPN. Isso garante que a VPN estará sempre disponível, desde que cada ponto VPN esteja com o serviço de multilink failover habilitado, garantindo a disponibilidade da comunicação com a Internet.

O administrador deve configurar os pontos VPN para ambas interfaces de rede WANs habilitadas no multilink para a mesma rede lan de destino, respectivamente para cada interface WAN do outro ponto VPN.

O procedimento de configuração deve ser aplicado em ambos os pontos VPN.

O serviço FailOver da VPN monitora o status dos links habilitados no multilink.

A VPN FailOver altera a prioridade de roteamento dos túneis VPN configurados, na ocorrência dos seguintes eventos:

- Se o multilink notificar falha na comunicação com o link em uso na configuração do túnel VPN ativo;
- Se houver falha na comunicação física com as interfaces de rede do túnel VPN ativo;

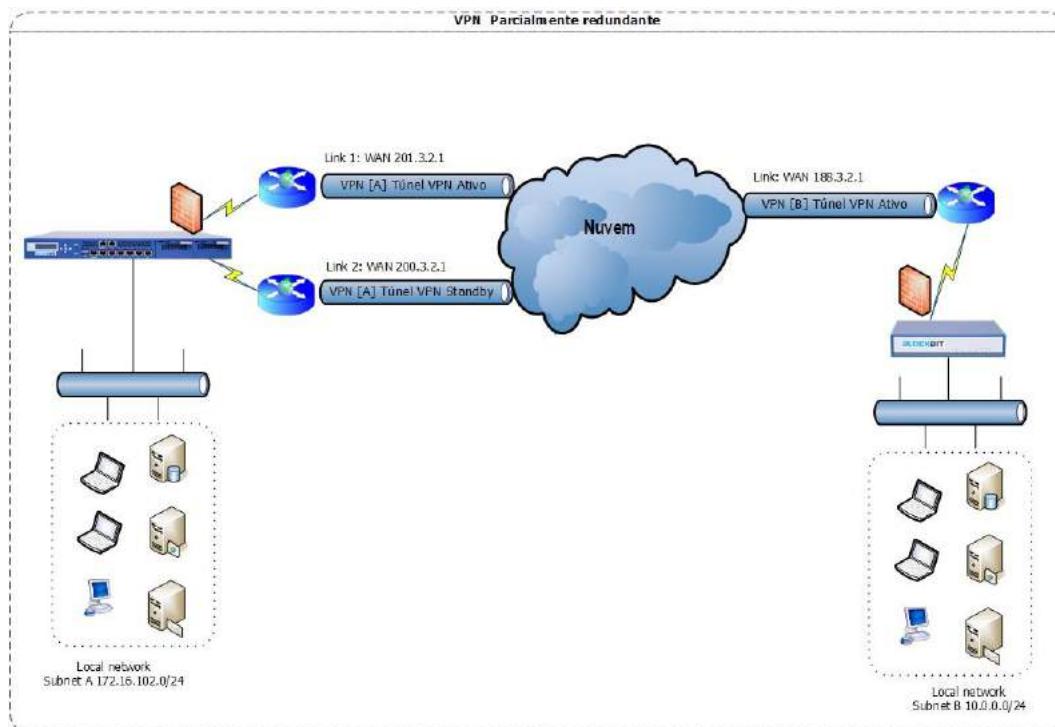
Se a comunicação com a rota do túnel ativo falhar, o serviço failover da VPN desativa e derruba o túnel ativo, e o próximo túnel failover habilitado na lista de prioridade é iniciado automaticamente.

**IMPORTANTE:** Quando um evento de failover ocorre, as conexões são perdidas em função do timeout e o tempo de reestabelecimento do túnel com o novo gateway multilink. Esse período depende dos tempos de configuração dos testes failover configurado no serviço Multilink. (Ver [Seção 17 – Multilink](#)).

No reestabelecimento do túnel VPN ocorre o mesmo processo.

### 21.3.3 VPN parcialmente redundante:

A configuração parcialmente redundante contempla somente um ponto VPN com conexões redundantes à Internet.



Este exemplo demonstra uma configuração VPN IPsec parcialmente redundante entre um dispositivo BLOCKBIT UTM e um ponto VPN IPsec (pode ser um dispositivo BB UTM ou outro dispositivo VPN com suporte a IPsec Padrão).

Somente em um ponto VPN o BLOCKBIT UTM tem duas interfaces conectadas à Internet através de diferentes provedores de internet - ISPs (Internet Service Provider). A ponta VPN IPsec Remoto possui somente uma interface conectada à internet.

---

<b>BB UTM VPN [A] – WAN 1</b>	<b>↔</b>
<b>BB UTM VPN [B] – WAN 1</b>	
<b>BB UTM VPN [A] – WAN 2</b>	<b>↔</b>

---

Este método não garante alta disponibilidade para uma conexão confiável entre dois pontos VPN IPsec. Em uma configuração de VPN parcialmente redundante somente o ponto com multilink habilitado garante disponibilidade para o tráfego VPN. Caso haja ocorrência de falha na comunicação com o ponto VPN IPsec remoto com único endereço WAN, a conexão com a VPN é perdida.

#### 21.3.4 Requisitos para a VPN FailOver

1. As interfaces do seu dispositivo BLOCKBIT UTM devem estar listadas e configuradas com o devido apontamento de gateway.
2. O Multilink Failover deve estar habilitado e configurado (Ver [Seção 17.2 - Configurações de Redundância](#)).
3. Configurar 2(dois) ou mais túneis VPN IPSec, ambos os tuneis VPN devem estar configurados para iniciar no modo “Aguardar”.
4. Para conexão de VPN utilizando links DSL, habilitar o serviço DDNS do ponto VPN com IP dinâmico (Ver [Seção 20 – DNS Dinâmico](#)).
5. Na configuração do túnel VPN dos pontos com links DSL, configurar os campos “Remote host”, “Local ID” e “Remoto ID” no padrão FQDN (Full Quality Domain Name). Exemplo: “host.domínio”.

Para o caso do site VPN com IP dinâmico, identificar com o nome do “host.domínio” de acordo a publicação no serviço DDNS (Ver [Seção 20 – DNS Dinâmico](#)).

## 21.4 Habilitando o túnel VPN IPSEC FailOver

Antes da habilitação dos túneis no modo failover, o administrador precisar configurar os túneis VPN.

Acesse **[Serviços] >> [VPN IPSEC]** e configure [N] túneis VPN IPsec para o mesmo ponto IPsec remoto para a mesma rede lan de destino baseado nas definições de compliance para habilitação do modo failover nos dispositivos BLOCKBIT UTM e o número de links redundantes habilitado no multilink. (Ver [Seção 21.2 - Configurando Túnel VPN IPsec](#)).

Configure todos os campos do formulário baseado nas informações levantadas e nas verificações dos requisitos pré-estabelecidos. Ao final clique em **[v] Habilitado** para habilitação do “Túnel” e selecione o modo de inicialização “Aguardar”, depois clique em **[ ]**.

**NOTA:** Para configurar a VPN FailOver é necessário habilitar o “Multilink”.

Acesse a Aba [FailOver] para habilitar e configurar o modo de redundância.

The screenshot shows the 'VPN IPSEC' interface with the 'Failover' tab selected. A table below the tabs displays a single row with the message 'Nenhum item encontrado' (No items found). There is a '+' button in the top right corner of the table area.

Para configuração clique em **Adicionar** [ + ]

This is a detailed view of the 'Adicionar failover' dialog. It includes fields for 'Nome' (Name) containing 'Túnel redundante VPN Matriz x VPN Filial - Link principal', 'Tunnel' (Tunnel) dropdowns, and 'Link' (Link) dropdowns. It also features a note about multilink and a 'Salvar' (Save) button.

**Note:** Para configurar o failover é necessário habilitar o multilink.

**Buttons:** Salvar

Defina um nome para o Grupo dos túneis redundantes, selecione os túneis VPN, relate-

ne-os ao link correspondente para o roteamento da conexão e clique em [ + ] para adicionar a lista de failovers. Depois clique em [ Salvar ]

Tunnel	Link
Selecionar	Selecionar
Selecionar	Selecionar
VPN Matriz x VPN Filial - Link 1	eth1 - Link Wan - Rede 172
VPN Matriz x VPN Filial - Link 2	eth2 - Link Wan 2 - Rede 192

**Adicionar failover**

<b>Nome</b>		
Túnel redundante VPN Matriz x VPN Filial - Link principal		
<b>Tunnel</b>	<b>Link</b>	
VPN Matriz x VPN Filial - Link 1	eth1 - Link Wan - Rede 172	+
VPN Matriz x VPN Filial - Link 2	eth2 - Link Wan 2 - Rede 192	-

**Observação:** Para configurar o failover é necessário habilitar o multilink

**Salvar**

Para a ordenação de prioridade entre os túneis failover clique no botão [⋮] para arrastar e ordenar a prioridade entre eles.

Dos túneis selecionados e adicionados, o primeiro túnel na lista é o principal e os demais abaixo são failover, isto é, ativados apenas em caso de falha do principal.

**VPN IPSEC**

Túneis	Failover	Acesso remoto	Monitor								
<table border="1"> <thead> <tr> <th>Nome</th> <th>Ação</th> </tr> </thead> <tbody> <tr> <td>Túnel redundante VPN Matriz x Filial</td> <td>[+]</td> </tr> <tr> <td>VPN Matriz x Filial - Link 1</td> <td>[ ]</td> </tr> <tr> <td>VPN Matriz x Filial - Link 2</td> <td>[ ]</td> </tr> </tbody> </table>				Nome	Ação	Túnel redundante VPN Matriz x Filial	[+]	VPN Matriz x Filial - Link 1	[ ]	VPN Matriz x Filial - Link 2	[ ]
Nome	Ação										
Túnel redundante VPN Matriz x Filial	[+]										
VPN Matriz x Filial - Link 1	[ ]										
VPN Matriz x Filial - Link 2	[ ]										

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



## 21.5 Configurando Acesso Remoto – VPN RAS

Acesse [Serviços] >> [VPN IPSEC].

Para configuração da VPN IPSEC RAS clique na aba **[Acesso Remoto]**.

No quadro **[VPN RAS]** configure todos os campos do formulário baseado nas informações levantadas nas verificações dos requisitos pré-estabelecidos. Ao final clique em **[V] Habilitar VPN RAS** para habilitação do serviço.

### VPN RAS

Habilitar VPN RAS

Host

vpn-bb.blockbit.com

Chave compartilhada PSK

\*\*\*\*\*

Rede virtual

192.168.254.0/24

DNS 1

192.168.1.1

DNS 2

Endereço do servidor DNS

Para permitir o acesso **VPN IPSEC RAS** a partir de clientes **VPN MS Windows®** utilizando senhas do tipo **EAP-MSCHAP v2**. Configure o quadro **[Autenticação (EAP-MS\_CHAP V2)]**, nele você deve configurar “*Usuários*”, “*Dispositivo*” e “*Senha*” para o acesso.

#### Autenticação (EAP-MSCHAP V2)

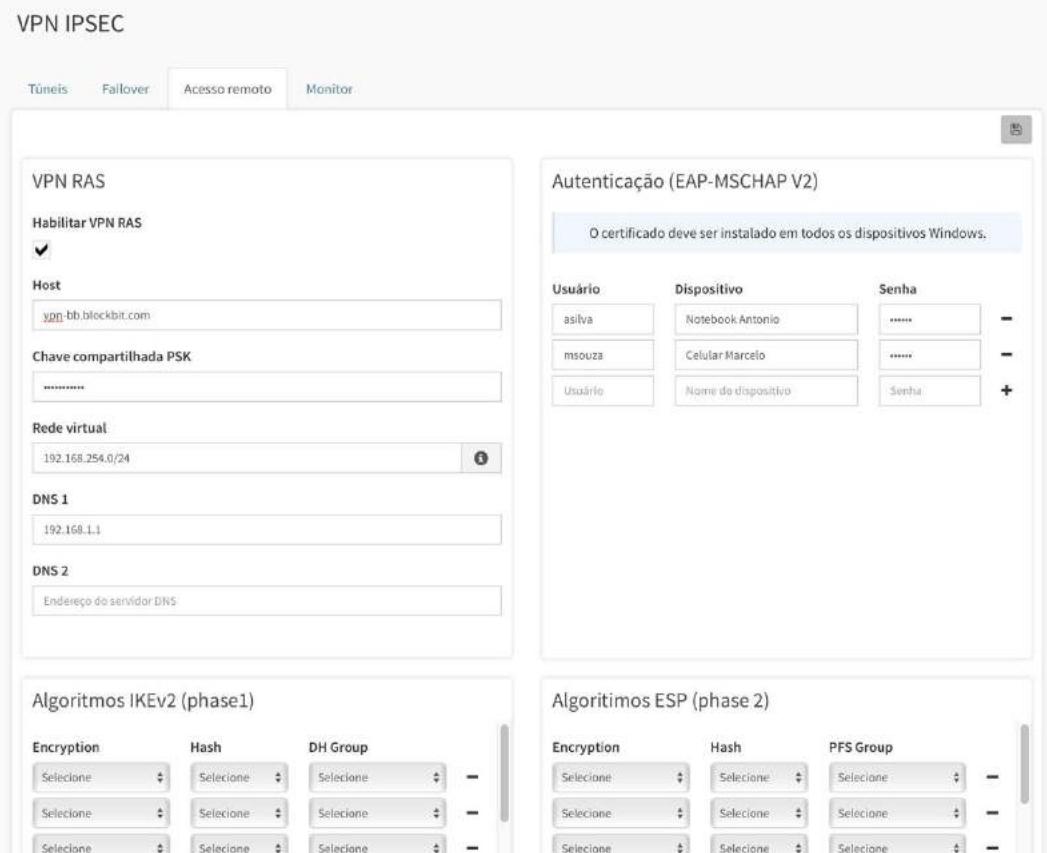
O certificado deve ser instalado em todos os dispositivos Windows.

Usuário	Dispositivo	Senha	-
asilva	Notebook Antonio	*****	-
msouza	Celular Marcelo	*****	+

**MPORTANTE:** O endereço de **host (FQDN)** configurado para o acesso **VPN RAS** deve estar publicado no servidor DNS válido e ser o mesmo utilizado na configuração para emissão da **C.A** no BLOCKBIT UTM.

**NOTA:** A conexão client VPN RAS requer a instalação da “**C.A (certificate Authority)**” em todos os dispositivos Windows.

Agora após a configuração de ambos os itens da **VPN RAS**. Clique em [  ]



The screenshot shows the 'VPN IPSEC' configuration page. The 'Acesso remoto' tab is selected. The 'VPN RAS' section contains fields for Host (vpn-bb.blockbit.com), Shared PSK (\*\*\*\*\*), Virtual Network (192.168.254.0/24), and DNS servers (192.168.1.1). The 'Autenticação (EAP-MSCHAP V2)' section includes a note about certificate installation and a table for users and devices. The 'Algoritmos IKEv2 (phase1)' and 'Algoritmos ESP (phase 2)' sections show dropdown menus for encryption, hash, and PFS group selection.

Após salvar e aplicar as configurações [  ] o serviço “Auto-configura” os campos de seleção das fases de autenticação [**Algoritmos IKEv2 (phase 1)**] e encapsulamento e criptografia [**Algoritmos ESP (phase 2)**].

Algoritmos IKEv2 (phase1)				Algoritmos ESP (phase 2)			
Encryption	Hash	DH Group		Encryption	Hash	PFS Group	
aes128	sha1	modp1024	-	aes128	sha1	modp1024	-
aes128	sha1	modp1536	-	aes128	sha1	modp1536	-
aes128	sha1	modp2048	-	aes128	sha1	modp2048	-
aes128	sha1	modp1024	-	aes128	sha256	ecp256	-
aes128	sha1	modp1536	-	aes128	sha256	modp1024	-
aes128	sha1	modp2048	-	aes128	sha256	modp1536	-
aes128	sha256	ecp256	-	aes128	sha256	modp2048	-
aes128	sha256	modp1024	-	aes128	sha1	modp1024	-
aes128	sha256	modp1536	-	aes128	sha1	modp1536	-
aes128	sha256	modp2048	-	aes128	sha1	modp2048	-
aes256	sha1	modp1024	-	aes128	sha256	modp1024	-
aes256	sha1	modp1536	-	aes128	sha256	modp1536	-
aes256	sha1	modp2048	-	aes128	sha1	modp2048	-
aes256	sha1	modp4096	-	aes128	sha256	modp4096	-
aes256	sha256	modp1024	-	aes128	sha256	modp1024	-
aes256	sha256	modp1536	-	aes128	sha256	modp1536	-
aes256	sha256	modp2048	-	aes128	sha256	modp2048	-
aes256	sha256	modp4096	-	aes128	sha384	ecp384	-
aes256	sha384	ecp384	-	aes128	sha384	modp1024	-
aes256	sha384	modp1024	-	aes128	sha384	modp1536	-
aes256	sha384	modp1536	-	aes128	sha384	modp2048	-
aes256	sha384	modp2048	-	aes128	sha1	Selecionar	-
aes256	sha384	modp4096	-	aes128	sha256	Selecionar	-
Selecionar	Selecionar	Selecionar	+	aes128	sha1	Selecionar	-
Selecionar	Selecionar	Selecionar	+	aes128	sha256	Selecionar	-
Selecionar	Selecionar	Selecionar	+	aes128	sha384	Selecionar	-
Selecionar	Selecionar	Selecionar	+	Selecionar	Selecionar	ecp256	-
Selecionar	Selecionar	Selecionar	+	Selecionar	Selecionar	ecp384	-
Selecionar	Selecionar	Selecionar	+	Selecionar	Selecionar	Selecionar	-
Selecionar	Selecionar	Selecionar	+	Selecionar	Selecionar	Selecionar	-
Selecionar	Selecionar	Selecionar	+	Selecionar	Selecionar	Selecionar	-

**NOTA:** Não se esqueça de APlicar a fila de comandos, clique no ícone:



## 21.6 Monitor VPN

Este recurso permite o administrador monitorar os túneis estabelecidos com todos os pontos de VPN, sejam eles, VPN IPSEC Tunnel ou VPN IPSEC RAS.

Clique em [Services] >> [VPN IPSEC] aba [Monitor].

VPN IPSEC							
Túneis	Failover	Acesso remoto	Monitor				
Conexão		Origem	Destino	IP/Rede	Tempo	Tráfego	Pacotes
👤 asilva	[]	77.77.77.7	199.99.99.10	192.168.254.1	00:00:36	3.98 KB	41
👤 Matriz x Filial	[]	88.88.88.8	199.99.99.10	172.16.0.10/24	00:10:36	1.96 MB	9.451

[] significa “Conexão da VPN IPSEC RAS”.

[] significa “Conexão da VPN IPSEC Tunnel”.

## 22 VPN SSL

---

A VPN SSL é o serviço responsável pelo gerenciamento no acesso de uma conexão segura sob o protocolo SSL a aplicativos e recursos da rede.

Diferentemente do IPSEC não estabelece conexões site to site. A VPN SSL trabalha na camada 7 (modelo OSI). Como SSL é um protocolo que está embutido na maioria das aplicações Web, este tipo de encapsulamento de protocolo se torna uma solução VPN mais compatível entre as aplicações. É uma modalidade de VPN que utiliza os recursos de um navegador WEB padrão para estabelecer sua conexão, funciona como um portal WEB (uma intranet pública) usado para prover aos usuários remotos acesso a aplicativos e recursos da rede privada de qualquer lugar do mundo.

O serviço de VPN SSL no BLOCKBIT UTM fornece o serviço de conexão VPN SSL Túnel que permite um usuário remoto devidamente autorizado utilizar um navegador Web moderno para acessar com segurança vários serviços da rede privada.

O tráfego entre o browser e o dispositivo BLOCKBIT UTM VPN SSL é criptografado, oferece versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação disponível através do “*Portal de autenticação*”.

## 22.1 Lista de aplicações no acesso VPN SSL

O serviço VPN SSL visa disponibilizar aos usuários o acesso de forma segura, a aplicações que ficam instaladas em uma rede privada. Através do “*Portal de Autenticação*” os usuários uma vez autenticados tem acesso ao **[Virtual Office]** um “bookmark” com a lista de aplicações disponíveis para acesso remoto.

O tráfego entre o browser e o dispositivo BLOCKBIT UTM VPN SSL é criptografado, oferece versatilidade, facilidade de uso, e controles específicos de grupos e usuários em cada modalidade de aplicação disponível através do “*Portal de autenticação*”.

A lista de aplicações disponíveis para cada usuário é definida através da interface de gerenciamento da VPN SSL, ou seja, somente os usuários previamente habilitados terão acesso às aplicações disponíveis no acesso VPN SSL.

O recurso de tunelamento de aplicações através do Portal, basicamente, consiste em fazer um desvio de Porta (Port Forward) para a aplicação de destino. Entretanto, para cada tipo de aplicação, será utilizado um método diferente.

Entre a lista de aplicações temos:

- **Aplicativos Web.**

Utilizam o recurso de Proxy Reverso no acesso ao servidor de páginas.

- **Aplicativos cliente/ servidor.**

Requer um cliente da aplicação Servidor.

- **Compartilhamentos de rede (SMB)**

Requer a configuração de um “Storage SMB” para o recurso de compartilhamento de rede.

- **Aplicativos de acesso remoto.**

- Terminal RDP
- Terminal VNC
- Terminal SSH

O portal disponibiliza um applet Java (mini aplicativo) para acesso a aplicação remota.

## 22.2 Requisitos da VPN SSL

Para a VPN SSL conseguir gerenciar uma conexão segura, precisamos antes certificar que atendemos alguns requisitos para então disponibilizar o serviço para a rede.

### 22.2.1 Requisitos BLOCKBIT UTM - VPN SSL.

1. Habilitar permissão no firewall para o serviço VPN SSL para a(s) “Zona(s) de rede” do(s) endereço(s) com permissão.  
Acesse **[Serviços] >> [Firewall]** – (Ver [Seção 11.1 – Serviços](#)).
2. Possuir uma base de usuários cadastrados no sistema, seja, usuário local; ou sincronizados (Windows/ Ldap).
3. Definir quais modelos de aplicações/aplicativos serão acessados remotamente.
  - ◆ Tunnel cliente/ servidor. Ex: “*Cliente de e-mail como o MS-Outlook*”.
  - ◆ Aplicações Web. Ex: “*Aplicação web – intranet*”.
  - ◆ Aplicativo de acesso remoto. Ex: “*Terminal SSH; Terminal VNC; Terminal Remote Desktop*”.
  - ◆ Compartilhamentos de rede SMB. Ex: “*Área comum servidor de arquivos*”.
4. Levantar os endereçamentos IPs e portas de serviço de cada aplicação para pré-configuração dos objetos **[Endereço IP]** e **[Serviço]**.
5. Para compartilhamento SMB. Requer configurar o item **[Sistema] >> [Armazenamento] >> [SMB]**.
6. Estabelecer política de USO para cada aplicação que será disponibilizada para seus respectivos usuários e seus direitos.
  - Aplicativos.
  - Lista de usuários/grupos com direito de acesso.

## 22.2.2 Requisitos nos dispositivos remotos – VPN SSL.

### 1. Navegadores web:

- Homologado somente para o navegador Mozilla Firefox versão 45.
- As aplicações Java oferecidas por meio de um navegador WEB para acesso aos aplicativos da VPN SSL operam como um applet Java (que interagem com o navegador) e requer o Plugin **NAPI** (Netscape Plugin Application Programming Interface).

### 2. Requer a instalação do JAVA – (Manter sempre atualizado – última versão).

O JAVA requer alguns ajustes de configuração para permitir execução das aplicações disponíveis pela VPN SSL.

#### Configurando o JAVA no Windows 10

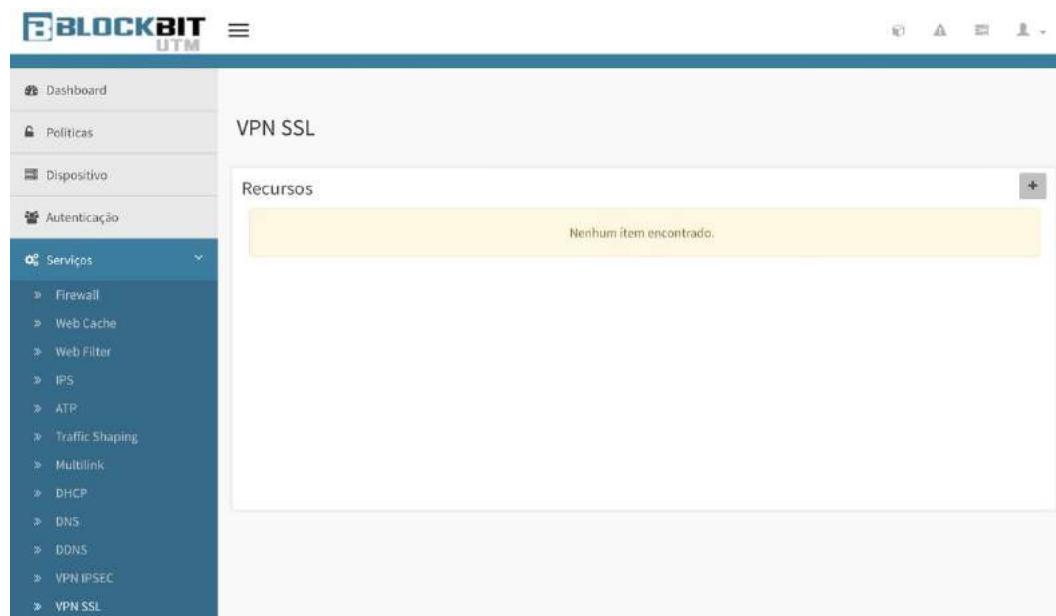


- Acesse o painel de controle do S.O. e clique em **JAVA** [ ]
- No painel de controle do JAVA.
- Na Aba **[General]**, no quadro **[Temporary Internet Files]** clique em **[Settings]**
  - Desabilitar o item
  - **[ ] keep temporary files on my computer**
- Na Aba **[Security]**, clique em **[Certificates...]**
  - Selecione o tipo de certificado para a importação.
  - Selecione >> **[Trusted Certificate]** na Aba **[User]** clique em **[Import]** altere a seleção do tipo de arquivo para **[All files]** e importe a CA. Ex.: “*Blockbit UTM Root CA.crt*”.

Finalizado! O JAVA está configurado para permitir a execução das aplicações do portal VPN SSL.

## 22.3 Configurando VPN SSL

Acesse [Serviços] >> [VPN SSL].



Para visualizar a lista de recursos que serão disponibilizados pelo *Portal de Autenticação* para o acesso via VPN SSL, e definir as políticas de acesso aos aplicativos da sua rede, clique em **Adicionar** [+] e navegue entre os tipos de recursos e em seguida defina suas políticas.

Túnel	Endereço
RDP	Porta
VNC	Porta local
SSH	Comando externo
WEB	Comando externo. Ex.: 'mstsc.exe /w:1024 /h:768'
SMB	Descrição

**Salvar**

### 22.3.1 Exemplo – Acesso web Tunnel para aplicações do tipo Cliente/ Servidor.

Este exemplo configura o acesso ao serviço de e-mail (*imap*) local através de um aplicativo cliente/ servidor.

*Política 1: Acesso ao Thunderbird - porta Imap 143.*

<b>Aplicativo cliente</b>	Mozilla Thunderbird.
<b>IP Local</b>	192.168.1.22/32
<b>Porta da aplicação</b>	143
<b>Porta local</b>	7155
(Porta alta randômica/ ou definida pelo usuário).	
<b>Comando externo</b>	thunderbird.exe
(Requer que o comando esteja no PATH do S.O.).	
<b>Descrição</b>	Thunderbird - IMAP
<b>Permissão</b>	<a href="mailto:todos@blockbit.com">todos@blockbit.com</a>
(Pode ser aplicada por usuário ou grupos).	

*Política 2: Acesso ao Thunderbird - porta SMPT submission 587.*

<b>Aplicativo cliente</b>	Mozilla Thunderbird.
<b>IP Local</b>	192.168.1.22/32
<b>Porta da aplicação</b>	587
<b>Porta local</b>	7156
(Porta alta randômica/ ou definida pelo usuário).	
<b>Comando externo</b>	thunderbird.exe
(Requer que o comando esteja no PATH do S.O.).	
<b>Descrição</b>	Thunderbird – SMTP
<b>Permissão</b>	<a href="mailto:todos@blockbit.com">todos@blockbit.com</a>
(Pode ser aplicada por usuário ou grupos).	

### 22.3.2 Exemplo – Acesso remoto – RDP (Remote Desktop).

Este exemplo configura o acesso ao serviço MS-Terminal Service remote desktop.

*Política 1: Acesso ao MSTS (RDeekTop) porta 3389.*

<b>Aplicativo</b>	Terminal RDeskTop (MSTSC).
<b>IP Local</b>	192.168.1.10/32
<b>Porta da aplicação</b>	3389
<b>Porta local</b>	59497 <small>(Porta alta randômica/ ou definida pelo usuário).</small>
<b>Comando externo</b>	mstsc.exe <small>(Requer que o comando esteja no PATH do S.O.).</small>
<b>Descrição</b>	Windows Server RDP
<b>Permissão</b>	<a href="mailto:todos@blockbit.com">todos@blockbit.com</a> <small>(Pode ser aplicada por usuário ou grupos).</small>

### 22.3.3 Exemplo – Acesso remoto – VNC (Remote Desktop).

Este exemplo configura o acesso ao serviço VNC remote desktop.

*Política 1: Acesso ao VNC (RDeekTop) porta 5800.*

<b>Aplicativo</b>	Terminal VNC RDeskTop
<b>IP Local</b>	192.168.254.184/32
<b>Porta da aplicação</b>	5800
<b>Porta local</b>	49701 <small>(Porta alta randômica/ ou definida pelo usuário).</small>
<b>Descrição</b>	Servidor App 01 VNC
<b>Permissão</b>	<a href="mailto:support@blockbit.com">support@blockbit.com</a> <small>(Pode ser aplicada por usuário ou grupos).</small>

#### 22.3.4 Exemplo – Acesso remoto – SSH (Secure Shell Remote Desktop).

Este exemplo configura o acesso ao serviço SSH – Secure Shell Remote Desktop.

*Política 1: Acesso ao terminal SSH porta 22.*

<b>Aplicativo</b>	Terminal SSH
<b>IP Local</b>	192.168.1.202/32
<b>Porta da aplicação</b>	22
<b>Porta local</b>	51342
(Porta alta randômica/ ou definida pelo usuário).	
<b>Descrição</b>	Servidor Web SSH
<b>Permissão</b>	<a href="mailto:support@blockbit.com">support@blockbit.com</a>
(Pode ser aplicada por usuário ou grupos).	

#### 22.3.5 Exemplo – Acesso aplicação Web (Http/Https).

Este exemplo configura o acesso a uma aplicação WEB interna (Intranet/Extranet).

*Política 1: Acesso a aplicação Web local (Intranet) colaboradores.*

<b>Aplicativo</b>	Aplicação WEB Local - Intranet
<b>Endereço da url</b>	http://intranet.blockbit.com:8080
<b>Porta local</b>	16133
(Porta alta randômica/ ou definida pelo usuário).	
<b>Descrição</b>	Intranet
<b>Permissão</b>	<a href="mailto.todos@blockbit.com">todos@blockbit.com</a>
(Pode ser aplicada por usuário ou grupos).	

### 22.3.6 Exemplo – Acesso a serviços de compartilhamento SMB.

Este exemplo configura o acesso a recursos de compartilhamento de rede SMB.

*Política 1: Acesso a área comum compartilhada – tipo SMB.*

<b>Aplicativo</b>	Área de dados compartilhada (SMB)
<b>Compartilhamento SMB</b>	Arquivos Marketing <small>(Nome do compartilhamento definido no SO).</small>
<b>Descrição</b>	Material Marketing
<b>Permissão</b>	<a href="mailto:todos@blockbit.com">todos@blockbit.com</a> <small>(Pode ser aplicada por usuário ou grupos).</small>

## 22.4 Adicionando um Túnel (Aplicativo Cliente/ Servidor).

Para adicionar um aplicativo “Túnel” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com um aplicativo “*Cliente / Servidor*”. Depois clique em [ **Salvar**].

Vamos exemplificar a configuração de acordo com as políticas definidas. (Ver [Seção 22.3.1 - Acesso web Tunnel...](#)).

**Exemplo – Acesso web Tunnel para aplicações do tipo Cliente/ Servidor**

**Política 1:** Acesso a porta Imap – porta 143.

Túnel	Endereço	192.168.1.22/32	
RDP	Porta	143	Porta local
VNC	Comando externo	thunderbird	
SSH	Descrição	Thunderbird IMAP	
WEB			
SMB			

**Política 2:** Acesso a porta SMPT submission – porta 587.

Túnel	Endereço	192.168.1.22/32	
RDP	Porta	587	Porta local
VNC	Comando externo	thunderbird	
SSH	Descrição	Thunderbird SMPT	
WEB			
SMB			

**ATENÇÃO:** Para o funcionamento do acesso a aplicação “*Cliente/servidor*”, o administrador deve configurar o aplicativo cliente do dispositivo remoto para o acesso aos aplicativos do tipo túnel para conectar-se no endereço de destino “*localhost*”, para a “*porta alta local*” definida e configurada de acordo a política de acesso ao recurso.

#### 22.4.1 Adicionando um acesso RDP.

Para adicionar um aplicativo “RDP” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com um aplicativo “*Remote Desktop*”. Depois clique em [].

Vamos exemplificar a configuração de acordo com as políticas definidas (Ver [Seção 22.3.2 - Acesso remoto RDP...](#)).

Recurso

Túnel	Endereço	Porta	Porta local
RDP	192.168.1.10/32	3389	59497
VNC			
SSH			
WEB	mstsc.exe		
SMB			

**Comando externo**

**Descrição**

The screenshot shows a configuration dialog for a Remote Desktop connection. On the left, a sidebar lists tunnel types: Túnel, RDP, VNC, SSH, WEB, and SMB. The RDP option is selected and highlighted with a blue bar. The main area contains fields for 'Endereço' (Address) set to '192.168.1.10/32', 'Porta' (Port) set to '3389', and 'Porta local' (Local Port) set to '59497'. Below these are sections for 'Comando externo' (External Command) containing 'mstsc.exe' and 'Descrição' (Description) containing 'Windows Server RDP'. At the bottom right is a blue 'Salvar' (Save) button.

## 22.4.2 Adicionando um acesso VNC.

Para adicionar um aplicativo “VNC” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com um aplicativo “Remote Desktop”. Depois clique em [ **Salvar**].

Vamos exemplificar a configuração de acordo com as políticas definidas (Ver [Seção 22.3.3 - Acesso remoto VNC...](#)).

Recurso

Túnel	Endereço	
RDP	192.168.254.184	[]
VNC	5800	[]
SSH		
WEB	Descrição Servidor App 01 VNC	
SMB		

**Salvar**

### 22.4.3 Adicionando um acesso SSH.

Para adicionar um aplicativo “SSH” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com um aplicativo “Remote SSH”. Depois clique em [].

Vamos exemplificar a configuração de acordo com as políticas definidas (Ver [Seção 22.3.4 - Acesso remoto SSH...](#)).

Recurso

Túnel	Endereço		
RDP	<input type="text" value="192.168.254.202/32"/>	[]	
VNC	<input type="text" value="22"/>	[]	Porta local <input type="text" value="51342"/>
<b>SSH</b>	<b>Descrição</b>		
WEB	<input type="text" value="Servidor Web SSH"/>		
SMB			

Salvar

#### 22.4.4 Adicionando uma Aplicação Web

Para adicionar um aplicativo “WEB” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com uma aplicação “WEB”. Depois clique em [ **Salvar**].

Vamos exemplificar a configuração de acordo com as políticas definidas (Ver [Seção 22.3.5 - Acesso aplicação Web...](#)).

Recurso

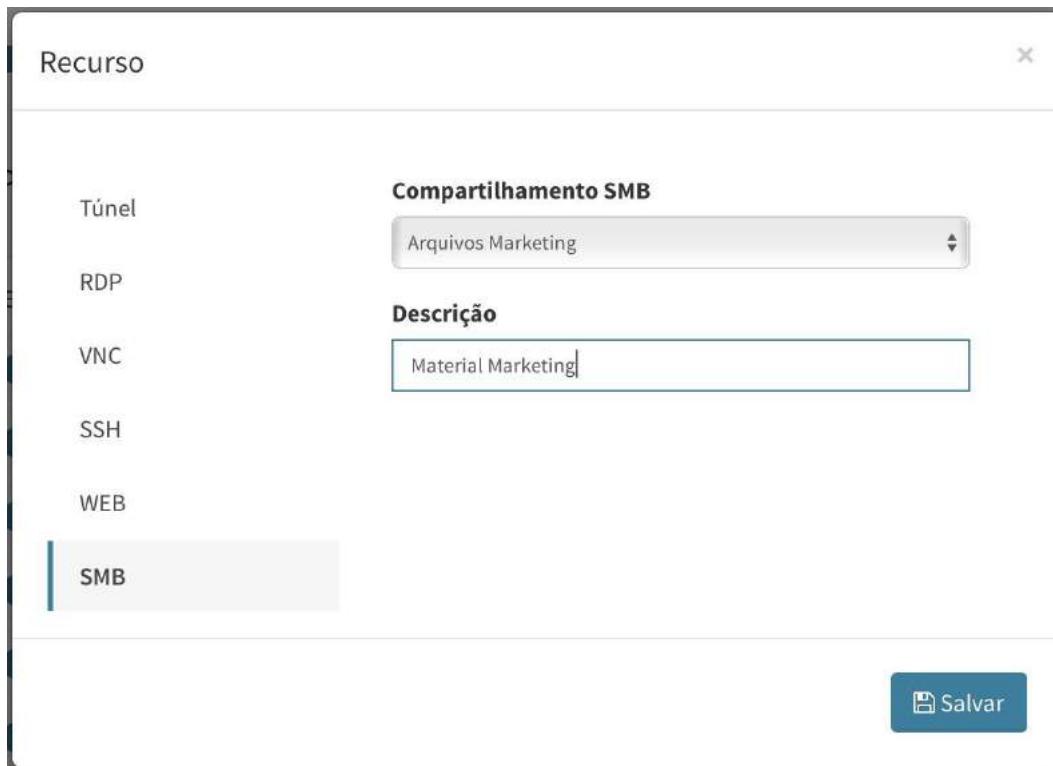
Túnel	Url	Porta local
RDP	<input type="text" value="http://intranet.blockbit.com:8080"/>	<input type="text" value="16133"/>
VNC	<b>Descrição</b> <input type="text" value="Intranet"/>	
SSH		
<b>WEB</b>		
SMB		

**Salvar**

#### 22.4.5 Adicionando um Compartilhamento SMB (samba)

Para adicionar um aplicativo “SMB” clique em **Adicionar** []. Configure o formulário de acordo com as especificações para conexão com um serviço de compartilhamento “SMB”. Depois clique em [].

Vamos exemplificar a configuração de acordo com as políticas definidas (Ver [Seção 22.3.6 - Acesso a serviços...](#)).



## 22.4.6 Gerenciando e Definindo Permissões.

Esta interface permite “Adicionar”, “Editar”, “Remover” as aplicações VPN SSL e gerenciar as *permissões* de acesso de cada aplicação cadastrada.

Recursos	
	Intranet
	Material Marketing
	Servidor App 01 VNC
	Servidor Web SSH
	Thunderbird IMAP
	Thunderbird SMTP
	Windows Server RDP

Agora podemos Habilitar as permissões e selecionar “*Usuários/Grupos*” e “*Tabela de horários*” com permissão de acesso as respectivas aplicações de acordo às políticas definidas. Clique em [ ] para cada aplicação da lista e selecione os “*Usuários*” ou “*Grupo*” com permissão sobre a aplicação de acordo com as definições das políticas aplicadas. Depois clique em [ ].

Permissões

Usuários  
Adicionar tag

Grupos  
todos@blockbit.com  Adicionar tag

Horário  
Comercial

Salvar

## 22.5 Estabelecendo Acesso VPN SSL

Dentre as políticas de acesso aos recursos de rede, o administrador pode definir que as comunicações com alguns destes serviços sejam disponibilizadas somente através de VPN.

Um dos meios para acesso via VPN às aplicações de rede é através do acesso ao portal de Autenticação. Somente o portal permite o acesso às aplicações de modo seguro e confiável, por estabelecer os acessos criptografados e independentes da origem, sejam as classes de rede “*LAN*”; “*DMZ*”; ou “*WAN*”.

Para estabelecer a comunicação com o “*Virtual Office*”, o usuário precisa primeiramente acessar o portal de autenticação

Uma vez autenticado, caso tenha permissão de acesso a algum aplicativo, o usuário terá acesso ao **[Virtual Office]** através de um “*bookmark*” com a lista de aplicações disponíveis para seu acesso.

### Acessando o portal de autenticação

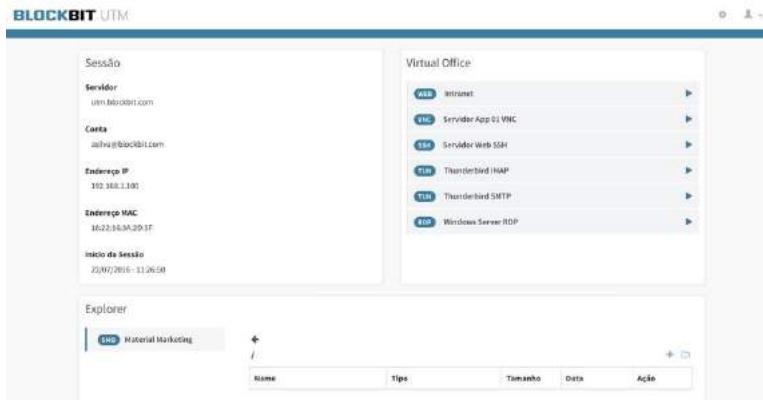
O Virtual Office é parte integrante do “*Portal de autenticação*” e tem como principal objetivo oferecer através de um navegador. Ex: MSIE ou Mozilla Firefox, executar “Aplicativos” e “Recursos de rede” sob uma conexão segura a VPN SSL.

Para acesso ao portal de autenticação, digite:

<https://utm.blockbit.com:9803> ou <https://192.168.1.1:9803>

Vamos fazer um acesso utilizando um usuário membro de um grupo com permissões no acesso a VPN SSL.





Agora para acesso em qualquer uma das aplicações basta clicar sobre a [Descrição] ou o ícone [ ].

**NOTA:** Sabemos que alguns recursos exigem a execução de um APPLET JAVA, pode ser que o navegador solicite permissão para execução do aplicativo.

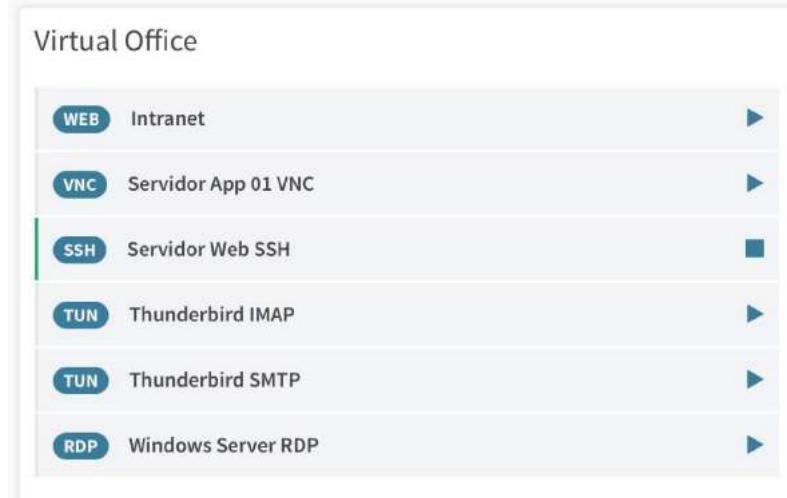
Se isso ocorrer, mesmo que o administrador já tenha aplicado os direitos e permissões no APPLET JAVA mencionados nos requisitos, **Permita sua execução.**

Vamos exemplificar alguns acessos:

O Navegador abre automaticamente uma **ABA** com o acesso a aplicação “WEB” definida na regra.

**NOTA:** TODA CONEXÃO TUNEL SSL executa uma conexão “localhost” na porta Forward “*porta local*” definida na política.

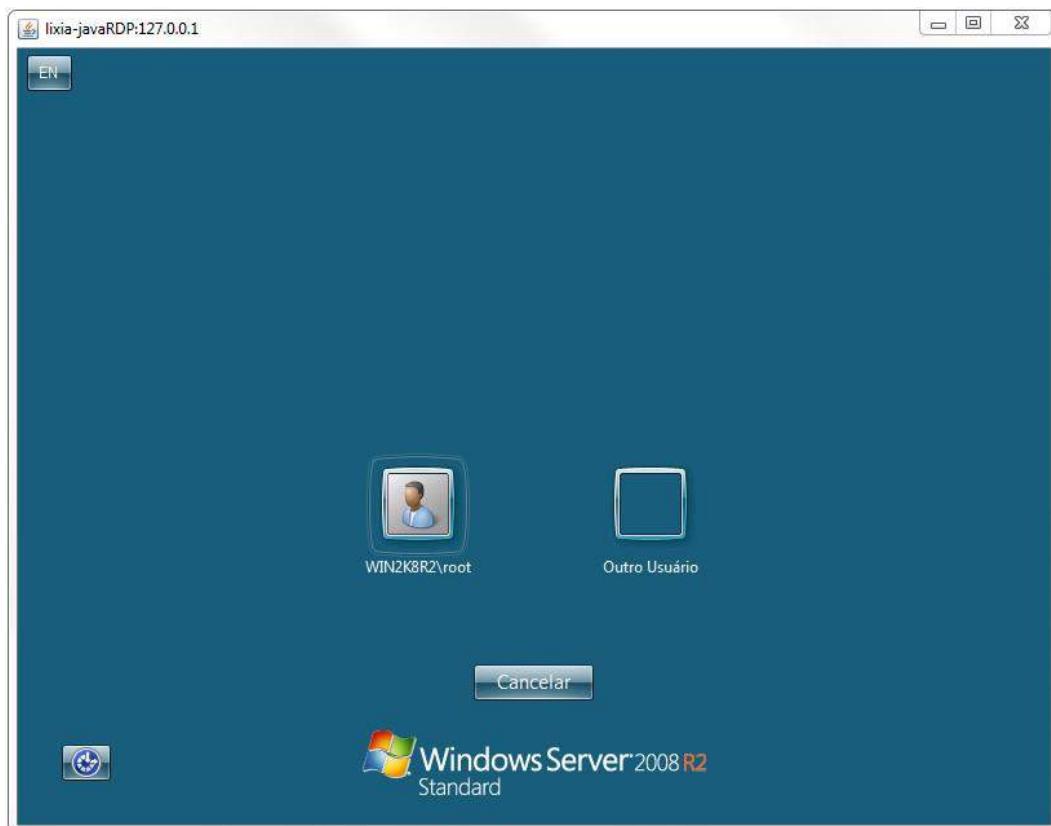
Enquanto o usuário estiver com a conexão estabelecida, no portal de autenticação do “usuário” o “status” de conexão é retornado assim:



Para derrubar a sessão o usuário basta clicar sobre o botão [ ].

Clicando sobre [ RDP Windows Server RDP ]

O navegador abre automaticamente em outra janela um quadro para seleção da resolução de tela para apresentação do Remote Desktop.



Coneção com o servidor Remote Desktop estabelecida com sucesso!

## 23 Entendendo as políticas de compliance

---

Todos os recursos de gerenciamento dos serviços UTM, “*Filtro de conteúdo Web*”, “*Filtro e controle de aplicativos da WEB 2*”, “*Interceptação SSL*”, “*Inspeção IPS*”, “*Inspeção ATP*”, “*Roteamento*”, “*Controle QoS (Traffic Shaping)*”, “*Garantia e prioridade de tráfego*”, “*Controle de Cota de tráfego e tempo*”, “*Controle de tamanho de arquivos*”, “*Filtros de cabeçalho e conteúdo*”, “*Balanceamento de link*”, “*Múltiplos serviços*”, “*NAT*” e “*Proxy*”, são aplicados através das políticas de compliance.

A definição das regras e políticas de segurança integram em uma mesma interface interativa todos esses recursos, e é possível aplicar em uma mesma política um conjunto de filtros que componham os recursos integrados. A interface permite rastrear todas as políticas a partir de “*TAGs*” que possibilitam agrupar as regras por finalidade o que facilita os filtros às pesquisas das políticas. As tags são adicionadas automaticamente pelo sistema ou o administrador pode definir uma.

---

## 23.1 Básico de Políticas de Compliance

1. Em apenas uma interface de configuração, é possível integração de [N] recursos em uma única política.

- Categoria WEB
- Controle de Aplicativos
- Controle de Banda
- Múltiplos Serviços
- QoS
- Cota de tempo e Tráfego
- Escolha de link e Redundância
- Controle de vírus e Malware

2. A configuração ou habilitação dos serviços e recursos, não implicam em criação de uma política de segurança.

À Exceção dos serviços “Multilink” e “Firewall”, que contemplam regras ou políticas exclusivas no próprio serviço, as políticas de segurança não são aplicadas individualmente em cada serviço.

3. As políticas de segurança integram [N] condições de análises, que interagem com os diversos recursos de cada serviço, e isso tudo em uma mesma política de segurança.

O que torna o gerenciamento das políticas muito mais fácil e dinâmico para o administrador.

4. As políticas atuam em camadas e o seu comportamento de análise atua no modo “First Match Wins”. (Literalmente quer dizer... O 1º entre os concorrentes VENCE).

5. As políticas de segurança são cadastradas por prioridade e suportam reordenação.

Através da avaliação dos logs e dos relatórios estatísticos, é possível reavaliar as prioridades e reordenar as políticas de segurança, de acordo com o volume ou importância do tráfego.

Por consequência melhora no desempenho do servidor.

6. As ações das políticas de segurança são:

- Permitir.
- Bloquear.
- Inspeção de Segurança: IPS.
- Inspeção de Segurança: ATP.

Estes são os primeiros conceitos básicos que o administrador deve conhecer.

**Recursos das políticas de compliance.**

- Método de operação.
  - First-match wins.
  - Ordenação por prioridade.

Relação direta com o desempenho do firewall suporta a funcionalidade multithread que disponibiliza o máximo proveito dos processadores. Permite ordenar as políticas, de modo que as políticas mais utilizadas sejam realocadas acima das políticas menos utilizadas, resultando em mais velocidade para as análises.

A definição das políticas de compliance atendem as seguintes especificações e conjunto de filtros e condições para as tomadas de ação.

Abaixo a lista das “Ações” **VERSUS** “Condições das regras”

Ações
Permitir
Bloquear
Inspeção: ATP
Inspeção: IPS

**V E R S U S...**

**Condição POR:** Condições das políticas.

	Agrupamento de devices ou zonas de rede. Device.
<b>Origem</b>	Endereço IP. Endereço MAC. Autenticação de (Usuários/ Grupos)
<b>Destino</b>	Endereço IP. Múltiplos serviços (Portas e Protocolos). Serviços Web - redirecionamento de serviços para o proxy. (*) Interceptação SSL para os serviços redirecionados para o proxy. (*)

	Categorias web. (*) Aplicativos (Para os aplicativos via proxy dos serviços de conexão HTTPS). (*)
<b>Conteúdo</b>	Navegadores. (*) Filtros de métodos do tráfego HTTP. (*) Filtros por URL (Palavra-chave ou expressões regulares). (*)
<b>Roteamento.</b>	Tabela de horário. Tabela de período/ data. Link redundante. (Por prioridade de link). Suporte a NAT. (Por device ou por endereço IP). Via Proxy Explicito (Para conexões de origem centralizadas via Terminal Service).
	QoS – (Por níveis de prioridade para qualquer tipo de conexão “origem/destino”). Filtro de tipo de conteúdo. (*) Filtro de cabeçalho HTTP. (*) Cota de Tempo e Tráfego. (*)
<b>Controles.</b>	Tamanho máximo de arquivo para download. (*) Tamanho máximo de arquivo para upload. (*) TTL (Time To Live). Tipos de pacotes. (Unicast/ Broadcast/ Multicast). Conteúdo do pacote (Hexa/ String). QoS - (Prioridades e roteamento dos pacotes por classes ToS e DSCP).
(*)	(*) Estes controles atendem SOMENTE ao tráfego de pacotes via proxy.

---

## 24 Políticas de Compliance

Neste tópico vamos abordar as políticas de compliance.

A solução contempla algumas políticas pré-configuradas pelo sistema. Essas políticas visam a implementação básica para o gerenciamento e controle do acesso a internet.

A implementação ÚNICA e EXCLUSIVA das políticas padrões não caracterizam que seu ambiente esteja com a melhor política implementada. Esse conjunto de políticas tem como finalidade única, auxiliar a fase inicial de implementação e não tem intenção nenhuma de se propor como uma política final.

### 24.1 Políticas Padrões

Vamos conhecer as políticas padrões, Clique em **[Políticas]**.

Nome	Ação
Webex	Permitir
Whatsapp	Bloquear
Skype	Bloquear
Risco de Segurança	Bloquear
Perda de Produtividade	Bloquear
SSL ByPass	Permitir
Segurança Ética	Bloquear
Filtro de Conteúdo	Inspeccionar ATP
Controle de Ameaças	Inspeccionar ATP

A partir deste tópico vamos expor como foram definidas as políticas de compliance padrões.

Definição de alguns critérios usados para elaboração das políticas padrões:

- Controlar e inspecionar todo o tráfego NAT da rede LAN – Inspecionar o tráfego usando os recursos da base do ATP (Advanced Threat Protection).
- Permitir o tráfego [WEB via Proxy] da rede LAN. Com interceptação SSL e inspeção profunda pelo ATP (Advanced Threat Protection).
- Permitir By-pass para o tráfego SSL [HTTPS] para as redes sem a instalação da CA. (Certification Authority) em seus dispositivos.
- Bloqueio do tráfego [WEB via Proxy] para sites de categorias com conteúdo inapropriado e que caracterize problemas de segurança ética.
- Bloqueio do tráfego [WEB via Proxy] para sites de categorias com conteúdo inapropriado e que caracterize perda de produtividade.
- Bloqueio do tráfego [WEB via Proxy] para sites de categorias com conteúdo inapropriado e que caracterize risco de segurança.
- Bloqueio do tráfego de serviços de mensageria e comunicadores sem Filtro ou monitoração.
- Bloqueio do tráfego de serviços de mensageria e comunicadores “Mobile” sem Filtro ou monitoração.
- Permitir o tráfego de serviços de Áudio e Vídeo conferencia.

Vale lembrar que as políticas são ordenadas por “*Prioridade*”. Vamos apresentá-las na ordem de configuração. As ações de cadastro das políticas acontecem de baixo para cima, ou seja, a última política cadastrada sempre fica ACIMA.

A 1ª política será listada abaixo, “*menor prioridade*”, e a última política listada acima, “*maior prioridade*”.

Lembrem-se as ações são aplicadas considerando o método “**First Match Wins**” (Que literalmente quer dizer... O 1º entre os concorrentes VENCE). Identificada a política em que o tráfego se enquadra nas **Condições definidas** encerra a análise abandonando a tabela das políticas e aplicando a “*Ação*” e o “*Roteamento*” definido.

### Definição das políticas padrões.

Foram aplicadas as políticas usando os critérios definidos acima. Segue abaixo as ordens das políticas que foram definidas considerando as ações e condições para cada um respectivamente conforme a descrição abaixo.

Detalhamento da ordem de configuração das políticas de compliance, e sua finalidade.

#### 24.1.1 Política 1 – Controle de Ameaças

Controle e inspeção do tráfego geral da rede local pelo ATP (*Advanced Threat Protection*) - (*Encaminhamento da rede local para a internet por mascaramento - NAT*).

Origem	LAN
Roteamento	Inspecionar (Nat)
Destino	Outros serviços

**Nat**

**Inspecionar: ATP**

#### 24.1.2 Política 2 – Filtro de Conteúdo

Filtros e controle do tráfego WEB (*Http* e *Https*) da rede local via **Proxy** com interceptação SSL e inspeção pelo ATP (*Advanced Threat Protection*).

Origem	LAN
Roteamento	Inspecionar: ATP
Destino	Serviços web
Conteúdo	Interceptar SSL

**Interceptar SSL**   **Serviços WEB**

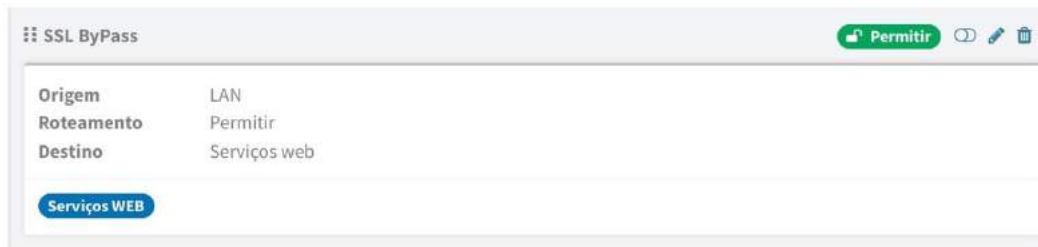
**Inspecionar: ATP**

### 24.1.3 Política 3 – SSL ByPass

Permissão By-pass para o tráfego WEB SSL (*Https*) da rede local **via Proxy**.

Regra conceitual durante a implementação.

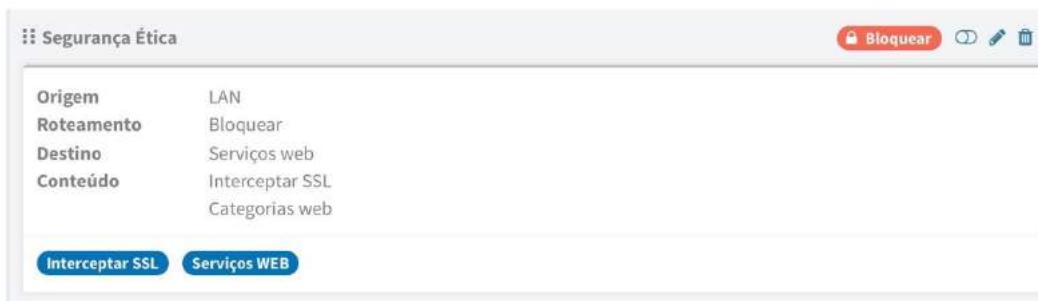
**Recomendação:** “Habilitar esta regra enquanto a CA. (Certification Authority) ainda não estiver instalada em todos os dispositivos da rede”.



### 24.1.4 Política 4 – Segurança Ética

Bloqueio do tráfego WEB (*Http* e *Https*) da rede local **via Proxy** com interceptação SSL para sites de categorias com conteúdo inapropriado e que caracteriza “*Falta de ética*”.

Lista de categorias incluídas na política: “*Adult Material, Adult Content, Nudity, Sex, Abused Drugs, Illegal or Questionable, Pedophilia, Violence and others*”.



### 24.1.5 Política 5 – Perda de Produtividade

Bloqueio do tráfego *WEB* (*Http e Https*) da rede local **via Proxy** com interceptação SSL para sites de categorias com conteúdo inapropriado e que caracteriza “*Perda de produtividade*”.

Lista de categorias incluídas na política: “*Entertainment, MP3 and Audio Download Services, Games, Shopping, Internet Auctions, Society and Lifestyles, Alcohol and Tobacco, Personals and Dating, Restaurants and Dining, Hobbies, Social Networking and Personal Sites, Sports, Sport Hunting and Gun Clubs*” and others.

Origem	LAN
Roteamento	Bloquear
Destino	Serviços web
Conteúdo	Interceptar SSL Categorias web

**Interceptar SSL**   **Serviços WEB**

### 24.1.6 Política 6 – Risco de Segurança

Bloqueio do tráfego *WEB* (*Http e Https*) da rede local **via Proxy** com interceptação SSL para sites de categorias com conteúdo inapropriado e que caracteriza “*Risco de segurança*”.

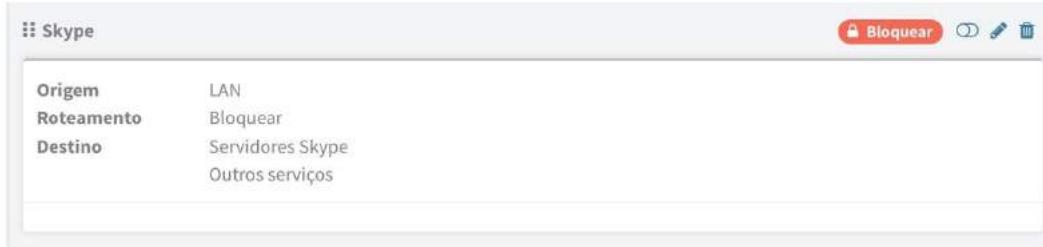
Lista de categorias incluídas na política: “*Hacking, Proxy avoidance, Web hosting, Computer Security, Internet Communication, Web Chat, Web Mail, Malicious, Spyware*” and others.

Origem	LAN
Roteamento	Bloquear
Destino	Serviços web
Conteúdo	Interceptar SSL Categorias web

**Interceptar SSL**   **Serviços WEB**

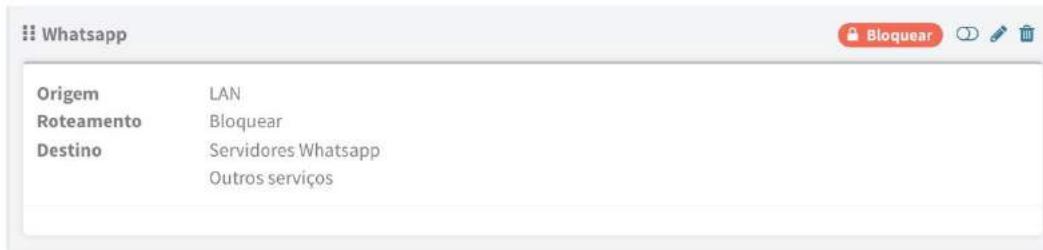
### 24.1.7 Política 7 – Skype

Bloqueio do tráfego de serviços de mensagerias e comunicação do aplicativo “*Skype*”.



### 24.1.8 Política 8 – Whatsapp

Bloqueio do tráfego de serviços de mensageria e comunicação mobile via aplicativo “*WhatsApp*”.



### 24.1.9 Política 9 – Webex

Permissão do tráfego de serviços de Áudio e Vídeo conferencia do aplicativo “*WebEX – WEB Cisco Conference*” por mascaramento (NAT) dos protocolo TCP e UDP.



**NOTA:** As políticas padrões são populadas no modo [  ] desabilitado.

## 24.2 Interface de Políticas de Compliance

Neste capítulo vamos conhecer a interface de configuração das políticas. Vamos navegar entre os tipos e condições possíveis para criação de uma política e identificar as principais diferenças para definição de políticas de acesso Web via Proxy, NAT e Encaminhamento.

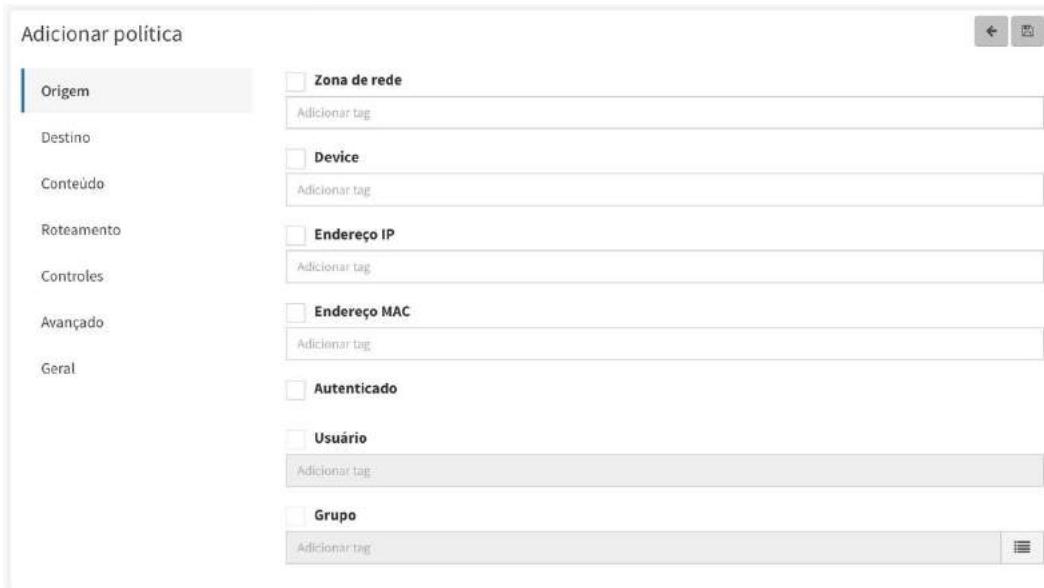
No menu principal acesse **[Políticas]**.

Name	Status	Actions	
Webs	Permitir		
Whatsapp	Blockear		
Skype	Blockear		
Risco de Segurança	Blockear		
Perda de Produtividade	Blockear		
SSL ByPass	Permitir		
Segurança Etica	Blockear		
Filtro de Conteúdo	Inspeccionar ATP		
Controle de Ameaças	Inspeccionar ATP		

Clique em **Adicionar** [].

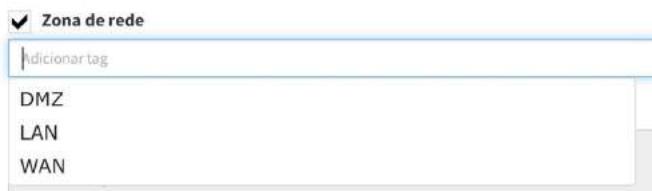
## 24.3 Origem

A aba Origem fornece diversos filtros para especificar o escopo de origem, sendo obrigatório a escolha de pelo menos um filtro.



### 24.3.1 Zona de Rede

As interfaces de rede podem ser sinalizadas com siglas como LAN, WAN e DMZ para facilitar a organização e criação de políticas segmentando por tipo rede.



Significado de algumas siglas:

- LAN (Local Area Network) – Refere-se a Rede Local.
- WAN (Wide Area Network) – Refere-se ao Link de Conexão Externa.
- DMZ (DeMilitarized Zone) – Refere-se a uma Rede de Serviços que estarão expostos a Conexão Externa.

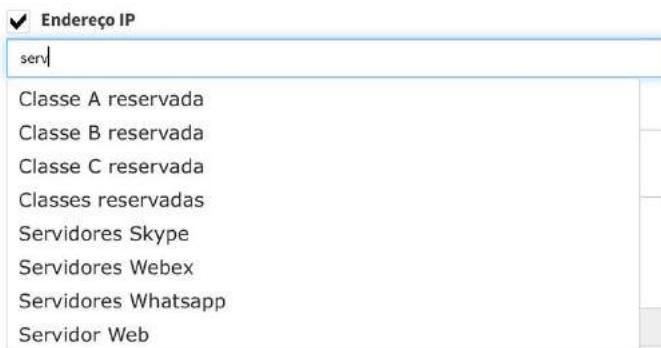
### 24.3.2 Device

Identificação da interface de rede a ser utilizada como filtro de origem.



### 24.3.3 Endereço IP

Objeto(s) de Endereço IP (IPs, redes ou conjuntos) para serem utilizados como filtro de origem.



### 24.3.4 Endereço MAC

Objeto(s) de Endereço Mac Address para serem utilizados como filtro de origem.



### 24.3.5 Autenticado

Opção que determina que a política exige autenticação.



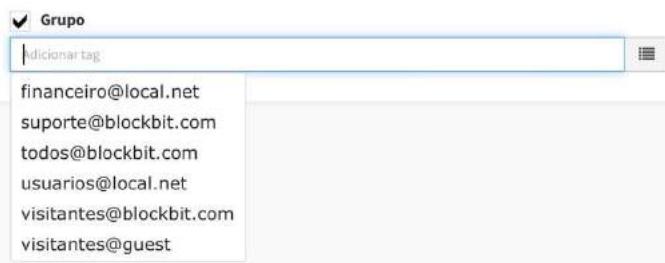
### 24.3.6 Usuário

Permite especificar usuário(s) em que a política se aplica.



### 24.3.7 Grupo

Permite especificar grupo(s) em que a política se aplica.

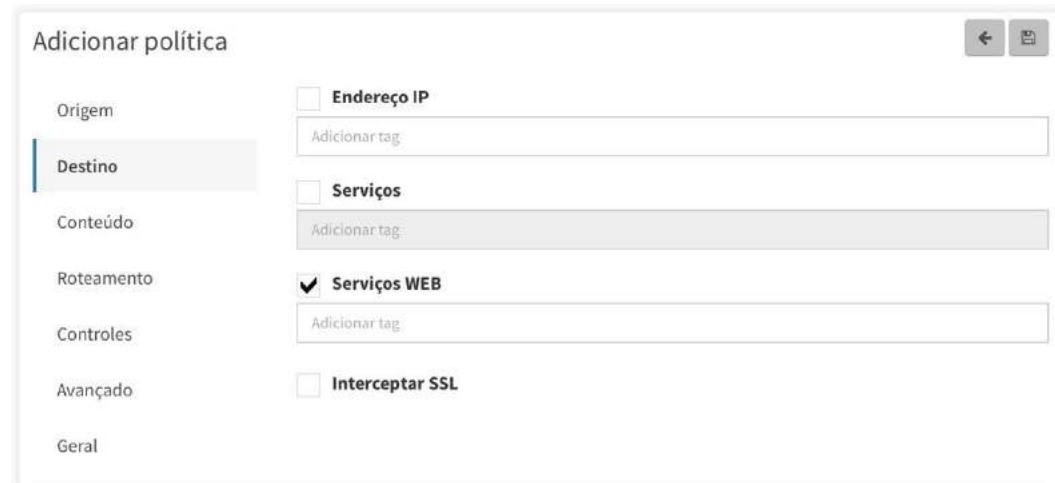


Utilizando o botão [ ] permite a seleção dos grupos.



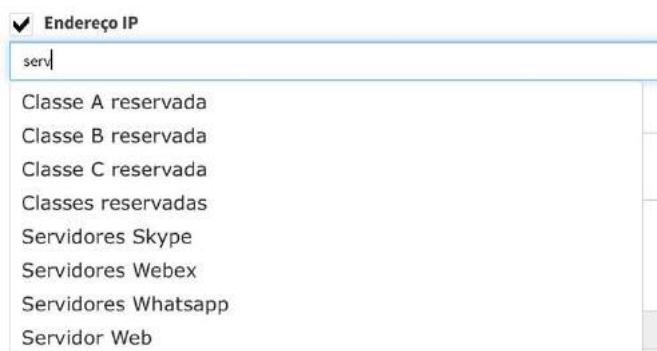
## 24.4 Destino

A aba Destino fornece diversos filtros para especificar o escopo de destino, sendo obrigatório a escolha de pelo menos um filtro.



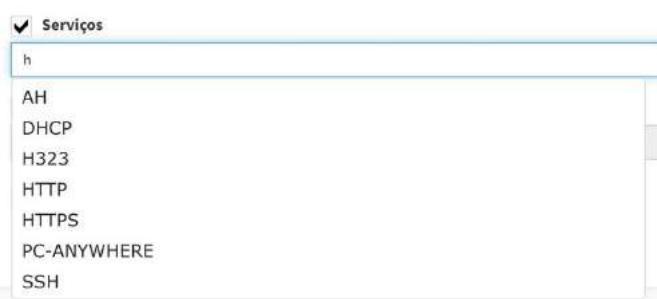
### 24.4.1 Endereço IP

Objeto(s) de Endereço IP (IPs, redes ou conjuntos) para serem utilizados como filtro de destino.



### 24.4.2 Serviços

Objeto(s) de serviço (protocolos e portas) para serem utilizados como filtro de destino.



#### 24.4.3 Serviços WEB

Objeto(s) de porta para serem utilizados como filtro de destino e que serão inspecionados pelo Filtro Web.

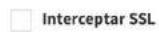
As portas podem ser manipuladas em **Serviços >> Web Cache**.

O Campo [Serviços WEB] vem pré-selecionado.



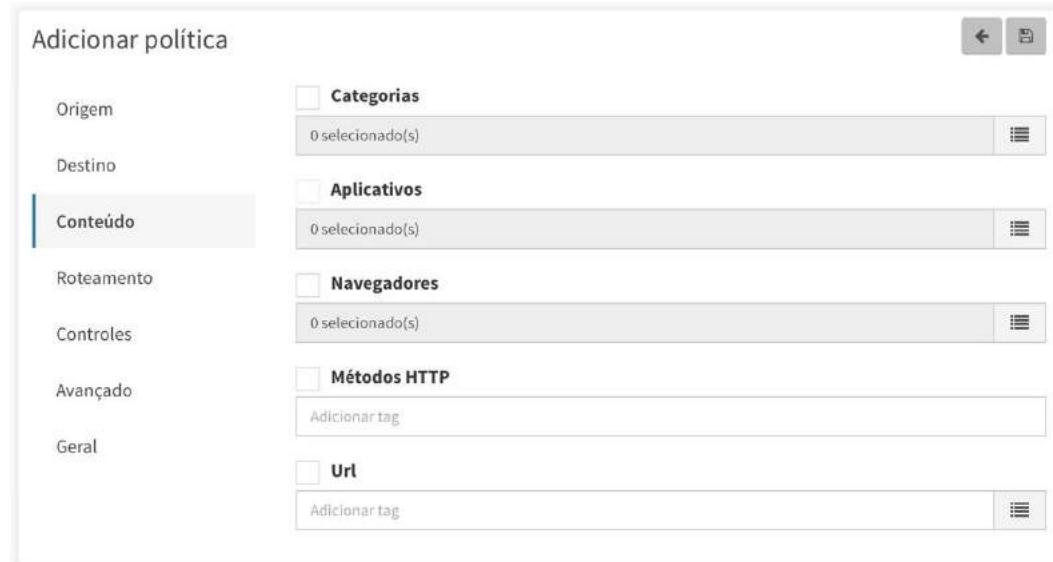
#### 24.4.4 Interceptar SSL

Utilizado em conjunto da opção Serviços WEB, intercepta conteúdo SSL permitindo a inspeção do seu conteúdo.



## 24.5 Conteúdo

A aba Conteúdo tem seus filtros ativados ao habilitar a opção Serviços WEB na aba Destino, e tem como objetivo configurar a ação do Filtro Web, permitindo a escolha de categorias, aplicativos, navegadores, métodos HTTP e URLs que serão aplicados a política.



### 24.5.1 Categorias

Permite configurar as categorias que se aplicam à política.

Para escolher as categorias, ative o filtro e clique no botão [ ], escolha as categorias desejadas e depois clique em [ Adicionar ], o botão [ Todos ], marca ou demarca todas as categorias.

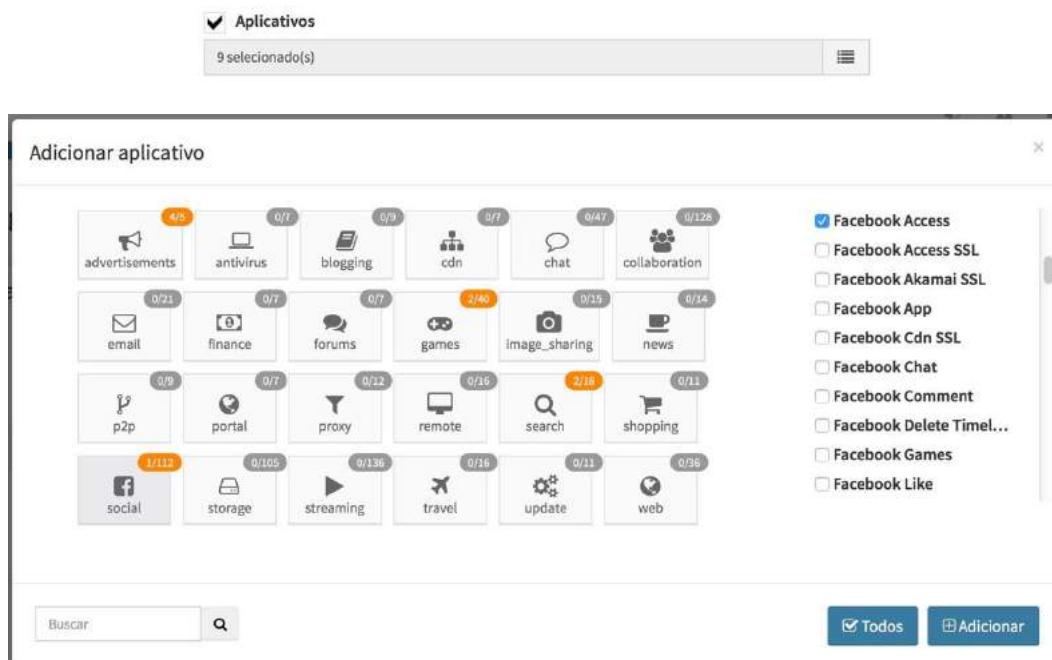


### 24.5.2 Aplicativos

Permite configurar Filtros de Aplicativos Web 2.0 que se aplicam à política.

Para escolher os aplicativos, ative o filtro e clique no botão [ ], escolha um grupo e escolha os aplicativos desejados na lista e depois clique em [ Adicionar ], o botão [ Todos ], marca ou demarca todas os aplicativos listados no grupo selecionado.

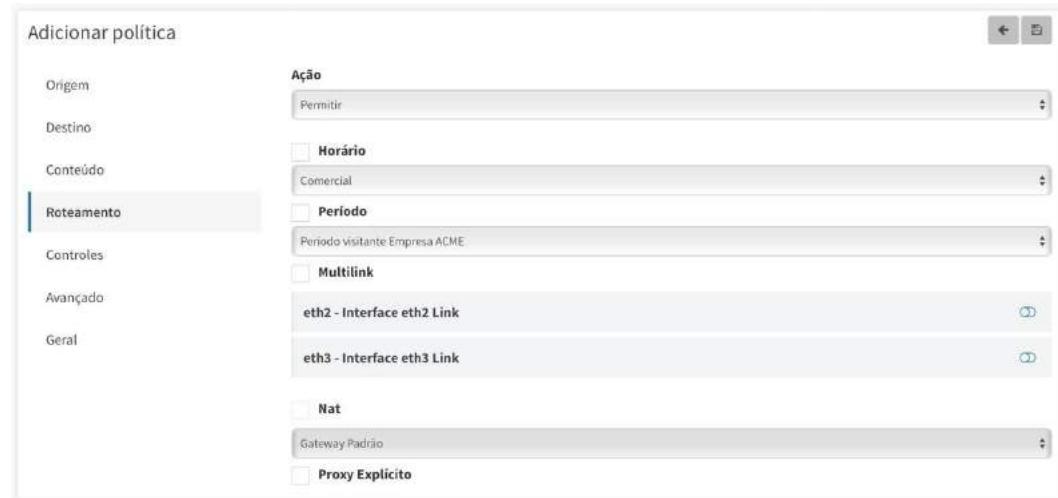
O campo [Buscar] facilita a localização da aplicação desejada, para utilizar basta digitar o texto a ser procurado e em seguida clicar no [ ]



**ATENÇÃO:** O Filtro de Aplicativos só é habilitado se associado à interceptação SSL na aba [DESTINO] em [Serviços WEB].

## 24.6 Roteamento

A aba Roteamento permite configurar a ação, horário, período, multilink, nat e proxy explícito para políticas que se enquadram nos filtros configurados em origem / destino / conteúdo.



### 24.6.1 Ação

Permite definir a ação que será aplicada na política: Permitir, Bloquear, Inspecionar:ATP e Inspecionar:IPS.

As ações de Inspecção ATP e IPS tem ação de Permitir e serão avaliados nos devidos módulos para análise profunda.



### 24.6.2 Horário

Permite definir um objeto de horário em que a política é válida.



### 24.6.3 Período

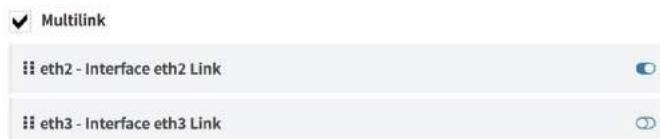
Permite definir um objeto de período em que a política é válida.



#### 24.6.4 Multilink

Permite configurar o uso do multilink na política, podendo escolher os links que se aplicam a política, clicando no botão [ ] e a ordenação de prioridade entre os links arrastando pelo [ ].

Dos links ativados, o primeiro link na lista é o primário e os demais abaixo são failover, isto é, ativados apenas em caso de falha do primário.



#### 24.6.5 NAT

Permite ativar o NAT e a escolha do endereço para tradução de origem, por padrão é configurado o IP do link do Gateway Padrão.

Esta opção fica indisponível ao habilitar **Serviços WEB** na aba **Destino**.



#### 24.6.6 Proxy Explícito

Ao ser ativado determina que a política é válida apenas para navegadores configurados para utilização de proxy e solicita autenticação no navegador.

Este item deve ser configurado quando for necessário fazer controle de conteúdo por sessão (usuário autenticado) em dispositivos do tipo remote desktop.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



## 24.7 Controle

Na aba **Controle** você configura o Controle de Banda, Filtro de tipo de conteúdo, Filtro de cabeçalho HTTP, Cotas e limites de download / upload.

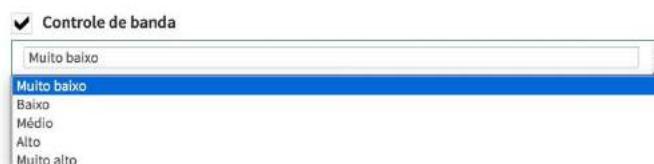
**Adicionar política**

**Controles**

- Origem**:  Controle de banda  
Muito baixo
- Destino**:  Filtrar tipo de conteúdo
- Conteúdo**: Adicionar tag
- Roteamento**:  Filtrar cabeçalho HTTP  
WWW-Authenticate
- Controles**:  Cota de tempo  
Filtro
- Avançado**:  Cota de tráfego  
Minutos por dia
- Geral**:  Tamanho máximo de download  
MB  
 Tamanho máximo de upload  
MB

### 24.7.1 Controle de Banda

Permite ativar e selecionar a prioridade do tráfego, os valores podem ser ajustados sem **Serviços > Traffic Shaping**.



### 24.7.2 Filtrar por Tipo de Conteúdo

Permite ativar o filtro por tipo de conteúdo, que bloqueia os tipos de conteúdo selecionados na lista.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.

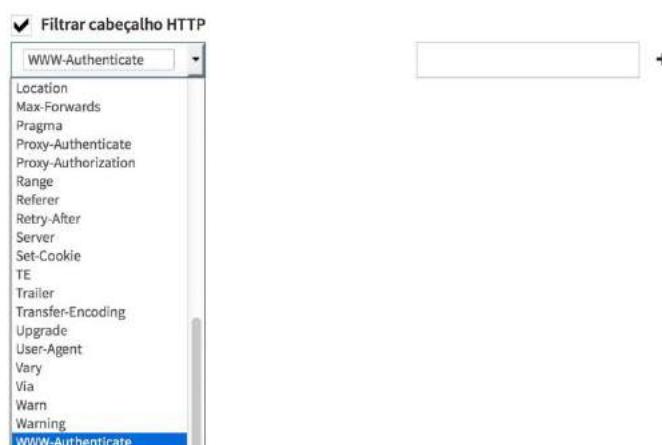


### 24.7.3 Filtrar Cabeçalho HTTP

Permite ativar o filtro cabeçalho HTTP, que **remove** os cabeçalhos selecionados na lista que contenham o valor preenchido no campo.

Para filtrar múltiplos cabeçalhos utilize o botão [ + ].

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



### 24.7.4 Cota de Tempo

Permite configurar uma quota de tempo para a política, em minutos ou horas por dia.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



### 24.7.5 Cota de Tráfego

Permite configurar uma quota de tráfego para a política, em MB por dia.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



### 24.7.6 Tamanho Máximo de Download

Permite configurar o tamanho máximo para download, em MB ou GB.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



### 24.7.7 Tamanho Máximo de Upload

Permite configurar o tamanho máximo para upload, em MB ou GB.

Para ser utilizado é necessário ativar a opção **Serviços WEB** na aba **Destino**.



## 24.8 Avançado

Na aba **Avançado** você configura o TTL, Tipo de pacote, Conteúdo do pacote, TOS e DSCP.

Adicionar política

Origem	<input type="checkbox"/> TTL Igual	
Destino	<input type="checkbox"/> Tipo de pacote UNICAST	
Conteúdo	<input type="checkbox"/> Conteúdo do pacote Hexa	
Roteamento	<input type="checkbox"/> Conteúdo do pacote Prioridade normal	
Controles	<input type="checkbox"/> TOS Igual	
Avançado	<input type="checkbox"/> DSCP UNICAST	
Geral	<input type="checkbox"/> DSCP BE (Best Effort)	

### 24.8.1 TTL

Permite configurar o valor TTL em que a política se aplica, usando comparador Igual, Menor ou Maior.



### 24.8.2 Tipo de Pacote

Permite escolher o tipo de pacote em que a política se aplica, escolhendo entre Unicast, Broadcast ou Multicast.



### 24.8.3 Conteúdo do Pacote

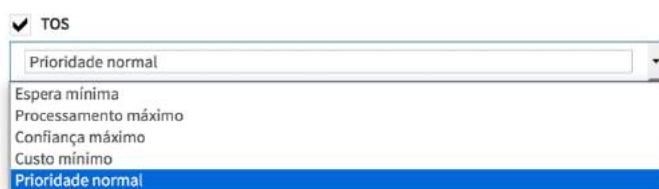
Permite definir uma String ou sequência hexadecimal para bloqueio de conteúdo.

Para ser utilizado é necessário ativar a **Ação Bloquear** na aba **Roteamento**.



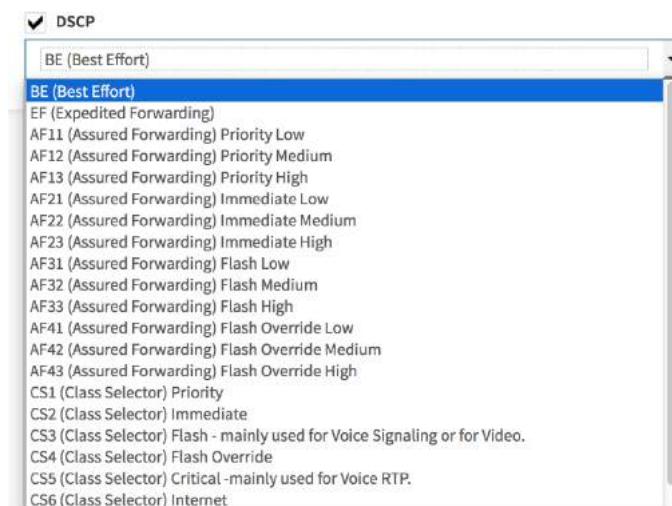
### 24.8.4 TOS

Ao ativar permite a marcação do pacote conforme as opções: Espera mínima, Processamento máximo, Confiança máxima, Custo mínimo e prioridade normal.



### 24.8.5 DSCP

Ao ativar permite a marcação do pacote conforme as opções.



## 24.9 Geral

Na aba Geral é obrigatório definir uma Descrição para a política e opcionalmente podem ser definidas Tags que auxiliam na organização e facilitam a busca de políticas.

Adicionar política

Origem	Descrição
Destino	
Conteúdo	Tags Adicionar tag
Roteamento	Interceptar SSL
Controles	Nat Serviços WEB
Avançado	
Geral	

## 24.10 Observações Importantes

Na aba **[Guias Destino]**.

O item “[v] Interceptar SSL” funciona exclusivamente quando selecionadas portas SSL no campo “Serviços Web”. Exemplo a porta 443.

Quando configuramos uma Política de compliance para “Serviços WEB”, o Firewall redireciona todo o tráfego das portas selecionadas para o Proxy.

Certifique-se que as condições da política estejam bem definidas para não gerar desvio de requisições de forma indevida.

**IMPORTANTE:** Cuidado com acessos a serviços do “Governo” e “instituições financeiras”. Recomenda-se para estes casos criar políticas do tipo SSL By-pass.

Na aba **[Conteúdo]**.

O campo “Aplicativos” é exclusivo a requisições com interceptação SSL.

Na aba **[Roteamento]**.

As ações “Inspecionar ATP” e “Inspecionar IPS” só são válidas se os respectivos serviços “ATP” e “IPS” estiverem devidamente configurados, ou seja, após a atualização da base de assinaturas.

Os serviços são automaticamente habilitados após o processo de atualização das bases de assinaturas já mencionados em capítulo anterior.

**Pronto!** Agora você já conhece um pouco da interface, vamos definir algumas políticas e configurá-las.

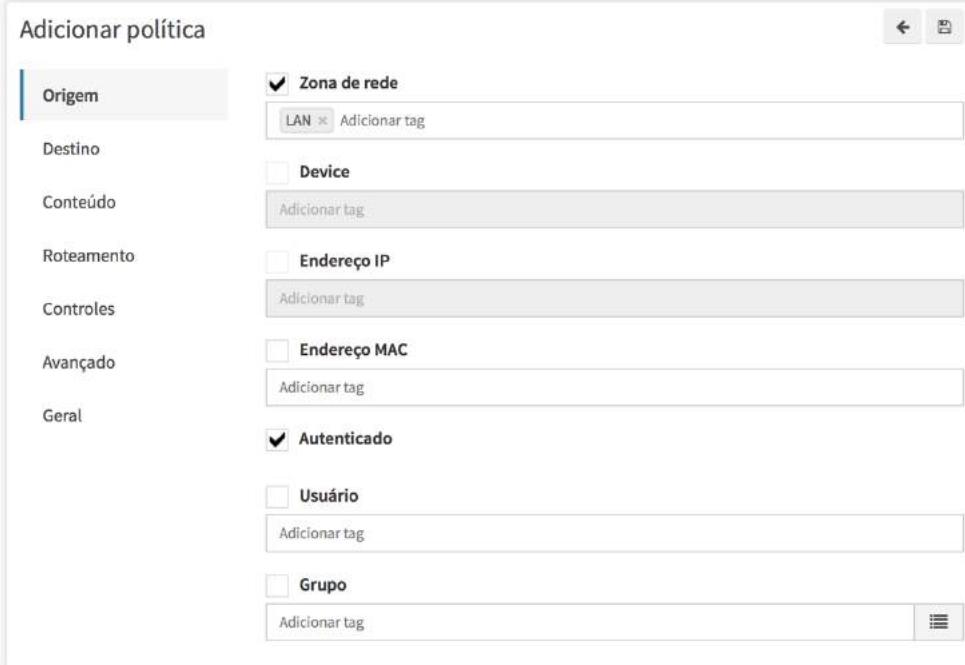
## 24.11 Exemplo 1 – Política de Navegação

Neste exemplo definimos e adicionamos uma política para acesso web com inspeção, no entanto, sem restrições ou qualquer filtro.

- [Origem] → Zona=LAN, Autenticado;
- [Destino] → Serviços WEB (80; 443) – Interceptar SSL;
- [Conteúdo] → Sem filtros – navegação livre;
- [Roteamento] → Ação=Inspecionar ATP, Aplicar roteamento default;
- [Controles] → Prioridade Média (Reserva 50% link);
- [Avançado] → Sem filtros, sem controles;
- [Geral] → Nome da política=“WEB - Navegação usuários”;

Para adicionar uma política de segurança clique em **[Políticas]**, depois clique em **Adicionar** []. Configure cada aba de acordo com a definição da política aplicada. Depois clique em [].

### 24.11.1 Origem



The screenshot shows the 'Adicionar política' (Add policy) dialog box with the 'Origem' (Source) tab selected. The configuration includes:

- Zona de rede:** LAN (checked)
- Autenticado:** Autenticado (checked)

## 24.11.2 Destino

Adicionar política

Origem	<input type="checkbox"/> Endereço IP Adicionar tag
<b>Destino</b>	<input type="checkbox"/> Serviços Adicionar tag
Conteúdo	<input checked="" type="checkbox"/> Serviços WEB 80 ✕ 443 ✕ Adicionar tag
Roteamento	<input checked="" type="checkbox"/> Interceptar SSL
Controles	
Avançado	
Geral	

## 24.11.3 Roteamento

Adicionar política

Origem	<b>Ação</b> Inspecionar: ATP
Destino	<input type="checkbox"/> Horário Comercial
Conteúdo	<input type="checkbox"/> Período Período visitante Empresa ACME
<b>Roteamento</b>	<input type="checkbox"/> Multilink eth2 - Interface eth2 Link
Controles	<input type="checkbox"/> eth3 - Interface eth3 Link
Avançado	<input type="checkbox"/> Nat Gateway Padrão
Geral	<input type="checkbox"/> Proxy Explícito

## 24.11.4 Controles

Adicionar política

Origem	<input checked="" type="checkbox"/> <b>Controle de banda</b>
Destino	<input type="checkbox"/> <b>Filtrar tipo de conteúdo</b>
Conteúdo	<input type="checkbox"/> <b>Adicionar tag</b>
Roteamento	<input type="checkbox"/> <b>Filtrar cabeçalho HTTP</b>
<b>Controles</b>	<b>Filtro</b>
Avançado	<input type="checkbox"/> <b>Cota de tempo</b>
Geral	<input type="checkbox"/> <b>Cota de tráfego</b>
	<input type="checkbox"/> <b>Tamanho máximo de download</b>
	<input type="checkbox"/> <b>Tamanho máximo de upload</b>

## 24.11.5 Geral

Adicionar política

Origem	<b>Descrição</b>
Destino	Navegação Web Usuários
Conteúdo	<b>Tags</b>
Roteamento	<input type="checkbox"/> Adicionar tag
Controles	
Avançado	
<b>Geral</b>	

<b>TAGS</b>	Buscar	<input type="button" value=""/>	<input type="button" value=""/>
<input type="button" value="Autenticado"/>	<input type="checkbox"/> <b>Navegação Web Usuários</b>	<input type="button" value="Inspecionar: ATP"/>	<input type="button" value=""/>
<input type="button" value="Serviços WEB"/>	<input type="checkbox"/> <b>Webex</b>	<input type="button" value="Permitir"/>	<input type="button" value=""/>
<input type="button" value="Interceptar SSL"/>	<input type="checkbox"/> <b>Whatsapp</b>	<input type="button" value="Bloquear"/>	<input type="button" value=""/>
<input type="button" value="Banda: Médio"/>			
<input type="button" value="Nat"/>			

## 24.12 Exemplo 2 – Política de Filtro WEB - bloqueando categorias

Vamos adicionar uma política aplicando um filtro de conteúdo, vamos definir os parâmetros para esta política e considerar o filtro à URL's que compreendam as categorias de “*Improdutividade*”. Para definir esta lista de categorias é interessante consultar antes em: **[Serviços] >> [Web Filter]**.

Lista das categorias identificadas como improdutivas.

- Entretenimento
- MP3
- Jogos de azar e apostas
- Jogos /Games
- Gestão de largura de banda
- Radio e TV na Internet
- Streaming mídia
- Sociedade e estilos de vida
- Anúncios pessoais e namoros
- Sites pessoais na Web
- Esportes
- Turismo

<b>[Origem]</b>	→ Endereço IP = “Rede Local”, Autenticado;
<b>[Destino]</b>	→ Serviços WEB (80; 443) – Interceptar SSL;
<b>[Conteúdo]</b>	→ Filtros por categorias de improdutividade;
<b>[Roteamento]</b>	→ Ação=Bloquear;
<b>[Controles]</b>	→ Sem controles; Interface desativada;
<b>[Avançado]</b>	→ Sem controles de conteúdo do pacote;
<b>[Geral]</b>	→ Nome da política=“Bloqueio WEB Perda Produtividade”; TAG = Bloqueios;

Para adicionar a política de segurança clique em **[Políticas]**, depois clique em **Adicionar** . Configure cada aba de acordo com a definição da política aplicada. Depois clique em .

### 24.12.1 Origem

Adicionar política

Origem	<input type="checkbox"/> Zona de rede Adicionar tag
Destino	<input type="checkbox"/> Device Adicionar tag
Conteúdo	<input type="checkbox"/> Endereço IP Rede Local <input type="button" value="X"/> Adicionar tag
Roteamento	<input checked="" type="checkbox"/> Endereço MAC Adicionar tag
Controles	<input type="checkbox"/> Autenticado
Avançado	<input type="checkbox"/> Usuário Adicionar tag
Geral	<input type="checkbox"/> Grupo Adicionar tag <input type="button" value="☰"/>

### 24.12.2 Destino

Adicionar política

Origem	<input type="checkbox"/> Endereço IP Adicionar tag
Destino	<input type="checkbox"/> Serviços Adicionar tag
Conteúdo	<input checked="" type="checkbox"/> Serviços WEB 80 <input type="button" value="X"/> 443 <input type="button" value="X"/> Adicionar tag
Roteamento	<input checked="" type="checkbox"/> Interceptar SSL
Controles	
Avançado	
Geral	

### 24.12.3 Conteúdo

Adicionar política

Origem  **Categorias**  
19 selecionado(s)

Destino  **Aplicativos**  
0 selecionado(s)

**Conteúdo**  **Navegadores**  
0 selecionado(s)

Roteamento  **Métodos HTTP**  
Adicionar tag

Controles  **Url**  
Adicionar tag

Avançado

Geral

Adicionar Objeto de Endereço IP

Gestão de largura de banda  
 Rádio e TV na Internet  
 Streaming mídia  
 Compartilhamento de arquivos peer-to-peer  
 Armazenamento/Backup pessoal em rede  
 Telefonia via Internet  
 Monitoramento indevido e invasão de privacidade  
 Sites Maliciosos  
 Spyware  
 Racismo/ódio  
 Religião  
 Religiões não-tradicionalis

Todos  Adicionar

#### 24.12.4 Roteamento

Adicionar política

Origem	Ação
	<input type="text" value="Bloquear"/>
Destino	
Conteúdo	
Roteamento	<input type="checkbox"/> Horário <input type="checkbox"/> Período <input type="checkbox"/> Multilink <input type="checkbox"/> eth2 - Interface eth2 Link <input type="checkbox"/> eth3 - Interface eth3 Link
Controles	
Avançado	
Geral	<input type="checkbox"/> Nat <input type="checkbox"/> Gateway Padrão <input type="checkbox"/> Proxy Explícito

#### 24.12.5 Geral

Adicionar política

Origem	Descrição
	<input type="text" value="Bloqueio WEB Perda Produtividade"/>
Destino	
Conteúdo	Tags
Roteamento	<input type="text" value="Bloqueio"/>
Controles	
Avançado	
Geral	

TAGS	
<input type="button" value="Autenticado"/>	Buscar <input type="text"/> <input type="button" value="Q"/>
<input type="button" value="Serviços WEB"/>	<input type="button" value="Bloquear"/> <input type="button" value="editar"/> <input type="button" value="deletar"/>
<input type="button" value="Interceptar SSL"/>	
<input type="button" value="Bloqueio"/> <input type="button" value="Banda: Médio"/>	<input type="button" value="Inspecionar: ATP"/> <input type="button" value="editar"/> <input type="button" value="deletar"/>
<input type="button" value="Nat"/>	<input type="button" value="Permitir"/> <input type="button" value="editar"/> <input type="button" value="deletar"/>

## 24.13 Exemplo 3 – Política de Filtro WEB - bloqueando aplicativos WEB 2.0

Vamos adicionar uma política aplicando filtros de aplicativos. Vamos considerar o filtro a Urls ou sites que executam aplicativos que compreendam as ações de improdutividade ou risco de segurança.

- [Origem] → Endereço IP = “Rede Local”, Autenticado;
- [Destino] → Serviços WEB (80; 443) – Interceptar SSL;
- [Conteúdo] → Filtros de Aplicativos;
- [Roteamento] → Ação=Bloquear;
- [Controles] → Sem controles; Interface desativada;
- [Avançado] → Sem controles de conteúdo do pacote;
- [Geral] → Nome da política=“Bloqueio de aplicativos WEB 2”;  
TAG = Bloqueios;

Lista dos aplicativos identificados como improdutivos ou de risco de segurança.

- Baidu Movies
- CDN – Content Delivery Network
- Dropbox
- Facebook (all)
- Google Drive
- Google Drive Upload
- Google Mail
- Google Photos / Google + Photos
- One Drive
- Skype Call Start
- Skype Call End

Para adicionar a política de segurança clique em **[Políticas]**, depois clique em **Adicionar** []. Configure cada aba de acordo com a definição da política aplicada. Depois clique em [].

### 24.13.1 Origem

Adicionar política

Origem	<input type="checkbox"/> Zona de rede Adicionar tag
Destino	<input type="checkbox"/> Device Adicionar tag
Conteúdo	<input type="checkbox"/> Endereço IP Rede Local <input type="button" value="X"/> Adicionar tag
Roteamento	<input checked="" type="checkbox"/> Endereço MAC Adicionar tag
Controles	<input type="checkbox"/> Autenticado
Avançado	<input type="checkbox"/> Usuário Adicionar tag
Geral	<input type="checkbox"/> Grupo Adicionar tag <input type="button" value="☰"/>

### 24.13.2 Destino

Adicionar política

Origem	<input type="checkbox"/> Endereço IP Adicionar tag
Destino	<input type="checkbox"/> Serviços Adicionar tag
Conteúdo	<input checked="" type="checkbox"/> Serviços WEB 80 <input type="button" value="X"/> 443 <input type="button" value="X"/> Adicionar tag
Roteamento	<input checked="" type="checkbox"/> Interceptar SSL
Controles	
Avançado	
Geral	

### 24.13.3 Conteúdo

**Adicionar política**

Origem  **Categorias**  
0 selecionado(s)

Destino  **Aplicativos**  
33 selecionado(s)

**Conteúdo**

Roteamento  **Navegadores**  
0 selecionado(s)

Controles  **Métodos HTTP**  
Adicionar tag

Avançado  **Url**  
Adicionar tag

Geral

**Adicionar Objeto de Endereço IP**

skype   Todos

## **24.13.4 Roteamento**

## Adicionar política

	Ação
Origem	<input type="text" value="Bloquear"/>
Destino	<input type="checkbox"/> Horário
Conteúdo	<input type="text" value="Comercial"/>
Roteamento	<input type="checkbox"/> Período
Controles	<input type="text" value="Período visitante Empresa ACME"/>
Avançado	<input type="checkbox"/> Multilink
Geral	<input type="text" value="eth2 - Interface eth2 Link"/> <input type="checkbox"/> <input type="text" value="eth3 - Interface eth3 Link"/> <input type="checkbox"/>
	<input type="checkbox"/> Nat
	<input type="text" value="Gateway Padrão"/>
	<input type="checkbox"/> Proxy Explicito

## **24.13.5 Geral**

**Adicionar política**

**Origem** **Descrição**  
Bloqueio Aplicativos WEB 2.0

**Destino** **Tags**  
Bloqueio Adicionar tag

**Conteúdo**

**Roteamento**

**Controles**

**Avançado**

**Geral**

TAGS		Buscar		
<a href="#">Autenticado</a>			<input type="button" value=""/>	<input type="button" value=""/>
<a href="#">Serviços WEB</a>		<b>## Bloqueio Aplicativos WEB 2.0</b>	<a href="#">Bloquear</a>	<input type="button" value=""/>
<a href="#">Interceptar SSL</a>		<b>## Bloqueio WEB Perda Produtividade</b>	<a href="#">Bloquear</a>	<input type="button" value=""/>
<a href="#">Bloqueio</a>	<a href="#">Banda: Médio</a>	<b>## Navegação Web Usuários</b>	<a href="#">Inspeccionar: ATP</a>	<input type="button" value=""/>
<a href="#">Nat</a>				

No exemplo 1, 2 e 3 definimos e adicionamos políticas de acesso “*WEB via Proxy*” e bloqueios de “*categorias e aplicativos*” de conteúdo inapropriado ou improdutivo.

## 24.14 Exemplo 4 – Política de NAT

Vamos adicionar uma política aplicando “*NAT (Network Address Translate)*” para serviços diversos. Vamos considerar o exemplo:

Mascaramento do servidor Windows para o serviço WSUS. Com o intuito de permitir o UPDATE automático sem a exigência de autenticação.

**NOTA:** Abaixo Link com a documentação da Microsoft com as informações necessárias para configurar o acesso ao serviço MS WSUS

[https://technet.microsoft.com/en-us/library/cc708602\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc708602(v=ws.10).aspx)

Para casos específicos definir e configurar antes os objetos que serão utilizados na política.

Objeto endereço “Servidores Wsus” ver lista de endereços na documentação em nota;

Objeto serviços “Service UPDATE MS WSUS”. Ver lista de portas na documentação em nota;

**Recomendação:** Para casos específicos como o exemplo dado, é recomendável configurar os objetos que serão utilizados, antes da configuração da política.

Exemplo: Definir o objeto de endereço “*Servidores Wsus*” - ver lista de endereços na documentação em nota.

Definir o objeto serviços “*Service UPDATE MS WSUS*” - ver lista de portas na documentação em nota.

- [Origem]** → Endereço IP = Servidor Windows AD/LDAP  
sem autenticação;
- [Destino]** → Endereço IP = “Servidores Wsus”  
Serviços = “Services UPDATE MS WSUS”
- [Conteúdo]** → Sem filtros; interface desativada;
- [Roteamento]** → Ação=Inspecionar IPS;  
→ Multilink (Habilitar FailOver Link 2 e Link 1);  
→ Habilitar mascaramento [Nat];
- [Controles]** → Sem controles; Interface desativada;
- [Avançado]** → Sem controles de conteúdo do pacote;
- [Geral]** → Nome da política = “NAT: Servidores MS-WSUS”;  
TAG = Bloqueios;

Para adicionar a política de segurança clique em **[Políticas]**, depois clique em **Adicionar** [+]. Configure cada aba de acordo com a definição da política aplicada. Depois clique em [ ].

#### 24.14.1 Origem

The screenshot shows the 'Adicionar política' (Add Policy) dialog box. The 'Origem' tab is active. In the 'Endereço IP' section, there is a checked checkbox next to 'Servidor Windows AD/LDAP'. Below it, there is a 'Adicionar tag' button. The other tabs ('Destino', 'Conteúdo', 'Roteamento', 'Controles', 'Avançado', 'Geral') are visible but not selected.

## 24.14.2 Destino

Adicionar política

Origem	<input checked="" type="checkbox"/> Endereço IP Servidores UPDATE MS WSUS <input type="button" value="Adicionar tag"/>
Destino	<input checked="" type="checkbox"/> Serviços Services UPDATE MS WSUS <input type="button" value="Adicionar tag"/>
Conteúdo	<input type="checkbox"/> Serviços WEB <input type="button" value="Adicionar tag"/>
Roteamento	<input type="checkbox"/> Interceptar SSL
Controles	
Avançado	
Geral	

## 24.14.3 Roteamento

Adicionar política

Origem	Ação Permitir
Destino	<input type="checkbox"/> Horário Comercial
Conteúdo	<input type="checkbox"/> Período Período visitante Empresa ACME
Roteamento	<input checked="" type="checkbox"/> Multilink ::: eth2 - Interface eth2 Link <input type="button" value=""/>
Controles	<input checked="" type="checkbox"/> ::: eth3 - Interface eth3 Link <input type="button" value=""/>
Avançado	<input checked="" type="checkbox"/> Nat Gateway Padrão
Geral	<input type="checkbox"/> Proxy Explícito

#### 24.14.4 Geral

Adicionar política

Origem	<b>Descrição</b>
	NAT Servidores MS - WSUS
Destino	<b>Tags</b>
	servidores <small>x Adicionar tag</small>
Roteamento	
Controles	
Avançado	
<b>Geral</b>	

TAGS

Nat	Multilink	Buscar	+	-
<b>servidores</b>	Autenticado	<b>⋮ NAT Servidores MS - WSUS</b>	<b>Permitir</b>	
Serviços WEB		<b>⋮ Bloqueio Aplicativos WEB 2.0</b>	<b>Bloquear</b>	
Interceptar SSL		<b>⋮ Bloqueio WEB Perda Produtividade</b>	<b>Bloquear</b>	
Bloqueio	Banda: Médio	<b>⋮ Navegação Web Usuários</b>	<b>Inspecionar: ATP</b>	

**IMPORTANTE:** Observar a necessidade de ordenar/reordenar as políticas.

Neste caso não vamos precisar reordenar.

As políticas estão bem definidas, a regra de NAT do servidor Windows AD/LDAP bem especifica considerando “Origem/Destino”, inclusive as portas de serviço.

As políticas de acesso e filtros WEB com inspeção e ordenadas de forma que aplicam 1º os bloqueios, depois a permissão.

Dessa maneira “*não conflitante*” com outras políticas, atendendo as especificações do modelo de políticas apresentadas e as considerações mencionadas na [seção 24.10 - Informações importantes](#).

**NOTA:** Não se esqueça de aplicar a fila de comandos. Clique em [ ].

**Definição de políticas finalizada!** Agora é aplicar testes.

Usar uma estação de trabalho devidamente configurada e navegar na WEB.

Depois verificar os registros de Tráfego no Dashboard.

## 25 Monitor

A solução BLOCKBIT UTM conta com um recurso muito útil para o gerenciamento dos serviços.

O monitor do [tráfego de rede] e o monitor do [tráfego WEB].

Clique em **[Dashboard]**.



## 25.1 Tráfego Geral

Este recurso permite ao administrador monitorar o tráfego de rede em tempo real, conta com a resposta garantida de qual acesso ou tentativa gerou LOG e grava seu histórico em banco de dados.

Para monitorar o tráfego geral clique em [Tráfego Geral] role a tela até o quadro [Monitor de tráfego].

Origem	Destino	Serviço	Tráfego	Velocidade	Pacotes
Nenhum ítem encontrado					

Você pode selecionar entre os tipos: “Estabelecidas” e “Novas”, e os filtros de pesquisa “Origem”, “Destino”, “Serviço” e “Política”.

**NOTA:** O serviço de monitoração exige pelo menos a especificação de um filtro “Origem”, “Destino” ou a especificação de uma “Política”.

Para monitorar clique em [Buscar].

## 25.2 Tráfego WEB

Este recurso permite ao administrador monitorar o tráfego de navegação WEB em tempo real, conta com a resposta garantida de qual acesso ou tentativa gerou LOG e grava seu histórico em banco de dados. Para monitorar o tráfego geral clique em [Web Filter] role a tela até o quadro [Monitor navegação].

Tempo	Origem	Tráfego	Velocidade	Destino
00:00:01	andre@blockbit.com	0 B	0 bps	31.13.73.7:443
00:00:01	andre@blockbit.com	514 B	0 bps	http://tt-10162-1.seg.t.taltarget.com/profile
00:00:01	andre@blockbit.com	1.0 kB	0 bps	http://comparecar.uol.com.br/App_Themes/TemaUOL_V...
00:00:02	andre@blockbit.com	1.9 kB	0 bps	http://metrics.uol.com.br/b/ss/uolcarros/1/H.27.5...
00:00:02	andre@blockbit.com	298 B	0 bps	http://149.154.175.50/api
00:00:02	andre@blockbit.com	298 B	0 bps	http://149.154.175.50/api
00:00:01	andre@blockbit.com	1.2 kB	0 bps	http://jsuol.com.br/c/busca/uolbusca.js
00:00:01	andre@blockbit.com	0 B	0 bps	54.94.250.161:443
00:00:01	andre@blockbit.com	0 B	0 bps	216.58.202.14:443

Você pode aplicar filtros de pesquisa do tipo: “Origem”, “Destino” e “Porta”. Para monitorar clique em [Buscar].

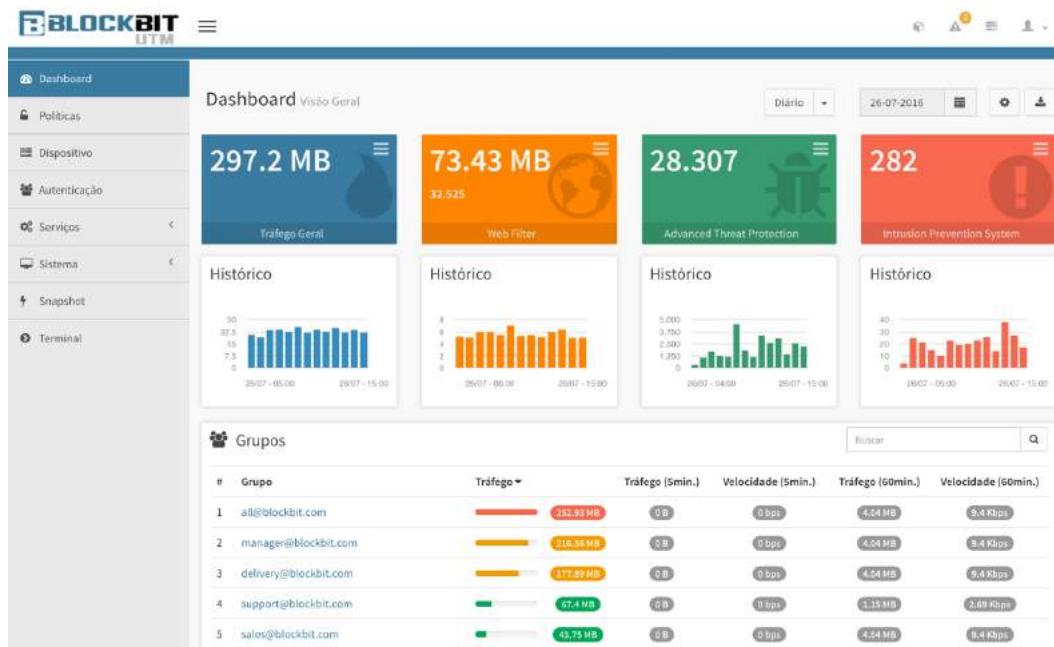
## 26 Relatórios

O BLOCKBIT UTM possui um recurso de gerenciamento da solução com os logs estatísticos e relatórios, “o Dashboard”. Um painel de controle que retorna informações essenciais para a administração e gerencia de eventos e informações que reúne dados *SUMARIZADOS* dos servidores.

Um recurso muito útil para o gerenciamento do sistema, principalmente para administradores que possuem muitos grupos; políticas, e usuários cadastrados.

Este recurso permite ao administrador a geração dos relatórios sumarizados e ainda conta com a opção de exportar no modo PDF. Também é possível extrair os relatórios no modo “*Detalhado*”, no entanto este relatório se limita aos últimos 7(sete) dias, é possível extraí-los no modo WEB ou exportar para o modo Texto “*arquivo .CSV*” .

No menu principal clique em **[Dashboard]**



A interface principal do “*Dashboard*” nos traz uma “*Visão geral*” de todos os recursos e serviços utilizados pela rede devolvendo ao sistema e ao administrador informações do tráfego geral, por “*Usuário*”, “*Serviços*”, “*Políticas*”, “*Categorias*”, “*Ameaças*”, “*Aplicativos*”, “*Ataques*” e “*Alertas de segurança*”, devolvendo informações importantes para sua gerência e administração.

Com o objetivo de analisar e verificar a existência de tráfego inapropriado e se os recursos estão funcionando de acordo com as políticas definidas. Nesta interface os relatórios estatísticos, para visualizar os diversos itens estatísticos aplique uma rolagem de tela “*Scrolling*”.

## 26.1 Serviços

#	Serviço	Tráfego ▾	Tráfego (5min.)	Velocidade (5min.)	Tráfego (60min.)	Velocidade (60min.)
1	admin	<div style="width: 100%;">136.46 MB</div>	910.04 KB	24.85 Kbps	10.49 MB	24.45 Kbps
2	http	<div style="width: 100%;">123.61 MB</div>	667.75 KB	18.23 Kbps	10.4 MB	24.23 Kbps
3	imap	<div style="width: 100%;">37.65 MB</div>	187.35 KB	5.12 Kbps	3.04 MB	7.09 Kbps
4	ldap	<div style="width: 100%;">5.03 MB</div>	15.9 KB	434.24 bps	344.26 KB	783.38 bps
5	xmpp	<div style="width: 100%;">2.64 MB</div>	17.2 KB	469.73 bps	206.83 KB	470.66 bps
6	smtp	<div style="width: 100%;">453.53 KB</div>	0 B	0 bps	35.45 KB	80.68 bps
7	telnet	<div style="width: 100%;">8.42 KB</div>	65 B	1.73 bps	611 B	1.36 bps
8	rsync	<div style="width: 100%;">8.28 KB</div>	65 B	1.73 bps	643 B	1.43 bps
9	snmp	<div style="width: 100%;">8.28 KB</div>	65 B	1.73 bps	643 B	1.43 bps
10	ssh	<div style="width: 100%;">6.6 KB</div>	0 B	0 bps	312 B	0.69 bps

## 26.2 Políticas

#	Política	Tráfego ▾	Tráfego (5min.)	Velocidade (5min.)	Tráfego (60min.)	Velocidade (60min.)
1	Threat Control	<div style="width: 100%;">29.65 MB</div>	1.45 MB	40.42 Kbps	40.44 MB	94.24 Kbps
2	Content Filtering	<div style="width: 100%;">20.33 MB</div>	112.88 KB	3.08 Kbps	30 MB	69.91 Kbps
3	Intercept SSL	<div style="width: 100%;">8.17 MB</div>	850.24 KB	23.22 Kbps	9.78 MB	22.78 Kbps
4	WEB: Users browsing	<div style="width: 100%;">2.19 MB</div>	156.1 KB	4.26 Kbps	2.75 MB	6.4 Kbps
5	SSL ByPass	<div style="width: 100%;">1.72 MB</div>	135.86 KB	3.71 Kbps	2.59 MB	6.04 Kbps
6	Skype	<div style="width: 100%;">1.56 MB</div>	195.66 KB	5.34 Kbps	1.74 MB	4.06 Kbps
7	Security Ethics	<div style="width: 100%;">1.27 MB</div>	69.21 KB	1.89 Kbps	1.38 MB	3.2 Kbps
8	Government services	<div style="width: 100%;">1.21 MB</div>	103.7 KB	2.83 Kbps	1.33 MB	3.05 Kbps
9	Security Risk	<div style="width: 100%;">577.15 KB</div>	59.16 KB	1.62 Kbps	779.05 KB	1.77 Kbps
10	Whatsapp	<div style="width: 100%;">321.42 KB</div>	1.51 KB	41.12 bps	434.89 KB	989.62 bps

## 26.3 Web Filter

#	Categoria	Tráfego ▾	Tráfego (5min.)	Velocidade (5min.)	Tráfego (60min.)	Velocidade (60min.)
1	Noticiários e mídia	<div style="width: 100%;"> </div>	1.9 MB	0 B	0 bps	0 B
2	Veículos	<div style="width: 100%;"> </div>	800.14 KB	0 B	0 bps	0 B
3	Publicações alternativas	<div style="width: 100%;"> </div>	524.33 KB	0 B	0 bps	0 B
4	Mecanismos de busca e portais	<div style="width: 100%;"> </div>	67.34 KB	24.51 KB	55.78 bps	24.51 KB
5	Anúncios publicitários	<div style="width: 100%;"> </div>	51.38 KB	0 B	0 bps	0 B
6	Negócios e Economia	<div style="width: 100%;"> </div>	33.65 KB	0 B	0 bps	0 B
7	Sistemas de evitação de proxy	<div style="width: 100%;"> </div>	16.24 KB	0 B	0 bps	0 B
8	Tecnologia da informação	<div style="width: 100%;"> </div>	5.67 KB	4.78 KB	10.89 bps	4.78 KB
9	Hospedagem de Web	<div style="width: 100%;"> </div>	3.8 KB	0 B	0 bps	0 B
10	Comunicações pela Internet	<div style="width: 100%;"> </div>	3.76 KB	0 B	0 bps	0 B

## 26.4 Advanced Threat Protection

#	Ameaça	Impacto	Hits ▾	Hits (5min.)	Hits (60min.)
1	MALWARE Mozilla User-Agent (Mozilla/5.0) In...	Alto	<div style="width: 100%;"> </div> 5.178	75	75
2	CHAT Jabber/Google Talk Outgoing Traffic	Baixo	<div style="width: 100%;"> </div> 30	0	0
3	POLICY Http Client Body contains pass= in cl...	Alto	<div style="width: 100%;"> </div> 25	0	0
4	POLICY HotSpotShield Activity	Alto	<div style="width: 100%;"> </div> 13	0	0
5	POLICY Suspicious inbound to mySQL, port 3...	Médio	<div style="width: 100%;"> </div> 5	0	0
6	POLICY SSH banner detected on TCP 443 lik...	Médio	<div style="width: 100%;"> </div> 6	0	0
7	POLICY Vulnerable Java Version 1.8.x Detected	Médio	<div style="width: 100%;"> </div> 6	0	0
8	POLICY External IP Lookup - checkip.dyndns...	Alto	<div style="width: 100%;"> </div> 5	0	0
9	POLICY iTunes User Agent	Alto	<div style="width: 100%;"> </div> 4	0	0
10	POLICY Possible IP Check api.ipify.org	Alto	<div style="width: 100%;"> </div> 4	0	0

## 26.5 Aplicativos WEB / ATP

#	Aplicativo	Hits ▾	Hits (5min.)	Hits (60min.)
1	WEB   Safari	<div style="width: 100%;"> </div> 6.365	52	526
2	WEB   Wunderlist Health (keep-alive)	<div style="width: 100%;"> </div> 3.128	20	240
3	ATP   IMTransferAgent	<div style="width: 100%;"> </div> 2.934	0	0
4	ATP   The Internet Archive	<div style="width: 100%;"> </div> 2.168	0	1.084
5	ATP   Microsoft Update	<div style="width: 100%;"> </div> 1.833	0	113
6	ATP   Gravatar	<div style="width: 100%;"> </div> 1.712	0	170
7	ATP   LivePerson	<div style="width: 100%;"> </div> 1.698	0	404
8	ATP   Quora	<div style="width: 100%;"> </div> 1.386	0	0
9	ATP   TED	<div style="width: 100%;"> </div> 944	0	0
10	ATP   Disqus	<div style="width: 100%;"> </div> 904	0	193

## 26.6 IPS – Intrusion Prevention System

#	Ameaça	Impacto	Hits ▾	Hits (5min.)	Hits (60min.)
1	SCAN Sip vicious User-Agent Detected (friend...	Médio	<div style="width: 100%;"> </div> 62	2	2
2	CINS Active Threat Intelligence Poor Reputat...	Médio	<div style="width: 100%;"> </div> 47	1	1
3	SCAN Potential SSH Scan	Médio	<div style="width: 100%;"> </div> 46	0	0
4	SCAN Sip vicious Scan	Médio	<div style="width: 100%;"> </div> 31	1	1
5	SCAN Behavioral Unusually fast Terminal Se...	Baixo	<div style="width: 100%;"> </div> 23	0	0
6	SCAN LibSSH Based Frequent SSH Connecti...	Alto	<div style="width: 100%;"> </div> 23	0	0
7	DROP Spamhaus DROP Listed Traffic Inboun...	Médio	<div style="width: 100%;"> </div> 19	0	0
8	CINS Active Threat Intelligence Poor Reputat...	Médio	<div style="width: 100%;"> </div> 18	1	1
9	SCAN NETWORK Incoming Masscan detected	Baixo	<div style="width: 100%;"> </div> 12	0	0
10	CINS Active Threat Intelligence Poor Reputat...	Médio	<div style="width: 100%;"> </div> 10	0	0

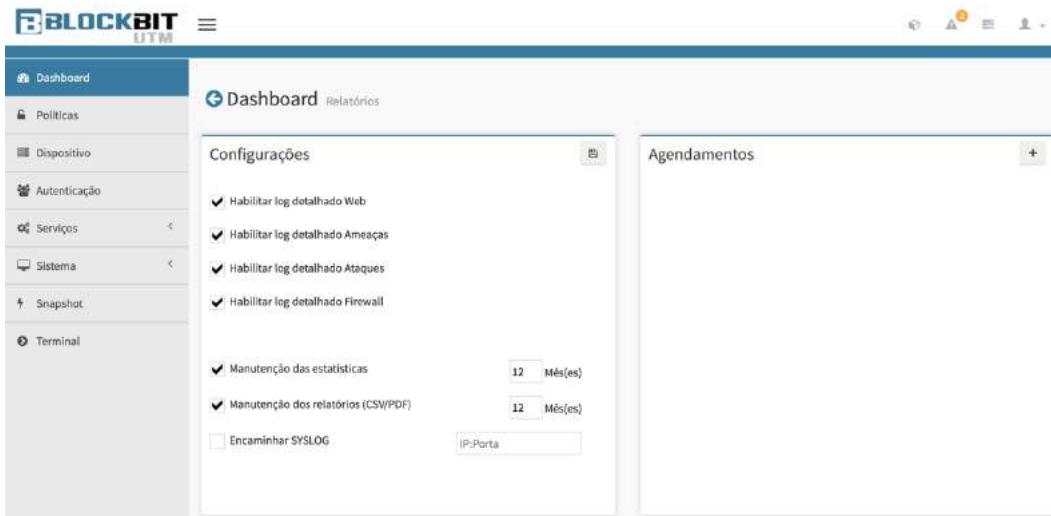
### [Alertas de Segurança]

#	Alerta	Hits
1	Proteção Pacotes Inválidos	46.873
2	Proteção DOS	9.851
3	Proteção Portscan	7.173

Para download dos relatórios sumarizados em PDF, no lado superior direito do Dashboard, clique em [  ]

Para extrair os relatórios detalhados, antes o administrador deve configurar e habilitar o recurso.

Para habilitar os relatórios detalhados, e o recurso de manutenção, no lado superior direito do Dashboard, clique em [  ] no quadro **[Configurações]** habilite os itens. Depois clique em [  ].



O Dashboard do BLOCKBIT UTM também conta com um recurso de agendamento para envio dos relatórios. No lado superior direito clique em [  ] **Dashboard Relatórios**. No quadro **[Agendamentos]** adicione os agendamentos específicos de cada tipo de relatório.

Tipos de relatórios disponíveis:

- Visão Geral
- Web Filter
- Ameaças e Aplicativos
- Ataques
- Estatísticas de Rede
- Produtividade
- Timeline

O administrador tem a opção de definir quais usuários podem ter acesso aos relatórios com a vantagem do acesso pelo Captive Portal.

Todos os tipos de relatórios extraídos são estatísticos, e devolvem os “*TOP level*” de cada item de recurso para cada tipo de relatório.

Ainda conta com o relatório de “*Produtividade*” em que pode selecionar o relatório por “*grupo*” de usuários. E o “*Timeline*” que devolve um histórico do dia ou mensal específico por “*usuário*”.

Selecione o tipo de relatório e qual usuário terá acesso a receber o link com o respectivo relatório. Depois clique em [  ].



O Acesso é disponibilizado a partir do “*Portal de autenticação*” como já mencionado. (Ver [Seção 10.6 – Captive portal](#)).

Ainda nesta interface temos o quadro **[Arquivos]** que mantém disponível para “Download” todos os relatórios “PDF’s” extraídos no período.

Arquivos							Buscar	Q
Relatório	Usuário / Grupo	Tipo	Período	Data	Tamanho	Ação		
Visão Geral	-	PDF	Diário 26-07-2016	26-07-2016	238,43 KB			
Timeline	jack@blockbit.com	PDF	Diário 19-07-2016	19-07-2016	113,68 KB			
Visão Geral	-	PDF	Diário 15-07-2016	15-07-2016	241,62 KB			
Relatório de Tráfego	-	CSV	Diário 15-07-2016	15-07-2016	24,39 MB			
Timeline	max@blockbit.com	PDF	Diário 19-05-2016	20-05-2016	82,15 KB			
Timeline	max@blockbit.com	PDF	Diário 16-05-2016	16-05-2016	79,96 KB			
Timeline	zac@blockbit.com	PDF	Diário 16-05-2016	16-05-2016	78,63 KB			

## 26.7 Relatórios Tráfego Geral

No menu [Dashboard] >> [Tráfego Geral] temos:

Relatórios estatísticos do sistema e um serviço de monitoração em tempo real

- Rede, Consumo de Banda, Desempenho; Tempo Real (ethx) e Histórico (ethx).
- Monitor de tráfego

### 26.7.1 Estatísticas do Servidor e Desempenho



### 26.7.2 Tempo Real e Histórico



## 26.8 Relatórios Tráfego Web

No menu [Dashboard] >> [Web Filter] temos:

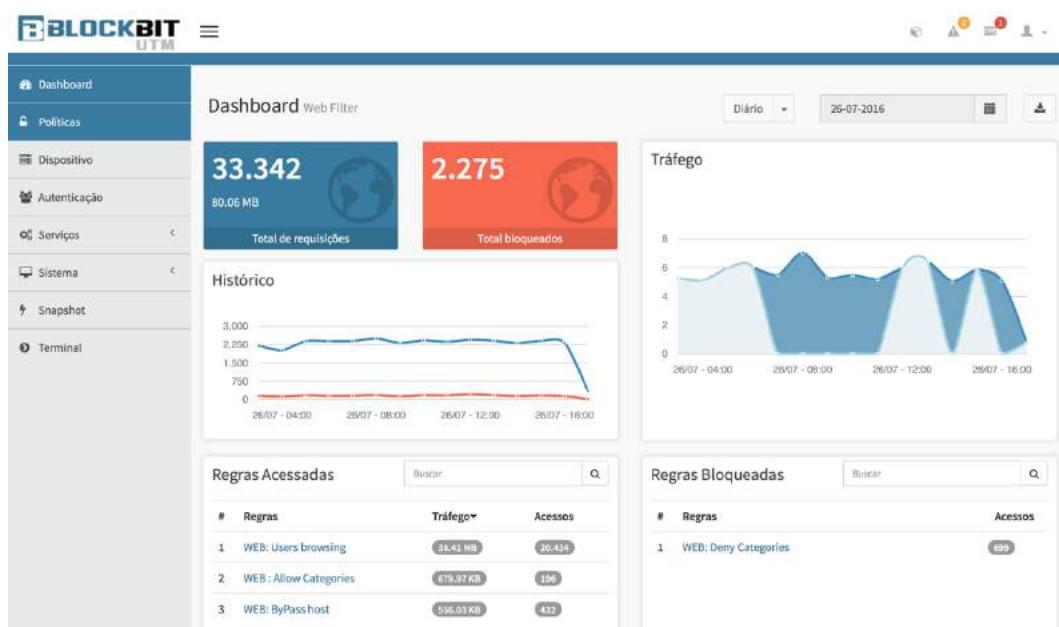
Relatórios estatísticos dos acessos WEB via proxy e um serviço de monitoração em tempo real.

- Total de requisições.
- Total bloqueados.
- Histórico.
- Tráfego.

E informações gerais referentes os filtros de conformidade.

- Regras Acessadas.
- Regras Bloqueadas.
- Usuários.
- Categorias Acessadas.
- Categorias Bloqueadas.
- Usuários x Categorias.
- Aplicativos Permitidos (WEB).
- Aplicativos Bloqueados (WEB).
- Usuários x Aplicativos (WEB).
- Content-types acessados.
- Content-types bloqueados.

Tudo isso para oferecer informações sólidas sobre o tráfego WEB, uma resposta rápida e um gerenciamento bem integrado com a opção de verificação “Diária” ou “Mensal” dos registros e ainda com a opção de extração no formato PDF.



Aqui podemos extrair os relatórios detalhados. Basta clicar sobre os itens de sumário, e aguardar a geração automática do respectivo relatório. No quadro **[Regras Acessadas]**, clique sobre a **[Regra]** para extrair o relatório detalhado desejado.

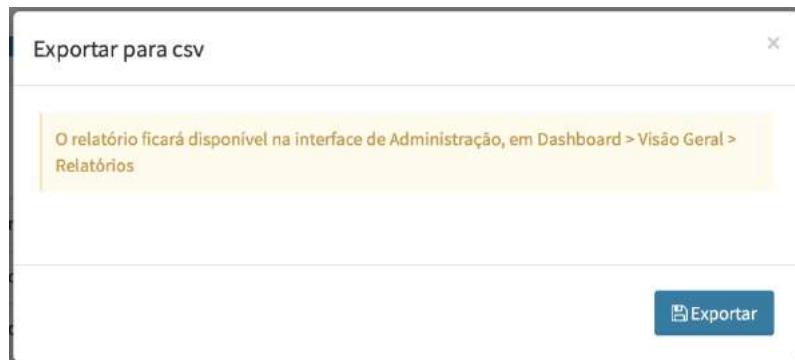
Regras Acessadas			
#	Regras	Tráfego	Acessos
1	WEB: Users browsing	38.41 MB	20.434
2	WEB : Allow Categories	679.97 KB	196
3	WEB: ByPass host	556.03 KB	432

Data	Usuário	Site	Ação
26-07-2016 03:06:00	olivia@blockbit.com	HTTP://CRL.MICROSOFT.COM	
26-07-2016 03:06:00	isabelle@blockbit.com	HTTP://A.WUNDERLIST.COM	
26-07-2016 03:06:00	isabelle@blockbit.com	HTTP://A2F5A7C5.CUL1.ORSP.F-SECURE.COM	
26-07-2016 03:06:00	isabelle@blockbit.com	HTTP://SOCKET.WUNDERLIST.COM	
26-07-2016 03:06:00	aidan@blockbit.com	HTTP://37.252.253.6	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://CONVERT-VIDEO-ONLINE.COM	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://SCSS-PROD-UE1-NOTIF-14.ADOBE.COM	
26-07-2016 03:06:00	matthew@blockbit.com	HTTP://FEDORAPROJECT.ORG	
26-07-2016 03:06:00	isabelle@blockbit.com	HTTP://A.WUNDERLIST.COM	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://CONVERT-VIDEO-ONLINE.COM	
26-07-2016 03:06:00	aidan@blockbit.com	HTTP://37.252.253.6	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://SCSS-PROD-UE1-NOTIF-14.ADOBE.COM	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://ARMML.ADOBE.COM	
26-07-2016 03:06:00	logan@blockbit.com	HTTP://CRL.MICROSOFT.COM	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://302-TROUTER-WEU-B.DRIP.TROUTER.IO	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://SCSS-PROD-UE1-NOTIF-14.ADOBE.COM	
26-07-2016 03:06:00	jack@blockbit.com	HTTP://434-TROUTER-WEU-B.DRIP.TROUTER.IO	
26-07-2016 03:06:00	noah@blockbit.com	HTTP://CONVERT-VIDEO-ONLINE.COM	
26-07-2016 03:06:00	aidan@blockbit.com	HTTP://37.252.253.6	

O administrador tem a opção de detalhar o relatório por usuário. Clique sobre o **[usuário]** que pretende detalhar.

Data	Usuário	Site	Ação
26-07-2016 03:06:00	olivia@blockbit.com	● http://cr1.microsoft.com	
26-07-2016 03:10:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	
26-07-2016 03:10:00	olivia@blockbit.com	● http://finance.services.appex.bing.com	
26-07-2016 03:17:00	olivia@blockbit.com	● http://cr1.microsoft.com	
26-07-2016 03:20:00	olivia@blockbit.com	● https://nexus.officeapps.live.com	
26-07-2016 03:27:00	olivia@blockbit.com	● http://foodanddrink.tile.appex.bing.com	
26-07-2016 03:27:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	
26-07-2016 03:27:00	olivia@blockbit.com	● http://service.weather.microsoft.com	
26-07-2016 03:30:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	
26-07-2016 03:35:00	olivia@blockbit.com	● https://go.microsoft.com	
26-07-2016 03:35:00	olivia@blockbit.com	● https://wscont.apps.microsoft.com	
26-07-2016 03:35:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	
26-07-2016 03:35:00	olivia@blockbit.com	● http://finance.services.appex.bing.com	
26-07-2016 03:35:00	olivia@blockbit.com	● http://cr1.microsoft.com	
26-07-2016 03:45:00	olivia@blockbit.com	● http://foodanddrink.tile.appex.bing.com	
26-07-2016 03:45:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	
26-07-2016 03:45:00	olivia@blockbit.com	● http://service.weather.microsoft.com	
26-07-2016 04:36:00	olivia@blockbit.com	● http://cr1.microsoft.com	
26-07-2016 04:40:00	olivia@blockbit.com	● http://pt-br.appex-rf.msn.com	

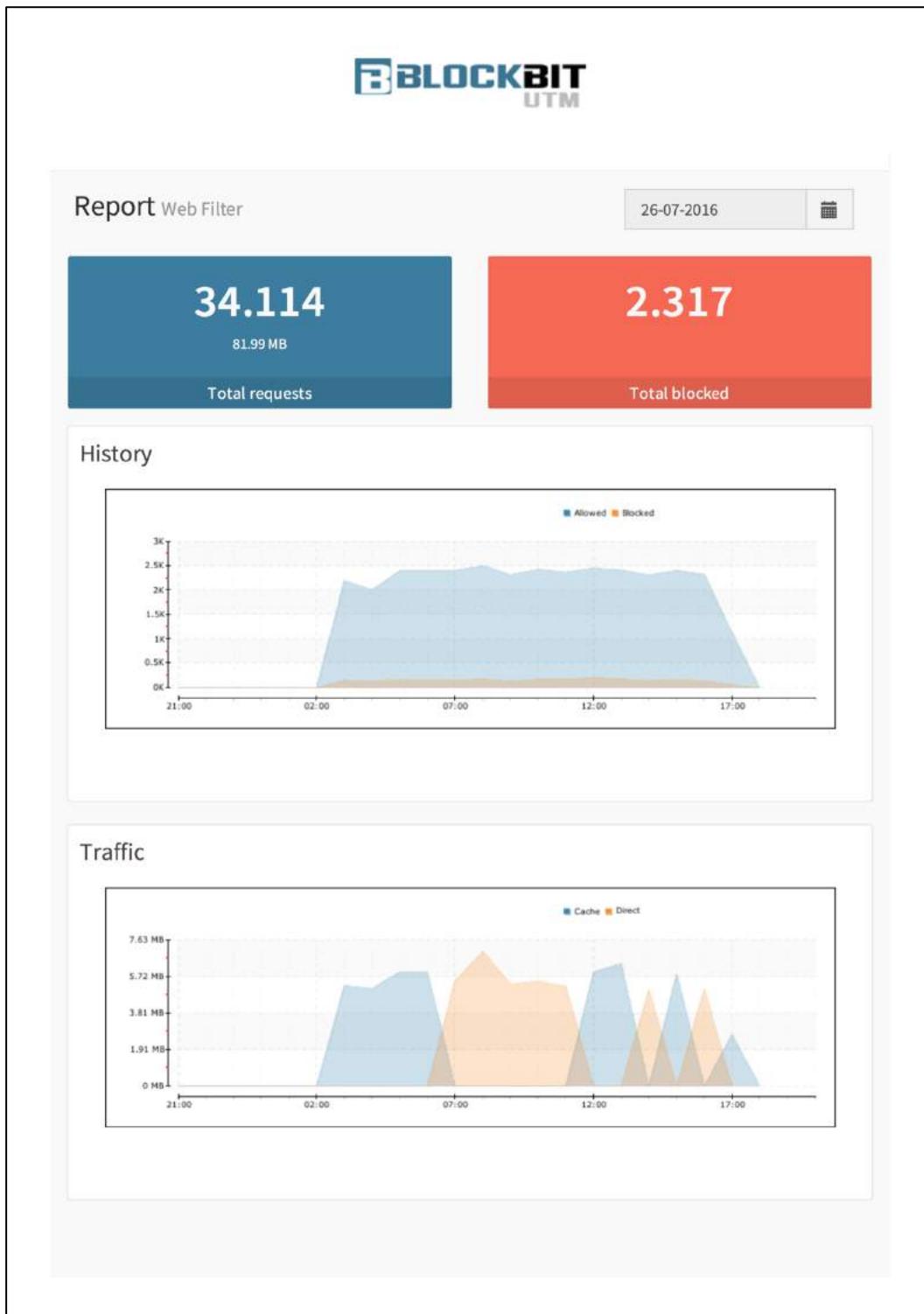
Para extrair os relatórios detalhados no formato **[CSV]**, clique em **[ ]**, em seguida clique em **[ Exportar ]**



Para visualizar o arquivo “.CSV”, acesse **[Dashboard] >> [Visão Geral]** e clique em **Relatórios - [ ]** e faça “Download” do arquivo.

Arquivos						
Relatório	Usuário / Grupo	Tipo	Período	Data	Tamanho	Ação
Relatório do Web Filter	-	CSV	Diário 26-07-2016	26-07-2016	7,09 MB	

Para extrair os relatórios no formato PDF, na interface principal do [Dashboard] >> [Web Filter] clique em [  ].



#	Rules	Traffic	Views
1	WEB: Users browsing	39.44 MB	20.931
2	WEB : Allow Categories	687.07 KB	198
3	WEB: ByPass host	556.03 KB	432

#	Rules	Views
1	WEB: Deny Categories	715

### Categories Accessed

#	Category	Traffic▼	Time	Views
1	Search Engines and Portals	6.5 MB	9h49m	2.552
2	Productivity Categories	4.33 MB	14h15m	3.651
3	Information Technology	4.3 MB	6h7m	797
4	Web Mail	3.13 MB	1h34m	152
5	Internet Communication	687.07 KB	3h18m	198
6	Instant Messaging	118.71 KB	0h15m	15
7	Freeware and Software Download	109.37 KB	0h57m	78
8	Restaurants and Dining	67.02 KB	0h42m	42
9	Advertisements	54.2 KB	0h21m	21
10	Educational Institutions	48.67 KB	0h21m	105

### Categories Blocked

#	Category	Views
1	Search Engines and Portals	327
2	Information Technology	116
3	Freeware and Software Download	89

## 26.9 Relatórios Ameaças e Aplicações

No menu [Dashboard] >> [Advanced Threat Protection] temos:

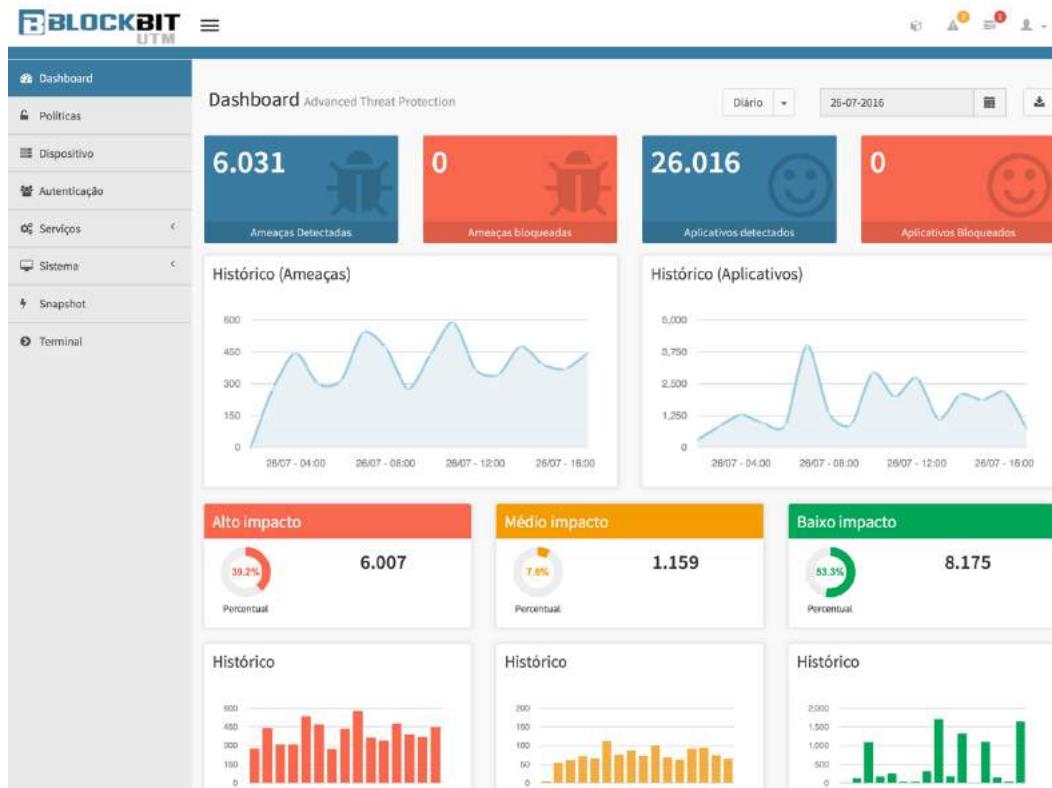
Relatórios estatísticos e históricos das ameaças e aplicativos detectados e bloqueados pelo sensor ATP.

- Ameaças Detectadas.
- Ameaças Bloqueadas
- Aplicativos Detectados.
- Aplicativos Bloqueados.
- Histórico das ameaças.
- Histórico dos aplicativos.
- Tráfego.
- (%) Alto Impacto.
- (%) Médio Impacto.
- (%) Baixo Impacto.
- Históricos (Alto/ Médio/ Baixo – Impacto).

E informações gerais referentes os filtros de conformidade.

- Ameaças Detectadas.
- Ameaças Bloqueadas.
- Ameaças x Usuários.
- Usuários.
- Aplicativos Detectados.
- Aplicativos Bloqueados.
- Aplicativos x Usuários.

Tudo isso para oferecer informações sólidas sobre as tentativas de ataques de Ameaças e Aplicativos detectados, uma resposta rápida e um gerenciamento bem integrado com a opção de verificação “Diária” ou “Mensal” dos registros e ainda com a opção de extração no formato PDF.



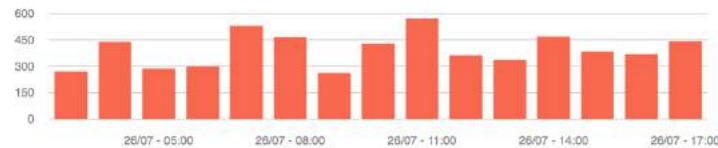
Neste quadro ainda podemos descer o nível de detalhamento do sumário e clicar sobre algum item de recurso.

No quadro [Ameaças Detectadas], clique sobre uma [Ameaça] específica para extrair um sumário mais detalhado.

Ameaças Detectadas			
#	Ameaças	Impacto	Detecções
1	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbou...	Alto	5.913
2	CHAT Jabber/Google Talk Outgoing Traffic	Baixo	31
3	POLICY Http Client Body contains pass= in cleartext	Alto	25
4	POLICY HotSpotShield Activity	Alto	14
5	POLICY Suspicious inbound to mySQL port 3306	Médio	9
6	POLICY SSH banner detected on TCP 443 likely pr...	Médio	6
7	POLICY Vulnerable Java Version 1.8.x Detected	Médio	6

### Ameaças Detectadas MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake

#### Histórico



#### Ameaças Detectadas

#	Usuários	Hits
1	thomas@blockbit.com	5913

A partir daí podemos detalhar o relatório detalhado de origem da **[Ameaça]**. Basta clicar sobre os **[Usuários]**, da lista e aguardar a geração automática do respectivo relatório.

Relatório de Ameaças						
Data	Usuário/IP	Origem	Destino	Tipo	Impacto	Detecção
26-07-2016 17:54	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:53	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:52	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:51	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:50	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:49	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:48	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:47	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:46	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:45	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:44	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:43	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:42	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:41	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:40	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
26-07-2016 17:39	andre@blockbit.com	127.0.0.1	127.0.0.1	Ameaça	alto	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake

Para extrair os relatórios detalhados no formato **[CSV]**, clique em **[ ]**, em seguida clique em **[ Exportar ]**



Para visualizar o arquivo “.CSV”, acesse **[Dashboard] >> [Visão Geral]** e clique em **Relatórios - [ ]** e faça “Download” do arquivo.

Arquivos						
Relatório	Usuário / Grupo	Tipo	Período	Data	Tamanho	Ação
Relatório do Web Filter	-	CSV	Diário 26-07-2016	26-07-2016	7,09 MB	

Para extrair os relatórios no formato PDF, clique em .



**Report Advanced Threat Protection**

26-07-2016 

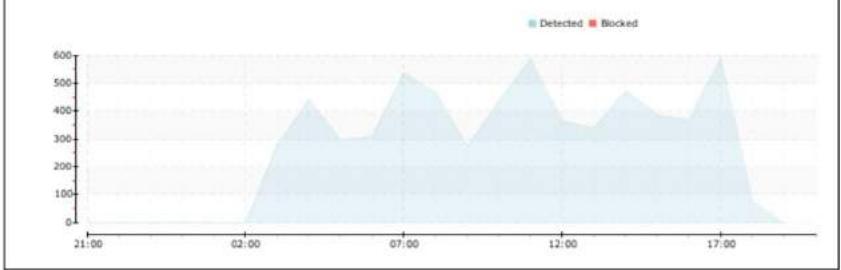
**6.255**

Detected Threats

**0**

Blocked Threats

**History (Threats)**



Detected Threats (blue line) and Blocked Threats (red line) over a 24-hour period from 21:00 to 17:00. The chart shows a fluctuating pattern with peaks around 07:00 and 12:00.

Legend: Detected (blue), Blocked (red)

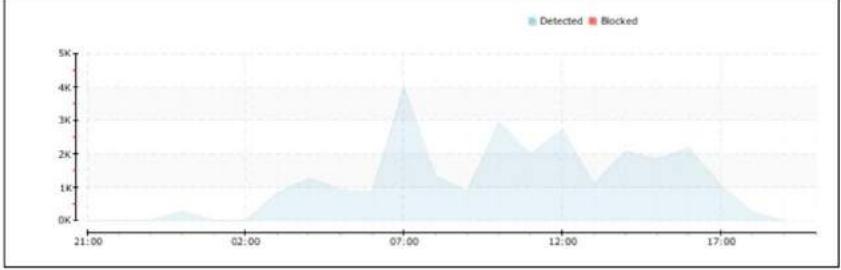
**26.588**

Applications detected

**0**

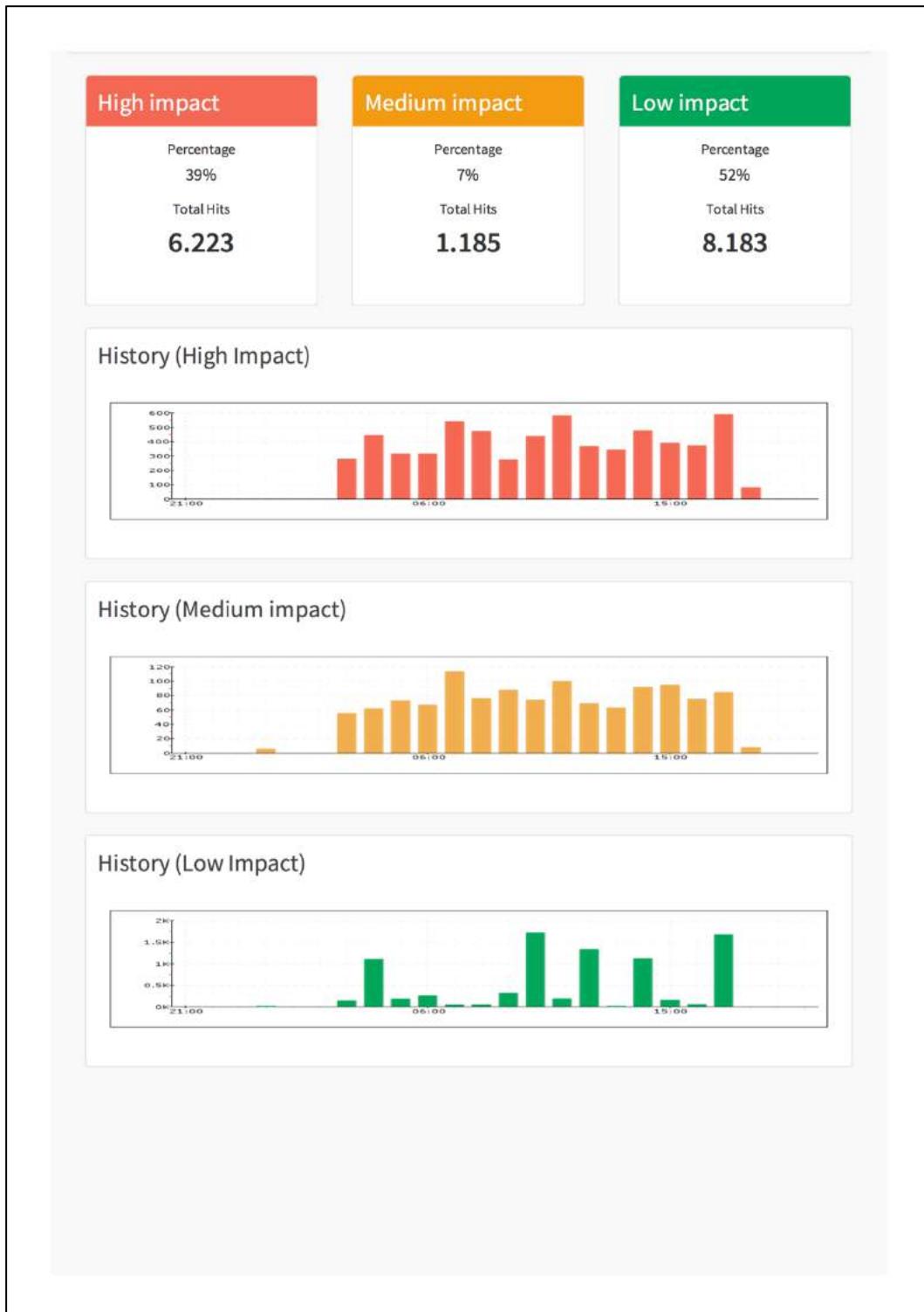
Blocked Applications

**History (Applications)**



Detected Applications (blue line) and Blocked Applications (red line) over a 24-hour period from 21:00 to 17:00. The chart shows a fluctuating pattern with peaks around 07:00 and 12:00.

Legend: Detected (blue), Blocked (red)



### Detected Threats

#	Threats	Impact	Detections
1	MALWARE Mozilla User-Agent (Mozilla/5.0) Inbou...	Alto	6.116
2	CHAT Jabber/Google Talk Outgoing Traffic	Baixo	39
3	POLICY Http Client Body contains pass= in cleart...	Alto	26
4	POLICY HotSpotShield Activity	Alto	15
5	POLICY Suspicious inbound to mySQL port 3306	Médio	9
6	POLICY SSH banner detected on TCP 443 likely p...	Médio	6
7	POLICY Vulnerable Java Version 1.8.x Detected	Médio	6
8	CHAT Google Talk (Jabber) Client Login	Alto	5
9	CHAT Google IM traffic Jabber client sign-on	Alto	5
10	POLICY iTunes User Agent	Alto	5

### Blocked Threats

#	Threats	Impact	Detections
Nenhum ítem encontrado			

### Applications Detected

#	Applications	Detections
1	IMTransferAgent	2.934
2	The Internet Archive	2.168
3	Microsoft Update	1.925
4	Gravatar	1.796
5	LivePerson	1.765
6	Disqus	1.579
7	Quora	1.386
8	TED	944
9	QualysGuard	900
10	AddThis	781

### Blocked Applications

#	Applications	Detections
	Nenhum item encontrado	

## 26.10 Relatórios Intrusion Prevention System

No menu [Dashboard] >> [Intrusion Prevention System] temos:

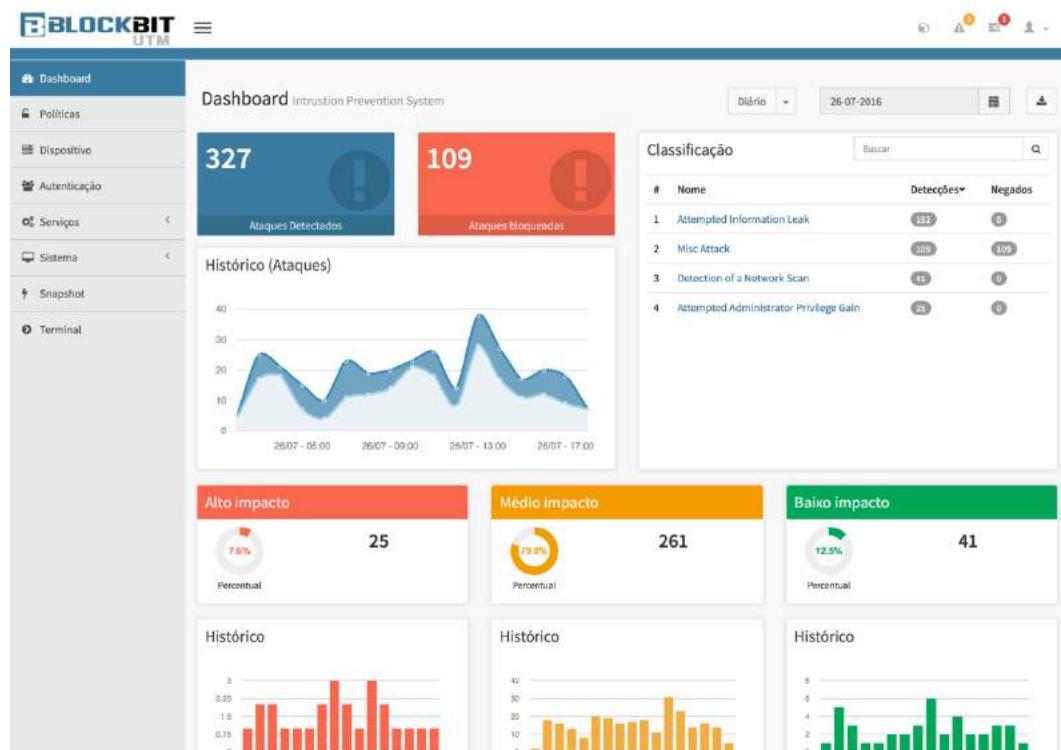
Relatórios estatísticos e históricos das ameaças e aplicativos detectados e bloqueados pelo sensor ATP.

- Ataques Detectados.
- Ataques bloqueados.
- Classificação.
- Histórico dos (Ataques).
- (%) Alto Impacto.
- (%) Médio Impacto.
- (%) Baixo Impacto.
- Históricos (Alto/ Médio/ Baixo – Impacto).

E informações gerais referentes os filtros de conformidade.

- Ataques detectados.
- Ameaças x IP de destino.
- Impactos x IP de destino.

Tudo isso para oferecer informações sólidas sobre as tentativas de ataques detectados, uma resposta rápida e um gerenciamento bem integrado com a opção de verificação “Diária” ou “Mensal” dos registros e ainda com a opção de extração no formato PDF.



Neste quadro ainda podemos descer o nível de detalhamento do sumário e clicar sobre algum item de recurso.

No quadro **[Ataques detectados]**, clique sobre uma **[ameaça]** específica para extrair o sumário mais detalhado.

The screenshot shows the 'Ataques Detectados' (Detected Attacks) section. At the top, there is a table with columns: # Ataques, Impacto (Impact), Detecções (Discoveries), and Negados (Rejected). The table lists seven attacks with their respective details:

# Ataques	Impacto	Detecções	Negados
1 SCAN Sip vicious User-Agent Detected (friendly-scanner)	Médio	88	0
2 CINS Active Threat Intelligence Poor Reputation I...	Médio	53	53
3 SCAN Potential SSH Scan	Médio	50	0
4 SCAN Sip vicious Scan	Médio	34	0
5 SCAN Behavioral Unusually fast Terminal Server ...	Baixo	25	0
6 SCAN LibSSH Based Frequent SSH Connections L...	Alto	25	0
7 DROP Spamhaus DROP Listed Traffic inbound gr...	Médio	21	21

Below the table, a detailed view for 'SCAN Sip vicious User-Agent Detected (friendly-scanner)' is shown. It includes a histogram titled 'Histórico' (Historical) showing the number of detections over time intervals from 26/07 - 05:00 to 26/07 - 18:00. The histogram bars range from approximately 0 to 10 detections. Below the histogram is a table of users associated with this attack:

# Usuários	Hits
1 187.8.187.104	34
2 187.8.187.120	34

A partir daí podemos visualizar o relatório detalhado de origem da **[ameaça]**. Basta clicar sobre os **[usuários]**, da lista e aguardar a geração automática do respectivo relatório.

The screenshot shows a detailed log of detected attacks. The table has columns: Data (Date), Usuário/IP (User/IP), Origem (Origin), Destino (Destination), Impacto (Impact), Detecção (Discovery), and Ação (Action). Two entries are listed:

Data	Usuário/IP	Origem	Destino	Impacto	Detecção	Ação
26-07-2016 18:05	187.8.187.104	74.208.164.171	187.8.187.104	Médio	SCAN Sip vicious User-Agent Detected (friendly-scanner)	<span>15</span>
26-07-2016 17:40	187.8.187.104	209.126.127.199	187.8.187.104	Médio	SCAN Sip vicious User-Agent Detected (friendly-scanner)	<span>19</span>

Para extrair os relatórios detalhados no formato **[CSV]**, clique em **[ ]**, em seguida clique em **[ Exportar ]**



Para visualizar o arquivo “.CSV”, acesse **[Dashboard] >> [Visão Geral]** e clique em **Relatórios** - [ ] e faça “Download” do arquivo.

Arquivos							Buscar	
Relatório	Usuário / Grupo	Tipo	Período	Data	Tamanho	Ação		
Relatório do Web Filter	-	CSV	Diário 26-07-2016	26-07-2016	7,09 MB			

Para extrair os relatórios no formato PDF, na interface principal do **[Dashboard] >> [Intrusion Prevention System]** clique em [ ].

**BLOCKBIT**  
UTM

**Report** Intrusion Prevention System      26-07-2016

**329**      **111**

Detected Attacks      Blocked attacks

**History (IPS)**

Legend: Detected (light blue), Blocked (red)

**Classification**

#	Name	Detections	Denied
1	Attempted Information Leak	0	0
2	Misc Attack	0	111
3	Detection of a Network Scan	0	0
4	Attempted Administrator Privile..	0	0

**High impact**

Percentage  
7%

Total Hits

**25**

**Medium impact**

Percentage  
79%

Total Hits

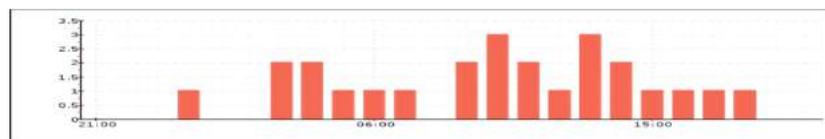
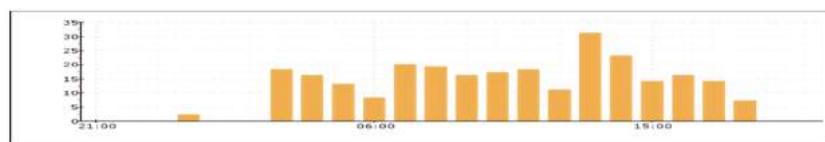
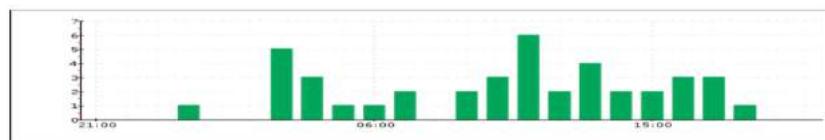
**263**

**Low impact**

Percentage  
12%

Total Hits

**41**

**History (High Impact)****History (Medium Impact)****History (Low Impact)**

### Detected Attacks

#	Intrusion Prevention System	Impact	Detections	Denied
1	SCAN Sip vicious User-Agent Detected (friendly-sc...	Médio	68	0
2	CINS Active Threat Intelligence Poor Reputation ...	Médio	54	54
3	SCAN Potential SSH Scan	Médio	50	0
4	SCAN Sip vicious Scan	Médio	34	0
5	SCAN Behavioral Unusually fast Terminal Server...	Baixo	25	0
6	SCAN LibSSH Based Frequent SSH Connections L...	Alto	25	0
7	DROP Spamhaus DROP Listed Traffic Inbound gr...	Médio	22	22
8	CINS Active Threat Intelligence Poor Reputation ...	Médio	19	19
9	SCAN NETWORK Incoming Masscan detected	Baixo	16	0
10	CINS Active Threat Intelligence Poor Reputation ...	Médio	16	16

### Attacks vs Users

#	User	Attack	Impact	Detections	Denied
1	187.8.187.120	SCAN Potential SSH Scan	Médio	50	0
2	187.8.187.104	CINS Active Threat Intelligence Poor Reputation ...	Médio	38	38
3	187.8.187.104	SCAN Sip vicious Scan	Médio	34	0
4	187.8.187.104	SCAN Sip vicious User-Agent Detected	Médio	34	0
5	187.8.187.120	SCAN Sip vicious User-Agent Detected	Médio	34	0
6	187.8.187.120	SCAN Behavioral Unusually fast Terminal Server...	Baixo	25	0
7	187.8.187.120	SCAN LibSSH Based Frequent SSH Connections L...	Alto	25	0
8	187.8.187.120	DROP Spamhaus DROP Listed Traffic Inbound gr...	Médio	22	22
9	187.8.187.120	CINS Active Threat Intelligence Poor Reputation ...	Médio	19	19
10	187.8.187.104	CINS Active Threat Intelligence Poor Reputation ...	Médio	16	16

Threats vs Users				
#	User	Impact	Detections	Denied
1	187.8.187.120	Médio	141	57
2	187.8.187.104	Médio	122	54
3	187.8.187.120	Baixo	41	0
4	187.8.187.120	Alto	25	0

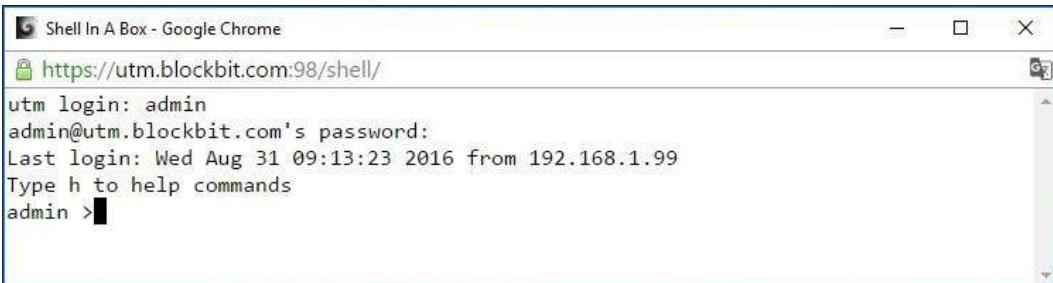
**NOTA:** Não é possível extrair os relatórios detalhados anteriores a data da sua habilitação.

**NOTA:** Para emitir os relatórios detalhados ou descer o nível de detalhamento dos relatórios estatísticos, basta um clique sobre os itens de sumário, e aguardar a geração automática do respectivo relatório.

## 27 Interface BLOCKBIT CLI (Linha de comandos)

O BLOCKBIT UTM disponibiliza um recurso de acesso a console CLI através da interface WEB, que possibilita ao administrador executar comandos de administração e troubleshooting dos principais serviços.

No menu principal clique em **[Terminal]**. Utilize o usuário “admin” e a senha personalizada. O acesso ao terminal é restrito, para listar os comandos disponíveis, digite: ***h***.



```
Shell In A Box - Google Chrome
https://utm.blockbit.com:98/shell/
utm login: admin
admin@utm.blockbit.com's password:
Last login: Wed Aug 31 09:13:23 2016 from 192.168.1.99
Type h to help commands
admin >
```

```
Type '?' or 'help' to get the list of allowed commands
admin >?
BlockBit console commands

arp                      fwrecovery          reset-admin-blocks
arping                   fwreload            reset-admin-password
authsync                 grep                reset-admin-sessions
configure-bgp            h                   rewizard
configure-hdim            host                route
configure-ospf           hostname             sar
configure-rip             ifconfig            service-start
configure-vmachine        ifstat               service-status
conntrack                iostat              service-stop
date                     iotest              show-auth-sessions
debug-auth               ip                  show-uuid
debug-dhcp                ipcalc              show-vpn-conn
debug-firewall           iplist              show-vpn-info
debug-threats            iptraf              shutdown
debug-vpn                 ldapsearch          speedtest
debug-web                 less                sysctl
dig                      lscpu              tcpdump
disable-bgp               lsusb              tcptop
disable-ospf              mkfs              tcptrack
disable-rip               more              telnet
enable-bgp                mtr                tracepath
enable-ospf               netads             traceroute
enable-rip                netstat            update-blockbit
enable-root               nslookup          update-license
enable-snmp              ntpdate            uptime
ethtool                  parted             vmstat
fdisk                    passwd            whois
free                     ping
fsck                     reboot
```

---

## 27.1 [arp]

Utilizado para mapear o endereço de rede (por exemplo, um endereço IPv4 para um endereço físico, como um endereço Ethernet (também chamado endereço MAC). Exibe e modifica esta tabela de relação de endereços da Internet para endereços Ethernet. O ARP foi implementado com muitas combinações de tecnologias de rede e camada de enlace de dados. O IPv4 é o caso mais comum

Utilize este comando para identificar um problema de comunicação de rede ou identificar eventos e status de IP conectados.

### Modo de uso

```
admin >arp -h
Usage:
arp [-vn] [<HW>] [-i <if>] [-a] [<hostname>] <-Display ARP cache
arp [-v] [-i <if>] -d <host> [pub] <-Delete ARP entry
arp [-vnD] [<HW>] [-i <if>] -f [<filename>] <-Add entry from file
arp [-v] [<HW>] [-i <if>] -s <host> <hwaddr> [temp] <-Add entry
arp [-v] [<HW>] [-i <if>] -Ds <host> <if> [netmask <nmask>] pub <'->
-a display (all) hosts in alternative (BSD) style
-e display (all) hosts in default (Linux) style
-s, --set           set a new ARP entry
-d, --delete        delete a specified entry
-v, --verbose       be verbose
-n, --numeric       don't resolve names
-i, --device        specify network interface (e.g. eth0)
-D, --use-device    read <hwaddr> from given device
-A, -p, --protocol  specify protocol family
-f, --file          read new entries from file or from
/etc/ethers

<HW>=Use '-H <hw>' to specify hardware address type. Default: ether
List of possible hardware types (which support ARP):
  ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
  dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi
(HIPPI)
  irda (IrLAP) x25 (generic X.25) infiniband (InfiniBand)
  eui64 (Generic EUI-64)
admin >
```

**Exemplo:** Apresentar a tabela de endereços IP e endereço de hosts físicos (dispositivos) na rede.

```
admin >arp -a
? (172.16.12.85) at 00:26:8b:04:eb:bd [ether] on eth0
? (192.168.254.15) at 00:30:48:c2:02:a4 [ether] on eth2.254
? (172.16.13.248) at 0c:c4:7a:11:0f:96 [ether] on eth0
? (172.16.12.81) at 00:30:48:de:78:ae [ether] on eth0
? (192.168.254.4) at e6:9c:1f:89:11:32 [ether] on eth2.254
? (192.168.253.34) at 7e:49:6f:55:42:00 [ether] on eth2.253
? (172.16.12.92) at <incomplete> on eth0
? (172.16.12.90) at 10:98:36:fb:c9:1b [ether] on eth0
? (172.16.20.22) at 00:0b:ab:f1:9b:bc [ether] on eth3
? (172.16.12.71) at <incomplete> on eth0
? (172.16.20.20) at 00:0c:29:b7:34:cf [ether] on eth3
? (172.16.20.19) at 04:7d:7b:fd:53:d7 [ether] on eth3
? (172.16.12.65) at 78:2b:cb:c4:e7:12 [ether] on eth0
? (172.16.12.64) at <incomplete> on eth0
? (172.16.12.77) at 90:b1:1c:f6:2f:e2 [ether] on eth0
? (192.168.254.22) at 00:e0:4c:68:19:bf [ether] on eth2.254
admin >
```

## 27.2 [arping]

Utilizado para descobrir e identificar os hosts conectados utilizando a associação da tabela ARP com a resposta análoga ao ping que utiliza o protocolo ICMP.

### Modo de uso

```
admin >arping -h
Usage: arping [-fqbDUAV] [-c count] [-w timeout] [-I device] [-s source]
destination
  -f : quit on first reply
  -q : be quiet
  -b : keep broadcasting, don't go unicast
  -D : duplicate address detection mode
  -U : Unsolicited ARP mode, update your neighbours
  -A : ARP answer mode, update your neighbours
  -V : print version and exit
  -c count : how many packets to send
  -w timeout : how long to wait for a reply
  -I device : which ethernet device to use
  -s source : source ip address
  destination : ask for what ip address
admin >
```

**Exemplo:** Descobrir o endereço MAC de um determinado IP

```
admin >arping -c 5 -I eth0 172.16.12.85
ARPING 172.16.12.85 from 172.16.12.1 eth0
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 6.465ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 2.099ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.773ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.761ms
^CSent 4 probes (1 broadcast(s))
Received 4 response(s)
admin >
```

---

## 27.3 [authsync]

Utilizado para análise do processo de sincronismo de usuários. Normalmente usado para “debug” as ocorrências durante o processo de sincronismo.

**Modo de uso**

```
admin >authsync
omne-apply-auth-sync: running
omne-apply-auth-sync: ldap total groups: 3
omne-apply-auth-sync: sync group n: g1, d: g1
omne-apply-auth-sync: sync group n: g2, d: g2
omne-apply-auth-sync: sync group n: g3, d: g3
omne-apply-auth-sync: ldap total users: 3
omne-apply-auth-sync: sync user l: ntavares, s: S-1-5-21-2770178991-
2145852632-2552727236, n: Nemias Tavares
omne-apply-auth-sync: sync user l: jcarvalhal, s: S-1-5-21-2770178991-
2145852632-2552727236, n: Jesias Carvalhal
omne-apply-auth-sync: sync user l: maderno, s: S-1-5-21-2770178991-2145852632-
2552727236, n: Marco Aderno
omne-apply-auth-sync: update users
omne-apply-auth-sync: update groups
omne-apply-auth-sync: Remove users and groups remotes not configured
omne-apply-auth-sync: finish
admin >
```

---

## 27.4 [enable-bgp]

Habilita o modo de configuração do protocolo de roteamento dinâmico BGP.

**Modo de uso**

```
admin >enable-bgp
admin
```

## 27.5 [configure-bgp]

Acessa o modo de configuração do protocolo de roteamento dinâmico BGP.

O acesso requer a senha personalizada do usuário “admin”

### Modo de uso

```
admin >configure-bgp
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^].
BLOCKBIT Dynamic Router Config
+
+
User Access Verification

Password:
localhost>
```

Para listar os comandos para configuração do protocolo, digite: ?

```
localhost> ?
echo      Echo a message back to the vty
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Description of the interactive help system
list      Print command list
quit      Exit current mode and down to previous mode
show      Show running system information
terminal  Set terminal line parameters
who       Display who is on vty
localhost>
```

---

## 27.6 [disable-bgp]

Desabilita o modo de configuração do protocolo de roteamento dinâmico BGP.

### Modo de uso

```
admin >disable-bgp
admin >
```

---

## 27.7 [enable-ospf]

Habilita o modo de configuração do protocolo de roteamento dinâmico OSPF.

**Modo de uso**

```
admin >enable-ospf  
admin >
```

---

## 27.8 [configure-ospf]

Acessa o modo de configuração do protocolo de roteamento dinâmico OSPF.

O acesso requer a senha personalizada do usuário “admin”

**Modo de uso**

```
admin >configure-ospf  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
BLOCKBIT Dynamic Router Config  
+  
+  
  
User Access Verification  
  
Password:  
localhost>
```

Para listar os comandos para configuração do protocolo, digite: ?

```
localhost> ?  
echo      Echo a message back to the vty  
enable    Turn on privileged mode command  
exit      Exit current mode and down to previous mode  
help      Description of the interactive help system  
list      Print command list  
quit      Exit current mode and down to previous mode  
show      Show running system information  
terminal  Set terminal line parameters  
who       Display who is on vty  
localhost>
```

## 27.9 [disable-ospf]

Desabilita o modo de configuração do protocolo de roteamento dinâmico OSPF.

**Modo de uso**

```
admin >disable-ospf  
admin >
```

---

## 27.10 [enable-rip]

Habilita o modo de configuração do protocolo de roteamento dinâmico RIP.

**Modo de uso**

```
admin >enable-rip  
admin >
```

---

## 27.11 [configure-rip]

Acessa o modo de configuração do protocolo de roteamento dinâmico RIP.

O acesso requer a senha personalizada do usuário “admin”

**Modo de uso**

```
admin >configure-rip  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
BLOCKBIT Dynamic Router Config  
+  
+  
User Access Verification  
Password:  
localhost>
```

Para listar os comandos para configuração do protocolo, digite: ?

```
localhost> ?
echo      Echo a message back to the vty
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Description of the interactive help system
list      Print command list
quit      Exit current mode and down to previous mode
show      Show running system information
terminal  Set terminal line parameters
who       Display who is on vty
localhost>
```

---

## 27.12 [disable-rip]

Desabilita o modo de configuração do protocolo de roteamento dinâmico RIP.

### Modo de uso

```
admin >disable-rip
admin >
```

---

## 27.13 [date]

Lista e permite alterar a data e hora atual.

### Modo de uso

```
admin >date --help
Usage: date [OPTION]... [+FORMAT]
      or: date [-u|--utc|--universal] [MMDDhhmm[[CC]YY][.ss]]
Display the current time in the given FORMAT, or set the system date.
...
Mandatory arguments to long options are mandatory for short options too.
-d, --date=STRING          display time described by STRING, not 'now'
-f, --file=DATEFILE        like --date once for each line of DATEFILE
-I[TIMESPEC], --iso-8601[=TIMESPEC] output date/time in ISO 8601 format.
                           TIMESPEC='date' for date only (the default),
                           'hours', 'minutes', 'seconds', or 'ns' for date
                           and time to the indicated precision.
-r, --reference=FILE       display the last modification time of FILE
-R, --rfc-2822              output date and time in RFC 2822 format.
Example: Mon, 07 Aug 2006 12:34:56 -0600
```

```
--rfc-3339=TIMESPEC      output date and time in RFC 3339 format.  
TIMESPEC='date', 'seconds', or 'ns' for  
date and time to the indicated precision.  
Date and time components are separated by  
a single space: 2006-08-07 12:34:56-06:00  
-s, --set=STRING          set time described by STRING  
-u, --utc, --universal    print or set Coordinated Universal Time (UTC)  
--help                   display this help and exit  
--version                output version information and exit
```

admin >

#### Exemplo 1.: Listar a data e hora atual

```
admin >date  
Thu Sep 1 09:59:08 BRT 2016  
admin >
```

#### Exemplo 2.: Atualizar data e hora baseado no fuso horário América/São Paulo.

```
admin > date --date='TZ="America/Sao_Paulo" 11:00'  
Thu Sep 1 11:00:00 BRT 2016  
admin >
```

---

## 27.14 [debug-auth]

Utilizado para verificar o log de debug das ocorrências no processo de autenticação dos usuários do blockbit UTM. Este comando serve para debug a autenticação dos usuários locais e sincronizados.

### Modo de uso

```
admin >debug-auth  
type=auth date=2016-07-13 13:13:18 AddrConn:172.16.12.114  
AddrMac:78:2b:cb:c0:12:3e Login:maderno Action:AUTH_LOGIN Reply:102  
AUTH_LOGIN_ERR_PAM msg:'Wrong Password'  
type=auth date=2016-07-13 13:16:25 AddrConn:172.16.12.89  
AddrMac:1c:87:2c:c5:9c:4a Login:toliveira Action:AUTH_SSO_WIN Reply:510  
AUTH_SSO_WIN_OK ticket:57ddcb336098c149eebca22604e3a01a
```

## 27.15 [debug-dhcp]

Utilizado para verificar os logs de debug referente ao processo de distribuição de IPs do serviço DHCP, e o mapa dos endereços IPs entregues na rede para as estações de trabalho.

```
admin >debug-dhcp
type=dhcp date=2016-07-13 13:23:21  DHCPREQUEST for 172.16.12.59 from
00:26:8b:04:e8:e7 via eth0
type=dhcp date=2016-07-13 13:23:21  DHCPACK on 172.16.12.59 to
00:26:8b:04:e8:e7 via eth0
type=dhcp date=2016-07-13 13:24:35  DHCPREQUEST for 172.16.12.149 from
f0:4d:a2:e1:a4:ae (BRDTGC5SRR1) via eth0
type=dhcp date=2016-07-13 13:24:35  DHCPACK on 172.16.12.149 to
f0:4d:a2:e1:a4:ae (BRDTGC5SRR1) via eth0
type=dhcp date=2016-07-13 13:25:25  DHCPINFORM from 172.16.12.65 via eth0: not
authoritative for subnet 172.16.12.0
admin >
```

---

## 27.16 [debug-firewall]

Utilizado para monitorar o serviço do firewall, a fim de identificar o tráfego passante pelas políticas de compliance. Exibe dados como: data, device, endereço MAC, endereço IP de origem/porta, endereço IP de destino/porta, protocolo, usuário, e o nome da política identificada.

### Modo de uso

```
admin >debug-firewall
type=firewall date=2016-07-13 13:26:23 in=eth0 out=eth1 mac=5c:c9:d3:56:11:c2
src=172.16.12.92:33849 dst=64.4.23.164:40001 proto=UDP
user=cbrandao@blockbit.com rule="NAT: Geral Usuarios - UDP - ICMP"
type=firewall date=2016-07-13 13:26:26 in=eth0 out=eth1 mac=6c:f0:49:f0:cc:21
src=172.16.12.93:52882 dst=177.190.148.120:443 proto=TCP user=- rule="NAT:
Geral Usuarios - TCP"
admin >
```

## 27.17 [debug-threats]

Utilizado para monitorar o serviço de identificação de ameaças [ATP].

### Modo de uso

```
admin >debug-threats  
log not found
```

---

## 27.18 [debug-vpn]

Utilizado para monitorar o processo de conexão do tráfego das conexões VPN IPSEC.

```
admin >debug-vpn  
06[NET] received packet: from 177.92.18.234[4500] to 200.146.46.194[4500] (92  
bytes)  
06[ENC] parsed INFORMATIONAL_V1 request 341152563 [ HASH N(DPD) ]  
06[ENC] generating INFORMATIONAL_V1 request 1237457568 [ HASH N(DPD_ACK) ]  
06[NET] sending packet: from 200.146.46.194[4500] to
```

```
Admin >
```

---

## 27.19 [debug-web]

Utilizado para monitorar as requisições “on line” passantes pelo web-proxy. Exibe dados como: data, endereço MAC, endereço IP de origem/porta, endereço IP de destino/porta, método http, protocolo, usuário, e a url.

### Modo de uso

```
type=web date=2016-09-1414:16:00 bytes=422752 mac=78:2b:cb:c0:12:3e  
src=172.16.12.114:41242 dst=104.239.173.143:443 code=TCP_MISS/200 method=GET  
rule=- user=maderno@labblockbit.com site=https://www.blockbit.com/  
url=https://www.blockbit.com/wp-  
type=web date=2016-09-1414:27:00 bytes=61 mac=00:18:8b:e1:70:bb  
src=172.16.12.212:49403 dst=23.41.173.28:443 code=TAG_NONE/- method=CONNECT  
rule=- user=- site=- url=23.41.173.28:443 agent=[-]  
type=web date=2016-09-1414:27:00 bytes=929 mac=a4:1f:72:fa:4d:39  
src=172.16.12.206:56526 dst=104.156.239.199:80 code=TCP_MISS/304 method=GET  
rule=WEB SSL: Usuarios Autenticados user=dnovais@labblockbit.com  
site=http://themesseo.com/medias/items/demo/AdminLTE-master/AdminLTE-  
master/pages/forms/general.html  
agent=[Mozilla/5.0(WindowsNT10.0;WOW64;rv:48.0)Gecko/20100101Firefox/48.0]
```

## 27.20 [dig]

Utilizado para realizar consultas DNS nos servidores de nomes de domínios, retorna informações tais como: endereços de host, autoridade NS de um domínio, autoridade MX de um domínio de e-mail e etc.

### Modo de uso

```
admin >dig -h
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
          {global-d-opt} host [@local-server] {local-d-opt}
          [ host [@local-server] {local-d-opt} [...] ]
Where: domain   is in the Domain Name System
       q-class  is one of (in,hs,ch,...) [default: in]
       q-type   is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
                  (Use ixfr=version for type ixfr)
       q-opt    is one of:
                  -x dot-notation      (shortcut for reverse lookups)
                  -i                   (use IP6.INT for IPv6 reverse lookups)
                  -f filename          (batch mode)
                  -b address[#port]    (bind to source address/port)
                  -p port              (specify port number)
                  -q name              (specify query name)
                  -t type              (specify query type)
                  -c class             (specify query class)
...
...
```

### Exemplo: Pesquisa simples sobre um domínio NS

```
admin >dig exemplo.org

; <>> DiG 9.10.2 <>> exemplo.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32418
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;exemplo.org.           IN      A

;; ANSWER SECTION:
exemplo.org.        14399   IN      A      195.22.8.70

;; Query time: 819 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Sep 20 09:38:10 BRT 2016
;; MSG SIZE  rcvd: 56

admin >
```

## 27.21 [ethtool]

Utilitário capaz de lhe apresentar e detalhar informações referente as interfaces rede, verificar as interfaces on line, off line, alterar velocidade, alterar forma de negociação e é até mesmo verificar qual interface está localizada fisicamente.

### Modo de uso

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
        [ speed %d ]
        [ duplex half|full ]
        [ port tp|aui|bnc|mii|fibre ]
        [ mdix auto|on|off ]
        [ autoneg on|off ]
        [ advertise %x ]
        [ phyad %d ]
        [ xcvr internal|external ]
        [ wol p|u|m|b|a|g|s|d... ]
        [ sopass %x:%x:%x:%x:%x:%x ]
        [ msglvl %d | msglvl type on|off ... ]
```

**Exemplo:** Identificando uma interface de rede especifica

```
admin >ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supported pause frame use: Symmetric
    Supports auto-negotiation: Yes
    Advertised link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised pause frame use: Symmetric
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    MDI-X: off (auto)
    Supports Wake-on: pumbg
    Wake-on: g
    Current message level: 0x00000007 (7)
                           drv probe link
    Link detected: yes
Admin >
```

## 27.22 [fdisk]

Utilitário usado para gerenciamento de partições de discos rígidos. É possível listar e identificar dispositivos de armazenamento do tipo HDD-SSD, criar partições físicas, lógicas, excluir, exibir informações e etc...

### Modo de uso

```
admin >fdisk -h
Usage:
  fdisk [options] <disk>      change partition table
  fdisk [options] -l <disk>    list partition table(s)
  fdisk -s <partition>        give partition size(s) in blocks
Options:
  -b <size>                  sector size (512, 1024, 2048 or 4096)
  -c[=<mode>]                compatible mode: 'dos' or 'nondos' (default)
  -h                          print this help text
  -u[=<unit>]                display units: 'cylinders' or 'sectors' (default)
  -v                          print program version
  -C <number>                specify the number of cylinders
  -H <number>                specify the number of heads
  -S <number>                specify the number of sectors per track
admin >
```

**Exemplo:** Para listar os discos e partições existentes:

```
admin >fdisk -l
WARNING: fdisk GPT support is currently new, and therefore in an experimental
phase. Use at your own discretion.

Disk /dev/sda: 128.0 GB, 128035676160 bytes, 250069680 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt

#      Start      End  Size   Type      Name
 1        2048     4095   1M  BIOS boot parti
 2       4096    1052671  512M Microsoft basic
 3     1052672    42049535 19.6G Microsoft basic
 4    42049536    70758399 13.7G Microsoft basic
 5    70758400    74891263   2G  Linux swap
 6    74891264    79024127   2G Microsoft basic
 7    79024128   250069646 81.6G Microsoft basic

Disk /dev/mapper/luks-ba8b8ea1-522e-49c2-9c48-02e8db50ec5d: 21.0 GB,
20988297216 bytes, 40992768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```

Disk /dev/mapper/luks-049e58a3-626a-46bf-8019-3db9fd8b6241: 87.6 GB,
87573208576 bytes, 171041423 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/luks-999d4257-849e-4a76-9bbf-6a0ae186ac98: 2113 MB,
2113929216 bytes, 4128768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/luks-92f58453-e018-4e1f-a014-2489dfb715e1: 14.7 GB,
14696841216 bytes, 28704768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/cryptoswap: 2116 MB, 2116026368 bytes, 4132864 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >

```

## 27.23 [fsck]

Utilitário usado para verificar e corrigir erros em discos e sistemas de arquivos.

### Modo de uso

```

admin >fsck -h
/usr/sbin/fsck.ext4: invalid option -- 'h'
Usage: /usr/sbin/fsck.ext4 [-panyrcdfvtDFV] [-b superblock] [-B blocksize]
                           [-I inode_buffer_blocks] [-P process_inode_size]
                           [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
                           [-E extended-options] device

Emergency help:
  -p          Automatic repair (no questions)
  -n          Make no changes to the filesystem
  -y          Assume "yes" to all questions
  -c          Check for bad blocks and add them to the badblock list
  -f          Force checking even if filesystem is marked clean
  -v          Be verbose
  -b superblock Use alternative superblock
  -B blocksize Force blocksize when looking for superblock
  -j external_journal Set location of the external journal
  -l bad_blocks_file Add to badblocks list
  -L bad_blocks_file Set badblocks list
admin >

```

**Exemplo:** Verificar se existem possíveis erros em determinada partição

```
Admin >fsck /dev/sda3
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/sda3: clean, 702/192000 files, 52661/768000 blocks
...
```

---

## 27.24 [fwrecovery]

Utilizado para casos de inacessibilidade da interface de administração WEB, ou do funcionamento de algum serviço que tenha intervenção direta dos permissionamentos do firewall. Sua finalidade é liberar o acesso irrestrito ao sistema. Este comando deve ser utilizado com responsabilidade e critério.

### Modo de uso

```
admin >fwrecovery
Recovery firewall
Be brief, be sure to apply the settings in the admin interface.

Firewall is open !!!
admin >
```

---

## 27.25 [fwreload]

Utilizado para recarregar todos os serviços do firewall, incluindo as políticas de entrada e segurança.

### Modo de uso

```
admin >fwreload
reloading firewall chains
reloading firewall zones
reloading firewall input
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
reloading firewall redirects
reloading firewall security rules
reloading firewall multilink rules
reloading firewall vpn rules
reloading firewall atp rules
admin >
```

---

## 27.26 [help]

Retorna a lista de comandos permitidos.

### Modo de uso

```
admin >help
arp          disable-ospf  hostname  ntpdate      show-vpn-info
arping       disable-rip   ifconfig  parted       shutdown
authsync     enable-bgp   ifstat    passwd       speedtest
clear        enable-ospf  iostat    ping         sysctl
configure-bgp enable-rip   iotest    reboot      tcpdump
configure-hdim enable-root ip        reset       tcptop
configure-ospf enable-snmp  ipcalc   reset-admin-blocks  tcptrack
configure-rip ethtool     iplist   reset-admin-password  telnet
conntrack    exit        iptraf   reset-admin-sessions  tracepath
date         fdisk       less     rewizard    traceroute
debug-auth   free        lscpu    route       update-blockbit
debug-dhcp   fsck        lsusb    sar         update-license
debug-firewall fwrecovery mkfs    service-start  uptime
debug-threats fwreload   more    service-status  vmstat
debug-vpn    grep        mtr     service-stop   whois
debug-web    help        netads  show-auth-sessions
dig          history    netstat  show-uuid
disable-bgp  host        nslookup show-vpn-conn
admin >
```

---

## 27.27 [host]

Semelhante ao comando ‘dig’ também é utilizado para auxiliar na pesquisa de resoluções do tipo DNS. O host é um utilitário muitas vezes usado para verificar se existe publicação de DNS reverso para um determinado host ou endereço IP.

### Modo de uso

```
admin >host
Usage: host [-aCdIriTwv] [-c class] [-N ndots] [-t type] [-W time]
           [-R number] [-m flag] hostname [server]
-a is equivalent to -v -t ANY
-c specifies query class for non-IN data
-C compares SOA records on authoritative nameservers
-d is equivalent to -
-l lists all hosts in a domain, using AXFR
-i IP6.INT reverse lookups
-N changes the number of dots allowed before root lookup is done
-r disables recursive processing
-R specifies number of retries for UDP packets
-s a SERVFAIL response should stop query
-t specifies the query type
-T enables TCP/IP mode
-v enables verbose output
```

```
-w specifies to wait forever for a reply
-W specifies how long to wait for a reply
-4 use IPv4 query transport only
-6 use IPv6 query transport only
-m set memory debugging flag (trace|record|usage)
-V print version number and exit
admin >
```

**Exemplo:** Realizar pesquisa das publicações DNS reverso para um determinado domínio.

```
admin >host www.uol.com.br
www.uol.com.br is an alias for homeuol.ipv6uol.com.br.
homeuol.ipv6uol.com.br has address 200.221.2.45
homeuol.ipv6uol.com.br has IPv6 address 2804:49c:3103:401:ffff:ffff:ffff:1
admin >
```

## 27.28 [Hostname]

Utilizado para exibir ou alterar o nome de host do seu servidor na rede.

### Modo de uso

```
admin >hostname -h
Usage: hostname [-b] {hostname|-F file}           set host name (from file)
          hostname [-a|-A|-d|-f|-i|-I|-s|-y]      display formatted name
          hostname                                display host name

          {yp,nis,}domainname {nisdomain|-F file}    set NIS domain name (from
file)                                         display NIS domain name
          {yp,nis,}domainname                         display dns domain name

          dnsdomainname                            display dns domain name

          hostname -V|--version|-h|--help          print info and exit

Program name:
          {yp,nis,}domainname=hostname -y
          dnsdomainname=hostname -d

Program options:
          -a, --alias          alias names
          -A, --all-fqdns      all long host names (FQDNs)
          -b, --boot            set default hostname if none available
          -d, --domain          DNS domain name
          -f, --fqdn, --long    long host name (FQDN)
          -F, --file            read host name or NIS domain name from given file
          -i, --ip-address      addresses for the host name
```

```

-I, --all-ip-addresses all addresses for the host
-s, --short           short host name
-y, --yp, --nis       NIS/YP domain name

Description:
This command can get or set the host name or the NIS domain name. You can
also get the DNS domain or the FQDN (fully qualified domain name).
Unless you are using bind or NIS for host lookups you can change the
FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
part of the FQDN) in the /etc/hosts file.

admin >

```

**Exemplo:** Utilizando o comando para exibir o nome atual do servidor.

```

admin >hostname
utm11.labblockbit.com
admin >

```

## 27.29 [ifconfig]

Utilizado para configurar e manter as configurações da interface. Com a possibilidade de tornar uma interface ativa ou desativar uma interface e ainda listar o status de cada uma delas. Também pode ser utilizado para otimizar a configuração do sistema.

### Modo de uso

```

admin >ifconfig -h
Usage:
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[[-]broadcast [<address>]] [[[-]pointopoint [<address>]]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [mtu <NN>]
[[[-]trailers] [[[-]arp] [[[-]allmulti]
[multicast] [[[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[[-]dynamic]
[up|down] ...
<HW>=Hardware Type.
List of possible hardware types:
loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive
(Adaptive Serial Line IP)

```

```
ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
irda (IrLAP) ec (Econet) x25 (generic X.25)
infiniband (InfiniBand) eui64 (Generic EUI-64)
<AF>=Address family. Default: inet
List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
admin >
```

**Exemplo:** Exibir as informações sobre todas as interfaces de rede, ativas e desabilitadas.

```
admin >ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
                ether 00:0c:29:71:fe:66 txqueuelen 1000 (Ethernet)
                RX packets 895243 bytes 676267249 (644.9 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 788242 bytes 687676742 (655.8 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.11 netmask 255.255.255.0 broadcast 192.168.0.255
                ether 00:0c:29:71:fe:70 txqueuelen 1000 (Ethernet)
                RX packets 829105 bytes 229214066 (218.5 MiB)
                RX errors 0 dropped 1472 overruns 0 frame 0
                TX packets 821284 bytes 646132739 (616.2 MiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4098<BROADCAST,MULTICAST> mtu 1500
        ether 00:0c:29:71:fe:7a txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## 27.30 [ifstat]

Utilizado para exibir a estatística do tráfego de rede.

### Modo de uso

```
admin >ifstat -h
Usage: ifstat [OPTION] [ PATTERN [ PATTERN ] ]
      -h, --help          this message
      -a, --ignore ignore history
      -d, --scan=SECS    sample every statistics every SECS
      -e, --errors show errors
      -n, --nooutput     do history only
      -r, --reset        reset history
      -s, --noupdate    don;t update history
      -t, --interval=SECS report average over the last SECS
      -V, --version      output version information
      -z, --zeros        show entries with zero activity
admin >
```

**Exemplo:** Listar relatório estatístico geral do tráfego de todas as interfaces da rede

```
admin >ifstat
#kernel
Interface      RX Pkts/Rate      TX Pkts/Rate      RX Data/Rate      TX Data/Rate
               RX Errs/Drop      TX Errs/Drop      RX Over/Rate      TX Coll/Rate
  lo           19982K 0           19982K 0           425601K 0           425601K 0
              0 0                 0 0                 0 0                 0 0
  eth0         896411 0           789041 0           676523K 0           687826K 0
              0 0                 0 0                 0 0                 0 0
  eth1         829588 0           821426 0           229273K 0           646217K 0
              0 1476                0 0                 0 0                 0 0
  eth3         302159 0           19735 0            24840K 0            1616K 0
              0 30                 0 0                 0 0                 0 0
  ifb0         537040 0           537040 0           107390K 0           107390K 0
              0 0                 0 0                 0 0                 0 0
  ipsec0       0 0                 0 0                 0 0                 0 0
              0 0                 0 0                 0 0                 0 0
admin >
```

---

## 27.31 [iotest]

Utilizado para executar um teste de escrita de (I/O) entrada e saída na estrutura de partições “filesystem” do disco do seu servidor BLOCKBIT.

### Modo de uso

```
admin >iotest
Testing root filesystem
1000000+0 registros de entrada
1000000+0 registros de saída
2048000000 bytes (2,0 GB) copiados, 89,0756 s, 23,0 MB/s
Cleaning
admin >
```

---

## 27.32 [ipcalc]

Utilitário para cálculo de máscara de rede/sub-redes IPv4 e IPv6. Possui opções para identificar o prefixo (máscara), o endereço de rede, e de broadcast.

### Modo de uso

```
admin >ipcalc -h
ipcalc: ip address expected
Usage: ipcalc [OPTION...]
  -c, --check      Validate IP address for specified address family
  -4, --ipv4       IPv4 address family (default)
  -6, --ipv6       IPv6 address family
  -b, --broadcast  Display calculated broadcast address
  -h, --hostname   Show hostname determined via DNS
  -m, --netmask    Display default netmask for IP (class A, B, or C)
  -n, --network    Display network address
  -p, --prefix     Display network prefix
  -s, --silent     Don't ever display error messages

Help options:
  -?, --help        Show this help message
  --usage          Display brief usage message
admin >
```

**Exemplo:** Calculando uma subnet, seu endereço de rede e broadcast.

```
admin >ipcalc -n -b -p 192.168.7.0/23
PREFIX=23
BROADCAST=192.168.7.255
NETWORK=192.168.6.0
admin >
```

---

## 27.33 [iplist]

Utilizado para listar as informações das interfaces de rede, endereços IPs, as zonas de rede associadas as respectivas interfaces de rede e etc.

### Modo de uso

```
admin >iplist
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:71:fe:66 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
            valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok

admin >
```

---

## 27.34 [iptraf]

Utilitário para monitoramento de rede para os protocolos TCP e UDP. Nele reúne-se uma variedade de estatísticas e gráficos de tráfego da rede, detalhamento estatístico das interfaces e indicadores de atividades.

### Modo de uso

```
admin >iptraf -h
usage: iptraf-ng [options]
      or: iptraf-ng [options] -B [-i <iface> | -d <iface> | -s <iface> | -z
<iface> | -l <iface> | -g]

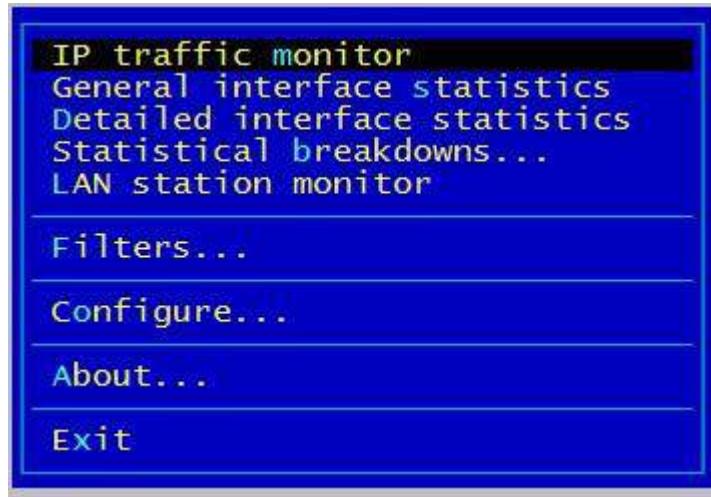
-h, --help                      show this help message
-i <iface>                      start the IP traffic monitor (use '-i all' for all
interfaces)
-d <iface>                      start the detailed statistics facility on an
interface
-s <iface>                      start the TCP and UDP monitor on an interface
-z <iface>                      shows the packet size counts on an interface
-l <iface>                      start the LAN station monitor (use '-l all' for all
LAN interfaces)
-g                                start the general interface statistics

-B                                run in background (use only with one of the above
parameters
-f                                clear all locks and counters
-t <n>                            run only for the specified <n> number of minutes
-L <logfile>                     specifies an alternate log file

admin >
```

**Exemplo:** Carregando a interface GUI do utilitário iptraf.

```
admin >iptraf  
admin >
```



---

## 27.35 [less]

Esse comando permite fazer a paginação de [arquivos](#) ou de uma entrada padrão. É possível direcionar a saída de outro comando usando o pipe “|”.

### Modo de uso

Utilize o comando less como saída de outro comando que devolva uma quantidade de informações muito extensa.

```
admin >iplist | less  
admin >  
  
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000  
    link/ether 00:0c:29:71:fe:66 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0  
        valid_lft forever preferred_lft forever  
eth0: negotiated 1000baseT-FD flow-control, link ok  
  
ZONE WAN (3) 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb  
    state UP qlen 1000  
    link/ether 00:0c:29:71:fe:70 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.11/24 brd 192.168.0.255 scope global eth1  
        valid_lft forever preferred_lft forever  
eth1: negotiated 1000baseT-FD flow-control, link ok  
ZONE (WAN) eth2: negotiated 1000baseT-FD flow-control, link ok
```

```
ZONE DMZ (2) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:71:fe:84 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.11/24 brd 172.16.102.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok
(END)
```

---

## 27.36 [lscpu]

Exibe informações sobre a arquitetura da CPU.

**Modo de uso.**

```
admin >lscpu
Architecture:           x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:             Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) per core:    1
Core(s) per socket:    4
Socket(s):              1
NUMA node(s):           1
Vendor ID:              GenuineIntel
CPU family:             6
Model:                 55
Model name:             Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
Stepping:               8
CPU MHz:                2400.093
BogoMIPS:               4000.16
Virtualization:         VT-x
L1d cache:              24K
L1i cache:              32K
L2 cache:                1024K
NUMA node0 CPU(s):      0-3
admin >
```

---

## 27.37 [lsusb]

Exibe informações sobre os dispositivos USB conectados ao servidor.

**Modo de uso**

```
admin >lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
```

---

## 27.38 [mkfs]

Utilizado para formatar um sistema de arquivos na arquitetura Linux/unix..

### Modo de uso

```
admin >mkfs -h
/usr/sbin/mkfs.ext4: invalid option -- 'h'
Usage: mkfs.ext4 [-c|-l filename] [-b block-size] [-C cluster-size]
                [-i bytes-per-inode] [-I inode-size] [-J journal-options]
                [-G flex-group-size] [-N number-of-inodes]
                [-m reserved-blocks-percentage] [-o creator-os]
                [-g blocks-per-group] [-L volume-label] [-M last-mounted-directory]
                [-O feature[,...]] [-r fs-revision] [-E extended-option[,...]]
                [-t fs-type] [-T usage-type ] [-U UUID] [-jnqvDFKSV] device [blocks-
count]
admin >
```

**Exemplo:** Para formatar um dispositivo identificado pelo comando fdisk -l.

Digite “**mkfs -t ext4 [/dev/sdx??]**”

```
admin > mkfs -t ext4 /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
488640 inodes, 1953152 blocks
97657 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2000683008
60 block groups
32768 blocks per group, 32768 fragments per group
8144 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information:
done
admin >
```

---

## 27.39 [more]

Esse comando permite fazer a paginação de [arquivos](#) ou de uma entrada padrão. É possível direcionar a saída de outro comando usando o pipe “|”.

### Modo de uso

Utilize o comando more como saída de outro comando que devolva uma quantidade de informações muito extensa.

```
admin >iplist | more
ZONE LAN (1) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0b:ab:ac:a3:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.16.20.1/24 brd 172.16.20.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 8: eth0.102@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.1/24 brd 172.16.102.255 scope global eth0.102
        valid_lft forever preferred_lft forever
eth0.102: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 7: eth0.101@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.1/24 brd 172.16.101.255 scope global eth0.101
        valid_lft forever preferred_lft forever
eth0.101: negotiated 1000baseT-FD flow-control, link ok
ZONE LAN (1)
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.12.1/23 brd 172.16.13.255 scope global eth0
        valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok
```

---

## 27.40 [mtr]

Utilitário para testes de roteamento, combina as funções do traceroute e do ping.

### Modo de uso

```
admin >mtr -h
usage: /usr/sbin/mtr [-BfhvwctglxspQomniuT46] [--help] [--version] [--report]
                      [--report-wide] [--report-cycles=COUNT] [--curses] [--gtk]
```

```
[--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns]
[--show-ips] [--address interface] [--filename=FILE|-F]
[--ipinfo=item_no|-y item_no] [--aslookup|-z]
[--psize=bytes/-s bytes] [--order fields]
[--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-
ttl=NUM]
[--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [-
-timeout=SECONDS]
[--interval=SECONDS] HOSTNAME
admin >
```

**Exemplo:** Teste de roteamento para um destino específico.

```
admin >mtr www.google.com.br
admin >
My traceroute [v0.85]
utm.blockbit.com (0.0.0.0)
Thu Sep 1 17:24:42 2016
Keys: Help Display mode Restart statistics Order of fields quit

Packets          Pings
Host
Loss% Snt Last Avg Best Wrst StDev
1. 10.70.64.1
0.0%   5   7.7 44.3  7.7 171.9  71.5
2. c9062541.virtua.com.br
0.0%   5   10.9 44.8 10.6 175.2  72.9
3. c9062825.virtua.com.br
0.0%   4   15.9 49.5 10.1 153.5  69.4
4. c9062a5d.virtua.com.br
0.0%   4   14.1 47.9 10.6 155.7  71.8
5. c9060776.virtua.com.br
0.0%   4   17.4 38.4 12.2 106.8  45.7
6. 209.85.244.43
0.0%   4   11.2 26.2 11.2 66.7   27.0
7. 209.85.245.151
0.0%   4   12.5 23.8 12.1 54.7   20.6
8. gru06s10-in-f3.1e100.net
0.0%   4   11.0 15.3 11.0 21.9   5.1
```

## 27.41 [netads]

Utilizado para testes de comunicação, integração de domínios, pesquisa e lista de uma base Active Directory do Windows.

### Modo de uso

```
admin >netads -h
Usage:
netads info          Display details on remote ADS server
netads join           Join the local machine to ADS realm
netads testjoin        Validate machine account
netads leave           Remove the local machine from ADS
netads status          Display machine account details
netads user            List/modify users
netads group           List/modify groups
netads dns             Issue dynamic DNS update
netads password        Change user passwords
netads changetrustpw   Change trust account password
netads printer          List/modify printer entries
netads search           Issue LDAP search using filter
netads dn               Issue LDAP search by DN
netads sid              Issue LDAP search by SID
netads workgroup        Display workgroup name
netads lookup            Perform CLDAP query on DC
netads keytab           Manage local keytab file
netads gpo              Manage group policy objects
netads kerberos         Manage kerberos keytab
netads enctype          List/modify supported encryption types
admin >
```

**Exemplo 1.:** Pesquisa dados do controlador de domínio especificado da rede.

```
admin >netads info 192.168.1.201
LDAP server: 192.168.1.201
LDAP server name: bblab-S2K12.labblockbit.com
Realm: LABBLOCKBIT.COM
Bind Path: dc=LABBLOCKBIT,dc=COM
LDAP port: 389
Server time: Qui, 01 Set 2016 17:50:21 BRT
KDC server: 192.168.1.201
Server time offset: 40
```

**Exemplo 2.: Testes de integração com o controlador de domínio da rede**

```
admin >netads join -U administrador
Enter administrador's password:
Using short domain name -- LABBLOCKBIT
Joined 'UTM11' to dns domain 'labblockbit.com'
admin >
```

---

**27.42 [nslookup]**

Utilizado para enviar demandas de pesquisa DNS para um servidor DNS remoto. Pode ser utilizado de forma interativa ou não.

**Modo de uso**

**Exemplo:** Solicitar a pesquisa referente um domínio específico para um servidor DNS.

```
admin >nslookup exemplo.org 208.67.222.222
Server:      208.67.222.222
Address:     208.67.222.222#53

Non-authoritative answer:
Name:   exemplo.org
Address: 195.22.8.70

admin >
```

---

**27.43 [ntpdate]**

Utilizado para ajustar a data e hora local do seu servidor consultando servidores NTP (Network Time Protocol) disponíveis na rede para determinar a hora correta.

**Modo de uso**

```
admin >ntpdate -h

/sbin/ntpdate: unknown option -h
usage: /sbin/ntpdate [-46bBdqsv] [-a key#] [-e delay] [-k file] [-p samples]
[-o version#] [-t timeo] [-U username] server ...
```

**Exemplo:** Atualizando a data e hora com os servidores NTP público.

```
admin >ntpdate a.ntp.br
1 Sep 18:06:33 ntpdate[8569]: adjust time server 200.160.0.8 offset -0.000371 sec
admin >
```

## 27.44 [parted]

Utilitário usado para manipular sistemas de arquivos e partições de discos. Geralmente será utilizado para particionamento de discos externos.

### Modo de uso

```
admin >parted
GNU Parted 3.2
Usando /dev/sda
Bem vindo ao GNU Parted! Digite 'help' para ver uma lista de comandos.
(parted)

(parted) help
  align-check TIPO N                         verifica a partição N para
  alinhamento de TIPO(mínimo|ideal)
  help [COMANDO]                            exibe a ajuda geral, ou ajuda para
  o COMANDO
  mklabel,mktable TIPO-RÓTULO              cria um novo rótulo de disco (na
  tabela de partição)
  mkpart TIPO-PART [TIPO-SISTARQ] INÍCIO FIM    cria uma partição
  name NÚMERO NOME                          renomeia a partição NÚMERO para
  NOME
  print [devices|free|list,all|NÚMERO]        exibe a tabela de partições,
  dispositivos disponíveis, espaço livre, todas as partições encontradas ou uma
  partição específica
  quit                                     sai do programa
  rescue INÍCIO FIM                         recupera uma partição perdida
  próxima do INÍCIO e FIM
  resizepart NÚMERO FIM                     redimensiona a partição NÚMERO
  rm NÚMERO                                apaga a partição NÚMERO
  select DISPOSITIVO                      escolhe o dispositivo para editar
  disk_set OPÇÃO ESTADO                   muda o estado de OPÇÃO no
  dispositivo selecionado
  disk_toggle [OPÇÃO]                      alterna o estado de OPÇÃO no
  dispositivo selecionado
  set NÚMERO OPÇÃO ESTADO                 muda a OPÇÃO na partição NÚMERO
  toggle [NÚMERO [OPÇÃO]]                  alterna o estado de OPÇÃO no NÚMERO
  da partição
  unit UNIDADE                             define como unidade padrão UNIDADE
  version                                  exibe o número da versão e
  informações de direitos autorais do GNU Parted
(parted)
```

---

## 27.45 [passwd]

Utilizado para definição, alteração da senha do usuário “admin” padrão do console.

### Modo de uso

```
admin >passwd
Mudando senha para o usuário admin.
Mudando senha para admin.
Senha UNIX (atual):
Nova senha:
Redigite a nova senha:
passwd: todos os tokens de autenticações foram atualizados com sucesso.
admin >
```

---

## 27.46 [ping]

Utilizado para testar a conectividade entre dispositivos na rede. Utiliza o datagrama do protocolo ICMP.

### Modo de uso

```
admin >ping 192.168.1.99
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_seq=1 ttl=128 time=2.65 ms
64 bytes from 192.168.1.99: icmp_seq=2 ttl=128 time=1.55 ms
64 bytes from 192.168.1.99: icmp_seq=3 ttl=128 time=6.86 ms
64 bytes from 192.168.1.99: icmp_seq=4 ttl=128 time=4.16 ms
64 bytes from 192.168.1.99: icmp_seq=5 ttl=128 time=16.5 ms
64 bytes from 192.168.1.99: icmp_seq=6 ttl=128 time=1.87 ms
64 bytes from 192.168.1.99: icmp_seq=7 ttl=128 time=4.58 ms
64 bytes from 192.168.1.99: icmp_seq=8 ttl=128 time=2.20 ms
64 bytes from 192.168.1.99: icmp_seq=9 ttl=128 time=1.61 ms
64 bytes from 192.168.1.99: icmp_seq=10 ttl=128 time=3.89 ms
^C
--- 192.168.1.99 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 1.553/4.598/16.589/4.298 ms
admin >
```

## 27.47 [reboot]

Utilizado para reinicializar o sistema.

**Modo de uso** [Saída padrão do comando]

```
admin >reboot
Connection to 192.168.1.1 closed by remote host.
Connection to 192.168.1.1 closed.
```

---

## 27.48 [reset-admin-blocks]

Utilizado para liberar sessões bloqueadas do usuário “*admin*” da interface WEB.

**Modo de uso** [Saída padrão do comando]

```
admin >reset-admin-blocks
blocked sessions removed
admin >
```

---

## 27.49 [reset-admin-password]

Utilizado para aplicar um reset (anular) a senha do usuário “*admin*” da interface WEB. Automaticamente é solicitado reaplicar uma nova senha.

**Modo de uso** [ Saída padrão do comando]

```
admin >reset-admin-password
Type admin password:
Re-type admin password:
admin >
```

---

## 27.50 [reset-admin-sessions]

Utilizado para remover as sessões “Ativas” do usuário “admin” da interface WEB.

**Modo de uso** [Saída padrão do comando]

```
admin >reset-admin-sessions
admin sessions removed
admin >
```

---

## 27.51 [route]

Utilizado para exibir e manipular a tabela de roteamento de endereços IPs.

**Modo de uso**

```
admin >route -h
Uso: route [-nNvee] [-FC] [famílias_de_endereços]   Lista as tabelas de roteamento do kernel
          route [-v] [-FC] {add|del|flush} ...           Modifica tabela de roteamento da família.

          route {-h|--help} [família_de_endereços]      Sintaxe para a AF (Família de endereços) especificada.
          route {-V|--version}                         Mostra a versão do comando e sai.
          -v, --verbose                            listagem detalhada
          -n, --numeric                           don't resolve names
          -e, --extend                            mostra outras/mais informações
          -F, --fib                               mostra a Base de Informações de Repasse (default)
          -C, --cache                            mostra cache de roteamento no lugar da FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
Lista das famílias de endereços possíveis (que suportam roteamento):
  inet (DARPA Internet)  inet6 (IPv6)  ax25 (AX.25 AMPR)
  netrom (NET/ROM AMPR)  ipx (Novell IPX)  ddp (Appletalk DDP)
  x25 (CCITT X.25)
admin >
```

**ATENÇÃO:** Rotas estáticas adicionadas através da console CLI (linha de comando) não são salvas e não são carregadas após o boot.

**Exemplo 1.: [Saída padrão do comando]**

```
admin >route -n
Tabela de Roteamento IP do Kernel
Destino      Roteador      MáscaraGen.      Opções Métrica Ref   Uso Iface
0.0.0.0      192.168.0.1    0.0.0.0          UG     0      0       0 eth1
192.168.0.0   0.0.0.0      255.255.255.0    U      0      0       0 eth1
192.168.1.0   0.0.0.0      255.255.255.0    U      0      0       0 eth0
admin >
```

**Exemplo 2:** Configurando um roteamento estático para uma rede extendida.

```
admin >route add -net 192.168.254.0/24 gw 172.16.102.1 dev eth3
admin >
admin >route -n
Tabela de Roteamento IP do Kernel
Destino      Roteador      MáscaraGen.      Opções Métrica Ref   Uso Iface
0.0.0.0      192.168.0.1    0.0.0.0          UG     0      0       0 eth1
172.16.102.0 0.0.0.0      255.255.255.0    U      0      0       0 eth3
192.168.0.0   0.0.0.0      255.255.255.0    U      0      0       0 eth1
192.168.1.0   0.0.0.0      255.255.255.0    U      0      0       0 eth0
192.168.254.0 172.16.102.1 255.255.255.0    UG     0      0       0 eth3
admin >
```

---

**27.52 [service-start]**

Utilizado para recarregar os serviços BLOCKBIT UTM.

**Modo de uso**

```
admin >service-start -h
usage: service-start <service-name>

blockbit-db      enabled:active
blockbit-shell    enabled:active
blockbit-admin    enabled:active
blockbit-auth     enabled:active
blockbit-proxy    enabled:active
blockbit-icap     enabled:active
blockbit-ips      enabled:active
blockbit-atp      enabled:active
blockbit-dhcp     enabled:active
blockbit-dns      disabled:unknown
blockbit-vpn-ipsec enabled:active
blockbit-vpn-ssl   enabled:active
admin >
```

**Exemplo:** Reiniciando o serviço de proxy

```
admin >service-start blockbit-proxy  
admin >
```

---

## 27.53 [service-stop]

Utilizado para desligar “parar” serviços do sistema. O nome do serviço deve especificado pelo comando.

**Modo de uso** [Saída padrão do comando]

```
admin >service-stop blockbit-vpn-ssl  
admin >
```

---

## 27.54 [service-status]

Exibe todos os serviços do sistema e o status atual.

**Modo de uso** [Saída padrão do comando]

```
admin >service-status  
blockbit-db           enabled:active  
blockbit-shell         enabled:active  
blockbit-admin         enabled:active  
blockbit-auth          enabled:active  
blockbit-proxy         enabled:active  
blockbit-icap          enabled:active  
blockbit-ips           enabled:active  
blockbit-atp           enabled:active  
blockbit-dhcp          enabled:active  
blockbit-dns            disabled:unknown  
blockbit-vpn-ipsec     enabled:active  
blockbit-vpn-ssl        enabled:active  
admin >
```

## 27.55 [show-auth-sessions]

Exibe as sessões dos usuários “Autenticados” no sistema BLOCKBIT UTM.

**Modo de uso** [Saída padrão do comando]

```
admin >show-auth-sessions
173144986235cd738121ad81ba815a19|1468410789|1468410789|dmorais@blockbit.com|172
.16.12.82|172.16.12.82|6c:f0:49:f0:cc:1e|OMNE WinAgent/3.0 (Microsoft Windows
NT 6.2.9200.0) .NET Framework/2.0.50727.8000|0|600
194a50c8765939ca74cbb968eb425154|1468405524|1468405524|cbrandao@blockbit.com|17
2.16.12.92|172.16.12.92|5c:c9:d3:56:11:c2|OMNE WinAgent/3.0 (Microsoft Windows
NT 6.2.9200.0) .NET Framework/2.0.50727.8000|0|600
57ddcb336098c149eebca22604e3a01a|1468408450|1468408450|toliveira@blockbit.com|1
72.16.12.89|172.16.12.89|1c:87:2c:c5:9c:4a|OMNE WinAgent/3.0 (Microsoft Windows
NT 6.2.9200.0) .NET Framework/2.0.50727.8000|0|600
```

---

## 27.56 [show-uuid]

Exibe o número de identificação do Appliance BLOCKBIT, esse ID é utilizado na identificação do hardware para validação da licença de uso.

**Modo de uso** [Saída padrão do comando]

```
admin >show-uuid
BlockBit Network Appliance UUID
94248368-3E53-11E6-AE26-EDD8677A1442
admin >
```

---

## 27.57 [show-vpn-info]

Exibe as informações da conexão, tais como: status, tráfego, tempo de atividade e estabelecimento da VPN IPSEC em operação e etc.

**Modo de uso** [Saída padrão do comando]

```
admin >show-vpn-info
  uptime: 3 hours, since Jul 14 10:53:29 2016
  malloc: sbrk 2727936, mmap 0, used 554592, free 2173344
  worker threads: 7 of 16 idle, 5/0/4/0 working, job queue: 0/0/0/0, scheduled: 8
Listening IP addresses:
  172.16.12.1
  192.168.0.2
  172.16.101.1
  172.16.102.1
  192.168.31.1
Connections:
  tun1: %any...187.8.187.66,0.0.0.0/0,::/0  IKEv2, dpddelay=10s
    tun1: local: [189.120.3.237] uses pre-shared key authentication
    authentication
      tun1: child: 172.16.12.0/23 172.16.20.0/24 172.16.102.0/24
  172.16.101.0/24 === 192.168.254.0/24 192.168.253.0/24 192.168.251.0/24 TUNNEL,
  dpdaction=restart
Security Associations (1 up, 0 connecting):
  tun1[2]: ESTABLISHED 56 minutes ago,
  192.168.0.2[189.120.3.237]...187.8.187.66[187.8.187.66]
    tun1[2]: IKEv2 SPIs: 1699a9f13c925cc6_i* 2452cf28b84353a8_r, pre-shared
    key reauthentication in 111 minutes
      tun1[2]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
      tun1{1}: INSTALLED, TUNNEL, ESP in UDP SPIs: 24017973_i c180bc7d_o
      tun1{1}: AES_CBC_256/HMAC_SHA1_96, 111679017 bytes_i (98292 pkts, 0s
ago), 5659513 bytes_o (65119 pkts, 0s ago), rekeying in 43 minutes
admin >
```

## 27.58 [show-vpn-conn]

Exibe os túneis de VPN IPSEC estabelecidos, e as informações básicas da configuração dos túneis, tais como: tipo de conexão (IKE v1/IKEv2, end. IPs dos pontos remotos e local, tempo de conexão, as redes conectadas sob a rede VPN (local/ remota).

**Modo de uso** [Saída padrão do comando]

```
admin >show-vpn-conn
tun1: #2, ESTABLISHED, IKEv2, 1699a9f13c925cc6:2452cf28b84353a8
    local '189.120.3.237' @ 192.168.0.2
    remote '187.8.187.66' @ 187.8.187.66
    AES_CBC-256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024
    established 3311s ago, reauth in 6734s
    tun1: #1, INSTALLED, TUNNEL-in-UDP, ESP:AES_CBC-256/HMAC_SHA1_96
        installed 297 ago, rekeying in 2706s, expires in 3304s
        in 24017973, 86460386 bytes, 78047 packets,      0s ago
        out c180bc7d, 4796101 bytes, 52833 packets,      0s ago
        local  172.16.12.0/23 172.16.20.0/24 172.16.102.0/24 172.16.101.0/24
        remote 192.168.254.0/24 192.168.253.0/24 192.168.251.0/24
admin >
```

---

## 27.59 [speedtest]

Utilizado para testes de conexão e identificação da taxa de transferência no tráfego de upstream e downstream de conexões e links?

**Modo de uso** [Saída padrão do comando]

```
admin >speedtest
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from NET Virtua (191.188.68.84)...
Selecting best server based on latency...
Hosted by JP PROVIDERS (Sao Paulo) [8.07 km]: 17.219 ms
Testing download speed.............................
Download: 30.03 Mbits/s
Testing upload speed.............................
Upload: 2.89 Mbits/s
admin >
```

## 27.60 [tcpdump]

É uma ferramenta de monitoração e sniffer utilizada para realizar captura e análise de pacotes que estão sendo transmitidos através da rede. Assim, ela permite o administrador analisar o comportamento da rede auxiliando na identificação de problemas, estações infectadas, tráfego malicioso, gargalos, etc.

### Modo de uso

```
admin >tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbdDefhHIJKLNOpqRStuUvxX] [ -B size ] [ -c count ]
           [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
           [ -i interface ] [ -j tstamptype ] [ -M secret ]
           [ -P in|out|inout ]
           [ -r file ] [ -s snaplen ] [ -T type ] [ -V file ] [ -w file ]
           [ -W filecount ] [ -y datalinktype ] [ -z command ]
           [ -Z user ] [ expression ]
admin >
```

**Exemplo:** Monitorando todo o tráfego da interface da rede local – interface Eth0.

```
admin >tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:35:53.129859 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 220346669, win
53006, length 0
20:35:53.133304 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.142155 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 1:189, ack 0,
win 21, length 188
20:35:53.142216 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 189:225, ack
0, win 21, length 36
20:35:53.142419 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 225, win 52950,
length 0
20:35:53.144878 IP utm.28489 > 172.16.13.245.domain: 49669+ PTR?
80.12.16.172.in-addr.arpa. (43)
20:35:53.145312 IP 172.16.13.245.58067 > google-public-dns-a.google.com.domain:
12406+ [1au] PTR? 80.12.16.172.in-addr.arpa. (54)
20:35:53.151967 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.158607 IP google-public-dns-a.google.com.domain > 172.16.13.245.58067:
12406 NXDomain 0/0/1 (54)
20:35:53.158889 IP 172.16.13.245.domain > utm.28489: 49669 NXDomain 0/0/0 (43)
Admin >
```

## 27.61 [tcptop]

Utiliza recursos do comando “*tcpdump*” para extrair e exibir informações de tráfego das interfaces de rede do servidor. Tais como: Total de pacotes capturados, total de pacotes recebidos, total de pacotes bloqueados pelo kernel e o total de pacotes trafegados pelo TOP 10 endereços IP.

### Modo de uso

```
admin >tcptop
you must specify the interface: [eth0,eth1 ...]
admin >
```

**Exemplo:** Exibir informações de tráfego top 10 da interface eth1.

```
admin >tcptop eth1
Wait capturing frames ...
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
10000 packets captured
10070 packets received by filter
21 packets dropped by kernel
    3268 IP 177.185.5.137
    3090 IP 192.168.0.2
    1626 IP 192.168.3.2
        481 IP 201.86.139.109
        290 IP 8.8.8.8 > 192
        288 IP 192.168.3.2 > 8
        246 IP 201.31.172.3
admin >
```

---

## 27.62 [tcptrack]

Exibe informações das conexões TCP de uma determinada interface de rede. Ele monitora as conexões e exibe seu status, end. IP de origem. End. IP de destino, consumo de banda.

### Modo de uso

```
admin >tcptrack
Usage: tcptrack [-dfhv] [-r <seconds>] -i <interface> [<filter expression>] [-T <pcap file>]
admin >
```

**Exemplo:** [Saída padrão do comando]

```
admin >tcptrack -i eth0

Client           Server           State      Idle A Speed
192.168.1.99:58944 192.168.1.1:22 ESTABLISHED 0s      3 KB/s
192.168.1.125:25301 192.168.1.1:80 ESTABLISHED 0s     235 KB/s
192.168.1.80:36524 192.168.1.1:98 ESTABLISHED 0s     189 KB/s
```

---

## 27.63 [telnet]

Utilizado para acesso remoto e testes de simulação de um terminal. Pode ser utilizado para teste de resposta de conexão de um serviço e até testes de envio de uma mensagem de e-mail.

### Modo de uso

```
admin >telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
            [-n tracefile] [-b hostalias] [-r]
            [host-name [port]]
admin >
```

**Exemplo:** [Saída padrão do comando]

```
admin >telnet
telnet> ?
Commands may be abbreviated. Commands are:

close          close current connection
logout         forcibly logout remote user and close the connection
display        display operating parameters
mode           try to enter line or character mode ('mode ?' for more)
open           connect to a site
quit           exit telnet
send            transmit special characters ('send ?' for more)
set             set operating parameters ('set ?' for more)
unset           unset operating parameters ('unset ?' for more)
status          print status information
toggle          toggle operating parameters ('toggle ?' for more)
slc            change state of special characters ('slc ?' for more)
z               suspend telnet
!               invoke a subshell
environ        change environment variables ('environ ?' for more)
?               print help information
telnet>
```

**Exemplo 1:** Testes de conexão com um serviço remoto Ts (terminal Service) em uma porta específica.

```
admin >telnet 172.16.13.245 3389
Trying 172.16.13.245...
Connected to 172.16.13.245.
Escape character is '^'.
```

**Exemplo 2:** Testes de conexão com um serviço remoto em uma porta específica com a resposta de falha na conexão.

```
admin >telnet 172.16.102.11 22
Trying 172.16.102.11...
telnet: connect to address 172.16.102.11: Connection timed out
admin >
```

## 27.64 [tracepath]

Traça um caminho para um endereço de rede designada , informando sobre o “tempo de vida ” ou lag TTL e a unidade de transmissão máxima (MTU ) ao longo do caminho .

### Modo de uso

```
admin >tracepath -h
Usage: tracepath [-n] [-b] [-l <len>] [-p port] <destination>
admin >
```

**Exemplo:** Testes para traçar o roteamento ou caminho até o end. [www.google.com.br](http://www.google.com.br) especificando a porta TCP/80 (http).

```
admin >tracepath -p 3389 172.16.13.245
1?: [LOCALHOST]                                     pmtu 1500
1: 172.16.13.245                                    0.555ms reached
    Resume: pmtu 1500 hops 1 back 128
admin >tracepath -n -b -p 80 www.google.com
1?: [LOCALHOST]                                     pmtu 1500
1: 10.70.64.1 (10.70.64.1)                         13.510ms
1: 10.70.64.1 (10.70.64.1)                         12.625ms
2: 201.6.37.65 (c9062541.virtua.com.br)           12.592ms
```

```
3: 201.6.40.37 (c9062825.virtua.com.br)           11.712ms
4: 201.6.42.93 (c9062a5d.virtua.com.br)           11.800ms
5: no reply
6: no reply
7: no reply
8: no reply
9: no reply
10: no reply
11: no reply
12: no reply
13: no reply
14: no reply
15: no reply
16: no reply
17: no reply
18: no reply
19: no reply
20: no reply
21: no reply
22: no reply
23: no reply
24: no reply
25: no reply
26: no reply
27: no reply
28: no reply
29: no reply
30: no reply
31: no reply
Too many hops: pmtu 1500
Resume: pmtu 1500
admin >
```

---

## 27.65 [traceroute]

Esse comando tem a mesma função do comando “*tracepath*”, traça um caminho para um endereço de rede designada. O comando “*traceroute*” suporta alguns parâmetros avançados que o diferencia do “*tracepath*”, incluindo a seleção de protocolos, como: TCP, Udp ou ICMP, em etc.

### Modo de uso

```
admin >traceroute --help
Usage:
traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ]
[ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w
waittime ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ]
host [ packetlen ]
```

```

Options:
  -4                      Use IPv4
  -6                      Use IPv6
  -d --debug              Enable socket level debugging
  -F --dont-fragment      Do not fragment packets
  -f first_ttl --first=first_ttl
                          Start from the first_ttl hop (instead from 1)
  -g gate,... --gateway=gate,...
                          Route packets through the specified gateway
                          (maximum 8 for IPv4 and 127 for IPv6)
  -I --icmp               Use ICMP ECHO for tracerouting
  -T --tcp                Use TCP SYN for tracerouting (default port is 80)
  -i device --interface=device
                          Specify a network interface to operate with
  -m max_ttl --max-hops=max_ttl
                          Set the max number of hops (max TTL to be
                          reached). Default is 30
  -N squeries --sim-queries=squeries
                          Set the number of probes to be tried
                          simultaneously (default is 16)
  -n                      Do not resolve IP addresses to their domain names
  -p port --port=port
                          Set the destination port to use. It is either
                          initial udp port value for "default" method
                          (incremented by each probe, default is
                          33434), or initial seq for "icmp" incremented
                          as well, default from 1), or some constant
                          destination port for other methods (with default of
                          80      for "tcp", 53 for "udp", etc.)
  -t tos --tos=tos
                          Set the TOS (IPv4 type of service) or TC (IPv6
                          traffic class) value for outgoing packets
  -l flow_label --flowlabel=flow_label
                          Use specified flow_label for IPv6 packets
  -w waittime --wait=waittime
                          Set the number of seconds to wait for response
                          to a probe (default is 5.0). Non-integer (float
                          point) values allowed too
  -q nqueries --queries=nqueries
                          Set the number of probes per each hop. Default is 3
  -r
                          Bypass the normal routing and send directly to a
                          host on an attached network
  -s src_addr --source=src_addr
                          Use source src_addr for outgoing packets
  -z sendwait --sendwait=sendwait
                          Minimal time interval between probes (default 0).
                          If the value is more than 10, then it specifies a
                          number in milliseconds, else it is a number of
                          seconds (float point values allowed too)
  -e --extensions
  -A --as-path-lookups
                          how ICMP extensions (if present), including MPLS
                          Perform AS path lookups in routing registries and
                          print results directly after the corresponding
                          addresses
  -M name --module=name
                          Use specified module (either builtin or external)
                          for traceroute operations. Most methods have
                          their shortcuts ('-I' means '-M icmp' etc.)

```

```

-O OPTS,... --options=OPTS,...
    Use module-specific option OPTS for the
    traceroute module. Several OPTS allowed,
    separated by comma. If OPTS is "help", print
    info about available options

--sport=num
    Use source port num for outgoing packets.
    Implies '-N 1'

--fwmark=num
-U --udp
    Set firewall mark for outgoing packets
    Use UDP to particular port for tracerouting
    (instead of increasing the port per each probe),
    default port is 53

-UL
    Use UDPLITE for tracerouting (default dest port
    is 53)

-D --dccp
    Use DCCP Request for tracerouting (default port
    is 33434)

-P prot --protocol=prot
    Use raw packet of protocol prot for tracerouting

--mtu
    Discover MTU along the path being traced. Implies
    '-F -N 1'

--back
    Guess the number of hops in the backward path and
    print if it differs

-V --version
    Print version info and exit

--help
    Read this help and exit

Arguments:
+ host          The host to traceroute to
    packetlen   The full packet length (default is the length of an IP
                header plus 40). Can be ignored or increased to a minimal
                allowed value

admin >

```

**Exemplo:** Testes para traçar o roteamento ou caminho até o end. IP de DNS da Google IP 8.8.8.8 no protocolo UDP(17).

```

admin >traceroute -n -p 53 -t 17 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.70.64.1  15.412 ms  15.242 ms  15.152 ms
 2  201.6.37.65  15.607 ms  15.618 ms  15.566 ms
 3  201.6.40.37  15.511 ms  16.380 ms  21.774 ms
 4  201.6.42.93  22.970 ms  22.917 ms  22.697 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
...
27  * * *
28  * * *
29  * * *
30  * * *
admin >

```

## 27.66 [update-blockbit]

Utilizado para verificação, download e instalação dos pacotes de atualização do BLOCKBIT UTM

**Modo de uso** [Saída padrão do comando]

```
admin >update-blockbit -h
Loaded plugins: fastestmirror
bases-local                                         | 2.9 kB  00:00:00
centos-local                                         | 2.9 kB  00:00:00
epel-local                                           | 2.9 kB  00:00:00
lux-local                                            | 2.9 kB  00:00:00
utm-local                                            | 2.9 kB  00:00:00
Loading mirror speeds from cached hostfile
Metadata Cache Created
omne-apply-update: running
omne-apply-update: test connection on: updates.blockbit.com
omne-apply-update: test connection on: license.blockbit.com
omne-apply-update: update packages
Loaded plugins: fastestmirror
bases-local                                         | 2.9 kB  00:00:00
centos-local                                         | 2.9 kB  00:00:00
epel-local                                           | 2.9 kB  00:00:00
lux-local                                            | 2.9 kB  00:00:00
utm-local                                            | 2.9 kB  00:00:00
Loading mirror speeds from cached hostfile
No packages marked for update
omne-apply-update: not found malwares in cache
omne-apply-update: not found url's in cache
omne-apply-update: finish
admin >
```

---

## 27.67 [update-license]

Utilizado para verificação e validação da licença de uso do sistema BLOCKBIT UTM.

**Modo de uso**

```
admin >update-license
status:false
admin >
```

## 27.68 [rewizard]

Utilizado para aplicar um reset (anular) as configurações do servidor BLOCKBIT UTM. Este comando só deve ser usado em casos que necessite realmente de reconfiguração total do sistema.

**Modo de uso** [Saída padrão do comando]

```
admin >rewizard -d
Do you want to reset this device (y/n)?y
omne-apply-cluster-reset: running
omne-apply-cluster-reset: stop postgres
omne-apply-cluster-reset: remove wizard flag
omne-apply-cluster-reset: remove databases
omne-apply-cluster-reset: remove sessions
omne-apply-cluster-reset: remove known_hosts
omne-apply-cluster-reset: finish
admin >
```

---

## 27.69 [shutdown]

Desliga ou reinicializa o sistema.

**Modo de uso** [Saída padrão do comando]

```
admin >shutdown -h
Connection to 192.168.1.1 closed by remote host.
Connection to 192.168.1.1 closed.
```

---

## 27.70 [exit]

O comando [exit] é utilizado para abandonar a sessão.

**Modo de uso**

```
admin >exit
```





It's easy to be secure.

[www.blockbit.com](http://www.blockbit.com)

**AMÉRICA DO NORTE (Sede)**

1450 Brickell Avenue – 14th floor  
Miami – FL – 33131  
UNITED STATES  
Tel: +1 305 373 4660

**EUROPA (Escritório Principal)**

2 Kingdom Street – 6th floor  
Paddington – London – W2 6JP  
UNITED KINGDOM  
Tel: +44 203 580 4321

**AMÉRICA LATINA (Escritório Principal)**

R. Eng. Francisco Pitta Brito, 779 - 3º andar  
São Paulo – SP – 04753-080  
BRASIL  
Tel: +55 11 2165 8888